# Bachelorthesis

## Gebäudeautomation mit Smart Home und deren Herausforderungen an die IT-Sicherheit

**Vorgelegt am:** 22.08.2016

**Von:** Tobias Pietzsch

Gartenstraße 14

08496 Neumark / OT Reuth

**Studiengang:** Wirtschaft

**Studienrichtung:** Wirtschaftsinformatik

**Seminargruppe:** WI13

**Matrikelnummer:** 4001456

**Praxispartner:** ESRA GmbH

Friedenstraße 64

08468 Reichenbach im Vogtland

**Gutachter:** B.A. Simon Strobel (ESRA GmbH)

Prof. Dr. Rainer Penzel (Staatliche Studienakademie Glauchau)

# Freigabeerklärung

Hiermit erklären wir uns einverstanden/nicht einverstanden*), dass die Bachelor-Thesis / ~~Diplomarbeit~~*) der/des Studenten/in

Name, Vorname: **Pietzsch, Tobias** SG: **WI13**

zur öffentlichen Einsichtnahme durch den Dokumentenserver der Bibliothek der Staatlichen Studienakademie Glauchau bereitgestellt wird.

Thema der Arbeit:
**Gebäudeautomation mit Smart Home und deren Herausforderungen an die IT-Sicherheit**.....

.....

.....

Reichenbach, 22.08.2016
.....
Ort, Datum

.....

Stempel, Unterschrift des Praxispartners

Arbeit zur Veröffentlichung freigegeben: ja □ nein □

…… …….
Datum Unterschrift Leiter/in d. Studiengang

*) Nichtzutreffendes bitte streichen

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| EIB | Europäischer Installationsbus |
| KNX | Kurzform von Konnex (Nachfolger EIB) |
| TAN | Transaktionsnummer |
| SMS | Short Message Service |
| SSL | Secure Layer Security |
| TLS | Transport Layer Security |
| AES | Advanced Encryption Standard |
| mW | Milliwatt |
| WLAN | Wireless Local Area Network |
| WPS | Wi-Fi Protected Setup |
| iOS | iPhone Software / Betriebssystem |
| API | Application Programming Interface |
| OS | Operation System |

# 1 Einleitung

Das Thema der Bachelorarbeit lautet „Gebäudeautomation mit Smart Home und deren Herausforderungen an die IT-Sicherheit“. Diese Arbeit soll die im vierten Semester angefertigte Studienarbeit mit dem Thema „Marktanalyse im Bereich Smart Home im Bezug für Eignung sicherheitstechnischer Anwendung und Möglichkeiten/ Schnittstellen zur Adaption bzw. Integration an professionelle sicherheitstechnischen Anlagen“ fortführen und ergänzen. Durch die Verknüpfung einer Smart Home Zentrale aus dem Hause HomeMatic mit einer professionellen Sicherheitsanlage aus dem Hause Jablotron, sollte eine Nutzung beider Systeme über die gleiche Steuerungseinheit erreicht werden. Ziel war die unkomplizierte Steuerung per Smartphone oder Bedienfeld an der Wand, umso den Luxus von Smart Home, aber auch die Sicherheit der professionellen Anlage, nutzen zu können. Durch diese Verknüpfung wurden aber erhebliche und nicht tragbare Sicherheitsrisiken festgestellt und die Weiterführung der Tests daraufhin eingestellt. Da die Technologie Smart Home aber einen stetig und rasant wachsenden Markt darstellt, soll dieses Thema mit Hilfe dieser Bachelorarbeit fortgeführt werden. Das Ziel dieser Arbeit ist es, auf Sicherheitsrisiken und mögliche Fehlbehandlungen mit Smart Home einzugehen um die Personen im Umgang mit dieser Technologie zu sensibilisieren. Durch das Vorrausschauen und Studieren dieser Marktentwicklung, ist es nur eine Frage der Zeit, bis diese Technologie in den unterschiedlichsten Gebäuden zum Einsatz kommt. In vielen Medienquellen hört man immer wieder über die Sicherheitsrisiken von Smart Home und dem intelligenten Haus. Das Smart Home eine potentielle Gefahr darstellt, vor allem in Bezug auf die Privatsphäre, steht außer Frage. Doch viele Menschen, vor allem die der Bundesrepublik Deutschland, treten dieser Technik noch mit großer Skepsis entgegen und wahren Distanz. In den USA dagegen nimmt Smart Home schon einen wichtigen Bestandteil von Gebäuden ein. Durch die ständigen Problemberichte über Smart Home, wird kein Vertrauen in diese Technologie vermittelt. Doch das das intelligent vernetzte Haus mittels Smart Home durchaus die häusliche Sicherheit revolutionieren kann, wird außer Acht gelassen. Eine bestehende Gefahr geht vor allem von dem Anwender aus, der diese Technologie falsch und unsachgemäß behandelt. Viele Smart Home Produkte sind von den Herstellern auf bekannte Sicherheitsmängel getestet und bei sachgemäßen Umgang für bedenkenlos erklärt worden. Doch die Nutzer selber stellen die Gefahr dar, und können durch ihr falsches Handeln oder ihr fehlendes Wissen die Sicherheitsrisiken und Bedrohungen hervorrufen, die in den Medien angeprangert werden. Die Nutzer müssen den sachgemäßen Umgang mit dieser Technik erlernen, aber auch darauf achten, dass die Abhängigkeit davon einen durchaus gefährdenden Faktor darstellen kann. Durch die immer weiter voranschreitende Digitalisierung unserer Umwelt und der Einsatz von computerbasierten Systemen in vielen

alltäglichen Dingen, zwingen die Menschen sich mit dieser Materie auseinanderzusetzen.

In dieser Bachelorarbeit soll gezielt auf die IT-Sicherheit eingegangen und Sicherheitsmängel in den Smart Home Systemen beschrieben werden. Dazu wird gezeigt, dass viele Sicherheitsmängel beseitigt werden können, wenn man seine eigene IT-Infrastruktur sicherer gestaltet und die Tipps, die in dieser Arbeit genannt werden befolgt. Somit steht einem „intelligent vernetzten Haus“ nichts mehr im Wege, was den Kriminellen das Handeln erschwert. Ganz nach dem Zitat von Manuel Schreiber: „Das Smart Home erleichtert das Leben, indem es all die Dinge automatisiert, die im Alltag nerven.“[1]

[1] Online: Manuel Schreiber, chip.de, 2015 (13.07.2016)

# 2 Gliederung und Vorgehensweise

Diese Bachelorarbeit ist in drei große Gebiete unterteilt und soll einen Einblick in die Notwendigkeit von IT-Sicherheit in Verbindung mit Smart Home geben. Als erstes soll es einen kleinen Exkurs in die Thematik Smart Home sowie IT-Sicherheit geben. Darunter wird die Definition von Smart Home fallen und diverse zukünftige Aussichten bezüglich dieser Technologie. Durch die immer weiter voranschreitende Digitalisierung unserer Umwelt entstehen immer mehr Daten, die verarbeitet werden müssen. Der dadurch entstehende Datenfluss spielt in der IT-Sicherheit eine große Rolle, denn durch den Einsatz von Technik in neuen Bereichen unseres Lebens, werden neue Daten generiert, die es vorher vermutlich nicht gab. Deshalb müssen diese neuen Daten sehr genau analysiert werden um mögliche Sicherheitsprobleme aufzudecken und dagegen vorzugehen .
Der zweite große Punkt in dieser Arbeit wird speziell die IT-Sicherheit von Smart Home betreffen. Darunter wird die eigentliche Definition von Sicherheit fallen. Das betrifft den allgemeinen Begriff Sicherheit sowie dessen Ausdehnung auf viele Lebensbereiche. Deshalb soll das Thema Sicherheit noch einmal speziell auf die IT-Sicherheit bezogen und bei diesem Thema wichtige Aspekte wie Schwachstellen und Angriffspunkte näher erläutert werden. Danach folgt die Sicherheitsbetrachtung von Smart Home. Dies wird noch einmal untergliedert in zwei Bereiche, Funkgesteuerte sowie Kabelgesteuerte Smart Home Produkte. Hier wird eine kurze Erläuterung der Funktionsweise sowie mögliche Sicherheitsrisiken aufgezeigt und genannt. Danach folgt die Erläuterung, der Notwendigkeit des Schutzes einer Hausautomation. In diesem Punkt werden die Sicherheitsrisiken an möglichen Schadensszenarien erläutert. Danach folgt die Betrachtung der Infrastruktur, denn auch die Beschaffenheit der Umgebung spielt für IT-Sicherheit eine sehr große Rolle. Es gibt wesentliche Unterschiede in der gewerblichen und in der privaten Anwendung, die in den Angriffszielen begründet sind. Ein weiterer Punkt soll danach die Betrachtung des Smartphones sein. Smartphones sind deshalb so wichtig bei der Betrachtung der IT-Sicherheit von Smart Home, weil diese Technik im überwiegendem Maße durch solche Endgeräte gesteuert wird und deshalb eine direkte Verbindung zu den Systemen existiert. Ist das Smartphone gefährdet, ist auch die Hausautomation einer Gefahr ausgesetzt. Hierbei soll aufgezeigt werden, wo die Unterschiede zwischen einem Android- und einem iOS-Gerät liegen. Dazu gibt es im Anhang einen praktischen Anwendungsfall, der zeigt wie einfach es ist, bei Android-Geräten Daten auszulesen und sich Zugriff darauf zu verschaffen. Der abschließende Punkt der Arbeit wird eine Empfehlung sein, wie man sein Eigenheim in Bezug auf IT-Sicherheit bei Einhaltung von Basisschutzmaßnahmen sicherer gestalten kann. Dazu soll ebenfalls eine kleine Checkliste im Angang zu finden sein, die unseren Mitarbeitern als Leitfaden zur Überprüfung der Smart Home Systeme dienen soll.

# 3 Einführung

## 3.1 Definition Smart Home

„Smart Home dient als Oberbegriff für technische Verfahren und Systeme in Wohnräumen und -häusern, in deren Mittelpunkt eine Erhöhung von Wohn- und Lebensqualität, Sicherheit und effizienter Energienutzung auf Basis vernetzter und fernsteuerbarer Geräte und Installationen sowie automatisierbarer Abläufe steht.“[2]
Die Möglichkeiten der Gebäudeautomation kann man in zwei wesentliche Anwendungsziele untergliedern. Eine Variante ist die Nutzung für private Zwecke, d.h. für Wohngebäude und die zweite Variante ist die Anwendung in öffentlichen Gebäuden wie z.B. Schulen, Büros oder Hotels.
Die Aufgaben eines Gebäudeautomationssystems bestehen dabei aus Steuerung, Regelung und Überwachung. Die Steuerung dient dazu, durch die Wahl einer oder mehrere Eingangsgrößen einen bestimmten Ausgangszustand hervorzurufen z.B. Anschalten der Innenraumbeleuchtung durch Betätigung eines Schalters. Die Regelung kann man bei der Temperaturkontrolle des Hauses anwenden, in dem ein Sollwert mit einem Istwert verglichen und dementsprechend gehandelt wird. Der letzte Punkt, die Überwachung, beobachtet den Istzustand und greift bei Veränderungen ein und reagiert dementsprechend darauf z.B. bei der Aktivierung eines Bewegungsmelders.[3]

## 3.2 Vor- und Nachteile Smart Home

Durch den Einsatz von Smart Home oder eines Systems zur Gebäudeautomation können einige Vor- und Nachteile entstehen, die nicht immer auf Anhieb erkennbar sind.

**Vorteile:**

- Energieeffizienz, Verbrauchsübersicht
- Komfortable Steuerung des Hauses
- Schutz vor Einbrüchen durch den Einsatz von Sicherheitskomponenten
- Schutz vor lebensbedrohenden Situationen z.B. Brandalarm

**Nachteile:**

- Höhere Anschaffungskosten
- Komplexität durch die vielen Möglichkeiten der Vernetzung
- Nachrüstung in älteren Gebäuden oft schwierig
- IT-Sicherheit ist nicht überall gegeben

[2] Online: wikipedia.org – Smart Home, 2015 (13.07.2016)
[3] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 8-9 (08.08.2016)

## 3.3 Zukunftsaussichten

Smart Home ist ein relativ neuer Markt der für viele Menschen, vor allem in Deutschland, noch große Skepsis hervorruft. Doch diese Technologie wird zukünftig eine große Rolle in unserem Leben spielen. Man kann sogar behaupten, dass diese Technik eine gleiche Entwicklung erlebt, wie die damalige Markteroberung durch Smartphones. Zu dieser Zeit war es eine technologische Revolution. Keine Tasten, große Displays und Internet für unterwegs. Doch auch diese vielen technischen Neuerungen und neuen Möglichkeiten der Handynutzung, schafften am Anfang eine gewisse Skepsis, vor allem bei den älteren Generationen. Es wurde als „Unsinn“ abgestempelt und als „technische Spielerei“ propagiert. Doch schaut man sich in den Städten Deutschlands um, sieht man nicht nur die Jugend mit Smartphones, sondern Menschen aller Altersgruppen. Man kann also ganz klar erkennen, dass diese Technologie ein Teil unseres Lebens darstellt und nicht mehr wegzudenken ist. Und genauso wird es in einigen Jahren mit Smart Home Systemen passieren. Dazu kommt, dass viele Neubauten schon heutzutage mit dieser Technologie ausgestattet werden. Es kann durchaus soweit kommen, das eine Ausrüstung oder Aufrüstung mit Smart Home, per Gesetz vorgeschrieben wird. Dies hat bereits mit der Pflicht zur Ausstattung von Neubauten mit Rauchmeldern begonnen. Dies könnte man mit Einbruchmeldeanlagen oder gewissen Energieeffizienzmaßnahmen fortsetzen. All diese Möglichkeiten bieten heute schon Smart Home Systeme und die Entwicklung geht noch weiter. Im Allgemeinen kann man behaupten, dass Smart Home eine nicht aufhaltbare Revolution im modernen Wohnen darstellt und bald einen festen Bestandteil in unserem sowie dem Leben der folgenden Generationen darstellen wird.

## 3.4 Der neue Datenfluss

In unserer heutigen Umwelt, gibt es kaum noch Bereiche, die nicht mit Computertechnik ausgestattet sind. Selbst das Aufschließen eines Autos, wird durch Computer überwacht und gesteuert. Was früher manuell gesteuert werden musste, wird heute durch eine Vielzahl an Technik unterstützt. Doch was in Autos schon heute zur Standardausführung zählt (KeyLess-Systeme) wird auch bald in vielen Wohnungen und Eigenheimen zum Einsatz kommen. Durch dieses Voranschreiten entstehen immer neue Möglichkeiten sein Leben von einem PC steuern und begleiten zu lassen. Doch durch diesen Einsatz entstehen immer neue und immer neuere Datenarten und höhere Datenmengen die verarbeitet werden müssen. Das bedeutet je weiter die Digitalisierung unsere Umwelt voranschreitet, desto mehr Rechentechnik und Speicherplatz benötigen wir, um die Datenmengen aufnehmen und verarbeiten zu können.

Leider ist es uns heute noch nicht möglich, diesen Datenfluss gezielt zu beeinflussen und zu steuern. Das Wissen über den Datenfluss ist deshalb so wichtig, da die Kenntnisse darüber einen großen Teil zur IT-Sicherheit beitragen. Je mehr über die eingesetzte Technik und die Funktionsweise bekannt ist, desto höher ist die Sicherheit. Jedoch ist unsere heutige Gesellschaft in dieser Weise noch recht gutgläubig und unwissend. Viele Smartphone-Nutzer wissen gar nicht welche Daten ihre Anwendungen und App´s generieren, geschweige denn, wo diese abgespeichert werden. In Sachen IT-Sicherheit und den Umgang mit ihrer eigenen digitalen Identität sind viele Personen zu naiv und glauben nicht das, was über Vorratsdatenspeicherung, wie von Eward Snowden aufgedeckt, und die NSA berichtet wird.

Durch die immer weiter steigende Anzahl der Daten, werden auch die Sicherheitsrisiken größer. Ein Beispiel hierfür sind Fitnessapplikationen die Herzfrequenz, Bewegung und vieles mehr aufzeichnen. Normalerweise sind ärztliche Informationen über die Patienten durch die ärztliche Schweigepflicht geschützt. Viele der Patienten wollen auch nicht, dass ihre Krankenakte offen liegt und irgendjemand über den gesundheitlichen Zustand ihres Körpers Bescheid weiß. Doch genau die gleichen Personen benutzen Fitness-Apps, die solch ein „Kranken- bzw. Fitnessbild“ eines jeden einzelnen erstellen können. Komischerweise ist dies für viele in Ordnung, da sie nicht wissen, dass auch diese Daten mit Sicherheit auf fremden Servern abgespeichert werden. Auch im Einsatz mit Smart Home werden sensible Daten generiert. So kann es sein, dass z.B. Zutrittskontrollen Informationen abspeichern, in welchen Abständen die Wohnung betreten oder verlassen wird. Dadurch ist auch ein erhebliches Maß an Datenschutz erforderlich, um zu verhindern, dass sensible Daten in falsche Hände geraten. Zum Beispiel durch die Aktivitätskontrolle der Wohnung durch Smart Home, können Kriminelle den besten Zeitpunkt für einen Einbruch auslesen. Deshalb ist es wichtig, seine Daten bestmöglich zu schützen. Die folgende Grafik soll die wachsenden Angriffsfläche im Internet darstellen und zeigen wie der Datenfluss durch voranschreitende Digitalisierung unserer Umwelt anschwillt.

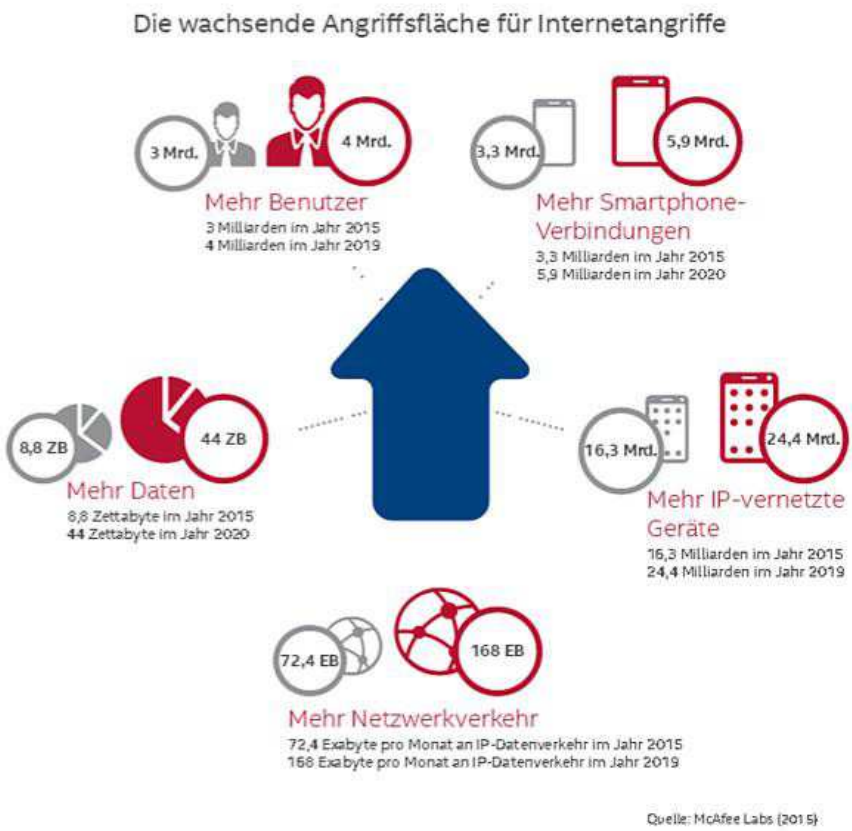


**Abbildung 1** Wachsende Angriffsfläche für Internetangriffe (online: internetworld.de, 2015, 15.07.2016)

# 4 Die Sicherheit von Smart Home

## 4.1 Definition von Sicherheit

Die Herkunft des Wortes Sicherheit stammt aus dem Lateinischen und bedeutet so viel wie sorglos sein („sēcūritās“; ursprünglich aus "sēcūrus" = "sorglos"[4]). Doch eine genaue Definition ist schwer zu finden, da jeder Mensch den Begriff individuell definiert und andere Sicherheitsvorstellungen besitzt. Im Grunde wird der Begriff Sicherheit in unserer heutigen Zeit in Zusammenhang mit „frei sein von Risiken und Gefahren“ gesetzt. Schaut man in das Rechtschreibwörterbuch von Konrad Duden, findet man eine Erklärung des Wortes Sicherheit:

„Zustand des Sicherseins, Geschützt sein vor Gefahr oder Schaden; höchstmögliches Freisein von Gefährdungen“[5]

## 4.2 Sicherheit aus heutiger Sicht

Das Thema Sicherheit spielt in unserer heutigen Welt eine noch größere Rolle als jemals zuvor. Jeden Tag sind unserer Medien durchzogen mit Terror und Gewalt und die Diskussionen über die Sicherheit und das Wohlergehen der Bevölkerung. Doch ein entscheidender Wandel in der Debatte der Sicherheit wurde durch den 11.Septemeber 2001 hervorgerufen, indem eine Terrorvereinigung das World Trade Center mit entführten Passagiermaschinen angriff und zerstörte. An diesem Tag verloren viele unschuldige Menschen ihr Leben.
Oft denkt man, dass der technologische Fortschritt dazu beiträgt, solche Terroranschläge künftig vereiteln zu können. Doch je mehr wir unsere Umwelt digitalisieren, umso mehr neue Gefahren können entstehen. In der westlichen Welt spielt vor allem die finanzielle Sicherheit und Möglichkeit der freien Entfaltung und Meinungsäußerung eine große Rolle. Dass diese Sicherheiten in vielen ärmeren Ländern geringere Rollen spielen und vielmehr eine gesicherte Ernährung bedeutend ist, ist jedem allgemein bekannt.
Aber auch die wirtschaftliche Sicherheit ist heutzutage von entscheidender Bedeutung, vor allem auch für die Bundesrepublik Deutschland. Die BRD ist eine der führenden Wirtschaftsnationen in der Europäischen Union und um dies weiterhin zu gewährleisten, ist ein großes Aufgebot an Sicherheitsmaßnahmen nötig. In diesem Punkt kommt die IT-Sicherheit ins Spiel, die in allen Lebensbereichen, wie sozial, wirtschaftlich und politische, zu einem Sicherheitsniveau beiträgt und vorausschauend bald das höchste Gut aller Sicherheiten in unserer Welt darstellen wird.

[4] Online: wertesysteme.de, 2014 (05.07.2016)
[5] Online: duden.de (05.07.2016)

## 4.3 Die Spezielle Rolle der IT-Sicherheit

Zu allen Aspekten der Sicherheit die in vorherigen Punkten behandelt wurden, vereint die IT-Sicherheit den Schutz von Kommunikations- und Informationstechnologien. In der modernen Welt spielt deshalb die IT-Sicherheit eine entscheidende Rolle, weil sie durchaus ausschlaggebend für andere Sicherheitsbereiche ist. So kommt es, dass heutzutage Politik und Wirtschaft auf eine funktionierende Sicherheit in IT-Bereichen angewiesen sind, um einen reibungslosen Ablauf zu gewährleisten. Somit hat sich die komplette Sicht auf das Thema Sicherheit gewandelt, denn was früher nur im direkten Zugriff möglich war, kann heute auch von der Ferne eingeleitet und gesteuert werden. Als Beispiel könnte man militärische Handlungen heranziehen. Was früher nur mit genug Arbeitskraft und Ressourcen möglich war, geht heute bequem aus der sicheren Entfernung eines Hauptquartiers. Bestes Beispiel wäre hierbei der kriegerische Einsatz von Drohnen. Durch diese globale Vernetzung hat sich unser Leben grundlegend geändert. Beherrscht man ein Computersystem oder zerstört es, kann ein Land im völligen Chaos versinken und das binnen weniger Stunden. Durch die Abhängigkeiten entstehen neue Risiken, die die IT-Sicherheit versucht zu neutralisieren. Die IT-Sicherheit wird deshalb, bald ein Hauptpunkt aller Sicherheitsbetrachtungen darstellen. Die folgenden Unterpunkte sollen die IT-Sicherheit besser verständlich machen und wichtige Begriffe, die in der IT-Sicherheit eine Rolle spielen, erklären.

### 4.3.1 Die Aspekte der IT-Sicherheit

Zu allererst sollte das Thema IT-Sicherheit nicht als statisches Problem bzw. Betrachtungsobjekt betrachtet werden, sondern als Dynamisches. Die IT-Sicherheit ist eine recht junge Thematik des komplexen Gebietes der Informationstechnologie. Sicherung von IT-Systemen war zu vergangenen Zeiten nicht nötig, da die Technik recht teuer war und somit nur für Fachexperten und Institute zur Verfügung stand. Doch durch die technologische Entwicklung besitzt nun fast jeder Haushalt mindestens einen PC mit Internetzugang. Ein Leben ohne die Technologie ist nicht mehr denkbar. Durch die immer weiter steigende Vernetzung und Komplexität von IT-Systemen bedarf es eines immer besseren Niveaus an IT-Sicherheit. Für eine wirksame IT-Sicherheit ist es deshalb wichtig zu wissen, was zu schützen ist und wovon die Bedrohungen ausgehen können. Denn jedes System hat unterschiedliche Anforderungen und nicht alles benötigt das gleiche Schutzbedarfsniveau. Für die Verwaltung und Verbesserung der IT-Sicherheit ist das IT-Sicherheitsmanagement verantwortlich. Dies wird in den nachfolgenden Punkten noch einmal kurz erläutert.[6]

[6] Online: Vgl. Stefan Sackmann, Enzyklopädie der Wirtschaftsinformatik, 2014 (06.07.2016)

### 4.3.2 Schutzziele und Bedrohungen

Die allgemeinen Punkte der Standard-Schutzziele in der IT-Sicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Die Vertraulichkeit beschäftigt sich vor allem mit der Vergabe der Informationen an den jeweiligen User. Das bedeutet, dass die Informationen nur diesen Personen zur Verfügung stehen, die entsprechende Rechte besitzen, die Informationen und Daten aufrufen und verarbeiten zu können. Ein Beispiel im privaten Sektor wäre die Passwortkontrolle der im Eigenheim eingesetzten IT-Systeme, egal ob Windows-PC oder Router. Haben Unbefugte darauf Zugriff, z.B. die Nachbarn, ist ein erheblicher Sicherheitsmangel gegeben. Die Integrität beschäftigt sich mit der Modifikation und Änderung von Daten. Dies ist besonders wichtig, um etwaige Änderungen nachvollziehen zu können. Somit dürfen keine unerlaubten Modifikationen vorgenommen werden, die unerkannt bleiben. Der letzte wichtige Punkt ist die Verfügbarkeit. Die Verfügbarkeit von Daten mit schnellen Zugriffszeiten ist ein absolutes Muss beim Einsatz von IT. Um einen reibungslosen Ablauf zu gewährleisten ist es auch erforderlich, redundante Systeme einzusetzen und eine Datensicherung zu implementieren.
Es gibt noch diverse andere wichtige Schutzziele wie zum Beispiel der Authentizität und Zurechenbarkeit. Jedoch würde eine so tiefgreifende Erklärung einzelner Schutzziele den Rahmen der Arbeit bei weitem sprengen.
Die Bedrohungen sind im Grunde genommen Gefährdungen der Schutzziele. Im IT-Sektor gibt es eine große Fülle an Bedrohungen und Risiken, die beachtet werden müssen. Bedrohungen sind immer potentielle Gefahren aus denen ein Schaden entstehen kann.[7]

### 4.3.3 Schwachstellen

Schwachstellen stellen in der IT-Sicherheit mögliche Angriffspunkte dar, die mit der Ausnutzung dieser, die Erreichung der geplanten Schutzziele verhindern. Die Arten von Schwachstellen können sehr vielseitig sein. Beispiele sind schlechte Designwahl, falsche Programmierung oder auch die Vernachlässigung der Betrachtung und die Analyse von Schwachstellen im Voraus. Die IT-Sicherheit hat deshalb die Aufgabe diese Schwachstellen zu finden und zu beseitigen. Dafür gibt es viele unterschiedliche Methoden und es bedarf einer gewissen Erfahrung um potentielle Schwachstellen aufspüren zu können. Trotz der Existenz von vielen analytischen Möglichkeiten ist die Identifikation jeder Schwachstelle nicht möglich und nicht durchsetzbar. Deshalb muss gleich am Anfang gesagt werden, dass eine hundertprozentige Sicherheit nie erreicht werden kann und nur ein Wunschdenken der Menschen darstellt.[8]

[7] Online: Vgl. Stefan Sackmann, Enzyklopädie der Wirtschaftsinformatik, 2014 (06.07.2016)
[8] Online: Vgl. Stefan Sackmann, Enzyklopädie der Wirtschaftsinformatik, 2014 (06.07.2016)

### 4.3.4 Angriffe

Angriffe sind die logischen Schlussfolgerungen bei der Entdeckung einer Schwachstelle. Ein Angriff kann viele unterschiedliche Absichten und Möglichketen besitzen. Man muss unterscheiden zwischen gezielten und nicht gezielten Angriffen. Nicht gezielte Angriffe Spam-Mails an viele tausend Adressaten ohne einen konkreten Zweck. Diese Angriffe sind oft schnell abzuwehren, jedoch im Umgang mit IT-Systemen täglich anzutreffen. Die eigentliche Betrachtung der IT-Sicherheit bezieht sich auf gezielte Angriffe eines Systems. Solche Angriffe werden durch eine geplante und durchgedachte Verfahrensweise angeführt und sind vor allem in gewerblichen oder staatlichen Einrichtungen anzutreffen. Beispiele für gezielte Angriffe wären die Smart Home Systeme von Hotels, Banken aber auch staatliche Institutionen. Hier wird der Zweck von Datendiebstahl, Sabotage aber auch Spionage verfolgt.[9]

### 4.3.5 Schutzmechanismen

Schutzmechanismen sind dazu da, bekannte Angriffe erfolgreich abzuwehren, die unter anderem mit Verschlüsselung und Unterbindung von unbefugten Zugriffen arbeiten. Um solche Schutzmechanismen erfolgreich platzieren zu können, bedarf es der Grundlagen der Kryptographie. Die daraus folgenden Mechanismen wie Verschlüsselung oder Zertifikation mit Hilfe digitaler Signaturen unterstützen die verschiedenen Schutzmechanismen. Eine andere Art von Angriffsschutz stellen diverse Programme dar, wie z.B. Antivirensoftware oder Malwareprogramme, die vor bekannten Würmern, Trojanern oder Viren schützen und so die mögliche Infizierung des Systems verhindern. Doch diese Arten von Schutzmechanismen sind elementar. Wichtig ist zu wissen, dass auch bei der Vielzahl an Möglichkeiten zum Systemschutz, immer ein Restrisiko besteht. Jedes System ist manipulierbar! Schutzmechanismen sind dazu da, diese Hackvorgänge so schwer und langwierig wie möglich zu gestalten. Ein sehr wirkungsvoller Schutzmechanismus ist und bleibt der korrekte und durchdachte Umgang mit möglichen Gefahren wie z.B. keine Mails unbekannter Herkunft zu öffnen.[10]

### 4.3.6 Management von IT-Sicherheit

IT-Sicherheit ist nicht nur dazu da, um potentielle Gefahren und Schwachstellen aufzuspüren, sondern vielmehr um ein gewisses Standardsicherheitsniveau zu halten. Dazu ist ein stetiger Lernprozess erforderlich, um auf mögliche Neuerungen angemessen reagieren und entdeckte Schwachstellen eliminieren zu können. Die Umsetzung der IT-Sicherheit ist ein komplexer und langwieriger Prozess. Das

[9] Online: Vgl. Stefan Sackmann, Enzyklopädie der Wirtschaftsinformatik, 2014 (06.07.2016)
[10] Online: Vgl. Stefan Sackmann, Enzyklopädie der Wirtschaftsinformatik, 2014 (06.07.2016)

Sicherheitsmanagement befasst sich mit der kompletten Aufgabenvielfalt zum Erreichen einer gesicherten IT (vgl. Abb.2). Die Einführung der Sicherheitskonzepte basieren auf Systemanalysen, Anwenderbefragungen sowie dem Erstellen und Testen von Konzepten. Von gleichrangiger Bedeutung ist die Beseitigung der potentiellen Gefahren wie die unsachgemäße Bedienung Daraus folgt die stetige Sensibilisierung der Anwender.
IT-Sicherheit wird in den nächsten Jahren noch ein größeres Aufgabengebiet umfassen. Somit gewinnt auch die IT-Sicherheit in Berufen zunehmend an Bedeutung, die sich nicht mit Computern und PCs beschäftigen. IT-Sicherheit ist der Grundbaustein für eine sichere und funktionierende IT-Infrastruktur.[11]

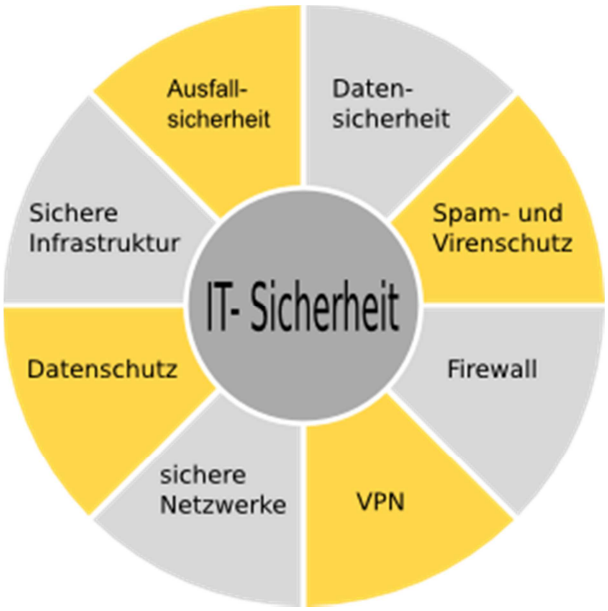


**Abbildung 2** Übersicht über die Aufgaben der IT-Sicherheit
(Online: linux-ag.com, 2012, 15.07.2016)

## 4.4 Mögliche Bedrohungen und Risiken von Smart Home

Durch die vielen Möglichkeiten von Angriffen und Bedrohungen aus der Sicht der IT-Sicherheit soll der nachfolgenden Abschnitt, die Angriffsmöglichkeiten auf Smart Home Systeme näher darstellen. Bei der Betrachtung von Smart Home spielen vor allem die Angriffsmöglichkeiten auf das Netzwerk und die Geräte bzw. deren Komponenten eine wesentliche Rolle. Möglichen Angriffsszenarien auf Hausautomationssysteme sollen in der folgenden Grafik (vgl. Abb. 3) verdeutlicht und im folgenden Abschnitt erläutert werden.

[11] Online: Vgl. Enzyklopädie der Wirtschaftsinformatik, Stefan Sackmann, 2014 (06.07.2016)

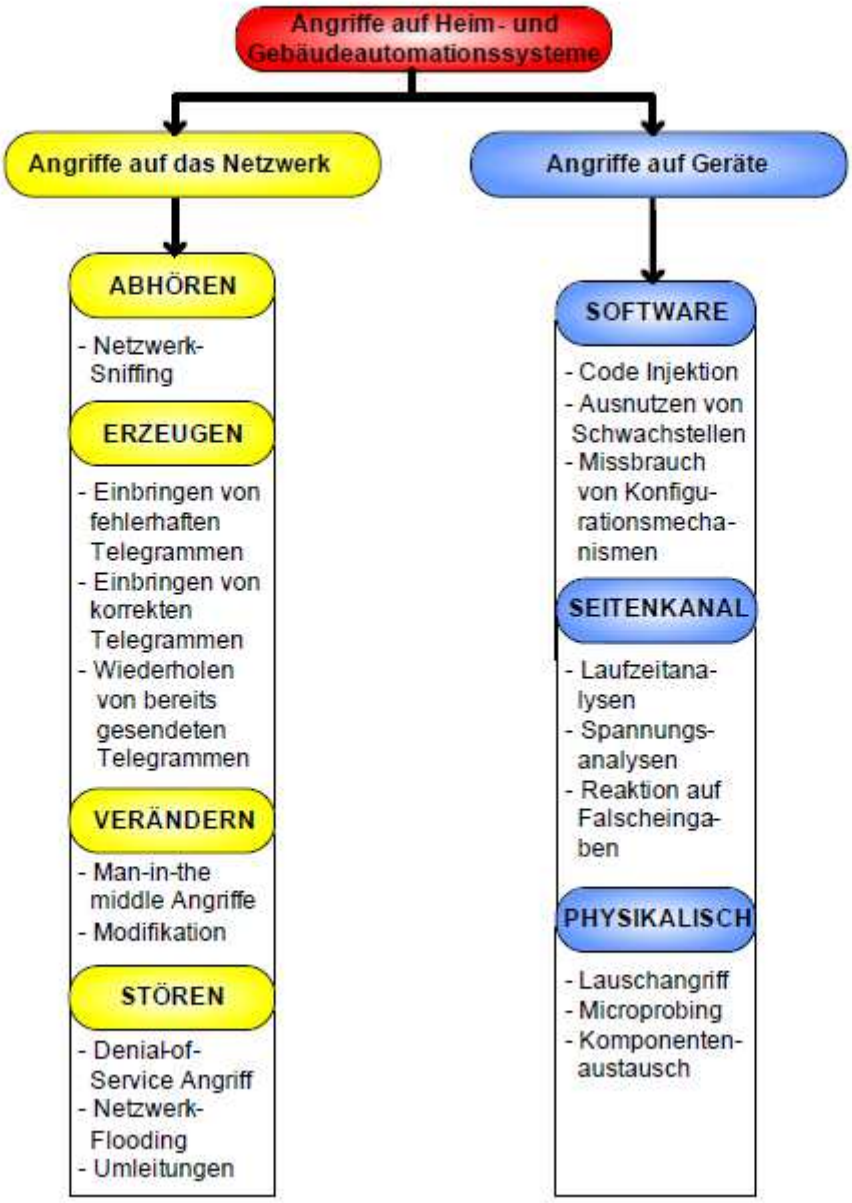


**Abbildung 3** Angriffe auf Heim- und Gebäudeautomationssysteme
Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 39 (08.08.2016)

### 4.4.1 Angriff auf das Netzwerk

Um den vollen Umfang und die volle Funktionalität eines Smart Home Systems nutzen zu können, bedarf es der Anbindung in ein Netzwerk für die Kommunikation der Komponenten sowie zur Nutzung der Steuerung von Unterwegs. Durch diese Möglichkeit, die Steuerung „nach außen“ zu tragen, ergeben sich automatisch Risiken und Bedrohungen. Durch die Anbindung an ein öffentliches Netz, in diesem Falle das Internet, ist theoretisch jedes System automatisch angreifbar und bedarf in vielerlei Hinsicht Schutzmaßnahmen. Nachfolgende mögliche Angriffsformen auf ein Netzwerk können unterschieden werden:

**Möglichkeit des Abhörens**

Die Möglichkeit des Abhörens von Gesprächen spielt in dieser Betrachtung eine unwesentliche Rolle und soll deshalb nicht dargestellt werden, sondern vielmehr das „Abhören“ und Mitschneiden des Datenverkehrs. Wie am Anfang erläutert, entsteht durch den Einsatz von Smart Home ein hoher Datenfluss. Um den Datenfluss abhören zu können, benötigt der Angreifer einen Zugriff auf das Netzwerk, was meist unautorisiert und unentdeckt passiert. Aus diesen Daten können Informationen abgeleitet werden, die für weitere Angriffsverfahren nötig sind. Dieses Abhören des Datenverkehrs wird auch als sogenanntes „Netzwerk-Sniffing“ bezeichnet und ist eine weit verbreitete Angriffsstrategie. Solche „Sniffing“ Tools sind kostenlos über das Internet beziehbar und relativ einfach zu bedienen, was das Gefahrenpotential erheblich steigert. Zudem sind viele Tools für die Analyse des eigenen Netzwerkes legal einsetzbar. Um dieses Abhören zu unterbinden sind einige Sicherheitsvorkehrungen notwendig. Im Grunde genommen wird dies mittels Verschlüsselung gewährleitet, bietet aber keinen 100%igen Schutz. Doch auch viele Smart Home Systeme, beispielsweise KNX, verschlüsseln die Kommunikation zwischen den Komponenten nicht, was ausgenutzt werden könnte. Weiterhin kann es sein, dass veraltete Verschlüsselungsverfahren wie WPS (WLAN) eingesetzt werden. Durch diese Abhörvorgänge ergeben sich wiederum neue Möglichkeiten für Angriffe. Deshalb ist es wichtig, veraltete Verschlüsselungsverfahren auszutauschen und durch neue zu ersetzen. Ebenso ist es wichtig veraltete Komponenten auszutauschen, falls es Sicherheitsprobleme gibt bzw. keine Unterstützung modernerer Verschlüsselungsverfahren existiert.[12]

**Möglichkeit des Erzeugens**

Eine weitere Möglichkeit ist die Erzeugung von eigenen Anwendungen oder Telegrammen, wie es in der obigen Grafik (vgl. Abb. 3) dargestellt wird. Dies wird auch als „Code-Injection“ für die Einschleusung eigener Telegramme oder auch als „Replay-Attacks“ für das Einschleusen bereits gesendeter Telegramme bezeichnet. Als Beispiel einer „Code-Injection“ kann man die Einbringung einer Schadsoftware über einen Mailanhang oder durch den Besuch einer manipulierten Website, nennen. Als Beispiel für „Replay-Attacks“ könnte man die gezielte Einflussnahme auf ein Schließsystem per Smart Home nennen. Durch das Abhören des Datenverkehrs, welcher bei der Betätigung des Türöffners erzeugt wird, kann man die Daten abfangen und erneut senden, um mit dem gleichen Effekt Zugriff auf Haus oder Wohnung zu erlangen. Zum Schutz vor einer solchen Attacke können vor allem gewisse Authentifizierungs- oder Autoritätsmaßnahmen vorbeugen. Aber auch die

[12] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 40 (08.08.2016)

Kontrolle der Daten von Aktualität und Ursprung sind mögliche Wege, diesem Missbrauch vorzubeugen.[13]

**Möglichkeit des Veränderns**

Um Veränderungen vornehmen zu können, benötigt man Zugriff auf die Kommunikationskomponenten, auf physikalischer oder logischer Ebene. Diese Angriffsmethode wird auch „Man-in-the-Middle“ genannt. Sie ist meist die Nachfolge von dem Erzeugen und Einschleusen von eigenen Codes in das System, um den Netzwerkzugriff zu erlangen und um Veränderungen für die eigenen Zwecke durchzuführen. Der Angreifer hat also vollen Zugriff auf das Netzwerk und kann alle möglichen Informationen, die zwischen den Komponenten ausgetauscht werden, einsehen und nach Belieben ändern. Solch ein Zugriff ist das schlimmste Szenario eines jeden IT-Sicherheitsexperten und die größte Gefahr von Smart Home, da solche Zugriffe oft lange Zeit ungedeckt bleiben, wenn der Angreifer keine besonderen Auffälligkeiten hinterlässt. Schützen kann man sich über den Einsatz von Verschlüsselungsverfahren aber auch durch Kontrollen der Identität. Somit können bereits die vorher notwendigen Schritte abgewehrt werden, um einen vollständigen Zugriff unterbinden zu können.[14]

**Möglichkeit des Störens**

Eine weitere Angriffsmöglichkeit auf ein Netzwerk, ist die Störung der Kommunikation bzw. Funktionsweise der Komponenten. Oft nennt man solche Attacken auch „Denial of Service Attacks“ die übersetzt „Dienstverweigerung“ bedeuten. In den meisten Fällen geht es darum, die Netzwerkteilnehmer mit bestimmten Befehlen oder durch das Übermitteln von vielen Daten und Informationen zu überfordern. Das System kommt mit der Verarbeitung nicht mehr nach und der Dienst weitere Befehle, z.B. vom eigentlichen Anwender können nicht mehr verarbeiten werden. Oft stürzt das System ab oder „friert“ ein, wie man es aus im Computerbereich kennt. Eine weitere Möglichkeit kann, vor allem bei der Anwendung von Funk Smart Home, die Störung des Funk- bzw. WLAN-Signals sein, um die Kommunikation zu verhindern. Man benötigt nur die Funkfrequenz und muss diese Signale mit einem Gerät überlagern. Ein ähnliches Verfahren ist die Kommunikationsstörung in Militärkreisen. Schützen kann man sich, wenn man die Netzwerkkommunikation überwacht und die durchschnittliche Anfragemenge kennt, um mögliche Überschwemmung und Steigerungen der Anfragen schnell zu ermitteln. Für eine solche Überwachung gibt es viele verschiedene Tools, aber für den privaten Sektor schwer einzusetzen sind. Diese Angriffe sind sehr weit verbreitet, einfach umzusetzen aber schwer zurückzuverfolgen, besitzen eine sehr hohe Schlagkraft und können erhebliche

[13] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 41 (08.08.2016)
[14] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 41 (08.08.2016)

Schäden verursachen. Somit sollte man bei kleinsten Anzeichen von langsamen Kommunikationswegen oder „Lag's" eine Überprüfung des Systems durchführen.[15]

### 4.4.2 Angriffe auf Geräte

Hat der Angreifer Netzwerkzugang, kann man auch Attacken auf eine eingebundene Komponente durchführen, um bestimmte Funktionen des Systems für den eigenen Nutzen anzuwenden. In den meisten Fällen haben Kriminelle die Absicht, bei dem Eindringen in ein Smart Home System dessen Kontrolle zu erlangen, um mögliche Vorteile daraus zu generieren. Es gibt auch hier wieder unterschiedlichste Möglichkeiten von Angriffen z.B. Softwareattacken, Seitenkanalattacken aber auch physikalischen Attacken. Oft ist der Angriff auf ein Gerät sehr schwierig, wenn Hersteller und Anwender diese Geräte ausreichend schützen, jedoch bei sorglosem Umgang und Missachtung von Sicherheitsvorkehrungen ein leichtes Angriffsziel. Nachfolgende mögliche Angriffsformen auf Geräte können unterschieden werden:

**Softwareattacken**

In vielen Fällen von Angriffen werden die Schwachstellen von Software ausgenutzt. Meist wird dabei der Zugriff über das Netzwerk genutzt. Diese sogenannten „Exploit"-Angriffe sind weit verbreitet und sollen Schwachstellen, die bei der Entwicklung und Programmierung übersehen wurden, oder Hintertüren, die durch die Entwickler eingebracht wurden um im Nachgang noch gewisse Konfigurationen vornehmen zu können. Die Funktion von „Exploit" beruht auf eigenen Programmcodes, die die Software systematisch auf Schwachstellen untersuchen und entwickelt wurden, um diese Schwachstellen zu finden und auf Sicherheitsprobleme hinzuweisen. Diese Möglichkeit wird aber auch missbraucht und für illegale Dinge eingesetzt. Ein Beispiel ist der Angriff auf die Firmware eines Routers, was durchaus ein attraktives Angriffsziel für Hacker darstellt. Ein Schutz wäre das Einspielen regelmäßiger Updates, da durch den Hersteller bekannte Schwachstellen relativ zügig geschlossen werden.[16] [17]

**Seitenkanalattacken**

Die Angriffsmöglichkeit von Seitenkanälen wird dem normalen Anwender eine unbekannte Attacke darstellen, spielt aber eine wesentliche Rolle in der IT-Sicherheit. Eine Seitenkanalattacke wird als krypthologische Methode bezeichnet und enthält die „physische Implementierung eines Kryptosystems in einem Gerät oder einer Software"[18]. Einfacher ausgedrückt kann durch die Überwachung der Stromaufnahme während der kryptografischen Berechnung an den Schlüssel gelangt

[15] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 41 (08.08.2016)
[16] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 41 (08.08.2016)
[17] Online: vgl. wikipedia.org – Exploit, 2016 (21.07.2016)
[18] Online: wikipedia.org - Seitenkanalattacken, 2016 (14.08.2016)

werden. Die Seitenkanäle werden vor allem für sichere Verbindungen nach außen verwendet und in potentiell gefährlichen oder zensierten Netzwerken eingesetzt. Bekannte Anwendungen für eine solche Verschlüsselung der Kommunikationskanäle sind z.B. Secure Shell (SSH) oder Virtual Private Network (VPN). Doch trotz Verschlüsselung kann durch eine gezielte Analyse viel über die Verbindung herausgefunden werden. Aus diesen Daten können auch Informationen über die verwendete Software abgeleitet werden und somit die Möglichkeit bieten, gezieltere Angriffe zu planen. Um dieser Attacke vorzubeugen ist das wichtigste Verfahren die Verschlüsselung der Daten, sowie die damit verbundene Verifizierung durch Zertifikate zwischen den beiden Kommunikationspartnern. Ebenso gibt es die Möglichkeit eine zusätzliche Absicherung durch kurz geltende Codes zu ermöglichen, z.B. TAN oder SMS-Verifizierungscodes.[19] [20]

**Physikalische Attacken**

Eine weitere große Gefahr geht, wie schon erwähnt, von der physikalischen Attacke („Man-in-the-Middle“) aus. Für eine physikalische Attacke benötigt man direkten Zugriff auf die IT-Komponenten und kann durch Erweiterung oder Austausch von Hardwarekomponenten eine Manipulierung oder Modifizierung des Systems vornehmen. Besondere Beachtung muss dabei externen Speichermedien geschenkt werden, wie z.B. USB-Sticks oder externen Festplatten. Doch auch andere anschließbare Komponenten wie Tastatur und Maus stellen eine potentielle Gefahr dar. So kann es sein, dass diese Geräte mit Schadsoftware infiziert werden und durch die Verbindung mit dem PC die Schadsoftware in das System eingeschleust wird. Somit ist es wichtig, externe Geräte, ohne genaue Betrachtung, nicht an das System anzuschließen. Vor allem in Firmennetzwerken ist das Anstecken privater externer Speichermedien oft verboten. Um sich vor solchen Angriffen schützen zu können, sollte darauf geachtet werden, welche Medien mit dem System verbunden werden bzw. USB-Ports und diverse andere Schnittstellen sperren.[21] [22]

### 4.4.3 Sonstige Risiken

Zusätzlich zu den Risiken an den Geräten existieren auch andere Schwachstellen in der Anwendung von Smart Home. Oftmals könnten diese Sicherheitsrisiken durch die behutsame Verwendung und durch die Überwachung und Gewährleistung der Sicherheit durch den Anwender vermindert werden. Mögliche Beispiele wären:

[19] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 42 (08.08.2016)
[20] Online: Vgl. Christophe Tremlet, Kristin Rinorther, elektronikpraxis.vogel.de, 2013 (21.07.2016)
[21] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 42 (08.08.2016)
[22] Online: vgl. wikipedia.org – Man-in-the-Middle-Angriff, 2016 (22.07.2016)

**Veraltete Soft- und Hardware**

In der Betrachtung von Smart Home Systemen spielen vor allem die Neuerungen und Verbesserungen eine große Rolle, da solche Systeme meist über einen längeren Zeitraum verwendet werden und im Regelfall ein Austausch der Komponenten nur bei einem Defekt oder einer Erweiterung des Systems erfolgt. Doch bei dem Einsatz eines Smart Home Systems sollte sich der Nutzer auch Gedanken über die IT-Sicherheit machen und gegebenenfalls unsichere Komponenten austauschen bzw. regelmäßige Updates durchführen. Das ist wichtig, da im Laufe des Betriebes immer wieder Schwachstellen auftauchen können und z.B. Verschlüsselungsverfahren über die Jahre an Aktualität und dadurch an Sicherheit verlieren. Durch die starke Weiterentwicklung der IT ist es möglich, dass bestimmte Sicherheitsvorkehrungen in kurzer Zeit an Aktualität verlieren, somit unsicher sind und keinen weiteren Support erhalten. Deshalb ist es ebenfalls ratsam, sich zu Neuerungen etc. zu informieren, um immer up-to-date zu sein.[23]

**Übertragungsmedien**

Durch die Vielzahl an Automationssystemen für das Haus, ist die Auswahl der Übertragungsmedien kein unerheblicher Punkt in Bezug auf die Sicherheit. Im wesentlichen Sinne hat jedes System seine Vor- und Nachteile. Durch eine Funkübertragung werden die Daten über eine große Reichweite ausgesendet und können dadurch auch auf Distanz aufgefasst bzw. durch die Störung des Signales unterbrochen werden. Doch auch kabelgebundene Anwendungen besitzen das Risiko, dass bei Anwendung im Außenbereich, durch Demontage von Komponenten ein Zugriff auf das System erfolgen kann. Die Gewährleistung der Sicherheit für solche Systeme stellt eine neue Herausforderung an die IT-Sicherheit dar, da durch die immer weitere Vernetzung von einfachsten Komponenten wie Steckdosen, Lichtschaltern etc. eine potentielle Gefahr entsteht. Wichtig ist dabei die fachgerechte Montage und Installation.[24]

**Fernwartungen**

Ein weiteres Risiko stellt die Möglichkeit, der heute weit verbreiteten Fernwartung dar. Das Positive an dieser technischen Möglichkeit ist eine schnelle Unterstützung sowie eine kostensparende Variante Systeme zu pflegen und zu steuern, ohne vor Ort zu sein. Auch hierbei können erhebliche Probleme entstehen, falls diese Verbindungen nicht ausreichend geschützt werden. Durch Fernwartungen wird die Steuerung des Gerätes über das Internet möglich. Eine solche Anbindung an das öffentliche Netz stellt immer ein erhebliches Sicherheitsproblem dar, denn die Angreifbarkeit ist stets gegeben. Um ein solches Risiko zu vermeiden, sollte im

[23] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 42 (08.08.2016)
[24] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 42-43 (08.08.2016)

Hausautomationsbereich auf Fernwartungen und Konfigurationen des Systems von unterwegs verzichtet und diese nur vor Ort vorgenommen werden. Ein Beispiel ist die oft angebotene Fernwartung von Routern, die aus der Sicht von Sicherheitsexperten grundsätzlich immer deaktiviert sein sollte.[25]

**Brute Force**

Eine der bekanntesten Angriffsmethoden um Passwörter zu knacken, ist die Brute Force-Methode. Diese Methode folgt einem einfachen Ablauf, dem Ausprobieren verschiedener Zeichenkombinationen. Je höher die Rechenleistung des Computers ist, umso schneller und mehr Zeichenkombinationen können pro Sekunde ausprobiert werden. Die Brute Force-Methode wird sehr oft in Bezug auf WLAN-Passwörter benutzt, da es Leute gibt, die ihr WLAN-Passwort kürzen, um es sich einfacher merken zu können. Die Länge des Schlüssels und die unterschiedlichen Kombinationen von Zeichen sind bei dieser Methode ausschlaggebend. Ein kurzes Beispiel soll die Brute Force Methode anhand eines WLAN-Schlüssels verdeutlichen. Alle Geräte, die sich in das mobile Netzwerk einwählen wollen, müssen sich über ein Passwort Zugriff verschaffen. Ohne dieses Passwort hat man theoretisch keinen Zugriff. Doch Wählt sich ein Gerät ein, wird das Passwort verschlüsselt übermittelt um es abzugleichen und der Anfrage des Gerätes statt zu geben. Fängt man diese Daten ab, ein sogenannter „Handshake“, besitzt man das WLAN-Passwort aber nur auf verschlüsselter Basis, was im Normalfall unbrauchbar ist. Um die Wartezeit auf die Nutzereinwahl zu verkürzen kann an den WLAN-Router ein Befehl gesendet werden, der einen eingewählten Nutzer kurz von der Verbindung mit dem Router trennt und sich meistens binnen Sekunden automatisch erneut einwählt. Dies fällt nicht wirklich auf, da Unterbrechungen in der Verbindung durchaus öfters auftreten können. Dieser Handshake wird jetzt per Brute-Force aus den unterschiedlichen Kombinationen überprüft. Dazu können Passwort-Listen heruntergeladen werden, die häufige Zeichenkombinationen aufgelistet haben, um die Methode zu beschleunigen. Außerdem kann ebenfalls ein Bereich eingegeben werden, in dessen Rahmen nach Kombinationen gesucht werden soll z.B. Angaben wie Vorname, Nachname, Geburtsjahr usw.[26]

## 4.5 Sicherheitsbetrachtung Smart Home

Die Sicherheitsbetrachtung von Smart Home stellt eine neue und besonders große Herausforderung an die zukünftige IT-Sicherheit dar. Da sich dieser Markt im Wachstum befindet, gibt es sehr viele Neuheiten und technische Veränderungen, auf die möglichst schnell reagiert werden muss.
Man unterscheidet im Wesentlichen zwischen funk- und kabelgesteuerter Technik.

[25] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 43 (08.08.2016)
[26] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 43-44 (08.08.2016)

Diese beiden Möglichkeiten der Hausautomation unterscheiden sich bei der Kommunikations- und Übertragungsmöglichkeit. Auch in Hinblick auf die IT-Sicherheit gibt es einige Aspekte, die unterschiedlich zu betrachten sind. Durch das Wachstum des Marktes werden immer mehr Hersteller auf diesen Markt aufmerksam und bieten ihre Produkte an. Durch diese Fülle an Anbietern ist es deshalb für den Endkunden schwer, dass passende Produkt zu finden. Oft ist es der finanzielle Rahmen, der beim Kauf eines Smart Home Produktes ein entscheidende Rolle spielt. Jedoch kann dies zu einem erheblichen Sicherheitsrisiko führen, wenn zu unbekannten Produkten und Herstellern gegriffen wird. In den meisten Fällen sind die getesteten Produkte durchaus sicher, bieten aber weniger Komfort und durchaus eine geringere Lebensdauer sowie Robustheit. Bei Verwendung von Sicherheitsmaßnahmen werden heutzutage standardmäßige Verschlüsselungen wie SSL oder AES verwendet. AES zum Beispiel ist sehr weit verbreitet und ohne Lizenz für jeden nutzbar. Trotz vieler freier und standardisierter Sicherheitsmaßnahmen raten IT-Sicherheitsexperten auf renommierte Hersteller von Smart Home zurückzugreifen, wenn in dem vernetzten Haushalt sicherheitsrelevante Anwendungen gesteuert werden sollen. In den meisten Fällen sind dies Türen und Fenster, da diese unmittelbaren Zutritt in das Haus gewähren können, aber auch Sicherheitssysteme wie Einbruch- und Brandmeldeanlagen.
Viele Hersteller zielen darauf ab, ihre Produkte so attraktiv wie möglich zu gestalten, und in diesem Punkt spielt die Sicherheit eine große Rolle. Deswegen versuchen sie ihre Produkte stetig zu verbessern und Sicherheitslücken durch Updates zu beseitigen. Viele Nutzer und Anwender sollten bei Interesse an Smart Home Anlagen die favorisierten Produkte und die dazu existierenden Tests studieren und davon ihre Kaufentscheidung abhängig machen. Durch eine Vielzahl an Magazinen und Zeitschriften, kann man sich einen guten Überblick verschaffen. Doch die wesentlichen Sicherheitsbedenken liegen nicht in dem Produkt alleine, sondern im Umgang damit. Die Produkte der Hersteller können nur so sicher sein, wie es die vorherrschende IT-Infrastruktur zulässt. Das bedeutet, wenn man z.B. ein ungesichertes WLAN besitzt, dass auch das Smart Home System unsicher ist.

### 4.5.1 Infrastrukturelle Probleme

Die Betrachtung der Sicherheit von Smart Home ist auch von den unterschiedlichen Einsatzorten abhängig. Nicht jeder Einsatzort birgt gleiche Gefahren und nicht jede Komponente wird überall gleich eingesetzt. Vor allem der Unterschied in der Infrastruktur und der Beschaffenheit der Gebäude spielt eine sehr wesentliche Rolle. Ein wichtiger Faktor zur Sicherung einer Technologie ist nicht allein die Sicherheit des Gerätes oder der Weg der Kommunikation mit anderen Komponenten, sondern auch der Einsatzort dieser Technologie. Ist dieser Einsatzort nicht ausreichend geschützt, nützen weder ein sicherer Systemaufbau noch verschlüsselte

Kommunikationswege etwas. Das System wird durch einen physikalischen Zugriff gefährdet. Deshalb spielen ebenso Planungen von Architekten eine große Rolle, im Öffentlichen Bereich mehr, als im Privaten. Auf der Messe „Light & Building“ wurde eine Lesung des Frankfurter Meixner-Schlüter—Wendt- Architekturbüro zum Thema Gebäudeautomation aus architektonischer Sicht gehalten. Es war klar zu erkennen, dass der Trend von Smart Home in der Planung von Gebäuden bereits einen großen Platz einnimmt und der Trend zu einer Hausautomation mit der Verknüpfung von Sicherheitsvorkehrungen geht. Ebenso wurde ganz klar gesagt, dass bei der Planung eines Gebäudes immer öfters IT-Experten zu Raten gezogen werden und zukünftig eine größere Rolle bei der Umsetzung eines Projektes spielen werden. In privater Anwendung von Smart Home Systemen haben meist nur die Eigentümer Zugriff auf das Gebäude und das System. In den meisten Eigenheimen wird die Smart Home Technik einfach in das Gebäude integriert und keiner Planung für IT-Sicherheitsmaßnahmen unterzogen.

#### 4.5.1.1 Privater Einsatz

Der Private Einsatz von Gebäudeautomation ist heutzutage am weitesten verbreitet. Der Unterschied zu öffentlichen Bereichen liegt ganz klar am Zugang zum Gebäude und dessen Smart Home System. Oftmals ist die Rechentechnik in keinem besonders abgesperrten Bereich anzutreffen und somit recht einfach zu erreichen. Für den privaten Bereich ist Smart Home ein vielseitig einsetzbares System, welches verantwortlich ist für die Energieeffizienz, Sicherheit sowie den Komfort. Im privaten Bereich sollten im Normalfall nur die Besitzer Zugang haben. Somit ist weniger wichtig, dass Smart Home Komponenten in versteckter Weise verbaut werden oder manipulationssicher, durch feste Montagemöglichkeiten, installiert werden. Hier dient es meist nur dem Nutzen und Sicherheitskonzepte für den Innenbereich des Gebäudes müssen weniger intensiv betrachtet werden. Voraussetzung dafür ist an dieser Stelle aber, die ausreichende Absicherung der Gebäudeaußenhülle. Deshalb ist es wichtiger bei der Verwendung von Smart Home die Sicherheitsvorkehrungen für den Außenbereich zu betrachten. Vor allem hier stellen Smart Home Produkte ein Problem dar, da Kriminelle schnell Manipulationen vornehmen können, z.B. an Lampen, Klingeln oder diversen anderen Geräten, ohne dass dies auf Anhieb entdeckt wird. Deshalb sollte im privaten Bereich darauf geachtet werden, das außenliegende Komponenten schwer zugänglich sind, oder durch diverse Schutzmaßnahmen extra abgesichert werden. Zudem sollte überlegt werden, ob der Einsatz außerhalb des Gebäudes notwendig ist. Bei der Entscheidung für die Verwendung im Außenbereich, sollte dafür zu Funkkomponenten gegriffen werden sowie darauf geachtet werden, dass die Funkreichweite begrenzt ist. Die Verlegung von BUS-Kabeln nach außen, ist durch die einfache Manipulation nicht ratsam.

#### 4.5.1.2 Öffentlicher Einsatz

Der öffentliche Einsatz von Smart Home Technologie ist momentan weniger verbreitet. Jedoch ist hier die Absicherung der Smart Home Komponenten noch wichtiger, als im privaten Bereich, da viele unterschiedliche Personen unerkannt Zugriff erlangen können. Die Sicherheitsmaßnahmen wie Einbruch- und Brandmeldeanlagen werden durch professionelle Errichter installiert wurden und spielen deshalb in der Smart Home Anwendung eine nicht so entscheidende Rolle, obwohl diese Systeme ebenfalls zur Gebäudeautomation gehören und durchaus mit Smart Home Komponenten per „EIB“ etc. verbunden werden können. Ein durchaus kritischen öffentlichen Einsatz von Smart Home, stellen Hotels dar. Ein Hacker hatte im Jahr 2014 auf der „Black Hat“ erfolgreich bewiesen, wie gefährlich eine unzureichende Absicherung sein kann. In Hotels kann in den meisten Fällen nicht auf Funkkomponenten zurückgegriffen werden, da die Reichweite begrenzt ist. Hier kommen deshalb kabelgesteuerte Systeme zum Einsatz, die auch über diverse Sicherheitsprobleme verfügen. Somit können BUS-Komponenten in einem Hotelzimmer demontiert werden z.B. die Wandlampe und durch Einsatz von bestimmter Technik manipuliert werden. Solche Komponenten müssen so abgesichert werden, dass eine Demontage ohne Alarmfunktion nicht möglich ist oder die verschiedenen Komponenten an Stellen installiert werden, wo ein schneller Zugriff unmöglich erscheint. Denn besteht einmal Zugriff auf das System, gibt es auch Möglichkeiten dieses System von der Ferne aus zu steuern. Somit ist die Planung von öffentlichen Gebäuden, wenn Smart Home zu Einsatz kommen soll, ein sehr wichtiger Punkt und sollte gut durchdacht werden. Im Öffentlichen Bereich ist eine Manipulation eines Smart Home Systems durchaus kritischer anzusehen und kann auch zu Gefährdungen von Menschenleben führen, falls diverse Sicherheitsvorkehrungen deaktiviert und eventuell die Menschen in einem Gebäude eingesperrt werden, wenn eine Türsteuerung vorhanden ist.[27]

### 4.5.2 Funk-Smart Home

Die Funktechnik ist im Smart Home Bereich sehr weit verbreitet und wird von vielen namhaften Herstellern angeboten. Durch den Einsatz der Funktechnik, ist es mittlerweile möglich, sein Gebäude ohne kabelgebundene Technik zu automatisieren. Diese Methode ist oftmals für bestehende Gebäude die wirtschaftlichere Variante. Grundsätzlich werden zwei vorkommende Funksysteme unterschieden. Das proprietäre und das standardbasierte Funksystem. Das proprietäre Funksystem ist meistens eine eigene Entwicklung des Herstellers, der eigene Verfahren, Hardware sowie Software zum Einsatz bringt und die Technologie auch nur über diesen Hersteller bezogen werden kann. Ein gutes Beispiel ist hierbei

[27] Online: vgl. Patrick Beuth, zeit.de, 2014 (28.07.2016)

der Anbieter HomeMatic, der einen Funkstandard namens „BidCos“ einsetzt. Bei diesem Funksystem ist der Kunde somit vom Hersteller abhängig und kann keine Produkte anderer Hersteller in das System integrieren. Bei HomeMatic und den Partnern stellt dies heutzutage aber kein Problem dar, da diese Technik stetig weiterentwickelt und eine breite Palette an diversen Komponenten angeboten wird. Der komplette Gegensatz sind die standardbasierten Funksysteme, die wie schon der Name verrät, standardisiert wurden und von vielen verschiedenen Herstellern Unterstützung finden. Im Grunde genommen sind für diese Standards viele Hersteller und Produktkomponenten am Markt und deshalb ist der Markt breiter gefächert und der Einsatz für längere Zeit gesichert. Wie aber verschiedene Marktstudien ergeben haben, unterscheiden sich die proprietären Funksysteme im Umfang und Nutzen nicht mehr von den standardisierten Systemen. Auch die Telekom bietet erweiterte Vernetzung mit verschiedenen Herstellern an und ermöglicht die Kommunikation mittlerweile mit standardisierten Funkprotokollen, über entsprechende Zusatztools wie Funk-Sticks und Ähnliches. Sehr viele Hersteller, ohne Betrachtung des Funkprotokolls, arbeiten über die lizenzkostenfreie Funkfrequenz von 434 MHz oder 868 MHz. Dieser Standard wird deshalb durch die Bundesnetzagentur streng überwacht und unterliegt diversen Auflagen. Die Auflagen sind z.B. die Begrenzung der Senderleistung (25 mW) sowie der maximalen Arbeitsleistung (36 Sekunden pro Stunde). Diese Funkfrequenzen sind ein Teil der ISM-Bänder („Industrial, Scientific and Medical Band“). Das heißt, dass diese Funkfrequenz nicht nur für die Gebäudeautomation, sondern auch für viele andere Bereiche in der Wissenschaft, Medizin und Industrie zum Einsatz kommt. Hinzu kommt die Nutzung von WLAN oder Bluetooth über diese Funkfrequenz. Eine weitere freie Funkfrequenz ist 2400 MHz, die aber in der Betrachtung von Reichweite und Durchdringung von Hindernissen wie z.B. Wänden, nicht so gut geeignet ist.

Wie bereits erwähnt basiert der Hersteller HomeMatic auf den Funkprotokoll „BidCos“, abgekürzt „Bidirectional Communication System“, und wurde von den hinter HomeMatic stehenden Firmen, eQ3 sowie ELV Elektronik AG, entwickelt. Da dieses Verfahren nicht standardisiert ist, können nur Produkte verwendet werden, die der Hersteller zur Verfügung stellt. Die Verknüpfung mit anderen Komponenten wird nicht unterstützt und kann durchaus zu Problemen führen. Jedoch ermöglicht der Hersteller eine reibungslose Verwendung von Smart Home im ganzen Haus, da er eine breite Palette an Produkten anbieten und keine Einbußen in der Gebäudevernetzung hinnehmen muss. Ein weiterer Hersteller und Partner von HomeMatic ist der Stromlieferant RWE sowie der Telekommunikationsanbieter Telekom, welche das ähnliche Funkprotokoll verwenden, aber im Aufbau einige Änderungen vorgenommen haben, um es massenmarkttauglich zu gestalten. Da die Verwendung von HomeMatic für den Laien einige Probleme darstellen kann, da diverse Installationen mit BUS etc. möglich sind, eignet sich dieses System eher für

technikversierte Anwender.
Die wohl bekanntesten Funkprotokolle auf dem Smart Home Markt sind ZigBee und Z-Wave.
Das ZigBee Protokoll, welches unter der Bezeichnung IEEE 802.15.4 standardisiert wurde, gehört zur Entwicklung der sogenannten ZigBee-Allianz und ist ein internationales Protokoll für Funknetz-Technik. Dieser ZigBee Vereinigung gehören mittlerweile über 250 Unternehmen an. Darunter zählen z.B.: Honeywell, Huawei, Samsung, Sony und viele weitere bekannte Hersteller. Ein positiver Aspekt dieses Protokolls, ist die sehr geringe Strombelastung (über Schlafmodus-Funktion), was positiv für batteriebetriebene Komponenten ist. Somit ist der Wartungsaufwand für den Wechsel der Batterien über mehrere Jahre nicht relevant.
Das zweite Verfahren ist das Z-Wave Protokoll, welches der Kommunikationsstandard der Firma Zensys aus Dänemark, sowie der ebenfalls existierenden Allianz von Z-Wave darstellt. Anders als bei dem ZigBee Protokoll wurde Z-Wave allein für die Gebäudeautomation entwickelt und ist unter der Bezeichnung G.9959 standardisiert. Die Z-Wave Allianz erreicht eine Vereinigung von über 300 Herstellern aus aller Welt und stellt im Bereich der Gebäudeautomation den weltmarktführenden Funkstandard dar. Beispiele für Mitglieder wären Sigma Designs, Assa Abloy, Bosch sowie D-Link. Viele Firmen die der Allianz von ZigBee angehören, sind ebenfalls Mitglied in der Z-Wave Vereinigung, da es durch den weltmarktführenden Smart Home Funk Standard bessere Möglichkeiten gibt, um eigene Smart Home Produkte auf den Markt zu bringen. Das Positive dabei ist, keine Produktabhängigkeit besteht und die Vernetzung der Komponenten diverser Hersteller möglich wird. Ein wichtiger Unterschied zwischen den beiden Funkprotokollen ist, dass ZigBee nicht nur für die alleinige Anwendung in der Gebäudeautomation konzipiert wurde, sondern vielmehr für die Kommunikation über Funk von unterschiedlichsten Komponenten aus allen Bereichen. Außerdem ist dieses Protokoll mehr für Entwickler gedacht, um eine möglichst breite Vernetzung von unterschiedlichsten Produkten diverser Hersteller zu ermöglichen, was durchaus zu Herausforderungen in der Installation führen kann.
Für die Anwendung im Smart Home Bereich zählt der Z-Wave Standard zur besseren Alternative, um sein komplettes Haus einfach und unkompliziert vernetzen zu können.[28] [29] [30]

### 4.5.3 Die IT-Sicherheit von Funk Smart Home

Die Betrachtung der IT-Sicherheit spielt im Bereich der Funk-Vernetzung eine große Rolle und wird immer wieder als ein unsicheres Verfahren dargestellt, da die

[28] Online: vgl. Boris Schiller, smarthomewelt.de – Z-Wave, 2015 ( 29.07.16)
[29] Online: vgl. Günther Ohland, pc-magazin.de – Übersicht Protokolle, 2013 (29.07.16)
[30] Online: vgl. Boris Schiller, smarthomewelt.de – BidCos, 2015 (29.07.2016)

Übertragung der Daten in einem relativ großen Radius, auch außerhalb des Gebäudes gewährleistet wird, und dadurch theoretisch das Abfangen dieser Daten durch Kriminelle relativ einfach ist. Um die Sicherheit dieser Funk-Vernetzung zu verstehen muss man die Funkprotokolle verstehen. Durch die Vielzahl an möglichen Protokollen die eingesetzt werden, gibt es theoretisch auch viele Schwachstellen, die ausgenutzt werden können.
Die IT-Sicherheit spielt also hierbei eine wesentliche Rolle, da ein physikalischer Zugang zum System nicht gegeben sein muss, wie im Gegensatz zu kabelgesteuerten Systemen.

**BidCos**

Bei der Betrachtung von BidCos, ist die IT-Sicherheit in diesem Protokoll durchaus gegeben, da die Kommunikation mit AES Verfahren auf 128 Bit Basis verschlüsselt wird. Eine Besonderheit ist die, wie abgekürzt im Namen vermerkt, bidirektionale Kommunikation, die eine Bestätigung des Empfängers benötigt, um die Kommunikation zu gewährleisten. Der Aufbau der Komponenten besteht dabei immer aus einer Zentrale, einem Aktor sowie einem Sensor. Die Zentrale ist die Steuerungseinheit die alle Befehle an die einzelnen Komponenten weiterleitet. Der Aktor setzt die empfangenen Signale physikalisch um (z.B. Türöffner, Rollläden). Der Gegensatz der Aktorik ist die Sensorik, die verschiedene Einflüsse aus der Umgebung wahrnimmt und diese Ergebnisse in ein Signal umwandelt, und einem Aktor zur Verarbeitung vorlegt (Thermostate, Bewegungsmelder).
Um einen Angriff auf dieses Verfahren durchzuführen, bedarf es einiger Kenntnisse im Hacking und dem Protokollaufbau. Die Herausforderung dieses Standards liegt ganz klar in der proprietären Vermarktung, da dadurch die Verwendung des Funkprotokolls nicht öffentlich möglich ist. Um überhaupt Zugang zum System erlangen zu können, muss man die Kommunikation entschlüsseln. Dazu muss man den Protokoll Header ermitteln, der aus Nutzdaten besteht, die in einer bestimmten Länge nacheinander angeordnet sind. Eine weitaus schwierigere Herausforderung ist aber die Analyse der Nutzdaten (engl. Payloads). Eine sehr aufwendige Möglichkeit ist die Nachkonstruktion (engl. Reserve Engineering) des Codes. Das Nachfolgende Beispiel soll einmal verdeutlichen, wie ein Payload aufgebaut sein kann. Dieser Payload ist von einer HomeMatic Zentrale.[31] [32]
Der prinzipielle Aufbau dieses Funkprotokolls lautet: „*ll*|*mc*|*cc*|*mt*|*src*|*dest*|*p...*“[33].

[31] Online: vgl. htw-dresden.de, 2013 (04.08.2016)
[32] Online: vgl. octopus-office.de – Bidirektional, 2016 (01.08.2016)
[33] Online: htw-dresden.de, 2013 (04.08.2016)

| Abk. | Byte-Nr. | Bedeutung |
|---|---|---|
| ll | 0 | Paketlänge |
| mc | 1 | Zähler für Nachrichten (message counter) |
| cc | 2 | Nachrichten-Flag (Bsp.: Burst-Mode) |
| mt | 3 | Nachrichten-Typ (Bsp.: ACK oder RESET) |
| src | 4-6 | Quelle |
| dest | 7-9 | Ziel |
| p | ab 10 | Payload |

**Abbildung 4** Aufbau HomeMatic Protokoll-Header
Online: htw-dresden.de, 2013 (04.08.2016)

„Beispiel: Payload eine Device Info Message

*[19][0011][4A4551303136333xxxxx][10][01][01][00]*

*[Firmware - 1 Byte][Gerätetyp - 2 Byte][Seriennummer - 10 Byte][Geräteklasse - 1 Byte][Peer Channel A - 1 Byte][Peer Channel B - 1 Byte][Unbekannt – 1 Byte]“*[34]

Die in diesem Beispiel gezeigte „Device Info Message“ ist der Ausgangspunkt für das Anlernen (engl. Pairing) zwischen zwei Komponenten. Ohne dieses Anlernen ist eine Kommunikation zwischen den Komponenten nicht möglich.
Im Grunde genommen ist dieses Funkprotokoll durchaus sicher und bietet gute Schutzmechanismen. Doch im Jahre 2014 zeigten die Computerexperten „Sathya“ und „Malli“ auf dem „30. Chaos Communication Congress“ in Hamburg eine Live-Attacke auf das HomeMatic System, indem sie den AES-Handshake nachkonstruierten, um so Zugriff auf das System zu erlangen. Dies gelingt aber nur bei der Verwendung des Standard- AES- Keys der Zentrale, deswegen wird empfohlen, diesen Key noch vor der vollständigen Nutzung, durch einen eigenen individuellen Key zu ersetzen.
Der Hersteller RWE, der mit dem gleichen Funkprotokoll arbeitet, legt vor allem auf Datensicherheit und Schutz vor ungewolltem Zugriff großen Wert. Deshalb wird die Kommunikation über das IPv6 Internetprotokoll geführt und ebenfalls mit 128 Bit AES verschlüsselt. Dadurch ist die RWE-Anwendung ein wenig sicherer als bei anderen Herstellern.[35] [36]
Die Verwendung von Funk-Komponenten mit dem BidCos Protokoll, kann nichts

[34] Online: htw-dresden.de, 2013 (04.08.2016)
[35] Online: vgl. htw-dresden.de, 2013 (04.08.2016)
[36] Online: vgl. siio.de, 2014 (04.08.2016)

entgegengesetzt werden und stellt eine sichere Vernetzung dar. Deshalb kann aus der IT-Sicherheit eine Empfehlung für dieses Protokoll ausgesprochen werden.

**ZigBee**

Bei der Betrachtung dieses Kommunikationsprotokolls, wird man schnell unterschiedliche Meinungen in den verschiedensten Medien finden.
Das ZigBee Protokoll besteht aus drei Gerätetypen, dem Router, dem Koordinator und dem Endgerät. Durch diese Vernetzung entsteht ein „vermaschtes Netz". Solch ein Netz bildet sich durch die Anmeldung der Endgeräte an einen Router (Stern-Topologie). Im ZigBee Protokoll können aber auch die Koordinatoren als Router dienen und bildet somit ein immer größeres Netzwerk (Baum-Topologie). Der Vorteil eines solchen „vermaschten Netzes" (engl. Mesh Network) ist, das bei einem Ausfall eines Routers die Daten trotzdem weitergeleitet werden können und somit der Ausfall des kompletten Systems verhindert wird. Doch das Problem liegt in diesem Netzwerk bei dem Koordinator. Denn dieser steuert das komplette Netzwerk, welches bei seinem Ausfall zusammenbrechen würde. Abhilfe kann nur mit Router Einstellungen am Router erfolgen, so dass dieser bei einem Ausfall den Koordinator ersetzen kann. Dies muss jedoch bereits beim Netzaufbau konfiguriert werden und ist oftmals bei Anwendern unbekannt.
Das ZigBee Protokoll setzt bei der Verschlüsselung auf das CCM Mode Verfahren mit dem Blockverschlüsselungsalgorithmus AES 128 Bit.
Das ZigBee Protokoll kennt dabei drei Geheimschlüssel, die in Link Key, Network Key und Master Key unterteilt, sowie durch einen Dienst verteilt und verwaltet werden. In den meisten Fällen sind diese Schlüssel vorinstalliert bzw. können bei Bedarf von dem Vertrauenscenter (Trust Center Applikation) abgerufen werden. Dieses Center wird durch den Koordinator bereitgestellt, kann aber auch von anderen Komponenten realisiert werden.
Der Hauptschlüssel (Master Key) befindet sich in jedem Knotenpunkt des ZigBee Netzes. Er ist für den vertraulichen Austausch der Link Keys zuständig. Dieser Link Key befindet sich zwischen zwei miteinander kommunizierenden Knoten und wird mittels AES auf 128 Bit Ebene verschlüsselt. Er dient dazu, dass die Informationen zwischen den zwei kommunizierenden Knoten wieder entschlüsselt und verwaltet werden können. Dieses Verfahren wird aber heutzutage in der Praxis noch nicht angewendet, da es große Schwierigkeiten gibt, diese Schlüssel auf die Funkkomponenten zu verteilen und eine reibungslose Kommunikation zu gewährleisten.
Der dritte und letzte Schlüssel ist der Network Key. Er wird im Vertrauenscenter mit 128 Bit AES erzeugt und mit jedem Gerät im Netz geteilt.
Eine Schwachstelle in diesem Netz ist die Verwendung eines festen und allgemein bekannten Schlüssels, um neue Module in diesem Netz anzumelden. Dieser

Vorgang kann abgehört und das System dadurch manipulierbar werden. Diese Schwachstelle wurde im Jahre 2015 auf der „Deepsec“ in Wien durch Security-Forscher an einem Türschloss öffentlich vorgeführt. Im Grunde genommen kommunizieren diese Geräte verschlüsselt, doch alle ZigBee Komponenten müssen das gleiche Schlüsselpaar kennen und akzeptieren. Bei der Anmeldung einer neuen Komponente im Netz, wird ein symmetrischer Schlüssel angefordert, da diese Komponente noch nicht bekannt ist. Dieser symmetrische Schlüssel wird dabei über Funk gesendet, wird aber nur mit dem asymmetrischen und öffentlich bekannten Schlüssel geschützt. Dabei kann durch Mitschneiden, der symmetrische Schlüssel herausgefunden werden. Es muss keine Neuanmeldung abgewartet werden, es reicht aus dem Netz eine Rejoin-Anfrage zu senden und somit eine Neuanmeldung vorzutäuschen. Man muss lediglich die Adresse des Gerätes und des Routers im ZigBee Netz kennen. Diese Rejoin-Attacke ist seit mehreren Jahren bekannt, kann aber durch Updates nicht behoben werden, da die Geräte keine Updates unterstützen. Des Weiteren können keine Sicherheitseinstellungen an den Geräten vorgenommen werden. Die einzige Möglichkeit besteht im Austausch der Komponenten durch neuere und sichere Geräte und durch den Einsatz der Master- und Linkschlüssel mithilfe des Trustcenters.[37] [38]

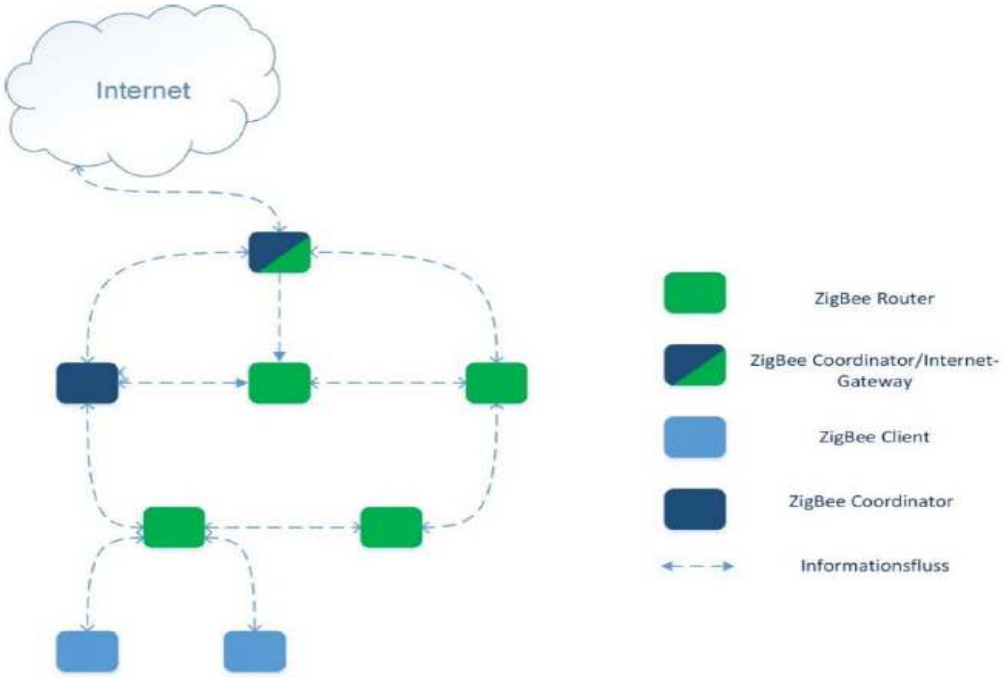


**Abbildung 5** ZigBee-Topologie
Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 28 (08.08.2016)

[37] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 26-27 (08.08.2016)
[38] Online: vgl. Hauke Gierow, golem.de, 2015 (10.08.2016)

**Z-Wave**

Auch das Kommunikationsprotokoll Z-Wave, welches nur für die Gebäudeautomation entwickelt wurde, besteht wie ZigBee aus einem „vermaschten Netz“ (Mesh-Network). Wie schon erwähnt, kann somit, ein weit reichendes Netzwerk aufgebaut werden, da die verschiedenen Komponenten auch als Signalvermittler dienen und somit weit entfernte Geräte ansteuern können. Diese Grafik soll die Überschneidung der Signale der einzelnen Komponenten besser darstellen. Somit kann Komponente A auch Komponente E erreichen, da die dazwischen liegenden Komponenten das Signal weiterleiten können.[39]

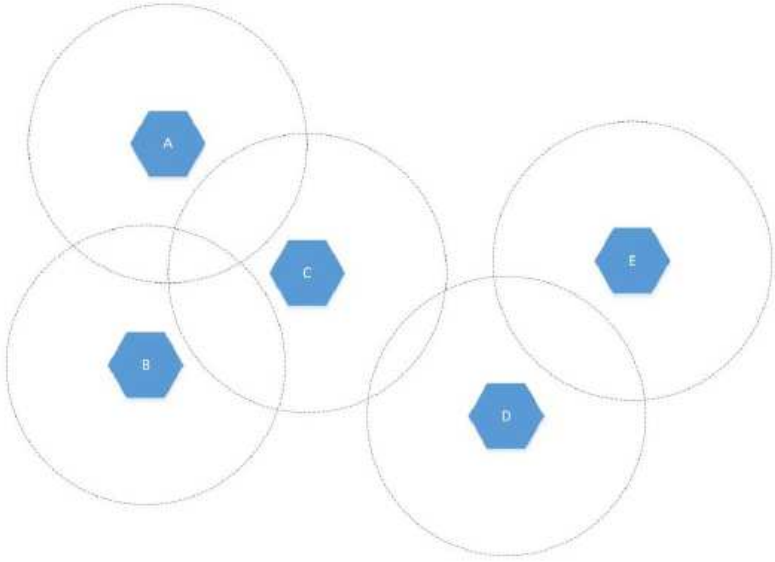


**Abbildung 6** Z-Wave Funknetzwerk
Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 29 (08.08.2016)

Dieses Protokoll unterscheidet zwischen drei unterschiedlichen Knotentypen, dem Controller, dem Routing Controller sowie Slaves. Der Controller kann mit vielen verschiedenen Knoten kommunizieren. Der Routing Controller kann dies nur mit bestimmten und festgelegten Knoten und der sogenannte „Slave“ kann überhaupt keine Kommunikation initiieren und nur auf Anfragen der Controller antworten. Entfällt ein Knoten in diesem Netz, formt sich das Netz automatisch neu, um die Funktionen aufrecht zu erhalten.
Das Z-Wave Protokoll ist durch einen 128 Bit MAC (Message Authentification Code) geschützt. Es wird ein einmaliger Code (Nonce) in 64 Bit Länge übertragen und somit die Daten des Senders transformiert. Daraus bildet sich ein sogenannter „Hashcode“, der dann an den Empfänger übermittelt wird, welcher dann wiederum diesen Code zurücktransformiert. Das hat den einfachen Zweck, dass schon

[39] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 28-30 (08.08.2016)

gesendete Anweisungen durch einen „Replay-Angriff“ nicht wiederholt werden können. Im Jahre 2013 wurde durch zwei IT-Sicherheitsforscher das Z-Wave Protokoll untersucht. Dabei gelang es, Kontrolle über ein Türschloss zu erlangen. Es wurde dabei eine Schwachstelle bei der Implementierung des Schlüsselaustauschs ausgenutzt. Die Hersteller hatten dabei angekündigt, diese Schwachstelle zu beseitigen. Unklar ist aber, ob diese Schwachstelle vom Hersteller selbst erzeugt wurde, oder durch die SDK für dieses Protokoll, welches dem Partner zu Verfügung gestellt wird, implementiert wurde. Es kann sein, dass diese Schwachstelle auch bei anderen Herstellern vorkommt. Für die Vernetzung eines Gebäudes eignet sich das Z-Wave Protokoll, genauso wie BidCos. Es ist wesentlich sicherer als ZigBee, kann aber auch Ziel eines Angriffes werden. Dazu kommt, dass auch hier darauf geachtet wird, dass die komplette IT und Vernetzung eines Gebäudes auf sicherheitsrelevante Dinge untersucht werden muss, da dieses Protokoll auch nur sicher sein kann, wenn der Rest gesichert ist.[40] [41]

An diesen Beispielen der verschiedenen Funk-Protokolle, kann man erkennen, dass es keine hundertprozentige Sicherheit gibt und durch die Nutzung solcher Technologie immer Schwachstellen existieren werden. Da die verwendeten Verschlüsselungsverfahren auf 128 Bit AES Basis längst nicht mehr aktuell sind, ist vielen Sicherheitsforschern und IT-Sicherheitsexperten seit Jahren bekannt. Oftmals gibt es keine Schwachstellen im eigentlichen Verschlüsselungsalgorithmus, sondern in der Implementierung von Geräten der Hersteller. Zweitens sind Systeme längst nicht mehr sicher wenn allein nur die Funktionsweise versucht wird geheim zu halten. Dies ist kein Hinderungsgrund für Kriminelle, die Funktionsweise schnell herauszufinden.

### 4.5.4 Kabelgesteuertes Smart Home

Die älteste Variante, sein Gebäude zu vernetzen, stellt kabelgestütztes Smart Home dar. Schon Anfang der 90er Jahre wurde eine solche Vernetzung durchgeführt. Heutzutage ist die kabelgesteuerte Variante noch der Favorit vieler Anwender, da kabelgesteuerte Systeme als sicher und nicht störanfällig deklariert werden. Leider ist eine solche Installation recht teuer und nicht in jedem Gebäude anwendbar. In vielen älteren Gebäuden ist eine solche Gebäudeautomation aus finanzieller so wie wirtschaftlicher Sicht nicht tragbar. Doch die vielen, fast unendlichen Möglichkeiten sein Haus zu vernetzen, sind ein großer Vorteil dieser Technik. In diesem Bereich gibt es viele verschiedene Anbieter, die mehr oder weniger bekannt sind. Den bekanntesten Hersteller und Standard stellt KNX dar, gefolgt von LON und BACnet. Die beiden letzten Standards sollen keine so wichtige Rolle in der Betrachtung

[40] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 28-30 (08.08.2016)
[41] Vgl. itwissen.info, 2015 (08.08.16)

spielen und werden deswegen etwas kürzer behandelt.[42]
KNX ist der Nachfolger und die technische Weiterentwicklung des europäischen Installationsbus (EIB), wurde international standardisiert (ISO/IEC 14543) und findet Anwendung in der Gebäudeautomation sowie Heimautomation. In einem KNX System werden viele verschiedene Komponenten unterschiedlichster Hersteller eingesetzt und unterstützt. Die Funktion von KNX besteht aus einem Netzwerk, zwischen Sensoren und Aktoren, die eine bestimmte Steuerung im Haus übernehmen, wenn eine Eingabe erfolgt. Diese Sensoren und Aktoren sind über ein Kabel, den sogenannten BUS miteinander verbunden und kommunizieren darüber. Somit hat jedes Gerät eine eigene physikalische Adresse, die, vorausgesetzt sie kommt nur einmalig vor, in der Programmierung frei vergeben werden kann. Das Prinzip ist gleich dem des Ethernets und der IP-Vergabe im Netzwerk. Die Sensoren senden Nachrichten aus, die die Aktoren auffangen und daraufhin reagieren. Dabei gibt es die Möglichkeit, dass ein Sensor mehrere Aktoren ansteuern kann. Einen Vorteil von KNX stellen die unterschiedlichsten Arten von Übertragungsmedien dar. Wie alle kabelgesteuerten Smart Home Systeme gilt natürlich die bekannte Zwei-Draht-Leitung (KNX Twisten Pair) als Hauptübertragungsmedium. Doch es gibt auch andere, wie z.B. die Übertragung über das 230 V Netz (KNX Power Line) und die Übertragung per Funk (KNX Radio Frequency). Die Konfiguration erfolgt über die datenbankbasierte „Engineering Tool Software“ (ETS) die herstellerunabhängig ist und für jedes KNX-System genutzt werden kann.[43]
Der zweite Standard LON (Local operating Network) wurde von dem US-amerikanischen Unternehmen Echelon Corporation in den 90er Jahren entwickelt. Dieser Standard wurde von IEC und der ISO anerkannt und im Jahren 2008 normiert und wird seitdem als LONTalk-Protokoll bezeichnet. Ein LON Netzwerk besteht aus unterschiedlichen Knoten, die auch als Sensoren oder Aktoren bezeichnet werden können und besitzen alle einen frei programmierbaren Chip (genannt Neuron). Diese Knoten sind in verschiedene Netzwerkvariablen untergliedert, die für die Kommunikation mit anderen Knoten zuständig sind. Die Kommunikation ist dabei unabhängig von der Zentrale und kann Informationen direkt untereinander austauschen. Der Aufbau an sich ist ähnlich dem des KNX-Systems und besitzt ebenfalls eine softwareseitige Verwaltung des Netzwerkes mit LNS (LonWorks Network Services), welche auf einer Client-Serverarchitektur beruht und eine integrierte Datenbank besitzt. Das Lon Netzwerk kann über die bekannte Zweidrahtleitung (LON FT-10), über ein 230 V Netz (LON-PLT) sowie über das Ethernet (LON IP) kommunizieren.[44,45]
Der dritte und letzte Standard dieser Arbeit ist das BACnet, was „Building Automation

[42] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 22 (08.08.2016)
[43] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 22 (08.08.2016)
[44] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 24 (08.08.2016)
[45] Online: Vgl. baunetzwissen.de (08.08.2016)

and Control networks“ bedeutet und in der ISO 16484 als Kommunikationsprotokoll ebenfalls standardisiert wurde. Er zählt zu den ältesten Standards in dieser Betrachtung und wurde bereits Ende der 80er Jahre von der ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) entwickelt. Die Kommunikation erfolgt über sogenannte BACnet-Objekte, die jedem Teilnehmer als Server-Objekte zur Verfügung gestellt werden. Dabei wird vor allem viel Wert auf die IT-Sicherheit gelegt und es bietet diverse Sicherheitsvorkehrungen.[46,47]

### 4.5.5 Die IT-Sicherheit von kabelgesteuertem Smart Home

Die Betrachtung der IT-Sicherheit ist bei kabelgesteuerten Smart Home Systemen eine echte Herausforderung, da diese Technologie einige bekannte Schwachpunkte aufweist und bei falscher Handhabung durchaus unsicherer als Funk-Technik ist. Die bereits genannten Standards KNX, LON und BACnet zählen zu den bekanntesten, jedoch wird vor allem das Hauptaugenmerk auf die KNX-Variante fallen, da dieser Standard die häufigste Anwendung findet, aber auch erhebliche Schwachstellen aufweist. Um Zugang zu diesem System zu erlangen, reicht es oftmals aus, einen physikalischen Zugang zu besitzen. Deshalb wurde lange Zeit die Notwendigkeit der Absicherung der Kommunikation nicht als beachtenswert angesehen bzw. nur unzureichend bis gar nicht abgesichert. Doch auch schon damals war die Gefahr durchaus bekannt, wie die Fernsehserie „Akte X“ beweist. Diese Serie, die im September 1994 startete, behandelte das „intelligente Gebäude“ in Folge 7 von Staffel 1. Das Firmengebäude einer Computerfirma wurde überwacht und war in verschiedenster Art und Weise verknüpft. Daran kann man erkennen, dass solche Vernetzungen keine Entwicklung der modernen Zeit sind, sondern durchaus schon damals zum Einsatz kamen, wenn auch nur in begrenztem Rahmen. Durch die Weiterentwicklung ist die Notwendigkeit einer funktionierenden IT-Sicherheit beim Einsatz solcher Systeme unbedingt notwendig. Im Folgenden sollen noch einmal die einzelnen Standards in Bezug auf ihre Sicherheit erklärt werden.

**KNX**

Das KNX-Protokoll ist sehr weit verbreitet und bietet sich ideal zur Umsetzung einer Gebäudeautomation mit der Möglichkeit einer Erweiterung der Komponenten und unterschiedlicher Übertragungswege an. Durch die einfache und komfortable Bedienung ist KNX besonders beliebt. Leider stellt die IT-Sicherheit nicht die Stärke von KNX dar. Viele Hersteller hielten es nicht für nötig, KNX ausreichend abzusichern, da ein physikalischer Zugang nötig ist, um Manipulationen am System vorzunehmen. Doch dadurch, dass immer mehr Gebäude, vor allem auch öffentliche Bereiche, mit Gebäudeautomation ausgestattet werden, ist das KNX Protokoll sehr

[46] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 26 (08.08.2016)
[47] Online: vgl. baunetzwissen.de (08.08.2016)

anfällig gegenüber kriminellen Aktivitäten .

Das Problem ist, dass das KNX bzw. EIB Protokoll aus den 90er Jahren stammt, wo das Thema IT-Sicherheit in privaten Haushalten noch keine große Rolle spielte. Ein Beispiel eines Sicherheitsproblems, ist die unverschlüsselte Kommunikation zwischen Server und den Komponenten. In privaten Häusern war dies viele Jahre kein Problem. Aber durch die Weiterentwicklung und Vernetzung von Komponenten auch außerhalb des privaten Umfeldes, entstehen neue Sicherheitsprobleme. Lichtsteuerungen für Außenbereiche, Steuerung des Pools oder auch die Öffnung des Briefkastens von außerhalb stellen erhebliche Probleme dar, da die Kommunikation über Kabel auch die außerhalb befindlichen Komponenten erreichen muss. Somit ist es einfach, diese zu demontieren und per PC mit einem BUS-Anschluss zu verbinden. Schon hat man Zugriff auf das innere System ohne im Gebäude zu sein. Zum Ansteuern einzelner Komponenten wird kein Passwort benötigt. Ein Passwortschutz ist meist nur im Konfigurationsmenü hinterlegt, aber nicht zwingend erforderlich und wird deshalb oftmals vernachlässigt.[48]

Wie unsicher und einfach manipulierbar KNX-Systeme sind, hat Dipl. Inf. Mark Semmler im Jahr 2014 mit seiner Anwendung „Draugr“ auf seiner Website beschrieben und erklärt.

„Draugr“ besteht aus einem einfachen Raspberry Pi und einem RT-OneWire Modul von Busware. Der Raspberry Pi ist ein kleiner Einplatinencomputer der entwickelt wurde, um vor allem jungen Menschen, das Programmieren und Tüfteln mit IT möglichst praxisnah zu vermitteln. Der Preis ist deshalb relativ gering (ca. 35 USD). Mittlerweile gibt es den Einplatinencomputer in der dritten Generation mit enormem Anstieg an Rechen- und Performanceleistung.

Die teuerste Komponente war Test das Rot-Modul von Busware (ca. 130€), welche dazu dient, mit dem KNX-Protokoll zu kommunizieren. Der Vorteil dieser Kombination des Einplatinencomputers und des ROT-Moduls ist der Stromverbrauch, der sowohl im Betrieb als auch im Standby-Modus extrem niedrig ist. Die Funktion der Anwendung ist das Abhören des BUS-Verkehrs sowie die Dekodierung der empfangenen Nachrichten der Systemkomponenten. In dem Programm kann man gewisse Standby-Zeiten einstellen, in dem die Anwendung in einen Ruhemodus verfällt. Nach dieser Ruhephase, beginnt das Programm mit der Aussendung von KNX-Telegrammen über eine im Netz freie oder über eine in der Kommunikation bereits definierte Adresse. Die Kommunikation zwischen den eigentlichen Komponenten, kann somit durch ein aggressives Standby-Zeitfenster so stark beeinflusst werden, dass das System unbrauchbar wird. Der Entwickler hat sich, auf Grund der dadurch entstehenden Sicherheitsprobleme entschieden, den Quellcode nicht zu veröffentlichen.

Das große Sicherheitsproblem liegt auch darin, dass diese Verwendung vielleicht

[48] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 23 (10.08.2016)

nicht unbedingt in privaten Haushalten zum Einsatz kommt, sondern vielmehr in öffentlichen Gebäuden wie z.B. Hotels. Durch den extrem niedrigen Stromverbrauch des Raspberry Pi, reicht eine Powerbank aus, um ihn versteckt zu installieren und z.B. in einem Hotelzimmer nach dem Anschluss an den BUS, in der Zwischendecke verschwinden zu lassen. Die Möglichkeit einer kabellosen Steuerung des Raspberry Pi erhöht das Sicherheitsrisiko zusätzlich, da somit auch von der Ferne aus zugegriffen werden kann.[49] Eine weitere Schwachstelle stellt das ETS-Tool dar, was jederzeit über Onlinehändler bezogen werden kann. Somit haben es Kriminelle noch einfacher in Systeme einzudringen, falls sie physikalischen Zugang zum System besitzen. Das ETS-Tool mit dazugehöriger Software darf deshalb nicht in die falschen Hände gelangen, da dies eine potentielle Gefahr darstellt
Doch die IT-Sicherheit wird auch bei den Herstellern von KNX-BUS Technik neuerdings näher betrachtet. Somit wurden auf der Messe Light + Building 2016 einige Komponenten vorgestellt, die die Kommunikation von Komponenten im Außenbereich mit 128 Bit AES verschlüsseln. Bis jedoch jeder Hersteller diese Verschlüsselung einsetzt, wird noch einige Zeit vergehen. Vor allem für den Einsatz in öffentlichen Gebäuden ist es erforderlich, die komplette Kommunikation zwischen den Komponenten zu verschlüsseln und somit einen großen Beitrag zur IT-Sicherheit zu leisten. Bestehende Systeme besitzen diese Schwachstellen jedoch auch weiterhin und es wird auf jedem Fall notwendig sein, diese Komponenten bzw. vielleicht sogar das komplette System auszutauschen.

**LON**

Das LON Protokoll besitzt für die bessere Gewährleistung der Sicherheit einen Dienst, der in einem Netzwerk durch Einträge in eine Konfigurationstabelle, die Absender eines Telegrammes mit Hilfe eines „Authentication Bits“ als berechtigt oder nicht berechtigt kennzeichnet. Somit wird die unberechtigte Nutzung von nicht autorisierten Komponenten verhindert. Zusätzlich können Schlüsselwörter in einer 48 Bit Länge vergeben werden. Dieses Verschlüsselungsverfahren wird immer dann aktiviert, wenn ein „Authentication Bit“ übermittelt wird. Die Funktionsweise besteht dabei aus einer 64 Bit Zahl, die vom Empfänger per Zufall generiert wird und diese Nachricht an den Sender zurückschickt. Der Sender wandelt daraufhin diese Zufallszahl in den 48 Bit Schlüssel um und schickt diese Nachricht per „Replay“ zurück an den Empfänger. Diese Nachricht wird dann ebenfalls mit dem 48 Bit Schlüssel umgewandelt und bei Übereinstimmung sind diese beiden Knoten authentifiziert und eine Kommunikation ist genehmigt. Die Sicherheit besteht dabei aber nur aus der Nichtkenntnis des 48 Bit Schlüssels und der zufallsgenerierten Zahl von unbekannten Komponenten. Das diese Verschlüsselung aber schon lange nicht mehr sicher ist und sogar schon 128 Bit-Verschlüsselungen umgangen werden

[49] Online: vgl. Mark Semmler, mark-semmler.de, 2014 (18.07.2016)

können, ist es nur ein Frage der Zeit, dass dieses Verfahren ersetzt oder verbessert werden muss. Zusätzlich gibt es bei der Nutzung von LON IP einen Sicherheitsalgorithmus namens MD5 (Message-Digest Algorithm 5).[50] Dieser kryptographische Algorithmus wurde im Jahre 1991 von Ronald L. Rivest entwickelt. Durch das Alter des Algorithmus ist es heutzutage aber ein sehr unsicheres Verfahren und kann mit wenig Aufwand manipuliert werden.[51] Somit ist die Sicherung des LONTalk Protokolls mehr als unzureichend und allein durch die bekannte Brute Force Attacke schnell angreifbar. Hier bedarf es einiger Neuerungen und Verbesserungen seitens der Entwickler.

**BACnet**

Dieser Standard wird zu den sichersten im kompletten kabelgesteuerten Smart Home Bereich gezählt, stetig weiterentwickelt und an die neuen Gegebenheiten angepasst. Die Sicherheit dieses Standards wird in dem BACnet Addendum 2008-g noch einmal näher zusammengefasst und spezifiziert. Dabei wird die Sicherheit durch die Authentifizierung der Geräte und Teilnehmer sowie durch eine Verschlüsselung ermöglicht. Das Sicherheitsmodell verwendet zu Umsetzung sogenannte „shared secret“ Schlüsselpaare. Solch ein Schlüsselpaar besteht dabei aus einem Signatur- sowie einem Verschlüsselungskey. Dabei muss man beachten, dass es sechs Arten dieser Schlüsselpaare gibt, die unterteilt werden in „General-Netzwerkzugriffsschlüssel, Benutzerauthentifizierungsschlüssel, anwendungs-spezifische Schlüssel, Installationsschlüssel, Verteilungs- und Device-Master-Schlüssel.“[52]
Eine Kommunikation zwischen den Komponenten kann dabei nur bei einer möglichst synchronen Zeit stattfinden, da die Kommunikation mit einem Zeitstempel arbeitet und bei der Verwendung einer anderen Zeit blockt. Zusätzlich ist der Authentifizierungsschlüssel für den Ursprung der Daten auf zwei Geräte limitiert. Wird diese Limitierung umgangen z.B. durch Klonen etc. kann die Authentifizierung nicht sichergestellt werden und die Kommunikation wird geblockt. Durch diese Verfahren ist der BACnet Standard die beste Wahl für eine sichere Verwendung von kabelgesteuertem Smart Home.[53]

Natürlich bietet jedes System Schwachstellen und auch hier kann keine vollständige Sicherheit gewährleistet werden. Deshalb sollte man sich mit dem Thema der IT-Sicherheit auseinandersetzen und versuchen, auch bereits existierende Systeme, abzusichern. Zahlreiche Hersteller unternehmen viele Anstrengungen, um ihre Produkte sicherer zu gestalten und haben die Notwendigkeit von IT-Sicherheit auch

[50] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 25 (10.08.2016)
[51] Online: vgl. Daniel Rehbein, daniel-rehbein.de, 2016 (10.08.2016)
[52] Kranz, H.R. BACnet Gebäudeautomation 1.12. cci Buch, 2013 (10.08.2016)
[53] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 26 und S.47-48 (10.08.2016)

in der privaten Anwendung zur Kenntnis genommen. Bei der Nutzung von kabelgesteuertem Smart Home sollte deshalb immer die Zugänglichkeit und Breite der Vernetzung, vor allem in Bezug auf den Außenbereich, im Auge behalten werden.

## 4.6 Hauptangriffsziel: Smartphone

Die mobilen Endgeräte, speziell Mobiltelefone, erfuhren innerhalb eines sehr geringen Zeitraumes eine enorme Weiterentwicklung. Smartphones dienen mittlerweile nicht mehr nur als Telefon, sondern vielmehr als mobiler PC und Multimediagerät. Durch diese Entwicklung sind die Nutzungsmöglichkeiten schier unendlich. So spielt das Smartphone bei der Gebäudeautomation, eine entscheidende Rolle. Es dient als Steuerungseinheit für das vernetzte Gebäude und erlaubt die bequeme Steuerung von unterwegs. Doch genau diese Funktionalität wirft in Bezug auf die IT-Sicherheit immer wieder große Bedenken auf. In vielen IT-Sicherheitsanalysen gilt bis heute das Betriebssystem Microsoft Windows auf einem Computer als Hauptangriffsziel für Cyberkriminalität. Durch die weite Verbreitung und den komplexen Einsatz dieser Distribution gelingt es Hackern recht einfach, Schadsoftware und Viren zu programmieren, die überall Systeme befallen können. In vielen Magazinen und Berichten wird deshalb immer empfohlen, für sicherheitsrelevante Systeme eine Linux-Distribution zu verwenden. Doch zu behaupten, dass Linux ein sicheres System ist, ist eine recht fahrlässige Aussage, da immer mehr Geräte mit einem Linux basierten Betriebssystem ausgestattet sind. Darunter zählen übrigens auch die Endgeräte, die auf Android basieren. Im Grunde genommen gibt es kein sicheres System und die Behauptung, dass Linux sicherer als Windows ist, ist schon lange nicht mehr aktuell.[54]

„Was soll denn schon passieren, es ist doch nur ein Smartphone!“[55]

Wenn man auf öffentlichen Plätzen Fragen zum Thema Sicherheit und Smartphone stellen würde, wäre dies mit hoher Wahrscheinlichkeit eine häufige Antwort. Doch es ist heutzutage recht häufig, dass viele Personen ihr Smartphone häufiger nutzen als den heimischen Computer. Deshalb ist dies ein attraktives Ziel für Kriminelle, da durch neue Applikationen und Möglichkeiten der Nutzung neue Angriffsziele entstehen. Beispiele wären hierfür Applikationen wie E-Mail, Facebook, diverse Banking- und Bezahlapplikationen. Die Gefahr einer finanziellen Katastrophe ist nicht unbedingt das Schlimmste, sondern die Verletzung der Privatsphäre und das diese Schäden nicht mehr behoben werden können. Mit relativ einfachen Mitteln können Telefongespräche belauscht werden, E-Mails und Nachrichten gelesen und sogar Kameras angezapft werden. Was für viele nur in Hollywoodfilmen möglich ist,

[54] Online: vgl. Henning Uhle, henning-uhle.eu, 2016 (14.07.2016)
[55] Online: Henning Uhle, henning-uhle.eu, 2016 (14.07.2016)

gibt es schon seit vielen Jahren und wird von diversen Nachrichtendiensten zur Überwachung von Personen genutzt. Das gefährliche daran ist, das diese Aktivitäten meist nicht erkannt werden und man von solchen Aktionen nichts mitbekommt. Deshalb ist dies ein nicht zu unterschätzendes Risiko, da auch in Bezug auf die Gebäudeautomation neue Möglichkeiten der Überwachung und Spionage entstehen. Die Hauptschwachstelle bei der Sicherheit eines Smartphones bleibt aber der Nutzer selber. Vielen Nutzern ist heute noch nicht bewusst, dass ihr Smartphone ein richtiger Computer ist und deshalb die gleichen Schutzmaßnahmen genießen sollte.

### 4.6.1 Die Infizierung eines Smartphones

Die Infizierungsarten eines Smartphones sind recht vielseitig. In den meisten Fällen erfolgt sie, wenn eine modifizierte oder eigens entwickelte Software auf das Gerät übertragen wird. Die Wege können E-Mail Anhänge, Bluetooth oder MMS-Nachrichten sein. In den meisten Fällen merken die Anwender gar nicht, dass eine Schadsoftware auf ihrem Gerät installiert wurde.

Ein schöner Vergleich stellt der Hollywood Blockbuster „Non-Stop“ mit dem Schauspieler Liam Nesson dar. Dieser Film aus dem Jahre 2014 handelt von einer Flugzeugentführung, in dem der Air Marschall zusehen muss, wie alle 20 Minuten eine Person stirbt, wenn die Forderungen der Entführer nicht erfüllt werden. Doch der bzw. die Entführer sind unbekannt und melden sich nur über das Mobiltelefon per SMS. Eine Szene in diesem Film verdeutlicht die Infizierung eines Smartphones. Ein Fluggast, ein Technikexperte, hilft dem Air Marschall und schreibt einen Schadcode für das Mobiltelefon des Entführers, um es auch im Lautlosmodus klingeln zu lassen. Die Übermittlung geschieht über das Versenden per Anhang an die Nummer des Entführers. Und wenige Augenblicke später klingelt es beim vermeintlichen Täter.

Viele Personen fragen sich nun, wie die Software auf das Handy gelangen konnte, ohne den Download zu bestätigen. Die Antwort ist ganz einfach. In vielen Applikationen wie E-Mail oder auch WhatsApp sind automatische Downloads von Anhängen in den meisten Fällen voreingestellt. Dabei ist es egal, in welcher Form der Schadcode übermittelt wird. Ein Schadcode kann an eine einfache PDF oder ein Bild angehangen werden. Ist der Download einmal erfolgt, ist es in den meisten Fällen zu spät. Im Grunde genommen kann ein Smartphone auf dem gleichen Weg infiziert werden wie ein Computer, d.h. beim Surfen im Internet, bei Downloads oder beim Austausch von Daten zwischen zwei Geräten. Doch besondere Vorsicht ist bei öffentlichen Dockingstationen für Smartphones gegeben. Durch Ladestationen in Flughäfen, Bars oder auch in öffentlichen Verkehrsmitteln können Viren, Würmer und Trojaner unbewusst übertragen werden.

## 4.6.2 Android vs. Apple

Smartphones zählen heutzutage zu unseren alltäglichen Dingen, somit ist der Markt recht vielseitig und viele Hersteller werben um die Gunst des Kunden. Doch die eigentliche Betrachtung soll nicht bei den Herstellern der Smartphones liegen, sondern vielmehr bei der Wahl des Betriebssystems. Die weit verbreitetsten und bekanntesten Betriebssysteme sind Android und iOS. Das Windows Mobile sowie das Blackberry OS sollen hierbei keine Berücksichtigung finden, da sie nur einen Bruchteil am Markt einnehmen. In vielen Bereichen haben die Android- und iOS- Betriebssysteme Vor- und Nachteile und natürlich auch unterschiedliche Sicherheitsvorkehrungen.

### 4.6.2.1 Die Sicherheit des Android-Betriebssystems

Das bekannteste Betriebssystem für Smartphones dürfte Android sein. Android dient aber nicht nur als Software-Plattform für Mobiltelefone, sondern findet auch Anwendung in diversen Mediaplayern, Netbooks und Tablet-PCs.
Android wurde vom Konzern Google Inc., Betreiber der gleichnamigen Suchmaschine, entwickelt und durch die Open Handset Alliance entwickelt. Der Grundbaustein liegt dabei auf dem Linux-Kernel. Wichtig ist dabei zu wissen, dass das Betriebssystem eine freie Software (Open-Source) und somit quelloffen ist.[56] Dadurch kann man für dieses Betriebssystem eigene Anwendungen entwickeln und Funktionen verbessern. Die Verbreitung von Android -Geräten ist von 2011 mit knapp 26 % auf knapp 85 % im Jahre 2014 angestiegen. Dies bedeutet, das Android über dreiviertel des gesamten Weltmarktes im Bereich der Smartphone-Betriebssysteme, einnimmt.
Die Entwicklung wird immer weiter vorangetrieben und die aktuellste öffentlich eingesetzte Version ist die 6.0.1, die im November 2015 veröffentlicht wurde. Google gibt jeder Version, seit V1.5, eine Bezeichnung einer Süßigkeit. Somit heißt die neuste offizielle Version „Marshmallow“.[57]

| **Versionsnummer** | **Bezeichnung** | **Weiterhin unterstützt?** |
|---|---|---|
| 1.0 | Base | Nein |
| 1.1 | Base_1.1 | Nein |
| 1.5 | Cupcake | Nein |
| 1.6 | Donut | Nein |
| 2.0.x / 2.1 | Eclair | Nein |
| 2.2.X | Froyo (Frozen Yoghurt) | Nein |
| 2.3.X | Gingebread | Nein |

[56] Online: vgl. wikipedia.org – Android-Betriebssystem, 2016 (09.08.2016)
[57] Online: vgl. Tobias Költzsch, golem.de, 2014 (09.08.2016)

| | | |
|---|---|---|
| 3.X.X | Honecomb | Nein |
| 4.0.X | Ice Cream Sandwich | Nein |
| 4.1.X / 4.2.X / 4.3.X | Jelly Bean | Nein |
| 4.4.X | KitKat | Nein |
| 5.0.X/ 5.1.X | Lollipop | Nein |
| 6.0.X | Marshmallow | Ja, aber nur 6.0.1 |
| 7.0.X | Nougat | Ja (Beta) |

**Tabelle 1** Übersicht Android-Versionen
Online: wikipedia.org, 2016 (09.08.2016)

Die Kritik an dem Betriebssystem in Bezug auf die Sicherheit liegt ganz klar in der Open Source Verwendung. Doch es gibt noch diverse andere Kritiken, die beachtet werden sollten. Den größten Kritikpunkt in Bezug auf Sicherheit stellt der PlayStore dar, worüber neue Applikationen, Filme und Musik gekauft und runtergeladen werden können. Auf Grund der Open-Source Software, ist die Entwicklung eigener App´s und deren Bereitstellung im Store recht einfach. Die Applikationen werden durch Google seit 2012 zwar überprüft, es gibt aber immer wieder Meldungen über den Befall von App´s mit Schadsoftware. Im Grunde genommen ist es recht einfach, Programme von Drittanbietern zu installieren. Ein weiterer ausschlaggebender Punkt sind die diversen Berechtigungen der Programme. Viele benötigen die Zustimmung des Nutzers, um auf verschiedene Funktionen des Smartphones zuzugreifen. Oft ist es der Fall, dass die Berechtigungen nichts mit der Funktionalität des Programmes zu tun haben, sondern vielmehr eine Sammlung der Nutzerdaten darstellt. Leider ist es meist so, dass viele Anwender die Berechtigungen bestätigen, ohne nachzudenken zu welchen Sicherheitsproblemen es, vor allem in Bezug auf die Privatsphäre, führen kann. Ein weiterer negativer Aspekt sind die sogenannten Administratorrechte auf Offiziellen Android- Geräten. Das Betriebssystem sieht jeden Besitzer als normalen Nutzer an, ähnlich einem Benutzerkonto eines Windows-PCs. Dies bedeutet, dass man nicht die komplette Berechtigung über sein Smartphone besitzt und viele Dinge nicht ändern kann. Besitzt man Root-Rechte, könnte man verschiedenen Programmen bestimmte Berechtigungen entziehen und somit die Gefahr bannen. Es gibt Tools, die auch für den normalen Nutzer diese Arbeit verrichten können. Leider sind diese aufwendig gestaltet und benötigen zusätzlichen Speicherplatz und Ressourcen. Durch die weite Verbreitung dieses Betriebssystems werden die Angriffe für Kriminelle besonders interessant, da sie dadurch ein weites Gefährdungsspektrum abdecken können. Die nachfolgende Grafik soll die Versionsverbreitung von Android anhand einer Statistik etwas genauer darstellen.

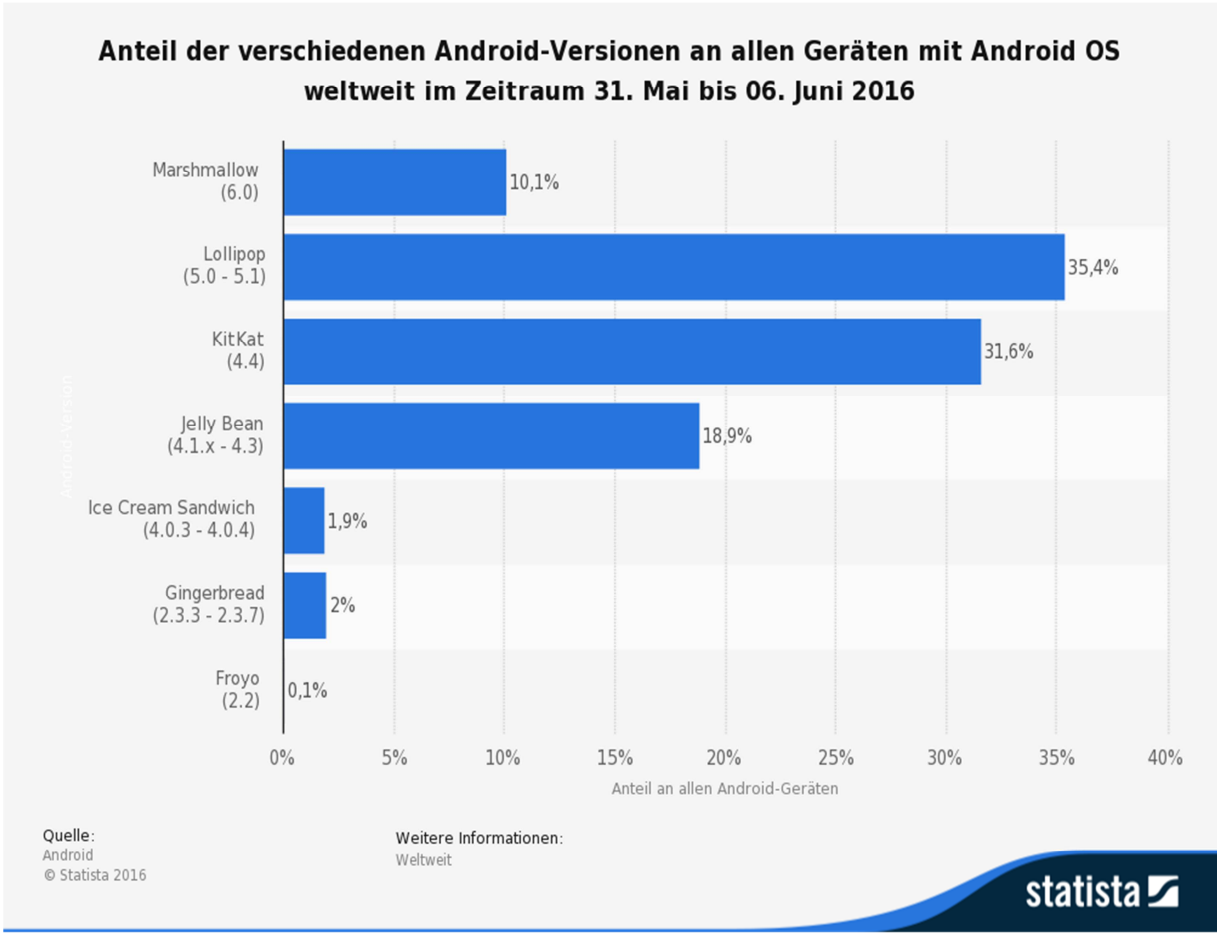


**Abbildung 7** Android-Versionen weltweit
Online: statista.com, 2016 (14.07.2016)

### 4.6.2.2 Die Sicherheit des Apple-Betriebssystems

Ein weiteres sehr bekanntes Betriebssystem, ist das iOS aus dem Hause Apple für iPhone, iPad und iPod. Im Gegensatz zu Android, wird das eigene Betriebssystem auch nur für die eigene Hardware eingesetzt und ist deshalb nicht für andere Hersteller lizensiert. Das iOS besteht aus Unix mit Mach-Kernel und ist ein eigenes Betriebssystem und basiert nicht wie Android auf einem bereits existierenden Betriebssystem wie Linux.[58]

| Versionsnummer | Weiterhin unterstützt |
|---|---|
| 1.0.X / 1.1.X | Nein |
| 2.0.X / 2.1.X / 2.2.X | Nein |
| 3.0.X / 3.1.X / 3.2.X | Nein |
| 4.0.X / 4.1.X / 4.2.X / 4.3.X | Nein |
| 5.0.X / 5.1.X | Nein |
| 6.0.X / 6.1.X | Nein |
| 7.0.X / 7.1.X | Nein |

[58] Online: vgl. developer.apple.com, 2013 (09.08.2016)

| | |
|---|---|
| 8.0 / 8.0.X / 8.1.X / 8.2 / 8.3 / 8.4 / 8.4.1 | Nein |
| 9.0 / 9.0.X / 9.1 / 9.2.X / 9.3 / 9.3.2 | Ja, aber nur 9.3.2 |
| 10.0 | Ja (Beta) |

**Tabelle 2** Übersicht IOS-Versionen
Online: wikipedia.org, 2016 (09.08.2016)

Vergleicht man Android und Apple, fällt dem versierten User auf, dass es in punkto Sicherheit diverse Vorteile gegenüber Android gibt.
Ein Vorteil bezieht sich auf den Store, indem neue Applikationen heruntergeladen werden können. Der Apple-Store prüft erst neu eingestellte Applikationen, bevor diese veröffentlicht werden. Dazu kommt, das nicht jeder Hobby-Programmierer Programme für das Betriebssystem iOS entwickeln darf, da die API´s nicht wie bei Android öffentlich zugänglich sind und zudem ein Entwicklerstatus vorhanden sein muss, ehe man überhaupt die Möglichkeit besitzt, selbst etwas zu programmieren. Deshalb ist für einen sicheren Umgang mit Smart Home immer ein Apple-Gerät die besser Alternative. Doch auch dieser Hersteller besitzt Schwachstellen und kann keine hundertprozentige Sicherheit garantieren. Zudem gibt es eine Möglichkeit, wie bei Android, sein iOS-System mithilfe eines „Jailbreaks“ zu verändern, um neue Möglichkeiten und neue Funktionen für sein iOS-Gerät freizuschalten. Doch diese Vorgehensweise sollte für einen sicheren Umgang vermieden werden, da dadurch alle Sicherheitsmaßnahmen des Herstellers umgangen werden und somit eine Infizierung nur eine Frage der Zeit darstellt. Die Mythen, dass ein Apple-Gerät nicht angreifbar ist, sind definitiv falsch. Das Apple durchaus weniger gefährdet ist als Android-Geräte ist klar, jedoch gibt es diverse iOS-Bedrohungen, die immer weiterentwickelt werden und gezielt diese Systeme angreifen sollen. Deshalb ist es genauso wichtig ein Apple-Gerät mit ausreichenden Sicherheitsvorkehrungen wie Virenschutz, iOS-Updates usw. zu schützen.

# 5 Basisschutz – Mögliche Schutzmaßnahmen

In diesem dritten und letzten Abschnitt sollen nun einige Varianten gezeigt werden, um den Umgang und die Verwendung von Smart Home und den verschiedensten Komponenten so sicher wie möglich zu gestalten. Die folgenden Möglichkeiten sind Schutzmaßnahmen, die von dem Anwender überprüft und bei Bedarf umgesetzt werden sollten. Für eine gute Sicherheit der eingesetzten Smart Home-Komponenten wird angeraten, Produkte von renommierten Herstellern zu beziehen, die einiges an Sicherheit bieten. Deswegen wird auf diese Sicherheit in diesem Abschnitt nicht noch einmal eingegangen, sondern nur auf die Sicherheitsmaßnahmen, die nach Erwerb und bei der Installation durch den Anwender umgesetzt werden sollten. Für viele Nutzer werden diese Sicherheitsmaßnahmen selbstverständlich sein, doch Gebäudeautomation wird in Zukunft auch von Personen eingesetzt, die dieses technische Verständnis nicht besitzen und deshalb gezielt durch diese Arbeit darauf hingewiesen werden, welche Maßnahmen notwendig sind, um sein „intelligentes Haus“ sicher zu gestalten.

## 5.1 Installation der Geräte

Der erste Punkt zum Basisschutz von Smart Home ist die Installation der Geräte. Natürlich ist vor der Installation eine ausreichende Planung erforderlich, welche Bereiche des Gebäudes automatisiert werden sollen und auf welche Bereiche verzichtet werden kann. Denn, je mehr Geräte und Komponenten in einem Smart Home vernetzt sind, umso mehr Schwachstellen und Angriffsflächen werden geboten. Somit ist eine gesunde Abwägung der benötigten Vernetzung ein absolutes Muss.
Bei der Einrichtung sollte vor allem bei kabelgesteuerter Technik darauf geachtet werden, dass die Verlegung von Komponenten in den Außenbereich eines Gebäudes ein erhebliches Sicherheitsrisiko darstellt, da viele Hersteller ihr Kommunikationsprotokoll, welches über den BUS kommuniziert, nur unzureichend bis gar nicht verschlüsseln. Es sollte darauf geachtet werden, dass die Zugänglichkeit der Komponenten in schwer zugänglichen Bereichen liegt oder auf Funk-Technik beim Einsatz im Außenbereich zurückgegriffen wird. Es gibt auch diverse Möglichkeiten in diesen Komponenten Manipulationsschutzmaßnahmen in Form eines Abziehschutzes einzubringen. Dadurch erkennt das Gerät die Manipulation und kann Alarm geben etc., wie es bei professionellen Sicherheitsanlagen wie z.B. Einbruchmeldeanlagen schon viele Jahre zum Einsatz kommt. Sicherlich muss man auch im Innenbereich des Gebäudes darauf achten, die Zugänglichkeit zu unterbinden, vor allem im Einsatz dieser Technik in einem Mehrfamilienhaus oder Gebäuden wo mehrere Personen Zugriff haben und eine gezielte Manipulation schnell durchzuführen wäre. Ein weiterer Aspekt ist die

Unterbringung der Zentrale oder des Servers, je nachdem welches System man verwendet, in einem separaten Raum, welcher elektronisch bzw. mechanisch extra abgesichert werden sollte. Was jetzt sehr utopisch klingt, kann durchaus bald zum regulären Sicherheitskonzept eines Smart Home Systems gehören.[59]

## 5.2 Sichere Passwörter

Eine weitere wichtige Absicherung ist nicht nur die Verwendung von Passwörtern, um den Zugang zu verhindern, sondern auch die Absicherung der Passwörter durch eine Vielzahl an verschiedenen Kombinationen zwischen Groß- und Kleinschreibung, Zahlen sowie Sonderzeichen. Die einfachste Methode, ein Passwort zu knacken ohne einen physikalischen Zugang zum System zu besitzen, ist die Brute-Force-Methode, die im oberen Abschnitt schon erklärt wurde. Die Wahl sicherer Passwörter sollte immer gleichbleibend ausfallen, egal ob bei dem schon genannten WLAN-Passwort, Passwörtern für Onlinekonten oder diversen anderen Passwörtern. Die folgende Tabelle soll verdeutlichen, welche Schwierigkeiten auf einen Hacker zukommen, wenn er per Brute-Force-Methode ein Passwort knacken will, was nach Einhaltung dieser Tipps abgesichert wurde.[60]

| Passwort besteht aus | Mögliche Kombinationen | Benötigte Zeit zum Entschlüsseln |
|---|---|---|
| **5 Zeichen**<br>(3 Kleinbuchstaben,<br>2 Zahlen) | $36^5$= 60.466.176 | 60.466.176 /<br>2.000.000.000 =<br>**0,03 Sekunden** |
| **7 Zeichen**<br>(1 Großbuchstabe,<br>6 Kleinbuchstaben) | $52^7$= 1.028.071.702.528 | 1.028.071.702.528 /<br>2.000.000.000 =<br>514 Sekunden =<br>**ca. 9 Minuten** |
| **8 Zeichen**<br>(4 Kleinbuchstaben,<br>2 Sonderzeichen,<br>2 Zahlen) | $68^8$= 457.163.239.653.376 | 457.163.239.653.376 /<br>2.000.000.000 =<br>228.581 Sekunden =<br>**ca. 2,6 Tage** |
| **9 Zeichen**<br>(2 Großbuchstaben,<br>3 Kleinbuchstaben,<br>2 Zahlen,<br>2 Sonderzeichen) | $94^9$= 572.994.802.228.616.704 | 572.994.802.228.616.704 /<br>2.000.000.000 =<br>286.497.401 Sekunden =<br>**ca. 9,1 Jahre** |
| **12 Zeichen**<br>(3 Großbuchstaben,<br>4 Kleinbuchstaben,<br>3 Sonderzeichen,<br>2 Zahlen) | $94^{12}$= 475.920.314.814.253.376.475.136 | 475.920.314.814.253.376.475.136 /<br>2.000.000.000 =<br>237.960.157.407.127 Sekunden =<br>**ca. 7,5 Millionen Jahre** |

**Abbildung 8** Passwortkombinationen
Online: password-depot.de, 2014 (28.07.2016)

Es ist aber ebenso wichtig ein Passwort zu wählen, welches keine logische Abfolge von Zahlen und Buchstaben enthält, wie z.B. Nachname und Geburtsjahr des

[59] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 61-62 (07.08.2016)
[60] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 56-57 (10.08.2016)

Nutzers. Hacker kennen die oft verwendete Kombination solcher Passwörter und werden die Möglichkeiten als erste ausprobieren. Natürlich sind solche Passwörter für den Nutzer einfach zu merken, aber nicht sehr optimal. Passwörter wie z.B. „KHP92_8FG30“ wären eine sichere Kombination ohne Logischen Zusammenhang. Natürlich sollten diese Passwörter aber auch nicht auf einem Zettel notiert und unter der Tastatur abgelegt werden. Dieser Klassiker ist leider heutzutage noch weit verbreitet, ist aber für einen Kriminellen eine Einladung, wenn er Zugang zum Gebäude besitzt.[61]

## 5.3 Verschlüsselte Kommunikation

In allen Bereichen der IT sollte immer auf eine ausreichende Verschlüsselung geachtet werden, die natürlich auch als sicher gilt. Viele Hersteller bieten in ihren Smart Home-Komponenten eine Verschlüsselung an, die aber nicht immer sicher ist, da es so viele mögliche Protokolle gibt, Informationen usw. zu verschlüsseln. Das bedeutet, dass Verschlüsselung nicht gleich Verschlüsselung ist und eine Versicherung darstellt, dass dadurch die Daten geschützt bleiben. Das Ziel einer Verschlüsselung ist immer die originalen Daten so zu transformieren, dass die mitgeschnittenen Daten keine logische Rekonstruktion ermöglichen und somit keinen Wert für einen Hacker haben. Doch da natürlich die originalen Daten für den legalen Benutzer trotzdem verwendbar bleiben müssen, ergibt sich logischer Weise hieraus eine Schwachstelle, denn es muss immer eine Möglichkeiten geben, die transformierten Daten in das Original zurück zu transformieren. Dabei muss zwischen den asymmetrischen sowie symmetrischen Verschlüsselungsverfahren unterschieden werden.[62]

### 5.3.1 Asymmetrisches Verschlüsselungsverfahren

Das wohl bekannteste Asymmetrische Verschlüsselungsverfahren ist die Verwendung von SSL/ TLS bei HTTPS Webseiten. Die SSL (Secure Sockets Layer) Verschlüsselung, auch bekannt über den Nachfolger TLS (Transport Layer Security), ist ein hybrides Verschlüsselungsverfahren und dient zur Sicherung der Kommunikation im Internet. Die SSL Verschlüsselung findet heutzutage in vielen Bereichen Anwendung, eine bekannte Anwendung ist die neue SSL Verschlüsselung bei dem Nachrichtendienst WhatsApp. Die neuste Version der SSL Verschlüsselung ist TLS 1.2 und ist seit 2008 im Einsatz. Die Weiterentwicklung zu TSL 1.3 in seit Anfang 2016 in Planung. Die Funktionsweise bedient sich der Verbindung von Client zu einem Server. Der Server muss anhand der Anfrage, sich durch ein Zertifikat authentifizieren, was der Client dann auf Echtheit überprüft. Diese Funktion kann auch umgekehrt passieren, sodass der Client dem Server ein Zertifikat schickt. Die

[61] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 56-57 (10.08.2016)
[62] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 53-54 (10.08.2016)

Verschlüsselung basiert auf einem öffentlichen Schlüssel und einem privaten Schlüssel. Der öffentliche Schlüssel wird in einem öffentlichen Verzeichnis abgelegt, wo jeder Zugriff darauf hat. Der private Schlüssel bleibt privat und wird nicht wie der öffentliche Schlüssel über das Internet versendet. Die Nachricht oder Information wird mithilfe des öffentlichen Schlüssels verschlüsselt und an den zuständigen Empfänger gesendet. Dieser kann nur mithilfe des privaten Schlüssels diese Nachricht entschlüsseln und lesen. Besitzt man diesen Schlüssel nicht, ist der Zugriff auf die Information gesperrt und es bedarf eines großen Aufwandes diesen zu knacken. Trotz einiger erfolgreicher Hackerangriffe und diversen Schwachstellen, ist das SSL Verfahren ein durchaus sicherer Verschlüsslungsalgorithmus und wird vielen Kriminellen die Arbeit erheblich erschweren.
Bei der Anwendung in Smart Home ist vor allem die Konfiguration der Zentrale über eine Weboberfläche immer eine Gefahr. Einige Hersteller, wie HomeMatic bieten die Kommunikation mittels SSL über die Ferne an und erreichen somit eine erhebliche Verbesserung der Sicherheit. Deshalb sollte darauf geachtet werden, dass diese Möglichkeit vorhanden ist und gegebenenfalls aktiviert wird. [63] [64] [65]

### 5.3.2 Symmetrisches Verschlüsselungsverfahren

Eines der wohl bekanntesten Symmetrischen Verschlüsselungsverfahren stellt die AES-Verschlüsselung dar. Bei der Betrachtung von Smart Home Produkten, vor allem in Bezug auf Funktechnik, wird dieser Verschlüsselungsalgorithmus in die Augen fallen. Die AES-Verschlüsselung zählt zurzeit zu einer der am meist verbreitetsten Verschlüsselungen von Funkprotokollen, aber auch von diversen anderen Anwendungen. AES bedeutet ausgeschrieben „Advanced Encryption Standard“ und zählt zu den Blockchiffrierungen. Es verwendet zum Entschlüsseln und Verschlüsseln jeweils die gleichen Schlüssel. Die AES-Verschlüsselung wird über die sogenannte Block- bzw. Schlüssellange definiert und es existieren heutzutage 128 Bit, 192 Bit sowie 256 Bit. Dieses Verfahren hat den Vorteil das es relativ schnell funktioniert, aber auch den Nachteil, das der Key, der zum Entschlüsseln benötigt wird, immer durch die Kommunikation zweier Komponenten übertragen wird und somit mitgeschnitten werden kann. Trotzdem ist die AES-Verschlüsselung eine sichere Methode und ist auch vom BSI als sichere Methode gekennzeichnet und abgenommen. Um einen solchen Schlüssel knacken zu können, benötigt man einiges an Kenntnis und Rechentechnik. Natürlich geht die Entwicklung voran und die Möglichkeiten einer schnelleren Verarbeitung mittels Brute Force usw. steigen. Deswegen sind 128 Bit Schlüssel heutzutage noch recht sicher, aber in wenigen Jahren mit Sicherheit nicht mehr anzutreffen, da 128 Bit Schlüssel schon

[63] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 54-55 (10.08.2016)
[64] Online: vgl. ssl-trust.com (06.08.2016)
[65] Online: Jan Kaden, connect.de, 2015 (26.07.2016)

heutzutage geknackt werden können, wenn auch nur mit erheblichen Aufwand und Kenntnissen. Aber natürlich ist die Sicherheit von Smart Home auch von anderen Faktoren abhängig.[66] [67]

## 5.4 Router

Eine wichtige Komponente für die Nutzung von Smart Home, auch von unterwegs, ist der Router. Der Router an sich ist dazu da, um eine Kommunikation über das Netzwerk zu ermöglichen. Dies bedeutet, dass jeder Haushalt oder jede Firma, die über einen Internetzugang verfügt, einen Router besitzen. Die Verbreitung der IT in deutschen Haushalten soll das folgende Bild einmal verdeutlichen.

**Ausstattung mit Gebrauchsgütern**

**Ausstattung privater Haushalte mit PC, Internetzugang und Breitbandanschluss im Zeitvergleich**

| Ausstattung | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Angaben in % | | | | | | | | | | |
| PC | 67 | 71 | 73 | 76 | 78 | 80 | 81 | 81 | 83 | - | 86 |
| Internetzugang | 58 | 61 | 65 | 69 | 73 | 77 | 77 | 79 | 82 | 84 | 85 |
| Breitbandanschluss | - | - | - | 50 | 60 | 70 | 72 | 75 | 78 | 81 | 82 |

- = Nichts vorhanden.

**Abbildung 9** Ausstattung mit Gebrauchsgütern (IT)
Online: destatis.de, 2015 (12.07.2016)

### 5.4.1 WLAN-Schlüssel

Eines der wohl wichtigsten Sicherheitsvorkehrungen des heimischen Netzes ist die Absicherung des Wireless LAN. Fast jeder Haushalt mit einer Anbindung an das „World Wide Web“ besitzt heutzutage einen Router, mit integrierter WLAN-Funktion. Durch mögliche Verbindungen der verschiedensten Endgeräte wie Smartphone, Tablet, Notebook oder sogar TV-Geräte stellt dies bei schlechter Absicherung eine große Gefahr für das heimische Netz dar. Das gilt auch für die Gebäudeautomation, die normalerweise über solche Endgeräte mit dem Router kommuniziert und somit die Steuerung ermöglicht. Um einem möglichen Missbrauch des WLAN vorzubeugen, ist eine ausreichende Absicherung per Passwort und die Nutzung einer guten Verschlüsselungsmethode notwendig. Im Normalfall ist heutzutage WPA2 als Verschlüsselungsmethode voreingestellt und stellt eine gute Sicherheit dar. Die etwas älteren Verfahren WPA oder WEP werden heutzutage kaum noch eingesetzt. Allerdings sind diese Verschlüsselungsmethoden durchaus noch gängig, da viele noch im Einsatz befindliche ältere Router WPA2 nicht unterstützen. Die unsicherste Methode bleibt WEP, welche ohne viel Grundkenntnisse und Zeitaufwand mithilfe des Programmes „Aircrack-ng“ geknackt werden kann. Dieses

[66] Online: vgl. Roland Freist, pcwelt.de, 2014 (08.07.2016)
[67] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 54 (10.08.2016)

Programm, welches stetig weiterentwickelt wird, ermöglichst es außerdem ein WPA oder WPA2 zu knacken. Doch ist dies mit erheblichem Mehraufwand verbunden, da es heutzutage nur mittels Brute-Force ermittelt werden kann. Jedoch gibt es auch die Möglichkeit, diese Passwörter zu knacken, was im Selbsttest mit Hilfe von „Backtrack R5“ umgesetzt wurde. Die im Punkt 5.2 „Sichere Passwörter“ erklärte Vorgehensweise, sollte ebenfalls beim WLAN-Schlüssel angewendet werden.
In den meisten Fällen verwenden die Hersteller lange und ausreichend sichere Standardpasswörter mit 12 oder 16 Stellen. Jedoch ist es immer wieder üblich, dass die Hersteller zur Vergabe von Passwörtern einen Standardalgorithmus verwenden, der durch Tools von Hackern ermittelt werden kann. Somit ist es von Vorteil, nach Erhalt des Routers, bei der Einrichtung ein eigenes Passwort zu vergeben mit mindestens zwölf Zeichen unter Verwendung von Buchstaben, Zahlen sowie Sonderzeichen. Oft werden Nachnamen oder Geburtsdaten verwendet. Dies sollte tunlichst vermieden werden, da dies von kundigen Personen schnell missbraucht werden kann. Das WLAN-Passwort ist erst durch eine willkürlich gewählte Zeichenkombination ausreichend geschützt.[68]

### 5.4.2 Konfigurationsmenü

Der nächste Schritt zur Absicherung des Routers ist der Schutz des Konfigurationsmenüs, um eventuelle Modifikationen durch Unbefugte zu verhindern. Bei den meisten Herstellern sind im Auslieferungszustand nur Standardpasswörter wie „0000“ oder gar keine Passwörter vergeben. Da der Zugriff auf den Router immer über die im Normalfall voreingestellte Adresse geschieht, ist es eine Leichtigkeit, das Konfigurationsmenü des Routers aufzurufen. Es ist im Grunde genommen genauso zu verfahren wie bei der Vergabe des WLAN-Passwortes, um einen optimalen Schutz zu gewährleisten.

### 5.4.3 Firmware

Als dritten und letzten Punkt bei der Betrachtung der Sicherheit von Routern stellt die Firmware eine weitere Schwachstelle dar. Unter Firmware versteht man die produktbezogene Software eines technischen Gerätes. Diese Software ist meist gar nicht oder nur mit speziellen Mitteln austauschbar und zwingend erforderlich für die Nutzung der Produkte. Firmware ist mit den Hardwarekomponenten eines Gerätes fest verbunden, die ohne diese Software nicht nutzbar wären. Anwendung findet Firmware in allen Bereichen wie z.B. Smartphones, Computer, Fernbedienungen, aber auch in Smart Home- Produkten wie Lichtschalter, Klingeln und Lampen. Es gibt zwei Arten von Firmware, einmal das eigentliche Betriebssystem der Komponenten und zweitens das „Vor-Betriebssystem“ zum Laden des eigentlichen

[68] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 52 (10.08.2016)

Kernbetriebssystems. Als ein Beispiel ist hier das BIOS der Hauptplatine eines PC´s zu nennen .

Bei vielen Herstellern werden die Firmwarestände ihrer Produkte stetig verbessert, um Sicherheitsprobleme zu lösen und neue Funktionen zu implementieren. Vor allem Smartphone-Besitzern sollten diese Updates bekannt vorkommen, da Google, der Hersteller der Android OS, in regelmäßigen Updates die Funktionen der Smartphones erweitert. Doch neue Funktionen und Möglichkeiten können auch neue Schwachstellen generieren, wenn diese nicht ausgiebig getestet wurden. Dies stellt einen regelmäßigen Kreislauf dar.

Vielen Nutzern ist heutzutage aber die Möglichkeit eines Firmware- Updates in Bezug auf Router noch fremd. Und genau diesen sorglosen Umgang nutzen kriminelle Computerspezialisten aus, um unerlaubten Zugriff zu erlangen. Deshalb ist das Einspielen der Updates ein wichtiger Punkt, genauso wichtig wie die regelmäßigen Updates bei Microsoft. Bei manchen Herstellern, z.B. der Telekom mit ihrem Produkt „Speedport“, ist standardmäßig die Aktualisierung der Firmware eingeschaltet und sollte nicht deaktiviert werden, wenn man sich Sicherheitsproblemen nicht aussetzen möchte. Es ist darauf zu achten, welcher Router-Typ verwendet wird, da nicht jeder Router, vor allem die älteren Generationen, diese Funktion bietet. Deshalb sollte regelmäßig nach Updates gesucht und diese manuell eingespielt werden. Eine Anleitung zur Vorgehensweise findet man gut beschrieben auf der jeweiligen Herstellerwebsite. Bei anderen Herstellern wie AVM oder Vodafone kann diese Verfahrensweise durchaus abweichen. Doch auch für diese Produkte gibt es einfach beschriebene Anleitungen im Internet. Sollte ihr Router, altersbedingt, keine Unterstützung durch Updates genießen, wäre es ratsam, diesen Router durch ein neueres und moderneres Modell auszutauschen.[69]

## 5.5 Client-Sicherheit

Eine weitere Maßnahme ist die Absicherung der Clients, die durch die Benutzung von Gebäudeautomation ein Sicherheitsrisiko darstellen können. Clients können in diesem Fall mobile- sowie Desktop-Geräte sein. Ist ein solcher Client unsicher oder nicht ausreichend geschützt, ermöglicht er die Infizierung des Systems und aller darin befindlichen Geräte. In den nachfolgenden Unterpunkten für mobile Geräte sowie Desktopclients sollen Möglichkeiten und Maßnahmen beschrieben werden, die zum Basisschutz eines Jeden gehören sollten.[70]

[69] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 48-49 (10.08.2016)
[70] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 60-61 (10.08.2016)

### 5.5.1 Mobile-Clients

Durch den Einsatz von mobilen Endgeräten und Anwendungen, eröffnen sich neue Schwachstellen, die ein erhebliches Sicherheitsrisiko darstellen können, da man seine Daten und Informationen des eigenen Netzes etc. nach außen trägt. Durch den weit verbreiteten Einsatz von mobilen Geräten, ist die Gefahr eines Verlustes oder einer Infizierung in fremden Netzen wesentlich höher als bei fest installierter Technik. Der Einsatz von Sicherheitssoftware wie Antivirenscanner etc. ist Pflicht. Es ist ebenfalls darauf zu achten, dass die Anwendungen und die Betriebssysteme einer regelmäßigen Updateeinspielung unterzogen werden. Außerdem ist die Nutzung von Displaysperren durch Muster, oder besser durch ein Passwort anzuwenden. Durch Nutzung beider Sperrmöglichkeiten ergibt sich ein zusätzlicher Punkt an Sicherheit. Ein weiterer Aspekt ist die Erstellung von regelmäßigen Backups, um einen kompletten Datenverlust zu kompensieren. Dazu gibt es gute Anwendungen in den Stores der Hersteller, die meistens sogar kostenlos genutzt werden können. Zusätzlich bieten die Gerätehersteller eigene Software für den PC an, um das Smartphone schnell sichern zu können, wie z.B. Samsung mit dem eigenen Programm „KIES“. Zudem gibt es meist die Möglichkeit ein verlorenes Smartphone über eine Zusatzfunktion im System, welche vorher eingestellt werden muss, zu orten und sogar sperren zu lassen. Der nächste Punkt ist besonders wichtig für Android-Nutzer bei der Installation von Anwendungen aus dem PlayStore. Viele Anwendungen benötigen Berechtigungen, die für die Funktionsweise nicht benötigt werden. Deshalb Apps´s mit kritischen Berechtigungen nur herunterladen, wenn diese für die Anwendung benötigt werden, z.B. eine Taschenlampe benötigt keinen Zugriff auf ID oder Internet des Smartphones. Außerdem ist darauf zu achten keine Anwendungen aus unbekannten Quellen zu installieren. Zum Schutz davor ist auf Android Smartphones diese Installation erst nach einer Extra- Abfrage durch den Anwender installierbar. Zudem sollten öffentliche WLAN-HotSpots nur im Notfall genutzt werden und in einem solchen Netz keine wichtigen Anwendungen wie Banking etc. geöffnet werden, um das Mitschneiden und Abfangen von Informationen zu unterbinden. Natürlich ist auch die Öffnung einer E-Mail unbekannten Ursprungs eine Gefahr, genau wie bei der Nutzung eines Computers. Diese E-Mails sollte gleich gelöscht bzw. die Anhänge nicht heruntergeladen werden. Eine weitere Möglichkeit sich zu schützen, ist die Installation von Werbeblockern, die auch Popups und Weiterleitungen durch das Anklicken von ungewollten Werbebannern unterbinden. Häufig kommt es vor, dass viele Nutzer Bluetooth aktiviert haben und nicht deaktivieren. Über diese Schnittstelle können ebenfalls unerlaubte Zugriffe erfolgen, also sollte man Bluetooth deaktivieren. Der letzte Punkt behandelt die Preisgabe von Informationen über das Internet, d.h. nur das preisgeben, was man will oder zwingend erforderlich ist. Außerdem ist es wichtig, dass vor allem bei der Nutzung von Online-Banking die Sicht auf das Smartphone für andere verwehrt bleibt. Hier

gibt es die Möglichkeit einer speziellen Schutzfolie, die den Bildschirm aus bestimmten Blinkwinkeln unleserlich macht. Das Wichtigste ist jedoch der sensible Umgang mit dem Smartphone durch den Nutzer und die Einhaltung dieser Tipps. Somit ist die Sicherheit eines Smartphone durchaus gewährleistet und macht es Kriminellen schwer, die Sicherheitsfunktionen zu umgehen.[71] [72] [73] [74]

### 5.5.2 Desktop-Clients

Desktopclients sind im Smart Home Bereich nicht so weit verbreitet, da vieles im „smarten“ Umgang mit einem mobilen Client erledigt wird. Jedoch stellen diese Clients auch eine potentielle Gefahr dar und sollten deshalb einer intensiven Betrachtung auf die IT-Sicherheit unterzogen werden. Desktopclients sind „stationäre“-PC´s. Die meisten Nutzer verwenden das Betriebssystem Microsoft Windows und sollten deshalb auch die regelmäßigen Updates aktiviert haben Dadurch werden Sicherheitslücken geschlossen und neue Funktionen implementiert. Natürlich gilt dies auch für andere Systeme wie Linux und MAC. Ebenfalls, wie bei den bereits aufgezählten Sicherheitsmaßnahmen der mobilen Clients, sollte ein Antivirenscanner installiert sein und darauf geachtet werden, dass dieser regelmäßige Updates erfährt. Ein weiterer wichtiger Punkt ist die Verwendung einer Firewall. Die Firewall dient als Schutz vor unerwünschten Netzwerkzugriffen. Sie besteht aus einer Softwarekomponente, die den Datenverkehr überwacht und nach festgelegten Regeln entscheiden darf, ob diese Daten durch die Firewall durchgelassen werden dürfen.[75] Ein normaler Windows Rechner besitzt standardmäßig die Microsoft Windows Firewall und sollte deshalb auch eingeschaltet werden. Für komplexere und größere Netzwerke gibt es zusätzliche Firewall-Lösungen, die aber im privaten Sektor noch keine große Rolle spielen, aber durchaus in der weiteren Vernetzung Einzug halten werden. Zur Einstellung und Konfiguration des Systems sollte ebenfalls ein sicherer Browser verwendet werden. Gute Browser wären z.B. Firefox, Google Chrome oder Opera. Auch dabei sollte auf regelmäßige Updates geachtet und die installierten Plug-Ins wie Adobe Flash regelmäßigen Updates unterzogen werden, da gerade Adobe-Produkte öfters Sicherheitsprobleme aufweisen. Eine weitere Maßnahme wäre die Absicherung des Zuganges durch Verschließen des Raumes und Verwendung eines Passwortes, was die Nutzung verhindern soll. Die Passwortverwendung ist eine sehr effektive Sicherheitsmaßnahme und sollte selbstverständlich sein. Sie gilt aber heutzutage zu den schwächsten aller Sicherheitsvorkehrungen, da z.B. Windows-benutzerpasswörter in wenigen Minuten geknackt werden können. Da die schnellste

[71] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 60-61 (10.08.2016)
[72] Online: vgl. Claudia Frickel, pc-magazin.de, 2016 (10.08.2016)
[73] Online: vgl. android-user.de, 2013 (10.08.2016)
[74] Online: vgl. Jens Gerke, wdr.de, 2016 (10.08.2016)
[75] Online: vgl. computeranleitungen.de, 2016 (10.08.2016)

Methode aber ein physischer Zugang ist, sollte deshalb der Zugang immer durch Abschließen etc. verhindert werden.[76]

## 5.6 KNX Spezifische Sicherheitsmaßnahmen

Wie schon mehrfach beschrieben, gibt es im Einsatz von kabelgesteuerten Smart Home-Systemen einige Schwachstellen. In der Anwendung von KNX-Technik sollte die Möglichkeit der Manipulation durch den Einsatz eines KNX-Guard verhindert werden. Dieser KNX-Guard ist eine zusätzliche Komponente eines Systems, welches nach der Installation und Einrichtung der Funktionen keinen Gerätezugriff über physikalische Telegramme mehr ermöglicht. Somit wird die Möglichkeit mithilfe der ETS-Software unberechtigt Manipulationen vorzunehmen, verhindert. Eine Alarmfunktion ist ebenfalls an Bord, wenn das Gerät den Versuch einer Manipulation entdeckt. Der KNX-Guard kann in drei Stufen eingestellt werden. Die erste Stufe, die „hohe Sicherheit“, ermöglicht einen Lesezugriff, aber keine Möglichkeit von Schreibvorgängen. Die zweite Stufe wäre die „höchste Sicherheit“, in der Veränderungen nur nach Entfernen des KNX-Guards möglich sind und somit keine Lese- sowie Schreibrechte vergibt. Die dritte und letzte Stufe wäre die benutzerdefinierte Sicherheit. Der BUS kann in dieser Stufe mithilfe eines „EIBDoktors“ aktiviert, deaktiviert oder parametriert werden. Ebenfalls können bereits eingespielte Telegramme durch die Verwendung eines Zeitstempels nicht erneut eingespielt werden, was die Möglichkeit von Replay-Angriffen verhindert. Eine weitere Möglichkeit zu Sicherung des KNX Systems wäre die Verwendung von EIBsec, welches eine Weiterentwicklung des EIB Ansatzes ist und in der TU München entwickelt wurde. Hiermit kommt die fehlende AES Verschlüsselung auf 128 Bit Basis zum Einsatz. Diese Verschlüsselung wird zusätzlich in kommende KNX-Komponenten integriert werden. Durch diese Erweiterungen lässt sich die BUS-Kommunikation zwischen den einzelnen Modulen gut überwachen. Es gibt durchaus weitere Maßnahmen, z.B. Sabotageschutz der Komponenten, die an eine bestehende Alarmanlage angebunden werden können. Doch dies sind alles Zusatzfunktionen und beim Kauf nicht enthalten. Deswegen sollte der Nutzer vorher gut überlegen, welche Sicherheitsvorkehrungen möglich sind.[77]

[76] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 60-61 (10.08.2016)
[77] Vgl. Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 46-47 (07.08.2016)

# 6 Fazit

Das Fazit dieser Arbeit lautet: Es gibt keine 100%ige Sicherheit von Smart Home! In einigen Jahren wird Smart Home ein alltäglicher Begleiter in unserem Leben sein und zu jedem modernen Wohnen dazugehören. Deshalb müssen die Personen, die solch eine Vernetzung in ihrem Eigenheim unterbringen wollen eine gewisse Akzeptanz aber auch Offenheit gegenüber dieser Technologie entwickeln. Smart Home kann viele Bereiche unseres Lebens einfacher, sicherer oder einfach nur besser gestalten als jemals zuvor. Durch diese Technologie eröffnen sich neue Möglichkeiten der Vernetzung und Anwendung von IT in den unterschiedlichsten Lebensbereichen. Doch die Personen müssen in diesen Bereichen den Umgang mit der IT lernen und ein Gefühl dafür entwickeln, welche Neuerungen und Vernetzungen sinnvoll sind. Die Absicherung der IT ist längst nicht mehr die Aufgabe von Computerexperten und Administratoren von großen Unternehmen, sondern wird immer mehr zu einer alltäglichen Pflicht in unserem Leben. Es sollte sich zu einer Lebenseinstellung herausbilden. Schon längst sind die Vernetzungen in unserer Umwelt so weittragend, dass auch Menschen ohne große Computerkenntnisse lernen müssen, dass dies eine immer größere Bedeutung in ihrem Leben erlangt. Zudem müssen viele Hersteller ihre Sicherheitskonzepte überdenken und endlich einen entscheidenden Schritt in der IT-Sicherheit wagen. Viele Smart Home Systeme sind durchaus sicher, doch in wenigen Jahren total veraltet. Es müssen für Smart Home-Systeme neue Möglichkeiten der Absicherung geschaffen werden, um den Kriminellen das Handeln zu erschweren. Die Zeit ist nicht mehr fern, wo Einbrüche über den „Kühlschrank“ erfolgen, nur weil dieser mit diversen anderen Komponenten im Haus vernetzt ist. Die Cyberkriminalität steigt stetig und stellt heutzutage schon Polizei und Behörden vor entsprechende Herausforderungen. Zudem wird es kommen, wie schon beschrieben wurde, dass bei der Planung von Gebäuden nicht nur ein Architekt und Bauarbeiter etc. benötigt werden, sondern auch IT-Sicherheitsbeauftragte, die Vorschläge erarbeiten, welche Vernetzung wo durchzuführen ist, um Manipulationen zu verhindern.

Alles in allem gibt es erheblichen Nachholebedarf im Thema IT-Sicherheit und intelligentes Wohnen. Doch solchen Systemen gehört die Zukunft und sie stellen eine sinnvolle Neuerung in der Gebäudevernetzung dar. Deshalb sind die Sicherheitsbedenken durchaus nachzuvollziehen, sollten aber nicht davon abhalten, die schier unendlichen Möglichkeiten, die die Nutzung von Smart Home bietet, intelligent und kreativ weiter zu entwickeln.

# Quellenverzeichnis

Sascha Remmers, Falk Gaentzsch, Norbert Pohlmann: Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014
1. Auflage Handwerkskammer Rheinhessen

Manuel Schreiber: Zitat, 2015
In: http://www.chip.de/artikel/Philips-Hue-Raspberry-PI-Star-Wars-und-mehr-Geschenkideen-von-Manuel-Schreiber_86546566.html (13.07.2016)

wikipedia.org – Smart Home: Zitat, 2015

In: https://de.wikipedia.org/wiki/Smart_Home (13.07.2016)

Abbildung 1: Wachsende Angriffsfläche für Internetangriffe
In: http://www.internetworld.de/technik/cybercrime/gefaehrlichsten-cyber-schwachstellen-2016-1063605.html?page=1_attacken-unter-der-guertellinie (15.07.2016)

wertesysteme.de: 2014
In: http://www.wertesysteme.de/alle-werte-definitionen/s-t/sicherheit/ (05.07.2016)

duden.de
In: http://www.duden.de/rechtschreibung/Sicherheit (05.07.16)

Stefan Sackmann: Enzyklopädie der Wirtschaftsinformatik, 2014
In: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit/index.html (06.07.2016)

Abbildung 2: Übersicht über die Aufgaben der IT-Sicherheit, 2012
In: http://www.linux-ag.com/uploads/images/grafiken/Torte_Trigonum_2_300x300.png (15.07.2016)

Abbildung 3: Angriffe auf Heim- und Gebäudeautomationssysteme
In: Sascha Remmers, Falk Gaentzsch, Norbert Pohlmann: Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014
1. Auflage Handwerkskammer Rheinhessen (08.08.2016)

wikipedia.org – Exploit: 2016
In: https://de.wikipedia.org/wiki/Exploit (21.07.2016)

wikipedia.org – Seitenkanalattacken: Zitat, 2016
In: https://de.wikipedia.org/wiki/Seitenkanalattacke (14.08.2016)

Christophe Tremlet, Kristin Rinorther: elektronikpraxis.vogel.de, 2013
In: http://www.elektronikpraxis.vogel.de/analogtechnik/articles/397781/index4.html (21.07.2016)

wikipedia.org – Man-in-the-Middle-Angriff: 2016
In: https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff (22.07.16)

Patrick Beuth: zeit.de, 2014
In: http://www.zeit.de/digital/datenschutz/2014-08/black-hat-2014-hotelzimmer-gehackt (28.07.16)

Boris Schiller: smarthomewelt.de – Z-Wave, 2015
In: http://smarthomewelt.de/z-wave-funksystem-home-automation-smarthome/ (29.07.2016)

Günther Ohland: pc-magazin.de – Übersicht Protokolle, 2013
In: http://www.pc-magazin.de/ratgeber/funkprotokolle-ueberblick-rwe-zwave-homematic-1530051.html (29.07.2016)

Boris Schiller: smarthomewelt.de – BidCos, 2015
In: http://smarthomewelt.de/bidcos-funkstandard-eq-3-hausautomation/ (29.07.2016)

htw-dresden.de: 2013
In: http://www2.htw-dresden.de/~wiki_sn/index.php5/HomeMatic (04.08.2016)

vgl.octopus-office.de – Bidirektional: 2016
In: http://www.octopus-office.de/info/bidirektionale-kommunikation/ (01.08.2016)

Abbildung 4: Aufbau HomeMatic Protokoll Header, 2013
In: http://www2.htw-dresden.de/~wiki_sn/index.php5/HomeMatic (04.08.2016)

siio.de: 2014
In: http://www.siio.de/sicherheitalarm/attacking-homematic-aes-signal-doch-nicht-sicher/ (02.08.16)

Hauke Gierow, golem.de, 2015
In: http://www.golem.de/news/smart-home-sicherheitsluecken-im-zigbee-protokoll-demonstriert-1511-117657.html (10.08.2016)

Abbildung 5: Angriffe auf Heim- und Gebäudeautomationssysteme
In: Sascha Remmers, Falk Gaentzsch, Norbert Pohlmann: Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 28
1. Auflage Handwerkskammer Rheinhessen (08.08.2016)

Abbildung 6: Angriffe auf Heim- und Gebäudeautomationssysteme
In: Sascha Remmers, Falk Gaentzsch, Norbert Pohlmann: Hausautomatisierung: IT-

Sicherheit im Haus der Zukunft, 2014, S. 29
1. Auflage Handwerkskammer Rheinhessen (08.08.2016)

Itwissen.info: 2015
In: http://www.itwissen.info/definition/lexikon/Z-Wave-Netz-Z-Wave-network.html (08.08.2016)

Baunetzwissen.de
In: http://www.baunetzwissen.de/standardartikel/Elektro_LON-Local-Operating-Network_153112.html (08.08.2016)

Mark Semmler: mark-semmler.de, 2014
In: https://www.mark-semmler.de/blog/knx-sicherheit-draugr-angriffe-gegen-knx-eib-hausautomatisierung (18.07.16)

Daniel Rehbein: daniel-rehbein.de, 2016
In: http://www.daniel-rehbein.de/hashwerte.html (10.08.2016)

Kranz, H.R. BACnet Gebäudeautomation 1.12. cci Buch, 2013
In: Angriffe auf Heim- und Gebäudeautomationssysteme
Sascha Remmers, Falk Gaentzsch, Norbert Pohlmann: Hausautomatisierung: IT-Sicherheit im Haus der Zukunft, 2014, S. 48
1. Auflage Handwerkskammer Rheinhessen (10.08.2016)

Henning Uhle: henning-uhle.eu, 2016
In: http://www.henning-uhle.eu/informatik/die-bedrohungslage-fuer-smartphones (14.07.16)

Wikipedia.org – Android-Betriebssystem, 2016
In: https://de.wikipedia.org/wiki/Android_(Betriebssystem) (09.08.2016)

Tobias Költzsch: golem.de, 2014
In: http://www.golem.de/news/mobile-betriebssysteme-android-laeuft-auf-fast-85-prozent-aller-smartphones-1408-108290.html (09.08.2016)

Tabelle 1: Übersicht Android-Versionen, 2016
In: https://de.wikipedia.org/wiki/Liste_von_Android-Versionen (09.08.2016)

Abbildung 7: Android-Versionen weltweit, 2016
In: http://de.statista.com/graphic/1/180113/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os.jpg (14.07.16)

Developer.apple.com: 2013
In:https://developer.apple.com/library/mac/documentation/Darwin/Conceptual/KernelProgramming/Mach/Mach.html (09.08.2016)

Tabelle 2: Übersicht IOS-Versionen, 2016
In: https://de.wikipedia.org/wiki/Apple_iOS (09.08.2016)

Abbildung 8: Passwortkombinationen
In: http://www.password-depot.de/know-how/brute_force_angriffe.htm (28.07.16)

Jan Kaden: connect.de, 2015
In: http://www.connect.de/ratgeber/smart-home-sicherheit-hacker-schwachstellen-schutz-tipps-3194959.html (26.07.2016)

ssl.trust.com: 2015
In: https://ssl-trust.com/Lexikon/SSL-Verschluesselung (06.08.2016)

Abbildung 8: Ausstattung mit Gebrauchsgütern (IT), 2015
In:https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/ZeitvergleichAusstattung_IKT.html (12.07.2016)

Roland Freist: pc-welt.de, 2014
In:http://www.pcwelt.de/ratgeber/Kommunikationsstandards_fuers_Smart_Home_im_Vergleich-Smart-Home-8947272.html (08.07.2016)

Claudia Frickel: pc-magazin.de, 2016
In: http://www.pc-magazin.de/ratgeber/it-sicherheit-trends-2016-neue-gefahren-und-wie-sie-sich-schuetzen-3195499.html (10.08.2016)

Jens Gerke: wdr.de, 2016
In: http://www1.wdr.de/verbraucher/digital/viren-trojaner-smartphone-100.html (10.08.2016)

android-user.de: 2013
In: https://www.android-user.de/14-tipps-die-ihr-android-handy-deutlich-sicherer-machen/ (10.08.2016)

computeranleitungen.de: 2016
In: https://www.android-user.de/14-tipps-die-ihr-android-handy-deutlich-sicherer-machen/ (10.08.2016)

Abbildung Anhang 3: android.gs
In: http://www.android.gs/wp-content/uploads/2013/05/Install-Boot-CWM-and-TWRP-Recovery-for-Samsung-Galaxy-S4-T-Mobile.jpg 18.07.16 (07.08.2016)

operating-system.org: 2001
In: http://www.operating-system.org/betriebssystem/_german/w-kernel.htm (10.08.2016)

droidwiki.de – Android Debug Bridge, 2016
In: https://www.droidwiki.de/wiki/Android_Debug_Bridge (10.08.2016)

pitu: linuxforen.de, 2005
In: http://www.linuxforen.de/forums/showthread.php?187978-remounten-einer-Partition-(rw-ro-Modi) (10.08.2016)

fibel.org
In: http://www.fibel.org/linux/lfo-0.6.0/node51.html (10.08.2016)

droidwiki.de – USB Debugging via Recovery, 2015
In: https://www.droidwiki.de/wiki/USB-Debugging_via_Recovery (10.08.2016)

# Anhangverzeichnis

# Beispiel: Umgehen der Sperre bei einem Android Smartphone

Nachfolgendes Beispiel soll verdeutlichen, wie einfach es ist, die Tastensperre eines Android-Smartphones zu umgehen, um die darauf existierenden Dateien einzusehen. Die Testphase soll demonstrieren, wie gefährlich der Verlust des Smartphones sein kann.
Durch den unerlaubten Zugriff konnten Dateien, Fotos, Videos, Nachrichten sowie diverse Applikationen und die damit verbunden Passwörter ausgelesen werden. Diese Demonstration soll zeigen, dass dadurch auch Smart Home Systeme angreifbar sind, wenn diese nicht direkt durch einen Hackerangriff betroffen sind, sondern nur durch ein Smartphone-Verlust ihre Sicherheit einbüßen können, wenn nicht sofort reagiert wird. Der Zeitaufwand dieses Testes betrug ca. eine Stunde und ist nach mehrmaligem Anwenden durchaus schneller durchzuführen.

## Das verwendete Smartphone


**Abbildung Anhang 1:** Samsung Galaxy S2 Ansicht

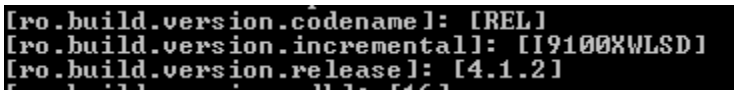


**Abbildung Anhang 2:** Build-Version

Das verwendete Smartphone, ist ein Samsung Galaxy S2 was am 19. Mai 2011 in Deutschland als Nachfolger des Samsung Galaxy S auf den Markt kam. Bei der Markteinführung besaß es die Android-Version 2.3.3 „Gingerbread“. Die Version dieses Smartphones betrug die letzte erhältliche Version 4.1.2 „JellyBean“ was 2016 noch ca. 20% der Smartphones betrifft.

Das Smartphone wurde durch eine Unachtsamkeit beschädigt. Das Touchscreen war dadurch nicht mehr nutzbar und reagierte auf keine Berührung. Das Display wies diverse grafische Fehler sowie verschwommen Texturen auf, d.h. es war durch die Tastensperre bzw. den Passwortschutz nicht mehr nutzbar.
Dem Besitzer war es wichtig die Daten zu retten, vor allem Videos und Bilder seiner Familie und Kinder. Im Normalfall kann man die Datensicherung per Anschluss an einen PC durchführen. Der Zugriff kann aber nur gewährt werden, wenn die Tastensperre deaktiviert wird. Dies war aber durch die Beschädigung des Touchscreens nicht mehr möglich, somit versagten auch Backup Tools wie das Samsung eigene Softwareprodukt „Kies“.
Ebenfalls waren einige Passwörter von Apps sowie dem hausinternen- und diversen anderen WLANS gespeichert. Dazu kam, dass der Besitzer eine Smart Home Zentrale besitzt, die er per App steuerte. Doch wie viele Nutzer legte er zur Sicherheit wichtige Passwörter auf seinem Handy in einer Textdatei ab, um so möglichst schnell das Vergessen zu umgehen. Ein erhebliches Sicherheitsrisiko, wie er später feststellte.

**Vorgehensweise:**

Um Zugriff auf das Smartphone zu bekommen sind gewisse Rechte erforderlich. Kauft man ein Smartphone mit dem Android Betriebssystem, besitzt man leider nur normale Nutzerrechte, wie schon zu Beginn erklärt. Hat man keine Administratorrechte, gibt es keinen Zugriff auf systemrelevante Dateien. Da die Speicherung wie bei einem PC auf dem Speicher erfolgt, müsste man theoretisch nur Administratorrechte sowie den Pfad der Datei wissen, um an solche systemrelevanten Dinge wie Passwörter und Zugriffsrechte zu gelangen. Es ist außerdem notwendig, die Entwickleroption USB-Debugging aktiviert zu haben, um einen vollen Zugriff über die ADB zu gewährleisten.

**Dinge die man benötigt:**

**- Odin (neuste Version 3.11.1)**
Odin ist ein einfaches Programm, was zum Rooten von Android Smartphones benötigt wird. Wichtig ist dabei, dieses Programm als Administrator auf dem PC auszuführen, um vollen Zugriff auf das Programm zu bekommen.

**- Micro USB-Kabel**
Hierbei reicht ein normales Micro-USB Kabel, was zum Ladevorgang bei jedem Smartphone dabei ist. Die Kabel sind international genormt und bei jedem Smartphone gleich.

**- Samsung Treiber für den PC**
Die zur Kommunikation benötigten Treiber werden bei einer Verbindung mit dem PC

automatisch installiert. Sollte dies nicht der Fall sein, so kann man sich ein Treiberpaket aus dem Internet herunterladen.

**- passender Kernel für das Smartphone**

Ein Kernel ist der Hauptkern jedes Betriebssystems, welches Prozess und Datenorganisationen festlegt. Man muss den Kernel ändern, um sich bzgl. Nutzerrechten auf Administratorlevel anzuheben. Wichtig ist zu wissen, welches Gerät und welche Android-Version man besitzt, um nicht den falschen Kernel aufzuspielen und somit das Smartphone unbrauchbar zu machen. Die aktuelle Android-Version kann auch durch die ADB vor dem Rooten über den Recovery-Modus ausgelesen werden. Sollte man keine Informationen über die Firmware wissen, so kann man sich über den Produktionscode, der sich unter dem Akku befindet, die Version ableiten. Wie sich der Code zusammensetzt ist ebenfalls im Internet sehr ausführlich beschrieben.[78]

**- Android Debug Bridge (abgekürzt adb)**

Das ADB ist eine Schnittstelle für Android Systeme, um eine Steuerung per USB-Kabel von einem Computer zu ermöglichen. Es gehört zu dem Android Software Development Kit (SDK), welches dazu da ist, eigene Software und Applikationen für Android zu programmieren, um sie z.B. im PlayStore zur Verfügung zu stellen. Es gibt auch eine einzelne Anwendung, die nur ADB umfasst (Minimal ADB and Fastboot) und für einen schnellen Einsatz besser geeignet ist.[79]

**- aktiviertes USB-Debugging**

Diese Funktion des Android Systems erlaubt es bei Aktivierung, das Smartphone in einen Debugging-Modus zu versetzen, wenn dieses an einen Computer angeschlossen wird. Diese Funktion ist standardmäßig deaktiviert und kann nur über die Entwickleroptionen aktiviert werden. Dies geschieht, wenn man über Einstellungen – Informationen über Telefon die Buildnummer sieben Mal hintereinander betätigt. Der USB-Debugging-Modus sollte im Normalfall deaktiviert sein, da es für Hacker umso einfacher ist, diese Funktion auszunutzen. Leider ist der Debugging-Modus auch auf anderem Wege aktivierbar, was das folgende Beispiel beweist.

**1. Schritt – Administratorrechte beschaffen**

Als ersten Schritt benötigen wir Administratorrechte. Im Linux-Bereich werden diese Rechte als „Root-Rechte“ bezeichnet und bedeuten so viel wie vollen Zugriff auf das Betriebssystem und die damit verbundenen Ressourcen und Komponenten. Da Android auf Linux basiert, ist es von Vorteil sich mit einfachen Befehlen auszukennen. Sollte man sich damit nicht auskennen, kann man sich recht schnell

[78] Online: vgl. operating-system.org, 2001 (10.08.2016)
[79] Online: vgl. droidwiki.de – Android Debug Bridge, 2016 (10.08.2016)

und einfach eine Übersichtsliste im Internet suchen. Das bedeutet das auch unerfahrene Nutzer diesen Schritt durchführen können, was das Sicherheitsproblem weiter verstärkt und bestätigt.
Der Root Vorgang soll in dieser Arbeit aber nicht näher erläutert werden, da es genug Anleitungen im Internet gibt, sowie heutzutage auch Anwendungen im PlayStore zur Verfügung stehen, die diesen Schritt automatisch durchführen können.

**2. Schritt – Recoverymodus aktivieren**

Jedes Smartphone besitzt zwei vorwiegend unbekannte Modi, die über eine Tastenkombination aufgerufen werden können. Die Modi sind ohne Touchscreen nur über die „Laut und Leiser Taste“ sowie mit dem Powerknopf als Bestätigung bedienbar.

Downloadmodus: Gleichzeitiges Drücken von Powerknopf – HomeButton – Leiser Button →Dieser Modus wird für das „rooten“ des Handys benötigt

Recoverymodus: Gleichzeitiges Drücken von Powerknopf – Home Button – Lauter Button

Der Recoverymodus ist wichtig, um Zugriff über ADB zu erlangen und die Passwortsperre zu umgehen. Ohne diesen Modus wäre eine Kommunikation mit dem PC nicht möglich. Dieser Modus wurde von den Entwicklern eingebracht, um bei Beschädigungen oder Softwareproblemen zumindest die enthaltenen Daten sichern zu können. Solche Hintertüren können aber somit für kriminelle Dinge, zweckentfremdet werden. Um aber den vollen Zugang zu erlangen, ist das Rooten unbedingt notwendig, weil dadurch Modifikationen wie z.B. „ClockworkMod Recovery“ neue und leichtere Kommunikationswege per ADB eingebracht werden.


**Abbildung Anhang** 3**:** ClockworkMod Recovery
andorid.gs (18.07.2016)

**3. Schritt – Zugriff über ADB**

Nun folgt der eigentliche Vorgang, um Zugriff auf das Smartphone zu erlangen. Im Normalfall sind durch das „Flashen“ des Systems Superuser bzw. Root Rechte vergeben worden. Doch dies hängt von der Custom ROM ab und ist nicht immer

enthalten z.B. wenn ein Herausgeber den Schutz vor Manipulationen an systemrelevanten Dateien wahren will. In diesem Falle besitzt man nur eingeschränkte Zugriffsrechte, so dass keine systemrelevanten Ordner eingesehen werden konnten, da kein USB-Debugging aktiviert wurde, bzw. nur eine Bestätigung auf dem Smartphone Bildschirm erschien, um diesen Modus durch den Computer zuzulassen. Da aber das Touchscreen defekt war, konnte dies nicht geschehen. Somit wurde das USB-Debugging manuell aktiviert. Nun folgt die schrittweise Abfolge und Erklärung der durchgeführten Schritte.


**Abbildung Anhang 4:** CMD-Administrator


**Abbildung Anhang 5:** Verzeichnisauswahl

Als Erstes öffnet man die Konsole von Windows (CMD) und führt diese als Administrator aus (Rechtklick- Ausführen als Administrator). Danach folgt die Navigation per Konsole in den Ordnerpfad der Android Debug Bridge per Ordnerauswahl „*cd*“. Nach dieser Navigation führt man die in diesem Ordner vorhandene „adb.exe“ durch die Eingabe von „adb“ aus. Danach folgt eine Abfolge von vielen Hinweisen und Möglichkeiten für die Steuerung per adb. Danach ist die Android Debug Bridge einsatzbereit.


**Abbildung Anhang 6:** ADB Device Scan

Daraufhin sollte man das im Recovery-Modus befindliche Smartphone mit dem PC verbinden und durch den Befehl „*adb devices*“ alle angeschlossenen Android-Geräte anzeigen lassen. Die Device-Nummer ist irrelevant und nur bei mehreren angeschlossenen Geräten von Bedeutung. Die Bezeichnung, die hinter der Nummer steht, ist für die Erkennung, ob man das Programm per ADB nutzen kann, wichtig. Steht dahinter „unauthorized“ besitzt man keine Root-Rechte und kann somit keinen Zugriff auf das Smartphone erlangen.

```
C:\Program Files (x86)\Android\android-sdk\platform-tools>adb devices
List of devices attached
304D19521D2BF98E        device


C:\Program Files (x86)\Android\android-sdk\platform-tools>adb root
adbd is already running as root

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb shell mount -o rw,
remount /;

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb pull /system/build
.prop build.prop
239 KB/s (2389 bytes in 0.009s)

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb pull /system/build
.prop C:\Users\Tobias\Desktop\Ordner\build.prop
166 KB/s (2389 bytes in 0.014s)

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb push C:\Users\Tobi
as\Desktop\Ordner\build.prop /system/build.prop
196 KB/s (2418 bytes in 0.012s)
```

**Abbildung Anhang 7:** USB-Debugging aktivieren

Um USB-Debugging ohne Bestätigung per Tastendruck durchzuführen, ist es zwingend erforderlich, dass das Smartphone schon gerootet wurde. Dies kann durch „*adb root*“ überprüft werden und ist durch eine positive Bestätigung erkenntlich. Um USB-Debugging aktivieren zu können muss man die Lese-Schreib-Rechte (rw) vergeben. Standardmäßig sind hier nur Lese-Rechte vergeben. Durch „adb shell mount –o rw, remount /;“ vergibt man diese Rechte. „In Linuxanwendungen ist die „Shell“ das Programm zur Kommunikation zwischen Anwender und dem Betriebssystem.“[80] Oft ist es auch der Fall, das bei Wartungen der Mount Zustand nur auf Lesen steht und somit mit Lese-Schreib-Rechten neu eingebunden werden muss (remount), Danach kopiert man mit dem Befehl „adb pull“ die Konfigurationsdatei build.prop und modifiziert diese mithilfe des Windows Editor und ergänzt am Ende der Datei die Zeile „persist.service.adb.enable=1“. Danach kopiert man die Datei zurück mit „adb push“ und überschreibt somit die alte Datei. Nun ist USB-Debugging standardmäßig eingeschalten und ohne Bestätigung auf dem Handydisplay nutzbar.[81][82]

```
C:\Program Files (x86)\Android\android-sdk\platform-tools>adb shell
root@android:/ # ls
acct                etc                 recovery.rc
app-cache           fota.rc             res
cache               init                sbin
config              init.goldfish.rc    sdcard
customkernel        init.rc             sys
d                   init.smdkc210.rc    system
data                init_kernel_only.rc tmp
dbdata              lib                 ueventd.goldfish.rc
default.prop        lpm.rc              ueventd.rc
dev                 mnt                 ueventd.smdkc210.rc
efs                 proc                vendor
root@android:/ #
```

**Abbildung Anhang 8:** Zugriff Ordnerstruktur

Nun ist der volle Zugriff gewährt und man kann alles vom System einsehen. Sogar die Installation von App´s mithilfe der ADB ist möglich. Eine äußerst gefährliche

[80] Online: fibel.org (10.09.2016)
[81] Online: vgl. pitu, linuxforen.de, 2005 (10.08.2016)
[82] Online: vgl. droidwiki.de – USB-Debugging via Recovery, 2015 (10.08.2016)

Tatsache, das Auslesen aller WLAN-Schlüssel, mit dem das Smartphone jemals verbunden war, soll noch demonstriert werden.


**Abbildung Anhang 9:** Auslesen WLAN-Schlüssel

Die Einsicht des Systemordners „data“ erfolgte durch den Befehl cd /data und danach die Auflistung mit „ls“ bzw. „ls –a“ für versteckte Dateien. Durch den Befehl „*adb pull /data/misc/wifi/wpa_supplicant.conf c:/Users/Tobias/Desktop/Ordner/wpa_supplicant.conf*“ wird die Konfigurationsdatei der WLAN-Netzwerke kopiert und mithilfe des Windows-Editors kann man diese dann lesen. Aus Sicherheitsgründen wurde der WLAN-Schlüssel unkenntlich gemacht.[83]

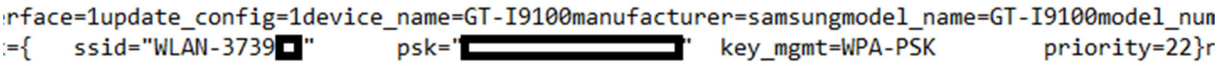


**Abbildung Anhang 10:** WLAN-Schlüssel

[83] Online: vgl. android-stackexchange.com, 2015 (10.08.2016)

# IT-Sicherheitscheckliste für Gebäudeautomationssysteme

## Installation

**Besitzen Sie bereits ein Smart Home System?**

☐ Ja
Hersteller:_____

☐ Nein

**Wie ist ihre Wohnsituation?**

☐ Wohnung

☐ Einfamilienhaus

☐ Mehrfamilienhaus

**Welche Smart Home Variante bevorzugen Sie?**

☐ Funk-Smart Home

☐ Kabelgesteuertes Smart Home

☐ Kombination aus beiden Varianten

**Wer führt die Installation / Montage durch?**

☐ Selbst

☐ autorisierte Firma

**Welche Bereiche im Inneren des Gebäudes möchten Sie vernetzen?**

☐ Türen

☐ Fenster

☐ Licht

☐ Heizung

☐ Küchengeräte (z.B. Kaffeemaschine, Ofen, Kühlschrank)

☐ Entertainmentgeräte (z.B. TV-Gerät, Spielkonsole, Musikanlage)

☐ Sicherheitsanlage (z.B. Einbruchmeldeanlage, Brandmeldeanlage)

☐ Anderer Vernetzungen:_____

**Möchten Sie den Außenbereich des Gebäudes vernetzen?**

☐ Ja

☐ Nein

## Router

**Besitzen Sie einen WLAN-fähigen Router?**

☐ Ja
Hersteller und Modellbezeichnung:_____

☐ Nein

**Ist der WLAN-Schlüssel ausreichend geschützt? (siehe Punkt 5.2 sowie 5.4.1!)**

☐ Ja

☐ Nein

**Haben Sie das Konfigurationsmenü des Routers ausreichend geschützt? (Siehe Punkt 5.4.2!)**

☐ Ja

☐ Nein

**Besitzt Ihr Router die neuste Firmware? Spielen Sie regelmäßige Updates auf?**

☐ Ja
Firmwareversion:_____

☐ Nein
Firmwareversion:_____

☐ Unbekannt

## Client-Sicherheit

**Was für Mobile Clients besitzen Sie?**

☐ Smartphone

☐ Laptop

☐ Tablet

**Welche Betriebssysteme besitzen Ihre mobilen Clients? (siehe Punkt 4.6.2.1)**

☐ Android
Version:_____

☐ iOS
Version:_____

☐ Windows
Version:_____

**Besitzen Sie einen Desktop-Client (z.B. Stand-PC)?**

☐ Ja

☐ Nein

**Welche Betriebssysteme besitzen Ihre Desktop Clients?**

☐ Windows
Version:_____

☐ Linux
Version:_____

☐ MAC
Version:_____

**Über welche Sicherheitsmaßnahmen verfügen ihre Clients bzw. ihre IT?**

☐ Antivirenprogramm

☐ Passwort-Schutz

☐ Fingerabdruck-Scanner

☐ Firewall

☐ VPN

**Nutzen Sie regelmäßige Updates für Betriebssysteme, Software und Treiber?**

☐ Ja

☐ Nein

Für eine Gewährleistung einer funktionierenden IT-Sicherheit schicken Sie die Checkliste bitte an die E-Mail: sicherheitscheck@smart_home.de. Ihre Liste wird umgehend geprüft und Sie erhalten umgehend eine Rückmeldung von einem unserer qualifizierten Mitarbeiter.

# Ehrenwörtliche Erklärung

"Ich erkläre hiermit ehrenwörtlich",

1. dass ich meine ……**Bachelorthesis**…..……mit dem Thema

**Gebäudeautomation mit Smart Home und deren Herausforderungen an die IT-Sicherheit**……
……

ohne fremde Hilfe angefertigt habe,

2. dass ich die Übernahme wörtlicher Zitate aus der Literatur sowie die Verwendung der Gedanken anderer Autoren an den entsprechenden Stellen innerhalb der Arbeit gekennzeichnet habe und

3. dass ich meine ……**Bachelorthesis** ……bei keiner anderen Prüfung vorgelegt habe.

Ich bin mir bewusst, dass eine falsche Erklärung rechtliche Folgen haben wird.

Reichenbach, 22.08.2016

_____ _____

Ort, Datum Unterschrift

BERUFSAKADEMIE SACHSEN
STAATLICHE STUDIENAKADEMIE
GLAUCHAU
UNIVERSITY OF COOPERATIVE EDUCATION

# Erklärung zur Prüfung wissenschaftlicher Arbeiten

Die Bewertung wissenschaftlicher Arbeiten erfordert die Prüfung auf Plagiate. Die hierzu von der Staatlichen Studienakademie Glauchau eingesetzte Prüfungskommission nutzt sowohl eigene Software als auch diesbezügliche Leistungen von Drittanbietern. Dies erfolgt gemäß § 7 des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz – SächsDSG) vom 25. August 2003 (Rechtsbereinigt mit Stand vom 31. Juli 2011) im Sinne einer Datenverarbeitung im Auftrag.

Der Studierende bevollmächtigt die Mitglieder der Prüfungskommission hiermit zur Inanspruchnahme o.g. Dienste. In begründeten Ausnahmefällen kann der Datenschutzbeauftragte der Staatlichen Studienakademie Glauchau sowohl vom Verfasser der wissenschaftlichen Arbeit als auch von der Prüfungskommission in den Entscheidungsprozess ein-bezogen werden.

| | |
|---|---|
| Name: | Pietzsch |
| Vorname: | Tobias |
| Matrikelnummer: | 4001456 |
| Studiengang | WI13 |
| Titel der Arbeit: | Gebäudeautomation mit Smart Home und deren Herausforderungen an die IT-Sicherheit |
| Datum: | 22.08.2016 |
| Unterschrift: | |