Computerwelt: Aktuelle IT-News Osterreich

15.06.2016 *pi/Rudolf Felser*

"Raub-as-a-Service": Was man bei der Sicherheit für das Smart Home bedenken sollte

"Durch die Anfälligkeit von Smart-Home-Systemen entwickelt sich ein Geschäftsmodell für Online- wie Offline-Kriminelle, das sehr beängstigend ist", sagt Security-Experte Franjo Majstor im Interview über Bedrohungen für und die Sicherheit von Smart Homes.

Smart Home - Attraktiv für Kriminelle
© CC0 Public Domain - pixabay.com

Franjo Majstor ist Certified Information Systems Security Professional (CISSP) und CTS (Chief Technology Strategist) bei dem kroatischen Startup Smart-Group. Außerdem hält der Security-Experte, der sich unter anderem mit den Bereichen Home Automation und IoT auseinandersetzt, einen Vortrag auf der SecureConference von (ISC)² am 30. Juni in Wien über das Thema "CIA (Confidentiality, Integrity and Availability) in ihrem Smart Home?". Im Interview spricht er über die aktuellen und zukünftigen Bedrohungen für das Smart Home.

Den Trend zur Heimautomatisierung gibt es schon seit ein paar Jahren. Aufgrund von neuen Technologien wie Smartphones und Cloud Serices wird dieser Markt nun zunehmend interessanter für Verbraucher und auch für nicht unbedingt technisch affine Personen. Was denken Sie als IT-Sicherheitsexperte, welche Bedrohungen für

Smart-Home-Systeme derzeit die größten sind?

In der Vergangenheit waren diese Heimautomatisierungssysteme mehr oder weniger isolierte Netzwerke innerhalb eines Hauses oder Apartments. Mit der Einführung von Smartphones und Cloud Services ändert sich der Markt ständig und wächst rasant. Sensoren sind in fast allem integriert, sind für nahezu alles verfügbar und Kosten wenig, so dass wir allgemein von dem Beginn der Ära des Internet of Things sprechen. Die Smart-Home-Industrie profitiert sehr davon. Der Trend, per Fernsteuerung Heizsysteme, Kühlsysteme, Licht, Fensterläden und anderes zu kontrollieren, hat sich weiterentwickelt, nun geht es darum, immer online und überall erreichbar zu sein. Das bedeutet jedoch auf der anderen Seite auch, dass Smart-Home-Systeme das neue, große Ziel für Cyberkriminelle und auch klassische Kriminelle darstellen. Wenn man darüber nachdenkt, dass das Heizsystem aufgrund einer Geo-Location-Funktion (GPS-Positions-Sendeempfänger) des eigenen Smartphones genau weiß, wo man sich gerade befindet, ist das aus Security-Sicht ein grauenvoller Gedanke. Natürlich geschieht dies in der Absicht, Energiekosten während der Abwesenheit zu sparen oder aber die Wohnung zu heizen, was im Übrigen einen großen Komfort bedeutet. Wenn allerdings dieses System gehackt oder missbraucht wird, d.h., wenn jemand unaufgefordert die Information über eine große Distanz hinweg darüber erhält, ob man selbst oder jemand anders von der Familie zu Hause oder eben nicht daheim ist, dann kann derjenige zum Beispiel gezielt einen Einbrecher in das Haus leiten. Also werden wir heute nicht nur über SaaS, IaaS, Paas, etc. reden, sondern über das "RaaS" also "Raub als Service". Durch die Anfälligkeit von Smart-Home-Systemen entwickelt sich ein Geschäftsmodell für Online- wie Offline-Kriminelle, das sehr beängstigend ist.

Was hat die Smart-Home-Industrie bisher getan, um ihre Technologien zu schützen?

Wir reden hier über IT-Lösungen und IT-Sicherheit, hier müssen wir zunächst konstatieren, dass es nirgends ein vollständig und auf Dauer sicheres Sicherheitssystem gibt. Aber mit einer guten Verschlüsselung und starken Sicherheitskontrollen können wir es "härten" oder zumindest unattraktiv genug für böse Jungs machen. Zu allererst lässt sich feststellen, dass die meisten der neu

eingeführten Smart-Home-Produkte Kommunikationsprotokolle wie ZigBee oder Z-Wave nutzen. Diese Technologien sind standardisiert und wurden unter der Annahme von Cyber-Attacken entwickelt. Um für die Sicherheit dieser Produkte zu sorgen, muss man sich als Informationssicherheits-Experte zunächst die sogenannte "CIA" anschauen. Wenn wir uns die Bauweise der Smart-Home-Systeme anschauen, dann fällt auf, dass sich ein Vergleich zwischen dieser Bauweise und der den Sicherheitsfachmännern sehr bekannten "CIA-Sichtweise" herstellen lässt.

Könnten Sie etwas mehr ins Detail gehen, warum ZigBee und Z-Wave sicherer oder unsicherer als andere Protokolle sind?

Aus der Sicht der Konnektivität sind es zwei gesonderte Netzwerke. Das ZigBee-Protokoll, obwohl es die gleiche 2.4 GHz Frequenz wie Wi-Fi nutzt, nutzt ansonsten eine unterschiedliche Modulation und verschiedene Kanäle, um nicht mit einem Heim-Wifi-Netzwerk zu kollidieren. Z-Wave benutzt, abhängig von der eingesetzten Region, eine Reichweite von 800-900 Mhz., was ein komplett anderes Frequenzspektrum darstellt, als es in Heimnetzwerken bislang üblich ist. Beide verwenden ein Gateway für die Kommunikation zwischen dem Heimnetzwerk, dem Internet und dem Radiosensor-Netzwerk. Sowohl ZigBee als auch Z-Wave kommunizieren verschlüsselt auf dem AES-Standard. Das ist ein guter Anfang, allerdings muss die Verschlüsselung auch angeschaltet, richtig initialisiert und über eine solide Schlüsselsteuerung verfügen.

Können Sie erklären, was Sie mit "CIA" meinen und wie man es zur Absicherung von Smart-Home-Lösungen einsetzt?

Mit dem "CIA"-Akronym denken Leser natürlich zuerst an eine gewisse Behörde. Aber wir beziehen uns auf die Sicherheitsaspekte der Vertraulichkeit (Confidentiality), Verfügbarkeit (Availability) und Integrität (Integrity). Man muss sich vor Augen führen, dass jedes einzelne Hardware-Element oder jede Hardwareverbindung verletzlich ist und eine potenzielle Schwachstelle enthalten kann. Verfügbarkeit (Availability) ist unsere erste Sorge, wenn man darüber nachdenkt, dass Teile unseres Smart-Home-Services in der Cloud gehostet sein könnten. Allgemein gesprochen ist das heute jedoch ein weniger wichtiges Anliegen in städtischen Bereichen, da dort die Konnektivität des Internets gut ist. Wichtiger sind zusätzliche Besonderheiten oder Updates und deren Ausführung. Das ist auch der Grund, warum das lokale Smart-Home-Gateway die Möglichkeit haben sollte, unabhängig zu agieren, auch wenn es die meiste Zeit eng mit dem Cloud-Dienst gekoppelt oder verbunden ist. Besonderheiten wie das letzte Set an Regeln oder die letzte Aktualisierung der Konfiguration durch den Cloud Service zu

verwalten, offenbaren die Möglichkeit, nicht nur unabhängig zu handeln, sondern auch Alarme etc. zu senden, ohne einen zentralisierten Dienst nutzen zu müssen. Allerdings sollte sich das nur auf Veränderungen in der Konfiguration, in den Regeln oder Szenarien beziehen und auch nur so lange, bis die Verbindung zu einem zentralisierten Softwaredienst wiederhergestellt ist.

Die Vertraulichkeit (Confidentiality) haben wir bereits kurz in Bezug auf das Thema der Verschlüsselung angesprochen. Selbst wenn es auf den ersten Blick nicht miteinander zusammenhängt, ist es aus vertraulicher Sicht auch wichtig, an die Verwundbarkeit der Software zu denken, die wir normalerweise minimieren, indem wir die benutzte Software flicken und neu laden. Meistens werden die Schwachstellen in den Anwendungen zuerst ausgenutzt, um Zugang zum privilegierten Modus zu erhalten und dann alle anderen Sicherheitsanwendungen wie Verschlüsselungen zu umgehen. Als Beispiel hierfür bietet sich eine verwundbare, abgelaufene Software der Webcam an, die nicht nur einen laufenden Videodienst mit der Möglichkeit eines Mikrofons enthält. Manche ausgeklügelten Webcam-Modelle können nicht nur einfach angeschaltet werden, sondern erlauben auch den Zugriff auf den Bildschirm des PCs oder Laptops. Hier kann dann herangezoomt werden, können Screenshots erstellt und alle Daten, die sonst vom Computer durch VPN, persönliche Firewalls, etc. geschützt werden, lassen sich abfangen. Die Möglichkeiten sind groß. Wenn wir wieder zurück an die Verschlüsselung und deren Nutzung in Heimautomatisierungs-Protokollen denken, ist die Erwähnung wichtig, dass sich sowohl ZigBee als auch Z-Wave-Protokolle an die Standardverschlüsselung halten. Trotzdem ist die Verschlüsselung nicht nur ein Algorithmus, der dazu gedacht ist, die Kommunikation zu verschlüsseln. Es geht vielmehr auch um das Generieren der Kodierungsschlüssel, um deren Management und Verbreitung. Das ZigBee-Protokoll ist eine Teilmenge des 802.15.4 Standards und hat ein gut zentralisiertes Schlüsselverteilungsschema, indem verschiedene Schlüssel für die Link- oder netzwerkbasierte Kommunikation genutzt werden. Der anfängliche Schlüssel, der an ein neues Gerät verteilt wird, ist mit einem sogenannten "Secret Master Key" verschlüsselt und von da an hängt jede Kommunikation von diesem ab. Der Secret-Master-Key sollte nur den Herstellern bekannt sein, die ZigBee-Produkte produzieren, und ist unbedingt geheim zu halten, was natürlich nicht Sicherheit für alle Ewigkeit garantiert, aber zumindest ein guter Anfang ist. Das Z-Wave-Protokoll verfügt über die starke Verschlüsselung und das Schlüsselmanagement, jedoch ist es wegen der Verzögerung und des Energieverbrauchs in batteriebetriebenen Sensoren angeraten, die Verschlüsselung nur optional und auch nur für die sicherheitsspezifischen Dienste wie Alarmanlagen oder Türverriegelungen zu nutzen.

Die Integrität (Integrity) wird meistens übersehen oder als am wenigsten wichtigster der drei Aspekte angesehen. Trotz allem

können fehlerhafte Daten zu drastisch schlechten Konsequenzen führen oder in vereinzelten Fällen das menschliche Leben beeinflussen, sie sollten also nicht außer Acht gelassen werden. Nun schauen wir uns noch einmal ZigBee und Z-Wave an. Während das Z-Wave-Protokoll nur CRC (Cyclic Redundancy Check) nutzt, also eine nicht kryptografische Kontrollsumme, hat ZigBee die MIC (Message Integrity Code) und MAC (Message Authentication Code) als Standard-Optionen festgelegt. Beides sorgt für die kryptografische Integritäts-Kontrollsumme der übermittelten Daten. Stress ist bei der Nutzung also unglücklicherweise garantiert, da die ZigBee-Standardentwickler die Entscheidung für den Schlüsselaustausch, welcher für MAC für eine Anforderung benutzt wird, der höheren Ebene überlassen haben.

Wie sieht die Zukunft der Smart-Home-Sicherheit aus?

Es besteht kein Zweifel daran, dass es noch einige Herausforderungen für unbedenkliche und sichere automatische Heimsysteme gibt; jedoch existieren sie schon in wesentlich besserer Form als die urheberrechtlich geschützten und meist völlig überteuerten Systeme von vor zehn Jahren. Lösungen, die den Einfluss und die Beteiligung von normalen Nutzern in sicherheitstechnischen Entscheidungen reduzieren und gleichzeitig attraktiv genug in Bezug auf Benutzerfreundlichkeit und Komfort sind, schaffen es in die Haushalte. Gleichzeitig minimieren sie den Energieverbrauch und die reduzieren die Energiekosten. Damit sorgen sie im Großen und Ganzen dafür, dass unser Zuhause nicht nur smarter, sondern in Zukunft auch sicherer wird.

ZUR PERSON

Franjo Majstor, CISSP ist Chief Technology Strategist bei der Smart-Group Ltd, einem Startup aus dem Bereich Home Automation/IoT. Er ist Autor zahlreicher IT-Sicherheitsbeiträge in der "Information Security Handbuch"-Serie von Hal Tipton & Mickey Krause, war lange Zeit als Security Consultant bei verschiedenen Herstellern tätig und spricht über verschiedene IT-Sicherheitsthematiken auf internationalen Sicherheitskonferenzen. Darüber hinaus ist er auch Mitglied des (ISC)² Austria Chapters in Wien. (pi/rnf)