Aber sicher bitte

So wird das Smart Home kein Einfallstor für Hacker

Kai-Oliver Detken

Das vernetzte Heim wird immer mehr Realität. Konnte man sich vor zehn Jahren noch kaum vorstellen, wozu man einen Ethernet-Anschluss im Wohnzimmer oder in der Küche benötigt, so ist dies heute bei Neubauten fast schon notwendiger Standard. Immer mehr Geräte besitzen oder benötigen einen Internetanschluss. Bequem kann dann per Smartphone-App von der Arbeit die Wäsche angestellt, die Jalousien heruntergefahren oder der Rasenmäher angesteuert werden. Nur vergessen die Hersteller bei allem Komfort häufig die IT-Sicherheit (Security by Design), weshalb theoretisch auch Außenstehende auf das Smart Home zugreifen können. Ist dies beim Ausschalten des Lichts im Wohnzimmer vielleicht noch zu vernachlässigen, wird die Berücksichtigung der IT-Sicherheit z.B. bei Alarmanlagen zwingend notwendig.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Die neue Bequemlichkeit, die man mithilfe von Smart-Home-Equipment genießt, kann auch zu neuen Sicherheitslücken führen. Denn alles, was in einem Smart Home aus der Ferne gesteuert werden kann, könnte auch ein Hacker durch potenzielle Sicherheitslücken ausnutzen. Dies kann sich vom Fernsehgerät über die Beleuchtung bis hin zur Heizung hinziehen, die alle Teil des sog. Internet of Things (IoT, Internet der Dinge) sind. Die gehackten Endgeräte könnten durch Hacking über sog. Botnetze in Zusammenschluss mit anderen Systemen auch zu einem IT-Risiko für die öffentliche Sicherheit werden, da Angriffe gegen Dritte darüber ausgeführt werden können.

Smart-Home-Infrastruktur

Der Begriff Smart Home beinhaltet technische Verfahren und Systeme in Wohnräumen und -häusern, in deren Mittelpunkt automatisierbare Abläufe und fernsteuerbare Endgeräte stehen. Darunter fällt die Vernetzung von Haustechnik und Haushaltsgeräten genauso wie die von Komponenten der Unterhaltungselektronik. Insbesondere die Kombination von Leuchten, Tastern und Geräten miteinander und die Möglichkeit der Datenspeicherung sowie die Abbildung einer gewissen Logik wird zusammenfassend als Smart Home angesehen.
Der Begriff Smart Home wurde bereits vor 20 Jahren etabliert, als im Rahmen eines Architekturwettbewerbs im Jahr 2005 auf dem Gelände der Bundesgartenschau in München das „Haus der Gegenwart" errichtet wurde. Dieses Projekt war als Weiterentwicklung eines herkömmlichen Einfamilienhauses angelegt, in dem sich alle elektronischen Vorgänge zentral steuern lassen. Zudem forscht das Fraunhofer-inHaus-Zentrum in Duisburg seit dem Jahr 2001 an neuartigen Systemlösungen durch Integration von Produktkomponenten aller Art im Wohnumfeld. Dies wird zusammen mit Herstellern, Dienstleistern und Nutzern bis heute betrieben. Ebenfalls im Jahr 2005 zeigte die Deutsche Telekom in Berlin, wie ein voll vernetztes Musterhaus aussehen könnte. Die Zielsetzung: Angeschlossene Haushaltsgeräte können über PDA-Endgeräte (Personal Digital Assistent) oder Multifunktionsbildschirme von unterwegs gesteuert und abgefragt werden. Seit 2013 existiert in Darmstadt ein neues Musterhaus der Deutschen Telekom, in dem Geräte unterschiedlicher Hersteller kombiniert wurden. Hier lassen sich Heizung, Lampen und Waschmaschine mit verschiedenen Funkstandards (u.a. Zigbee, DECT, WLAN, Bluetooth) per Smartphone, Tablet oder PC steuern und kontrollieren. Das Musterhaus wurde von der Initiative Qivicon ins Leben gerufen, um die Herstellerkompatibilität zu fördern.
Bild 1 zeigt, dass die gesamte Kommunikation der Home-Base von Qivicon verschlüsselt über das Internet stattfindet – unabhängig vom Anbieter. Alle Nutzerdaten werden dabei ausschließlich auf Servern der Deutschen Telekom in Deutschland gespeichert, wodurch auch die DSGVO-Konformität sichergestellt ist. Seit 2012 fördert das BMWI zusätzlich das Zertifizierungsprogramm „Smart Home und Building", damit gemeinsame Standards und Prüfkriterien für systemübergreifende Interoperabilität entwickelt werden können.

Mögliche Sicherheitsrisiken

Durch die Vernetzung möglichst vieler Komponenten können natürlich auch unerwünschte Dritte versuchen, sich mit dem Smart-Home-System zu verbinden. Da alle Informationen an einer Schnittstelle zusammenlaufen und zentral gesteuert werden können,

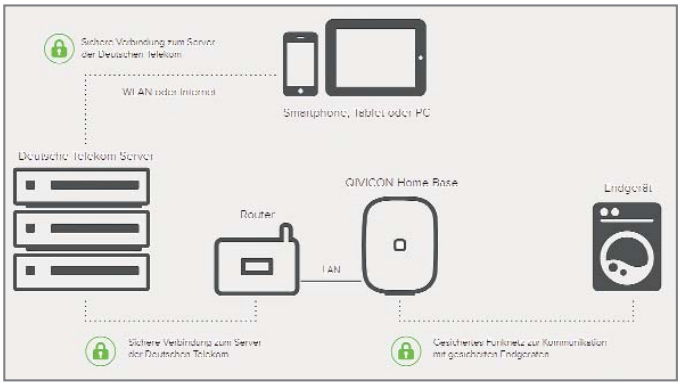

Bild 1: Einsatzszenario des Qivicon-Smart-Homes
(Quelle: www.qivicon.com)

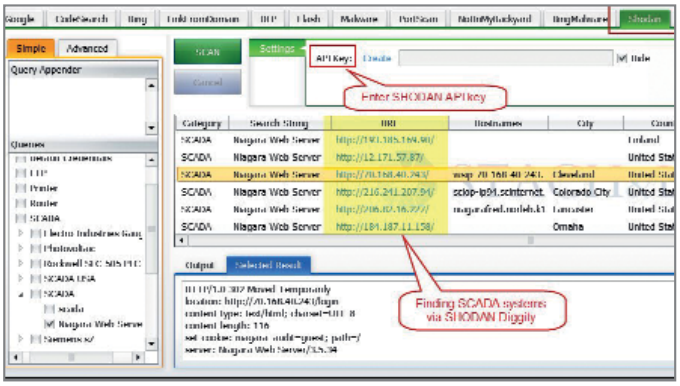

Bild 2: Oberfläche Diggity für Shodan
(Quelle: https://tinyurl.com/yybjat82)

steigt damit auch das Risiko eines externen Angriffs. Als Folge könnten die Bewohner eines Hauses überwacht oder z.B. die Haustür geöffnet werden. Die Überwachung kann allerdings auch durch den Anbieter von Smart-Home-Equipment vorgenommen werden, um das Verhalten von Kunden auszuspionieren oder gezielt Werbung zu setzen. Damit verstoßen sie auf jeden Fall gegen den Datenschutz. Nutzerdaten können z.B. aber auch Einbrechern helfen zu erkennen, wann das Haus nicht bewohnt ist.

Ein weiteres Sicherheitsrisiko sind IP-Kameras, die im gehackten Zustand einiges über das Privatleben der Bewohner verraten. Sprachassistenten wie Alexa (Amazon Echo) oder Siri (Apple) werten zudem alle gesprochenen Worte der Benutzer aus, um sich ständig bei neuen Anfragen zu verbessern. Dies beinhaltet, dass die Befehle für spätere Analysen aufgezeichnet werden müssen. Wie Untersuchungen ergaben, wurde aber nicht nur die Kommunikation mit dem Sprachassistenten mitgeschnitten. Dadurch lassen sich im einfachsten Fall Profile erstellen und das Kaufverhalten beeinflussen (Stichwort: gläserner Kunde). Die Nichtabschaltbarkeit solcher Assistenten und die Ungewissheit, was mit den Daten gemacht wird, hat zumindest in Deutschland zu einem eingeschränktem Kaufverhalten geführt.

Suchmaschinen wie Shodan (**www.shodan.io**) haben sich darauf spezialisiert, bestimmte Arten von Computern und Diensten, die mit dem Internet verbunden sind, über eine Reihe von Filtern zu finden. Daher wird Shodan primär eingesetzt, um Systeme mit niedrigen Sicherheitsvorkehrungen zu finden. Dies beinhaltet auch Steuerungssysteme wie z.B. Scada für kritische Infrastrukturen wie Wasseranlagen, Stromnetz und Kraftwerke. Viele IoT-Endgeräte verwenden dabei eine einfache Authentifizierung mittels Benutzernamen und Passwort, die über einen Webbrowser eingegeben werden kann. Daher wird das Internet nach öffentlich zugänglichen Geräten untersucht, die mindestens einen offenen Port besitzen.

Shodan wurde für diese Funktion häufig kritisiert, da sich durch sie Hacker eine Opfermaschine suchen können. Aber letztendlich hilft sie dabei, bekannte Sicherheitslücken zu finden und rechtzeitig zu schließen. Aus diesem Grund verwenden Internetsicherheitsspezialisten, Forscher und Strafverfolgungsbehörden diese Plattform. *Bild 2* zeigt die Möglichkeit einer Bulk-Suche und Verarbeitung mittels Shodan Diggity. Dieses Tool bietet eine Scan-Schnittstelle über die Shodan-API und liefert eine komfortable Liste von 167 Suchanfragen bereits mit.

Erschreckend ist auf jeden Fall, dass sehr viele Smart-Home-Endgeräte offen zugänglich sind. Dies reicht vom Babyphone mit Videounterstützung bis hin zu Alarm- oder Produktionssystemen. Vor diesen Lücken sind auch die großen Hersteller nicht gefeit, so dass man sich hier nicht pauschal in Sicherheit wiegen kann. Außerdem zeigt Shodan, dass bekannte Sicherheitslücken häufig nicht geschlossen werden. So tauchte z.B. die OpenSSL-Lücke Heartbleed im Jahr 2014 auf, die zwei Drittel der Serversysteme weltweit betraf. Heartbleed war ein schwerer Fehler in der OpenSSL-Implementierung, mit dessen Hilfe Angreifer Teile des Speichers des betroffenen Servers lesen konnten, wodurch Benutzerdaten angezeigt wurden. Dadurch konnten öffentliche Server wie VoIP-Systeme, Router, Netzdrucker usw. von Hackern übernommen werden. Shodan zeigte drei Jahre später, dass immer noch zahlreiche Server die Lücke mit der Bezeichnung CVE-2014-0160 nicht geschlossen hatten. Dabei hätte man durch Patchen, Schaffen eines neuen privaten Schlüssels und die Neuausstellung der Sicherheitszertifikate relativ einfach Abhilfe schaffen können. Man sollte daher Suchmaschinen wie Shodan nicht verteufeln, sondern eher die Chance sehen, mit ihrer Hilfe seine Systeme einem Sicherheitscheck unterziehen zu können.

BSI-Empfehlungen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich des Smart-Home-Themas seit einiger Zeit angenommen. Die Risiken und Gefahren wurden gesammelt, analysiert und entsprechende Sicherheitsempfehlungen ausgegeben:

- Das Smart Home sollte mit einer Firewall abgesichert werden. Den Fernzugriff von außen auf die eigenen Geräte sollte man immer verschlüsselt durchführen.
- Das Passwort sollte keine zu einfachen Kombinationen enthalten, sondern aus einer willkürlichen Kombination aus Zahlen, Sonderzeichen sowie Groß- und Kleinbuchstaben bestehen.
- Die Smart-Home-Geräte sollten möglichst lange vom Hersteller mit-

tels Sicherheitsupdates unterstützt werden. Dadurch lassen sich zwar nicht grundsätzlich Sicherheitslücken ausschließen, aber das Risiko wird deutlich minimiert. Natürlich muss man diese Patches auch gelegentlich einspielen.
- Die Datenschutzerklärung sollte aufmerksam gelesen werden, um zu erkennen, was der Hersteller offiziell an den eigenen Daten auswertet. Die DSGVO schließt allerdings nicht den Datenmissbrauch aus, der evtl. inoffiziell begannen wird.

Beim Kauf sollte auf die Verbreitung des Herstellers und seiner Lösung geachtet werden. Dies erhöht die Chance auf regelmäßige Updates und ein langlebiges Produkt.

Absicherung eines Smart Home

Unabhängig von den BSI-Empfehlungen gibt es weitere Dinge, die man bei der Umsetzung einer Smart-Home-Infrastruktur beachten sollte. So sollte z.B. vor dem Kauf einer Herstellerlösung geklärt werden, ob diese überhaupt verschlüsselte Kommunikation zulässt. Auch sollte man überprüfen, ob normalerweise Sicherheitsupdates langfristig von dem Hersteller bereitgestellt, welche Daten an den Hersteller übermittelt und wie sie dort verarbeitet bzw. genutzt werden.

Hat man sich für eine Smart-Home-Lösung entschieden, sollten als erstes die voreingestellten Standardpasswörter durch eigene erneuert werden. Eigentlich ein trivialer Hinweis, jedoch ist es erschreckend, wenn man eingerichtetes Netz-Equipment untersucht, wie oft man die Herstellerpasswörter wiederfindet. Teilweise werden sogar Herstellertutorials von IT-Administratoren haargenau abgearbeitet – inklusive der dort enthaltenen Passwörter. Es kommt daher nicht nur darauf an, ein starkes Passwort zu definieren, sondern überhaupt das Standardpasswort abzuschaffen.

Des Weiteren sollten alle drahtlosen Geräte immer mit einer sicheren Verschlüsselung ausgestattet sein. Bei WLAN-Geräten sollte daher immer auf WPA2 mit dem Advanced Encryption Standard (AES) gesetzt werden. Dieser Standard gilt bislang als nicht angreifbar, solange keine einfachen Passwörter benutzt wurden. Allerdings kann die Sicherheit trotz WPA2-Einsatz auch durch Lücken im Betriebssys-tem ausgehebelt werden. Daher sollte man dies immer auf dem neuesten Stand halten, was leider selten der Fall ist – speziell bei Home-Smart-Lösungen. Während in Unternehmensnetzen ein zentraler WLAN-Controller für das Ausrollen neuer Softwarepatches sorgt, fehlt dies in Heimnetzen völlig. Jedes Endgerät muss separat gepflegt werden, was relativ zeitaufwendig ist und entsprechendes Wissen voraussetzt, oder der Hersteller muss per Cloud-Anbindung dafür sorgen.

Bei der Smart-Home-Einrichtung sollten die IoT-Geräte ebenfalls in ein separates VLAN (virtuelles LAN) ausgelagert werden, damit bei erfolgreicher Kompromittierung nicht das gesamte Netz betroffen ist. Durch diese Netzsegmentierung haben intelligente Hausgeräte keine Verbindung zu sensiblen Daten oder Geräten. Allerdings setzt dies voraus, dass die verwendeten Switche und der Router VLAN-Funktionalität besitzen, was gerade bei im Haushalt verwendeten Switchen nur selten der Fall ist.

Auch sollten Gäste keinen direkten Zugang in das hauseigene WLAN erhalten. Sinnvoller ist, diese in einem separaten VLAN zu lassen, in dem nur der Zugriff auf das Internet gestattet wird. Dadurch können die wichtigen Zugangsdaten nicht von Fremden genutzt werden, wenn z.B. ein Gastendgerät gehackt werden sollte. Dann müssen aber die WLAN-Access-Points neben der VLAN-Funktionalität in der Lage sein, verschiedene SSIDs anzubieten – auch keine Selbstverständlichkeit bei Consumer-Geräten.

Um nicht beliebigen Endgeräten eine Verbindung zum Internet zu ermöglichen, sollten voreingestellte UPnP-Funktionen oder DHCP für beliebige Geräte deaktiviert werden. Denn standardmäßig sind Internetrouter von den Providern oder Herstellern so konfiguriert, weil man davon ausgeht, dass der Normalanwender kein ausreichendes Wissen vorhalten kann. Die UPnP-Funktionalität ist in der Lage, Netzgeräte ohne Benutzerinteraktion zu finden, automatisch anzumelden und, wenn der Router dies unterstützt, mit dem Internet zu verbinden. DHCP vergibt in der Standardkonfiguration automatisiert IP-Adressen für beliebig anfragende Geräte. Was auf der einen Seite die Vernetzung erleichtert, kann auf der anderen Seite zu massiven Sicherheitsproblemen führen. Daher sollte DHCP so eingerichtet werden, dass nur anhand der MAC-Adresse bekannte Endgeräte sich anmelden dürfen.

Der Zugang aus der Ferne, der im Smart-Home-Umfeld einen hohen Mehrwert besitzt, muss ebenfalls ausreichend abgesichert werden. Dafür sind VPN-Zugänge unabdingbar, die sicher verschlüsselte Verbindungen ermöglichen. Allerdings muss der Internetrouter entsprechende VPN-Varianten (z.B. OpenSSL, OpenVPN, IPsec) anbieten. Um nicht von der Routerkonfiguration abhängig zu sein, bieten jedoch viele Smart-Home-Hersteller den direkten Zugang auf ihre Geräte über die eigene Cloud an. Das heißt, das intelligente Endgerät nimmt direkt Verbindung zur Hersteller-Cloud auf, die dann einen Zugang für den Anwender ohne VPN-Funktionalität anbietet (s. Bild 1). Damit ist der Endbenutzer allerdings komplett von der Absicherungsqualität des Herstellers abhängig. Nutzt er verschie-dene Hersteller, muss er zudem diversen Hersteller-Clouds den Zugang zu seinem Netz erlauben.

Fazit

Smart-Home-Lösungen bieten einen großen Mehrwert für den Hausbesitzer und werden sich daher zukünftig weiter am Markt etablieren. Bei der Auswahl der Lösungen darf man sich nicht nur von der Funktionalität beeindrucken lassen, sondern muss auch die Sicherheit im Auge behalten. Denn die gewonnene Energieeinsparung oder Lebensqualität kann bei Nichteinhaltung der Absicherungsstandards rasch ins Negative umschlagen. In jedem Fall sollte sich der Nutzer unbedingt mit der Technik beschäftigen, sich nicht auf die Aussagen der Hersteller verlassen und gegebenenfalls professionelle Hilfe ins Haus holen. *(bk)*