

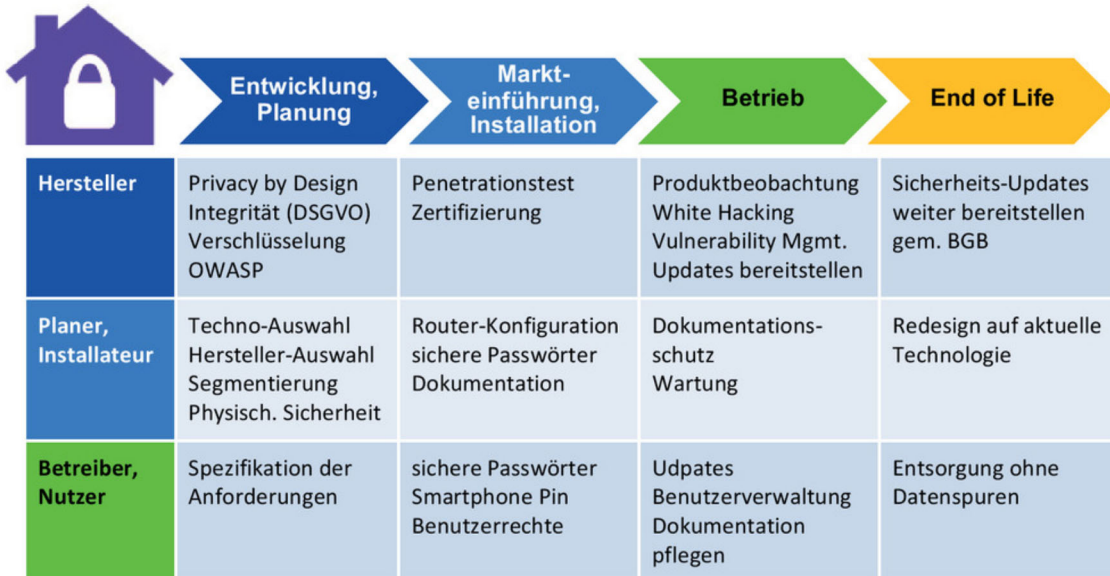
IM FOKUS

Qualität und Sicherheit im Smart Home

Smart Home Security ist Teamwork

Vielleicht haben Sie vor einigen Monaten im Fernsehen den Kriminalfilm „Das Haus“ gesehen? Ein Smart Home, das Ängste schürt. Es bestellt Unmengen an Lebensmitteln für den Kühlschrank, sperrt die Bewohner aus erzieherischen Gründen über Nacht aus, filmt selbstständig den Seitensprung der Ehefrau, um das Video dem Ehemann zu zeigen, und bringt dann auch noch zwei Gäste brutal um, indem es sie in die Sauna lockt und nicht wieder rauslässt. Ein solcher Blödsinn ist für Menschen, die sich mit der smarten Technik auskennen, kaum zu ertragen. Leider prägt es ein suspektes Bild von Smart Home und schürt Technik-Ängste, wenn nicht sogar Verschwörungstheorien. Bestimmt steckt Bill Gates dahinter? Dagegen brauchen wir ein aufgeklärtes Verständnis. Wo stecken tatsächlich die Risiken und wie kann man sie beherrschen? Der Artikel will dazu einen Beitrag leisten.

Dabei kommen wir gleich zu einer unbequemen Wahrheit. Es sind nicht nur etwa die anderen, die bösen Hersteller, die schuld daran sind, wenn es mit der Cybersecurity hapert. Natürlich tragen sie einen wesentlichen Teil der Verantwortung, aber auch ein sehr sicheres Gerät kann zur Virenschleuder werden, wenn es falsch installiert wird oder der Nutzer leichtfertig alle Sicherheitsaspekte ignoriert. IoT-Security ist Teamwork: Hersteller, Installateure und Anwender sind gemeinsam für die Cybersecurity im Smart Home verantwortlich, von der Wiege bis zur Bahre und darüber hinaus, wie die Tabelle zeigt.



Grafik: Günter Martin

Smart Home Security ist Teamwork.

IM FOKUS

Qualität und Sicherheit im Smart Home

Risiken

Bei der Cybercrime Konferenz des Bundeskriminalamts im Mai diesen Jahres wurde über die stark zunehmende Cyberkriminalität berichtet. Computer von Unternehmen, Behörden und auch von Privatpersonen sind von Ransomware bedroht. Hacker verschlüsseln die Daten und legen damit die Computer lahm. Es werden zum Teil zweistellige Millionenbeträge erpresst. Nach der Zahlung werden die Daten tatsächlich wieder entschlüsselt. Es folgt dann häufig noch eine zweite Attacke. Egal, ob das Lösegeld bezahlt wurde oder nicht, es wird gedroht, Daten im Internet zu veröffentlichen.

Grundsätzlich könnten Hacker auch in Smart Home Geräte eindringen und ein ganzes Gebäude lahmlegen. Erst nach Zahlung des Lösegelds gehen Heizung und Licht wieder an und Rollläden hoch. Das scheint aber bisher kaum vorzukommen. Einige Berühmtheit hat der Fall eines Hotels in Österreich erlangt. Hier wurde die Schließanlage der Hotelzimmer von der Ferne gehackt. Der Hacker sperrte so die Hotelgäste aus und erpresste den Hotelbesitzer [*]. In einem anderen Fall haben Informatiker der Universität Erlangen/Nürnberg smarte Leuchten attackiert, die nicht einmal am Internet hingen. Ein einzelner Funkbefehl aus mehr als 100 Metern Entfernung hat ausgereicht, die Leuchten zum Blinken zu bringen. Der Nutzer selbst konnte die Leuchten nicht mehr steuern. Die Schwachstelle lag im Funkstandard „ZigBee“, der schon kurz danach aufgerüstet wurde. Was hier mit wenigen Leuchten gezeigt wurde, kann weitreichende Auswirkungen haben, wenn die Leuchten miteinander „vermesht“ sind. Konkret: Eine einzelne infizierte Leuchte kann alle benachbarten infizieren und diese jeweils die nächsten Nachbarn. Dies passiert alles ohne Internet, ausschließlich über die Funkverbindung.

Dass Smart Home Besitzer bisher praktisch nicht unter Erpressungen leiden, heißt nicht, dass das Smart Home eine sichere Festung gegen Cyber-Angriffe ist. Das Gegenteil ist der Fall! Die smarten Geräte werden zu hunderten erfolgreich angegriffen, ohne dass es der Nutzer überhaupt merkt. Die Geräte werden durch eine Malware namens Mirai infiziert und zentral ferngesteuert, um gemeinsam und massiv Unternehmen oder die öffentliche Infrastruktur anzugreifen. Diese Bedrohung nennt sich IoT-Botnetz. So wurden zum Beispiel Ende 2016 rund 500.000 fast ausschließlich privat genutzte Webcams über das Internet von Mirai gekapert. Die infizierten Webcams haben dann alle gleichzeitig Server großer Unternehmen an der Ostküste der USA aufgerufen. Vor diesem geballten Zugriff konnten die Server nur in die Knie gehen. So waren die Server großer Unternehmen wie Amazon, Spotify, Twitter, Netflix oder PayPal über Stunden nicht erreichbar. Das wird als DoS-Angriff bezeichnet. Die Abkürzung steht für „Denial of Services“, also „Verweigerung des Dienstes“.

Der Nutzer in seinem Smart Home bekommt im Regelfall nichts davon mit, was seine Geräte gerade anrichten. Sie funktionieren normal weiter. Es wird aber durchaus diskutiert, ob er oder der Installateur nicht Verantwortung tragen und zur Rechenschaft gezogen werden kann, wenn sie die Geräte grob fahrlässig ungeschützt ins Internet lassen. Was können Hersteller, Installateure und Nutzer tun, um ein gutes Sicherheitsniveau zu erreichen?

Hersteller

Für Hersteller beginnt die Sicherheit bereits mit dem Produktdesign. Das ist sogar gesetzlich verankert. Im Artikel 25 der Datenschutzgrundverordnung wird verlangt, dass Datenschutz und Datensicherheit proaktiv in der Produktentwicklung berücksichtigt werden. Artikel 32 stellt Anforderungen an die Integrität, unter anderem

durch Verschlüsselung der Datenübertragung. Eine angemessene Verschlüsselung ist eine der wichtigsten Maßnahmen, Hackern das Leben schwer zu machen. Zum Gerät gehört meist eine App. Hier gibt es mit den „OWASP Top 10“ [*] eine regelmäßig aktualisierte Liste der wichtigsten Sicherheitsmaßnahmen. Die Abkürzung steht für „Open Web Application Security Project“, einer neutralen Organisation, die Tools und Dokumente für App-Entwickler bereitstellt. Hat der Hersteller sein Produkt in den Markt eingeführt, haftet er nach dem Produkthaftungsgesetz, und zwar regelmäßig verschuldensunabhängig. Das allein ist Grund genug zur Produktbeobachtung. Wie erweist sich das Produkt im Praxis-Einsatz? Einige Unternehmen zahlen White Hackern, die sie auf Sicherheitslücken aufmerksam machen, ordentliche Prämien. In jedem Fall muss es im Unternehmen ein Vulnerability-Management geben um Schwachstellen zu erkennen, zu bewerten und zu beheben. Für die Behebung einer Sicherheitslücke muss möglicherweise die Software in den Geräten, die beim Kunden bereits im Einsatz ist, geändert werden. Der Hersteller muss Updates bereitstellen. Das steht seit knapp einem Jahr sogar im BGB §327f [4]. Irgendwann wird das Gerät abgekündigt, also nicht weitervertrieben. Die Sicherheits-Updates müssen trotzdem weiterentwickelt werden. Sie sind für den Zeitraum bereitzustellen, den der Verbraucher „vernünftigerweise erwarten kann“, verlangt das BGB [*].

Planer, Installateur

Bei der Planung darf es nicht nur um Funktionalität und Kosten gehen. Auch die Datensicherheit muss geplant werden. Das beginnt mit der **Technologie-Auswahl**. Die Grundregel einer professionellen Planung, Systembrüche zu vermeiden, ist auch der Datensicherheit zuträglich. Jedes Interface, das zwischen zwei Systemwelten vermittelt muss, ist ein potenzielles Risiko.

Bereits bei der **Planung**, spätestens aber bei der Installation, geht es auch um die physische Sicherheit. Smarte Geräte in öffentlich zugänglichen Bereichen sollten gegen Demontage geschützt werden. So ist es zum Beispiel einem Hacker gelungen, über das Thermometer im Aquarium eines Casinos in Las Vegas in die Kundendatenbank des Casinos einzudringen [*]. Was beim Casino das Aquarium-Thermometer war, ist im Smart Home die vernetzte Wetterstation oder Webcam im Außenbereich, deren Diebstahl das Eindringen ins WLAN ermöglichen könnte. Zur physischen Sicherheit gehört auch, dass Unterverteilungsanlagen, Gateway und Router für unbefugte Personen schwer zugänglich sein sollten, d.h. am besten immer verschlossen sind bzw. sich in verschlossenen Räumlichkeiten befinden.

Das Haupteinfalltor für Hacker ist der **Router**. Idealerweise sollte er nach der Technischen Richtlinie für Router-Sicherheit „BSI TR-03148“ zertifiziert sein. Unabhängig von der Zertifizierung sollte bei der Router-Konfiguration beachtet werden: Port-Weiterleitungen nicht aktivieren, wenn sie nicht wirklich unbedingt benötigt werden. Eine Port-Weiterleitung bewirkt, dass Anschlusspunkte im heimischen Netz von außen aus dem Internet erreichbar sind. Das wird im Smart Home höchstens für Webcams, auf die man remote per App zugreifen will, benötigt. Der zweite Punkt ist das Abschalten der Fernadministration, über die der Router remote gesteuert werden kann. Ausnahme: Die Fernadministration wird zwingend benötigt. Der dritte Punkt ist die Segmentierung. Auch die einfachen Router für den privaten Einsatz bieten oft die Option, zwei oder mehr getrennte W-LANs einzurichten. Eines sollte für die smarten Geräte und das andere für die weitere IT (PC/Notebooks, Network Disks) im Haus verwendet werden.

IM FOKUS

Qualität und Sicherheit im Smart Home

Mit der Installation sollen **sichere Passwörter** vergeben werden. Die Realität sieht oft anders aus. Mancher Installateur nutzt bei jeder Installation das gleiche Passwort. Oder es wird ein Passwort vergeben, das sich einfach ableiten lässt. Typische Beispiele sind der Kundenname oder das Installationsdatum. Dieses Vorgehen erleichtert später die Wartung, weil dem Installateur das Passwort geläufig ist. Es stellt aber ein hohes Sicherheitsrisiko dar.

Auch nicht besonders sicher ist die **Erstellung der Dokumentation** über die Installation. Bei Bedarf wird im Haus nachgeforscht und gemessen, wie was installiert ist. Dabei stören Sicherheitsfunktionen, die das Eindringen erschweren. Je offener das System ist, umso einfacher lässt es sich auch ohne Dokumentation erschließen. Auf diesem Weg führt fehlende Dokumentation zu Problemen bei der Datensicherheit. Die Dokumentation soll nicht nur erstellt, sie muss anschließend auch sicher verwahrt werden. Sie enthält sensible Informationen wie Passwörter. In Zukunft geht die Dokumentation in Richtung des digitalen Gebäudewillings im BIM, dem Building Information Management.

Mit der **Wartung** sollen Funktionsfähigkeit und Sicherheit über lange Zeit gewährleistet werden. Während die Hardware kaum altert, altert die Software umso mehr in dem Sinne, dass sie neuen Anforderungen oder Bedrohungen nicht mehr genügt. Sie muss durch die vom Hersteller verfügbaren Updates aktuell gehalten werden.

Irgendwann reicht dann die Leistungsfähigkeit der Hardware nicht mehr aus, oder die Software wird nicht mehr gepflegt. Dann muss die Hardware gewechselt werden. Spätestens, wenn es soweit ist, sollte über ein grundsätzliches **Redesign** nachgedacht werden, um nicht nur einzelne Komponenten, sondern das gesamte System auf den neuesten technischen Stand zu bringen.

Betreiber und Nutzer

In den seltensten Fällen kommen Hacker vor Ort ins Haus und haben physischen Zugriff auf die Geräte. Sie kommen über das Internet. Ein Smart Home braucht kein Internet. Licht, Heizung, Beschattung etc. lassen sich in einem lokalen und sicheren Heimnetz-Segment ohne Internet-Kontakt steuern. Das Internet kommt erst ins Spiel, wenn der Nutzer mit seiner App auch remote Geräte steuern können möchte oder ihm zusätzliche Services wichtig sind, zum Beispiel die Sprachsteuerung über Alexa und Co. Genau das muss für die Planung herausgefunden werden. Welche Anforderung hat der Nutzer, was davon braucht Internetzugang, was geht lokal?

Wenn es ins Internet geht, kann man Hacker trotzdem effektiv draußen halten. Es gibt hierzu gemeinsame Empfehlungen der SmartHome Initiative, der Polizei und des Verbands der Sachversicherer (VdS) [*]. Für deren Umsetzung muss der Nutzer kein Sicherheits-Experte sein. Drei zentrale Punkte sind:



Foto: Günter Martin

ZUR PERSON

Günter Martin ist Diplom-Informatiker und Geschäftsführer der CorDev GmbH. Das Unternehmen berät Anbieter von IoT-Geräten, zum Beispiel auch smarter Haushaltsgeräte, bei der Entwicklung und Vermarktung. Daneben ist er Beirat für Cybersecurity bei der Smart Home Initiative Deutschland tätig.

- 1 **Passwort:** Mit der Inbetriebnahme haben Anwender oder Betreiber die Verantwortung für sichere Passwörter, sofern dies nicht vom Installateur bereits erledigt wurde. Das WLAN-Passwort zu ändern, ist ein Albtraum. Selbst ohne Smart Home kommt leicht eine zweistellige Anzahl von Geräten zusammen, die im heimischen WLAN hängen und sich nach der Änderung nicht mehr einwählen können: Smartphones, PC, Drucker, Fernseher, Internet-Radio etc. Also gleich vom Start ab ein sicheres Passwort vergeben und nicht erstmal „nur zum Testen“ mit einem einfachen beginnen.
- 2 **Router-Sicherheit:** Wenn bei der Installation des Routers so verfahren wurde, wie oben beschrieben, ist die Welt in Ordnung. Kommen weitere smarte Geräte dazu und werden selbst installiert, dann besteht die Gefahr, dass diese plötzlich Tore öffnen (Portfreigabe), die vorher aus gutem Grund verschlossen waren. Bei etablierten Herstellern ist man recht sicher, bei vermeintlichen Schnäppchen ist Vorsicht geboten.
- 3 **Update:** Die größte Herausforderung besteht darin, das System über die Jahre im Betrieb dauerhaft sicher zu halten. Die vom Hersteller bereitgestellten Sicherheits-Updates müssen installiert werden. Bei manchen Systemen lässt sich einstellen, dass dies automatisch geschieht. Diese Einstellung sollte aktiviert sein.

Nicht so kritisch, wie die vorgenannten Punkte, aber doch zum Schluss erwähnenswert, ist die Entsorgung. Wenn ein smartes Gerät entsorgt werden soll, ist es Elektroschrott und landet nicht im Hausmüll. Das ist Allgemeinwissen. Was aber nur wenigen bewusst ist: Die Geräte können auch im defekten Zustand noch sensible Daten enthalten. So können smarte Glühbirnen noch im Müll das WLAN-Passwort verraten, wie es Bastler bei Birnen verschiedener Hersteller herausgefunden haben.

>> TEXT: GÜNTER MARTIN

* Bei Interesse zu den genauen wissenschaftlichen Quellangaben wenden Sie sich bitte an die Redaktion der BusSysteme. Alle Quellenangaben liegen vor.

Info

Eine gute Einführung in Building Information Modeling (BIM) gibt die diesjährige Ausgabe 2 der BusSysteme.

www.arnoldverlag.de/BusSysteme-02-2022/AV10018.1

ESYLUX

NEU! INTEGRIERTE STEUEREINHEIT
FÜR BIS ZU 16 GRUPPEN

RAUMÜBER- GREIFENDE LICHTSTEUERUNG FÜR DALI-2. **ESY!**



DALI-2

**APC10:
DALI-2-PRÄSENZMELDER MIT
APPLICATION CONTROLLER (APC)**

- Intelligente Steuerung von bis zu 16 Gruppen
- Steuereinheit, Tastereingänge und Busspannungsversorgung integriert
- BMS-Präsenzmelder als ergänzende Eingabegeräte erhältlich
- Einfache Konfiguration per ESY-App

PERFORMANCE FOR SIMPLICITY

ESYLUX Deutschland GmbH
info@esylux.de | www.esylux.de