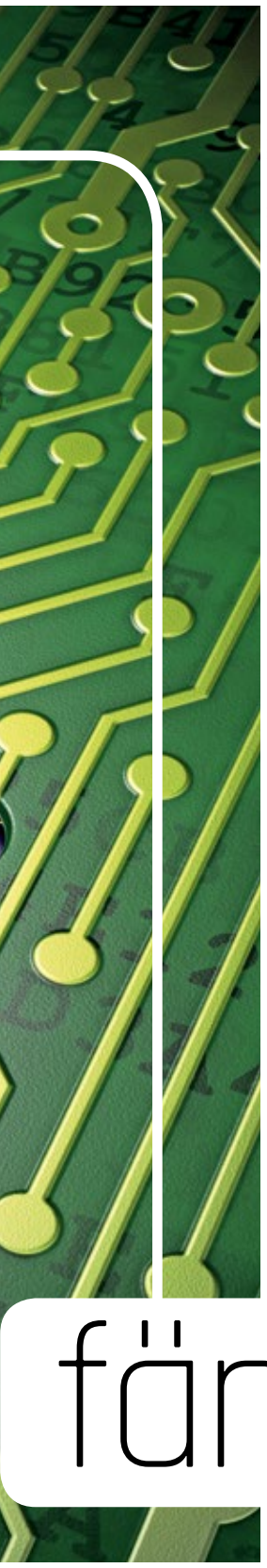
Sicherheit

Der Autor

Dr. Klaus Gütter (58) studierte an den Universitäten Würzburg und Erlangen Physik, bevor er 1990 mit Softwareentwicklung für EIB/KNX begann. 1992 gründete er die auf Gebäudeautomation, Netzwerk- und KNX-Sicherheit spezialisierte IT GmbH.



Illu: Maksim Kabakou, shutterstock

fängt im Haus an

Von intelligenter Haustechnik versprechen sich viele mehr Sicherheit für ihr Zuhause, gleichzeitig besteht eine eher diffuse Angst vor Hackern und Datenklau. Smarthome-Experte Dr. Klaus Gütter zeigt in seinem Gastbeitrag, dass sich diese beiden Aspekte nicht widersprechen. Und, dass es sinnvoll ist, sich über die Sicherheit des eigenen Smarthomes Gedanken zu machen.

Eine aktuelle Studie zum Interesse am Smarthome kam zu einem auf den ersten Blick kuriosen Ergebnis: An zweiter Stelle der Gründe für das Interesse an intelligenter Haustechnik lag der Wunsch nach mehr Sicherheit. Unter den Gründen dagegen lagen Sicherheitsbedenken ebenfalls auf Platz zwei. Das Verhältnis von Smart Home und Sicherheit ist also von Chancen und Risiken gleichermaßen geprägt.

Chancen und Risiken

Dabei ist völlig klar: Ein Smarthome bietet gegenüber einem konventionellen Haus auf jeden Fall mehr Sicherheit. Es kann erkennen, ob jemand da ist oder nicht. Wenn sich im Abwesenheitsmodus automatisch der Herd oder das Bügeleisen abschaltet, dann sind Brandursachen eliminiert. Auch eine Warnung vor offenen Fenstern beim Verlassen schützt gegen Schlagregen ebenso gut wie vor ungebetenen Gästen.

Andererseits hat es beispielsweise in Hotels schon Einbruchserien per Keycards gegeben, da hier viele identische Schließsysteme das Vorgehen vereinfachen. Der oft in Hacker-Szenarien skizzierte „Einbruch per Laptop“ spielt dagegen im Heimbereich keine Rolle – auch, weil Smarthomes meist individuell konfiguriert werden und daher der Aufwand für Einbrecher im Vergleich zu rustikaleren Methoden zu hoch ist.

Relevanter ist ein möglicher Verlust der Privatsphäre. Angreifbare Geräte oder Fehlkonfigurationen könnten Unbefugten Informationen über die Lebensgewohnheiten liefern, Zugriff auf Kameras bieten oder sensible Daten wie Passwörter für Onlinedienste liefern. Obwohl bislang kein konkreter Fall bekannt geworden ist, sollten Nutzer das Risiko eines Eingriffs von außen auf ihr Smarthome durchaus ernst nehmen. Ein solcher Angriff bringt im Zweifel hohen Schaden – von Fehlfunktionen über Schäden an Gebäude und Einrichtung bis hin zu einer Erpressung.

Deshalb sollte man zunächst einmal untersuchen, welche Angriffspunkte das eigene Smarthome und Heimnetzwerk bieten. In komplexen Installationen sollte dies der Systemintegrator schon bei der Planung tun und dabei auch gleich ein maßgeschneidertes Paket zur Absicherung erstellen. Wer seine Haustechnik selbst vernetzt, der kann die folgenden Punkte auf die eigene Ausstattung übersetzen.

Haus-Installation und Netzwerk

Zunächst ein Blick in das eigene Netzwerk – auf vernetzte Geräte, Sensoren, Aktoren und Automatisierungskomponenten, die im Haus miteinander kommunizieren. Meist findet zumindest ein Teil der Kommunikation über ein IP-Netzwerk, also ein kabelgebundenes LAN oder ein WLAN statt. Hier müssen direkte Zugriffe möglicher Angreifer verhindert werden. Eine einfache Möglichkeit dafür ist der Aufbau eines separaten Haustechniknetzwerks, das vom restlichen Heimnetzwerk und vom Internet getrennt ist.

Im Heimbereich ist dafür recht günstig ein „virtuelles LAN“ ausreichend. Ein solches VLAN wird über spezielle Netzwerk-Switches einge-

Für den Aufbau sicher voneinander getrennten Netzwerkabschnitten, sogenannten VLANs, ist ein Netzwerk-Switch notwendig, der sich dafür programmieren lässt – etwa der Netgear GS716. www.netgear.de

richtet, die mehrere abgeschottete Netzwerkbereiche einrichten können. Meist möchte man sein Smarthome auch von außen fernsteuern – also ist doch ein Internetzugang nötig. Der sollte aber keinesfalls offen sein wie ein Scheunentor – wie dies in der Vergangenheit oft der Fall war: 2014 hat die TU Wien über 3000 ungeschützte KNXnet/IP-Router im Internet gefunden, die vollen Zugriff auf die dahinter liegenden KNX-Installationen erlaubten – vom Mithören über das Auslösen von Schaltvorgängen bis zur Umprogrammierung oder gar Beschädigung von Geräten.

Ein anderes Problem hat eine Schadsoftware namens „Mirai“ gezeigt. Sie kaperte rund eine halbe Million Kameras, Videorecorder und andere vernetzte Geräte in Heimnetzwerken und programmierte sie zu einem „Botnetz“, das gezielt unliebsame Internetserver lahmlegen konnte.

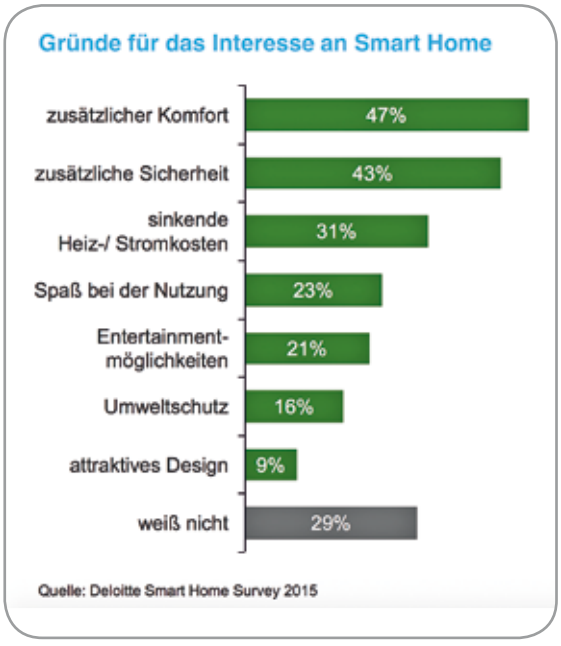
Besonders sensibel sind Funksysteme, da diese von außen leicht gestört oder missbraucht werden können. Eine starke Verschlüsselung der Funksignale ist hier Pflicht. Das KNX-RF-Funksystem etwa erfüllt diese Anforderungen mit dem neu eingeführten Standard „KNX Secure“. Geräte, die diesen Standard unterstützen, kommen allerdings erst jetzt auf den Markt. Andere Funksysteme wie ZigBee sind bereits mit Verschlüsselungen geschützt. Doch auch hier werden immer wieder Sicherheitslücken durch Fehler in der Umsetzung einzelner Produkte gefunden. Deswegen sollte das Gateway zwischen dem Funksystem und verkabelten Systemen so konfiguriert sein, dass nur bekannte Nachrichten weitergeleitet werden.

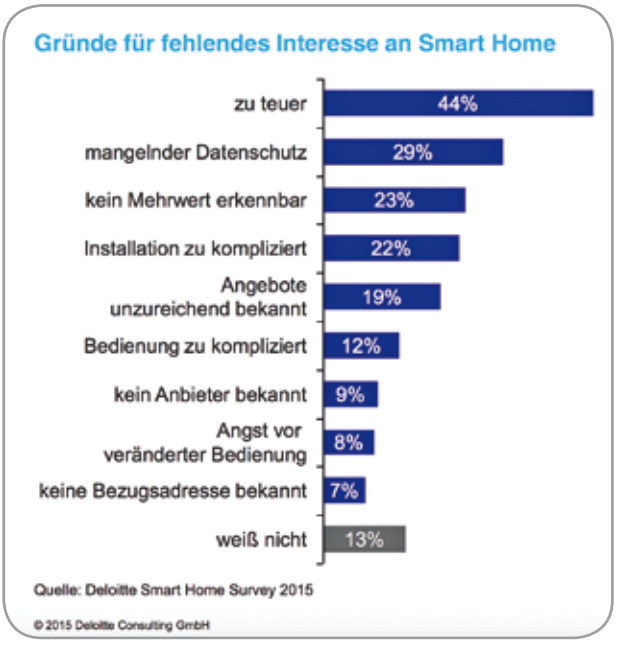
Unabhängig von der eingesetzten Technologie müssen vernetzte Systeme regelmäßig gewartet werden. Software-Updates erweitern eben nicht nur Funktionen, sie schließen gerade bei Anlagen mit Internetanbindung potentielle Sicherheitslücken. Deshalb ist es wichtig, dass man solche Geräte, ebenso wie etwa den WLAN Router oder den PC, mit allen Updates des Herstellers auf dem Laufenden hält. In professionell geplanten Anlagen sollte diesen Service der Systemintegrator übernehmen. Ein Smarthome-Wartungsvertrag ist daher durchaus sinnvoll.

Schwachstelle Visualisierung

Will man sein Smarthome über eine externe Visualisierung wie etwa eine App fernsteuern, dann muss es per Netzwerk verbunden sein – einschließlich Sicherheitsvorkehrungen wie ein eigenständiges Netzwerk, Login über Benutzername und Passwort oder über Client-Zertifikate. Die Kommunikation zwischen Endgerät und Visualisierungsserver sollte verschlüsselt sein, um jedes Mithören des Datenverkehrs auszuschließen. Für dem Fernzugriff von außerhalb gibt es

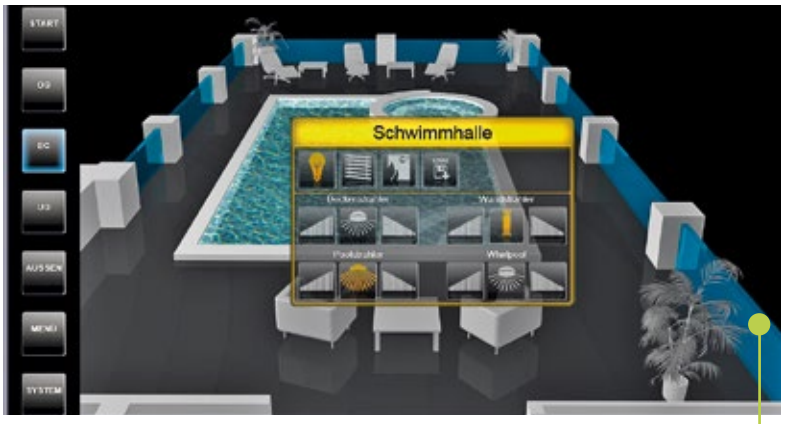
Smarthome-Ambivalenz: Sowohl der Bedarf an Sicherheitsfunktionen als auch die Furcht vor Sicherheitslücken spielen in der Wahrnehmung von Smarthome-Systemen bei Nutzern eine wichtige Rolle.





weitere Herausforderungen: Empfohlen wird der Aufbau eines VPN (Virtual Private Network). Das ist eine Verlängerung des lokalen Netzwerks über einen sicheren Tunnel durchs Internet bis zum Smartphone oder dem entfernten PC. Eine VPN-Variante sind Portalsysteme. Hier bauen das Smartphone und der Visualisierungsserver je eine Verbindung zu einer „Vermittlungsstelle“ auf (siehe unten rechts). Das ist einfach einzurichten, allerdings sollten dabei alle Daten durchgehend verschlüsselt übertragen und gespeichert werden – was nicht immer der Fall ist.

Einige Visualisierungssysteme laufen nicht im Haus, sondern auf Servern des Systembetreibers – also in der Cloud. Das kann ein Sicherheitsvorteil sein, da ein solcher Dienst in der Regel gut gewartet wird. Oder aber ein Nachteil, da er viele Smarthomes verwaltet und daher ein lohnendes Ziel für Angreifer darstellt. Ein Sicherheitsproblem betrifft dann gleich sehr viele Kunden. Hier sind Anbieter in der Pflicht, die Sicherheit ihrer Angebote klar zu dokumentatieren.



Sicherer Server vom Experten

Elvis ist ein Steuerungs- und Visualisierungssystem für verschiedene Smarthome-Standards wie KNX, Modbus, M-Bus und DLNA. Es besteht aus einem Server sowie Clients (Visualisierungsoberflächen) für Windows, iOS, Android und Internetbrowser.
In puncto Sicherheit sind folgende Eigenschaften bemerkenswert:
• Verschlüsselte, über Zertifikate gesicherte Netzwerkkommunikation.
• Unterstützt verschiedene Authentifizierungsverfahren (Benutzername/Passwort, Clientzertifikat, etc.).
• Verschlüsselt gespeicherte Zugangsdaten, etwa zum Mailserver.
• Redundanter Betrieb möglich. Automatische Umschaltung, wenn einer der Server ausfällt.
Ein Sicherheitsassistent hilft bei der Einhaltung empfohlener Sicherheitsmaßnahmen. Sichere Lösungen sind damit einfach realisierbar.
www.it-gmbh.de/produkte/elvis-3.html

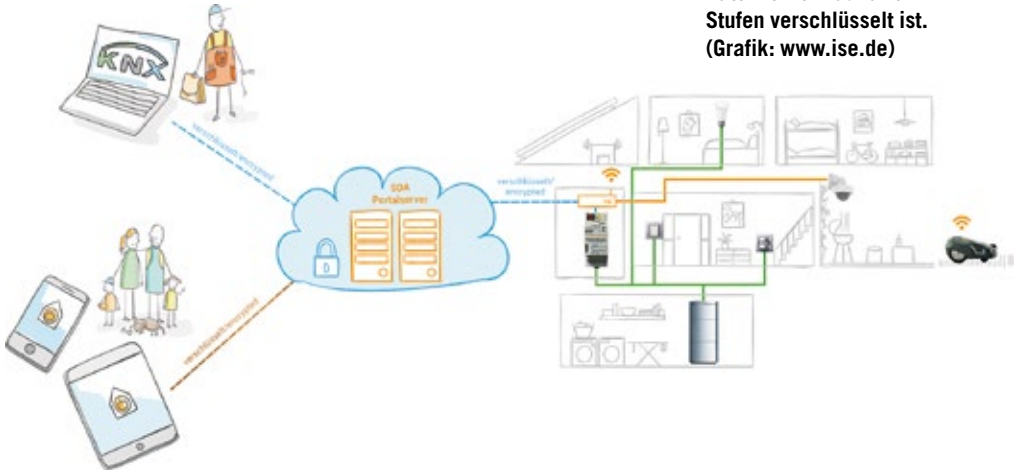
Externe Dienstleister

In einem Smarthome fallen viele Daten an, die auf die eine oder andere Art ausgewertet werden können. Es wird erwartet, dass es in Zukunft vermehrt Dienstleister geben wird, die dies erledigen und so etwa auch Aktionen auslösen. Ein Energieversorger bietet etwa Verbrauchs- und Tarifoptimierung an und möchte gezielt Lasten ab- und zuschalten, ein Pflegedienst überwacht die Aktionen des Bewohners um nach dem Rechten zu sehen. Das Sicherheitskonzept des Anbieters muss mindestens die folgenden Kriterien erfüllen:
- Die Übertragung muss verschlüsselt, sowie gegen „Man-in-the-Middle“-Attacken (Mithören) und „Replay“-Attacken (Abspielen aufgezeichneter Kommunikation) geschützt erfolgen.
- Die beim Dienstleister gespeicherten und verarbeiteten Daten dürfen nur für Autorisierte zugänglich sein.
- Nicht mehr benötigte Daten müssen gelöscht werden.

Seriöse Anbieter stellen dies in der Datenschutzerklärung dar. Hier kann der Verbraucher auch ein Stück weit mithelfen: Dem Dienstleister sollten nur die Daten zur Verfügung gestellt werden, die zur Erfüllung der Aufgabe erforderlich sind.

Fazit: Zur Planung eines Smart Homes gehört ein individuelles Sicherheitskonzept – je nach Art des Objekts und den Bedürfnissen der Bewohner. Die gute Nachricht: Richtig und technisch aktuell konfiguriert, sind die Risiken beherrschbar, und das Smarthome selbst ist kein Risiko, sondern im Gegenteil ein Gewinn an Sicherheit.

Dem Bauherren und Systemintegrator hierfür die Technik und Richtlinien an die Hand zu geben, ist eine Aufgabe, der sich Institutionen, Hersteller und Experten für intelligente Häuser aber verstärkt stellen müssen. Dr. Klaus Gütter



Für den Remote-Zugriff via „Portal-System“ schaltet sich ein Server in die Kommunikation ein, der den Zugang zur Smarthome-Zentrale als auch die Adresse des Endgerätes für die Steuerung kennt. Wichtig ist, dass der Datenverkehr auf allen Stufen verschlüsselt ist. (Grafik: www.ise.de)

Foto: ISE GmbH (2), Deloitte Consultin GmbH (2), IT GmbH, Netgear