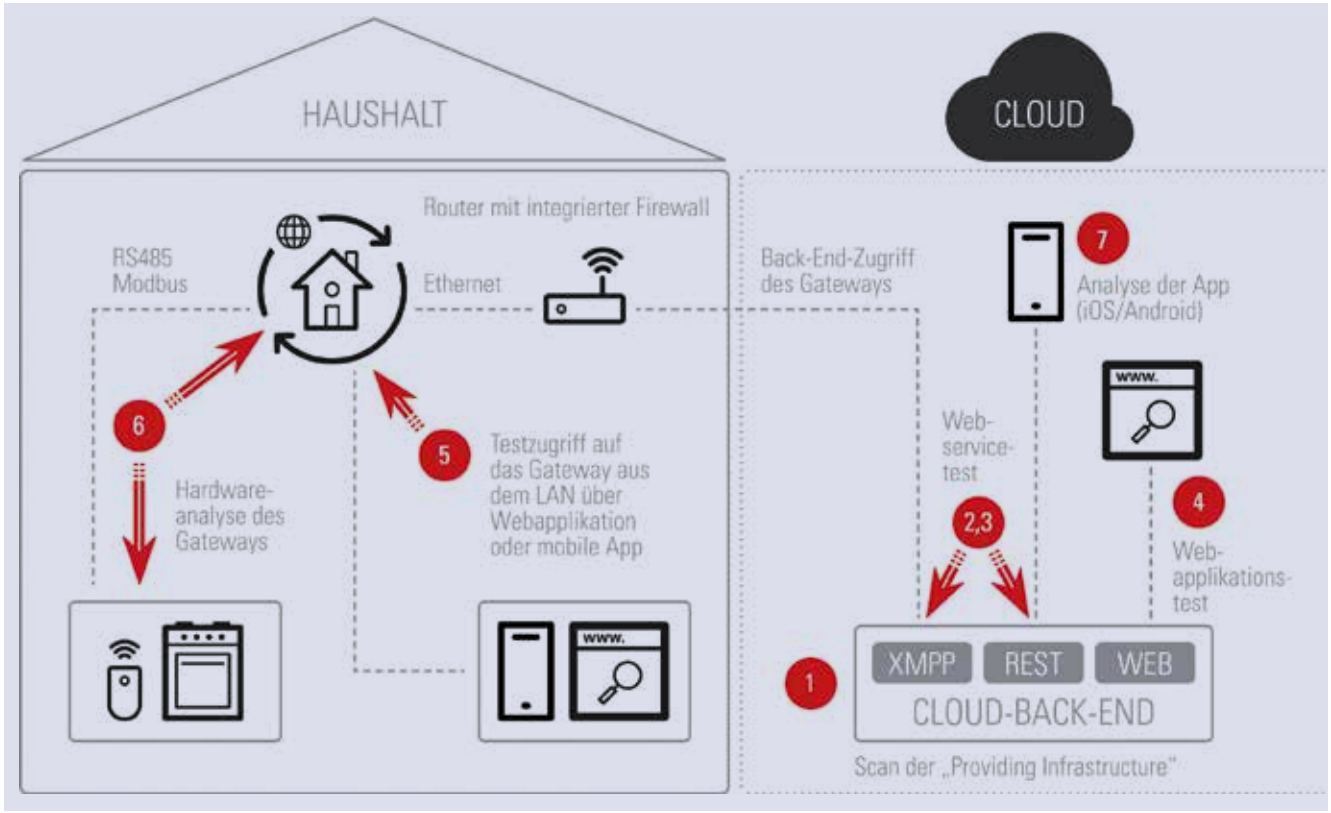

Grafik: Syss GmbH

Komponenten des IoT: Immer mehr miteinander vernetzte Produkt, erhöhen zwar den Komfort für den Nutzer, aber auch die Anfälligkeit gegenüber Cyberangriffen.

Internet der Dinge

Smart genug?

Sebastian Schreiber

Das Internet der Dinge macht den Alltag zunehmend komfortabler, geht aber auch mit erheblichen Sicherheitsrisiken einher. Die Smartness der Hersteller und Nutzer sollte mit dieser Entwicklung unbedingt Schritt halten.

Während Ihr Auto gerade für Sie einparkt, schalten sich zu Hause schon mal Licht und Heizung an. Wenig später freuen Sie sich über die Warenlieferung, die Ihr fast leerer Kühlschrank ohne Ihr Zutun bestellt hat. Unsere Haushalte werden „smarter", das heißt: Immer mehr elektronische Geräte werden über das Internet miteinander verknüpft und agieren zunehmend eigenständig, und mit der steigenden „Intelligenz" der Dinge nimmt die Notwendigkeit menschlicher Aktionen ab.

2020, so prognostizieren Analysten, werden über 30 Milliarden Geräte mit dem Internet verbunden sein, miteinander kommunizieren und die getauschten Daten aufbereiten. Das Internet der Dinge (Internet of Things – IoT) macht den Alltag zunehmend komfortabler, geht aber auch mit erheblichen Sicherheitsrisiken einher.

Internet der Dinge: in Grundzügen

IoT bezeichnet – ähnlich wie M2M (Machine to Machine) oder Industrie 4.0 – die Kommunikation zwischen intelligenten Geräten ohne aktives Zutun des Menschen. Das Internet der Dinge kombiniert unterschiedliche Technologien, die die Erfassung und Analyse sowie den Austausch von Daten ermöglichen und daraus Aktionen ableiten.

IoT-Geräte sollen sich durch eine lange Betriebszeit sowie durch eine geringe Energieaufnahme auszeichnen. Ihre zahlreichen Sensoren und Eingabegeräte, etwa Berührungserkennung und Grafikdisplays, erfordern zugleich eine enorme Rechenleistung. Notwendig sind außerdem diverse Schnittstellen wie USB, Ethernet oder Funkverbindungen (Bluetooth Low Energie (BLW) und WiFi). Und nicht zuletzt sollen die Privatsphäre der Nutzer und hohe Sicherheitsstandards gewahrt sein. IoT-Geräte besitzen häufig eine eigene IP-Adresse und sind als eigenständiges Gerät im lokalen Netz oder auch im Internet erreichbar.

Internet der Dinge: unter Attacke

Die digitalen Risiken, die für mit dem Internet verbundene Geräte entstehen – also nicht nur innerhalb eines geschlossenen Firmennetzes angesprochen werden können –, betreffen folgende Ebenen:

- Hardware: IoT-Geräte interagieren mit ihrer Umgebung meist über Sensoren. Signale können verändert, Sensoren gestört und dadurch Fehlfunktionen erzeugt werden.
- Netzwerk: Der Informationsaustausch zwischen den Komponenten kann dahingehend manipuliert werden, dass die verwendete Software ungewollte Aktionen auslöst.
- Back-End- oder Cloud-Lösung: Die gespeicherten Betriebsdaten des IoT-Produkts können missbraucht werden.
- Applikationsoberfläche: Schwachstellen in der Bedienung einer Webanwendung oder eines mobilen Geräts können ausgenutzt werden.

Entsprechend vielfältig sind die Angriffe, denen IoT-Geräte zum Opfer zu fallen drohen: 2016 sind tausende IoT-Geräte für Distributed Denial-of-Service (DDoS)-Angriffe ausgenutzt und große Teile des Internets lahmgelegt worden. Betroffen waren unter anderem Riesen wie Amazon, Netflix, Spotify und Twitter. Derartige Angriffe und Ausfälle bedeuten für Hersteller und Dienstleister nicht nur einen Image-, sondern auch einen immensen wirtschaftlichen Schaden. Betreffen DoS-Vorfälle die Steuerung eines Herds oder die Funktion eines Herzschrittmachers oder werden vernetzte Autos gehackt, sind Menschenleben in Gefahr.

IoT-Geräte können sich schnell mit Malware infizieren. 2016 sind circa 900.000 Router der Telekom Opfer eines Botnet-Angriffs geworden. Nur im ersten Moment erheiternd wirkt der Fall des Smart Lock-Nutzers, dessen Nachbar sich ohne Schlüssel Zugang zur Wohnung verschafft: Wer per Smartphone-App mit Smart Lock seine Haustür steuert und zudem einen Sprachassistenten aktiviert hat, braucht nur noch ein Fenster offen zu lassen, um Fremden Zutritt zu gewähren. Ein „Siri, unlock the front door“ („Siri, öffne die Haustür“) reicht völlig aus. Zum Tool für Angriffe können auch Suchmaschinen werden. Shodan und Censys können viele IoT-Systeme finden und private Kameras, Wetterstationen, ja selbst Einrichtungen der öffentlichen Strom- und Wasserversorgung ansteuern. Gerade in Bezug auf kritische Infrastrukturen ist das hiervon ausgehende Sicherheitsrisiko immens hoch, wie die Malware Stuxnet gezeigt hat.

Wie teuer den Steuerzahlern ein Angriff auf Smart City-Lösungen zu stehen kommen kann, mussten im März 2018 die Bewohner von Atlanta feststellen: Ein Ransomware-Angriff legte die Stadt tagelang lahm und brachte Kosten von fast 17 Millionen Dollar mit sich. IT-Sicherheitsforscher gehen davon aus, dass Angriffe, die IoT-Geräte ausnutzen, in Zukunft zunehmen werden.

Internet der Dinge: im Test

Vor dem Hintergrund dieser Gefahren sollten Hersteller in die Pflicht genommen und Sicherheitstests zum integralen Bestandteil des Entwicklungsprozesses von IoT-Geräten werden. Ein entscheidendes Instrument der Risikominimierung ist der IoT-Penetrationstest. Auf der Grundlage einer passgenauen Auswahl an Tests und Tools bezüglich der Geräteanforderungen können zuverlässige Erkenntnisse über den Sicherheitsstatus gewonnen werden. Die Funde und erzielten Testergebnisse sollten für den Hersteller genau dokumentiert und Empfehlungen für die Behebung von Schwachstellen ausgesprochen werden, sodass das IT-Sicherheitsniveau nachhaltig gesteigert werden kann. Geprüft werden sollten die Dienste im Back-End, um die Gefahr einer Rechteausweitung eines Angreifers, die zur Kompromittierung des Systems führen kann, zu evaluieren. Webservice und Datenverkehr müssen auf ihre Manipulierbarkeit getestet und es muss sichergestellt werden, dass das IoT-Gerät in der Lage ist, die Legitimität einer Anfrage zu prüfen. Auch mögliche Implementierungsfehler in der Hardware, beispielsweise bei den verbauten Sensoren, müssen ausgeschlossen werden.

Internet der Dinge: mit Sicherheit

Die Hersteller und Nutzer des Internets der Dinge sollten also so intelligent sein, ihre Geräte nicht nur so smart, sondern auch so sicher wie möglich zu machen. Für Hersteller bedeutet dies, IT-Sicherheit in Form von passenden Architekturen und geeigneten sicherheitsbezogenen Entwürfen als festen Bestandteil in die Planungs- und Entwicklungsphase zu implementieren. Zwei Beispiele: Angriffsflächen lassen sich minimieren, indem vor dem Entwicklungsprozess entschieden wird, welche Komponenten für den tatsächlichen Betrieb des Gerätes benötigt werden. Da die Kommunikation zwischen Schnittstellen und deren Absicherung ein neuralgischer Punkt ist, sollten bereits bei der Konzeption eines IoT-Gerätes grundlegende Funktionsbestandteile auf Sicherheit unterersucht werden.

Vor der Markteinführung des Produkts sollten Sicherheitstests durch einen unabhängigen Dienstleister durchgeführt wurden. Wird IT-Sicherheit schon im Entstehungsprozess beachtet, müssen im Betrieb weniger Sicherheitslücken aufwendig behoben werden.

Bild: Andreas Albrecht

Wie leicht IoT-Komponenten manipuliert werden können, demonstriert Sebastian Schreiber, Geschäftsführer der Syss GmbH, immer wieder auf Vorträgen.

Nutzer sollten die voreingestellten Passwörter von IoT-Geräten generell ändern. Die Geräte sollten stets in einem separaten Netzwerk isoliert werden, da sie eine nicht einzuschätzende Gefahr für das lokale Netzwerk darstellen, in dem sich private Dokumente, Videos und Bilder befinden.

Wir alle sollten so intelligent sein, unsere immer „smarter“ werdende Lebens- und Arbeitswelt auch immer sicherer zu machen – erst recht, wenn 5 G-Netze das Internet der Dinge in eine neue Ära führen werden.

Sebastian Schreiber, Geschäftsführer der SySS GmbH, www.syss.de

www.sicherheit.info