Smart Home? Aber sicher!

Wie Sie schnüffelnde Geräte isolieren und Ihre Privatsphäre schützen

Smart-TV, Überwachungskameras, Heizungsthermostate und Schaltsteckdosen: Alles wird smart, alles kommuniziert über das Internet, am besten mit einer App auf dem Smartphone. Dafür durchlöchern die Gadgets die Router-Firewall wie einen Schweizer Käse. Arglose Kunden können das Risiko mangels Herstellerangaben unmöglich abschätzen.

Von Mirko Dölle

Es gibt kaum mehr ein Gerät im Haushalt, das nicht mit dem Internet vernetzt ist – entweder über Ihr WLAN oder über eine Steuereinheit. So heizt das Smart Home schon ein, wenn Sie sich auf den Heimweg machen, das Smart-TV streamt Videos direkt aus dem Internet, die Webcam sieht im Garten nach dem Rechten und der Staubsauger-Roboter hält sie in Echtzeit über den Stand der Hausarbeiten auf dem Laufenden.

Damit solche Informationen nicht nur im lokalen Netz, sondern auch unterwegs abrufbar sind, untertunneln die Geräte regelmäßig die Firewall Ihres Routers und stellen eine direkte Verbindung mit Servern des Herstellers her. Diese Server dienen wiederum der App als zentrale Anlaufstelle, um jederzeit und von überall einen eigenen Tunnel ins Heimnetz graben und damit die Bilder der Webcam abrufen oder den Heizungsthermostat einstellen zu können.

Bedrohung von innen

Doch damit gewährt man auch den Herstellern indirekt Zugriff auf das eigene Netzwerk, mit dem die IoT-Geräte ständig verbunden sind. Hinzu kommt, dass man als Kunde weder Einblick in die Firmware noch in die exakte Hardwareausstattung der IoT- und Smart-Home-Geräte hat. Wer denkt, wir würden hier unbegründet Panik verbreiten, kann ab Seite 72 nachlesen, welche IoT-Geräte ungeschützte Root-Server, undokumentierte Web-Frontends oder gar Mikrofone enthalten, von denen der Käufer nichts weiß.

Wie viele Sicherheitslücken in IoT-Geräten schlummern, mit denen Angreifer die Geräte übernehmen oder sensible Informationen ausspähen können, kann der Kunde unmöglich abschätzen. Die Politik scheint das Problem inzwischen erkannt zu haben: So will die CDU noch in der laufenden Legislaturperiode ein neues Produkthaftungsgesetz für mangelhafte Software auf den Weg bringen. Schließt ein Hersteller bekannt gewordene Sicherheitslücken nicht, soll er künftig für daraus entstehenden Schaden haften.

Doch auch damit bleiben IoT-Geräte undurchschaubare Blackboxes, die keinesfalls im gleichen Netzwerk betrieben werden dürfen, wo PCs, Smartphones, Tablets und NAS arbeiten und sensible Informationen erbeutet werden könnten. Wie Sie Ihr Netz mit modernen Access Points und Netzwerk-Switches aufteilen und die IoT- und Smart-Home-Geräte sinnvoll voneinander und von anderen Geräten isolieren, erfahren Sie ab Seite 76.

Besonders kritisch sehen wir dabei versteckte Sensoren wie etwa ein Mikrofon in einer Schaltsteckdose, über deren Existenz der Hersteller nirgends ein Wort verliert: Das untergräbt das Vertrauen der Kunden und schürt verständlicherweise Ängste. Vielleicht muss auch hier ein Gesetz her, das die Hersteller verpflichtet, sämtliche enthaltenen Sensoren auf der Verpackung aufzulisten. Nur so könnten Kunden schon vor dem Kauf erkennen, dass ein Produkt potenzielle Überwachungstechnik enthält. Auf Prospekte, Produktspezifikationen und Handbücher ist heute nachweislich kein Verlass.

(mid@ct.de) c't

Ungeahnter Mehrwert: Die von Aldi im Januar verkauften WLAN-Schaltsteckdosen enthalten ein nirgends dokumentiertes, nur mit Standard-Passwort gesichertes Web-Frontend. Darüber gelangt man sogar an das WLAN-Passwort.