Quelle: eQ-3 (alle Bilder)

Bild 1: *Eine nachweisbar sichere Smart-Home-Lösung nimmt den Endkunden die Angst vor Datenmissbrauch und Hacker-Angriffen*

IT-Sicherheit und Datenschutz

Wie sicher ist das smarte Zuhause?

Für immer mehr Menschen gehört intelligente Technologie zu ihrem Alltag wie das Auto oder Telefon. Doch mit der Verbreitung der intelligenten Alleskönner wächst auch die Sorge vor Datenlecks und digitalen Attacken auf das smarte Zuhause.

Deutlich macht das unter anderem die Bitkom-Studie »Das intelligente Zuhause: Smart Home 2021«: 39% der Befragten geben an, aus Angst vor dem Missbrauch persönlicher Daten bislang keine Smart-Home-Anwendungen zu nutzen; ein Anstieg um 6% gegenüber dem Vorjahr. Die Furcht vor Hacker-Angriffen treibt sogar 41% der Studienteilnehmer um und ist damit laut der Umfrage mittlerweile der größte Vorbehalt gegenüber smarter Technik. Aber wie sicher ist das smarte Zuhause denn nun wirklich?

Das deutsche Unternehmen eQ-3, Hersteller des Smart-Home-Systems »Homematic IP«, setzt z. B. auf moderne Technologie und Sicherheitsstandards, um seine Anwender zu schützen (**Bild 1**). Die gesamte Kommunikation zwischen Geräten in einem Smart Home ist dabei kryptografisch gesichert (**Bild 2**). Für die Authentifizierung und Verschlüsselung aller Daten in der Cloud-Kommunikation setzt das System, ähnlich wie bei der Funkkommunikation, auf etablierte Methoden wie CCM (kurz für: »Counter with CBC-MAC«, es macht aus einer Blockchiffre ein Authenticated-Encryption-Verfahren) und AES-

Bild 2: *Der Betriebsmodus für Blockchiffren CCM und der Verschlüsselungsstandard AES-128 sorgen für eine gesicherte Datenübertragung der Smart-Home-Geräte*

Bild 3: *Werden Datenpakete bereits während der Installation verschlüsselt und authentifiziert, ist das Mitlesen oder das Verändern von Daten unmöglich*

Bild 4: *Die »Homematic IP«-App kann ohne Registrierung verwendet werden, es wird nur eine IP-Adresse verschlüsselt erfasst*

128 (Advanced Encryption Standard mit einer Schlüssellänge von 128 Bit) und verwendet zudem ein zertifiziertes und patentiertes Verfahren für den Austausch der Schlüssel. Bereits während der Installation werden Datenpakete auf diese Weise verschlüsselt und authentifiziert. Ein Mitlesen oder Verändern von Daten ist somit unmöglich (**Bild 3**). Darüber hinaus wird die Cloud des Smart-Home-Systems ausschließlich auf deutschen Servern betrieben, die höchste Sicherheitsstandards erfüllen müssen.

Klare Kennzeichnung ist wichtig

Um das Sicherheitsniveau beständig auf höchstem Niveau zu halten, ist eine kontinuierliche Überprüfung unerlässlich. »Homematic IP« wird deshalb seit Jahren durch unabhängige Institute auf den Prüfstand gestellt. AV Test bescheinigt der Smart-Home-Lösung ein in allen relevanten Bereichen durchdachtes Sicherheitskonzept. Der Schutz des Systems vor unberechtigten Zugriffen steht besonders im Fokus der Analyse. Das Institut bestätigt, dass es keine Hinweise auf spürbare und/oder kritische Schwachstellen und Verwundbarkeiten gibt. Der VDE hat eine eigene Testplattform entwickelt, mit der alle derzeit am Markt eingesetzten Lösungen umfassend evaluiert, geprüft und zertifiziert werden können. Das Ergebnis: Das System von eQ-3 wurde als einzige Smart-Home-Lösung zum fünften Mal in Folge für Protokoll-, IT- und Datensicherheit zertifiziert.

Privates muss privat bleiben

Beim Datenschutz geht der Hersteller aus Leer einen heutzutage ungewöhnlichen Weg: Für die Verwendung der »Homematic IP«-App ist keinerlei Registrierung notwendig (**Bild 4**). Das ist nicht nur anwenderfreundlich, es dient auch dem Datenschutz. Die Nutzung des Systems erfolgt anonym, lediglich die verschlüsselte Erfassung der IP-Adresse ist aus technischen Gründen notwendig. So besteht erst gar nicht die Gefahr, dass persönliche Daten in falsche Hände geraten könnten.

Ist das smarte Zuhause also sicher? Ja – zumindest, wenn ein nachweislich sicheres Smart-Home-System zum Einsatz kommt. Gerade No-Name-Produkte von Billiganbietern können tatsächlich ein Sicherheitsrisiko darstellen. Wer sich und seine Kunden jedoch vor dem Kauf informiert und auf unabhängige Überprüfungen achtet, der ermöglicht ein smartes und gleichzeitig sicheres Wohnen.

Autor:
Johannes Rohe,
PR Manager, eQ-3 AG, Leer

5 Tipps für ein sicheres Smart Home:

1. Bei Smart Home-Systemen auf unabhängige, vertrauenswürdige **Prüfsiegel** (z. B. von VDE und von AV-Test) achten, welche die Sicherheit und den Datenschutz attestieren
2. Regelmäßige Soft- und Firmware-**Updates** schließen etwaige Sicherheitslücken
3. Sichere und unterschiedliche **Passwörter** verwenden. Sichere Passwörter besitzen mindestens acht Stellen und bestehen idealerweise aus einer Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Beim Generieren und Verwalten von Passwörtern helfen Passwort-Manager
4. Das Sicherheitsniveau ist immer nur so groß wie das schwächste Glied. Deshalb müssen alle **Geräte gesichert** sein, mit denen auf das Smart Home zugegriffen wird. Gleiches gilt auch für alle Geräte im Heimnetz. Gefährdet sind u. a. Computer, Tablets und Smartphones. Anti-Virus-Software hilft zusätzlich
5. Für Besucher ein **Gast-WLAN** einrichten. Auch wenn Gäste nichts Böses im Schilde führen, könnten sich auf ihren Geräten schädliche Viren befinden.