Zum Europäischen Datenschutztag

3 Tipps für sichere Smarthome-Verbindungen

Wie sicher ist das Smarthome? Pünktlich zum Europäischen Datenschutztag am 28. Januar sollten drei Tipps beachtet werden, um das Zuhause nicht nur smart, sondern auch sicher zu machen.

Foto: Datensicherheit keine Unmöglichkeit – auch mit smarten Geräten und Anwendungen im Zuhause.

Jährlich findet am 28. Januar der Europäische Datenschutztag statt. Ziel des Aktionstags ist es, alle Bürger für das wichtige Thema Datenschutz zu sensibilisieren. Mehr Reflexion über Datentransfers, – das bedeutet zu verstehen, in welchen Situationen sensible Informationen gefährdet sind. Mit dem zunehmenden Gebrauch von Smarthome-Produkten vermehren sich die Fragen: Sind meine Daten sicher? Und wie kann ich mich ausreichend schützen? Anbieter gibt es viele, daher ist es wichtig, auf folgende Dinge zu achten, um nicht nur smart, sondern auch sicher in das neue Jahr zu starten.

1. Lokale Datenspeicherung statt externer Cloud

Die meisten Smarthome-Systeme basieren auf Cloud-Lösungen. Für den Betrieb müssen Daten aus der Hand gegeben werden. Die Ansicht, Speicherung und Auswertung sensibler Daten erfolgt nicht lokal beziehungsweise Zuhause, sondern extern auf einem Server: In Echtzeit transportiert das System private Einblicke, wie etwa Videos der Überwachungskamera an die Cloud. Risiken durch Datenlecks und Angriffe von außen auszuschließen, ist nahezu unmöglich. Besonders schwierig wird es bei

Herstellern im Ausland ohne gesetzliche Datenschutzbestimmungen, z. B. haben US-Server keinen Schutz vor behördlicher Überprüfung und Auswertung. Smarthome-Alarmsysteme wie die XT1 Plus vom deutschen Unternehmen LUPUS-Electronics verzichten daher auf eine Cloud.

Statt in einer Cloud können Smarthome-Systeme mit einer Basisstation die Datenspeicherung vollkommen lokal organisieren. Die Kommunikation zwischen der Station und den Komponenten basiert auf modernem Funk. So funktioniert das Smarthome sogar vom Internet abgeschnitten. Die Daten verlassen zu keiner Zeit das Haus. Die Steuerung von Licht, Heizung oder Sicherheitskontakten findet über eine App oder manuell statt. Hackern bleibt nur der erfolglose direkte Angriff auf die einzelne Basisstation, die TLS 256 Bit verschlüsselt sein sollte. Im Ernstfall wird der sofortige Alarm gesendet.

2. TLS 256 Bit-Verschlüsselung

TLS bedeutet Transport Layer Security (TLS). Dabei handelt es sich um ein Protokoll, das die Daten, die zwischen Anwendungen, z.B. zwischen App und Basisstation, über das Internet übertragen werden, verschlüsselt. Auf diese Weise können Lauscher und Hacker nicht erkennen, was übermittelt wird. 256 Bit beschreibt die Länge des Schlüssels, mit dem die Kommunikation gesichert ist. Da ein Bit immer eine 0 oder eine 1 ist, ergibt sich daraus sich eine Folge von 256 Nullen und Einsen, also 2^256 Möglichkeiten. Damit ist diese Verschlüsselung eines der sicherstes Verfahren der Welt.

3. Zusätzlicher Schutz durch Rolling Code

Das sogenannte Rolling Code-Verfahren schützt die Funkverbindungen zwischen den Sensoren und der Basisstation gegen Sabotage-Versuche von außen. Gesichert wird der Zugriff auf authentifizierte, drahtlose Bediengeräten wie z. B. Fernbedienungen oder Keypads. Dabei wechseln nach jedem Befehl bzw. nach jeder Datenübertragung die Codezahlen. Die Empfangseinrichtung reagiert nur auf die nächsten den Hackern unbekannte Zahlen, nicht auf bereits genutzte. Die Rolling Code-Varianten unterscheiden sich von Hersteller zu Hersteller und liegen im Durchschnitt bei ca. einer Millionen Kombinationen. Die meisten Varianten bietet LUPUS-Electronics, deren Anlagen über 536 Millionen unterschiedliche Kombinationen umfassen, was sie besonders sicher gegen Angriffe von außen macht.

Fazit: Information ist alles

Fest steht: Ob intelligente Steuerungen oder Überwachungskameras – Smarthome-Produkte können die Energieeffizienz, das Sicherheitsgefühl und den Komfort verbessern. Und das ganz ohne Sorgen. Moderne, zertifizierte Produkte vereinen alle Standards. Wer sich beim Gerätehersteller informiert, muss sich um Hacker keine Gedanken machen und kann alle Vorteile genießen.

Über LUPUS Electronics

LUPUS-Electronics wurde von den drei Brüdern Philip, Jan-Michael und Matthias Wolff gegründet und beschäftigt an seinem Hauptstandort in Landau in der Pfalz 30 Mitarbeiter. Das Familienunternehmen zählt zu den führenden deutschen Markenherstellern für innovative, leicht bedienbare und professionelle Sicherheits- und Automationstechnik. LUPUS-Systeme bündeln die Vorzüge von professioneller elektronischer Alarmanlage, Smarthome- und Videoüberwachungstechnik. Das Portfolio umfasst mit über 70 Produkten neben Smarthome-Alarmanlagen und verschiedenen Kameramodellen auch Zubehör, Monitore und Rekorder und eignet sich für den Einbau in Wohnungen, Ein- und Mehrfamilienhäusern, Ladengeschäften, Büroräumen und Industriebetrieben.

Energiesparen mit LUPUS: https://www.lupus-electronics.de/de/energie-sparen

Alarmkamera LE232: https://youtu.be/JY-5W11qjew

IoT-Rauchmelder: https://www.lupus-electronics.de/de/rauchmelder/

Instagram: https://www.instagram.com/lupus_de/

Twitter: https://twitter.com/lupus_de

Facebook: https://www.facebook.com/lupuselectronics

Weiteres Presse- und Bildmaterial steht Ihnen hier zur Verfügung.

Pressekontakt: Kruger Media GmbH – Brand Communication | Torstraße 171 | 10115 Berlin
Carina Hartmann | Telefon: 0177-4697814 | E-Mail: carina.hartmann@kruger-media.de