Wohnen&Leben

Smarthome sicher machen

So schützen Sie Ihr Smarthome gegen Hacker

Foto: iStockphoto/NicoElNino

Einerseits können Smarthome-Anwendungen helfen, das Eigenheim abzusichern. Andererseits sind sie häufig nur schlecht gegen digitale Einbrecher geschützt. Mit unseren einfach umsetzbaren Sicherheitstipps schützen Sie Ihr Zuhause wirksam gegen Hacker.

Warum ist es so wichtig, das Smarthome gegen Hacker zu schützen?

Die meisten Smarthomes sind nur schlecht gegen Hacker geschützt. Einfache Standardpasswörter wie „12345“ sind zwar einfach zu merken, können aber sehr einfach geknackt werden. Dabei ist ein Smarthome-System immer nur so sicher wie das schwächste Glied in der Kette. Bereits ein schlecht gesichertes Gerät im Netzwerk reicht, um zum Einfallstor zum Hacker werden.

Das bedeutet: **Alle Komponenten des Systems müssen sicher sein,** also nicht nur das Gerät selbst, sondern auch die dazugehörigen Smartphone-Apps oder PC-Programme sowie die Cloud des Anbieters.

Denn in einem Smarthome-System sind **verschiedene Haushalts- und Multimediageräte miteinander vernetzt** − lokal oder über das Internet. Vom Nutzer können Sie komfortabel mit einer zentralen Fernsteuerung bedient werden. Die einzelnen Geräte verhalten sich dabei ähnlich wie Computer und kommunizieren untereinander per WLAN oder Bluetooth oder senden Informationen an eine Cloud.

Bei einem Smarthome-System werden Haushalts- und Multimediageräte miteinander verknüpft, um sie komfortabel per zentraler Fernsteuerung zu bedienen. Pixabay

Was passiert bei einem Hackerangriff

Wenn beispielsweise die Überwachungskamera gehackt wird, können die digitalen Eindringlinge mitschauen. Einbrecher sehen, wann die Bewohner das Haus betreten und wieder verlassen. Oder noch bequemer: Per Fernzugriff wird einfach die Haustür geöffnet. Der Nutzer hat dabei kaum eine Chance zu entdecken, ob das Gerät gehackt wurde.

So schützen Sie Ihr Smarthome gegen Hacker

Weiteres Problem: Die Privatsphäre der Bewohner ist nicht mehr sicher. Über gehackte Haushaltsgeräte können **Viren oder Spionageprogramme** eingeschleust werden. Im schlimmsten Fall könnte es passieren, dass plötzlich die Lampen aufflackern und die Bewohner per Einblendung auf dem Smart-TV-Bildschirm zu einer Lösegeldzahlung aufgefordert werden.

Kaufen Sie sichere Geräte

Der Schutz Ihrer Privatsphäre fängt schon beim Kauf an. Erkundigen Sie sich bereits **vor dem Kauf neuer Geräte,** welche Daten von Ihnen gesammelt und wie diese gespeichert werden. Wenn nicht klar ist, was mit Ihren Daten passiert: Finger weg!

AV-Test (Forschungsinstitut für IT-Sicherheit in Deutschland) führt regelmäßig unabhängige Tests von IT- und Sicherheitsprodukten fürs Smarthome durch.

Grundsätzlich gilt: Nutzen Sie ausschließlich Produkte nach DIN VDE V 0826-1 **mit zertifizierter App.** Dies bildet übrigens auch eine Grundlage für die eventuelle Förderung durch die KfW.

Nutzen Sie verschlüsselte Kommunikation

Achten Sie darauf, ob die Geräte eine **verschlüsselte Kommunikation** unterstützen. Wenn die Geräte unverschlüsselt kommunizieren, sind der Nutzername und das Passwort sowie alle Steuerbefehle für den Hacker in Klartext zu sehen - so ist ganz leicht eine komplette Fernsteuerung möglich. Die Verschlüsselung sollte möglichst über HTTPS bzw. TLS erfolgen.

Wenn Sie WLAN nutzen, achten Sie auf den **aktuellsten Verschlüsselungsstandard (WPA2).**

Richten Sie ein sicheres Heimnetzwerk ein

Generell gilt: Setzen Sie möglichst auf **Kabel statt WLAN**. Ein Gerät ohne WLAN-Zugang ist immer sicherer als ein Gerät, das ans Internet angeschlossen ist. Bei einigen Smarthome-Basisstationen lässt sich die Kommunikation mit dem Internet per Schalter einfach deaktivieren.

Viele Router bieten die Möglichkeit, ein **separates WLAN-Netzwerk fürs Smarthome** einzurichten. Das hat einen großen Vorteil: Haben es die Hacker beispielsweise geschafft, über Ihre Wohnzimmerleuchte ins Netzwerk einzudringen, haben sie direkten Zugriff auf alle Geräte, die sich im Netzwerk befinden. Mit einem separaten Netzwerk können Sie das verhindern.

Eine solche Trennung der Netzwerke ist allerdings nicht für alle Smarthome-Geräte möglich und sinnvoll. Wenn sie beispielsweise von Ihrem smarten Fernseher auf Ihre Mediendateien auf dem Rechner zugreifen möchten, müssen sich beide Geräte im selben Netzwerk befinden.

Moderne Router bieten die Möglichkeit, ein Virtuelles Privates Netzwerk (VPN) einzurichten, also eine besonders sichere Verbindung zum Internet. Die Datenpakete werden dabei in ein VPN-Protokoll gelegt und durch einen sicheren „Tunnel“ zugestellt. Foto: Pixabay

Schützen Sie Ihr Heimnetzwerk

Eigentlich eine Selbstverständlichkeit: Installieren Sie eine **Firewall und ein Virenschutzprogramm** und achten Sie darauf, dass dieses permanent aktiviert ist.

Ein anderer häufiger Fehler, obwohl es eigentlich jeder weiß: Verwenden Sie keine Standardpasswörter. Achten Sie darauf, voreingestellte Passwörter sofort durch **eigene, individuelle Passwörter** zu ersetzen. Ein gutes Passwort sollte mindestens acht Zeichen lang sein und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen. Viele Menschen benutzen das einmal überlegte, etwas kompliziertere Passwort für viele verschiedene Programme - das alles macht es Hackern unnötig leicht.

Hier geht's zur Themenübersicht von Wohnen & Leben: **www.wul-infos.de**