„Datensicherheit ist Teamwork“

Hersteller und Nutzer sind gleichermaßen in der Verantwortung

Wie sicher sind Daten in einem intelligent vernetzten Zuhause? Darüber wird in Zusammenhang mit Smart Home immer wieder kontrovers diskutiert. Die Deloitte-Studie „Smart Home Consumer Survey 2018“ zeigt, dass die damit verbundenen Bedenken für etwa ein Drittel der Nichtnutzer sogar der Grund sind, sich gegen smarte Lösungen zu entscheiden. Natürlich lässt sich der Verlust oder ein Diebstahl von Daten nie ganz ausschließen. Dennoch gilt: Wer bestimmte sicherheitstechnische Vorkehrungen trifft, kann die Risiken deutlich minimieren.

Günter Martin
© TÜV Rheinland

Angst vor Wohnungseinbruch und Spionage

Ein Einbrecher, der sich in die Sicherheitsinfrastruktur eines Smart Home hackt, die Bewohner ausspioniert, um den besten Zeitpunkt für die Tat herauszufinden, die smarte Schließanlage der Haustür manipuliert und schließlich ohne große Mühe die Wohnung leerräumt: Ein fiktives Szenario wie dieses verunsichert viele potenzielle Nutzerinnen und Nutzer von Smart Home-Anwendungen. „Die Angst vor Einbrüchen durch Hacker ist groß. Eine solche Vorgehensweise halte ich im Privatbereich – und andere Experten übrigens auch – jedoch für sehr unwahrscheinlich“, betont Günter Martin, Fachmann für Internet- und IT-Sicherheit bei TÜV Rheinland. „Denn es ist viel einfacher, eine Tür aufzubrechen oder ein Fenster aufzuhebeln. Einbrecher machen sich in aller Regel nicht die Mühe, sich in ein Smart Home-System zu hacken. Meistens können sie das auch gar nicht“, stellt er klar. Darüber hinaus besteht bei vielen aber auch die Sorge, dass personenbezogene Daten aufgrund von Sicherheitsmängeln verloren gehen oder in falsche Hände geraten. Denn ein Smart Home sammelt viele Informationen über den Alltag der Bewohner. „Wenn Dritte Zugriff auf solche Daten erhalten, können sie diese auch zweckentfremden. Damit das nicht passiert, ist der effektive Schutz bzw. die Sicherung der Daten wichtig“, weiß der IT-Experte.

Sichere Passwörter und regelmäßige Updates

Hersteller und Nutzer sind gleichermaßen dafür verantwortlich, eine smarte Infrastruktur vor einem Zugriff durch unbefugte Dritte zu schützen. „Datensicherheit im Smart Home ist Teamwork“, erklärt Günter Martin. „Der Nutzer kann nicht viel tun, wenn ein Produkt in punkto Datensicherheit mangelhaft ist. Andersherum kann ein Anbieter noch so viel in die Sicherheitsinfrastruktur investieren, wenn Geräte falsch installiert sind oder der Nutzer die kontinuierliche Absicherung vernachlässigt.“ Das Wichtigste ist, voreingestellte Standardpasswörter zu erneuern und dabei sichere Kombinationen zu wählen. „Einfache Begriffe oder Zahlenreihen wie 1234 sind zwar sehr häufig verwendete Passwörter. Aber die sind nicht sicher!“, mahnt Martin. „Man muss überall da, wo es möglich ist, ein Passwort vergeben, das schwer zu erraten oder zu entschlüsseln ist.“ Das ist besonders wichtig, wenn eine Internetverbindung und somit eine Verbindung nach außen besteht, zum Beispiel über den WLAN-Router oder das Smartphone, über die man sich aus der Ferne mit dem Heimnetzwerk verbindet. Solange die Datenübertragung ausschließlich im internen Netzwerk bleibt, kann es auch Sicherheitslücken geben, führt der Experte aus. „Aber dann müsste ein Täter sehr nah am Gebäude stehen, um sich einzuloggen.“ Günter Martin vergleicht das mit einer Haustür: „Die muss man auch immer richtig abschließen, um Fremde fernzuhalten. Bei Zimmertüren, wie auch bei den Passwörtern von Geräten im internen Netzwerk, die von außen nicht erreichbar sind, ist der Schutz weniger entscheidend.“

Datensicherheit und Datenschutz

Unter Datenschutz versteht man den Schutz vor einem Missbrauch personenbezogener Daten und demnach auch den Schutz der Privatsphäre eines Einzelnen. Anbieter von Smart Home-Lösungen müssen bestimmte gesetzliche Regeln einhalten, wie sie mit Nutzerdaten umgehen dürfen.

Die Datensicherheit, auch Cyber Security, betrifft wiederum das unberechtigte Eindringen in IT-Systeme. Sie schützt somit vor Hacker-Angriffen. Um ein hohes Maß an Datensicherheit zu erreichen, gibt es technische und organisatorische Maßnahmen, die zum Teil gesetzlich vorgeschrieben sind.

Zusätzlich zu sicheren Passwörtern ist es wichtig, die vom Hersteller angebotenen Updates durchzuführen, um entstandene Sicherheitslücken zu schließen. „Ein verantwortungsbewusster Anbieter beobachtet den Markt und reagiert auf Bedrohungen. Cyberkriminelle kommen immer wieder auf neue Ideen. Dem kann man nur mit regelmäßigen Updates etwas entgegensetzen.“

Hersteller unter die Lupe nehmen

Während in punkto Datensicherheit Anbieter und Nutzer naturgemäß an einem Strang ziehen und beide Seiten Hackerangriffe vermeiden

wollen, gibt es beim Datenschutz einen Interessensgegensatz. „Anbieter möchten möglichst viel über ihre Kunden wissen, Nutzer ihre Privatsphäre schützen“, erklärt Günter Martin. So sieht die Europäische Datenschutz-Grundverordnung, kurz DSGVO, unter anderem eine Datenminimierung vor: Personenbezogene Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. „Die Forderung nach Datenminimierung sollte bereits beim Produktentwurf berücksichtigt werden. Das Gerät sollte technisch nur die Daten liefern können, die für den vereinbarten Zweck gebraucht werden und andere Daten erst gar nicht erfassen können. Unsere Praxis zeigt, dass es in diesem Punkt noch Nachholbedarf auf Seiten der Hersteller gibt“, so der TÜV Rheinland-Experte. Besonders kritisch mit Blick auf die DSGVO sieht Günter Martin die teils verwendeten Datenschutzerklärungen. „Die Bearbeitung personenbezogener Daten unterliegt laut DSGVO immer einer Zweckbindung. Häufig sind Einwilligungen aber zu umfassend formuliert und erlauben die Datennutzung zu Zwecken, die mit der eigentlichen Anwendung nichts zu tun haben“, führt Martin aus. Verbraucher sollten in jedem Fall prüfen, ob eine Datenschutzerklärung vorliegt, empfiehlt er. Gemäß DSGVO muss diese in verständlicher Form verfasst sein. „Darin steht dann, was der Hersteller mit meinen Daten macht, beispielsweise ob er sie für Werbezwecke an Dritte weitergibt. Will ich das nicht, sollte ich auf einen anderen Hersteller zurückgreifen.“

Speicherung vor Ort oder in der Cloud

Es gibt zwei Möglichkeiten, wie Daten im Smart Home gespeichert werden: Lokal innerhalb des smarten Netzwerks oder außerhalb in einer Cloud. Was zur Anwendung kommt, hängt meist vom Hersteller beziehungsweise dem System ab. Für sicherer hält Günter Martin die lokale Datenspeicherung. Denn in diesem Fall müsste ein Hacker erst einmal in das Heimnetzwerk eindringen, was bei einer guten Sicherung mittels starker Passwörter schwierig ist. Allerdings muss man dann auch selber für das Datenmanagement sorgen, was eine technische Herausforderung sein kann. Bei Cloud-Diensten ist das meist einfacher, erklärt er: „Dann liegen die Daten zwar außerhalb meines Hauses, was die Gefahr eines Zugriffs durch Dritte erhöht. Die großen Anbieter leisten aber einen guten Service und versuchen alles, um die Daten zu schützen. Es ist meiner Einschätzung nach unwahrscheinlich, dass ein Fremder in das Cloud-Netzwerk eindringen kann.“

Verhalten bei Datendiebstahl

Selbst wenn man alle Sicherheitsmaßnahmen beachtet, besteht immer ein Restrisiko, dass Cyberkriminelle in ein Smart Home-System eindringen und auf persönliche Daten zugreifen. Hat man den geringsten Verdacht, dass es zu einem solchen Vorfall gekommen ist, empfiehlt Günter Martin, sich an die Service-Hotline des Herstellers beziehungsweise des Händlers zu wenden. „Hier sollte man genau schildern, was passiert ist. Ein renommierter Anbieter wird versuchen, mir sofort zu helfen. Meist wird man an einen Experten weitergeleitet.“ Hat der Datendiebstahl Folgen, sollte man in jedem Fall auch die Polizei informieren. „Sie kann schließlich nur tätig werden und ermitteln, wenn sie von solchen Fällen Kenntnis hat. Deshalb ist eine Anzeige sehr wichtig“, betont Martin abschließend. *MW*

Weitere Informationen zu Datensicherheit und Datenschutz finden Sie auf der Internetseite

- **des Bundesamts für Sicherheit in der Informationstechnik unter www.bsi.bund.de und**
- **der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.bfdi.bund.de.**

Auch informieren Hersteller und Anbieter von Smart Home-Systemen auf ihren Webseiten über Datensicherheit und Datenschutz, insbesondere unser Inserent

- **eQ-3 AG Smart Home, www.homematic-ip.de**

Wichtige Sicherheitstipps

- **Nutzen Sie starke Passwörter für alle Smart Home-Komponenten**
  - **Mindestens zehn Zeichen**
  - **Kombination aus Groß-/Kleinbuchstaben, Sonderzeichen und Zahlen**
  - **Keine Begriffe, die man im Wörterbuch findet**
- **Verwenden Sie für jede Anwendung ein anderes Passwort**
- **Nutzen Sie für den Router den aktuellsten Verschlüsselungsstandard (WPA2)**
- **Installieren Sie eine Firewall und ein Virenschutzprogramm**
- **Führen Sie immer alle verfügbaren Software-Updates durch**
- **Lassen Sie die Geräte sich nicht automatisch mit dem Internet verbinden, sondern nur, wenn Sie das wollen bzw. es wirklich notwendig ist**
- **Minimieren Sie die Datenspeicherung auf das Notwendige**
- **Schalten Sie die Geräte möglichst ab, wenn Sie sie nicht benutzen**
- **Achten Sie bei der Nutzung mobiler Endgeräte im öffentlichen Raum darauf, dass niemand Ihre Daten- bzw. Passworteingabe beobachten kann**