Schlaues Haus lockt Kriminelle

SMART HOME: Vernetzte Technologien versprechen Sicherheit und Komfort, aber stattdessen kommen Datenspione und Einbrecher ins Haus.

Einbrecher haben es in vielen digitalen Häusern einfach. Da lassen sich vernetzte Türschlösser knacken, Lichtsysteme und Heizungen manipulieren.

Foto [M]: panthermedia.net/gurZZZa/Helma Spona/VDIn

VON UWE SIEVERS

Niemand saugt gern Staub. Deshalb entwickelt die Industrie Staubsaugroboter. Die fahren durch die Wohnung und sammeln den Dreck ein. Das ist jedoch nicht das Einzige, was sie einsammeln. Damit die Roboter nicht überall gegenfahren, sind sie mit Sensoren ausgestattet. Einige Modelle verfügen zusätzlich über eine Kamera. Mit diesen Kameras entstanden zahlreiche Youtube-Videos, in denen die rollenden Automaten Hunde und Katzen durch die Wohnung scheuchen. Nebenbei fallen auf der Fahrt durch die Zimmer detaillierte Daten über den Grundriss der Wohnung, deren Ausstattung und über Standorte von Möbeln sowie andere Einrichtungsdetails an.

Neugierige Staubsaugroboter

Dass diese Daten auch bei den Herstellern der Roboter landen, ist nicht verwunderlich. Die entdecken inzwischen den Wert der Daten für sich: Der US-Hersteller iRobot plant, von seinen Staubsaugerrobotern zusammengetragene Daten zu versilbern: Informationen über die Lebens- und Wohnverhältnisse der Kunden sollen in Zukunft an Amazon, Apple oder Google verkauft werden, erzählte der Chef des Unternehmens, Colin Angle, der Nachrichtenagentur Reuters.

Auch beim Smart Home geht es also massiv um persönliche Daten. „In der Diskussion über Cybersicherheit für das Smart Home werden die Themen Datenschutz und Privatsphäre vernachlässigt“, bemängelt dann auch Marco Preuß, Leiter des europäischen Forschungs- und Analyseteams beim Anbieter von IT-Sicherheitssoftware Kaspersky.

Digitaler Schlüssel unter digitaler Fußmatte

Allerdings ist es nicht nur um den Datenschutz oftmals schlecht bestellt: Defizite existieren auch bei der IT-Security. Die Anbieter solcher Geräte werben zwar gerade mit erhöhter Sicherheit für die eigenen vier Wände, doch manchmal resultiert daraus das Gegenteil.

Beispielsweise bei smarten Vorhänge- und Türschlössern, die sich per Funk öffnen und schließen lassen. Eigentlich sollten gerade diese Schlösser mehr Sicherheit bringen, doch Hacker des Chaos Computer Clubs (CCC) hatten mit ihnen ein leichtes Spiel: Das Bluetooth-Schloss von Master Lock ließ sich mit einem starken Magneten öffnen. Und selbst das mit zeitgemäßer Kryptografie ausgestattete Modell des Herstellers Noke war nach kurzer Zeit gehackt. Die App, über die das Schloss bedient wird, war so simpel programmiert, dass sich recht leicht der Verschlüsselungscode auslesen ließ, wie ein CCC-Hacker beim letzten Chaos Communication Congress vorführte.

Ähnliches hatten US-Sicherheitsforscher bereits ein halbes Jahr zuvor festgestellt. Von 16 untersuchten Funkschlössern konnten sie zwölf knacken. Schwer war das nicht, denn einige übermittelten die Passwörter unverschlüsselt als Klartext, bei anderen wurde einfach der Datenverkehr mitgeschnitten und erneut abgespielt, also eine sogenannte Replay-Attacke durchgeführt.

Einbrecher müssten sich also nur in Empfangsweite des Schlosses aufhalten, warten, bis es vom Eigentümer geöffnet wird, diesen Funkverkehr mitschneiden und später nach Belieben wiederholen. Der smarte Einbruch macht keinen Krach und erfordert auch keine Gewalt.

Feriendomizile im Visier

Ganz anders geht es Vermietern von Feriendomizilen mit Nummernschlössern eines US-amerikanischen Herstellers. Die digitalen Zugänge wurden zum Problem: Sie bleiben einfach zu.

Die Türschlösser von Lockstate haben ein Tastenfeld, um Codes zum Öffnen einzugeben. Sie können sogar per WLAN programmiert werden. Dadurch sind sie bei Kurzzeitvermietungen und Urlaubsunterkünften beliebt: Statt für jeden neuen Feriengast eine Schlüsselübergabe zu organisieren, wird einfach vom Büro oder Wohnzimmer aus das Türschloss per Funk neu programmiert. Deshalb kooperiert Lockstate sogar mit dem Vermietungsportal Airbnb.

Doch jetzt hat Lockstate mit einem fehlerhaften Firmware-Update seine Smart-Locks lahmgelegt. Sie ließen sich danach nicht mehr per Tastenkombination öffnen, sondern nur noch klassisch mit einem Schlüssel. Betroffene Vermieter oder Eigentümer müssen deshalb die Schlösser ausbauen und einschicken. Wer von Deutschland aus sein Feriendomizil auf Mallorca vermietet, hat nun eventuell nicht nur verärgerte Feriengäste vor verschlossener Tür stehen, sondern auch eine ungeplante Reise vor sich.

Tatort Alarmanlage

Manche verlassen sich nicht allein auf Schlösser, sondern installieren zusätzlich eine Alarmanlage. Doch auch die werden für Einbrecher zunehmend attraktiver: Wie eine Analyse des Computermagazins c‘t schon vor einem Jahr ergab, erlauben verschiedene smarte Anlagen via Internet Zugriff auf Protokoll- und Logdateien und – sofern im Gerät hinterlegt – sogar auf E-Mail-Adressen und Telefonnummern. Dadurch können Kriminelle wertvolle Informationen ermitteln und die Gewohnheiten der Bewohner nachvollziehen. Einige Modelle lassen sich über das Internet ein- und ausschalten – leider auch von Unbefugten: Standardpasswörter wie „1234“ machen das möglich. Damit die Einbrecher anschließend wissen, wo sie hinmüssen, kann der Standort abgefragt werden.

Einige Hersteller gestalten ihre Alarmanlage als Schaltzentrale des smarten Home. Daraus ergeben sich noch ganz andere Möglichkeiten. Alles, was darüber gesteuert werden kann, kann angegriffen beziehungsweise missbraucht werden, ob Heizung, Strom oder Licht.

Angreifbare Heizungen und Lichtsysteme

Ein Beispiel für derartigen Missbrauch lieferte die smarte Beleuchtungsserie Hue von Philips. Die Lampen können mit einer App gesteuert werden, bieten verschiedene Lichtvariationen – ließen sich aber über das Funkprotokoll Zigbee auch mit Malware infizieren. Das hatte ein Team von Sicherheitsspezialisten aus Israel und Kanada im letzten Jahr herausgefunden. Sie gingen so weit, Daten durch schnelles, mit bloßem Auge nicht sichtbares Ein- und Ausschalten in die Außenwelt zu funken. In einem Youtube-Video führten sie die Möglichkeiten vor: Eine Drohne fliegt zu einem mit dem Leuchtenset ausgestatteten Bürogebäude, infiziert die Lampen im Vorbeiflug und lässt sie zur Demonstration im Gleichtakt SOS funken. Youtube-Zuschauer waren begeistert, Besitzer der recht teuren Leuchten eher erschrocken. Doch die Lücke wurde von Philips sofort geschlossen, nachdem die Forscher das Unternehmen informierten.

Router schützen nicht

Um Smart Home zum Erfolg zu führen, müssen die Hersteller in Sachen Sicherheit noch dazulernen. Der Einsatz sicherer Protokolle sollte genauso selbstverständlich werden wie die Implementierung aktueller Kryptoverfahren.

Ferner müssen sie die Rolle der DSL-Router überdenken. Da sich Smart-Home-Komponenten normalerweise im heimischen WLAN befinden, glauben Produzenten ebenso wie Nutzer, durch den Router seien die Geräte gegenüber dem Internet abgeschottet.

Aber „Router sind der am häufigsten genutzte Angriffsweg ins Smart Home“, warnt Marco Preuß von Kaspersky. Der Angriff auf die DSL-Router der Deutschen Telekom Ende letzten Jahres lieferte ein eindrucksvollen Beispiel: Fast 1 Mio. Kunden war für ein bis zwei Tage vom Internet getrennt. Bei vielen war das Telefon stillgelegt, aber auch so mancher Fernseher mit dem Entertain-Dienst. rb