Bad Sodener Erklärung zu Sicherheit im SmartHome und durch SmartHome Techniken

Bad Soden am Taunus, 10. Oktober 2017 | Technische Assistenzsysteme, so genannte SmartHome Technik, finden zunehmend Einsatz in Wohnungen und Häusern. Im Kraftfahrzeug sind solche Systeme längst Standard geworden zur Verbesserung des Komforts, der Sicherheit und zur Reduzierung des Energieverbrauchs. Im Wohnbereich gelten die gleichen Gründe für die Installation von smarter Technik: Energieverbrauch senken, Komfort – besonders für ältere Menschen – erhöhen und Sicherheit verbessern.

Das Thema Sicherheit im SmartHome wird gegenwärtig kontrovers diskutiert. Einerseits kann SmartHome zur Vorbeugung gegen Einbruch beitragen und Feuer oder Überflutung frühzeitig erkennen und melden, andererseits steht die smarte Technik im Verdacht, Bewohner auszuspähen und sogar zu ermöglichen, dass Einbrecher per Internet Wohnungen öffnen.

Im Oktober 2017 wurden während der SmartHome Security Conference in Bad Soden wichtige Aspekte zwischen Experten von Industrie, Verbänden, Behörden, Versicherungswirtschaft und zertifizierenden Instituten diskutiert und die folgenden Statements herausgearbeitet. Diese sollen Bürgern, Medien, Politik und Verwaltung die Fakten aufzeigen und Hinweise für künftige Entscheidungen geben.

Zusammenfassung

- Smarte Häuser und Wohnungen sind – wenn SmartHome Produkte fachgerecht installiert wurden- grundsätzlich sicherer als konventionelle. SmartHome ist dabei eine wertvolle Ergänzung zu mechanischer Sicherungstechnik
- Fälle von Einbrüchen „per Handy“ sind bisher nicht bekannt
- Bei Angriffen auf Smart Home bzw. IoT-Produkte steht aktuell nicht das Eigenheim im Fokus. Stattdessen wird versucht, Geräte und Dienste für andere kriminelle Zwecke zu missbrauchen.
- Der Einsatz von SmartHome-Technik kann vor Sach- und Personenschäden schützen und potentielle Einbrecher abschrecken
- SmartHome braucht nicht zwingend das Internet
- Sichere Router sind eine Grundvoraussetzung für SmartHome mit Internetzugang
- Cloud-Only-Lösungen sind potentiell gefährdet, da sie im Gegensatz zu rein lokalen Lösungen einen zusätzlichen Angriffsvektor bieten und sind gefährlich, da sie nicht über Notlaufeigenschaften verfügen.
- Bestimmte Cloud-Dienste sind gut geeignet, eine sichere Kommunikation zwischen SmartHome Systemen, Bewohnern und Dienstleistern zu gewährleisten.

SmartHome und Einbruch

Es wird behauptet, dass SmartHome-Technik den Einbruch in Wohnungen und Häuser vereinfacht. Einbrecher würden statt Brecheisen das Smartphone verwenden, um Türen spurlos zu öffnen.

In Deutschland ist bisher kein einziger Fall bekannt, bei dem Einbrecher sich smarter Technik bedient hätten, um sich so Zugang zu Wohnungen und Häusern zu verschaffen. Es lassen sich jedoch elektronisch betätigte Türen falsch konfigurieren mit der Folge, dass sich bei Kenntnis dieses Sachverhalts Türen aus der Ferne öffnen lassen. Eine ordnungsgemäße, fachgerechte Installation qualitativ hochwertiger Produkte verhindert dies jedoch zuverlässig.

SmartHome Systeme verfügen meist über eine so genannte Anwesenheitssimulation. Das heißt, das System spielt einem äußeren Betrachter beispielsweise durch Rollläden und Licht ein bewohntes Haus vor. Einbrecher suchen vorzugsweise Häuser, bei denen eine Anwesenheit von Bewohnern nicht festzustellen ist.

Kameras, die sichtbar am Gebäude montiert sind, können potentielle Einbrecher abschrecken. Ist ein Einbruch erfolgt, können vorhandene Kameras durch Videodokumentation, der Polizei helfen, die Täter zu identifizieren.

Eine weitere Schutzmaßnahme sind Sensoren an Türen und Fenstern. Es gibt Sensoren, die das Öffnen von Fenstern oder auch schon das Hantieren an den Fenstern erkennen und melden. Ein smartes Haus kann sich dadurch wehren, dass es beispielsweise die Rollläden herunterfährt, Licht einschaltet, Lärm erzeugt und den Einbruchsversuch per Telekommunikation meldet.

Die herkömmlichen Brand- und Einbruchmeldeanlagen, zertifiziert nach DIN, EN oder VdS, werden vielfach gesetzlich oder vom Versicherer gefordert. Bei Smart Home-Produkten ist der Wunsch des Privatanwenders nach Schutz und Komfort die Triebfeder. Sie bieten dann eine Alternative, wenn vom Versicherer keine Maßnahmen gefordert werden und dennoch ein gewisser Schutz erreicht werden soll.

Sollen IoT- / Smart Home-Geräte auch sicherheitstechnische Funktionen übernehmen (z.B. Einbruchmeldung, Brandmeldung), müssen die Geräte daher den geltenden Normen entsprechen und entsprechend zertifiziert und geprüft sein. Andernfalls sind deutlich die Unterschiede zu benennen, damit sich Käufer ein objektives Bild von den Eigenschaften und der Leistungsfähigkeit der Produkte im Vergleich zu entsprechenden, zertifizierten und geprüften Produkten machen können. Orientierung für Endverbraucher bieten hier Tests und Zertifizierungen unabhängiger Testinstitute. Der Einbau soll Fachbetrieben vorbehalten sein. Do-it-yourself ist nicht empfehlenswert, damit die hohe Produktqualität nicht durch falschen Einbau konterkariert wird.

Bürgerrelevanz ■■■■□
Handlungsbedarf Industrie ■■■□□
Handlungsbedarf Handel / Handwerk ■■■□□
Handlungsbedarf Politik ■■□□□

SmartHome und Schutz vor Sach- und Personenschäden

Einige SmartHome Systeme sind dank spezieller Sensoren in der Lage, bestimmte Gefahrensituationen bereits in der Entstehung zu erkennen und zu melden. Dazu gehören Brandmelder (Heimrauchmelder), Wasserleckage-, Überflutungs-, Gasleckage-, CO- und CO2-Melder. Solche Sensoren melden Abweichungen vom Normalzustand an das verbundene SmartHome-System und dieses alarmiert durch Geräusch, Sprachansagen oder per Telekommunikation. Für kritische Gefahren sollte die Aufschaltung auf eine zertifizierte Notruf- und Service-Leitstelle auf Grundlage der entsprechenden Normen favorisiert werden.

Gleichzeitig lassen sich Gas- oder Wasser-Leitungen zusperren. Ein SmartHome System kann allerdings auch Fluchtwege eröffnen und Orientierung geben, beispielsweise durch das Hochfahren von Rollläden und das Einschalten von Beleuchtung. SmartHome Technik kann so dabei helfen, Schäden frühzeitig zu erkennen, zu begrenzen und Leben zu retten. Eine Gefahr für die Bewohner geht von dieser Technik nicht aus. Allerdings könnten minderwertige oder falsch installierte Systeme massenhaft Fehlalarme auszulösen und anfällig für Cyberangriffe sein.

Bürgerrelevanz ■■■■□
Handlungsbedarf Industrie ■■■■■
Handlungsbedarf Handel / Handwerk ■■■□□
Handlungsbedarf Politik ■■□□□

SmartHome und das Internet

SmartHome und Internet sind nicht zwingend voneinander abhängig. Ein SmartHome funktioniert grundsätzlich auch ohne das Internet. Das Internet ist nur dann notwendig, wenn Meldungen an Empfänger außerhalb des SmartHomes gesandt werden, oder Anweisungen von außerhalb durch das SmartHome empfangen werden sollen. In der Regel wird man auf diese Fernbedienbarkeit nicht verzichten wollen. Dazu muss das SmartHome System mit dem Netzwerk (LAN) in Haus oder Wohnung verbunden werden. Das Bindeglied zwischen dem Netzwerk im Haus und dem Internet ist der Router. Diesen gilt es, so zu konfigurieren, dass das häusliche Netzwerk sicher gegen Eindringversuche aus dem Internet ist. Dies gilt unabhängig von der SmartHome-Installation. In aller Regel werden Router durch die Bewohner selbst installiert, die nicht über das notwendige Fachwissen verfügen, eine sichere Konfiguration herzustellen. Wir begrüßen deshalb ausdrücklich die Initiative „Router-TR“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Hier entsteht zusammen mit der Industrie und den Verbänden eine Technische Richtlinie (TR) die den Auslieferzustand von Consumer-Routern festlegt. Demnach werden Router werksseitig entsprechend sicher ausgeliefert. Nutzer müssen zwar bestimmte Eingaben vornehmen, sicherheitsrelevante Einstellungen können allerdings nur bewusst verändert werden. Auch das wichtige Thema der sicherheitsrelevanten Updates wird in der TR geregelt. Somit kann künftig davon ausgegangen werden, dass die empfindliche Schnittstelle zwischen dem privaten Netzwerk zu Hause und dem öffentlichen Internet weitgehend sicher ist und sicher gehalten wird.

Zusätzlich gilt es, auch andere Geräte, etwa mobile Endgeräte, PCs und andere Geräte, die eine Verbindung mit dem Internet, dem Heimnetzwerk sowie Smart Home-Geräte herstellen, entsprechend abzusichern.

Käufer müssen die Möglichkeit haben, die Netzwerkfunktionen von IoT- und Smart Home-Geräten jederzeit mit einfachen Mitteln zu deaktivieren. Geräte, die grundsätzlich ohne die Netzwerkfunktionalität nutzbar sind, müssen auch ohne diese in einem „Stand-Alone-Mode“ weiter ihren Dienst verrichten (Beispiele: Kühlschrank, Waschmaschine, Kaffeevollautomat).

Bürgerrelevanz ■■■■□
Handlungsbedarf Industrie ■■■■■
Handlungsbedarf Handel / Handwerk ■■■■■
Handlungsbedarf Politik ■■■■■

Cloud-Only SmartHome

SmartHome als Cloud-Only-Lösung, also ohne lokalen SmartHome Controller, ist von der ständigen Verfügbarkeit des Internets abhängig. Sensoren melden ihre gemessenen Werte direkt über das lokale Netzwerk, den Router und das Internet an einen Cloud-Server. Dort sind die Regeln gespeichert, nach denen die Sensorwerte zu Aktor-Reaktionen im Haus führen sollen. Problematisch ist, dass bei Ausfall des Internets Sensorwerte nicht gesendet und Aktorbefehle nicht empfangen werden können. Kritisch ist auch zu sehen, dass es oftmals unklar ist, ob die Sensordaten aus der Wohnung anders als zum eigentlichen Zweck, nämlich der Abarbeitung der Regeln und Steuerung der Aktoren, verwendet werden.

Ähnlich verhält es sich mit IoT-Produkten (Internet of Things), beispielsweise besonders leicht zu installierende Netzwerkkameras. Diese Kameras suchen und finden aus dem privaten lokalen Netzwerk den Weg zu ihrem Heimatserver irgendwo in der weltweiten Cloud. Sie übertragen Fotos, Videos, ggf. Sprache und sogar gesammelte Daten aus dem Router an den Cloudserver. Per Internetbrowser oder Smartphone App kann der Nutzer die Videos, die sich in der Cloud befinden, sehen. Diese meist sehr preisgünstigen Produkte stellen ein potentielles Sicherheitsrisiko dar.

Arbeiten IoT- / Smart Home-Geräte mit Cloud-Anbindung, muss der Anbieter auf dem Produkt bzw. in der Anleitung Auskunft darüber geben, wo sich das Cloud-Rechenzentrum befindet und durch welchen Rechtsraum die Daten übermittelt werden.

Da häufig die Speicherung der Cloud-Daten nicht nach deutschem Recht erfolgt, ist eine rechtliche Überprüfung sehr schwierig bzw. aussichtslos. Wir raten deshalb von Cloud-Only-Lösungen jeglicher Art ab. Bei Geräten, die qua Funktionsweise auf den Datenaustausch mit Clouddiensten über das Internet angewiesen sind, ist der Nachweis entsprechender Schutzfunktionen sowie die Einhaltung von Datenschutzbestimmungen über entsprechende Test- bzw. Gütesiegel oder Zertifikate empfehlenswert.

Bürgerrelevanz ■■■■□
Handlungsbedarf Industrie ■■■■■
Handlungsbedarf Handel / Handwerk ■■■■■
Handlungsbedarf Politik ■■■□□

SmartHome und Cybercrime

Die Internetkriminalität macht auch vor dem SmartHome nicht halt. Zwar spielt sie hier bisher eine untergeordnete Rolle, dies könnte sich jedoch ändern. Denkbar wäre das Eindringen in das SmartHome System, die Verschlüsselung des Systems und Entschlüsselung gegen die Zahlung eines Lösegeldes. Mit einem sicher konfigurierten Router und regelmäßigen Sicherheitsupdates wird die Wahrscheinlichkeit hierfür verringert. Sollte die Übernahme eines SmartHome Systems dennoch gelingen, ließe sich das gekaperte System leicht wiederherstellen.

Gefährlicher wäre die heimliche Übernahme und die potentielle Nutzung von tausenden von Systemen (Botnet) für Denial of Service Attacken beispielsweise gegen Industrie- und Regierungs-Netzwerke. Dies ist verschiedentlich bei primitiven SmartHome Geräten (Internet of Things) wie vernetzten Haushaltsgeräten gelungen. Die Fehler sind bekannt und müssen durch die Hersteller abgestellt werden. Unsichere Geräte dürfen nicht in Verkehr gebracht werden. Hersteller müssen ihre IoT- und Smart Home-Geräte Penetrationstests unterziehen. Die Ergebnisse dieser Tests sind durch die Hersteller in aggregierter Form zu veröffentlichen. Darum unterstützt und empfiehlt die SmartHome Initiative bereits im Markt bewährte Sicherheitszertifikate unabhängiger Testinstitute wie die des VdS, des TÜV Rheinland oder des AV-TEST Institutes.

Sicherheitsupdates müssen automatisch auf die Geräte erfolgen. Das heißt, vernetzbare Geräte müssen über das Netzwerk updatebar sein. Weiterhin muss es eine einfache Möglichkeit geben, dem Hersteller erkannte Sicherheitslücken zu melden. Gleichzeitig verpflichten sich die Hersteller, den Verbraucher unverzüglich und umfassend über erkannte Sicherheitslücken zu informieren und ggf. geeignete Rückrufprozesse einzurichten. Sie müssen angemessene und wirksame Maßnahmen zum Notfallmanagement treffen und vorhalten.

Bürgerrelevanz ■■■■□
Handlungsbedarf Industrie ■■■■■
Handlungsbedarf Handel / Handwerk □□□□□
Handlungsbedarf Politik ■■■■■

Alarmierung und Back-Up per Cloud-Dienst

Entdeckt ein SmartHome System eine Unregelmäßigkeit, beispielsweise den Ausfall der Tiefkühltruhe, der Heizung oder einen Einbruchsversuch, soll es die Bewohner bzw. Eigentümer oder einen Dienstleister unverzüglich, nachvollziehbar und sicher informieren. Als technisch gut geeigneten Weg haben sich bestimmte gesicherte Cloud-Dienste herausgestellt. Sie bieten Ende zu Ende Verschlüsslung und garantieren die Zustellung der Nachrichten sogar bei stumm-geschaltetem Smartphone innerhalb weniger Sekunden. Klassische Medien wie SMS und E-Mail können dies alles nicht bieten und sind für die Alarmierung deshalb nicht zu empfehlen.

Speichert ein SmartHome System Daten und Regeln, so sollen diese regelmäßig und automatisch gesichert werden, um bei Ausfall der Hardware schnell und fehlerfrei ein Recovery durchführen zu können. Dazu empfiehlt sich, die notwendigen Daten individuell verschlüsselt auf einen gesicherten Cloudserver auszulagern.

Support und Supportzeitraum

Hersteller und beauftragte Betreiber verpflichten sich, die IoT- und SmartHom-Produkte für einen Mindestzeitraum mit sicherheitsrelevanten Updates zu bedienen. In diesem Zusammenhang wird selbstverständlich erwartet, dass sämtliche sonstigen Hersteller- und Betreiberpflichten (u. a. nach dem Produktsicherheitsgesetz, den gesetzlichen nationalen Datenschutzanforderungen, dem Produkthaftungsgesetz etc.) erfüllt werden. Der Mindestzeitraum für den Support von IoT-Geräten sollte sich nach der durchschnittlichen Nutzungsdauer der Geräte richten. Hersteller und beauftragte Betreiber verpflichten sich, ihre Produkte in diesem Zeitraum zu beobachten und bekannte Sicherheitslücken umgehend zu schließen. Bei SmartHome-Produkten, die fest mit dem Gebäude verbunden werden (z.B. IP-fähige Kameras und Gegensprechanlagen) sollte der Support für mindestens 10 Jahre gewährleistet sein. Für den Nutzer muss erkenntlich sein, wie lange ein Gerät vom Hersteller mit Updates versorgt oder Support bereitgestellt wird. Hier wird empfohlen, die Geräte und den Verkaufskarton mit einem Aufdruck zu versehen.

Bürgerrelevanz ■■■■■■
Handlungsbedarf Industrie ■■■■■■
Handlungsbedarf Handel / Handwerk ■■■■■■
Handlungsbedarf Politik ■■■■■■

Die Unterzeichner