Positionspapier

des Gesamtverbandes der Deutschen Versicherungswirtschaft

zu den Anforderungen an Smart Home Installationen sowie Geräten des „Internet der Dinge“

Einleitung

Die Ausstattung von Alltagsgegenständen mit Netzwerkfunktionalität (IoT) schreitet weiter voran. Zugleich drängen zahlreiche Anbieter in den Markt für intelligente Gebäudetechnik. Die Cybersicherheit dieser Produkte ist in vielen Fällen fraglich. Dies hat nicht nur Auswirkungen für die Käufer unsicherer Produkte, sondern auch für Dritte: Am Beispiel des Mirai-Botnetzes wurde deutlich, wie leicht sich IoT-Geräte als Angriffsvehikel nutzen lassen – beispielsweise für DDoS-Attacken.

Die Anbieter von IoT- / Smart Home-Produkten zu verpflichten, „sichere“ Geräte anzubieten, wird die Vulnerabilität der Geräte nicht signifikant senken. Hierfür gibt es einen wesentlichen Grund: Schon die Steuersoftware einfacher IoT-Geräte ist so umfangreich, dass kein Beweis im engeren Sinne erbracht werden kann, dass das Programm fehlerfrei ist. „Sicher“ im engeren Sinne ist daher kein Gerät. Weiterhin ist Sicherheit nicht statisch, da sich Risiken mit dem technologischen Fortschritt auch weiterentwickeln.

Statt die Hersteller also auf „sichere“ Produkte zu verpflichten, muss vielmehr ein Weg eingeschlagen werden, auf dem Hersteller ihre Produkte auch nach dem Verkauf beobachten und sie im durchschnittlichen Nutzungszeitraum in Bezug auf die Cybersicherheit weiter pflegen („Support“). Dies ist gegenwertig nicht selbstverständlich. Denn viele IoT- und Smart Home-Produkte werden in einer Preisklasse angeboten, die es dem

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5350
Fax: +49 30 2020-6350

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39
ID-Nummer 6437280268-55

Ansprechpartner:
Oliver Hauner
Sach- und Technische Versicherung, Schadenverhütung, Statistik

E-Mail: o.hauner@gdv.de

www.gdv.de

Zertifikat seit 2014 audit berufundfamilie

Hersteller schwer macht, große Summen für die Softwareentwicklung auszugeben, geschweige denn, den Support inkl. Fehlerbereinigungen („Bugfixes“, „Patches“) für viele Jahre zu gewährleisten.

Wenn die Risiken dieser Geräte aber auf Dauer tragfähig sein sollen, müssen sich Produkt- und Supportphilosophie grundlegend ändern. Daher werden von der Versicherungswirtschaft an die Gerätekategorie „Smart Home“ bzw. „Internet der Dinge“ folgende Anforderungen gestellt:

Anforderungskatalog

Support

Hersteller müssen sich verpflichten, die IoT und Smart Home Produkte für einen Mindestzeitraum mit sicherheitsrelevanten Updates zu bedienen.
In diesem Zusammenhang wird selbstverständlich erwartet, dass sämtliche sonstigen Herstellerpflichten (u. a. nach dem Produktsicherheitsgesetz, dem Produkthaftungsgesetz etc.) erfüllt werden.

Supportzeitraum

Der Mindestzeitraum für den Support von IoT-Geräten sollte sich nach der durchschnittlichen Nutzungsdauer der Geräte richten. Hersteller müssen sich verpflichten, ihre Produkte in diesem Zeitraum zu beobachten und bekannte Sicherheitslücken umgehend zu schließen.
Bei Smart Home-Produkten, die fest mit dem Gebäude verbunden werden (z.B. IP-fähige Kameras und Gegensprechanlagen) sollte der Support für mindestens 10 Jahre gewährleistet sein.

Kennzeichnung des Supportzeitraums

Für den Nutzer muss erkenntlich sein, wie lange ein Gerät vom Hersteller mit Updates versorgt oder Support bereitgestellt wird. Hier wird empfohlen, die Geräte mit einem Aufdruck zu versehen.

Sicherheitsrelevante Updates

Sicherheitsupdates müssen automatisch auf die Geräte geladen werden. Weiterhin muss es eine einfache Möglichkeit geben, dem Hersteller erkannte Sicherheitslücken zu melden. Gleichzeitig verpflichten die Hersteller sich, den Verbraucher unverzüglich und umfassend über erkannte Sicherheitslücken zu informieren und ggf. geeignete Rückrufprozesse einrichten. Sie müssen angemessene und wirksame Maßnahmen zum Notfallmanagement treffen und vorhalten (Business / IT Service Continuity sowie Disaster Recovery).

Externe Absicherung

Hersteller von IoT- / Smart Home-Produkten müssen ihren Kunden die Möglichkeit bieten, diese nachträglich auch durch Produkte von Drittanbietern abzusichern.

„Offlinefunktion“

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

Zugangssicherung

Setzt ein Hersteller Verschlüsselungsmechanismen ein, so sind diese zu benennen und deren sichere Implementierung durch eine Prüf- und Zertifizierungsstelle zu belegen. Zugangssicherungen z.B. durch Passwörter müssen definierte Mindeststandards erfüllen. Beispielsweise:

- Passwörter dürfen nicht regelhaft vorhersagbar sein
- Verpflichtende Änderung von Standardpasswörtern

Penetrationstests für sicherheitsrelevante IoT-Produkte

Hersteller sollten Ihre IoT- und Smart Home-Geräte Penetrationstests unterziehen müssen. Die Ergebnisse der Pentests sind durch die Hersteller in aggregierter Form zu veröffentlichen.

Cloud

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

Datenschutz

Die Hersteller verpflichten sich, die geltenden Datenschutzbestimmungen zu beachten, ggf. in einem eigenen Verhaltenskodex. Es muss Transparenz darüber geschaffen werden, welche Daten für welchen Zweck wohin übermittelt werden und wie lange sie wo gespeichert werden.

Neutrale Zertifizierung

Zukünftig muss es eine Standardisierung hinsichtlich der Datensicherheit und der Qualität der Installation mit den o.g. Kernforderungen geben. Als transparenzschaffende Begleitung für die Kaufentscheidung der Verbraucher ist daher eine neutrale Zertifizierung oder ein „Produktsiegel" nach vorher festgelegten und normierten technischen Mindeststandards für die Sicherheit von IoT- und Smart Home-Produkten erforderlich. Eine entsprechende Kennzeichnung der Geräte schafft zudem eine hinreichende Orientierungshilfe im Markt.

Sollen IoT- / Smart Home-Geräte auch sicherheitstechnische Funktionen übernehmen (z.B. Einbruchmeldung, Brandmeldung), müssen die Geräte den geltenden Normen entsprechen und entsprechend zertifiziert sein. Andernfalls sind deutlich die Unterschiede zu benennen, damit sich der Käufer ein objektives Bild von den Eigenschaften und der Leistungsfähigkeit der Produkte im Vergleich zu entsprechenden, zertifizierten Produkten machen kann.

Es darf keine Scheinsicherheit entstehen.

Berlin, den 29.05.2017