Verbraucherzentrale Bundesverband e.V. : Hintergrundpapier zum Thema Smart Home

- Das Zuhause der Zukunft: Wie digital werden wir wohnen? -

Im Hintergrundpapier zum Thema Start Home informiert die Verbraucherzentrale Bundesverband e.V. (kurz vzbv) über diverse Mängel im Verbraucherschutz, der IT-Sicherheit und des Datenschutzes bezüglich Smart Homes. Zunächst wird eine Definition von „Smart Home“ gegeben und gesagt, dass viele Kunde, die bereits wissen worum es sich bei Smart Home Geräten handelt, über eine Anschaffung nachdenken und der Thematik sehr offen und interessiert gegenüber stehen. Gleichzeitig warnt die Verbraucherzentrale aber auch vor einem noch sehr unreguliertem Markt für Start Home Geräte. „Teilweise sind die Preise für den versprochenen Zusatznutzen deutlich zu hoch. Zum anderen bringen die neuen Systeme auch neue Herausforderungen für Haftung, Gewährleistung, Kompatibilität, IT-Sicherheit, Datensicherheit und Datenschutz.“, so die Verbraucherzentrale.
Im Weiteren wird auf die Produkthaftung und das Vertragsrecht eingegangen. Da „smarte“ Geräte nicht nur Befehle vom Eigentümer sondern auch von Dritten entgegen nehmen können, bzw. zum teil autonom Handeln, ist nicht immer nachvollziehbar wer eine bestimmte Anweisung gab. Dies führt, laut Verbraucherzentrale dazu, dass Vertragsbeziehungen unklar werden und dementsprechend die Haftung keinem bestimmtem Vertragspartner zugeordnet werden kann. Weitere Haftungslücken werden dem Kunden aufgezeigt und die Verbraucherzentrale Bundesverband e.V. fordert eine „umfassende Prüfung des gesetzlichen Rahmens für Smart Home-Produkte und Anwendungen. Der Fokus sollte dabei auf der Identifizierung von Haftungslücken im Vertragsrecht (Gewährleistung) und außervertraglichen Be-reich (Delikts- und Produkthaftungsrecht) liegen.“ Auch EU-Richtlinien für digitale Inhalte sollten Start Homes mit einbeziehen, sodass „Verbraucher im Zu-hause der Zukunft auch genauso abgesichert sind wie heute.“
Im Hinblick auf Datenschutz und -sicherheit äußert sich die Verbraucherzentrale eher allgemein und gibt an, dass viele Softwareentwickler für Smart Homes sehr wenig Wert auf die Sicherheit solcher Anwendungen legen. Dabei wird sich auf eine Studie der EU Kommission berufen[1].
Smart Homes benötigen sicherheitstechnische Mindestanforderungen wie beispielsweise individuelle Passwörter für jedes Gerät oder die Verschlüsselung personenbezogener Daten, so die vzbv. Demnach sollte die Sicherheit auch bei den Herstellern einen wesentlich größeren Stellenwert bekommen und eine Befolgung der Vorgaben der Datenschutzgrundverordnung[2] muss selbstverständlich sein.

Verbraucherzentrale Bundesverband e.V.: Hintergrundpapier zum Thema Smart Home, 2017

---

[1] European Commission: Smart Grid Laboratories Inventory 2016, 2016, S. 59, Joint Research Centre: Brüssel.

[2] Datenschutz-Grundverordnung DSGVO, https://dsgvo-gesetz.de 2017

IoT Privacy and Security Challenges for Smart Home Environments

Die Autoren benennen im Abschnitt „ Security Threats in the Smart Home“ drei Arten von Sicherheitsbedrohungen in Smart Homes. Vertraulichkeitsbedrohungen umfasse jegliche ungewollte Preisgabe von Informationen, egal ob Daten zum Benutzer oder nur Messdaten von Thermometern oder ähnlichem. Selbst scheinbar harmlose Daten können dazu verwendet werden um beispielsweise zu erkennen ob und wann sich Personen im Haus befinden. Eine weitere Form der Bedrohung seien Authentifizierungsbedrohungen. Diese können dazu führen dass Fremde Zugriff auf persönliche Daten bekommen oder Steuerinformationen manipulieren können. Die dritte und größte Bedrohung, so Lin und Bergmann, sind Zugriffsbedrohungen durch welche Angreifer vollen Zugriff auf Smart Home Geräte oder das gesamte Netzwerk erlangen und dadurch das komplette Smart Home manipulierten oder lahmlegen können. Im weiteren Abschnitt werden noch daraus resultierende Angriffsmöglichkeiten, sowie Beispiele von Angriffen genannt.

Huichen Lin, Neil Bergmann; *IoT Privacy and Security Challenges for Smart Home Environments, 06.2016*