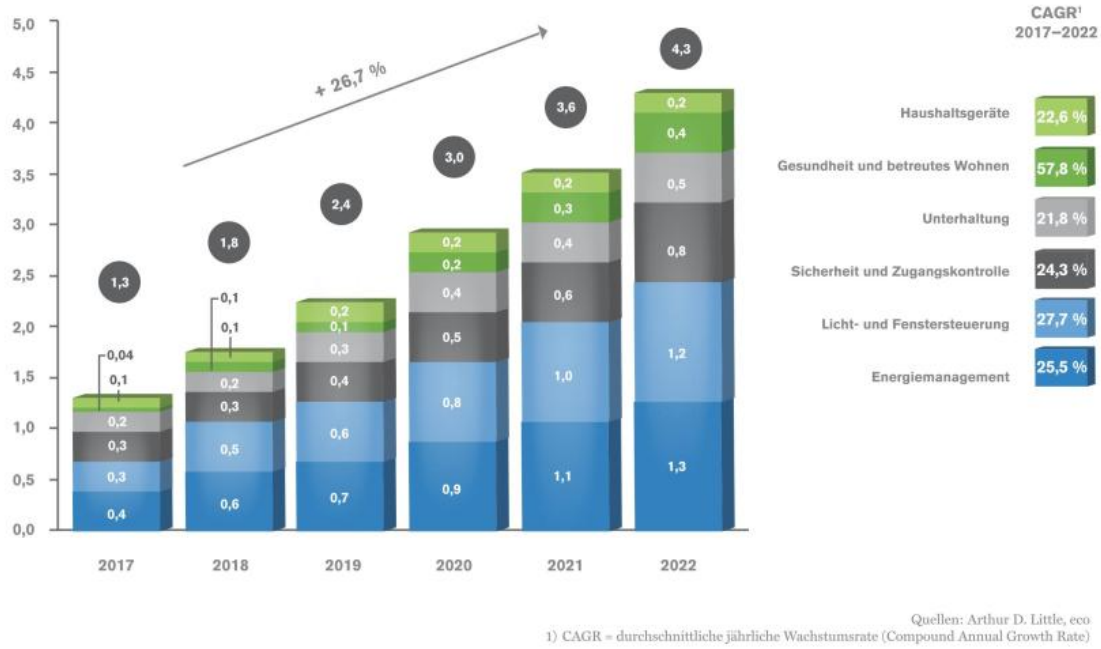
Das smarte Home Office: Gefahr für den Datenschutz?

Smart Home klingt nach Vernetzung im Privathaushalt. In Wirklichkeit aber bringt Smart Home auch Risiken für betriebliche Daten mit sich. Höchste Zeit, sich zu informieren.

Smart Home: Bald auch bei Ihnen daheim?

Der deutsche Smart-Home-Markt boomt und wird sich bis 2022 auf 4,3 Milliarden Euro verdreifachen, so die Studie „Der deutsche Smart-Home-Markt 20172022. Zahlen und Fakten“ des Verbands der Internetwirtschaft (eco) anlässlich der Internationalen Funkausstellung (IFA) 2017 in Berlin.



Quellen: Arthur D. Little, eco
1) CAGR = durchschnittliche jährliche Wachstumsrate (Compound Annual Growth Rate)

Viele Neuheiten auf der IFA drehten sich um das vernetzte Zuhause. Für das hohe Interesse an Smart Home und die Vielfalt an neuen Angeboten gibt es gute Gründe: Die Vernetzung von Waschmaschine, Fernseher oder Heizung sorgt für mehr Komfort im Alltag und kann zudem zu Energieeinsparungen führen, wie das BSI (Bundesamt für Sicherheit in der Informationstechnik) ausführt.

Bequem, aber nicht ohne Risiko

Doch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt: Smart-Home-Geräte werden per Software gesteuert und können über das Internet mit der Außenwelt und untereinander vernetzt werden. Gerade das bringt neue Risiken mit sich, die Nutzer im Blick haben sollten.
https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/willkommen_im_sicheren_smart_home.html

Auch die Aufsichtsbehörden für den Datenschutz und die Verbraucherschützer machen auf die Risiken aufmerksam. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz, Prof. Dr. Kugelmann, zum Beispiel sagte: „Es wird zunehmend deutlich, dass in einer digitalisierten Umwelt vermeintlich belanglose technische Daten wie zum Beispiel die Verbrauchswerte der Heizung geeignet sind, Dritten tiefe Einblicke in den Lebensalltag Einzelner zu verschaffen."

Smart Home: keine reine Privatsache

Nun scheinen diese Datenrisiken nur den Privathaushalt zu betreffen, also kein Problem für den betrieblichen Datenschutz zu sein. Dem ist aber nicht so: Durch die Nutzung privater Geräte zu betrieblichen Zwecken (BYOD = Bring Your Own Device), die private Nutzung betrieblicher Geräte und durch Telearbeit kommt es dazu, dass Firmengeräte oder betrieblich genutzte Geräte in das Smart Home eingebunden werden. Damit werden die Smart-Home-Risiken plötzlich zu Unternehmensrisiken.

Wer ein Smart Home hat und darin ein Home Office betreibt, verzichtet meist darauf, für das Home Office ein eigenes, getrenntes Netzwerk zu betreiben. Stattdessen arbeiten die vernetzte Heizung des Hauses und der Drucker im Home Office im gleichen Netzwerk. Die App zur Steuerung des Smart Home läuft auf dem gleichen Smartphone wie die betrieblichen Apps. Es ist deshalb entscheidend, dass die Datensicherheit im Smart Home stimmt – für den privaten Nutzer und für das betroffene Unternehmen.

Smart Home braucht mehr Datenschutz, auch aus Unternehmenssicht

Wie eine Studie des Digitalverbands Bitkom ergab, wünschen sich die Smart-Home-Nutzer und -Interessenten mehr Sicherheit: So sagen 92 Prozent derjenigen, die bereits Smart-Home-Anwendungen besitzen, dass ihnen unabhängige Zertifikate und Siegel zur Sicherheit vor Hacker-Angriffen sehr oder eher wichtig sind. Einen vom Hersteller garantierten Schutz vor Hacker-Angriffen finden 89 Prozent wichtig.

Auch Datenschutz spielt eine große Rolle beim Kauf. So sagen 84 Prozent, dass ihnen ein hoher Datenschutzstandard wichtig ist, ein unabhängiges Siegel dafür wäre für 79 Prozent ein wichtiges Kaufargument. Zwei Drittel (68 Prozent) achten beim Kauf außerdem darauf, dass die Smart-Home-Daten nur in Deutschland gespeichert werden.

Diese Forderungen an Smart Home werden auch den Unternehmen im Datenschutz helfen. Achten Sie deshalb auf sichere Smart-Home-Lösungen, für sich selbst und für den betrieblichen Datenschutz!

Eine Beitrag von Georg Baumann, TÜV-zertifizierter Datenschutzbeauftragter und Datenschutzauditor/Dozent für Datenschutz und IT-Recht und Experte der AKADEMIE ZUKUNFT HANDWERK