

8 Schritte für optimale Sicherheit im Smart Home

Safer Internet Day 2017

- 1.** Bereits bei der Auswahl des Produktes sollte neben dem Preis-Leistungsverhältnis die IT-Sicherheit eine kaufentscheidende Rolle spielen. Entscheiden Sie sich für vertrauenswürdige Anbieter, die auch Support für die Einrichtung und den Betrieb des Produktes anbieten.
- 2.** Erkundigen Sie sich beim Kauf des Produktes über den Umfang und die Länge der Updategarantie (End Of Service (EOS)). Betreiben Sie das Produkt nicht über diesen Zeitrahmen hinaus.
- 3.** Stellen Sie sicher, dass das Produkt aktuelle Sicherheitsfunktionen anbietet (wie beispielsweise eine passwortgeschützte Administrationsoberfläche und verschlüsselte Informations- und Datenübertragung).
- 4.** Folgen Sie den Installationsanweisungen des Produktes, informieren Sie sich ausführlich in der Betriebsanleitung über spezifische Sicherheitskonfigurationen.
- 5.** Voreingestellte Passwörter sollten durch hinreichend starke, selbstgewählte Passwörter ersetzt werden. Verwenden Sie dazu ein komplexes Passwort, welches nur für diesen Dienst genutzt wird. Passwort-Manager unterstützen bei der Generierung sicherer Passwörter und verwalten diese.
- 6.** Aktivieren Sie nur solche Dienste und Funktionen, die sie für Ihren persönlichen Einsatz des Gerätes benötigen.
- 7.** Verwenden mehrere Benutzer dasselbe Gerät, ist die Einrichtung unterschiedlicher Nutzerprofile mit den jeweils notwendigen Rechten sinnvoll. Auf diese Weise wird sichergestellt, dass nur befugte Anwender beispielsweise Einkäufe tätigen oder Sicherheitskonfigurationen verändern können.
- 8.** Während des Betriebes des Gerätes sollte regelmäßig überprüft werden, ob neue Updates/Patches zur Installation zur Verfügung stehen. Eine zeitnahe Installation schließt etwaige Sicherheitslücken.

Ihre Ansprechpartner



Marc Fliehe, CISSP
Bereichsleiter
Information Security
T 030 27576-242
m.fliehe@bitkom.org



Christian Kulick
Bereichsleiter
Smart Home & Smart City
T 030 27576-115
c.kulick@bitkom.org