Weiterführende Links

- Bundesamt für Sicherheit in der Informationstechnik BSI
  https://www.bsi-fuer-buerger.de
- Landeskriminalamt Nordrhein-Westfalen –
  Empfehlung zur Sicherung digitaler Hautechnik
  http://www.polizei.nrw.de/media/Dokumente/Behoerden/LKA/140811_LKA_SmartHome_Empfehlungen.pdf

ZVEI
Die Elektroindustrie

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Elektroinstallationssysteme
Lyoner Straße 9
60528 Frankfurt am Main

Ansprechpartner:
Dr. Arnaud Hoffmann

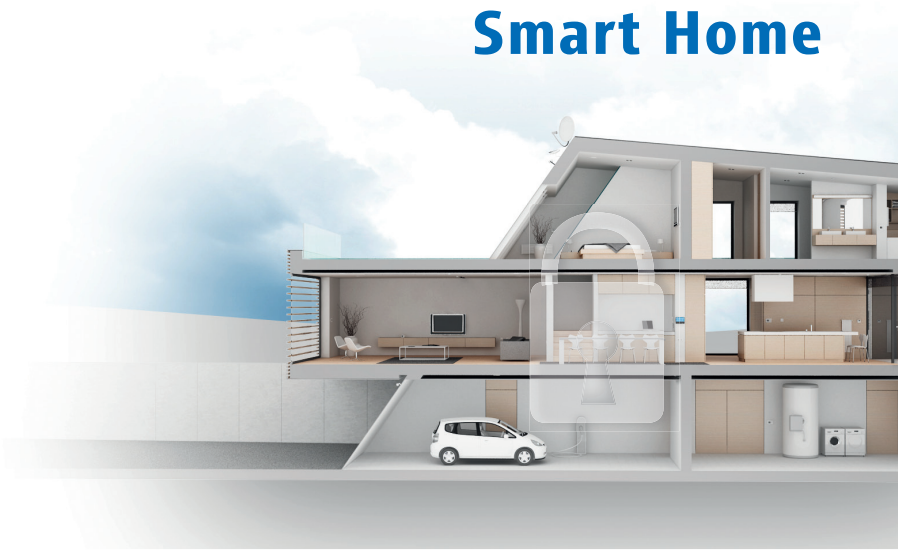
Telefon: +49 69 6302-222
E-Mail: hoffmannA@zvei.org

www.zvei.org

August 2015

Empfehlung

Datensicherheit im Smart Home



Bildnachweis: © ZVEI

Zentralverband Elektrotechnik- und Elektronikindustrie

Datensicherheit im Smart Home

Die digitalisierte Vernetzung von Hausgeräten, Multimedia und klassischen Gebäudefunktionen (Licht, Jalousie, Heizung etc.) ermöglicht eine Steigerung des Komforts, der Sicherheit und der Energieeffizienz. Doch jede Vernetzung birgt das Risiko eines Angriffs auf das Smart Home und somit auf die Privatsphäre. Aus einer bewussten Manipulation kann im schlimmsten Fall auch ein finanzieller Schaden entstehen. Durch eine sorgfältige Abschottung des Systems erhöht man die Sicherheit vor Angreifern. Je nach Beschaffenheit des Systems oder Geräts stehen unterschiedliche Möglichkeiten zur Verfügung.

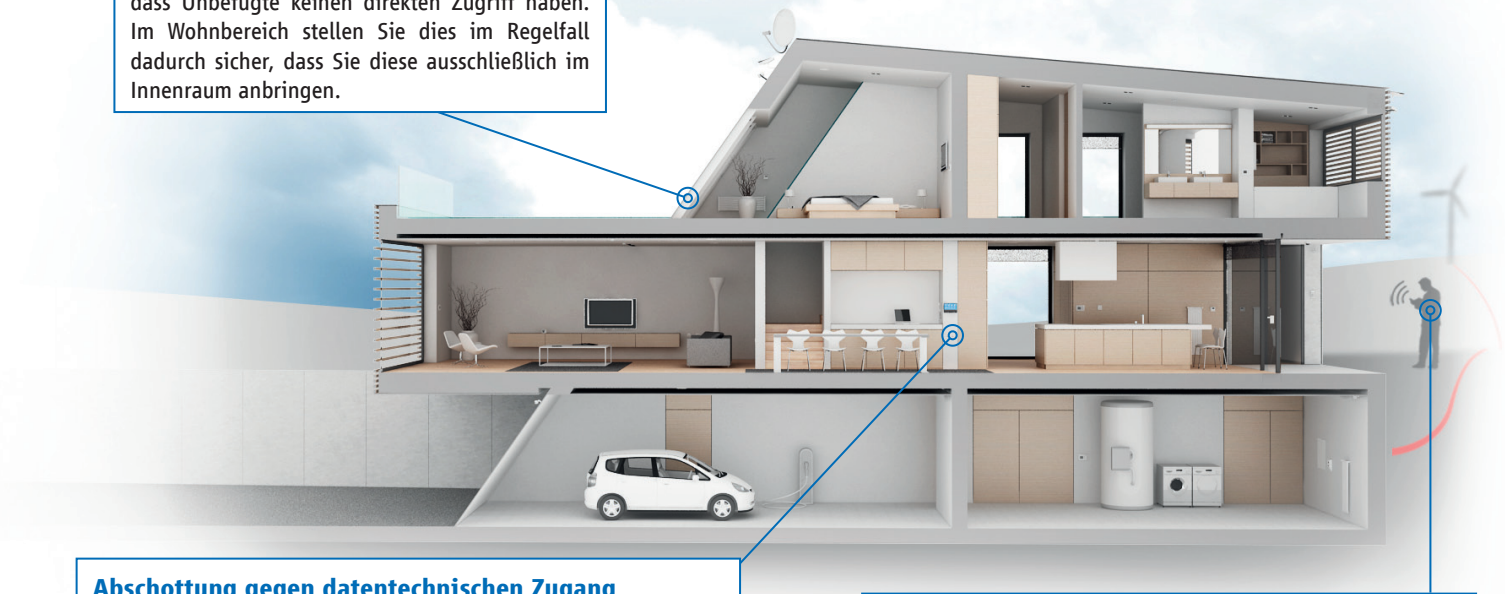
Allgemeine Sicherheitseinstellungen

Für alle Smart-Home-Geräte und -Systeme, Internetrouter sowie Computer gilt:

- Verwenden Sie sichere Passwörter (siehe auch Bundesamt für Sicherheit in der Informationstechnik, Thema: Passwörter)
- Aktivieren Sie sämtliche verfügbaren Sicherheitseinstellungen (Datenverschlüsselung, Adressfilter, Zertifikate etc.)
- Nutzen Sie eine sichere WiFi-Verschlüsselung (WPA2 + AES, Stand 2015)
- Anti-Viren-Software und Personal Firewalls auf allen Computern aktivieren (immer aktiv, tägliches update).
- Sämtliche Software, Firmware oder Betriebssysteme müssen auf allen Geräten, Systemen und Computern regelmäßig mit Updates aktuell gehalten werden. Aktivieren Sie falls verfügbar Auto-Update-Funktionen.

Abschottung gegen physischen Zugang

Sofern es möglich ist, sollten Sie alle Geräte und Kommunikationsleitungen so anbringen, dass Unbefugte keinen direkten Zugriff haben. Im Wohnbereich stellen Sie dies im Regelfall dadurch sicher, dass Sie diese ausschließlich im Innenraum anbringen.



Abschottung gegen datentechnischen Zugang

Insbesondere wenn der physische Zugang nicht zu 100 Prozent geschützt werden kann (Außenbereich, Funknetze, Powerline etc.), ist die Sicherung des datentechnischen Zugangs mittels Versschlüsselung und Authentifizierung von höchster Wichtigkeit. In der Gebäudeautomation stehen hierfür verschlüsselte Datenprotokolle zur Verfügung (z. B. KNX Data Security, verfügbar ab ETS 5.5).

Wichtig: In einem Datennetzwerk kann jedes angeschlossene Gerät zum Einfallstor werden. Ein Angreifer erlangt unter Umständen dabei nicht nur Zugriff auf das Gerät, sondern auch auf alle anderen im Netzwerk verbundenen Geräte, Systeme und Computer.

Fernzugriff per Smartphone oder Tablet

- Aktivieren Sie einen Fernzugriff nur wenn nötig.
- Nutzen Sie ausschließlich authentifizierte und verschlüsselte Kommunikation.
- Nutzen Sie VPN-Tunnel anstelle von Port-Weiterleitungen.