Security und Privacy im Smart Home aus Sicht des Nutzers

Dr. Siegfried Pongratz

ITG Workshop, 23. Oktober 2015, Offenbach

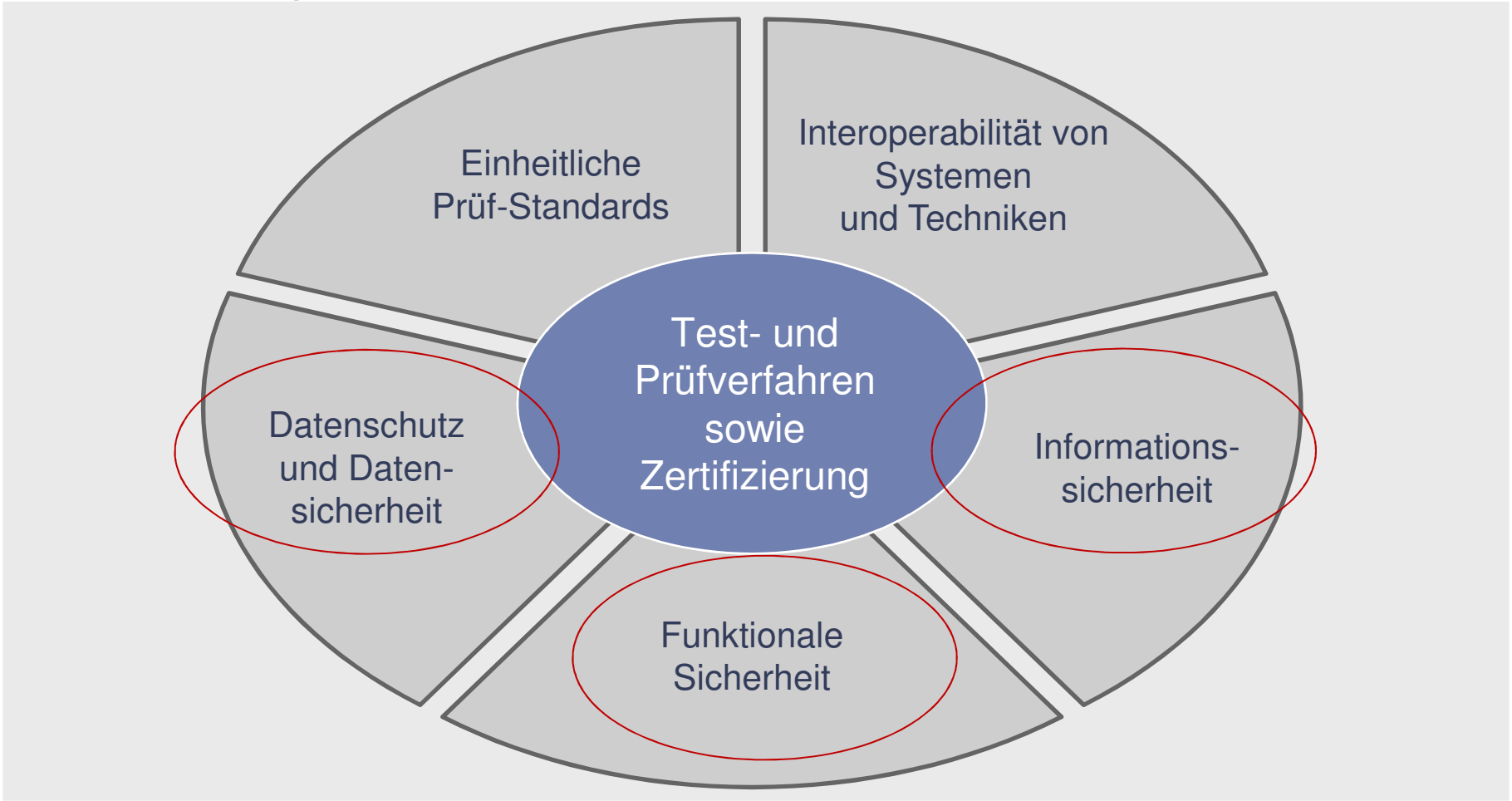
Beispiele die den Nutzer betreffen können

- Schnittstellen, die angegriffen werden:
  - Webseiten
  - Wartungszugänge
  - Mitarbeiter-PCs
  - Offene Ports
- Angriffsvektoren
  - Exploits von bekannten Schwachstellen
  - Brute-Force-Attacken auf schwache Passwörter und Verschlüsselungen
  - Social Hacking
- Maßnahmen
  - Sicherheitskonzepte (Bürosysteme, Produktivsysteme)
  - Verschlüsselungen (Daten, Kommunikation)
  - Update-Policy

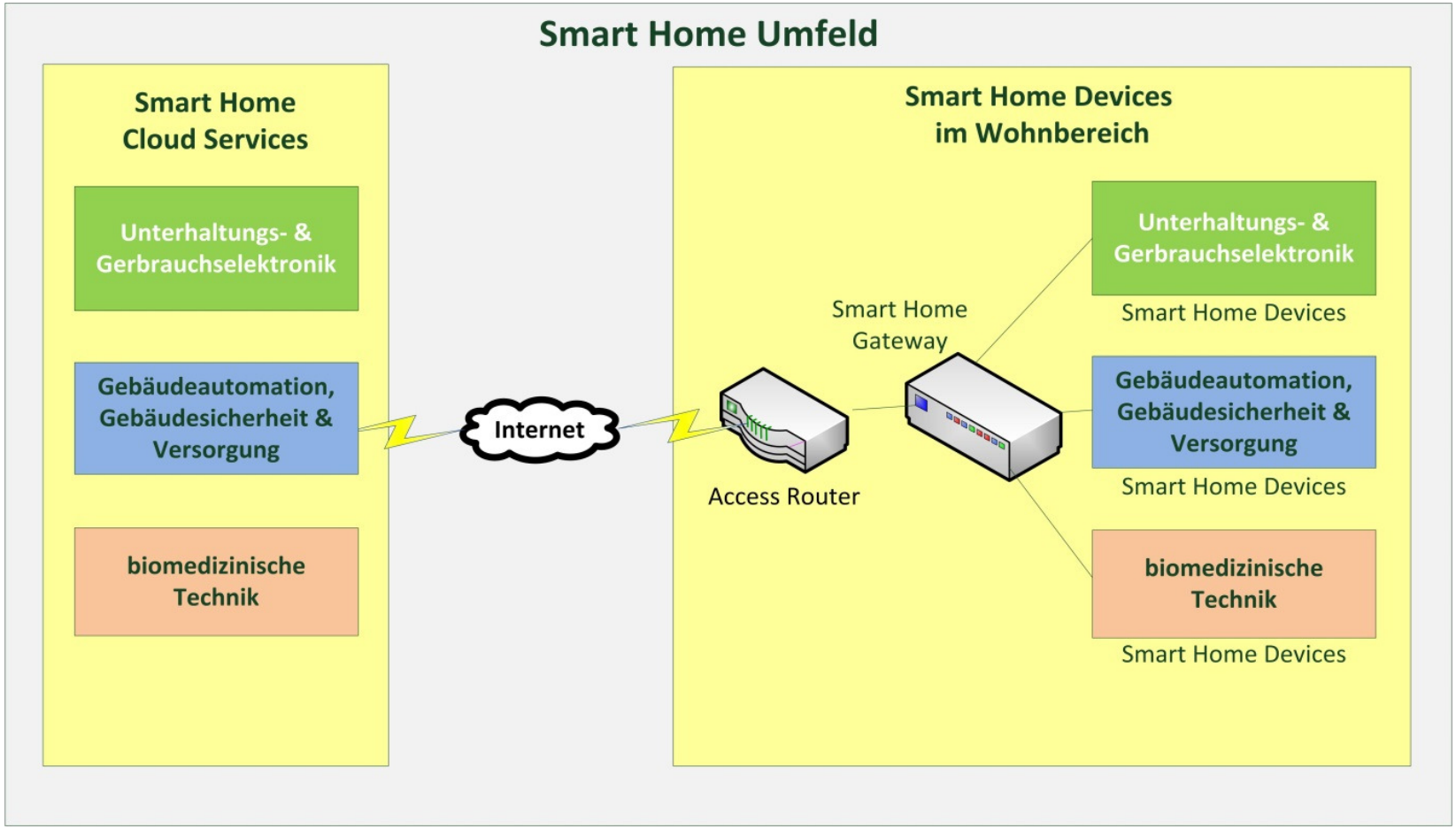
Quelle: Flickr Ines Hegedus-Garcia

Zielsetzung der VDE Smart Home Test-Plattform

Smarte Technologien



Smart Home Testportfolio



Problematiken der IT-Sicherheit im Smart Home Umfeld

1. Funktionalität vor Sicherheit
   → Sicherheit wird erst nachträglich priorisiert

2. Angriffe können mit weit verbreiteten Software-Werkzeugen durchgeführt werden
   → „Black-Hat“ Hacker haben bereits bewährte Tools zur Hand

3. Smart Home Systeme werden nicht von System-Administratoren gesichert und gewartet
   → oft nimmt der Endverbraucher das System in Betrieb und verwaltet es allein

→ Verunsicherung der Benutzer

→ **Besondere Anforderung an Smart Home Geräte und Systeme**

Foto: Petra Bork / pixelio.de

Foto: VDE

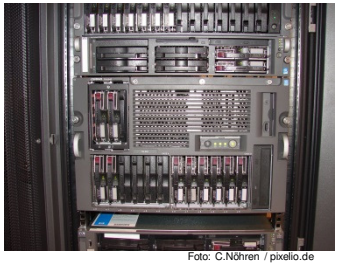


Foto: C.Nöhren / pixelio.de

Prüfung der Informationssicherheit

Lösungsansatz

- Standards/Normen für Informationssicherheit im Smart Home werden zur Zeit noch entwickelt: DKE AK 716.0.1

DKE
VDE DIN

- Um handlungsfähig zu sein, bis eine Norm zur Verfügung steht, wurde eine Prüfbestimmung für Smart Home Informationssicherheit und Datenschutz entwickelt:

  VDE-PB-0004:2014-12 und VDE-PB-0005:2014-12

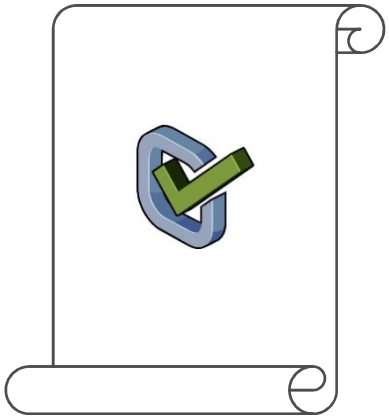
Durch Genehmigung des VDE Zertifizierungsausschuss ist eine Labelvergabe auf Grundlage dieser Dokumente möglich

VDE
Smart Home
Informationssicherheit geprüft
ID 40039154

Grundlagen der Prüfbestimmung

BSI Sicherheitsstandard Common Criteria und BSI Grundschutz

- Die Standards wurden in der Prüfbestimmung konkretisiert auf die Anforderungen von Smart Home Umgebungen
- Die Prüfbestimmung wurde erweitert um Aspekte des Datenschutzes
- Die Prüfung soll anwendbar sein für den gesamten Smart Home Bereich :
  - Energie, Komfort, Multimedia, Sicherheit, AAL



Ziele der Informationssicherheits-Prüfung

1. **Bestätigung zur grundsätzlichen Umsetzung eines IT-Schutzkonzepts**
   →Die Architektur, das Software-Design und die Implementierung ermöglicht die Einhaltung von IT-Schutz-Anforderungen in ausreichendem Maße.
   Prüfungen: Dokumentenprüfung, Labortests

2. **Bestätigung der wirksamen Umsetzung des IT-Schutzes**
   →Die Maßnahmen wurden für Endanwender wirksam umgesetzt.
   Prüfungen: Labortests, Penetrations-Tests

3. **Bestätigung zur Vollständigkeit der Dokumentation bezüglich IT-Sicherheit**
   →Die Dokumentation ist vollständig und bietet dem Endanwender alle notwendigen Informationen zur sicheren Verwendung
   Prüfung: Dokumentenprüfung

Prüfung des Datenschutzes

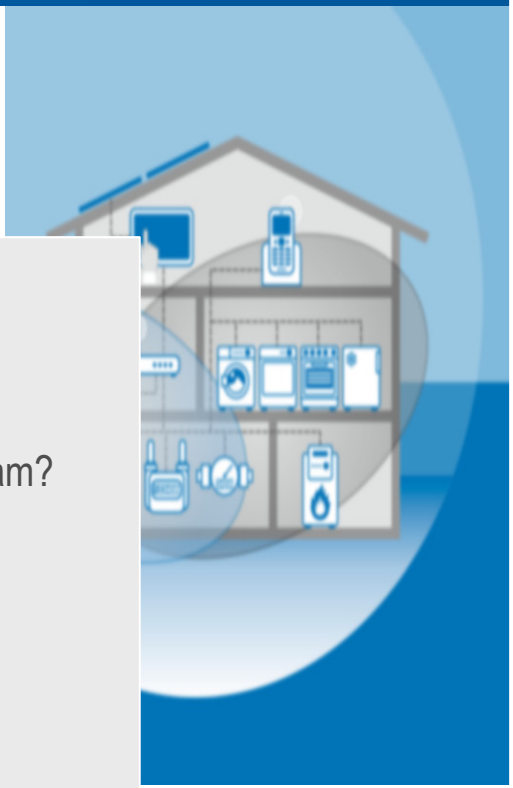
1. Identifikation der Datenschutzrelevanz

- Werden personenbezogene oder personenbeziehbare Daten erfasst, verarbeitet, gespeichert oder übermittelt?
- Darauf folgt die Eingruppierung in die entsprechende Datenschutzklasse

2. Prüfung des Datenschutzes entsprechend der Datenschutzklasse

- Wird der Benutzer über die Erfassung und Verarbeitung seiner datenschutzrelevanten Daten in der Benutzerdokumentation vollständig informiert?
- Wenn eine Datenschutzrelevanz besteht, wird geprüft, ob eine „verantwortliche Stelle“ klar definiert ist?
- Zusätzlich: Prüfung ob der Zugang zu datenschutzrelevanten Daten und die Speicherung entsprechend sicher realisiert ist

Prüfung der Smart Home Geräte



- **Aufgabenbereich**
  Prüfung der Smart Home Geräte und Kommunikationsgateways
  - **Sicherheitsziele**
    Werden alle geforderten Sicherheitsziele erfüllt? Ist die Implementierung wirksam?
  - **Lebenszyklus Prüfung**
    Wird die Informationssicherheit in allen Phasen des Lebenszyklus von der Installation über die Wartung bis zur Stilllegung gewahrt?
- **Prüfbereiche der Geräteprüfung**
  - Sicherheitsziele Informationssicherheit und Datenschutz
  - Produktdokumentation
  - Lebenszyklus
    - Installation
    - Konfiguration
    - Betrieb
    - Störung
    - Wartung
    - Stilllegung

Prüfung der Cloud-Dienste

- **Aufgabenbereich**
  Prüfung der Backend oder Cloud Anwendung für Smart Home Systeme
  - **Zugänge**
    Alle Zugänge zu den Server-Farmen und Dienste werden überprüft und bewertet (auch Vor-Ort-Prüfungen und Begutachtung bestehende Zertifizierungen)
  - **Implementierung**
    Die Implementierung der Sicherheitsmaßnahmen der Cloud-Kommunikation wird über externe und interne Penetrationstests überprüft .
    Organisatorische und vertraglich geregelte Sicherheitsmaßnahmen werden ebenfalls überprüft.
- **Prüfbereiche der Cloud-Prüfung**
  - Sichere Rechenzentren (Zugangsschutz, Brandschutz etc.)
  - Netzwerksicherheit
  - Anwendungs- und Plattformsicherheit
  - Sicherheit des Life-Cycle Managements
  - Datenschutz bei Cloud Services

Prüfung der Apps auf mobilen Endgeräten

- **Aufgabenbereich**
  Prüfung der Applikationen auf Smartphones und Tablets zur Steuerung der Smart Home Systeme
  - **Schutz vor Ausspähung und Sicherer Datenübertragung**
    Es wird überprüft, wie eine sichere Datenübertragung realisiert wurde und ob ausreichender Schutz gegenüber Ausspähung auf dem Gerät implementiert wurde.
  - **Sichere Software Entwicklung**
    Entwicklungsprozesse in Hinblick auf Informationssicherheit werden geprüft.
- **Prüfbereiche der App-Prüfung**
  - Informationen zur Funktion
  - Zugriffsschutz
  - Datenschutz
  - Sichere Datenübertragung
  - Software-Entwicklung und Lebenszyklus

Funktionale Sicherheit aus Sicht der Informationssicherheit

- Wenn in Geräten Kommunikationsschnittstellen zur Verfügung stehen (z.B. Smart Home Kommunikation), müssen diese Schnittstellen in einer Risikobewertung mit betrachtet werden.
  Und zwar aus dem besonderen Blickwinkel der Informationssicherheit (IT-Security) bzw. Cyber-Security.
  Denn zusätzlich zu einer Fehlbedienung, muss auch der Fall der Sabotage (Cyber-Crime) in die Risikobewertung miteinfließen.

- Um die Eintrittswahrscheinlichkeit für Cyber-Crime Gefährdungen zu vermindern, besitzt die Informationssicherheit die folgenden Sicherheitsziele:
  - **Integrität:** Ist das Signal echt? (Wurde es nicht manipuliert?)
  - **Authentizität:** Ist das Signal von einer berechtigten Instanz?
  - **Verfügbarkeit:** Ist der Dienst blockiert ?

Zur Risikobewertung der Funktionalen Sicherheit müssen eventuell auch die Aspekte der Informationssicherheit mit berücksichtigt werden.

Die Ziele der Informationssicherheit (IT-Security) können dann auch auf diesen Bereich der Funktionale Sicherheit bezogen werden (IT-Safety).

Vielen Dank für Ihre Aufmerksamkeit

VDE – Ihr zuverlässiger Partner für Prüfung und Zertifizierung

Dr. Siegfried Pongratz
Leiter Smarte Technologien

+49 69 8306 819
siegfried.pongratz@vde.com