

TeleTrust-Informationstag

"IT-Sicherheit im Smart Home und der Gebäudeautomation"

Berlin, 12.11.2014

RWE Smart Home: IT-Sicherheit beim Kunden vor Ort

Dr. Michael Westermeier, RWE Effizienz GmbH

RWE SmartHome: Komfort, Sicherheit & Energieeffizienz



**Temperiert
Heizkörper
nach Wunsch
im Tagesverlauf**



**Schaltet
elektrische
Geräte ein
und aus**



**Schaltet und
koordiniert die
Beleuchtung**



**Ist fern-
steuerbar,
auch per
Smartphone**



**Zentrale
Steuerung und
Konfiguration der
Geräte über PC**



**Visualisiert
PV-Erzeugung,
Speicherung und
Verbrauch**

RWE SmartHome: Hardware, Software & Usability



Positionierung im Deutschen SmartHome-Markt 2011...

Erschwingliche, intuitive und vielseitige Massenmarktprodukte fehlten 2011 im Hausautomatisierungsmarkt.



Heim-/ Handwerk

- Kostengünstige Geräte
- Do-it-yourself Lösung (nur für Techniker)
- Einfaches Design
- Eingeschränkter Funktionsumfang

Preis:

50 – 2.000 EUR*



RWE Smart Home

- Bezahlbar
- Leicht zu bedienen
- Attraktives Design
- Integriert alle wesentlichen Anwendungsbereiche

Preis:

350 – 2.000 EUR*



Luxus

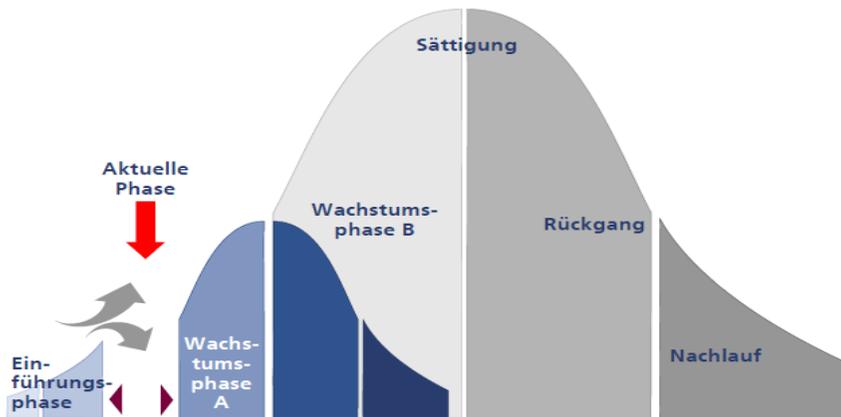
- Teuer
- Aufwendige Installation und Unterhaltung
- Gehobenes Design
- Individuelle Wünsche vollständig anpassbar

Preis:

> 10.000 EUR*

*abhängig von der Zahl der Komponenten

Der SmartHome-Markt 2014: Neue Player, viel Bewegung...



Quelle: KOTSCHI CONSULTING: „Smart Home Monitor 2014“, Wiesbaden 2014



Sicherheit im RWE SmartHome-System

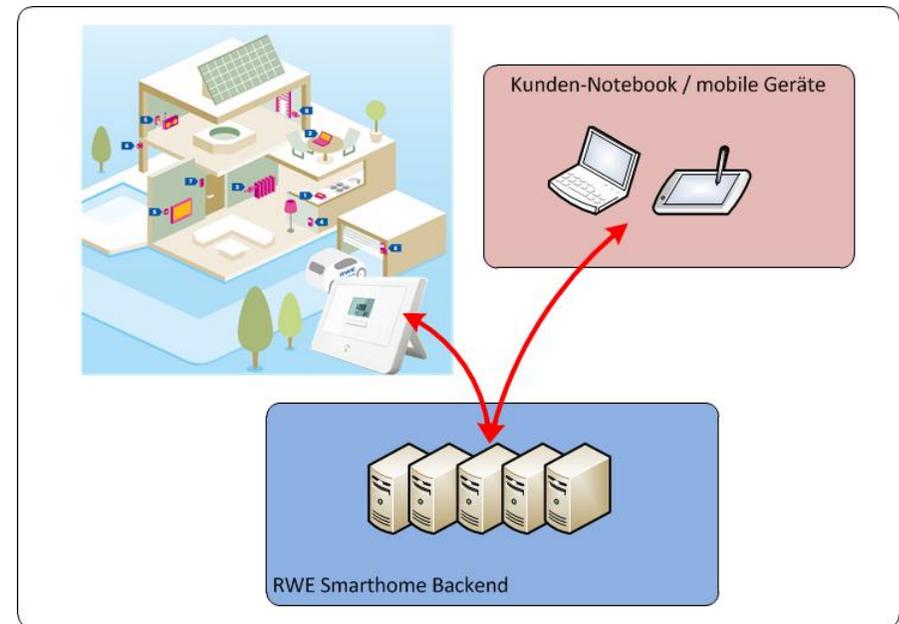
- Systemsicherheit ???
- Datenschutz ???

...steht bei RWE SmartHome an erster Stelle!



RWE SmartHome - Kommunikationsschema

- Zentrales Steuergerät beim Kunden (SHC)
 - kommuniziert mit Aktoren und Sensoren über Funk
 - kommuniziert mit PCs und mobilen Devices über IP (LAN/WLAN/Internet) zur Steuerung der Aktoren
- SmartHome-Backend im RWE Data Center
 - Portalseite für Kunden zur Initialisierung und Konfiguration des SHCs sowie zur Steuerung der Hauskomponenten



Die RWE SmartHome Backend-Server

- Drei-Schichten-Modell
Web-Server ↔ Applikations-Server ↔ Datenbank-Server
- Netzwerk-Separierung der Schichten untereinander sowie gegenüber Internet und RWE-Netzwerk durch Firewalls
- Externe Kommunikation über HTTPS mit zertifikatsbasierter Authentisierung

Die RWE SmartHome Zentrale



- Client-Zertifikat im TP-Module
- Kommunikation erfolgt über HTTPS mit zertifikatsbasierter Authentisierung
- Gehärteter Boot-Loader
- Firmware-Updates/ OTAU nur über signierte Installationsdateien
- Keine GUI-Komponenten enthalten

Zertifikate, Authentisierung & Verschlüsselung

- SmartHome-interne Zertifizierungsstelle (CA)
- SHC erhält initial ein Clientzertifikat
- Kommunikation SHC ↔ Backend ausschließlich über HTTPS
- Funk-Kommunikation SHC ↔ Geräte und Geräte ↔ Geräte:
 - CosIP, wireless mBus
 - AES-Verschlüsselung auf MAC-Layer (teilweise auch Applikations-Layer)
 - Sichere Funknetz-Inclusion über Backend-Schlüsselaustausch

Funktionssicherheit/ Ausfallsicherheit beim Kunden

- Gerätegrundfunktionen (bspw. Licht schalten, Heizen etc.) auch ohne zentrale Stelle (SHC) und Internet vorhanden
- Direkte Funk-Kommunikation einfacher Geräteverknüpfungen zwischen den beteiligten Geräten
- Resend-/ Acknowledgement-Funktionen im Funkverkehr
- Komplette Offline-Steuerung vom PC möglich durch Installation lokaler Steuerungssoftware

Organisatorische Maßnahmen

- TÜV Zertifizierung zum Produktstart (für Version 1.0)
- Erste deutsche VDE-SmartHome-Sicherheit Zertifizierung in 2014
- Bedrohungsanalyse inkl. Quellcodeanalyse durch spezielles Entwicklungsteam
- Regelmäßige Threat-Model-Analysis bei neuen Funktionen
- RWE EffzG PO, RWE EffzG ISO, RWE IT, Dienstleister (Prog.)

Projektbezogene Daten

- Gerätedaten (SHC-Konten, Gerätekonfigurationen)
 - Benutzerdaten (Kunden, [Mitbenutzer], ...)
 - Sitzungsdaten (Angemeldete Geräte)
 - [Nutzungsdaten (Schaltvorgänge, Ereignisse, ...)]
- ➔ Alle personenbezogenen Daten werden in SQL-Datenbanken in der Sicherheitszone „High“ gespeichert

RWE SmartHome - Datenerfassung

- Kunden können für nahezu alle Geräte eine Datenspeicherung aktivieren
- Daten werden zunächst auf SmartHome Controller gepuffert
- Übertragung zum SmartHome Backend erfolgt sobald bestimmte Menge an Daten erreicht ist



RWE SmartHome – „Device-Activity Logging“

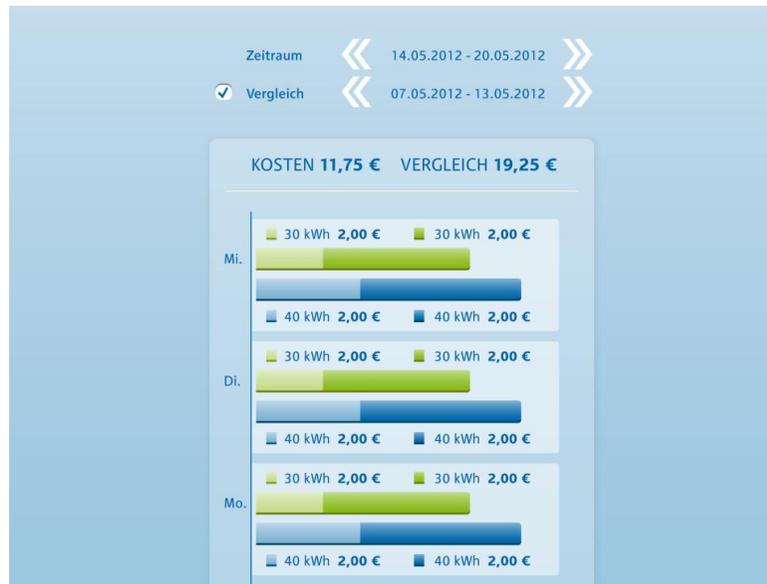
- Zustimmung zu spezieller Datenschutzvereinbarung notwendig
- Jedes Gerät muss individuell aktiviert werden




- Ansicht einer 3 Tageshistorie über Oberfläche
- .csv Datei kann für 30 Tage Historie exportiert werden
- Nach 30 Tagen werden Daten gelöscht

RWE SmartHome – „Power Control“

- Erfassung von Zählerdaten über Kundenschnittstelle
- Zustimmung zu spezieller Datenschutzvereinbarung notwendig



- Kunden stehen unterschiedliche Reports zur Verfügung
- Je nach Version stehen Daten für unterschiedliche Zeiträume zur Verfügung
- Aggregation der Daten abhängig von Zeitraum

- Vielen Dank für die Aufmerksamkeit!