Karlsruhe Institute of Technology (KIT)
Institute of Telematics

TELEMATICS TECHNICAL REPORTS

Bedrohungsanalyse eines Smart-Home-Szenarios zur Visualisierung von Energieverbrauchsdaten im Vorfeld einer Steuerentscheidung

Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL)
Arbeitsgruppe: Prototyp für Intelligente Infrastrukturen und Energie

Mit Beiträgen von:
Anton Hergenröder, Christian Haas, Roland Bless, Denise Dudek, Martina Zitterbart, Thomas Bräuchle, Oliver Raabe, Simon Greiner, Bernhard Beckert, Kaibin Bao, Hartmut Schmeck

Editoren: Kaibin Bao, Anton Hergenröder, Christian Haas

September 15, 2014, Rev. 1.0

TM-2014-1

ISSN 1613-849X

http://doc.tm.kit.edu/tr/

Institute of Telematics
Karlsruhe Institute of Technology (KIT)
Zirkel 2, 76131 Karlsruhe, Germany

Die Integration von vernetzter Sensorik, Gebäudeautomationstechnik und fernsteuerbaren Haushaltsgeräten zu einem intelligenten Haushalt (Smart-Home), welches seinerseits in einem Smart-Grid vernetzt ist, ermöglicht vielfältige Ansätze zur intelligenteren Nutzung von verfügbaren Energieressourcen und Steigerung des Wohnkomforts. Diese verteilten IT-Systeme eröffnen neue Angriffsmöglichkeiten auf Privathaushalte und müssen besonders sicher und privatsphärengerecht konzipiert sein. In diesem Dokument untersucht daher die KASTEL-Arbeitsgruppe „Intelligente Infrastrukturen und Energie“ Bedrohungen auf die IT-Sicherheit einer Smart-Home-Architektur.

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument enthält eine Bedrohungsanalyse eines „Smart-Home“-Szenarios welche im Rahmen des Teilprojektes *Intelligente Infrastrukturen und Energie* des Projekts KASTEL realisiert wurde. In diesem Dokument sind das Lasten- und das Pflichtenheft eines sicheren „Smart-Home“ sowie eine Bedrohungsanalyse praktisch vereint, da eine Analyse der Bedrohungen nicht ohne eine zugrunde liegende, ausformulierte Architektur möglich ist. Es wird ein Szenario „Smart-Home“ beschrieben, welches im Rahmen des Projekts teilweise als Prototyp realisiert werden soll. Das zu realisierende Szenario stellt dabei einen Ausschnitt aus einem Zukunftsszenario dar, welches die Einbettung von Smart-Homes als aktive Teilnehmer im Smart-Grid vorsieht. Vollständig lässt sich das Zukunftsszenario im Rahmen des Projekts KASTEL mit den verfügbaren Mitteln nicht umsetzen.

Das betrachtete Teilszenario soll die Funktionalität der Darstellung im Vorfeld einer Steuerentscheidung im Smart-Home ermöglichen, die eine gesamtenergetische Betrachtung erfordert. Die gesamtenergetische Betrachtung enthält Verbrauchs- und Erzeugungswerte von Haushaltsgeräten und des gesamten Haushalts sowie Tarif- und Anreizsignale von Energiedienstleistern.

Im Projekt KASTEL liegt der Forschungsschwerpunkt auf der informationstechnischen Sicherheit des Smart-Home. Dabei ist die Sicherheit von einzelnen Systemkomponenten, sowie deren Zusammenspiel und somit des Gesamtsystems zu gewährleisten. Beim Entwurf und der Umsetzung des Szenarios sind aktuelle gesetzliche Vorgaben sowie Schutzprofile und technische Richtlinien für die Sicherheit von Smart-Meter-Systemen zu berücksichtigen und auf ihre Tauglichkeit in dem Zukunftsszenario zu untersuchen. Ein Ziel der Arbeitsgruppe *Intelligente Infrastrukturen und Energie* war, eine sichere Smart-Home-Architektur zu entwerfen, die einerseits aktuelle Entwicklungen in der Funktionsvielfalt eines Smart-Home nicht einschränkt und andererseits sichere Kommunikation verschiedener Smart-Home-Anwendungen ermöglicht. Für die Kommunikationssicherheit wurden aktuelle Arbeiten und Protokolle aus dem Standardisierungsprozess der IETF (Home Networking Working Group) hinsichtlich Sicherheit und Funktionalität untersucht und wo passend, in die Smart-Home-Architektur eingebunden.

Im Rahmen der Bedrohungsanalyse wurde die Smart-Home-Architektur hinsichtlich potenzieller Bedrohungen auf die Kommunikation und die Anwendungssoftware interdisziplinär untersucht. Ziel war die Identifizierung aller potenziellen Bedrohungen, sowie deren Bewertung und weitestgehende Behandlung in den darauf folgenden Arbeitsschritten.

Vor der Durchführung der Bedrohungsanalyse wurden sowohl die schützenswerten Güter identifiziert als auch ein Angreifermodell entwickelt. Die schützenswerten Güter wurden aus der Perspektive aller im Smart-Home wirkenden Rollen, wie Haushaushaltsmitglied oder Energiemanagementadministrator, beschrieben und deren Wichtigkeit bewertet. Beispielsweise wurde als schützenswertes Gut mit dem höchsten Wert für ein Haushaltsmitglied die Vertraulichkeit der Energieverbrauchsdaten identifiziert, da anhand der Energieverbrauchsdaten unter anderem Rückschlüsse auf die Anwesenheit von Haushaltsmitgliedern im Smart-Home gezogen werden können.

1.1 Gliederung

Das Dokument ist wie folgt gegliedert. Zunächst wird die aktuelle Situation im Energienetz und im Privathaushalt in Kapitel 2 beschrieben. Auf dieser Basis, sowie den aktuellen Entwicklungen und Visionen im Bereich intelligente Infrastrukturen und Energie wird ein Zukunftsszenario in Kapitel 2.1 beschrieben, das als Rahmen für das in diesem Projekt zu realisierende Teilszenario dient. Dabei wird an dieser Stelle auch der Rahmen für die Sicherheitsanforderungen festgelegt. Anschließend wird in den nachfolgenden Kapiteln das Teilszenario „Darstellen im Vorfeld einer Steuerentscheidung, die eine gesamtenergetische Betrachtung erfordert“, in Form eines Lasten bzw. Pflichtenheftes definiert. Hierfür werden zunächst die Akteure und deren Rollen im Teilszenario in Kapitel 3.1 beschrieben. Danach werden die bekannten, notwendigen Systemkomponenten identifiziert und in Kapitel 3.2 dargestellt. Schließlich werden funktionale Anforderungen an den Prototypen im Kapitel 3.3 festgelegt und die hierfür notwendigen Daten im System identifiziert.

2 Motivation und Kontext

Die elektrische Energieversorgung wird traditionellerweise von Großkraftwerken gewährleistet, die ihren Strom über ein weitläufiges Übertragungsnetz in die regionalen Verteilnetze einspeisen. Über das Verteilnetz gelangt der Strom an Groß- und Kleinverbraucher. Bedingt durch die Netzinfrastruktur entstanden so vertikal integrierte Monopole unter staatlicher Regulierung.

Seit der Liberalisierung des Stromenergiemarktes im Jahre 1998 soll nunmehr schrittweise die Strombelieferung durch Wettbewerb optimiert werden. So hat der Endkunde die freie Wahl zwischen mehreren Energielieferanten. Jedoch bestehen auch im liberalisierten Energiemarkt aufgrund der Netzinfrastruktur systembedingt natürliche Monopole, die unter staatlicher Regulierung stehen.

So ist der Übertragungsnetzbetreiber für den sicheren und zuverlässigen Systembetrieb innerhalb seines Versorgungsgebietes, der sogenannten Regelzone, verantwortlich. Weiterhin sorgt er in der Rolle des Bilanzkreiskoordinators für den marktinternen Informationsaustausch. Der Verteilnetzbetreiber ist u.a. für den Netzzugang aller Stromnetzteilnehmer verantwortlich. Die jeweiligen Netzbetreiber sorgen für Betrieb, Wartung, Ausbauplanung und Stabilität ihrer Stromnetze.

Der Energielieferant kann in verschiedenen Regelzonen mit Strom handeln und so am liberalisierten Stromenergiemarkt teilnehmen. Zum Handeln mit Strom ist ein Energiekonto notwendig, ein sogenannter Bilanzkreis.

Ein Bilanzkreis kann rein virtuell als Handelsbilanzkreis existieren und/oder aus Einspeise- und Entnahmestellen von Stromkunden bestehen. Da systembedingt im ganzen Stromnetz jederzeit Stromerzeugung und -verbrauch sich entsprechen müssen, wird diese Eigenschaft auch von einem Bilanzkreis gefordert. Für jeden Bilanzkreis ist ein sogenannter Bilanzkreisverantwortlicher zu benennen, der für diese Aufgabe zuständig ist.

Aus einer Abwägung zwischen Informationsübertragungsaufwand und Effizienzgesichtspunkten wird die bilanzierungsrelevante Zeit in 15-minütige Blöcke aufgeteilt. Die durchschnittliche Einspeisung und Entnahme aus dem Bilanzkreis innerhalb der Blöcke soll möglichst gleich sein. In der Realität ist der Stromverbrauch jedoch nicht exakt zu prognostizieren, sodass immer eine Differenz bestehen bleibt. Schwankungen gleicht prinzipiell der Übertragungsnetzbetreiber aus, wofür er Verträge für Regelenergie mit Kraftwerken schließt. Die Differenz wird dem Bilanzkreisverantwortlichen als Ausgleichenergie in Rechnung gestellt.

Zur korrekten Abrechnung der Ausgleichsenergie wären also Lastgangkurven jeder Entnahme- und Einspeisestelle notwendig. Diese Lastkurven werden bei Kraftwerken

und Großverbrauchern (ab einem Jahresverbrauch von 100.000 Kilowattstunden) in Form einer registrierten Lastgangmessung (RLM) erfasst. Danach werden sowohl die Arbeit als auch die Leistung in Rechnung gestellt. Bei Kleinverbrauchern hingegen wird nur die Verbrauchssumme turnusgemäß (üblicherweise jährlich) abgelesen und in Rechnung gestellt. Hierbei werden im Rahmen des synthetischen Verfahrens je nach Kundengruppe normierte Standardlastprofile (SLP) zugrunde gelegt. Das Lastprofil wird mit dem Jahresverbrauch multipliziert, um so den Lastgang eines Haushalts möglichst genau zu bestimmen. Beim sogenannten analytischen Verfahren hingegen wird die gesamte Verbrauchszeitreihe eines Verteilnetzes herangezogen. Abzüglich Kraftwerkseinspeisung, Großkundenverbrauch und Netzverluste erhält man so den Summenlastgang aller Kleinkunden. Die Einzellastgänge ergeben sich dann durch Aufteilung nach Jahresverbrauch.

Die Prozessabläufe und Datenflüsse zwischen den Akteuren des Energiemarktes sind derzeit in allgemein verbindlichen Festlegungen der Bundesnetzagentur geregelt (GPKE, WiM, MaBiS). Die danach geltenden Vorgaben an Kommunikationsabläufe, Nachrichtenformate und Kompetenzen der beteiligen Akteure stehen vor der Herausforderung sich der Fortentwicklung der rechtlichen Rahmenbedingungen und politischen Zielsetzungen im Bereich des Klima- und Umweltschutzes anzupassen. Aufgrund der immer komplexer werdenden Kommunikationsszenarien, die sich von einem „offline“- hin zu einem „online“-Markt entwickeln, müssen die bestehenden Strukturen und Festlegungen der Marktkommunikation dahingehend optimiert und angepasst werden.

2.1 Zukunftsszenarios „Intelligente Infrastrukturen und Energie“

Das Smart-Home-Szenario ist ein Teil einer Vision, durch Informations- und Kommunikationstechnologie sowie Gebäudeautomation einzelne Komponenten im Haushalt und Haushalte untereinander zu einem intelligenten System zu vernetzen, welches Komfort und Energieeffizient erhöht. Im Folgenden werden einzelne Aspekte des Zukunftsszenarios erläutert, um den Entwurf des Smart-Home-Szenarios zu motivieren.

2.1.1 Vision des Smart-Home als variable Last im Energiesystem

Unter Berücksichtigung der Ziele der Europa 2020-Strategie und der politischen Zielsetzungen im Bereich des Klima- und Umweltschutzes im Rahmen der Realisierung der Energiewende, müssen die bestehenden Prozesse des Energiemarktes um die Integration und Förderung volatiler Energiequellen angepasst werden. Insbesondere intelligente Messsysteme innerhalb eines Smart Home können dazu dienen, den Energieverbrauch der Bewohner zu optimieren. Andererseits kann das Smart-Home als variable Last in das Energiesystem eingebettet werden. Denn zur Wahrung der Netzstabilität müssen sich Energieverbrauch und -erzeugung stets die Waage halten. Da der Verbrauch im klas-

sischen Stromsystem bestenfalls prognostizierbar, jedoch insbesondere bei Kleinkunden nicht steuerbar ist, muss die Energieerzeugung an den Energiebedarf optimierend angepasst werden. Diese Situation ändert sich mit der großflächigen Einführung von dezentral erzeugten erneuerbaren Energien, deren Erzeugungsleistung jedoch durch Unwägbarkeiten hinsichtlich der Verfügbarkeit der natürlichen Ressourcen geprägt ist. Beispielsweise lassen sich diese Systeme in Abwesenheit von Wind oder Sonne im Gegensatz zu klassischen Kraftwerken nicht bedarfsgemäß hochfahren.

Eine Möglichkeit zum Ausgleich stellt die Verschiebung von Stromlasten auf der Verbraucherseite dar. Dies wird durch Energiespeicher oder zeitliche Verschiebungen von Arbeitsvorgängen, die elektrischen Strom benötigen, realisiert. Solche Mittel sollen auch in einem automatisierten und intelligenten Haushalt (Smart-Home) zur Verfügung stehen. Spülmaschinen, Waschmaschinen und Trockner können ihre Startzeit nach hinten verschieben, sofern der Benutzer die Freiheiten dafür einräumt. Heizungs- und Kühlsysteme sind in der Lage, ihre Arbeit vorzuziehen ohne ihre Funktionserfüllung zu beeinträchtigen. Insbesondere auch durch die erwartete Einführung der Elektromobilität, werden in Zukunft noch größere Energiemengen durch Kleinkunden verschoben werden können.

Hieraus ergibt sich die Notwendigkeit technischer Funktionalitäten, die die Umsetzung der Energieoptimierung ermöglichen. Aus der Binnensicht des Smart-Home soll dies durch eine Kombination aus einem Smart-Meter-Gateway und einem Energiemanagement erzielt werden. Zentral ist dabei die Verbrauchsvisualisierung für Hausbewohner, um deren Verbrauchsverhalten zu beeinflussen und eine gezielte verbrauchsoptimierte Steuerung einzelner Haushaltsgeräte zu ermöglichen. Außerdem dient die Visualisierung der feingranularen Verbrauchswerte auf einem mobilen Endgerät der Nachvollziehbarkeit des Energieverbrauchs. Diese Funktionen sollen einerseits durch lokalen Zugriff aus der Sphäre des Smart-Home, wie auch durch externen Zugriff über eine Web-Schnittstelle auf die entsprechenden Messdaten verwirklicht werden können.

Weiterhin wird das Verfahren der Zählerstandsgangmessung eingeführt, welches die Erfassung echter Lastgänge ermöglicht. In einem festgelegten Intervall werden Messdaten erfasst und sowohl auf dem Smart-Meter-Gateway wie auch auf dem lokalen Energiemanagement sicher gespeichert. Zum Zwecke der Stromabrechnung können tarifierte Messdaten abgerufen und an die entsprechenden Marktakteure weitergeleitet werden. Auch die Durchführung einer korrekten Bilanzierung und Netzentgeltberechnung kann unter den jeweils beteiligten Marktakteuren anhand der Zählerstandsgangmessung auf Basis von Echtzeitdaten ermöglicht und optimiert werden.

Eine Übertragung der Messdaten an den Energielieferanten wiederum ermöglicht die Bildung von Anreiztarifen anhand derer dem Letztverbraucher ein Anreiz zur Energieeinsparung oder Steuerung des Energieverbrauchs geschaffen werden kann.

Eine Kombination dieser Funktionalitäten kann eine effektive Integration eines Smart-Home als variable Last in das moderne Energiesystem (Smart-Grid) gewährleisten.

2.1.2 Gebäudeautomation

Neben der Rolle im Energiesystem ist die Gebäudeautomation ein fester Bestandteil eines Smart-Home. Hier ist eine der treibenden Grundfragen, wie Technologie im Privathaushalt den Lebensstandard erhöhen und/oder übergangslos – ubiquitär – in das tägliche Leben des Bewohners integriert werden kann. Beides erfordert die Integration verschiedener Geräte in einem verteilten System. Die Anwendungsarten, die in einem integrierten Smart-Home umsetzbar sind, sind äußerst vielfältig: Beispielsweise werden durch die autonome Erfassung eines Anwesenheitsprofils Heizungs- und Kühlsysteme effizienter gesteuert, eine intelligente Kombination aus Verschattungs- und Leuchtsysteme sorgen für eine konstante Beleuchtung. Desweiteren alarmieren Sensoren im Haus den Bewohner über unbefugte Gebäudezugriffe.

Das übergeordnete Ziel der Benutzbarkeit gibt dabei einige Anforderungen an die Smart-Home Infrastruktur vor:

1. *Erweiterbarkeit*: Es muss möglich sein, neue Geräte mit wenig Aufwand in das bestehende System zu integrieren.

2. *Vernetzung*: Um eine Gesamtfunktionalität zu erbringen, die über die Summe ihrer Teile hinausgeht, müssen die beteiligten Rechnersysteme miteinander kommunizieren.

3. *Anbindung*: Um durch den Bewohner sinnvoll nutzbar zu sein, müssen entsprechende Schnittstellen zur Interaktion – speziell auch nach außen – angeboten werden.

Dadurch wird der Privathaushalt zu einem Teilnehmer am globalen Kommunikationsnetz, mit allen Gefahren und Schutzbedürfnissen, die damit einhergehen. Darüber hinaus ergibt sich durch das Szenario selbst eine sehr starke soziale Komponente: Die kommunizierten Daten werden aus dem direkten Umfeld von Privatpersonen ohne einschlägige Vor- bzw. Ausbildung erhoben. Demzufolge rücken auf menschliche Manipulierbarkeit zielende Angriffsarten weiter in den Vordergrund (*social engineering*).

Die Möglichkeit, ein vom Angreifer manipuliertes Gerät physikalisch einzuschleusen, z.B. als Werbegeschenk im Briefkasten, öffnet den ohnehin schon sensiblen und von Großunternehmen wie Google oder Facebook als Marketingplattform umkämpften Privatbereich in einer neuen Dimension. Es sind somit Schadensszenarien denkbar, in denen Privatpersonen durch unbefugte Kleinstgeräte ohne ihr Wissen ausspioniert werden. Auf diesem Weg ergeben sich auch Möglichkeiten zur Sabotage – z.B. durch Störung der internen Kommunikationspfade – oder zur Erlangung von unbefugtem Zugang – etwa durch das Ausschalten einer Alarmanlage.

2.1.3 Smart-Grid-Funktionalität

Die nachfolgende Zusammenstellung der relevanten Use Cases des Energiemarktes (Smart-Grid) soll einen Überblick über die relevanten Informations- und Datenflüsse zwischen

den verschiedenen Akteuren des Energiemarktes geben. Diese Use Cases beschreiben die wesentlichen Funktionalitäten, die eine rechtskonforme Integration eines Smart-Home ermöglichen. Sie stammen aus den Prozessfestlegungen der Bundesnetzagentur (BNetzA) für die Marktkommunikation im Bereich der Elektrizitätsversorgung, aus dem Schutzprofil und der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie aus der Orientierungshilfe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und des Düsseldorfer Kreises.

2.1.3.1 Verbrauchsvisualisierung

Der erste gesetzlich vorgesehene Mechanismus zur Effizienzsteigerung ist das in § 21d Abs. 1 EnWG angelegte Widerspiegeln des Stromverbrauchs (Verbrauchsvisualisierung). Anhand der Visualisierung der feingranularen Verbrauchswerte auf einem lokalen Endgerät (z.B. via Home-Display) soll die Nachvollziehbarkeit des Energieverbrauchs für den Letztverbraucher ermöglicht werden. Hierfür muss es für jeden Zähler eine lokale Schnittstelle am Smart-Meter-Gateway geben. In diesem Use Case verbleiben die feingranularen Verbrauchswerte im Hoheitsbereich des Letztverbrauchers. Es ist aber auch möglich, die feingranularen Verbrauchsdaten an einen externen Marktteilnehmer (z.B. an den Lieferanten) zur dortigen Aufbereitung und Visualisierung zu versenden. Über eine Web-Schnittstelle kann der Letztverbraucher nach erfolgreicher Authentifizierung die Daten dort abrufen und sich anzeigen lassen.

2.1.3.2 Vollständige Abrechnung des Stromverbrauchs

Eine vollständige Abrechnung beinhaltet die Prozesse der Tarifierung, die Abrechnung der Netzentgelte gegenüber dem Netznutzer sowie den Prozess der Bilanzierung.

Die Tarifierung ist die Zuordnung der jeweiligen Messwerte eines Zählers zu einem Tarifprofil. Sie kann zum einen zentral bei einem externen Marktteilnehmer (beim Lieferanten) stattfinden, oder aber dezentral auf dem Smart-Meter-Gateway. Bei der zentralen Tarifierung fließen die konkreten Messdaten vom Letztverbraucher zum Lieferanten und werden dort einem Tarifprofil zugeordnet. Bei der dezentralen Tarifierung werden die Messdaten auf dem Smart-Meter-Gateway den Tarifregistern zugeordnet, die vom Lieferanten dort hinterlegt wurden. Diese dezentrale Tarifierung ermöglicht daher eine Aggregierung in verschiedene Tarifstufen auf dem Smart-Meter-Gateway, sodass nicht die reinen Messwerte an den Lieferanten übermittelt werden müssen, sondern lediglich die nach Tarifen aggregierten Registerwerte.

Die Netzentgeltberechnung nach den Festlegungen der Bundesnetzagentur beinhaltet die Feststellung und Berechnung der Netzentgelte, die der Lieferant gegenüber dem jeweiligen Netzbetreiber für die Nutzung der Netzinfrastruktur zu entrichten hat. Die Verbrauchsdaten der Standardlastprofil-Kunden (SLP-Kunden, deren Verbrauch unter 100.000 Kilowattstunden liegt) werden zu diesem Zweck derzeit einmal jährlich an den

Verteilnetzbetreiber übermittelt. Die Abrechnung der Netzentgelte gegenüber Großkunden (in der Regel Industriekunden ab einem Jahresverbrauch von 100.000 Kilowattstunden) hingegen erfolgt über die sogenannte registrierende Leistungsmessung (RLM). Diese sieht eine tägliche Übermittlung der viertelstündlichen Lastgänge der Großkunden an den Verteilnetzbetreiber vor um anschließend die Netzentgeltberechnung gegenüber dem Lieferanten zu ermöglichen.

Für den Prozess der Bilanzierung sind innerhalb einer Regelzone von einem oder mehreren Netznutzern sogenannte Bilanzkreise zu bilden. Ein Bilanzkreis in einer Regelzone enthält die einem Netznutzer zugeordneten Einspeise- und Entnahmestellen. § 4 Abs. 2 der Stromnetzzugangsverordnung schreibt vor, dass für jeden Bilanzkreis von den bilanzkreisbildenden Netznutzern gegenüber dem Betreiber des jeweiligen Übertragungsnetzes (ÜNB) ein Bilanzkreisverantwortlicher (BKV) zu benennen ist. Dieser Bilanzkreisverantwortliche ist verantwortlich für eine ausgeglichene Bilanz zwischen Einspeisungen und Entnahmen in einem Bilanzkreis in jeder Viertelstunde und übernimmt als Schnittstelle zwischen Netznutzern und Betreibern von Übertragungsnetzen die wirtschaftliche Verantwortung für Abweichungen zwischen Einspeisungen und Entnahmen eines Bilanzkreises.

Da bei SLP-Kunden nur eine jährliche Ablesung der Zählerstände erfolgt, kann die Bilanzierung auf Basis der Verbrauchsdaten der SLP-Kunden nur anhand von Jahresprognosewerten gebildet werden. Bei RLM-Kunden hingegen erfolgt eine tägliche Übermittlung der Verbrauchswerte. Somit ist ein täglich aufgelöstes Verbrauchsprofil eines Großkunden verfügbar, das den Prozess der Bilanzierung vereinfacht. Bei der neu einzuführenden Zählerstandsgangmessung werden die Zählerstände am Ende jeder Viertelstunde gespeichert. Die Differenz der einzelnen Zählerstande ergibt dann den Verbrauch in kW pro Viertelstunde in Echtzeit. Damit wird für den Bilanzkreisverantwortlichen anhand entsprechender Übermittlungsintervalle die Möglichkeit geschaffen, exakt zu bilanzieren und die viertelstündliche Energieversorgung optimal zu berechnen.

2.1.3.3 Gestaltung von Anreiztarifen

Eine Datenerhebung und -weiterverwendung kann zulässig sein, wenn damit dem Letztverbraucher die Umsetzung variabler Tarife ermöglicht wird. Hierzu ist gesetzlich vorgesehen (§ 40 Abs. 5 EnWG), dass Lieferanten – soweit technisch machbar und wirtschaftlich zumutbar – für Letztverbraucher von Elektrizität einen Tarif anzubieten haben, der einen Anreiz zu Energieeinsparung oder Steuerung des Energieverbauchs setzt. Hierzu muss allerdings eine Auswertung der Verbrauchsprofile vorgenommen werden, die wiederum unter dem Vorbehalt der Veranlassung durch den Letztverbraucher stehen muss.

2.1.3.4 Daten für das Zu- und Abschalten von Lasten

Im Rahmen der Systemverantwortung der Verteilnetzbetreiber (VNB) kann es für diese vorteilhaft sein, mit den Endkunden ab- bzw. zuschaltbare Lasten vertraglich zu vereinbaren. Insbesondere ist gesetzlich vorgesehen, dass Verteilnetzbetreiber denjenigen Letztverbrauchern und Lieferanten im Bereich der Niederspannung ein reduziertes Entgelt berechnen können, wenn ihnen im Gegenzug die Steuerung von vollständig unterbrechbaren Verbrauchseinrichtungen zum Zwecke der Netzentlastung gestattet wird. Zu diesem Zweck soll die Verwendung von Verbrauchsdaten des Letztverbrauchers zulässig sein, sofern dem Stand der Technik entsprechende Datensicherheitsmaßnahmen eingehalten werden.

2.1.3.5 Einspeisen und dezentrale Abrechnung

Personenbezogene Messdaten können in diesem Use Case dazu verwendet werden, um die Einspeisung von Energie und die darauf bezogene Abrechnung zu ermöglichen. Zweck dieses Use Cases ist es, die von einem sogenannten Prosumer eingespeiste Energiemenge zwischen diesem und dem Abnehmer abrechnen zu können. Dazu sollen die Einspeisedaten auf dem Gateway dem hinterlegten Tarifprofil zugeordnet werden. Dabei ist zwischen dem Daten- und dem Energiefluss zu unterscheiden. Der Datenfluss betrifft die Abrechnung (bzw. Vergütung) zwischen Prosumer und Abnehmer. Die Abnahme von Strom nach dem EEG (Erneuerbare-Energien-Gesetz) hingegen erfolgt durch den Netzbetreiber.

2.1.3.6 Ermittlung Netzzustand

Um die Energieversorgung sicherzustellen, ist in begründeten und dokumentierten Fällen die Verwendung personenbezogener Messdaten zur Ermittlung des Netzzustandes zulässig. Hierbei handelt es sich um Netzzustandsdaten (wie Spannung, Phasenwinkel und Frequenz), die zu diesem Zweck vom Letztverbraucher an den Verteilnetzbetreiber übertragen werden können.

2.1.4 Externe Anbindungsarten

Die Darstellung der Verbrauchsdaten im Smart-Home kann, wie schon in Abschnitt 2.1.1 und 2.1.3 angesprochen, sowohl intern als auch extern über eine Web-Schnittstelle erfolgen.

Die darzustellenden Daten selbst können auf einem eigenen Server des Bewohners hinterlegt sein, auf den der Bewohner Zugriff hat, wenn er sich außerhalb seiner Wohnung aufhält. Ein solcher Server wird sich in der Regel nicht in der Wohnsphäre des Smart-Home-Bewohners befinden, sondern allenfalls als virtueller Server oder Root-Server von einem Host-Provider zur Verfügung gestellt werden.

Weiter können darzustellende Smart-Home-Verbrauchsdaten auch über Anzeigedienste von Drittanbietern abrufbar sein. Beispiele für Drittanbieter in diesem Sinne sind etwa Google, Amazon und andere Cloud-Anbieter. In diesem Fall ist die Ausgestaltung der Anzeige im Unterschied zur Lösung mit eigenem oder selbstverwaltetem Server nicht in der Verwaltung durch den Bewohner selbst. Bei der Anzeige über Drittanbieter werden die Verbrauchsdaten dem gewählten Drittanbieter zur Verfügung gestellt. Dies kann insbesondere in beliebig genauer Auflösung erfolgen. Der Drittanbieter stellt seinerseits die Plattform zur Darstellung und eine Schnittstelle zum Abruf – in der Regel wohl über http/REST – bereit.

2.1.5 Smart-Meter-Gateway: Vertrauenswürdige Energiemarkt-Schnittstelle des Smart-Home

Während einerseits für Energiemanagement und Gebäudeautomation detaillierte Daten zum Stromverbrauch und Verbraucherverhalten benötigt werden, ist andererseits sicherzustellen, dass diese sensiblen Daten nur an Dritte weitergegeben werden, wenn diese zweckmäßig benötigen werden. Führt beispielsweise der Energielieferant die Abrechnung durch, so muss dieser nur den Gesamtstromverbrauch des Haushalts, nicht aber den Verbrauch einzelner Geräte kennen. Je nach Tarif wird er diesen auch nicht in hoher Präzision für kurze Zeitabschnitte benötigen, sondern nur in Tages- oder gar Jahresblöcken. Gleichzeitig muss hier aber auch garantiert werden, dass dem Energielieferanten die tatsächlichen Stromverbräuche übermittelt werden, und nicht etwa vom Verbraucher gefälschte Werte. Ähnliche Anforderungen gelten beispielsweise auch beim Zugang zu sensiblen Daten seitens der Netzbetreiber.

Im Smart-Home dient das Smart-Meter-Gateway als Schnittstelle zwischen Haushalt und externen Akteuren zur Übermittlung solcher vertraulicher Daten. Zusammen mit der Messeinrichtung bildet das Smart-Meter-Gateway ein Messsystem nach § 2 Abs. 3 MsysV bzw. § 21d Abs. 1 EnWG. Anforderungen an Vertraulichkeit werden im Schutzprofil BSI-CC-PP-0073 sowie in der Technischen Richtlinie TR-03109 gestellt und müssen also durch das Smart-Home-Gateway umgesetzt werden.

Im einfachsten Fall hat das Gateway innerhalb des Smart-Home lediglich Zugriff auf einen geeichten Gesamtstromverbrauchzähler. Wenn ein Letztverbraucher aber, zur besseren Steuerung und Prognose der Netzlast, seinem Stromnetzbetreiber eingeschränkte Informationen etwa zu gerätespezifische Stromverbräuche, oder das Energiemanagement geplante stromintensive Verbrauchsvorgänge (man denke an das Laden eines Elektro-Mobils) zur Verfügung stellen will, muss das Gateway auch Zugriff auf entsprechende Sensoren haben. Dies eröffnet weitere interessante Anwendungen: So könnten Temperatursensoren, zusätzlich zu ihrer Funktion in der Heimautomatisierung, auch als Feuermelder dienen. Das Gateway stellt hier sicher, dass Sensorinformationen nur im Notfall das Smart-Home verlassen. Abseits der Stromenergie könnte ein Smart-Home-Gateway weiterhin zur sicheren Übertragung von Gas-, Wasser- und Wärmeverbrauchsdaten die-

nen.

2.1.6 Rollen des Energiemarkts

Für eine umfassende Bewertung des Teilszenarios sind die externen Marktrollen des Energiesektors und die internen Rollen in der Sphäre des Smart-Home zu betrachten. Die Marktollen des Energiesektors sind als gesetzliche Funktionsbeschreibungen zu verstehen, die insbesondere im Energiewirtschaftsgesetz (EnWG) definiert werden. Auch die internen Rollen des Smart-Home-Prototypen können als Funktionsbeschreibungen verstanden werden.

Begrifflich und inhaltlich muss dabei von den Akteuren unterschieden werden. So kann ein Marktakteur (beispielsweise die örtlichen Stadtwerke als juristische Person) mehrere Marktrollen einnehmen (beispielsweise Netz- und Messstellenbetrieb sowie Stromlieferant). In der Sphäre des Smart-Home gilt dasselbe. Dementsprechend kann es einen Bewohner geben, der Vertragspartner bzw. Kunde des Stromlieferanten ist und damit die Rolle des Letztverbrauchers einnimmt (beispielsweise der Haushaltsvorstand als natürliche Person). Andererseits gibt es Bewohner, die zum Haushalt gehören (Mitbewohner, weitere Familienmitglieder) und den Gesamtverbrauch zwar beeinflussen, jedoch nicht in vertraglichen Beziehungen zum Lieferanten stehen.

Daher gilt, dass Rollen als Funktionsbeschreibungen von einem oder mehreren Akteuren (also konkreten natürlichen oder juristischen Personen) wahrgenommen werden können und daher keine Kongruenz zwischen Rolle und Akteur besteht.

Übertragungsnetzbetreiber (ÜNB) Der Übertragungsnetzbetreiber ist eine regulierte Dienstleistungsmarktrolle und für den sicheren Betrieb eines Energienetzgebietes, der sogenannten Regelzone, verantwortlich. Zudem koordiniert der ÜNB den Informationsaustausch bezüglich Bilanzkreisen. Er ist für die Verfügbarkeit von ausreichend Regelenergie verantwortlich und rechnet dessen Nutzung mit den Bilanzkreisverantwortlichen (VNB und Energielieferant) ab.

Verteilnetzbetreiber (VNB) Der Verteilnetzbetreiber ist eine regulierte Dienstleistungsmarktrolle und für den Betrieb eines Verteilnetzes zuständig. Dazu gehört beispielsweise auch die Schaffung von physikalischen Zugängen für Energiekunden zum Energienetz. Die Verwaltung von Zuordnungslisten zwischen Zählpunkten und Bilanzkreisen fällt auch in den Zuständigkeitsbereich des Verteilnetzbetreibers. Das Verteilnetz überspannt ein Bilanzierungsgebiet.

Energielieferant (LF) Ein Energielieferant ist eine Energiemarktrolle, die im Endkundenwettbewerb mit anderen Energielieferanten steht. Ein Energielieferant steht im direkten Vertragsverhältnis zum Letztverbraucher. Er ist dafür zuständig, den vom Kunden

benötigten Strom am Energiemarkt zu beziehen. Für die Abrechnung der Energienutzung des Bewohners muss der Stromverbrauch mit einem Stromzähler gemessen werden. Ohne Einschränkung der Allgemeinheit wird hier angenommen, dass der Energielieferant genau einen Bilanzkreis besitzt und die Rolle des Bilanzkreisverantwortlichen für diesen Bilanzkreis inne hat.

Messstellenbetreiber (MSB) Der Messstellenbetreiber ist für den Betrieb der Messsysteme und für das Ablesen der Zählstände verantwortlich. Diese Rolle kann auch von einer Fachkraft, die das Messsystem installiert, repräsentiert werden.

Smart-Meter-Gateway-Administrator Der Smart-Meter-Gateway-Administrator ist eine im BSI-Schutzprofil definierte Rolle. Der Gateway Administrator ist dafür zuständig, das Gateway zu verwalten und zu konfigurieren.

Demand Side Manager Der Demand Side Manager beeinflusst durch ein Anreizsignal den Energieverbrauch des Smart-Home. In dem hier betrachteten System beeinflussen Anreizsignale die Tarifsignale des Energielieferanten. Zur Zweckerfüllung muss der Demand Side Manager von allen Messsystemen im Bilanzkreis mindestens die aktuelle Verbrauchs- und Einspeiseleistung erfahren.

Letztverbraucher Der Letztverbraucher ist das Haushaltsmitglied, das die Interessen aller Haushaltsmitglieder in Bezug auf die Stromnutzung vertritt. Er steht als einzige Person aus dem Haushalt im direkten Vertragsverhältnis zum Energielieferanten und erhält als Energiekunde Zugriff auf die Energieverbrauchsmesswerte, die vom Messsystem erhoben werden.

3 Systemmodell

3.1 Rollen des Smart-Home-Szenarios

Im Smart-Home-Szenario sind verschiedene juristische oder natürliche Personen involviert, die definierte Funktionen des Smart-Homes nutzen können. Um den Funktionsumfang klar einzugrenzen, wurden Rollen und deren Zweck im Szenario identifiziert. Eine juristische oder natürliche Person kann ein oder mehrere Rollen ausüben.

Haushaltsvorstand Der Haushaltsvorstand vertritt die Interessen aller Haushaltsmitglieder. Er entspricht dem Letztverbraucher aus Sicht des Energiemarkts und nur er hat damit exklusiv den Zugriff auf widergespiegelte Daten des Messsystems. Der Haushaltsvorstand ist gleichzeitig ein Haushaltsmitglied.

Haushaltsmitglieder Die Haushaltsmitglieder sind die Bewohner und des Nutzer des Smart-Home. Sie haben grundsätzlich Zugang zum Smart-Home. Durch ihre Anwesenheit und Nutzung der im Smart-Home befindlichen Geräte verändern sie Sensordaten, die Rückschlüsse auf ihr Nutzungsprofil erlauben. Sie dürfen ihre eigenen Nutzungsprofile einsehen.

Energiemanagement Administrator Der Energiemanagement Administrator ist ein spezifisches Haushaltsmitglied, das die Steuerbox einrichten und Zugriffsrechte der Steuerbox verwalten darf.

Externe berechtigte Personen Externe berechtigte Personen sind Personen, denen Zugang zum Haushalt gewährt wird, die allerdings keine Haushaltsmitglieder sind. Solche Personen sind beispielsweise Gäste von Haushaltsmitgliedern oder beauftragte Handwerker. Sie dürfen Geräte im Haushalt nutzen, sollen aber keine Informationen erhalten, die Rückschlüsse auf das Verhalten von Bewohnern erlauben.

Externe unberechtigte Personen Externe unberechtigte Personen sind nicht berechtigt, das Haus zu betreten. Sie können dennoch Zugriff auf gewisse Teile des Smart-Homes, wie dem Funknetz, haben oder sich dazu verschaffen. Externe unberechtigte Personen sollen aber keinen Zugriff auf jegliche Informationen aus dem Smart-Home bekommen.

Externer Widerspiegelungsdienstleister Der externe Widerspiegelungsdienstleister hält Serversysteme oder Clouddienste außerhalb des Smart-Home bereit, welche vom Energiemanagement Administrator spezifizierte Daten speichert und dem Haushaltsvorstand widerspiegelt.

3.2 Systembeschreibung und Teilsysteme

Das Smart-Home besteht natürlicherweise aus räumlich getrennten Teilsystemen. Für den Prototypen *Intelligente Infrastrukturen und Energie* wurde eine Auswahl an Teilsystemen getroffen, die als Ganzes ein System zur Energieeffizienzsteigerung durch Widerspiegeln des Energieverbrauchs realisiert. Die Auswahl, welche in Abbildung 3.1 als grau gestrichelte Linie dargestellt ist, stellt eine klare Systemgrenze für die Realisierung des Prototypen dar. In die Sicherheitsanalyse müssen jedoch auch Umgebungskomponenten einbezogen werden. Für Umgebungskomponenten (siehe Abschnitt 3.2.2) bestehen bereits genaue Sicherheitsspezifikationen zur Verfügung, die für die zu betrachteten Teilsysteme (Abschnitt 3.2.1) berücksichtigt werden.

3.2.1 Teilsysteme

Energiemanagement Das Energiemanagement erfasst Zustände der Haushaltsgeräte und steuert diese nach Vorgaben des Bewohners und nach externen Signalen. Dazu werden auch Zustands- und Verbrauchsdaten über verschiedene Kommunikationswege autorisierten Rollen widergespiegelt. Das Energiemanagement steht im Besitz des Bewohners.

Haushaltsgeräte Haushaltsgeräte erfüllen für Haushaltsmitglieder eine Funktion und benötigen dazu elektrische Energie. Die Nutzung der Geräte beeinflusst den Stromverbrauch und die Zustandsinformationen der Haushaltsgeräte. Darüber lassen sich Rückschlüsse auf das Verhalten der Haushaltsmitglieder ziehen.

Informationstablet Das Informationstablet dient dem Darstellen von aktuellen und historischen Mess- und Zustandsdaten aus dem Smart-Home. Das Informationstablet befindet sich innerhalb des Smart-Homes, und steht im Besitz des Bewohners. Es ermöglicht *internen* Zugang zu o.g. Daten.

Smartphone Das Smartphone dient dem Darstellen von aktuellen und historischen Mess- und Zustandsdaten aus dem Smart-Home. Das Smartphone kann sich sowohl innerhalb als auch außerhalb des Smart-Homes befinden. Es ermöglicht *externen* Zugang zu o.g. Daten.

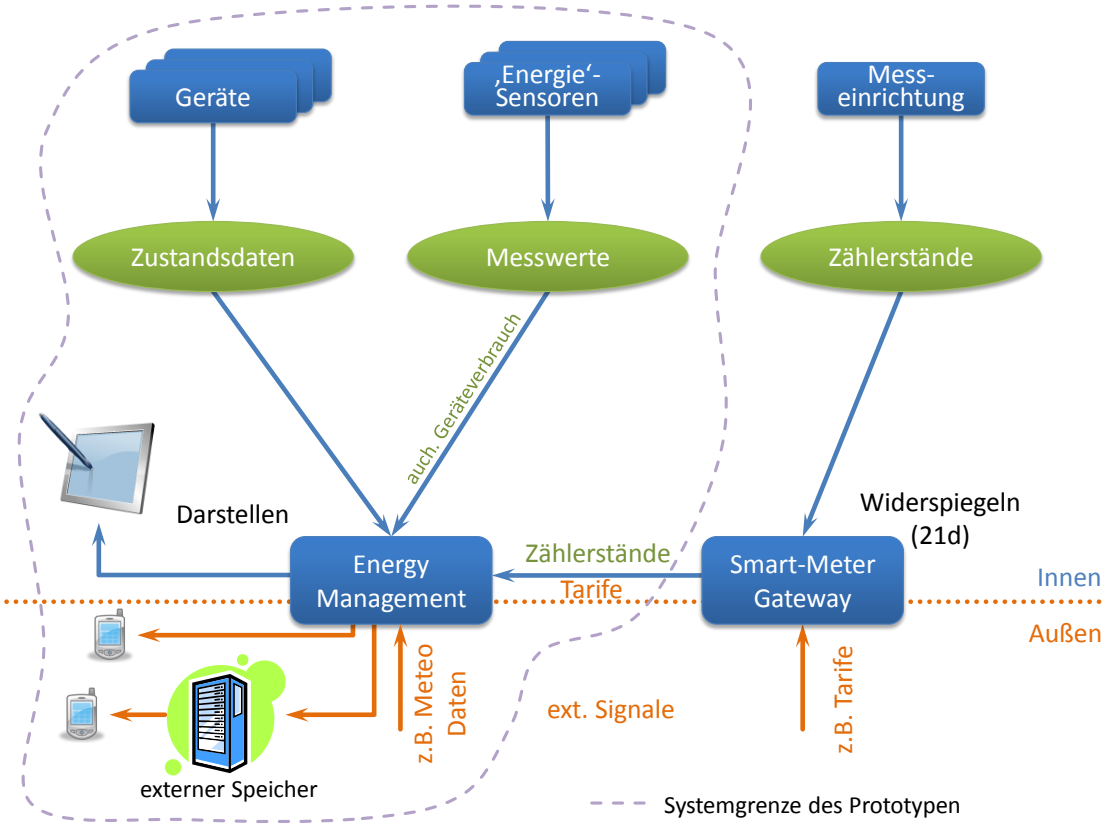

Abbildung 3.1: Informationsflüsse im Smart-Home

Sensoren Sensoren im Smart-Home erfassen Messwerte von Haushaltsgeräten oder der Umgebung. Diese Daten lassen Rückschlüsse auf das Verhalten der Haushaltsmitglieder zu.

3.2.2 Umgebungskomponenten

Messeinrichtung Die Messeinrichtung erfasst die elektrische Energieentnahme und -einspeisung des gesamten Smart-Homes. Über Schnittstellen bietet es die Messwerte anderen Teilsystemen an. Es ist eine Messeinrichtung im Sinne von § 2 Absatz 1 MsysV. Die Messeinrichtung unterliegt der Kontrolle des Messstellenbetreibers.

Smart-Meter-Gateway Das Smart-Meter-Gateway ist eine Kommunikationsschnittstelle zwischen Smart-Home und dem Energiemarkt. Es stellt dem Energiemanagement Zählerstände aus der Messeinrichtung sowie Signale von Energiemarktteilnehmern zur

Verfügung.

3.3 Funktionale Anforderungen

Die Grundfunktionalität des Prototypen ist „Darstellen im Vorfeld einer Steuerentscheidung, die eine gesamtenergetische Betrachtung des Smart-Home erfordert“. Alle Funktionen und Daten die darüber hinaus beschrieben werden, dienen lediglich der Motivation des Teilszenarios und werden entsprechend gekennzeichnet. Sie bilden den Rahmen in dem der Prototyp entwickelt werden soll.

3.3.1 Anwendungsfälle

UC 1 Der Haushaltsvorstand oder ein Haushaltsmitglied möchte eine Darstellung des aktuellen Energieverbrauchs im Smart-Home am internen Informationstablet.

UC 2 Der Haushaltsvorstand oder ein Haushaltsmitglied möchte eine Darstellung des historischen Energieverbrauchs im Smart-Home am internen Informationstablet.

UC 3 Der Haushaltsvorstand oder ein Haushaltsmitglied möchte eine Darstellung des aktuellen Zustands aller Haushaltsgeräte am internen Informationstablet.

UC 4 Der Haushaltsvorstand oder ein Haushaltsmitglied möchte eine Darstellung der aktuellen Tarifsignale am internen Informationstablet.

UC 5 Der Haushaltsvorstand oder ein Haushaltsmitglied möchte eine Darstellung des aktuellen Energieverbrauchs, des historischen Energieverbrauchs, der aktuellen Tarifsignale und des aktuellen Zustands bestimmter Haushaltsgeräte im Smart-Home auf seinem Smartphone außerhalb des Hauses.

Abgrenzung Die folgenden Anwendungsfälle werden hier dargestellt, um Erweiterungen des Systems aufzuzeigen und den Entwurf für diese Erweiterungen offen zu halten. Jedoch sind diese Anwendungsfälle nicht Gegenstand des Entwurfs und der Implementation.

UC 6 Der Verteilnetzbetreiber will Informationen über den Energieverbrauch/-erzeugung zum Zwecke der Bilanzierung.

UC 7 Der Bewohner will seine Haushaltsgeräte aus der Ferne steuern.

UC 8 Der Energielieferant will Informationen über den Energieverbrauch/-erzeugung zum Zwecke der Abrechnung.

UC 9 Der Demand Side Manager will verschiebbare, zu- und abschaltbare Lasten im Haushalt steuern.

UC 10 Der Haushaltsvorstand oder ein Haushaltsmitglied möchte eine Darstellung des historischen Energieverbrauchs, der bei dem externen Widerspiegelungsdienstleister gespeichert ist.

3.3.2 Daten

Im Rahmen des Smart-Home-Energiemanagement sind mehrere Datenquellen vorgesehen:

Datengruppe D Gesamter Verbrauch elektrischer Energie aus einer Messeinrichtung.

Datengruppe T Signale externer Energiemarktteilnehmer, die über das Smart-Meter-Gateway zur Verfügung gestellt werden.

Datengruppe S Messwerte der einzelnen Energiesensoren (inklusive Geräteverbrauchsdaten).

Datengruppe E Weitere Daten, die Einfluss auf eine Steuerentscheidung des Energiemanagements oder des Bewohners haben können.

Datengruppe Z Zustandsdaten der einzelnen Haushaltsgeräte.

Die anfallenden Daten werden allesamt von der jeweiligen Datenquelle auf das Smart-Home-Energiemanagement übertragen. Die Datenübertragung erfolgt zum Zwecke der Darstellung des Gesamtverbrauchs und der Nutzungszeit der elektrischen Energie sowie zur Darstellung aller Gerätezustands- und Verbrauchsdaten.

Im Gesamtsystem werden folgende Daten erhoben und ausgetauscht:

	Bezeichnung	Datentyp / Wertebereich
D1	Wirkenergiezähler–Energiebezug	COSEM-Register “1-0:1.8.0*255”
D2	Aktueller Wirkleistungsbezug	COSEM-Register “1-0:1.7.0*255”
D3	Wirkenergiezähler–Energieeinspeisung	COSEM-Register “1-0:2.8.0*255”
D4	Aktuelle Wirkleistungseinspeisung	COSEM-Register “1-0:2.7.0*255”
T1	Tarifsignal des Energielieferanten	Array aus 96 integer, Einheit: ct / kWh
S1	Stromverbrauch eines Haushaltsgeräts	integer, Einheit: W
E1	Meteorologische Daten	aktuelle Außentemperatur als double, Witterungslage als enumeration
Z1	Haushaltsgeräte-UID	32 bit unsigned integer
Z2	Geräteklasse	16 bit enumeration [DIN EN 50523]
Z3	Gerätestatus	8 bit enumeration [DIN EN 50523]
Z4a	Programmname	string
Z4b	Programmparameter	key-value-map (string, string)
Z4c	Programmdauer	unsigned integer, Einheit: min
Z5	Programmlastgang	integer-array, Einheit: W

3.3.3 Funktionen des SmartHome

3.3.3.1 F1: Darstellen im Vorfeld einer Steuerentscheidung, die eine gesamtenergetische Betrachtung erfordert

F1 b: Darstellen im privatdispositiven Bereich

F1 b DD: Stromzählerstände

Die Messeinrichtung erzeugt Zählerstände, welche den Stromverbrauch des gesamten Smart-Home angeben.

Die folgenden Daten werden an der Messeinrichtung erhoben:

- D1: Wirkenergiezähler–Energiebezug,
- D2: Aktueller Wirkleistungsbezug,
- D3: Wirkenergiezähler–Energieeinspeisung,
- D4: Aktuelle Wirkleistungseinspeisung.

Die Zählerstände werden zunächst an das Smart-Meter-Gateway übertragen.

Die Zählerstände werden vom Energiemanagement in regelmäßigen Abständen beim Smart-Meter-Gateway abgeholt.

Je nach Datenhaltungsschema (siehe F1 b S) werden die Zählerstände im Energiemanagement gespeichert und / oder an einen externen Server weitergeleitet.

Die Stromzählerstände sollen so gespeichert werden, dass zumindest die Verbrauchs- und Einspeisesumme in den folgenden Zeitspannen zu erkennen ist: (vgl. TR03109-1, Seite 52)

- D11: die letzten 7 Tage, Tagessummen,
- D12: die letzte Woche,
- D13: der letzte Monat,
- D14: der gleiche Monat des Vorjahres,
- D15: das letzte Jahr,
- D16: die letzten 15 Monate, monatsweise aufgeschlüsselt.

F1 b DZ: Zustandsdaten

Die Geräte erzeugen Daten, über die ihr aktueller Zustand ermittelt werden kann (Zustandsdaten).

Die folgenden Zustandsdaten werden von den Geräten erhoben:

- Z1: Geräte-UID,
- Z2: Geräteklasse nach DIN EN 50523,

- Z3: Status ibid.,
- Z4a: Programmname,
- Z4b: Programmparameter,
- Z4c: Programmdauer,
- Z5: Programmlastgang.

Die Zustandsdaten werden an das Teilsystem Energiemanagement übertragen.

Je nach Datenhaltungsschema (siehe F1 b S) werden die Zählerstände im Energiemanagement gespeichert und / oder an einen externen Server weitergeleitet.

Für das Energiemanagement sind mindestens die Daten Z1, Z3, Z4a-c oder Z1, Z3, Z5 notwendig.

F1 b DS: Sensordaten von Energiesensoren

Energiesensoren erfassen den aktuellen Verbrauch des Smart-Home feingranular.

Folgende Daten werden erfasst:

- S1: Strommess-Sensoren—aktueller Stromverbrauch pro Gerät. Jeder Sensor vermisst dabei genau ein Gerät,
- S2: Temperatur-Sensoren—aktuelle Raumtemperatur,
- S3: Wärmeverbrauchssensoren—Energieverbrauch durch Heizung.

Die Daten S2 und S3 sind als alternative Beispiele für Energiesensorikdaten zu lesen.

Die Zustandsdaten werden an das Teilsystem Energiemanagement übertragen.

Je nach Datenhaltungsschema (siehe F1 b S) werden die Zählerstände im Energiemanagement gespeichert und / oder an einen externen Server weitergeleitet.

F1 b DT: Signale vom Smart-Meter-Gateway

Das Tarifsignal wird vom Energiemanagement in regelmäßigen Abständen beim Smart-Meter-Gateway abgeholt.

Folgende Daten werden übertragen:

- T1: Tarifsignale des Energieanbieters.

Je nach Datenhaltungsschema (siehe F1 b S) werden die Zählerstände im Energiemanagement vorgehalten und / oder an einen externen Server weitergeleitet.

F1 b DE: Externe Signale

Externe Anbieter erzeugen zusätzliche informative Daten.

Dies sind zum Beispiel:

- E1: Meteorologische Daten,
- E. . . n: weitere energetisch relevante, aber vom Smart Home nicht erfasste Daten.

Die externen Signale werden an das Teilsystem Energiemanagement gesendet.

Je nach Datenhaltungsschema (siehe F1 b S) werden die Zählerstände im Energiemanagement vorgehalten und / oder an einen externen Server weitergeleitet.

F1 b S: Datenhaltung

Der Energiemanagement-Administrator kann wählen, wo die Daten aus F1 b DD, DZ, DS, DT und DE gespeichert werden sollen. Es wird grundsätzlich zwischen zwei Möglichkeiten unterschieden:

1. Datenhaltung auf dem Energiemanagement: Sämtliche Daten werden auf der Plattform des Energiemanagement gespeichert,
2. Datenhaltung auf einem externen Server oder Cloud des externen Widerspiegelungsdienstleisters: Ausgewählte Daten werden an externe Server übertragen. Der Energiemanagement-Administrator konfiguriert, welche Daten übermittelt werden.

F1 b Z: Datenzugriff

Die in F1 b S gespeicherten Daten können auf zwei Wegen zugänglich gemacht werden. Ein Zugriff auf diese Daten kann immer nur lesend und nach einer erfolgreichen Authentifizierung erfolgen.

1. Der Zugriff erfolgt lokal innerhalb des Smart-Home über das Smart-Home-Tablet,
2. Der Zugriff erfolgt über das Internet mit dem Smart-Home-Tablet.
   a) Wobei die Übertragung via eine im Internet verfügbare Web-Schnittstelle zum Smart-Home geschieht.
   b) Oder der Zugriff über einen externen Server oder Cloud erfolgt, in der auch die Daten gehalten werden.

F1 c: Anzeigefunktionalität

Die Anzeige erfolgt intern am Teilsystem Informationstablet oder extern am Smartphone.

Das Teilsystem Energiemanagement stellt dem Teilsystem Informationstablet die anzuzeigenden Informationen zur Verfügung.

Das Teilsystem Energiemanagement oder der externe Speicher stellt dem Smartphone die anzuzeigenden Informationen zur Verfügung.

Das Informationstablet stellt dem Bewohner (der Haushaltsvorstand oder ein Haushaltsmitglied) eine Benutzerschnittstelle zur Verfügung – diese kann

- grafisch,
- oder textuell

sein.

F1 c I: Informationstypen

Das Teilsystem Informationstablet oder das Smartphone kann folgende Informationstypen anzeigen:

- I1: Gerätezustandsdaten,
- I2: Energieverbrauchsdaten,
- I3: Sonstige.

Es stellt hierfür dem Bewohner eine entsprechende Auswahlfunktionalität zur Verfügung.

F1 c A: Auswahl

Der Bewohner kann auswählen, welche Daten angezeigt werden sollen.

Insbesondere kann er nach folgenden Kriterien auswählen:

- A0: Informationstyp s. F1 c I,
- A1a: Gerätetyp,
- A1b: Geräteklasse,
- A2: Raum, bzw. mehrere Räume, sofern zutreffend,
- A3: Sensor-Typ, sofern zutreffend,
- A4: Gesamtsicht.

Das Teilsystem Informationstablet oder das Smartphone stellt hierfür Auswahlmöglichkeiten zur Verfügung.

F1 c GV: Genauigkeit Verbrauchsdatenanzeige

Der Bewohner kann sich die Verbrauchsdaten in unterschiedlicher Genauigkeit darstellen lassen.

Verbrauchsdaten der Umgebungskomponente Messeinrichtung liegen maximal sekundengenau vor.

Verbrauchsdaten der Teilsysteme Sensorik liegen in der Auflösung 12 bis 60 Messwerte pro Minute (1 - 5 Sekunden) vor.

Das Teilsystem Energiemanagement bzw. der externe Speicher stellt Aggregationsfunktionen zur Verfügung, um die Daten in unterschiedlicher Auflösung bereitzustellen.

Dem Informationstablet werden aktuelle Verbrauchsdaten aus der Umgebungskomponente Messeinrichtung und den Teilsystemen Sensorik in höchstmöglicher Auflösung zur Verfügung gestellt.

Dem Smartphone werden keine aktuellen Verbrauchsdaten aus dem Teilsystem Sensorik zur Verfügung gestellt.

Dem Smartphone werden Verbrauchsdaten aus der Umgebungskomponente Messeinrichtung in der Auflösung von 1 Messwerten pro Stunde zur Verfügung gestellt. Es werden dabei die Verbrauchsdaten der letzten voll vergangenen Stunde zur Verfügung gestellt.

F1 c GZ: Genauigkeit Gerätezustandsdatenanzeige

Der Bewohner kann sich die aktuellen Gerätezustandsdaten darstellen lassen.

Das Teilsystem Energiemanagement bzw. der externe Speicher stellt Funktionen zur Verfügung, um die Daten zu filtern und unterschiedliche Teile der Daten bereitzustellen.

Es werden die aktuellsten dem Energiemanagement bzw. dem externen Speicher zur Verfügung stehenden Daten bereitgestellt.

Dem Smartphone werden die aktuellen Zustandsdaten nur für Geräte folgender Klassen zur Verfügung gestellt: Klimaanlage, Kühlschrank mit Gefrierabteil, Gefrierschrank, Weinkühlschrank, Kühlschrank, Durchlauferhitzer, Heißwasserspeicher.

Dem Informationstablet werden die aktuellen Zustandsdaten für Geräte aller Klassen zur Verfügung gestellt.

F1 c HV: Historie Verbrauchsdatenanzeige

Es liegen am Teilsystem Energiemanagement oder am externen Speicher die Verbrauchsdaten der letzten 12 Monate vor.

Diese können am Teilsystem Informationstablet oder am Smartphone bei Bedarf erfragt werden.

Das Teilsystem Energiemanagement bzw. der externe Speicher stellt Funktionen zur Verfügung, um die Daten zu filtern und unterschiedliche Teile der Daten in unterschiedlicher Auflösung bereitzustellen.

Daten aus dem Teilsystem Sensorik können entsprechend **F1 c A** aggregiert für alle Sensoren, oder für Teilmengen der Sensoren zur Verfügung gestellt werden.

Dem Informationstablet werden historische Verbrauchsdaten aus dem Teilsystem Messeinrichtung in beliebig hoher Auflösung bereitgestellt (insofern diese dem Energiemanagement bzw. dem externen Speicher zur Verfügung stehen).

Dem Informationstablet werden historische Verbrauchsdaten aus dem Teilsystem Sensorik nur in Histogrammen folgender Klassifizierung zur Verfügung gestellt:

- Verbrauch nach Uhrzeit (Breite der Klassen: 2 Stunden),
- Verbrauch nach Wochentag.

Dabei müssen Daten aus Erhebungszeiträumen von mindestens 4 zusammenhängenden Wochen zu Grunde gelegt werden. Die Startzeitpunkte dieser Abschnitte können nur in Abständen von 4 Wochen gewählt werden.

Dem Smartphone werden historische Verbrauchsdaten aus dem Teilsystem Messseeinrichtung in Auflösung von höchstens 1 Messwert pro Stunde zur Verfügung gestellt.

Dem Smartphone werden keine historischen Verbrauchsdaten aus dem Teilsystem Sensorik zur Verfügung gestellt.

F1 c HZ: Historie Zustandsdatenanzeige

Es liegen am Teilsystem Energiemanagement oder am externen Speicher die Gerätezustandsdaten der letzten 12 Monate vor.

Diese können am Teilsystem Informationstablet oder am Smartphone bei Bedarf erfragt werden.

Das Teilsystem Energiemanagement bzw. der externe Speicher stellt Funktionen zur Verfügung, um die Daten zu filtern und unterschiedliche Teile der Daten in unterschiedlicher Auflösung bereitzustellen.

Daten aus dem Teilsystem Sensorik können entsprechend **F1 c A** aggregiert für alle Geräte, oder für Teilmengen der Geräte zur Verfügung gestellt werden.

Dem Informationstablet werden die Zustandsdaten aus dem Teilsystem Messeinrichtung in beliebig hoher Auflösung bereitgestellt (insofern diese dem Energiemanagement bzw. dem externen Speicher zur Verfügung stehen).

Dem Informationstablet werden die Zustandsdaten aus dem Teilsystem Sensorik nur nach folgender Klassifizierung zur Verfügung gestellt:

- Gerätezustand nach Uhrzeit (Breite der Klassen: 2 Stunden),

- Gerätezustand nach Wochentag.

Dabei müssen Daten aus Erhebungszeiträumen von mindestens 4 zusammenhängenden Wochen zu Grunde gelegt werden. Die Startzeitpunkte dieser Abschnitte können nur in Abständen von 4 Wochen gewählt werden.

Dem Smartphone werden keine historischen Zustandsdaten zur Verfügung gestellt.

3.4 Sicherheitsanforderungen

Im System Smart-Home sind mehrere Rollen tätig, deren unterschiedliche Interessen und Bedürfnisse zu einer unterschiedlichen Bewertung von schützenswerten Gütern und deren Werten führt. Aus diesem Grund werden hier die Güter und deren Werteabschätzung aus der Sicht der jeweiligen system-internen Rolle beschrieben.

3.4.1 Sicht des Haushaltsvorstands

Zu schützendes Gut	**Werteskala: 1 bis 5**
Vertraulichkeit der Gerätezustände (Datengruppe Z) gegenüber Dritten. Ermöglicht detaillierte Rückschlüsse auf das Verhalten von Haushaltsvorstand und -mitgliedern. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)*	Höchster Wert (5)
Vertraulichkeit der Energieverbrauchsdaten (Datengruppe D) gegenüber Dritten. Ermöglicht detaillierte Rückschlüsse auf das Verhalten von Haushaltsvorstand und -mitgliedern. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)*	Höchster Wert (5)
Vertraulichkeit der Stromsensordaten (Datum S1) gegenüber Dritten. Ermöglicht detaillierte Rückschlüsse auf das Verhalten von Haushaltsvorstand und -mitgliedern. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)*	Höchster Wert (5)

Zu schützendes Gut	Werteskala: 1 bis 5
Vertraulichkeit der Wärmefluss- und Temperatursensordaten (Datum S2 & S3) gegenüber Dritten. Ermöglicht grobe Rückschlüsse auf die Anwesenheit von Haushaltsvorstand und -mitgliedern. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)*	Hoher Wert (4)
Vertraulichkeit der Datengruppen Z,S,D gegenüber den Haushaltsmitgliedern *Gefahr der innerfamiliären Überwachung*	Niedriger Wert (2)
Vertraulichkeit externer Signale (Gruppe T) Öffentliche Daten	Ohne Wert (1)
Vertraulichkeit weiterer externer Signale (Gruppe E) Öffentliche Daten	Ohne Wert (1)
Integrität externer Signale (Gruppe T) *Finanzieller Schaden beim folgen falscher Tarifsignale (Eigentum Art. 14 GG)*	Höchster Wert (5)
Integrität der Daten Z, D, S1, S3 Bedingt möglicherweise eine Anpassung auf ungünstige Betriebsparameter von Geräten oder ungünstiges Verhalten von Haushaltsvorstand bzw. -mitgliedern. *Irreführung durch Darstellung von falschen Energieverbrauchs-/Zustands-/Wärmeflussdaten (evtl. Eigentum Art. 14 GG)*	Hoher Wert (4)
Integrität der Datengruppen S2 *Irreführung durch Darstellung falscher Temperaturdaten*	Niedriger Wert (2)
Verfügbarkeit der externen Signale (Gruppe T) Nichtverfügbarkeit verhindert Steuerentscheidungen.	Hoher Wert (4)
Verfügbarkeit der Datengruppen Z,S,D Nichtverfügbarkeit verhindert Steuerentscheidungen.	Hoher Wert (4)
Vertraulichkeit des Zugangskennworts	Höchster Wert (5)

3.4.2 Sicht von Haushaltsmitgliedern

Zu schützendes Gut	Werteskala: 1 bis 5
Vertraulichkeit der Gerätezustände (Datengruppe Z) gegenüber Dritten. Ermöglicht Rückschlüsse auf das Verhalten von Haushaltsvorstand und -mitgliedern. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)*	Höchster Wert (5)

Zu schützendes Gut	Werteskala: 1 bis 5
Vertraulichkeit der Energieverbrauchsdaten (Datengruppe D) gegenüber Dritten. Ermöglicht Rückschlüsse auf das Verhalten von Haushaltsvorstand und -mitgliedern. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)*	Höchster Wert (5)
Vertraulichkeit der Stromsensordaten (Datum S1) gegenüber Dritten. Ermöglicht Rückschlüsse auf das Verhalten von Haushaltsvorstand und -mitgliedern. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)*	Höchster Wert (5)
Vertraulichkeit der Wärmefluss- und Temperatursensordaten (Datum S2 & S3) gegenüber Dritten. Ermöglicht grobe Rückschlüsse auf die Anwesenheit von Haushaltsvorstand und -mitgliedern. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)*	Hoher Wert (4)
Vertraulichkeit der Datengruppen Z, S1, D gegenüber dem Haushaltsvorstand Detaillierte Zustandsdaten erlauben Rückschlüsse auf anwesende Bewohner. *Gefahr der innerfamiliären Überwachung*	Mittlerer Wert (3) bis Hoher Wert (4)
Vertraulichkeit der Datengruppen S2, S3 gegenüber dem Haushaltsvorstand Temperatur- und Wärmeflussdaten lassen nur bedingt Rückschlüsse auf das Verhalten zu. *Gefahr der innerfamiliären Überwachung*	Niedriger Wert (2)
Integrität externer Signale (Gruppe T) *Finanzieller Schaden beim folgen falscher Tarifsignale (Eigentum Art. 14 GG)*	Höchster Wert (5)
Integrität der Daten Z, D, S1, S3 Bedingt möglicherweise eine Anpassung auf ungünstige Betriebsparameter von Geräten oder ungünstiges Verhalten von Haushaltsvorstand bzw. -mitgliedern. *Irreführung durch Darstellung von falschen Energieverbrauchs-/Zustands-/Wärmeflussdaten (evtl. Eigentum Art. 14 GG)*	Hoher Wert (4)
Integrität der Datengruppen S2 *Irreführung durch Darstellung falscher Temperaturdaten*	Niedriger Wert (2)

Zu schützendes Gut	Werteskala: 1 bis 5
Verfügbarkeit der externen Signale (Gruppe T) Nichtverfügbarkeit verhindert Steuerentscheidungen.	Hoher Wert (4)
Verfügbarkeit der Datengruppen Z,S,D Nichtverfügbarkeit verhindert Steuerentscheidungen.	Hoher Wert (4)
Vertraulichkeit des Zugangskennworts	Höchster Wert (5)

3.4.3 Sicht des Externen Verbrauchsvisualisierers

Zu schützendes Gut	Werteskala: 1 bis 5
Integrität der Datengruppen Z,S,D *Falsche Auswertungsergebnisse, evtl. Eigentumsinteressen (Art. 14 GG), Berufsfreiheit (Art. 12 GG)*	Hoher Wert (4)
Vertraulichkeit der Datengruppen Z,S,D *Reputationsverlust bei Bekanntwerden von Datenverlust, evtl. Eigentumsinteressen (Art. 14 GG), Berufsfreiheit (Art. 12 GG)*	Mittlerer Wert (3) bis Hoher Wert (4)
Vertraulichkeit des Zugangskennwörter	Mittlerer Wert (3) bis Hoher Wert (4)

3.4.4 Sicht des Energiemanagement Administrator

Zu schützendes Gut	Werteskala: 1 bis 5
Vertraulichkeit des Zugangskennwörter	Höchster Wert (5)

3.4.5 Sicht von Externen berechtigten Personen

Zu schützendes Gut	Werteskala: 1 bis 5
Vertraulichkeit der Datengruppen Z,S1,D Anwesenheit und Tätigkeit kann ermittelt werden. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) durch Gefahr der Überwachung*	Mittlerer Wert (3)
Vertraulichkeit der Datengruppen S2,S3 Anwesenheit kann möglicherweise über Temperaturdifferenzen ermittelt werden. *Gefährdung der Privatsphäre (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) durch Gefahr der Überwachung*	Niedriger Wert (2)

3.4.6 Sicht von Externen unberechtigten Personen

Zu schützendes Gut	Werteskala: 1 bis 5
-	-

3.5 Anwendungsarchitektur

Zur Analyse der Sicherheit wird zunächst die Anwendung in Form von Datenflussdiagrammen entworfen und modelliert. Im Entwurf setzt die beschriebenen Informationsflüsse (Abbildung 3.1) und die Funktionalen Anforderungen (Kapitel 3.3) um. Mit den Diagrammen werden Informations- bzw. Datenflüsse, daten-verarbeitende Prozesse, Datenspeicher und externe Entitäten modelliert. In der folgenden Tabelle sind die Elemente eines Datenflussdiagramms aufgelistet.

Element	Symbol	Bezeichnung
Externe Entität	Rechteck	Repräsentiert externe Datenquellen oder Datensenken für das modellierte System. Jede Entität außerhalb der Kontrolle der Applikation, wie Personen und externe Systeme.
Prozesse	Kreise	Eine Aktivität, Subsystem, Code oder Anwendung, die Daten transformiert oder verarbeitet.
Datenspeicher	Offene Rechtecke	Ruhende Daten, wie Registrierungsschlüssel, Datenbanken oder Dateien
Datenflüsse	Pfeile	Daten in Bewegung. Beschreibt, wie Daten zwischen Elementen fließen, z.B. Funktionsaufrufe und Netzwerkdaten.
Vertrauensgrenzen	Gestrichelte Linien	Beschreibt ein Punkt innerhalb der Applikation wo Daten von einem Level an Privilegien zu einem anderen wechseln, wie Netzwerksteckdosen, externe Entitäten und Prozesse mit verschiedenen Vertrauensstufen.

Im Kontextdiagramm (Abbildung 3.2) wird dargestellt, wie das betrachtete System mit den beschriebenen Rollen interagiert und welche Funktionen es denen bereitstellt. Im Datenflussdiagramm ergeben sich folgende Besonderheiten:

- Die Rollen Haushaltsvorstand und Haushaltmitglied sind als Entität „Haushaltsmiglied“ zusammengefasst, da das System dem Haushaltsvorstand keine zusätzlichen Funktionen bereitstellt.
- Eine Externe berechtigte Person werden verkürzt mit „Gast“ bezeichnet.
- Haushaltsmitglied und Gast können physisch direkt auf Haushaltsgeräte im System zugreifen. Das wird im Diagramm zur Vollständigkeit modelliert.

- Externe unberechtigte Personen werden nicht explizit modelliert, da sie keine Funktion des System nutzen dürfen.
- Der externe Widerspiegelungsdienstleister wird verkürzt als „Externer Speicher“ bezeichnet.

Zur Durchführung der Bedrohungsanalyse ist das Kontextdiagramm nicht detailliert genug. Erst wenn mehr Einzelheiten des Systems in einem „Ebene 0“-Datenflussdiagramm (siehe Abbildung 3.3) modelliert sind, können die Bedrohungen aufgezählt werden.

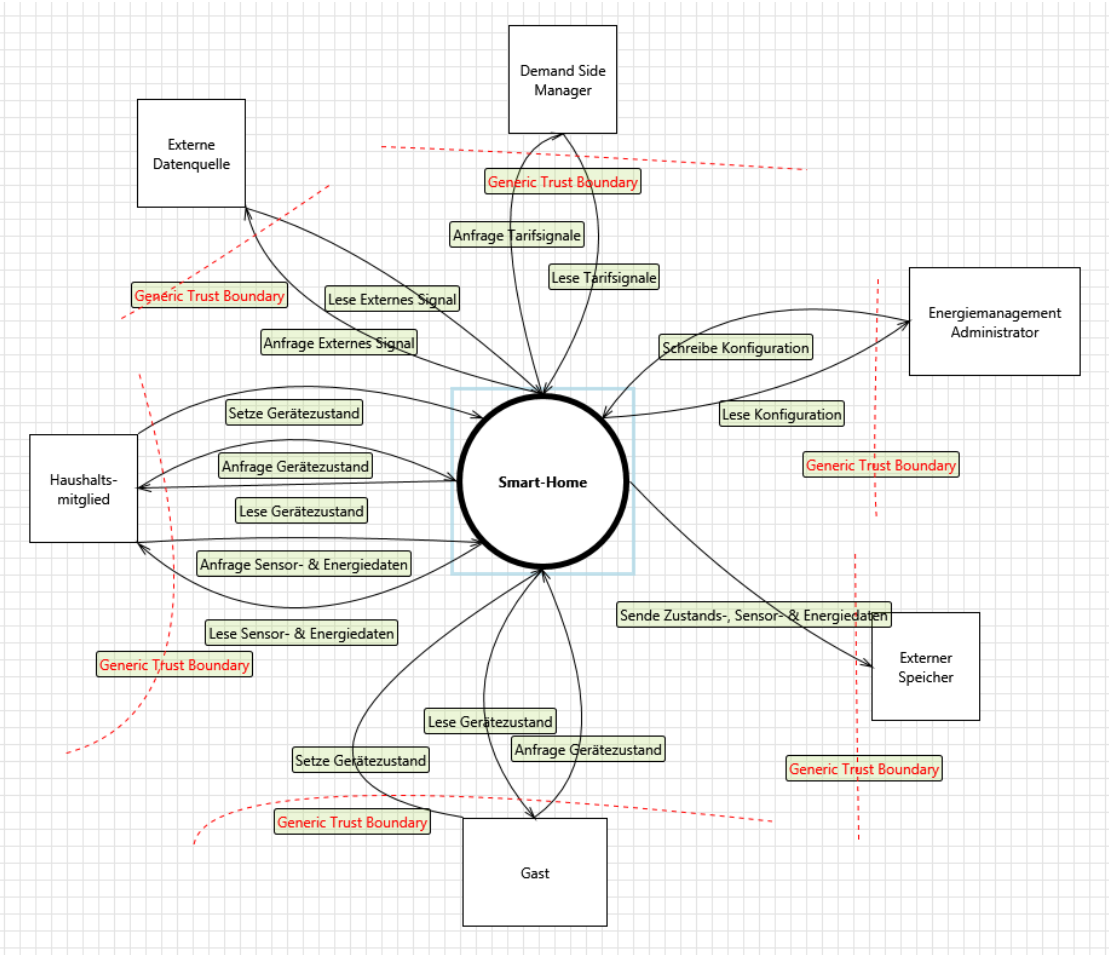

Abbildung 3.2: Datenflussdiagram des Einsatzkontexts des Smart-Home-Systems

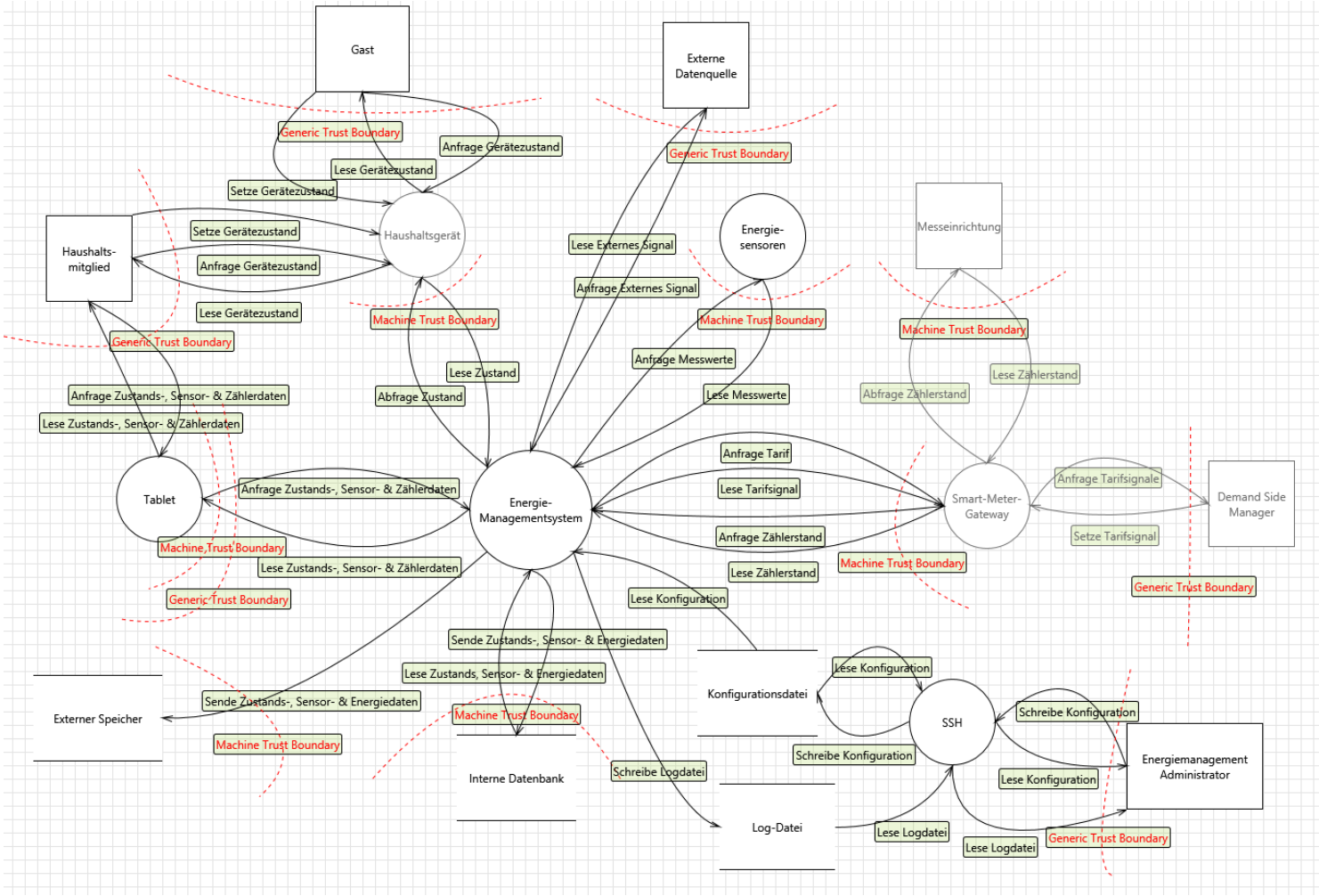

Abbildung 3.3: „Ebene 0“-Datenflussdiagram des Smart-Homes

Für spätere Referenzierungen werden im Folgenden alle Diagrammelemente aus Abbildung 3.3 aufgezählt:

Elementtyp	**Id**	**Bezeichnung**
Externe Entitäten	(1.0)	Haushaltsmitglied
	(2.0)	Gast
	(3.0)	Energiemanagementadministrator
	(4.0)	Demand Side Manager
	(5.0)	Messeinrichtung
Prozesse	(6.0)	Energiemanagementsystem
	(7.0)	Tablet
	(8.0)	Energiesensoren
	(9.0)	SSH
	(10.0)	Haushaltsgerät
	(11.0)	Smart-Meter-Gateway
Datenspeicher	(12.0)	Konfigurationsdatei
	(13.0)	Interner Speicher
	(14.0)	Externe Datenquelle
	(15.0)	Externer Speicher
	(16.0)	Log-Datei
Datenflüsse	(6.0 $\leftrightarrow$ 7.0)	Anfrage / Lese Zustands-, Sensor- & Energiedaten
	(6.0 $\leftrightarrow$ 8.0)	Anfrage / Lese Messwerte
	(6.0 $\leftrightarrow$ 10.0)	Abfrage / Lese Zustand
	(6.0 $\leftrightarrow$ 11.0)	Abfrage / Lese Tarifsignal
	(6.0 $\leftrightarrow$ 11.0)	Abfrage / Lese Zählerstand
	(6.0 $\leftrightarrow$ 13.0)	Lese / Schreibe Zustands-, Sensor- & Energiedaten
	(6.0 $\leftrightarrow$ 14.0)	Anfrage / Lese Externes Signal
	(6.0 $\rightarrow$ 15.0)	Sende Zustands-, Sensor- & Energiedaten
	(6.0 $\rightarrow$ 16.0)	Schreibe Logs
	(7.0 $\leftrightarrow$ 1.0)	Anfrage / Lese Zustands-, Sensor- & Energiedaten
	(9.0 $\leftrightarrow$ 3.0)	Lese / Schreibe Konfiguration
	(9.0 $\rightarrow$ 3.0)	Lese Logdatei
	(10.0 $\leftrightarrow$ 1.0)	Abfrage / Lese / Setze Zustand
	(10.0 $\leftrightarrow$ 2.0)	Abfrage / Lese / Setze Zustand
	(11.0 $\leftrightarrow$ 4.0)	Abfrage / Lese Tarifsignal
	(11.0 $\leftrightarrow$ 5.0)	Abfrage / Lese Zählerstand
	(12.0 $\leftrightarrow$ 9.0)	Lese / Schreibe Konfiguration
	(16.0 $\rightarrow$ 9.0)	Lese Logdatei

Elementtyp	Id	Bezeichnung
	(12.0 → 6.0)	Lese Konfiguration

3.5.1 Sicherheitsannahmen

Sicherheitsannahmen für einzelne Elemente im „Ebene 0“-Datenflussdiagramm werden nun hier spezifiziert. Die mit (*) markierten Eigenschaften dienen nur zum besseren Verständnis des Entwurfs und wirken sich nicht auf die spätere Analyse aus.

Energiemanagementadministrator (3.0)

- Annahme: Die Zugangsdaten des Energiemanagementadministrators sind ausschließlich ihm bekannt.

Energiemanagementsystem (6.0)

- Plattform (*): Mini-PC, x86_64, z.B. Intel NUC Kit DN2820FYKH
- Betriebssystem (*): Linux, CentOS 6.5
- Annahme: Kein besonderer physikalischer Schutz
- Laufzeitumgebung (*): Java OpenSDK 1.7.55
- Anwendung (*): Organic Smart Home 2.0 (managed Java)
- Verwendete Bibliotheken (*): u.a. Jetty 9.0
- Annahme: Alle Zugangsdaten sind in Klartext in der Konfigurationsdatei gespeichert.
- Annahme: Eine Fehlgeschlagene Energie-, Zustands- und Tarifdatenerfassung wird in dem Protokoll (16.0) notiert. Das Protokoll ist nur durch den Energiemanagementadministrator einsehbar. Die Erfassung wird zur nächsten Messperiode (in den meisten Fällen eine Sekunde später) wiederholt.
- Annahme: Die abgerufenen Daten jedes Haushaltsmitglieds werden im Protokoll (16.0) vermerkt.

Tablet (7.0)

- Plattform (*): Android-Tablet Nexus 7
- Betriebssystem (*): Android 4.3
- Annahme: Kein besonderer physikalischer Schutz
- Laufzeitumgebung (*): Firefox Mobile 30.0

Energiesensor (8.0)

- Plattform (*): Embedded System, ARM-basiert
- Betriebssystem (*): Linux 2.6
- Annahme: Kein besonderer physikalischer Schutz
- Anwendung (*): Unmanaged C-Code

SSH (9.0) Teilt sich selbe Plattform und Betriebssystem mit Energiemanagementsystem (6.0).

- Anwendung (*): OpenSSH 5.3 (unmanaged C-Code)
- Annahme: Passwortbasierte Authentifikation ist ausgeschaltet. D.h. nur die Authentifikation ist ausschließlich mit Public-Key-Verfahren möglich.

Haushaltsgerät (10.0)

- Plattform (*): Embedded System ARM-basiert
- Betriebssystem (*): Linux-stämmig
- Annahme: Kein besonderer physikalischer Schutz
- Laufzeitumgebung (*): Java / ProSyst mBS 5.3 (OSGi)
- Anwendung (*): Miele@Home 4.0.16
- Kommunikation: Haushaltsgerät gehört zur Klasse der „EMS-only Geräte“ (Abbildung 4.1).
- Annahme: Anwendungscode ist proprietär und nicht änderbar oder einsehbar.
- Annahme: Haushaltsgerät erlaubt keine Aktivierung, wenn das Gerät nicht vorher durch einen Benutzer „programmiert“ wurde. Beispielsweise kann ein Herd aus der Ferne nicht angeschaltet werden oder die Waschmaschine kann nicht gestartet werden, wenn physikalisch am Gerät kein Waschprogramm gewählt wurde.
- Annahme: Das Haus, indem das Gerät steht ist physikalisch adäquat gesichert.

Smart-Meter-Gateway (11.0)

- Annahme: Konform zu Common-Criteria-Schutzprofil SMGW-PP, Version 1.2
- Annahme: Konform zu BSI TR-03109, Version 1.0

Konfigurationsdatei (12.0)

- Annahme: Betriebssystem-ACL erzwingen, dass ausschließlich Energiemanagementadministrator (3.0) die Datei schreiben darf.
- Annahme: Betriebssystem-ACL erzwingen, dass nur Energiemanagementadministrator (3.0) und Prozess Energiemanagementsystem (6.0) die Konfigurationsdatei lesen können.

Interner Speicher (13.0) Teilt sich selbe Plattform und Betriebssystem mit Energiemanagementsystem (6.0).

- Anwendung (*): MySQL 5.5.38
- Bemerkung: Interner Speicher (13.0) bezieht sich auf eine gesonderte Datenbank.
- Annahme: DBMS enthält Authentifikationsinformationen und erzwingt die Authentifikation.
- Annahme: DBMS enthält Autorisationsinformationen und erzwingt die Autorisation.
- Annahme: DBMS schützt Authentifikations- und Autorisationsinformationen.
- Annahme: Ausschließlich der Prozess Energiemanagementsystem (6.0) darf schreiben und lesen.

Externe Datenquelle (14.0) Die externe Datenquelle wird als Webservice mit HTTP/REST-Interface mit XML-Antwort angenommen.

- Externe Datenquellen werden in der Konfigurationsdatei spezifiziert.
- TLS 1.2 wird für die Kommunikation eingesetzt.
- Der Domänenname des Webservices wird durch eine PKI überprüft. Die Standard-Root-CAs des Betriebssystems werden als vertrauenswürdig erachtet.
- Eine fehlgeschlagende Zertifikatsprüfung wird im Protokoll notiert. Nach einer Stunde wird eine erneute Abfrage gestartet.

Datenfluss zwischen Energiemanagementsystem und Energiesensoren (6.0) $\leftrightarrow$ (8.0)

- Übertragung der Messwerte im XML-Format.
- Energiemanagementsystem registriert sich bei Energiesensor für regelmäßiges Versenden der aktuellen Messwerte.
- Regelmäßig bedeutet ein Datenpaket mit allen verfügbaren Messwerten pro Sekunde.
- Falls 10 Sekunden kein Datenpaket eintrifft, wird das Fehlen in der Log-Datei notiert und ein Registrierungsversuch wird gestartet.
- Kanal wird über DTLS 1.2 geschützt.
- Gegenseitige Authentifikation mit einer der im Kommunikationsgrobentwurf genannten Methoden: Zertifikate, Priv/Pub Key, symmetrische Schlüssel

Datenfluss zwischen Energiemanagementsystem und Haushaltsgerät (6.0) $\leftrightarrow$ (10.0)

- HTTP/REST-Abfrage mit XML-Antwort.
- HTTPS mit TLS 1.2.
- Authentifikation des Energiemanagements mit HTTP-Basic-Authorization.
- Authentifikation des Haushaltsgeräts mit einer der im Kommunikationsgrobentwurf genannten Methoden: Zertifikate, Priv/Pub Key, symmetrische Schlüssel.

Datenfluss zwischen Energiemanagementsystem und interne Datenbank (6.0) $\leftrightarrow$ (13.0)

- Die Kommunikation läuft unverschlüsselt über ein Unix-Socket, der durch einen Dateinamen identifiziert wird.
- Annahme: Der Zugriffsschutz des Betriebssystems schützt den Socket vor Veränderung, indem ausschließlich Energiemanagementsystem und interne Datenbank darauf zugreifen dürfen.

Datenfluss zwischen Haushaltsmitglied und Haushaltsgerät (1.0) $\leftrightarrow$ (10.0) Dies beschreibt den Grenzfall, wenn ein Haushaltsmitglied physikalisch mit dem Haushaltsgerät interagiert oder innerhalb des Hauses direkt mit einem beliebigen Endgerät auf die Haushaltsgeräte zugreifen möchte.

- EMS-only Geräte sind über einem Netzwerk dem Haushaltsmitglied oder dem Gast nicht zugänglich, siehe Abbildung 4.1.

Datenfluss zwischen Energiemanagementadministrator und SSH (3.0) $\leftrightarrow$ (9.0)

- Der Energiemanagementadministrator kennt den Host-Schlüssel des SSH-Dienstes.
- Authentifikation des Energiemanagementadministrators erfolgt mittels Public-Key-Verfahren. Der öffentliche Schlüssel des Energiemanagementadministrators ist dem SSH-Dienst bekannt.
- Annahme: Nur der Energiemanagementadministrator kennt seinen privaten Schlüssel.

3.5.2 Sicherheitshinweise

Es folgen Sicherheitshinweise, die von den Rollen des Systems bei Einrichtung und Betrieb zu achten haben. Die spätere Analyse setzt die Einhaltung dieser Sicherheitshinweise voraus.

- Gut gewählte Zugangsinformationen für das Energiemanagementsystem sollen beim Haushaltsgerät hinterlegt werden.
- Haushaltsgerät muss bei der Installation ein selbst-signiertes Zertifikat generieren. Das Zertifikat wird vom Energiemanagementadministrator in die Konfiguration eingetragen.
- Falls der Energiemanagementalgorithmus auf externe Daten zugreift, muss der Kommunikationskanal zu der Quelle dieser Daten durch TLS (HTTPS) gesichert sein.
- Haushaltsmitglieder haben keinen direkten Zugriff auf EMS-only Haushaltsgeräte. Sollte das Gerät erreichbar erscheinen, ist das eine Fehlkonfiguration oder ein Angriff. In jedem Fall ist der Quelle nicht zu vertrauen.
- Das Schlüsselmaterial zum Authentifizieren des Energiemanagementsystems muss im Energiesensor konfiguriert sein.
- Das Schlüsselmaterial der Energiesensoren müssen in der Konfigurationsdatei des Energiemanagementsystems beschrieben werden.
- Der Energiemanagementadministrator kennt den Host-Schlüssel des SSH-Dienstes und unterlässt bei fehlgeschlagenem Schlüsselabgleich jegliche weitere Handlung.

3.6 Kommunikationsarchitektur

Ein Ziel der Arbeitsgruppe *Intelligente Infrastrukturen und Energie* war, eine sichere Smart-Home-Architektur zu entwerfen, die einerseits aktuelle Entwicklungen in der Funktionsvielfalt eines Smart-Home nicht einschränkt und andererseits sichere Kommunikation verschiedener Smart-Home-Anwendungen ermöglicht. Für die Kommunikationssicherheit wurden aktuelle Arbeiten und Protokolle aus dem Standardisierungsprozess der IETF (Home Networking Working Group) [4] hinsichtlich Sicherheit und Funktionalität untersucht und wo passend, in die Smart-Home-Architektur eingebunden. Beim Entwurf der prototypischen Smart-Home-Architektur wurden aktuelle gesetzliche Vorgaben sowie Schutzprofile und die Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [1, 2] für die Sicherheit von Smart-Meter-Systemen berücksichtigt und auf ihre Tauglichkeit in dem hypothetischen Gesamtszenario untersucht.

3.6.1 Annahmen

Im folgenden werden die Annahmen beschrieben und begründet, auf denen der Grobentwurf der Kommunikationsarchitektur basiert.

- Unterschiedliche Schicht-2 Protokolle, vergleiche Abbildung 3.5. Beispiele: Ethernet 802.3, WLAN 802.11agn, IEEE 802.15.4. Es ist in Smart-Homes von stark heterogenen Netzen auszugehen, sodass die Geräte über unterschiedliche Kommunikationsschnittstellen verfügen und daher über unterschiedliche physikalische Medien mit dem Smart-Home-Netz verbunden werden müssen.

- Wir nehmen an, dass alle Geräte den IPv6-Standard vollständig unterstützen. Aufgrund der Vielzahl an Geräten und der bereits ausgegangenen IPv4-Adressen erscheint IPv6 hier als einzig zukunftssichere Lösung.

- Auf den Einsatz von DNS(SEC) wird verzichtet. DNS(SEC) würde den administrativen Aufwand für das Smart-Home-Netz so erhöhen, dass dieser für Normalverbraucher als unrealistisch eingestuft wird.

- Keine Untersuchung von verschiedenen Schlüsselmanagement-Aspekten im Rahmen der Bedrohungsanalyse. Es wird davon ausgegangen, dass Endgeräte notwendige Schlüssel besitzen. Es können beispielsweise Zertifikate, asymmetrische oder symmetrische Schlüssel zum Authentifizieren der Geräte und für Verschlüsselung genutzt werden.

- Keine nähere Betrachtung von QoS-Mechanismen im Smart-Home. QoS-Mechanismen können der Separation von Verkehr dienen, und so z.B. DoS-Angriffe auf Teile des

Smart-Homes abwehren. Aufgrund der zusätzlichen Komplexität soll zunächst darauf verzichtet werden.

- Im Grobentwurf wird kein Intrusion Detection System (IDS) vorgesehen.
- Es wird angenommen, dass das Smart-Meter-Gateway (SMG) die Schutzprofile des BSI umsetzt. Die Sicherheit des Smart-Meter-Gateways selbst wird nicht betrachtet.
  - Richtlinien des BSI decken nicht vollständig die Smart-Home-Sicherheit ab, sondern beschränken sich auf die Sicherheit des Smart-Homes als Energiemarktteilnehmer.
  - Zugriff auf Smart-Home interne Geräte (Controllable Local Systems (CLS)) über SMG wird betrachtet.
  - Es wird angenommen, dass SMG IPv6 fähig ist und als TLS-Proxy für den Zugriff anderer Energiemarktteilnehmer auf die CLS funktioniert.
- Potentielle Angreifer können sich sowohl im als auch außerhalb des Smart-Homes befinden. Es wird demnach von internen und externen Angriffen ausgegangen. Interne Angreifer können insbesondere Geräte im Haus korrumpieren und eigene Geräte mitbringen und integrieren.

3.6.2 Entwurfsentscheidungen

In diesem Kapitel werden grundlegende Entwurfsentscheidungen beschrieben, die für die Kommunikationsarchitektur getroffen wurden und auf den Annahmen aus Abschnitt 3.6.1 basieren.

Bei den Geräten wird zwischen EMS-only Geräten und Geräten mit einer Anbindung an das Internet unterschieden, sodass die EMS-only Geräte sich in der EMS-Sicherheitszone befinden und dementsprechend vertrauenswürdiger sind, da sie keine weiteren direkten Kommunikationsverbindungen haben außer zum EMS.

Unter Beachtung der BSI Schutzprofile und der entsprechenden technischen Richtlinien gibt es Geräte im Smart-Home die von einem externen Marktteilnehmer (EMT) über ihren Zustand abgefragt oder auch gesteuert werden können.

3.6.2.1 Einschränkung der Kommunikation

Es wird zwischen Funktionalen Domänen und Sicherheitszonen unterschieden:

Funktionale Domänen Eine funktionale Domäne beinhaltet Komponenten des Smart-Home-Systems die gemeinsam eine bestimmte Funktion 3.3.3 erfüllen.

Sicherheitszonen Das Smart-Home ist in Sicherheitszonen unterteilt die einen unterschiedlichen Schutzbedarf aufweisen. Die Sicherheitszonen sind in Abbildung 3.4 dargestellt.

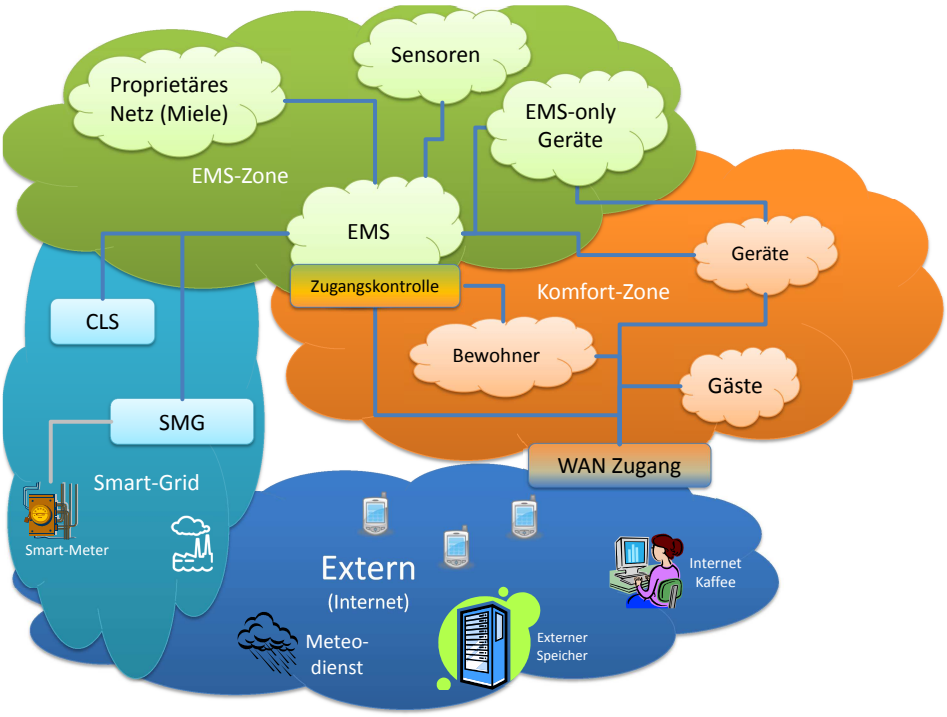

Abbildung 3.4: Sicherheitszonen im Szenario Smart-Home

Funktionale Domänen können sich über mehrere Sicherheitszonen erstrecken und umgekehrt. Zonenübergänge müssen kontrolliert erfolgen. Der Router des Energiemanagementsystems (EMS-Router) spielt dabei eine zentrale Rolle. Sicherheitszonen sind somit orthogonal zu dem Domänenmodell und physischer Topologie.

Die Kontrolle bzw. die Einschränkungen der Kommunikation erfolgt durch folgende Maßnahmen:

- Lokale Firewallregeln im Endsystem
- Firewall auf dem EMS-Router
- Firewall auf dem Smart-Home Edge Router (z.B. ein DSL-Router)

- Subnetze, Adressvergabe
- Trennung der Kommunikation bereits im Switch (VLANs) wäre wünschenswert, wird jedoch im Grobentwurf nicht umgesetzt. Kommunikation zwischen verschiedenen Sicherheitszonen muss demnach über den EMS Router erfolgen.

3.6.2.2 Routing

Beim Routing wird intern und extern einheitlich IPv6 eingesetzt, da es als zukunftssicher gilt und auch für Kleinstgeräte (z.B. Sensornetze) in Form von 6LowPAN verfügbar ist.

- Per default wird keine globale IPv6 Adresse vergeben. Die Adressvergabe intern basiert auf Unique Local Adresses (ULAs). Die Abbildung der Adressen erfolgt hierbei über Sicherheitszonen, ähnlich der HomeNet Architektur [3, Sec. 2.4]:

  > A home network running IPv6 should deploy ULAs alongside its globally unique prefix(es) to allow stable communication between devices (on different subnets) within the homenet where that externally allocated globally unique prefix may change over time, e.g., due to renumbering within the subscriber's ISP, or where external connectivity may be temporarily unavailable.
  >
  > In the case where home automation networks are being set up in a new home/deployment (as early as during construction of the home), such networks will likely need to use their own /48 ULA prefix. Depending upon circumstances beyond the control of the owner of the homenet, it may be impossible to renumber the ULA used by the home automation network so routing between ULA /48s may be required. Also, some devices, particularly constrained devices, may have only a ULA (in addition to a link- local), while others may have both a GUA and a ULA.

- Multi-Homing möglich: Nur intern kommunizierende Geräte verwenden ULAs. Extern kommunizierende Geräte bekommen zusätzlich eine globale IPv6 Adresse. Dies macht die Nutzung verschiedener VLANs und VLAN-Tagging ggf. überflüssig.

  Homenet-Architektur:

  > When an IPv6 node in a homenet has both a ULA and a globally unique IPv6 address, it should only use its ULA address internally, and use its additional globally unique IPv6 address as a source address for external communications.
  >
  > Devices in a homenet may be given only a ULA as a means to restrict reachability from outside the homenet. ULAs can be used by default for devices that, without additional configuration (e.g., via a web interface), would only offer services to the internal network.

- Kein Einsatz von IPsec im Grobentwurf.
  - Die Konfiguration von IPsec ist nur von einem Netzwerkadministrator bzw. mit entsprechenden Kenntnissen möglich.
  - Schlüsselmanagement für Schlüsselnutzung in IPsec ist nicht Teil von IPsec und stellt somit eine Anforderung von IPsec dar, die jedoch im Grobentwurf im Rahmen der Bedrohungsanalyse nicht betrachtet wird.
  - Du es keine Konfigurations- bzw. Informationsschnittstelle zwischen IPsec und der Anwenung gibt, ist IPsec unflexibler aus Sicht der Anwendung als Sicherung auf Transportschicht mit z.B. (D)TLS.

3.6.2.3 Adressvergabe

Es wird kein Protokoll zur automatischen Konfiguration von Hosts (z.B. DHCP) vorgesehen. Es wird demnach auf DHCPv6 verzichtet. Ein DHCPv6-Server kann Ziel eines Angriffs sein und somit weitere Angriffe ermöglichen (Maskerade, Man-in-the-middle, usw.). Die Adresskonfiguration Smart-Home-Intern erfolgt mit SLAAC (Stateless Address Auto Configuration).

- Adressvergabe (vor allem der Präfixe) erfolgt nur durch EMS-Router und Smart-Home Edge Router (z.B. Fritzbox).
- Adressvergabe erfolgt statisch, d.h. die Geräte bekommen immer gleiche Präfixe zugewiesen und suchen sich immer die gleiche Adresse in dem vorgegebenen Adressbereich aus.
- Beim Einfügen eines Gerätes in das Smart-Home-Netz entscheidet der Haushaltsvorstand (sieht 3.1) in welches Subnetz das Gerät eingefügt werden soll und u.U. welche genaue Adresse es bekommen soll. Die entsprechende Konfiguration der Router und des einzufügenden Gerätes wird anschließend vom Energiemanagement-Administrator (siehe 3.1) vorgenommen.

3.6.2.4 Transportprotokolle

Nach Möglichkeit wird auf Transportschicht das UDP-Protokoll verwendet. TCP soll nur wenn unbedingt notwendig eingesetzt werden, denn es bringt an vielen Stellen unnötige Komplexität mit sich.

Gründe für Nutzung von UDP statt TCP sofern möglich:

- TCP-Mechanismen zur Fluss- und Staukontrolle sowie übrige Zustandshaltung bieten Angriffsmöglichkeiten. Durch Nutzung von UDP werden Angriffe auf TCP Mechanismen ausgeschlossen.

- Für Sensorknoten ist UDP wegen Ressourceneinschränkungen besser geeignet, da es ressourcenschonender ist als TCP.

Die Absicherung des Transports erfolgt durch (D)TLS mit Authentizitäts-, Integritätsschutz und Verschlüsselung. Geräte müssen sich somit beim Aufbau einer (D-)TLS Session authentifizieren. Alles Notwendige für einen (D)TLS Verbindungsaufbau wie beispielsweise Schlüsselmaterial wird als vorhanden angenommen.

3.6.2.5 Schicht-2 Topologie

Die Abbildung 3.5 zeigt den Entwurf einer Schicht-2 Topologie welcher konform zu den Annahmen und den beschriebenen Designentscheidungen sowie der geforderten Funktionalität ist.

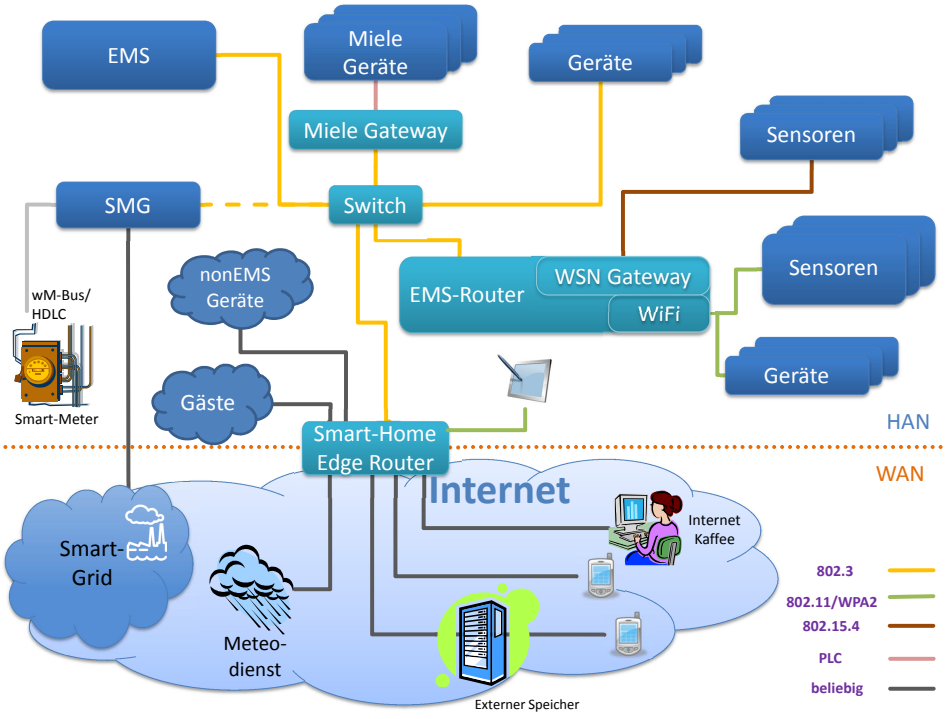

Abbildung 3.5: Schicht-2 Netzarchitektur

3.6.3 Funktionale Domänen

Im Smart-Home wird zwischen folgenden funktionalen Domänen unterschieden:

Stromzählerstände EMS fragt Stromzählerstände vom SMG ab. Die Stände kommen dabei vom Smart-Meter.

Zustandsdaten EMS sammelt Zustandsdaten der Geräte.

Energiesensoren EMS sammelt Sensordaten der Energiesensoren.

Tarifsignale EMS fragt Tarifsignale vom SMG ab. Die Signale kommen dabei aus dem Smart-Gird.

Externe Signale EMS fragt verschiedene energetisch relevante Informationen (z.B. meteorologische Daten) von Anbietern im Internet ab.

Datenhaltung intern EMS speichert die Daten in einer internen Datenbank.

Datenhaltung extern EMS speichert die Daten auf einem externen Server bzw. in der Cloud.

Interner Zugriff (Datenhaltung auf EMS) Informationstablet fragt Daten zur Anzeige vom EMS ab.

Interner Zugriff (Datenhaltung extern) Informationstablet fragt Daten zur Anzeige vom externen Server ab.

Externer Zugriff (Datenhaltung auf EMS) Ein externes Gerät im Internet greift auf das EMS zu über ein Webinterface.

Externer Zugriff (Datenhaltung extern) Ein externes Gerät im Internet fragt Daten von dem externen Server bzw. der Cloud ab.

3.6.4 F1: Darstellen im Vorfeld einer Steuerentscheidung, die eine gesamtenergetische Betrachtung erfordert

Im Folgenden werden zu jeder Funktion aus dem Abschnitt 3.3.3 die beteiligten Komponenten des Smart-Home-Systems aufgezählt, sodass der Informationsfluss jeder Funktion im Smart-Home nachvollzogen werden kann.

F1 b: Darstellen im privatdispositiven Bereich

F1 b DD: Stromzählerstände

Beteiligte Komponenten:

- Messeinrichtung (Smart-Meter)
- Smart-Meter-Gateway (SMG)
- Energiemanagement (EMS)

- EMS Switch
- EMS Router

F1 b DZ: Zustandsdaten

Beteiligte Haushaltskomponenten:

- Drahtgebundene Geräte: Switch
- Drahtlose Geräte: Kommunizieren direkt mit den Funkschnittstellen des EMS-Routers
- Proprietär kommunizierende Geräte (z.B. PLC von Miele): Entsprechendes Gateway
- Energiemanagement (EMS)
- EMS Switch
- EMS Router

F1 b DS: Sensordaten von Energiesensoren

Beteiligte Haushaltskomponenten:

- Sensoren
- Energiemanagement (EMS)

F1 b DT: Signale vom Smart-Meter-Gateway Die Signale kommen aus dem Smart-Grid zum SMG.

Beteiligte Haushaltskomponenten:

- Smart-Meter-Gateway (SMG)
- Energiemanagement (EMS)
- EMS Switch
- EMS Router

F1 b DE: Externe Signale Die Signale kommen aus dem Internet von diversen Anbietern.

Beteiligte Haushaltskomponenten:

- Externe Anbieter
- Energiemanagement (EMS)
- EMS Switch
- EMS Router
- DSL Router

F1 b S: Datenhaltung intern

Beteiligte Haushaltskomponenten:

- Energiemanagement (EMS)

Für die Datenhaltung in der internen Datenbank ist keine Kommunikation notwendig da die Datenbanksoftware auf dem gleichen Endsystem läuft wie das Organic Smart Home.

F1 b S: Datenhaltung extern

Beteiligte Haushaltskomponenten:

- Externer Server
- Energiemanagement (EMS)
- EMS Switch
- EMS Router
- DSL Router

F1 b Z: Datenzugriff

Beteiligte Komponenten - interner Zugriff (Datenhaltung auf EMS):

- Informationstablet
- Energiemanagement (EMS)
- EMS Router

Beteiligte Komponenten - interner Zugriff (Datenhaltung auf externem Server):

- Informationstablet
- Externer Server
- EMS Switch
- EMS Router
- DSL Router

Beteiligte Komponenten - externer Zugriff (Datenhaltung auf EMS):

- SmartPhone
- Energiemanagement (EMS)
- EMS Switch
- EMS Router
- DSL Router

Beteiligte Komponenten - externer Zugriff (Datenhaltung auf externem Server):

- SmartPhone
- Externer Server
- Das Internet

4 Bedrohungsanalyse

4.1 Angreifermodell

Die Entwicklung sicherer Systeme in allen Bereichen der Kommunikation erfordert eine gründliche und konsistente Definition des Wortes *Sicherheit*. Der Begriff der Sicherheit ist direkt abhängig vom Begriff des *Angreifers*. In Szenarien ohne Angreifer ist jedes funktionierende System „sicher“. Tritt jedoch eine Entität hinzu, welche versucht, ein *unbefugtes* Ziel zu erreichen, muss ein sicheres System in der Lage sein, dieser Entität das Erreichen ihres Ziels zu versagen. Ein Ziel ist unbefugt, wenn es im Sinne des Betreibers des (Kommunikations-)Systems verwehrt bleibt – wenn also seitens des Betreibers das Bestreben vorhanden ist, das Erreichen des Ziels unmöglich zu machen.

Eine solche Entität, die in einem System versucht, unbefugte Ziele zu erreichen, wird als *Angreifer* bezeichnet. Ein Angreifer wird also zum Einen darüber definiert, welche *Ziele* er erreichen will. Zum Anderen muss klar herausgestellt werden, welche *Mittel* ihm hierzu zur Verfügung stehen. Ein Angreifer, welcher keine Mittel hat, um ein von ihm gewünschtes Ziel zu erreichen, ist der triviale schwache Angreifer, von dem keinerlei Bedrohung ausgeht. Somit lässt sich der Begriff des Angreifers auf das Vorhandensein von unbefugten Zielen und zur Verfügung stehenden Mitteln zurückführen.

Im obigen Sinne ist ein System also *sicher*, wenn es einem zuvor bestimmten Angreifer das Erreichen seiner Ziele verwehrt.

Der folgende Abschnitt des vorliegenden Dokuments befasst sich mit der Erfassung von Angreifern im Smart Home in einem generischen Angreifermodell. Dazu werden zunächst allgemeine Eigenschaften eines Angreifers festgehalten; daraufhin wird auf Eigenschaften von Angreifern eingegangen, die speziell im Smart Home von zusätzlicher Bedeutung sind. Abschließend werden in Abschnitt 4.1.3 Merkmale von Angreifern genannt, die verschieden starke Angreifer differenzieren lassen.

4.1.1 Allgemeine Eigenschaften eines Angreifers

Häufig wird in der wissenschaftlichen Literatur ein bestimmter Angreifer implizit angenommen. Dabei handelt es sich um den sogenannten *Dolev-Yao* oder *Man-in-the-Middle*-Angreifer , dessen Mittel und Einschränkungen im Folgenden beschrieben sind. Dazu wird zunächst in Abschnitt 4.1.1.1 auf seine Fähigkeiten eingegangen; die Einschränkungen des Dolev-Yao-Angreifers sind in Abschnitt 4.1.1.2 beschrieben.

4.1.1.1 Allgemeine Mittel

Unter den Mitteln, die ein Angreifer zur Verfügung hat, um seine Ziele zu erreichen, wird die Gesamtheit seiner Fähigkeiten verstanden. Diese sind nachfolgend erfasst und erläutert.

Globalität Zunächst einmal ist der Dolev-Yao-Angreifer ein *global* agierender Angreifer. Das bedeutet insbesondere, dass von Seiten des Entwicklers eines Systems angenommen werden muss, dass der Angreifer überall im Netz präsent sein könnte; in diesem Zusammenhang wird auch von der Omnipräsenzeigenschaft des Dolev-Yao-Angreifers gesprochen. Dabei bedeutet der Begriff *omnipräsent*, dass der Angreifer Zugriff auf sämtliche im Netz ausgetauschten Nachrichten hat. Er ist jedoch i.A. nicht in der Lage, die Kommunikationsparteien bzw. -systeme zu kompromittieren.

Kollaboration Ein Angreifer als Entität, die in einem Kommunikationsnetz versucht, unbefugte Ziele zu erreichen, ist dort durch seine Instanzen – abstrakte Komponenten, die seine Mittel repräsentieren und einsetzen – vertreten. Der Dolev-Yao-Angreifer besitzt die Eigenschaft der *instantanen Kollaboration*; das bedeutet, Wissen, das bei einer Instanz vorhanden ist, ist instantan auch bei allen anderen Instanzen des Angreifers vorhanden. Dazu benötigt der Dolev-Yao-Angreifer keine explizite Kommunikation über das angegriffene Netz. Es wird angenommen, dass zur Zusammenarbeit der Angreiferinstanzen ein irgendwie gearteter separater Kanal genutzt wird.

Abhörfähigkeit Unter der Abhörfähigkeit eines Angreifers wird dessen Fähigkeit verstanden, durch lesenden Zugriff auf das Kommunikationsmedium Wissen über die stattfindenden Kommunikationsprozesse zu erlangen. Im Falle des Dolev-Yao-Angreifers wird insbesondere durch dessen Omnipräsenz angenommen, dass der Angreifer sämtliche Kommunikation des angegriffenen Systems mithören kann. Das bedeutet, er hat Zugang zu allen einem Kommunikationsvorgang zugeordneten Informationen. Dies sind im Einzelnen: Informationen über die beteiligten Kommunikationspartner, Informationen zu Zeit und Ort des Kommunikationsvorgangs und die übermittelten Inhalte.

Injektionsfähigkeit Injektionsfähigkeit bezeichnet die Fähigkeit des Angreifers, Nachrichten beliebigen Inhalts zu erzeugen und in das Kommunikationsmedium einzuspielen. Dazu verschafft sich der Angreifer schreibenden Zugriff auf das eingesetzte Medium. Insbesondere kann der Angreifer auch Nachrichten mit gefälschtem Sender-Identifikator – beispielsweise mit gefälschter Geräteadresse – erzeugen und sich so als legitimer Teilnehmer des Kommunikationsnetzes ausgeben. Dieses spezielle Verhalten wird auch mit dem Begriff *Maskerade* bezeichnet.

Manipulationsfähigkeit Der Begriff Manipulationsfähigkeit bezeichnet die Fähigkeit eines Angreifers, durch schreibenden Zugriff auf das Medium kommunizierte Inhalte während der übermittlung zu verändern. Er ist insbesondere auch in der Lage, Nachrichten so zu verändern, dass sie nicht mehr als Nachrichten erkannt werden können und somit effektiv „gelöscht“ werden. Dabei handelt es sich jedoch nicht um eine physikalische Löschung der Nachricht auf dem Medium. Eine solche echte Löschung ist nicht möglich. Manipulationsfähigkeit und Injektionsfähigkeit unterscheiden sich darin, dass bei der Manipulation bestehende Inhalte während des Transits überschrieben werden, während bei der Injektion neue Inhalte erzeugt werden. Insbesondere beinhaltet die Manipulation *keine* Initiierung von Kommunikationsvorgängen.

4.1.1.2 Allgemeine Einschränkungen

Neben den im vorangegangenen Abschnitt erläuterten Fähigkeiten, ist der Dolev-Yao-Angreifer in Bezug auf gegebenenfalls eingesetzte kryptografische Bausteine – das heißt insbesondere Schlüsselmaterial und Einweg-Hashfunktionen, sowie kryptographische Funktionen und durch sie erzeugte Nachrichtenteile – eingeschränkt wie nachfolgend beschrieben.

Polynomiale Gebundenheit Darunter wird verstanden, dass der Angreifer nicht in der Lage ist, in polynomialer Zeit Schlüsselmaterial zu erraten. Das bedeutet, dass er verschlüsselte Inhalte nicht lesen kann und Signaturen oder Message Authentication Codes nicht fälschen kann, wenn er den zugehörigen Schlüssel nicht kennt. Er ist des Weiteren nicht in der Lage, aus dem Funktionswert einer kryptographischen Hashfunktion auf deren Eingabewert zu schließen. Dies bedeutet implizit, dass die eingesetzten kryptographischen Funktionen „perfekt“ sind, also keine Schwächen aufweisen, die den Angreifer in die Lage versetzen, einen ihm unbekannten Schlüssel oder Eingabewert einer Hashfunktion effizient zu erraten.

In den beiden Abschnitten 4.1.1.1 und 4.1.1.2 wurden die grundlegenden Fähigkeiten und Einschränkungen des in der Literatur gängigen allgemeinen Dolev-Yao-Angreifers zusammengefasst und definiert. Der folgende Abschnitt 4.1.2 befasst sich mit zusätzlichen Mitteln und Einschränkungen eines Angreifers in Smart-Home-Szenarien.

4.1.2 Smart-Home-Spezifische Eigenschaften eines Angreifers

Der in Abschnitt 4.1.1 beschriebene Angreifer trägt den Möglichkeiten Rechnung, die in Szenarien in klassischen Netzen gegeben sind. Allerdings bieten typische Smart Home =Szenarien Angreifern noch zusätzliche Möglichkeiten, in Erscheinung zu treten, die durch das obige Modell nicht abgedeckt sind. Dies resultiert in zusätzlichen Fähigkeiten, die einem Angreifer in einem Smart Home zugestanden werden müssen; diese Fähigkeiten werden in Abschnitt 4.1.2.1 genannt und erläutert.

Es gibt allerdings auch Faktoren, die die Handlungsfähigkeit eines Angreifers in Smart Home-Szenarien einschränken können. Darauf wird in Abschnitt 4.1.2.2 eingegangen.

4.1.2.1 Smart-Home-Spezifische Fähigkeiten eines Angreifers

Durch den für viele Szenarien und Einsatzbereiche typischen Umstand, dass Komponenten im Smart Home unter Umständen frei zugänglich sind, ergeben sich für einen Angreifer weitere Mittel, die Funktion des angegriffenen Netzes zu beeinträchtigen. Diese sind im Folgenden beschrieben.

Zerstörung von Komponenten Durch die Zugänglichkeit der Komponenten in vielen Einsatzbereichen besteht die Gefahr, dass ein Angreifer die ungeschützten Komponenten gewaltsam zerstört. Die zerstörte Komponente fällt somit dauerhaft aus.

Zugriff auf Datenspeicher Sind Komponenten physisch zugänglich, kann der Angreifer die auf den Komponenten gespeicherten Daten auslesen und gegebenenfalls überschreiben. Dies beinhaltet auch auf den betreffenden Komponenten gespeichertes Schlüsselmaterial. Somit kann der Angreifer durch Auslesen des Datenspeichers Kenntnis über die kryptographische Geheimnisse erlangen. In diesem Zusammenhang wird von *korrumpiertem Schlüsselmaterial* gesprochen.

Zugriff auf Programmspeicher Neben dem Datenspeicher ist es auch möglich, dass der Programmspeicher einer Komponente einem Angreifer zum Opfer fällt. Der physische Zugriff ermöglicht dem Angreifer die Reprogrammierung der betreffenden Komponenten. In diesem Zusammenhang wird von *korrumpierten Komponenten* gesprochen. Das Korrumpieren einer Komponente kann als solches nicht erkannt werden, da sie sich auf unbestimmte Zeit völlig protokollkonform verhalten kann und sich in dieser Zeit nicht als korrumpierte Komponente zu Erkennen geben muss. In diesem Fall spricht man vom *byzantinischen* Verhalten korrumpierter Komponenten.

Zugriff auf Sensorik Weniger aufwändig als das Manipulieren oder Auslesen des Speichers einer Komponente ist häufig der Zugriff auf die Sensorik. Dies ist der Tatsache geschuldet, dass Sensoren naturgemäß der Umwelt ausgeliefert sein müssen, um die benötigten Daten zu erfassen. Gelingt es einem Angreifer, den Sensor-Input zu manipulieren, kann er damit die Daten fälschen, die im Smart Home verarbeitet werden, ohne auf das Medium zur Manipulation oder Injektion von Nachrichten zugreifen zu müssen.

Abschirmen einzelner Komponenten Sind einzelne Komponenten drahtlos an das System angebunden, so kann ein Angreifer versuchen, bestimmte Knoten im Netz abzuschirmen. Dies kann er durch gezieltes *Jamming* des genutzten Funkkanals erreichen.

Die betroffenen Komponenten können dann keine Nachrichten mehr empfangen, solange der Kanal nicht wieder freigegeben ist.

Erschöpfen der Energieressourcen Die zur Verfügung stehende Energie ist eine der kritischsten Ressourcen für viele Komponenten im Smart Home. Die Energieversorgung dieser Komponenten wird nur durch Batterien, selten durch alternative Stromquellen wie beispielsweise Solarzellen, gewährleistet. Dadurch ist Energie für diese Komponenten nur in beschränktem Umfang vorhanden. Das wiederholte bzw. andauernde Erzwingen von Sende- und Empfangsvorgängen, sowie von rechenintensiven Code-Ausführungen durch den Angreifer kann auf Dauer zur Erschöpfung des Energievorrats und damit zum Ausfall der betroffenen Komponenten führen. Zur Durchführung dieses Angriffs bedient sich der Angreifer seiner in Abschnitt 4.1.1.1 genannten Fähigkeiten und Mittel.

4.1.2.2 Smart-Home-Spezifische Einschränkungen eines Angreifers

Neben spezifischen Mitteln, die einem Angreifer in einem Smart Home zur Verfügung stehen, können aus der Tatsache, dass es sich bei dem angegriffenen Kommunikationsnetz um ein Smart Home-Netz handelt, auch Einschränkungen für den Angreifer erwachsen.

Einschränkungen des Zugangs zu Komponenten Obwohl grundsätzlich in vielen Einsatzbereichen die Möglichkeit gegeben ist, dass ein Angreifer sich physischen Zugang zu den Komponenten verschafft, können Komponenten auch in schwer- bis gar nicht zugänglichen oder überwachten Gebieten ausgebracht werden. Auch innerhalb von nicht öffentlichen Gebäuden angebrachte Komponenten sind für einen Angreifer nur schwer zugänglich. In solchen Fällen ergibt sich für den Angreifer eine Einschränkung der Fähigkeiten, die ihm aufgrund der Zugänglichkeit der Komponenten zugesprochen werden; im Einzelnen als der Fähigkeiten, Komponenten zu zerstören und ihren Speicher zu manipulieren oder auszulesen.

Einschränkungen im Bezug auf das Korrumpieren von Komponenten Selbst wenn ein Angreifer Zugriff auf die Komponenten eines Smart Home-Netzes hat und es ihm gelingt, in diesem Komponenten zu korrumpieren, ist ihm dies nicht in unbeschränktem Umfang möglich. Der Angreifer ist in seiner Fähigkeit, Komponenten zu korrumpieren oder sonst zu manipulieren, durch die Kosten beschränkt, die ihm dadurch entstehen. Jeglicher Eingriff in das bestehende Kommunikationssystem kostet den Angreifer *Ressourcen*, die ihm nur in begrenztem Maße zur Verfügung stehen. Ist sein Ziel die Reprogrammierung von Komponenten, muss er sich zunächst das *Wissen* aneignen, das nötig ist, um dies zu tun. Dann benötigt er *Zeit* zur Erstellung des zu verwendenden Programms, was immer auch mit einer *monetären* Investition verbunden ist. Daher wird im Allgemeinen angenommen, dass ein Angreifer nicht beliebig viele Komponenten in einem

Netz korrumpieren kann, sondern durch eine obere Schranke $\mathcal{B} < n$ in dieser Fähigkeit beschränkt ist, wobei n die Gesamtzahl der Knoten im Smart Home darstellt.

4.1.3 Merkmalraum eines Angreifers

Dieser Abschnitt des vorliegenden Dokumentes beschreibt Merkmale, die die Fähigkeiten eines Angreifers in Smart-Home-Szenarien erfassen und die Klassifikation von Angreifern erlauben. Zunächst werden diese Merkmale aufgezählt und mögliche Ausprägungen definiert. Im Anschluss werden drei verschiedene Angreiferklassen anhand der Merkmale differenziert.

Lokalität des Angreifers Dieses Merkmal dient zur Beschreibung der Präsenz des Angreifers in einem System. Meist wird von einem global anwesenden Angreifer ausgegangen, jedoch kann der Angreifer auch durch Beschränkungen der Zugänglichkeit des Netzes auf gewisse Bereiche eingeschränkt sein, innerhalb derer er agieren kann. Dieses merkmal kann die im Dolev-Yao-Modell angenommene Globalität des Angreifers überschreiben.

Zugriff auf Komponenten Hiermit wird quantifiziert, welche Möglichkeiten zum Zugriff auf Komponenten ein Angreifer hat. Der Zugriff kann sich etwa auf die Zerstörung von Komponenten und der Manipulation der Sensorik beschränken, oder aber auch die Möglichkeit des passiven Auslesens bzw aktiven Manipulierens der Komponenten beinhalten. Dabei ist zu beachten, dass eine Ordnung bezüglich der Stärke des Angreifers impliziert ist: Es wird angenommen, dass ein Angreifer, der beispielsweise in der Lage ist, Sensordaten zu manipulieren, auch in der Lage ist, Komponenten zu zerstören. Umgekehrt kann aber nicht geschlossen werden, dass ein Angreifer, der Sensordaten manipulieren kann, auch etwa den Speicher des Komponenten auslesen kann.

Anteil manipulierter Komponenten Dieses Merkmal erfasst schließlich den Anteil der durch den Angreifer manipulierten Knoten. Welcher Art die Manipulation ist, ist mit der Ausprägung des obigen Merkmals *Zugriff auf Komponenten* festgelegt. Besteht die Art des Zugriffs im Reprogrammieren der Komponenten (s.o.), so entspricht das Merkmal der in Abschnitt 4.1.2.2 beschriebenen oberen Schranke $\mathcal{B}$ für das Korrumpieren von Komponenten.

4.1.4 Angreiferklassifikation

Aus den obigen Merkmalen lassen sich Angreifer in einem Smart Home klassifizieren; die Klassen unterscheiden sich dabei hauptsächlich darin, inwiefern der Angreifer über geheimes, im Kommunikationsnetz verwendetes Wissen verfügt, und inwieweit er in der Lage ist, das Verhalten der Komponenten zu beeinflussen.

4.1.4.1 Externer Angreifer

Der externe Angreifer ist der schwächste Angreifer, der angenommen wird. Im Sinne des oben genannten Merkmalraums ist der externe Angreifer wie folgt charakterisiert:

Ort des Angreifers Global verteilt *oder* lokal eingeschränkt

Zugriff auf Komponenten Kein *oder* Zerstörerisch *oder* Manipulation der Sensorik

Anteil manipulierter Komponenten Angabe in Prozent der Gesamtpopulation

Soweit nicht anders vorgegeben, verfügt dieser Angreifer ansonsten über die Fähigkeiten und Einschränkungen des Dolev-Yao-Modells.

4.1.4.2 Passiv interner Angreifer

Unter einem passiv internen Angreifer wird ein Angreifer verstanden, der zwar an internes, im Smart Home vorhandenes Wissen gelangen kann, das Verhalten der Komponenten aber nicht grundlegend verändern kann. Er ist im Sinne der oben genannten Merkmale charakterisiert durch folgende Ausprägungsschar:

Ort des Angreifers Global verteilt *oder* lokal eingeschränkt

Zugriff auf Komponenten Auslesen des Speichers

Anteil manipulierter Komponenten Angabe in Prozent der Gesamtpopulation

Soweit nicht anders vorgegeben, verfügt dieser Angreifer ansonsten über die Fähigkeiten und Einschränkungen des Dolev-Yao-Modells.

4.1.4.3 Aktiv interner Angreifer

Der aktive, interne Angreifer ist in Bezug auf seine Fähigkeiten der stärkste anzunehmende Angreifer. Er ist nicht nur in der Lage, an internes Wissen des Systems zu gelangen, sondern auch Komponenten gezielt zu reprogrammieren, d.h. zu korrumpieren. Die folgenden Ausprägungen der genannten Merkmale charakterisieren den aktiven internen Angreifer:

Ort des Angreifers Global verteilt *oder* lokal eingeschränkt

Zugriff auf Komponenten Reprogrammieren der Knoten

Anteil manipulierter Komponenten Angabe in Prozent der Gesamtpopulation

Soweit nicht anders vorgegeben, verfügt dieser Angreifer ansonsten über die Fähigkeiten und Einschränkungen des Dolev-Yao-Modells.

Die Klassifikation von Angreifern lässt sich verfeinern, indem für die jeweiligen Klassen anhand der Merkmale *Ort des Angreifers* beziehungsweise *Anteil manipulierter Knoten* Unterklassen gebildet werden. Allerdings explodiert dadurch der Modellraum des Angreifers und wird schnell unübersichtlich, weswegen die Unterscheidung von Unterklassen nach Möglichkeit sparsam verwendet werden sollte.

Des Weiteren sind Überlagerungen und Kombinationen von Angreifern möglich. Beispielsweise kann in einem Szenario ein externer Angreifer global präsent sein, während lokal eingeschränkt auch ein passiv interner Angreifer oder ein aktiv interner Angreifer angenommen werden muss. In diesem Fall ist es bei der Entwicklung von sicheren Systemen sinnvoll, die Kosten abzuwägen, die durch die Differenzierung entstehen – beispielsweise kann es durchaus günstiger sein, statt eines lokal eingeschränkten aktiven Angreifers einen global verteilten aktiven Angreifer anzunehmen und das System entsprechend zu entwickeln, anstatt zwei interoperable Systeme zu entwickeln, die jeweils regional auf die entsprechenden Angreifer zugeschnitten sind.

4.2 Kommunikationssicherheit

4.2.1 Betrachtete Bedrohungen

Für die Manipulation der Kommunikation ergeben sich folgende Bedrohungen:

- **Mitlesen von Dateneinheiten:** Es können sowohl Metadaten (Kopfdaten und Anhangdaten) als auch Nutzdaten ausgelesen werden.
- **Einspielen von neuen, zusätzlichen Dateneinheiten:** Es können sowohl Dateneinheiten mit ungültiger als auch mit gültiger Syntax (syntaktisch konform) eingespielt werden. Bei gültiger Syntax kann weiterhin unterschieden werden zwischen ungültigen Protokollparametern und gültigen Parametern.
- **Ändern des Inhalts von Dateneinheiten:** Es können sowohl Änderung von Daten in der Nutzlast als auch Änderungen von Metadaten durchgeführt werden. Bei Metadaten kann weiterhin zwischen Kopfdaten (Einfügen zusätzlicher Erweiterungskopfdaten oder ändern der existierenden Kopffelder) und Anhangdaten unterschieden werden.
- **Ändern der Reihenfolge von Dateneinheiten:** Die Reihenfolge der Dateneinheiten wird auf dem Übertragungsweg vertauscht.
- **Löschen von Dateneinheiten:** Dateneinheiten werden auf dem Übertragungsweg gelöscht.

- **Duplizieren/Wiedereinspielen von Dateneinheiten:** Dateneinheiten werden dupliziert und unter Umständen erneut eingespielt.
- **Verzögern von Dateneinheiten:** Dateneinheiten werden auf dem Übertragungsweg verzögert.
- **Umleiten von Dateneinheiten:** Dateneinheiten werden auf dem Übertragungsweg umgeleitet. Typische Angriffsbeispiele hierfür sind der Man-in-the-Middle Angriff, Connection Hijacking oder ein Reflection-Angriff.
- **Unterbinden der Kommunikation:** Die Kommunikation kann vollständig unterbunden werden, beispielsweise durch das durchtrennen einer direkten Kabelverbindung.

Weitere, nicht die Kommunikation betreffende Bedrohungen im Smart Home-Szenario sind:

- **Kompromittieren von Schlüsselmaterial:** Das auf den Komponenten gespeicherte Schlüsselmaterial (Beispielsweise Sitzungsschlüssel, Schlüssel zur Authentifikation, Passwörter) wird ausgelesen.
- **Autorisierungsverletzung:** Beispielsweise unautorisiertes Zugriff auf aktuelle Energiebedarfsdaten.
- **Maskerade:** Hierbei gibt eine Instanz vor, sie besitze eine andere Identität, beispielsweise um im Anschluss eine Autorisierungsverletzung zu begehen oder sich der Haftung zu entziehen bzw. Nachverfolgung zu entgehen.
- **Manipulation der Hardware:** Die einzelnen Komponenten im Smart Home werden physikalisch manipuliert. Beispielsweise durch das Trennen von Verbindungsleitungen, das Eindringen in Sensoren. Ziel kann es sein,deren Aufbau zu analysieren, Speicherbereiche auszulesen oder zu beschreiben. Weiterhin kann es möglich sein, ganze Komponenten auszutauschen.
- **Erzeugung eines Ressourcenmangels:** Es wird versucht, ein Ressourcenmangel (Beispielsweise Speicher oder Energie) bei den einzelnen Komponenten zu erzeugen. Hierfür können sowohl Manipulation der Kommunikation als auch Manipulation der Hardware eingesetzt werden.

4.2.2 Analyse

In diesem Abschnitt erfolgt die beispielhafte Betrachtung unterschiedlicher Angriffe. Hierfür werden drei exemplarische Angreifer verwendet, welche sich durch ihre Lokalität

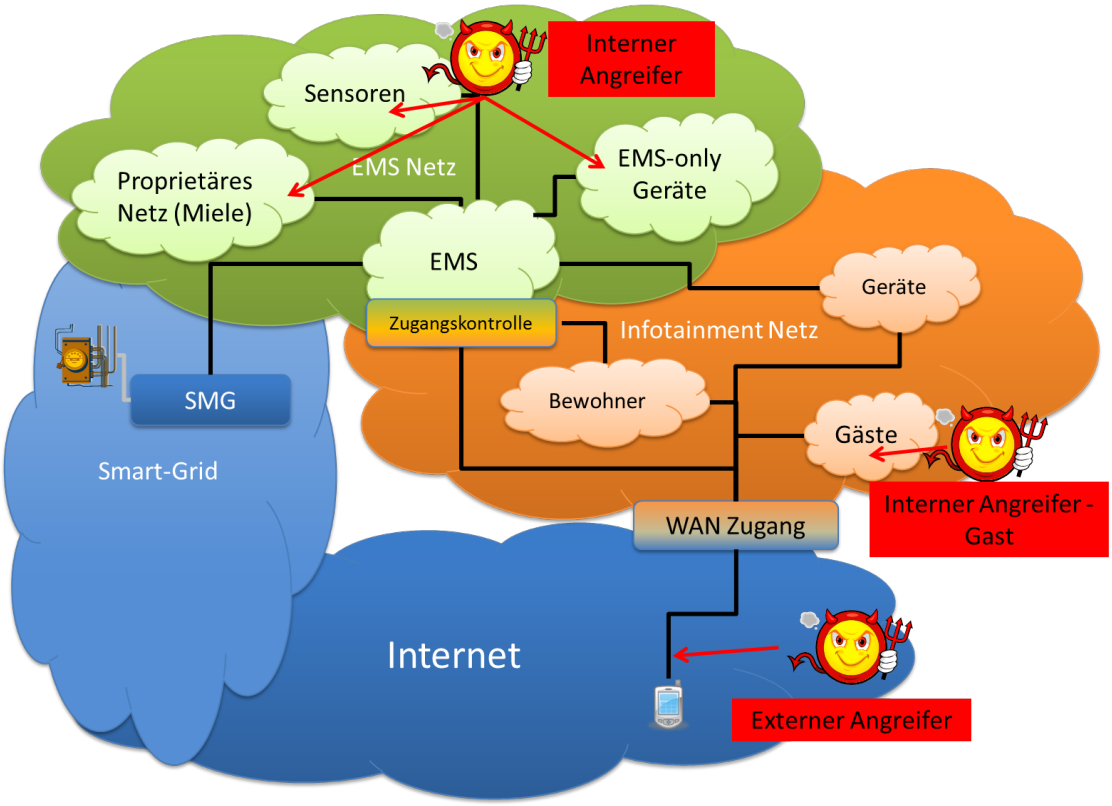

Abbildung 4.1: Lokationen der drei Angreifer innerhalb der Angriffsanalyse

unterscheiden. In Abbildung 4.1 sind die im Rahmen dieser Angriffsanalyse exemplarisch verwendeten Angreiferlokationen eingezeichnet.

Im einzelnen werden folgende Angreifer betrachtet:

- **Externer Angreifer:** Ein externer Angreifer, beispielsweise ein Hacker, versucht von außerhalb über das Internet Angriffe auf das Smart Home durchzuführen.
- **Interner Angreifer im Gastnetz:** Ein interner Angreifer, der sich im Smart Home internen Gastnetz befindet. Beispielsweise könnte es sich um einen Gast mit Tablet-PC handeln, der mit diesem Zugang zum Internet haben möchte.
- **Interner Angreifer:** Ein interner Angreifer, der eine Komponente des Smart Homes korrumpiert und somit in seine Gewalt gebracht hat oder eigene Geräte im internen Netz angeschlossen hat. Beispielsweise könnte ein Angreifer einen Energiesensor korrumpiert haben.

4.2.3 Externer Angriff

Hat der Angreifer keinen Zugriff auf das interne Kommunikationsnetz, kann er versuchen, Angriffe auf externe Kommunikationsvorgänge durchzuführen. Alle Angriffe betreffen nur die Kommunikationsstrecke, die zwischen dem WAN-Zugang und dem Kommunikationspartner außerhalb des Smart Home liegt.

Abhören Ist die externe Kommunikation unverschlüsselt, besteht die Möglichkeit des Abhörens durch einen Angreifer, was gegebenenfalls zur Vorbereitung weiterer Angriffe genutzt werden kann. Zur Sicherung der externen Kommunikation wird im Rahmen der Smart-Home-Architektur (D)TLS mit Verschlüsselung eingesetzt, ein Abhören der Anwendungsdaten oberhalb von Schicht 4 der ISO/OSI-Architektur ist somit nicht möglich. Für den Angreifer ist es jedoch möglich, Nachrichteneinheiten in Schichten 2–4 abzuhören und entsprechend Informationen aus den Kopffeldern auszulesen. Beispielsweise ist es somit möglich, eine Verkehrsanalyse durchzuführen.

Zwischenschalten Ein Angreifer kann sich auf der externen Kommunikationsstrecke mittels verschiedener Methoden aktiv zwischenschalten und die Kommunikation beeinflussen. Sofern keine Ende-zu-Ende-Integritätssicherung erfolgt, kann ein Angreifer beispielsweise weitreichenden Einfluss auf den Kommunikationsvorgang ausüben (Einfügen, Löschen oder Verändern von Daten). Dadurch können gegebenenfalls Komponenten des Smart Home gefährdet werden.

Zur Sicherung der externen Kommunikation wird im Rahmen der Smart Home Architektur (D)TLS zum Schutz der Integrität und der Authentizität der Anwendungsdaten verwendet. Das Ändern von Anwendungsdaten und das Einspielen von neuen, zusätzlichen Anwendungsdaten sind somit nicht möglich.

Ein Schutz der Kommunikation auf Schicht 2–4 der ISO/OSI-Architektur ist nicht vorgesehen. Das Ändern des Inhalts von Dateneinheiten auf diesen Schichten und das Einspielen von neuen, zusätzlichen Dateneinheiten sind somit möglich. Da (D)TLS Schutz vor Replay Angriffen bietet, ist ein Duplizieren bzw. Wiedereinspielen von Anwendungsdaten zwar möglich, wird jedoch von (D)TLS erkannt und eine Auslieferung der duplizierten Anwendungsdaten an die Anwendung verhindert. Das Ändern der Reihenfolge von Dateneinheiten wird bei Verwendung von TCP/TLS durch TCP erkannt und die Daten werden in der korrekten Reihenfolge an die Anwendung weitergereicht, bei DTLS bleibt die Reihenfolge verändert, was jedoch auf Anwendungsebene behandelt werden muss. Das Löschen von Dateneinheiten ist für den Angreifer möglich, jedoch wird das Fehlen der Dateneinheit durch TCP erkannt (bei TCP/TLS) und diese erneut übertragen. Bei Einsatz von DTLS muss die Anwendung fehlende Daten behandeln. Das Verzögern und Umleiten von Dateneinheiten ist möglich, ebenso das Unterbinden der Kommunikation. Jede dieser Bedrohungen wird jedoch von (D)TLS erkannt und führt im schlimmsten Fall zum Abbruch der Verbindung.

Angriffe auf die Verfügbarkeit (Denial-of-Service) Ein Angreifer kann versuchen, den Smart-Home-Edge-Router bzw. eine interne Komponente im Infotainment- bzw. EMS-Netz mit einem DoS-Angriff zu beeinträchtigen. Dies wird durch die Firewall-Funktion des Smart-Home-Edge-Routers und des EMS Routers jedoch verhindert. Fällt der Smart-Home-Edge-Router aus, sind keine externen Kommunikationsvorgänge mehr möglich.

Wird der Smart-Home-Edge-Router selbst kompromittiert, können von diesem aus weitere Angriffe auf Geräte des Infotainmen-Netzes und gegebenenfalls des EMS-Netzes stattfinden. Der EMS-Router kann jedoch beispielsweise Angriffe, die auf Ressourcenknappheit durch Fluten mit Datenpaketen abzielen, dadurch unterbinden, dass er eine Bandbreitenbegrenzung für externe Kommunikation bzw. Kommunikation zum und vom Smart-Home-Edge-Router aus vorsieht. Eine alternative Möglichkeit besteht in der Markierung und Behandlung des Verkehrs als Lower Effort. Dieser Schutz ist allerdings ineffektiv gegen Angriffe vom Smart-Home-Edge-Router, welche auf die Begrenztheit der Verarbeitungsleistung von Komponenten abzielen (Auslastung von Komponenten), sofern der Angreifer in der Lage ist, authentische TLS-Dateneinheiten zu erzeugen.

4.2.4 Interner Angriff

Es ist davon auszugehen, dass ein Angreifer sich physikalisch, unautorisierten Zugang zu Komponenten innerhalb des Smart-Home verschaffen kann. Hierbei ist zu unterscheiden, ob er sich physischen Zugang zur Kommunikationsinfrastruktur (beispielsweise einem Switch oder Router) oder zu einem Kommunikationsmedium (beispielsweise Kabel oder Luftschnittstelle) verschafft. Weiterhin ist es anzunehmen, dass der Angreifer eine Komponente des Smart-Home (beispielsweise einen Energiesensor oder Router) korrumpieren kann und somit vollständige Kontrolle über diese Komponente erhält.

Abhören Ein simpler Angriff, nachdem der Angreifer sich unautorisierten Zugang verschafft hat, ist das Abhören von Kommunikationsvorgängen. Abhören dient häufig zur Vorbereitung weiterer Angriffe, beispielsweise zum Auslesen von Schlüsselmaterial – sofern diese überhaupt bzw. ungeschützt übertragen werden.

Mitlesen von Schicht 2 bis Schicht 4 Nachrichten wird durch die Sicherheitsarchitektur nicht verhindert. Dies bedeutet, dass ein Angreifer alle Nachrichten in den Schichten 2 bis 4 mitlesen kann, sofern er physischen Zugriff auf das entsprechende Subnetz bzw. auf das entsprechende Schicht-2-Medium hat. Beispielsweise ist es somit möglich, eine Verkehrsanalyse durchzuführen.

Zur Sicherung der Kommunikation wird im Rahmen der Smart-Home Architektur (D)TLS mit Verschlüsselung eingesetzt, ein Abhören der Anwendungsdaten der nicht korrumpierten Geräte oberhalb von Schicht 4 ist somit nicht möglich.

Zwischenschalten Ein Schutz der Kommunikation in den Schichten 2–4 der ISO/OSI-Architektur ist nicht vorgesehen. Jedoch wird mit Hilfe der Aufteilung des Netzes in unterschiedliche Sicherheitszonen und funktionalen Domänen versucht, unerwünschte Kommunikationsvorgänge zu verhindern. Die technische Realisierung der Zonen bzw. Domänen erfolgt mit Hilfe unterschiedlicher IP-Subnetze. Eine Kommunikation von Komponenten in unterschiedlichen Zonen bzw. Domänen muss zwangsläufig über den EMS-Router stattfinden. Hier können entsprechend den Firewall-Regeln unerwünschte Kommunikationsvorgänge unterbunden werden.

Hat ein Angreifer somit keine Komponenten korrumpiert, kann er lediglich Angriffe auf die Subnetze ausführen, auf die er physischen Zugriff hat. Das Ändern des Inhalts von Dateneinheiten in den Schichten 2–4 und das Einspielen von neuen, zusätzlichen Dateneinheiten sind prinzipiell möglich. Da (D)TLS Schutz vor Replay Angriffen bietet, ist ein Duplizieren bzw. Wiedereinspielen von Schicht-2–4-Dateneinheiten zwar möglich, wird jedoch von (D)TLS erkannt und eine Auslieferung der duplizierten Anwendungsdaten an die Anwendung verhindert. Das Ändern der Reihenfolge von Dateneinheiten wird bei Verwendung von TCP/TLS durch TCP erkannt und die Daten werden in der korrekten Reihenfolge an die Anwendung weitergereicht, bei DTLS bleibt die Reihenfolge verändert, was jedoch auf Anwendungsebene behandelt werden muss. Das Löschen von Dateneinheiten ist für den Angreifer möglich, jedoch wird das Fehlen der Dateneinheit durch TCP erkannt (bei TCP/TLS) und diese erneut übertragen. Bei Einsatz von DTLS muss die Anwendung fehlende Daten behandeln. Das Verzögern und Umleiten von Dateneinheiten ist möglich, ebenso das Unterbinden der Kommunikation. Jede dieser Bedrohungen wird jedoch von (D)TLS erkannt und führt im schlimmsten Fall zum Abbruch der Verbindung.

Hat ein Angreifer ein Gerät korrumpiert, kann er beliebige Anwendungsdaten als legitimer Teilnehmer des Netzes versenden und versuchen neue Kommunikationsverbindungen zu etablieren. Hierdurch ist es unter Umständen auch möglich, Komponenten in anderen Sicherheitszonen bzw. Domänen anzugreifen. Hierbei ist entscheidend, ob entsprechende Zonenübergänge im EMS-Router aufgrund der Anwendungsfunktionalität bzw. der Zugehörigkeit der Komponente zu funktionalen Domänen erlaubt sind.

Angriffe auf die Verfügbarkeit (Denial-of-Service) Hat ein Angreifer Zugang zum internen Netz, kann er verschiedene Angriffe auf die Verfügbarkeit durchführen.

Das Einfügen von Dateneinheiten durch den Angreifer in das Netz kann beispielsweise Ressourcenmangel (etwa hinsichtlich von Leitungskapazität, Verarbeitungskapazität oder Speicherkapazität) erzeugen. Auch wenn die Dateneinheiten nicht authentisch sind, werden sie unter Umständen durch die Schicht-2- oder -3-Komponenten bis zum Ziel weitergeleitet, was Leitungskapazität und Verarbeitungskapazität beansprucht. Auch hier ist zu entscheiden, ob entsprechende Zonenübergänge durch den EMS-Router erlaubt sind.

Eine weitere Angriffsmöglichkeit bieten die Zugriffsverfahren bei auf mehrere Nutzer aufgeteilten, insbesondere drahtlosen Medien. Hier kann durch Jamming oder geschicktes Eingreifen der Zugriff durch andere Geräte auf das Medium gegebenenfalls unterbunden werden, sodass Geräte nicht mehr miteinander kommunizieren können.

Das Einfügen von Nachrichten in Transportverbindungen ist prinzipiell möglich. DoS-Angriffe in Schicht 4 wie etwa TCP-SYN-Flooding sind damit nicht ausgeschlossen. Weitere potenziell erfolgreiche DoS-Angriffe in Schicht 4 sind das Löschen von Dateneinheiten der Transportschicht durch Löschen oder Verändern von IP-Paketen.

Hijacking Eine Übernahme von Schicht 3 oder 4 Kommunikationsbeziehungen (zum Beispiel mittels ARP-Angriffen) ist möglich, da dies nicht durch (D)TLS verhindert wird. Allerdings kann ein Angreifer ohne eine korrumpierte Komponente sich nicht als legitimer Kommunikationsteilnehmer ausgeben oder durch (D)TLS gesicherte Nachrichteneinheiten lesen oder manipulieren.

4.2.5 Interner Angriff – Gast

Ein Angreifer kann Zugriff auf das Gastnetz im Smart-Home haben. Dies kann zum Beispiel möglich sein, indem der Angreifer den Tablet-PC eines Gastes korrumpiert hat. Geräte im Gastnetz haben die Möglichkeit, die Internetverbindung des Haushalts zu nutzen. Das Gastnetz setzt auf Schicht 2 802.11 (Wifi) ein. Der Zugang wird über WPA2 geschützt.

Abhören Der Angreifer kann keine Nachrichten abhören, da WPA2 eingesetzt wird.

Angriffe auf die Verfügbarkeit (Denial-of-Service) Der Angreifer kann versuchen, mit Hilfe von Jamming oder geschicktes Eingreifen der Zugriff durch andere Geräte auf das Medium gegebenenfalls unterbunden wird, sodass andere Geräte nicht mehr miteinander kommunizieren können.

Ebenso kann versuchen, durch das Versenden von Schicht-3-Nachrichten den Smart-Home Edge Router oder den EMS-Router hinsichtlich von Leitungskapazität oder Verarbeitungskapazität zu überlasten.

Eine Kommunikation zu Komponenten im Smart-Home wird durch den EMS-Router verhindert.

4.3 Anwendungssicherheit

4.3.1 Betrachtete Bedrohungen

Für die Analyse der Anwendungssicherheit werden folgende Bedrohungen betrachtet:

Kategorie Spoofing / Imitation

- **Imitierung einer Entität zum Senden von Daten:** Ein Angreifer könnte vortäuschen, eine bestimmte Entität (Prozess, Externe Entität oder Datenquelle) zu sein, um unautorisierten Zugriff auf den Empfänger der Daten zu erlangen oder um falsche Daten an den Empfänger zu schicken.
- **Imitierung einer Entität zum Empfangen von Daten:** Ein Angreifer könnte vortäuschen, eine bestimmte Entität (Prozess, Externe Entität oder Datenquelle) zu sein, um an Informationen der Datenquelle zu gelangen.

Kategorie Tampering / Manipulation

- **Unzureichende Eingabevalidierung in einem Prozesses oder Datenspeicher:** Ein Angreifer könnte einen Datenfluss zu einem Prozess oder Datenspeicher manipulieren. Daraus können folgende Attacken gegen den Prozess folgen: Denial of Service, Elevation of Privilege oder Informationsoffenlegung.

Kategorie Repudiation / Abstreiten

- **Abstreitbarkeit des Empfangs von Daten:** Eine Entität könnte behaupten, keine Daten von der Quelle außerhalb der Vertrauensgrenze erhalten zu haben.
- **Abstreitbarkeit von Ereignissen im System:** Eine Entität könnte behaupten, das bestimmte Ereignisse im System nicht stattgefunden haben.

Kategorie Information Disclosure / Offenlegen von Informationen

- **Abhören des Datenflusses:** Ein Datenfluss könnte mitgehört werden. In Abhängigkeit davon, welche Daten versandt werden, kann der Angreifer diese benutzen, um weitere Teiles des Systems anzugreifen, oder die Informationen veröffentlichen, was rechtliche Folgen haben könnte.
- **Schwacher Transit von Zugangsdaten:** Zugangsdaten im Netzverkehr werden oft von Angreifern mitgehört. Die Zugangsdaten sind eventuell wiederverwendbar (replay). Oder sie sind direkt in einer Nachricht enthalten.
- **Schwache Zugriffskontrolle auf Ressource:** Unzureichender Schutz einer Ressource kann dazu führen, dass Angreifer Informationen lesen können, die nicht offengelegt werden sollen. Die Authorisationseinstellungen sollten geprüft werden.

Kategorie Denial of Service

- **Absturz eines Prozesses:** Wenn ein Prozess abstürzt, hängt, stoppt oder verlangsamt ist, kann die Verfügbarkeit nicht gewährleistet werden.
- **Unterbrechung des Datenflusses:** Ein externer Angreifer könnte Datenflüsse, die Vertrauensgrenzen überschreiten, in jede Richtung unterbrechen.

Kategorie Elevation of Priviledge / Rechte erweitern

- **Elevation durch Imitation:** Der Angreifer könnte den Kontext einer Entität imitieren, um zusätzliche Rechte zu erlangen.
- **Elevation durch Ausführung von Code aus der Ferne:** Ein Angreifer könnte fähig sein, Code aus der Ferne in einem Prozess auszuführen.

4.3.2 Analyse

Die Bedrohungen werden in Hinblick auf die Realisierbarkeit von den drei gleichen exemplarischen Angreifern untersucht, analog zur Analyse in Kapitel 4.2.2. Für die Analyse der Anwendungssicherheit für die Angreifer weitere Annahmen getroffen:

- **Externer Angreifer:** Ein passiver externer Angreifer, der keinen physischen Zugriff auf Smart-Home-Kompontenen und -Netze hat und nicht in der Lage ist, Komponenten im Smart-Home zu Korrumpieren besitzt.
- **Interner Angreifer im Gastnetz:** Ein passiver interner Angreifer, der physischen Zugriff auf Haushaltsgeräte und Sensoren hat, sowie auf die Sicherheitszone „Infotainment Netz“. Der Angreifer kann keine Komponenten korrumpieren.
- **Interner Angreifer:** Ein aktiver interner Angreifer, der Komponenten des Smart-Homes korrumpieren kann oder eigene Geräte im internen Netz anschließen kann. Er hat physischen Zugriff auf alle Komponenten.

4.3.2.1 Imitation einer Entität zum Versenden von Daten

Bei der Netzwerkkommunikation wird stets (D)TLS verwendet, um die Authentizität der versandten Daten sicherzustellen. Der Schutz ist wirksam, solange die genutzten Schlüssel geheim bleiben. Gelingt es dem Angreifer, einen Kommunikationspartner zu korrumpieren, können die Schlüssel offengelegt oder getauscht werden, um die Imitation zu realisieren. Somit können externe Angreifer und passive interne Angreifer im Gastnetz diese Imitation nicht realisieren, während ein aktive interne Angreifer über die Schlüssel erfolgreich imitieren kann.

Bei der Interprozesskommunikation oder bei der Kommunikation zwischen Prozess und Datenspeichern setzt das Betriebssystem eine Zugriffskontrolle durch. Dadurch wird verhindert, dass die Prozess- oder Datenspeicheridentität (entspricht z.B. den Dateinamen) nicht imitiert werden kann. Nur wenn ein Angreifer die Zugriffsrechte oder die Zugriffskontrolle des Betriebssystems manipulieren kann, gelingt ihm ein Angriff. Auch hier können externe Angreifer und passive interne Angreifer im Gastnetz diese Imitation nicht realisieren, während ein aktive interne Angreifer nicht abgewehrt wird.

Die Bedrohung „Imitation einer Entität zum Versenden von Daten“ kann an folgenden Stellen im System auftreten:

- Der Angreifer könnte das Energiemanagement imitieren und kann so Gerätezustande, Sensorwerte oder Energiezählerwerte auslesen und Rückschlüsse auf Verhalten von Haushaltsmitgliedern ziehen (Güterwert 5). Externe Signale könnten auch durch Imitation ausgelesen werden, allerdings müssen diese Informationen nicht geheim gehalten werden.

  Da sich das Energiemanagementsystem gegenüber Haushaltsgeräten, Sensoren und dem Smart-Meter-Gateway jeweils mit Hilfe von (D)TLS authentifizieren muss, bevor eine Datenabfrage beantwortet wird, kann unter den gegebenen Annahmen nur eine erfolgreiche Imitation stattfinden, wenn der Angreifer es schafft, das Energiemanagementsystem zu korrumpieren (vgl. Kapitel 4.2.4, Abhören). Das kann nur einem aktiven internen Angreifer gelingen.

- Der Angreifer könnte auch Haushaltsgeräte, Sensoren, Smart-Meter-Gateway oder externe Datenquelle imitieren, um falsche Daten an das Energiemanagement zu senden. In Folge werden den Haushaltsmitgliedern falsche Daten angezeigt, die falsche Steuerentscheidungen treffen und so zu ökonomischen Schaden kommen könnten (Güterwert 4-5).

  Da sich auch hier Haushaltsgeräte, Sensoren, Gateway und externe Datenquelle authentifizieren, gelingt einem Angreifer der Imitationsangriff nur, wenn er den jeweiligen Knoten oder das Energiemanagementsystem korrumpieren hat. Das kann nur einem aktiven internen Angreifer gelingen. Im Falle der externen Datenquelle kann auch die Imitation durch eine manipulierte PKI stattfinden.

- Der Angreifer könnte vorgeben, ein Haushaltsmitglied oder ein Gast zu sein, um Zugriff auf Haushaltsgeräte zu erlangen.

  Dieser Zugriff ist nur auf physischen Wege möglich. Es wird angenommen, dass Angreifer kein physischer Zugang eingeräumt wird, den er nutzt, um Haushaltegeräte zu steuern.

- Der Angreifer könnte vortäuschen, der Energiemanagementadministrator zu sein.

Der Energiemanagementadministrator muss sich gegenüber dem SSH-Prozess authentifizieren. Laut Annahme kommt der Angreifer nicht an dessen Schlüsselmaterial heran und diese Bedrohung kann nicht realisiert werden.

- Ein Angreifer könnte die Konfigurationsdatei imitieren. Dadurch können für den Haushaltsmitglied falsche Datenquellen konfiguriert oder Datenquellen entfernt werden, die in Folge von falschen Steuerentscheidungen ökonomischen Schaden verursacht (Güterwert 4).

  Für die Imitation muss der Zugriffsschutz des Betriebssystems ausgehebelt werden. Beispielsweise durch Ändern von Mountpoints, Umbenennung von Dateinamen oder Ändern der Dateisystemrechte. Nur aktive Angreifer können eine solche Bedrohung realisieren, indem die Plattform des Energiemanagementsystems korrumpiert wird.

- Ein Angreifer könnte die interne Datenbank imitieren, um falsche Energieverbrauchsdaten an das Energiemanagement zu senden. Dem Haushaltsvorstand kann in Folge einer falschen Steuerentscheidung ökonomischer Schaden entstehen (Güterwert 4).

  Für die Imitation muss der Zugriffsschutz des Betriebssystems ausgehebelt werden. Nur aktive Angreifer können eine solche Bedrohung realisieren, indem die Plattform des Energiemanagementsystems korrumpiert wird. Externe Angreifer und passive interne Angreifer können diese Bedrohung nicht realisieren.

- Ein Angreifer könnte das Energiemanagementsystem imitieren, um falsche Daten an das Tablet zu schicken. In Folge von falschen Steuerentscheidungen kann ökonomischer Schaden verursacht werden (Güterwert 4).

  Wenn das Tablet oder das Energiemanagementsystem vom Angreifer korrumpiert ist, gelingt ein solcher Angriff. Ansonsten authentifiziert sich das Energiemanagementsystem korrekt gegenüber dem Tablet.

- Ein Angreifer könnte sich gegenüber dem Energiemanagementsystem als Haushaltsmitglied ausgeben. Er bekommt dadurch Zugriff auf Gerätezustande, Sensorwerte oder Energiezählerwerte und kann Rückschlüsse auf Verhalten von Haushaltsmitgliedern ziehen (Güterwert 5).

  Dies ist nicht realisierbar, da laut Annahme die Zugangsdaten des Haushaltsmitglieds geheim bleiben.

4.3.2.2 Imitation einer Entität zum Empfangen von Daten

Diese Bedrohung ist sehr ähnlich zur Bedrohung 4.3.2.1 und kann mit den gleichen Maßnahmen abgewehrt werden. Allerdings kann sich die Bedrohung anders auswirken, da das Ziel ist, durch Imitation eines Datenempfängers Informationen offenzulegen.

Wie in Kapitel 4.3.2.1 beschrieben, sind durch den Einsatz von (D)TLS bei Netzwerkverbindungen und Zugriffsschutz bei Verbindungen der selben Plattform Angriffe von externen Angreifern und passiven internen Angreifern abgewehrt. Aktive interne Angreifer können diesen Schutz durch ihre Fähigkeit, Komponenten zu korrumpieren, umgehen.

Die Bedrohung „Imitation einer Entität zum Empfangen von Daten“ kann an folgenden Stellen im System auftreten:

- Der Angreifer könnte sich als Haushaltsgerät, als externe Datenquelle, als Sensor oder als Smart-Meter-Gateway ausgeben, um Daten vom Energiemanagementsystem zu empfangen und offenzulegen.

  Die gesendeten Daten sind lediglich eine Anforderung für Messwerte und enthalten somit keine geheimzuhaltenden Daten. Zudem ist die Verbindung mittels (D)TLS gesichert. Die Bedrohung ist damit nicht relevant.

- Der Angreifer könnte sich als Energiemanagements ausgeben, um geheimzuhaltende Zustands-, Sensor-, und Messwerte zu empfangen. Die Vertraulichkeit ist gefährdet (Güterwert 5).

  Das Energiemanagementsystem muss sich mit Hilfe von (D)TLS gegenüber allen Datenquellen authentifizieren. Zudem können Angreifer aufgrund der Verschlüsselung nicht mithören. Nur der aktive interne Angreifer, der bereits einen der beteiligten Knoten korrumpiert hat, kann diese Bedrohung realisieren.

- Der Angreifer könnte sich als SSH-Prozess ausgeben, um Daten des Energiemanagementadministrators abzufangen. Vor allem könnte die Konfigurationsdatei abgehört werden, die für weitere Angriffe genutzt werden kann.

  Die Kanalverschlüsselung von SSH stellt Authentizität und Integrität des Energiemanagementadministrators sicher, sofern der SSH-Prozess nicht korrumpiert wurde. Nur ein aktiver interne Angreifer kann den SSH-Prozess korrumpieren. Andere Angreifer können diese Bedrohung nicht realisieren.

- Der Angreifer könnte sich als Haushaltsmitglied ausgeben, um Zustands-, Sensor-, und Messwerte beim Energiemanagementsystem abzurufen. Die Vertraulichkeit ist gefährdet (Güterwert 5).

  Ein Haushaltsmitglied authentifiziert sich mit einer Benutzername/Passwort-Kombination am Energiemanagement. Sofern der Angreifer nicht in Besitz dieser Zugangsdaten ist, kann er solche Angriffe nicht ausführen. Die Verbindung zum Übertragen der Zugangsdaten ist mit (D)TLS geschützt.

- Der Angreifer könnte die Konfigurationsdatei imitieren, um Zugangsdaten für Messsysteme zu erhalten. Daraufhin könnte der Angreifer Zustands-, Sensor-, und Messwerte abrufen und offenlegen (Güterwert 5).

Der Zugriffsschutz des Betriebssystems verhindert die Imitation der Konfigurationsdatei. Nur ein aktiver interne Angreifer mit Fähigkeit zur Korrumpierung des Betriebssystems kann einen solchen Angriff realisieren.

- Der Angreifer könnte die interne Datenbank imitieren und die Speicherung der aktuellen Zustands-, Sensor-, und Messwerte abfangen. Die Daten sind in Folge dessen für den Angreifer offengelegt (Güterwert 5). Auch könnte durch das Abfangen der Datenfluss zur internen Datenbank blockiert werden und die Darstellungsfunktion wird beeinträchtigt (Güterwert 4).

  Der Zugriffsschutz des Betriebssystems verhindert die Imitation der Konfigurationsdatei. Nur ein aktiver interne Angreifer mit Fähigkeit zur Korrumpierung des Betriebssystems kann einen solchen Angriff realisieren.

- Der Angreifer könnte den externen Speicher imitieren und die Speicherung der aktuellen Zustands-, Sensor-, und Messwerte abfangen. Die Daten sind in Folge dessen für den Angreifer offengelegt (Güterwert 5).

  Bei der Verwendung von TLS authentifiziert sich der Angreifer gegenüber dem Energiemanagement. Die Angreifer sind nach Annahme nicht in der Lage, an das Schlüsselmaterial des externen Speichers zu gelangen. Somit bleibt nur eine Manipulation des Energiemanagements, indem beispielsweise falsche Zertifikate installiert werden. Solche Angriffe kann nur der aktive interne Angreifer durchführen.

4.3.2.3 Unzureichende Eingabevalidierung

Eine unzureichende Eingabevalidierung eines Prozesses kann ein Angreifer nutzen, um Daten eines Datenspeichers zu manipulieren, Code entfernt auszuführen (siehe Kapitel 4.3.2.11), Prozesse oder Datenflüsse zu unterbrechen, oder Entitäten zu imitieren.

Die Möglichkeit, eine solche Bedrohung zu realisieren hängt von den Zugriffsmöglichkeit des Angreifers auf Datenflüsse und die Codequalität der Prozesse ab und muss im Einfall betrachtet werden. Prinzipiell kann die Angriffsfläche durch Maßnahmen wie Netzseparation, Pentesting, Fuzzing oder Code Reviews reduziert werden.

- Wenn Eingaben im Haushaltsgerät, Energiesensor oder Smart-Meter-Gateway nicht richtig validiert werden, könnte ein Angreifer dies ausnutzen, um weitere Angriffe durchzuführen. Beispielsweise könnten Geräte umkonfiguriert werden, um die Verfügbarkeit der Darstellungsfunktion zu beeinträchtigen (Güterwert 4). Es könnten auch Messwerte abgerufen werden und die Vertraulichkeit der Messdaten gefährden (Güterwert 5).

  Externe Angreifer und interne Angreifer im Gastnetz haben keinen Zugang zu den befinden (vgl. Abbildung 4.1). Nur Interne Angreifer können eine solche Bedrohung realisieren. Daher müssen alle Daten, die über unauthentifizierte Kommunikationskanäle verschickt werden, besonders sorgfältig geprüft werden.

- Eingabevalidierung im Energiemanagementsystem oder in SSH: Auch hier könnte ein Angreifer Steuerentscheidungen der Haushaltsmitglieder durch Beeinträchtigung der Verfügbarkeit verhindern (Güterwert 4) oder das Gerät korrumpieren und weitere Angriffe fahren. Der Angreifer könnte selbst Verbindungen zum Energiemanagementsystem aufbauen oder sich in vorhandene Verbindungen, z.B. dem Abruf eines externen Signals, einklinken (vgl. Kapitel 4.2.3, Zwischenschalten).

  Das Energiemanagementsystem ist aus allen Netzen erreichbar und damit können alle Angreifertypen eine neue Verbindung zum Energiemanagementsystem aufbauen und diese Bedrohung realisieren. Vorhandene Verbindungen können nicht Manipuliert werden, da sie durch (D)TLS bzw. SSH geschützt sind. Unauthentifizierte Daten müssen hier besonders geprüft werden.

4.3.2.4 Abstreitbarkeit des Empfangs von Daten und Abstreitbarkeit von Ereignissen im System

Abstreiten von Ereignissen oder Datenempfang können nur natürliche oder juristische Personen. Da im betrachteten System nur die Interessen von Haushaltsvorstand und Haushaltsmitglied relevant sind, ergeben sich nur wenige Bedrohungen durch Abstreitbarkeit:

- Ein Haushaltsmitglied könnte abstreiten, die Visualisierung genutzt zu haben.

  Da der Zugriff protokolliert wird, ist die Abstreitbarkeit zunächst möglich, solange der Zugriff ausschließlich über das Energiemanagementsystem erfolgt und das Protokoll nicht manipuliert wurde. Ein Haushaltsmitglied als aktiver interne Angreifer könnte allerdings das Protokoll manipulieren und die Abstreitbarkeit ausnutzen.

- Gäste oder Haushaltsmitglieder könnten abstreiten, Haushaltsgeräte genutzt zu haben.

  Die Möglichkeit, den aktuellen Zustand sowie deren historischen Zustandsverlauf der Haushaltsgeräte darzustellen, verringert die Wahrscheinlichkeit, dass diese Bedrohung realisiert wird. Eine Zuordnung von Gerätenutzung und Nutzer kann das System allerdings nicht ermitteln. Somit können Gäste oder Haushaltsmitglieder als passive interne Angreifer diese Bedrohung realisieren.

- Der Energiemanagementadministrator könnte abstreiten, die Konfigurationsdatei gelesen oder verändert zu haben.

  Das Lesen der Konfigurationsdatei ist keine zusätzliche Bedrohung da davon ausgegangen wird, dass er diese Daten ohnehin kennt.

  Änderungen sollten jedoch nicht abstreitbar sein. Das Einloggen und Ausloggen des Energiemanagementadministrators wird protokolliert. Das Energiemanagementsystem protokolliert ebenfalls mit, falls die Konfigurationsdatei geändert wurde.

Allerdings hat der Energiemanagementadministrator als aktiver interner Angreifer die Fähigkeit, das System zu korrumpieren und dadurch das Protokoll zu verändern. Der Energiemanagementadministrator kann dadurch Konfigurationsänderungen plausibel abstreiten.

4.3.2.5 Abhören des Datenflusses

Beim Übertragen von Zustands-, Sensor-, und Zählerdaten sowie der Konfiguration und dem Protokoll besteht die Gefahr, dass ein Angreifer den Datenfluss abhören kann. Die Übertragung über Netzwerk wird mit (D)TLS oder dem SSH-Protokoll verschlüsselt und ist vor dem Abhören sicher, solange der Angreifer das Schlüsselmaterial nicht kennt. Bei der Datenflüssen innerhalb einer Plattform sorgt der Zugriffsschutz des Betriebssystems für einen grundlegenden Schutz vor dem Abhören.

Externe Angreifer und passive interne Angreifer werden durch diese Maßnahmen vor einer Realisierung der Bedrohung abgehalten. Ein aktiver interner Angreifer kann durch Korrumpierung von einem der beteiligten kommunizierenden Komponenten oder dem Betriebssystem den Schutz aushebeln und erfolgreich abhören.

Die Bedrohung „Abhören des Datenflusses“ kann an folgenden Stellen im System auftreten:

- Ein Angreifer könnte die Übertragung der Gerätezustände, der externen Signale, der Sensormesswerte oder der Energiezählerwerte zum Energiemanagementsystem abhören.

  Dies wird durch den Einsatz von (D)TLS verhindert, solange der Angreifer keine an der Kommunikation beteiligten Geräte korrumpiert hat. Einen solchen Angriff kann damit nur von einem aktiven internen Angreifer durchgeführt werden.

- Der Angreifer könnte die Übertragung der Zustands-, Sensor-, und Zählerdaten an ein Haushaltsmitglied oder an den externen Datenspeicher abhören.

  Diese Übertragung wird das durch den Einsatz von TLS geschützt. Der externe Angreifer und passive interne Angreifer im Gastnetz können damit diese Bedrohung nicht realisieren. Ein aktiver interner Angreifer könne den Zertifikatsspeicher auslesen oder manipulieren, um eine Man-in-the-Middle-Attacke durchzuführen und ist in der Lage, diesen Datenfluss abzuhören.

- Der Angreifer könnte die Übertragung der Zustands-, Sensor-, und Zählerdaten zu und von der internen Datenbank abhören.

  Die Übertragung geschieht über Unix-Sockets, deren Zugriffskontrolle von dem Betriebssystem durchgesetzt wird. Nur ein aktiver interner Angreifer, der die Zugriffskontrolle aushebeln kann, ist in der Lage, die Übertragung abzuhören.

- Der Datenfluss zum Übertragen der Konfiguration oder des Protokolls über SSH könnte abgehört werden.

  Die Übertragung der Konfiguration wird durch das SSH-Protokoll vor dem Abhören geschützt. Durch einen aktiven Man-in-the-Middle-Angriff lassen sich die Übertragung abhören, was die Kenntnis von Schlüsselmaterials des SSH-Prozesses erfordert. Ein aktiver interner Angreifer kann somit einen solchen Angriff durchführen. Externe Angreifer und passive interne Angreifer können diese Bedrohung nicht realisieren.

4.3.2.6 Schwacher Transit von Zugangsdaten

Bei der Übertragung von Zugangsdaten könnten diese von einem Angreifer abgehört und wiederverwendet werden. Wiederverwendbare Zugangsdaten sind beispielsweise Benutzername/Passwort-Paare, wie sie bei der HTTP-Basic-Authorization übertragen werden. Solche Netzwerkverbindungen sind durch TLS geschützt, diese können jedoch unter Umständen von einem aktiven Angreifer abgehört werden. Aktive interne Angreifer können somit die Bedrohung realisieren, während externe Angreifer und passive interne Angreifer im Gastnetz nicht die Fähigkeit dazu haben.

Authentifikationsverfahren, die auf kryptographische Verfahren beruhen, übertragen in der Regel keine wiederverwendbaren Zugangsdaten und können durch Abhören nicht angegriffen werden.

Die Bedrohung „Schwacher Transit von Zugangsdaten“ kann an folgenden Stellen im System auftreten:

- Die Zugangsdaten eines Haushaltmitglieds für das Energiemanagementsystem könnten bei der Übertragung abgehört werden. Mit den Zugangsdaten kann ein Angreifer auf alle im Energiemanagementsystem gespeicherten Zustands-, Mess- und Zählerdaten zugreifen. (Güterwert 5)

  Die Übertragung der Zugangsdaten wird mittels TLS geschützt. Somit müsste der Angreifer das Energiemanagementsystem oder das Tablet korrumpieren, um die Übertragung abhören zu können. Dies gelingt nur einem aktiven internen Angreifer.

- Die Zugangsdaten des Energiemanagementsystems für ein Haushaltsgerät könnten bei der Übertragung abgehört werden. Dies dient als Grundlage für weitere Angriffe. Beispielsweise könnten die Zugangsdaten zum Auslesen der Gerätezustände genutzt werden und dadurch auf das Verhalten von Haushaltsmitgliedern aufzeichnen (Güterwert 5).

  Das Abhören der Zugangsdaten ist in diesem Fall durch die Verwendung von TLS verhindert. Das Haushaltsgerät authentifiziert sich zuerst gegenüber dem Energiemanagementsystem, bevor das Energiemanagementsystem die Zugangsdaten über-

mittelt. Nur aktive interne Angreifer können Energiemanagement oder Haushaltsgerät korrumpieren und die Kommunikation mit dem Haushaltsgerät vortäuschen.

- Die Zugangsdaten des Energiemanagementsystems für die externe Datenquelle könnten bei der Übertragung abgehört werden. Die Zugangsdaten könnten für weitere Angriffe genutzt werden. Beispielsweise, um die Verfügbarkeit der externen Datenquelle zu reduzieren (Güterwert 4).

  Das Abhören von Zugangsdaten ist nicht möglich, da zur Kommunikation TLS eingesetzt wird. Die externe Datenquelle authentifiziert sich, bevor die Zugangsdaten übertragen werden.

- Die Zugangsdaten des Energiemanagementsystems für den externen Speicher könnten bei der Übertragung abgehört werden. Die Zugangsdaten könnten für weitere Angriffe genutzt werden. Ein Angreifer kann die Zugangsdaten einsetzen, um bestenfalls die Verfügbarkeit des externen Widerspiegelns zu reduzieren (Güterwert 4). Hier nicht modelliert, aber höchstwahrscheinlich dienen die gleichen Zugangsdaten zum Widerspiegeln der gespeicherten Werte. Somit könnte der Angreifer die Vertraulichkeit der Zustands-, Mess- und Zählerdaten kompromittieren (Güterwert 5).

  Die Übertragung der Zugangsdaten ist mit TLS geschützt, allerdings könnte ein korrumpiertes Energiemanagementsystem diesen Schutz außer Kraft setzen. Nur aktive interne Angreifer könnten somit diese Bedrohung realisieren.

- Die Zugangsdaten des Energiemanagementsystems für einen Energiesensor können bei der Übertragung nicht abgehört werden, da Zertifikate, Priv/Pub Key oder symmetrische Schlüssel zum Einsatz kommen. Dabei werden keine wiederverwertbaren Zugangsdaten übertragen.

- Die Zugangsdaten des Energiemanagementadministrators für den SSH-Zugang können nicht abgehört werden, der Administrator sich mit Public-Key-Verfahren authentifiziert. Dabei werden keine wieder-verwertbaren Zugangsdaten übertragen.

4.3.2.7 Schwache Zugriffskontrolle auf Ressource

Durch Lücken in der Zugriffskontrolle, wie sie beispielsweise durch ein Betriebssystem durchgesetzt wird, könnte sich ein Angreifer Zugriff auf Datenbanken und andere Ressourcen beschaffen. Dabei muss der Angreifer in der Lage sein, Teile des Betriebssystems zu korrumpieren. Nur der aktive interne Angreifer hat diese Fähigkeit.

Die Bedrohung „Schwache Zugriffskontrolle auf Ressource“ kann an folgenden Stellen im System auftreten:

- Der Zugriffsschutz auf die interne Datenbank könnte unwirksam sein. Wenn sich ein Angreifer Zugriff verschaffen kann, kann er alle gespeicherten Zustands-, Mess- und Zählerdaten offenlegen. (Güterwert 5)

  Nach Annahme ist die Zugriffsschutz richtig konfiguriert, in dem nur das Energiemanagementsystem Zugriff auf die interne Datenbank hat. Allerdings könnte ein Angreifer das Energiemanagementsystem imitieren oder die Zugriffsrechte ändern. Das wird nur einem aktiven internen Angreifer gelingen, der sich bereits Zugang zum Betriebssystem des Energiemanagementsystems verschafft hat.

- Der Zugriffsschutz die Konfigurationsdatei könnte unwirksam sein. Wenn sich ein Angreifer Zugriff verschaffen kann, kann er zukünftige Zustands-, Mess- und Zählerdaten offenlegen. (Güterwert 5)

  Auch hier kann nur ein aktiver interner Angreifer diese Bedrohung realisieren, wenn er bereits das Betriebssystem korrumpiert hat.

4.3.2.8 Absturz eines Prozesses

Durch Ausnutzung von Schwachstellen könnte ein Angreifer Daten an ein Prozess schicken, der daraufhin verlangsamt wird, abstürzt oder hängt. Eine Voraussetzung dafür ist, dass der Angreifer fähig sein muss, Daten an den Prozess zu schicken. Durch die Trennung der Komponenten in Sicherheitszonen wird die Angriffsfläche reduziert, jedoch nicht vollständig verhindert. Zudem kann ein Angreifer möglicherweise physisch ein Prozess zum Absturz bringen. Nur externe Angreifer sind von einer Realisierung ausgeschlossen, interne Angreifer im Gastnetz und aktive interne Angreifer haben die Fähigkeit, mit entsprechenden Aufwand einen Prozess zum Absturz zu bringen.

An den folgenden Stellen im System kann die Bedrohung „Schwache Zugriffskontrolle auf Ressource“ auftreten:

- Ein Haushaltsgerät oder Energiesensoren könnten abstürzen, hängen, stoppen oder verlangsamt werden. Es werden keine Zustandsinformationen an das Energiemanagement gesendet und die Darstellungsfunktion ist beeinträchtigt (Güterwert 4). Der Komfort der Haushaltsmitglieder wird dadurch auch gemindert.

  Der Angreifer könnte durch bestimmte Eingaben über das Netzwerk oder direkt physisch am Gerät den Absturz auslösen. Über das Netzwerk hat nur der aktive interne Angreifer Zugriff, physisch jeder interne Angreifer. Die Bedrohung ist somit nur für den externen Angreifer nicht realisierbar.

- Das Energiemanagement, der SSH-Prozess und die interne Datenbank könnten abstürzen, hängen, stoppen oder verlangsamt werden. Haushaltsmitglieder könnten dadurch die Darstellungsfunktion nicht nutzen (Güterwert 4) und Messdaten könnten nicht aufgezeichnet werden. Wird der SSH-Prozess zum Absturz gebracht,

können keine Konfigurationsänderung erfolgen und die Protokolle können nicht eingesehen werden.

Die Prozesse laufen auf der selben Plattform und beispielsweise das Energiemanagement ist in jedem Netzwerk erreichbar. Ein Absturz kann durch eine Eingabe des Angreifers ausgelöst werden. Somit kann diese Bedrohung von externen Angreifern, internen Angreifern im Gastnetz und aktiven internen Angreifern realisiert werden.

- Das Tablet könnte abstürzen, hängen, stoppen oder verlangsamt werden. Die Darstellungsfunktion könnte über das Tablet nicht genutzt werden (Güterwert 4).

  Das Tablet befindet sich im Gastnetz und ist von internen Angreifern im Gastnetz und aktiven internen Angreifern erreichbar. Durch bestimmte Eingaben können eventuell Abstürze ausgelöst werden.

4.3.2.9 Unterbrechung des Datenflusses

Ein Datenfluss kann über ein Kommunikationsnetz abgewickelt werden, zwischen Komponenten auf einer Plattform stattfinden oder über eine physische Schnittstelle stattfinden. Ist ein Kommunikationsnetz beteiligt, können Angreifer mit Zugriff auf das beteiligte Teilnetz oder Sicherheitszone DoS-Angriffe durchführen (siehe Kapitel 4.2.4, Angriffe auf die Verfügbarkeit). Datenflüsse zwischen Komponenten auf einer Plattform werden durch das Betriebssystem vermittelt. Durch Angriffe wie die Erschöpfung von Ressourcen oder Anhalten von Prozessen kann ein Datenfluss unterbrochen werden.

Die Unterbrechung von Datenflüssen kann an folgenden Stellen im System auftreten:

- Der Datenfluss zwischen Energiemanagement und Haushaltsgeräte oder Energiesensoren könnte durch einen Angreifer unterbrochen werden. Damit ist die Verfügbarkeit der Widerspiegelungsfunktion beeinträchtigt (Güterwert 4).

  Nur der aktive interne Angreifer hat Zugriff auf das EMS-Netz, dessen Angriff nicht verhindert werden kann. Das EMS-Netz ist durch die Firewall des Smart-Home-Edge-Routers geschützt. Externe Angreifer oder interne Angreifer im Gastnetz können somit diese Bedrohung nicht realisieren.

- Der Datenfluss zwischen Energiemanagement und externe Datenquelle könnte durch einen Angreifer unterbrochen werden. Damit könnte die Verfügbarkeit von Teilen der Widerspiegelungsfunktion beeinträchtigt sein (Güterwert 4).

  Alle Angreifer können einen solchen Angriff durchführen, da es eine externer Kommunikationsvorgang ist.

- Der Datenfluss zwischen Energiemanagement und Smart-Meter-Gateway könnte durch einen Angreifer unterbrochen werden. Damit ist die Verfügbarkeit der Widerspiegelungsfunktion beeinträchtigt (Güterwert 4).

Nur der aktive interne Angreifer kann sich Zugriff zur Sicherheitszone Smart-Grid verschaffen, um den Datenfluss zu stören. Externe Angreifer oder interne Angreifer im Gastnetz können diese Bedrohung nicht realisieren.

- Der Datenfluss zwischen SSH und Energiemanagementadministrator könnte durch einen Angreifer unterbrochen werden. Der Administrator hat dadurch keinen Zugriff auf die Logdatei und die Konfiguration.

  Die Bedrohung ist nicht verhinderbar, aber vernachlässigbar. Da administrative Aufgaben selten anfallen, kann sich der Administrator direkt mit dem Energiemanagementsystem verbinden und erleidet höchstens einen Komfortverlust.

- Der Datenfluss zwischen Energiemanagement und Tablet könnte durch einen Angreifer unterbrochen werden. Damit ist die Verfügbarkeit der Widerspiegelungsfunktion beeinträchtigt (Güterwert 4).

  Wenn sich das Tablet im Haus befindet, ist es mit dem WLAN-Gastnetz verbunden. Nur interne Angreifer und interne Angreifer im Gastnetz können diese Bedrohung realisieren. Externe Angreifer haben keinen Zugriff auf hausinterne Netze.

- Unterbrechung des Datenflusses zwischen Energiemanagement und interner Datenbank. Die Messdaten können dadurch nicht gespeichert oder nicht gelesen werden und die Verfügbarkeit der Widerspiegelungsfunktion ist beeinträchtigt (Güterwert 4).

  Der Datenfluss findet im Betriebssystem statt und kann durch externe Ereignisse kaum gestört werden. Kann allerdings ein aktiver interner Angreifer das Betriebssystem korrumpieren, ist auch das möglich. Passive interne Angreifer im Gastnetz und externe Angreifer können diese Bedrohung nicht realisieren.

- Der Datenfluss zwischen Energiemanagement und externem Speicher könnte durch einen Angreifer unterbrochen werden. Damit könnte die Verfügbarkeit von Teilen der Widerspiegelungsfunktion beeinträchtigt sein (Güterwert 4).

  Alle Angreifer können einen solchen Angriff durchführen, da es einen externen Kommunikationsvorgang ist.

4.3.2.10 Elevation durch Imitation

Diese Bedrohung zielt auf die Fälle ab, in denen der Kontext einer Entität imitiert wird, um im Gesamtsystem im Vergleich zu einer Ausgangsentität mehr Rechte zu erlangen. Sämtliche Bedrohungen setzen voraus, dass bereits eine Entität vom Angreifer korrumpiert wurde und sind damit nur durch einen aktiven internen Angreifer realisierbar.

- Ein durch einen Angreifer korrumpiertes Tablet könnte ein Haushaltsmitglied imitieren, um zusätzliche Rechte zu erlangen.

Das Tablet könnte die Zugangsdaten eines Haushaltsmitglieds speichern und wiederverwenden, um auf das Energiemanagement zuzugreifen. Die geheimzuhaltenden Zustands-, Sensor-, und Messwerte könnten so dem Angreifer offengelegt werden (Güterwert 5).

Diese Bedrohung bleibt offen und durch keine Sicherheitsmaßnahme behandelt.

- Ein durch einen Angreifer korrumpiertes Haushaltsgerät oder Energiesensor könnte das Energiemanagement imitieren, um zusätzliche Rechte zu erlangen.

  Die Datenquellen könnten sich gegenseitig abfragen und Informationen gegenüber dem Angreifer offenlegen. Beispielsweise könnte ein Sensor das Energiemanagement imitieren, um Daten eines Haushaltsgeräts abzurufen. Dies gelingt jedoch nicht, da (D)TLS eingesetzt wird und das Schlüsselmaterial der anderen Datenquellen nicht bekannt ist.

  Gegenüber einem Haushaltsmitglied ein Energiemanagement zu imitieren ist nicht möglich, da die Messsysteme und die Haushaltsmitglieder keinen Zugriff auf die gleiche Sicherheitszone haben.

- Ein durch einen Angreifer korrumpiertes Tablet könnte den Energiemanagement imitieren, um zusätzliche Rechte zu erlangen.

  Das Tablet befindet sich in der Sicherheitszone „Infotainment Netz“ und kann sich höchstens gegenüber anderen Haushaltsmitgliedern als Energiemanagement ausgeben. Dies wird jedoch durch die Nutzung von TLS unterbunden.

- Ein durch einen Angreifer korrumpiertes Smart-Meter-Gateway könnte den Energiemanagement imitieren, um zusätzliche Rechte zu erlangen.

  Da sich das Smart-Meter-Gateway in der Sicherheitszone „Smart-Grid“ befindet, hat das Smart-Meter-Gateway keinen Zugang zu den anderen Kommunikationspartnern des Energiemanagements. Die Imitation kann somit nicht durchgeführt werden.

- Ein durch einen Angreifer korrumpiertes Energiemanagement könnte ein Haushaltsgerät, einen Energiesensor, ein Tablet, eine interne Datenbank oder eine externe Datenquelle imitieren, um zusätzliche Rechte zu erlangen.

  Da das Energiemanagement nahezu alle Daten verarbeitet, kann das Imitierten der Entitäten zu keiner Rechteerweiterung führen.

- Ein durch einen Angreifer korrumpiertes Energiemanagement könnte das Smart-Meter-Gateway imitieren, um zusätzliche Rechte zu erlangen.

  Durch Imitation des Smart-Meter-Gateways wären Zugriffe auf Geräte in der Sicherheitszone „Smart-Grid“ möglich. Da das Energiemanagement keinen Zugang zu dieser Zone hat, kann keine Imitation durchgeführt werden.

- Ein durch einen Angreifer korrumpiertes SSH könnte den Energiemanagementadministrator imitieren, um zusätzliche Rechte zu erlangen.

  Der Energiemanagementadministrator interagiert nur mit dem SSH-Prozess. Durch die Imitation des Energiemanagementadministrator kann der SSH-Prozess keine zusätzlichen Rechte erlangen.

4.3.2.11 Elevation durch Ausführung von Code aus der Ferne

Durch Ausnutzung von Schwachstellen könnte ein Angreifer beliebige Befehle in einem Prozess ausführen. Der Prozess wird dadurch korrumpiert und zahlreiche Folgeangriffe auf das System eröffnen sich dem Angreifer. Im Entwurf lässt sich lediglich die Angriffsfläche reduzieren, indem die Möglichkeiten des Angreifers, Code einzuschleusen, reduziert werden. Erst die Implementierung lässt sich mit Codeanalysen, Fuzzing und Pentesting prüfen.

In den folgenden Fällen sind wird zur Realisierung der Bedrohung von einem aktiven Angreifer ausgegangen. Von den betrachteten Angreifern ist nur der interne Angreifer ein aktiver Angreifer. Passiven Angreifer wird nach Definition nicht die Fähigkeit zugesprochen, Komponenten zu korrumpieren.

- Ein Angreifer könnte über ein korrumpiertes Haushaltsgerät, Tablet, Energiesensor, Smart-Meter-Gateway, interne Datenbank, als externe Datenquelle oder als Haushaltsmitglied fähig sein, beliebigen Code im Energiemanagement auszuführen.

  Dadurch bekommt der Angreifer Zugriff auf alle aufgezeichneten Zustands-, Sensor-, und Messwerte (Güterwert 5), in der Konfigurationsdatei gespeicherten Zugangsdaten und kryptographische Schlüssel. Da das Energiemanagementsystem in allen Netzwerken erreichbar ist, daher lässt sich diese Bedrohung nicht grundsätzlich abwehren.

- Ein Angreifer könnte über ein korrumpiertes Energiemanagement fähig sein, beliebigen Code im Smart-Meter-Gateway auszuführen.

  Der Angreifer wäre dadurch in der Lage, Zählerstände zu Manipulieren oder sich mit CLS-Geräten zu verbinden.

- Ein Angreifer könnte über ein korrumpiertes Energiemanagement fähig sein, beliebigen Code im Energiesensor auszuführen.

- Ein Angreifer könnte über ein korrumpiertes Energiemanagement fähig sein, beliebigen Code im Tablet auszuführen.

- Ein Angreifer könnte beliebigen Code im Haushaltsgerät auszuführen, entweder in der Rolle Haushaltsmitglied oder Gast, oder über ein korrumpiertes Energiemanagement.

Da Haushaltsgeräte physische Systeme sind, könnten die Geräte je nach Geräteklasse dazu gebracht werden, um Wasser- oder Feuerschäden zu verursachen.

- Ein Angreifer könnte als Haushaltsmitglied fähig sein, beliebigen Code im Tablet auszuführen.
- Ein Angreifer könnte als Energiemanagementadministrator fähig sein, beliebigen Code im SSH-Prozess auszuführen.

  Ein Angreifer in der Rolle Energiemanagementadministrator hat bereits sehr umfangreiche Rechte. Die Motivation könnte trotzdem darin liegen, das Protokoll zu manipulieren.

5 Fazit

Die eingesetzten Sicherheitsmaßnahmen im Entwurf entsprechen dem Stand der Technik. Trotzdem konnte durch die Bedrohungsanalyse gezeigt werden, dass einige der betrachteten Angriffe unter bestimmten Voraussetzungen immer noch durchgeführt werden können. Diese offenen Bedrohungen werden im Folgenden diskutiert.

Angriffe basierend auf korrumpierten Komponenten Die im Entwurf verwendeten Schutzmechanismen sind größtenteils wirkungslos, sofern ein Angreifer es schafft, einzelne Komponenten im Smart-Home so zu korrumpieren, dass der Angreifer

- geheimes Schlüsselmaterial auslesen kann,
- gespeicherte vertrauliche Informationen direkt ausgelesen können,
- Befehle des Angreifers auf den Komponenten ausgeführt werden können oder
- sich Zugriff auf weitere Sicherheitszonen im Netzwerk verschaffen kann.

Die Korrumpierung kann durch die Realisierung einer der folgenden Bedrohungen stattfinden:

- Unzureichende Eingabevalidierung,
- Schwacher Transit von Zugangsdaten,
- Elevation durch Imitation, oder
- Elevation durch Ausführung von Code aus der Ferne.

Diese Bedrohungen lassen sich kaum zur Entwurfszeit abmildern, da sie von Verwundbarkeiten in der Implementierung verursacht werden. Lediglich der schwache Transit von Zugangsdaten lässt sich vermeiden, indem keine wiederverwendbaren Zugangsdaten übertragen werden.

Der Schaden im Erfolgsfall solcher Angriffe ist jedoch meist auf die korrumpierten Komponenten beschränkt. Je nach Rolle der korrumpierten Komponente kann der Schaden entsprechend gering ausfallen. Erlangt der Angreifer beispielsweise durch Korrumpieren eines Sensors über diesen vollständige Kontrolle, so kann der Angreifer lediglich die Daten des Sensors auslesen bzw. fälschen. Sollten andererseits zentrale Komponenten wie der EMS-Router oder das EMS-System selbst korrumpiert werden, ist die Sicherheit des gesamten Systems zur Sammlung und Darstellung der Daten (siehe Kapitel 3) betroffen.

Angriffe auf die Verfügbarkeit Die Bedrohungsanalyse hat gezeigt, dass Angriffe auf die Verfügbarkeit des Netzes je nach Angreifer weiterhin möglich sind. Dies wird durch die eingesetzten Schutzmechanismen, insbesondere wenn ein Angreifer Geräte korrumpiert, nicht vollständig verhindert. Insbesondere der Verzicht auf QoS-Mechanismen und ein Intrusion-Detection-System machen die Verhinderung bzw. Erkennung von DoS-Angriffen schwierig bis unmöglich. Es bleibt zu untersuchen, inwieweit der Einsatz von IDS in Smart-Homes die Risiken möglicher Angriffe reduzieren kann.

Gegenseitige Überwachung unter Haushaltsmitgliedern Die Darstellung des Energieverbrauchs und der Gerätezustände erfolgt im aktuellen Entwurf für sämtliche Geräte im Haushalt und für alle Haushaltsmitglieder gleich. Somit kann jedes Haushaltsmitglied auf alle aufgezeichneten und aktuellen Daten zugreifen, auch von außerhalb des Hauses. Durch die Analyse dieser Daten lassen jedoch Rückschlüsse auf einzelne Ereignisse im Haushalt zu und die Haushaltsmitglieder lassen sich dadurch überwachen. Diese Form der Überwachung nicht direkt ersichtlich, wie es beispielsweise bei Kamerasystemen der Fall ist.

Diese Bedrohung konnte durch das entworfene System bisher nicht adressiert werden, da das System nicht in der Lage ist, Messdaten bestimmten Haushaltsmitgliedern als deren Verursacher zuzuordnen. Die Darstellung des Energieverbrauchs darf kein Mittel zur Überwachung werden. Daher muss nach Möglichkeiten geforscht werden, wie die Privatsphäre im Haushalt erhalten werden kann, ohne auf eine Analyse des Energieverbrauchs verzichten zu müssen.

Ein Ansatz beruht auf dem Aspekt, dass das entworfene System nicht in der Lage ist, die Verursacher bestimmter Messdaten zu bestimmen. Ist dies bekannt, kann eine effektive Zugriffskontrolle realisiert werden.

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073)*. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013. URL: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf`.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Technische Richtlinie (BSI TR-03109)*. Techn. Ber. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013. URL: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf`.

[3] T. Chown u. a. *IPv6 Home Networking Architecture Principles*. Draft by IETF Working Group: Home Networking. Revision 17. Internet Engineering Task Force, 2014.

[4] *IETF Home Networking (Active WG)*. Online. URL: `http://tools.ietf.org/wg/homenet/`.