Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik

Abschlussarbeit

zur Erlangung des akademischen Grades

Bachelor of Science (B.Sc.)

Entwurf, prototypische Implementierung und Evaluation eines Sicherheitskonzepts für die Authentifizierung und Autorisierung von Fernzugriffen auf eine Automatisierungsanlage

---

Vorgelegt von	Kevin Sapper
am	14. Oktober 2014
Referent	Prof. Dr. Reinhold Kröger
Korreferent	Prof. Dr. Martin Gergeleit

Erklärung gemäß ABPO

Ich erkläre hiermit,

- dass ich die vorliegende Abschlussarbeit selbstständig angefertigt,
- keine anderen als die angegebenen Quellen benutzt,
- die wörtlich oder dem Inhalt nach aus fremden Arbeiten entnommenen Stellen, bildlichen Darstellungen und dergleichen als solche genau kenntlich gemacht und
- keine unerlaubte fremde Hilfe in Anspruch genommen habe.

Wiesbaden, 14. Oktober 2014 _____

Kevin Sapper

Erklärung zur Verwendung der Bachelor-Thesis

Hiermit erkläre ich mein Einverständnis mit den im folgenden aufgeführten Verbreitungsformen dieser Abschlussarbeit:

Verbreitungsform	**Ja**	**Nein**
Einstellung der Arbeit in die Hochschulbibliothek mit Datenträger		×
Einstellung der Arbeit in die Hochschulbibliothek ohne Datenträger	×	
Veröffentlichung des Titels der Arbeit im Internet	×	
Veröffentlichung der Arbeit im Internet		×

Wiesbaden, 14. Oktober 2014 _____

Kevin Sapper

Zusammenfassung

Im Rahmen dieser Thesis wird ein Entwurf eines Sicherheitskonzept für Automatisierungsanlagen am Beispiel von Kälteanalgen mit Steuerungstechnik der Eckelmann AG entwickelt werden. Der Entwurf wird in einer prototypischen Implementierung erprobt, welche abschließend auf Tauglichkeit hin evaluiert wird.

Abstract

In the context of this thesis a security concept for automation systems is developed. As an example of such a system a refrigeration control systems with control engineering from the Eckelmann AG is used. The design is tested on a prototype implementation which is finally evaluated for suitability.

Inhaltsverzeichnis

> Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain.
>
> *Kevin Mitnick*

Kapitel 1

Einführung

Das Zielobjekt dieser Thesis ist eine Automatisierungsanlage, für diese soll ein Sicherheitskonzept zur Authentifizierung und Autorisierung von Fernzugriffen erstellt werden.

Die Bachelorarbeit wird bei der Firma Eckelmann AG in Wiesbaden-Erbenheim absolviert. Die Eckelmann AG ist ein mittelständisches Unternehmen mit circa 350 Mitarbeitern. Die Firmengeschichte reicht über 35 Jahren zurück. Sie wurde im Jahr 1977 von Dr. Gerd Eckelmann als Dr.-Ing. Eckelmann GmbH gegründet. Im Jahre 2001 findet die Umwandlung zur Eckelmann AG statt. Zur Eckelmann AG gehören mittlerweile 5 Tochtergesellschaften, davon drei in Deutschland, eine in China und eine in Tschechien. Seit 1986 gibt es den Standort in Erbenheim. Spezialisiert ist das Unternehmen in der elektrischen Automation von Maschinen und Anlagen. Die Leistungen gliedern sich dabei in die Bereiche Elektronische Entwicklung und Fertigung, Software-Entwicklung, Elektroanlagen und Schaltschrankbau sowie Vorgehensmodelle für die Entwicklung. Diese Leistungen werden in vielen verschiedenen Branchen, wie z.B. Maschinenbau, Chemie & Pharma, Schiffbau oder Industriekälte & Gewerbekälte, erbracht.

Eine Automatisierungsanlage besteht aus einer Reihe von Sensoren und Aktoren, die zentral und/oder dezentral automatisiert gesteuert werden. Die Automatisierungsanlage, die in dieser Thesis betrachtet wird, ist eine Kälteanlage für Supermärkte mit Steuerungstechnik der Eckelmann AG. Für die Steuerungstechnik der Anlagen gibt es mehrere beteiligte Parteien. Den Hersteller, den Besitzer sowie die Kältetechnikunternehmen. Besitzer spielen im Verlauf dieser Thesis lediglich eine untergeordnete Rolle, da diese meist die komplette Verantwortung an der Anlagen an die Kältetechnikunternehmen abgeben. Der Hersteller liefert die gesamte Technik, welche die Automatisierung und Überwachung der Anlage ermöglicht. Die Kältetechnikunternehmen sorgen für die Inbetriebnahme der Kälteanlage, führen regelmäßige

Wartungsarbeiten durch und Überwachen die Funktionstüchtigkeit. Der wichtigste Aspekt für die Thesis ist die Überwachung, welche in Fernservice-Zentralen der Kältetechnikunternehmen stattfindet. Dazu wird ein Fernzugriff auf die Kälteanlage zwingend benötigt. Der Fernzugriff ist eine kostengünstige Möglichkeit für die Kältetechnikunternehmen, viele Kälteanlagen zentral zu überwachen. Durch die Fernwartung ist es auch möglich, regulierend in das Ökosystem einer Kälteanlage einzugreifen, deswegen spielt der Aspekt der Nachvollziehbarkeit eine große Rolle für diese Unternehmen. Nachvollziehbarkeit wird durch Sicherheitsmaßnahmen erreicht, genauer durch Authentifizierung, Autorisierung und Auditing. Unter dem Schlagwort Industrie 4.0 werden immer mehr Firmen darauf aufmerksam, dass durch die zunehmende Vernetzung von Automatisierungsanlagen Sicherheitsrisiken durch Angreifer entstehen, welche das System aus der Ferne kompromittieren können. Durch die Anwendungsintegration zwischen Kälteanlage und Fernservice-Zentrale werden die Daten auch für Angreifer immer einfacher zugreifbar. Dies liegt auch daran, dass die proprietären Datenformate des Herstellers, die zwischen den Komponenten der Steuerungstechnik genutzt werden, für die Fernservice-Zentralen interpretiert und in menschenlesbare Formate gepackt werden. Um Maßnahmen gegen Angreifer umzusetzen, muss zunächst ein Überblick der möglichen Gefährdungen geschaffen werden. Aus diesem Grund werden Sicherheitskonzepte erstellt. Ein Entwurf eines solchen Sicherheitskonzeptes, mit Fokus auf Authentifizierung und Autorisierung, ist der Hauptbestandteil dieser Thesis. Für dessen Erstellung werden im Grundlagenteil verschiedene Vorgehensweisen betrachtet, dabei werden Vorgehen von Sicherheitsstandards und spezielle Methodiken zur Problemstrukturierung, bei der Bedrohungsanalyse, aufgegriffen. Die Grundlagen in Kapitel 2 vermitteln zudem alle zum Verständnis benötigten Kenntnisse über die Steuerungstechnik und bestehende Hardware- und Softwaremodule. In Kapitel 3 werden als erster Teil des Sicherheitskonzeptes die Bedrohungen allgemein, das heißt ohne auf bestimmte Technologien einzugehen, erfasst und Maßnahmen gegen diese gefunden. Kapitel 4 geht anschließend auf ein konkretes System ein. Hierbei liegt der Informationsfluss der Systemkomponenten im Fokus. Anhand der Gegenmaßnahmen aus Kapitel 3 und 4 führt Kapitel 5 eine prototypische Implementierung durch. Diese soll es erlauben, dass sich der Benutzer aus der Ferne sicher am System anmelden kann, um auf bestimmte Services zugreifen zu können. Abschließend wird durch eine Evaluation in Kapitel 6 die prototypischen Implementierung auf Tauglichkeit geprüft. Dadurch soll herausgefunden werden, ob sich das Konzept für den produktiven Einsatz eignet und welche Einschränkungen vorhanden sind.

Kapitel 2

Grundlagen

Dieses Kapitel soll die nötigen Grundkenntnisse zum Verstehen dieser Thesis vermitteln. Zunächst wird ein Überblick einer Kälteanlage, aus der Sicht der Eckelmann AG, vermittelt und wichtige Komponenten und Funktionen erläutert. Danach werden Sicherheitsstandards und Modelle beleuchtet, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt sowie Methodiken zum Vorgehen an eine Bedrohungsanalyse erklärt. Abschließend werden die verbreitetsten Verfahren zur Authentifizierung aufgelistet.

2.1 Kälteanlagen

Die genaue Funktionsweise einer Kälteanlage ist für diese Arbeit nicht relevant. Dennoch gibt es einige Aspekte, die ein Sicherheitskonzept beeinflussen können. Einer dieser Aspekte ist die Trägheit. Beim Einsatz von Kälte geschieht nichts in Bruchteilen von Sekunden. Das Kühlen von Waren ist, ebenso wie das Erwärmen, ein langsamer Prozess. Im Folgenden befindet sich eine Auflistung von Komponenten einer Kälteanlage, welche für das Sicherheitskonzept von Relevanz sind. Die Beschreibungen der Komponenten einer Kältekälteanlage beziehen sich auf die Firma Eckelmann und können von Systemen anderer Hersteller abweichen.

2.1.1 E*LDS

E*LDS (Long-Distance-Service) ist die Produktreihe, die von der Eckelmann AG zur Steuerung und Verwaltung von Kälteanlagen entwickelt wird. Abbildung 2.1 zeigt die typische Vernetzung der Komponenten. Diese beinhaltet Verbundsteuerungen zur Kälteerzeugung, Kühlstellenregler zur temperaturgenauen Reglung aller Arten von Kühlmöbeln und Kühlräumen, Funk-Temperatursensoren und den Markt-

rechner als zentrale Intelligenz einer Kälteanlage [3]. Über den seriellen Feldbus Controller Area Network (CAN) sind sämtlichen E*LDS-Komponenten der Anlage verbunden. Zusätzlich können über die Modbus-Schnittstelle, welche ebenfalls ein serieller Feldbus ist, Fremdsysteme anderer Hersteller angebunden werden. Für die Vorort-Bedienung kann der Touch-Screen des Marktrechners genutzt werden. Alternativ kann ein PC mit einem CAN-Bus-PC-Adapter verbunden werden und über die Software LDSWin zugreifen. Der Fernzugriff kann über eine Wählverbindung (Modem) oder über VPN, je nach Verfügbarkeit, geschehen. Auch hier wird der Zugriff durch die Software LDSWin ermöglicht.

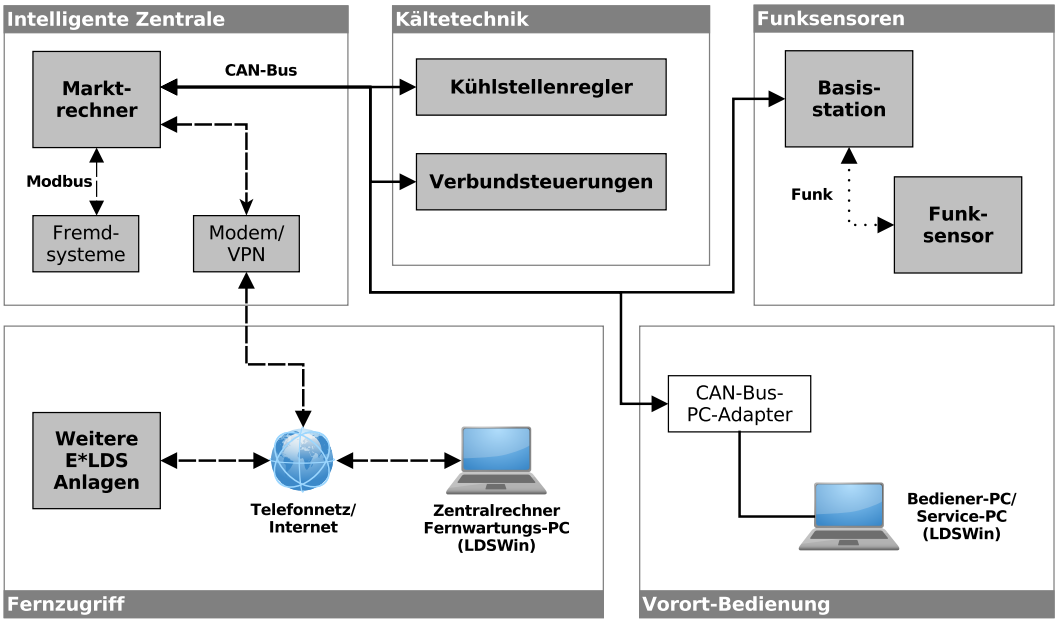

Abbildung 2.1: Übersicht einer Kälteanlage

2.1.2 Marktrechner

Betrachtet man eine Kälteanlage, dann ist der Marktrechner ihr Herzstück. Über den CAN-Bus ist er in der Lage, Komponenten zentral zu parametrieren und zu überwachen. Sämtliche Betriebsdaten und Betriebszustände, Meldungen und Alarme aus der Überwachung werden auf seinem internen Speicher archiviert [3].

Hardware Der Marktrechner verfügt über einen 32-Bit-Prozessor aus der ARM-Prozessorfamilie. Für die persistente Datenspeicherung steht eine fest verbaute SD-Karte zur Verfügung und 256-MB flüchtigen Speicher sind vorhanden. Als Zentrale Komponente benötigt der Marktrechner einige Schnittstellen für die Kommunikation, diese sind in Abbildung 2.2 zu sehen. Über den Ethernet-Port ist der

Marktrechner mit dem Unternehmensnetzwerk verbunden, darüber kann die Fernwartung erfolgen. Über die drei RS-232 COM-Schnittstellen kann ein PC vor Ort angeschlossen werden, die Fernwartung via Modem erfolgen, das M-Bus-Gateway zur Verbrauchsdatenerfassung verbunden oder Sonderfunktionen, beispielsweise Gebäudeleittechnik oder sonstige Fremdsysteme, integriert werden. Über die RS-485 COM-Schnittstelle besteht die Möglichkeit Modbus-Regler hinzuzufügen. Die USB-Anschlüsse sind für zukünftige Benutzung vorgesehen. Einer der beiden CAN-Bus-Anschlüsse wird benutzt, um mit den E*LDS-Komponenten zu kommunizieren. Der zweite CAN-Anschluss ist ebenfalls für zukünftige Benutzung vorgesehen. Über die zwei Digitaleingänge können entweder Alarme entgegengenommen oder Energiezähler ausgelesen werden. Die Benutzerinteraktion findet über ein 7-Zoll Touch-Display statt.

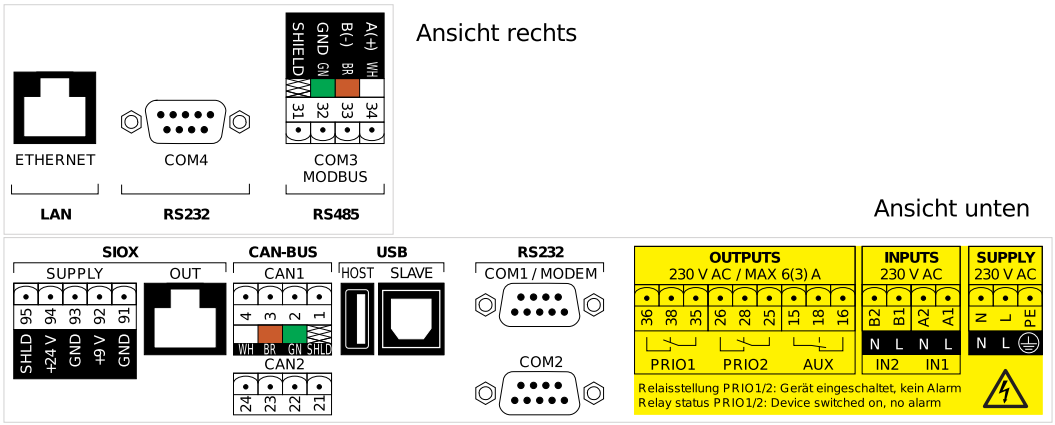

Abbildung 2.2: Schnittstellen des Marktrechners

Software Das Betriebssystem auf dem Marktrechner ist eine eigene Linux-Distribution, welche mit der Software ptxdist der Pengutronix e.K. erstellt wird. Ptxdist bringt einige hundert Module und Bibliotheken mit. Darunter sind etwa der leichtgewichtige HTTP-Server lighttpd, der SSH-Server openssh oder das Synchronisierungstool rsync. Mit ein wenig Konfigurationsaufwand können auch eigene Module hinzugefügt werden. Über eine Toolchain, die ebenfalls von der Pengutronix e.K. geliefert wird, kann eine sehr schlanke Distribution für viele Prozessorarchitekturen erzeugt werden, die auf den eigenen Software-Stack zugeschnitten ist. Die eigenen Softwaremodule sind in C++ geschrieben und nutzen das Qt-Framework.

Funktionen Alle Daten und Meldungen, die der Marktrechner sammelt und aufbereitet, müssen ausgewertet werden. Die 24-Stunden-Überwachung vor Ort, durch einen Mitarbeiter des Eigentümers, ist nicht wirtschaftlich. Auch das fachliche Wissen zur Betreuung einer Kälteanlage ist beim Endkunden nicht vorhanden. Deshalb

übernehmen heutzutage großteils Fernservice-Zentralen (FSZs) die Überwachung von Kälteanlagen. FSZs haben in der Kältetechnik ausgebildete Mitarbeiter, die Daten und Meldungen der Marktrechner interpretieren können. Der Marktrechner kann aus der Ferne über eine Ethernet- oder eine Modem-Verbindung erreicht werden. Letztere wird, aufgrund ihres aussterbendes Charakters, an dieser Stelle nicht weiter betrachtet. Für den Zugriff auf die Ethernet-Schnittstelle sind Fernservice-Zentralen über VPN mit einem oder mehreren Unternehmensnetzwerken ihrer Kunden verbunden (Abbildung 2.3). Über dieses können die Marktrechner erreicht werden. Auf diese Weise kann eine einzige Fernservice-Zentrale tausende Marktrechner überwachen. Der Marktrechner fungiert dabei als Server, das heißt, Daten und Meldungen müssen aktiv von einer Fernservice-Zentrale abgeholt werden. Ist aus den abgeholten Daten ersichtlich, dass ein Fehler in der Anlage aufgetreten ist, kann die Fernservice-Zentrale entweder direkt eingreifen oder einen Monteur zum betreffenden Kunden schicken, der die Anlage instand setzt.

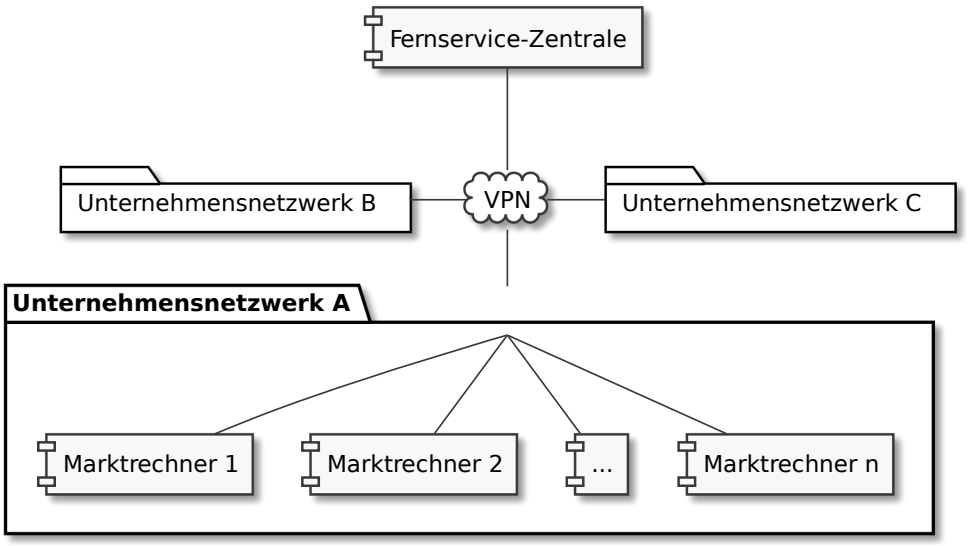

Abbildung 2.3: Aktuelle Architektur

Beim Einsatz von VPN ist die Kommunikation von der Fernservice-Zentrale bis zum Unternehmensnetzwerk abgesichert. Im Lokal Area Network (LAN) des Unternehmens ist der gesamte Datenverkehr zu und von den Marktrechnern allerdings unverschlüsselt. Aktuell gibt es zwei Arten von Datenverkehr zwischen Marktrechner und FSZ, zum einen über das proprietäre Protokoll des Herstellers und zum anderen über Webservices auf Basis von einfachen XML-RPCs.

2.1.3 RestGateway

Das RestGateway ist die Neuauflage des XML-RPC. Es wurde vom Author dieser Thesis im Rahmen des vor der Thesis absolvierten Praktikums entwickelt. Es basiert auf dem Representational State Transfer (REST) Konzept zur Entwicklung von Webanwendungen. REST ist keine explizite Norm, sondern bezeichnet vielmehr die Idee, dass eine URL genau einen Ressource oder eine Liste von Ressourcen als Ergebnis einer serverseitigen Aktion liefert [5]. REST nutzt Standard HTTP-Befehle, um lesend und schreibend auf Ressourcen zuzugreifen. Zur Zeit sind ausschließlich lesende Zugriffe implementiert, welche über URLs abgerufen werden können. Diese Aufrufe liefern interpretierte Inhalte im XML- oder JSON-Format. Zudem gibt es eine generische Schnittstelle, welche als Proxy für CAN-Nachrichten fungiert, wodurch beliebige CAN-Nachrichten über HTTP/S gesendet werden können. Auch solche, die schreibend auf das System zugreifen. Das RestGateway bietet keinerlei Mechanismus für die Authentifizierung und Autorisierung. Eine Erweiterung wäre auf Basis dieser Arbeit vorgesehen. Das RestGateway kann in zwei Ausführungen installiert werden, entweder als Modul auf dem Marktrechner (Abbildung 2.4), oder auf einem externen Server (Abbildung 2.5). Die unterschiedlichen Ausführungen werden durch das LanGateway-Modul des Marktrechners ermöglicht. Dieses ist eine TCP-Schnittstelle, welche als Proxy zwischen TCP-Netzwerk und CAN-Netzwerk fungiert. Über TCP werden die CAN-Nachrichten, ohne Daten-Wrapper wie XML, als Bytestrom übertragen.

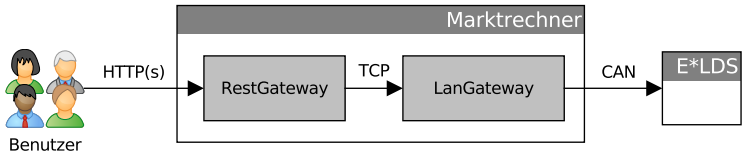

Abbildung 2.4: RestGateway als Marktrechner-Modul

Intern ist das RestGateway ein Wrapper über dem LanGateway, welches interpretierte Inhalte in einem menschenlesbaren Format liefert.

Extern bietet das RestGateway die Möglichkeit, über die REST-Schnittstellen verschiedene Marktrechner abzufragen. Dieses Feature ist vor allen Dingen für Fernservice-Zentralen interessant, da dort viele Marktrechner verwaltet werden (vgl. 2.1.2). Des Weiteren können über diesen Weg neue Funktionen ohne großen Installationsaufwand erprobt werden, denn es wird kein aufwendiges Update der Marktrechner-Software notwendig. Ein solches Update ist deshalb so aufwendig, da zahlreiche Marktrechner aktualisiert werden müssen und dies jeweils vor Ort geschehen muss, was zu erheblichen Kosten führt.

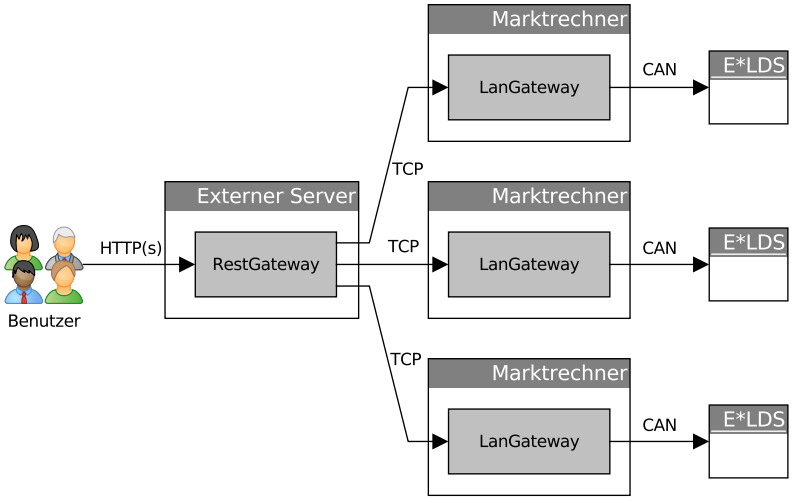

Abbildung 2.5: RestGateway auf externen Server

2.1.4 Alarmmanagement

Das Alarmmanagement beschreibt die Reaktion auf Fehlfunktionen einer Kälteanlage. Jede Kälteanlage ist anders aufgebaut und nutzt unterschiedliche Kühlmöbel, weshalb Alarme speziell konfiguriert werden müssen. Ein Alarm trifft eine Aussage über den Betriebszustand der Kälteanlage, beispielsweise soll ein Alarm ausgelöst werden, wenn die Temperatur in einem Kühlmöbel einen bestimmten Grenzwert über- beziehungsweise unterschreitet. Damit auf Alarme reagiert werden kann, werden Anlagen überwacht. Alarme können von Fernwarten in bestimmten Intervallen, etwa alle 15 Minuten, ausgelesen werden. Alternativ können Alarme durch das System selbstständig, per E-Mail- oder per Kurzmitteilung (SMS), versenden werden. Zusätzlich ist im Marktrechner eine Hupe installiert, die auf Fehlfunktionen vor Ort aufmerksam macht.

2.1.5 Offline-Konfiguration

Eine Offline-Konfiguration ist eine an den Markt angepasste Konfiguration der Kälteanlage, welche vor Inbetriebnahme erstellt wurde. Ein Teil ist unter anderem die genaue Parametrierung der Kühlgeräte und Kühlmöbel, unter Berücksichtigung der darin zu lagernden Waren. Ein weiterer Teil der Offline-Konfiguration sind auch die Alarme. Die technische Konfiguration des Marktrechners, beispielsweise Netzwerkkonnektivität, Internetzugang oder Berechtigungsnachweise, sind aktuell nicht in der Offline-Konfiguration enthalten.

2.2 Sicherheit

Viele Sicherheitssysteme heutzutage sind *"sicher"*, da sich niemand die Mühe gemacht hat, diese anzugreifen [50, s. 0]. Ein Großteil der Probleme von Sicherheitskonzepten entsteht, weil die Anforderungen an Sicherheit erst im Nachhinein aufkommen, wenn das eigentliche System schon fertig konzipiert oder implementiert ist. Meist wird dann versucht, die Sicherheit irgendwie noch an das System anzuheften. Sicherheit wirkt in diesen Fällen oft wie ein fünftes Rad am Wagen, wodurch Systeme entstehen, die für den Anwender extrem mühselig zu benutzen sind. Dabei sollte berücksichtigt werden, dass Benutzer Sicherheit lieber ausschalten oder umgehen, als sich damit auseinanderzusetzen [50, s. 5].

Bevor über potentielle Eigenschaften eines Sicherheitssystems nachgedacht wird, ist daher zunächst das Umfeld zu betrachten, in welchem das System eingesetzt werden soll [50, s. 4]. Wird heutzutage über Sicherheit diskutiert, so ist meistens ausschließlich die Kryptographie gemeint. Auch wenn die Kryptographie ein Hauptbestandteil jedes Sicherheitssystems ist, ignorieren praktisch alle Angriffe diese und attackieren den Weg wie diese genutzt wird [50, s. 1]. Ein bekanntes Beispiel ist der Heartbleed-Bug[1], der eine Lücke in der Heartbeat-Implementierung der OpenSSL Bibliothek ausnutzt, um sich Zugriff auf den privaten Kommunikationsschlüssel zu verschaffen. Es ist daher nicht sinnvoll, die kryptographischen Mittel auszureizen, wenn kein Angreifer versucht diese zu attackieren. Zudem wird durch Verschlüsselung das Hauptproblem eines Sicherheitssystems, nämlich *"Vertrauen"*, nur unzureichend betrachtet. Das Problem, die Authentifizierung effizient und zuverlässig über einen einzigen Kommunikationskanal zu lösen, besteht bis heute, ohne dass es eine etablierte Lösung dafür gibt (vgl. 2.3).

Teil des Sicherheitskonzeptes dieser Arbeit wird es sein, dieses Authentifizierungsproblem auf geeignete Weise zu berücksichtigen, ohne dass durch den Einsatz einer bestimmten Technologie im Extremfall enorme Kosten entstehen können. Ein solcher Extremfall würde eintreten, wenn beispielsweise durch die Kompromittierung der Software oder Hardware alle Berechtigungsnachweise manuelle ausgetauscht werden müssen.

2.2.1 Sicherheitsstandards

Sicherheitsstandards sind von staatlichen Behörden oder Organisationen (DIN, ISO) festgelegte Anforderungen an sichere Systeme, die sich anhand von Stufen klassifizieren. Je höher die Stufe, desto mehr Aufwand ist nötig, um das Sicherheitsniveau zu gewährleisten. Der erste Sicherheitsstandard mit hohem Verbreitungsgrad war

[1] (Q2/2014) weitere Informationen unter http://heartbleed.com

der Trusted Computer System Evaluation Criteria (TCSEC) und wurde 1983 vom amerikanischen Department of Defense (DoD) veröffentlicht. Vor 1990 veröffentlichten auch andere Regierungen, unter anderen Kanada, Westdeutschland, Frankreich und Großbritannien eigene Standards. Da diese Standards nur in den jeweiligen Ländern verwendet wurden und es keine internationale Anerkennung gab, hat die EU 1990 den Standard Information Technology Security Evaluation Criteria (ITSEC) für europäische Staaten veröffentlicht. Dieser Standard war jedoch auf Europa begrenzt, weshalb 1996 mit den Common Criteria for Information Technology Security Evaluation (CC) ein weltweit anerkannter Standard gebildet wurde. Beteiligte Staaten an den CC sind Australien/Neuseeland, Kanada, Frankreich, Deutschland, Japan, Niederlande, Spanien, Großbritannien und die USA.

Common Criteria for Information Technology Security Evaluation

Die Common Criteria for Information Technology Security Evaluation sehen sieben Sicherheitsstufen für die Klassifizierung vor. Diese Evaluation Assurance Level (EAL) sind bis Stufe 4 international anerkannt. Der Aufwand, der für die Stufen 5-7 betrieben werden muss, ist allerdings so umfangreich, dass er nur für eine Minderheit an Unternehmen in Frage kommt. Die aktuelle Version 3.1. Release 4 wurde im September 2012 veröffentlicht. Alle weiteren Erläuterungen beziehen sich auf diese Version und sind den Quellen [53, 54, 55, 49] entnommen.

Klassifizierung Die Klassifizierung wird in Abbildung 2.6 gezeigt. Die sieben EAL-Stufen haben Anforderungen in sechs Assurance-Klassen (Assurance class), wobei eine Assurance-Klasse aus mindestens einer Assurance-Familie (Assurance Family) besteht. Die Familien sind dabei selbst in Stufen eingeteilt. Die Anzahl der Stufen in den Familien ist von Familie zu Familie unterschiedlich. Beispielsweise fordert EAL-3 aus der Klasse "Tests" in der Familie "Analyse der Abdeckung" (ATE_COV) die Stufe 2 und EAL-7 aus der gleichen Familie Stufe 3. Einige Familien sind erst ab höheren EAL Stufen erforderlich.

Vorgehen Für die Zertifizierung sehen die CC zwei Möglichkeiten vor: Zum einen kundengetrieben, zum anderen entwicklergetrieben. Bei der ersten Möglichkeit stellt der Kunde seine Anforderungen an Hardware und Software in einem Protection Profile (PP) zusammen. Anhand dessen kann er das im PP beschriebene System oder Produkt in Auftrag geben. Alternativ kann er anhand dessen existierende Lösungen evaluieren. Die Entwickler müssen mit dem Security Target (ST) nachweisen, dass das entwickelte System/Produkt den Anforderungen aus dem Protection Profile genügt. Mit Hilfe von PP und ST kann von einer unabhängigen Prüfstelle zertifiziert

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Abbildung 2.6: Evaluation assurance level Zusammenfassung aus [49]

werden, dass die Inhalte und die Umsetzung der beiden Dokumente der Wahrheit entsprechen.

Die Inhalte aus Protection Profile und Security Target sind großteils identisch. Das ST muss jedoch zusätzlich konkrete beschreiben, wie die Anforderungen des PP erfüllt wurden. Bei der zweiten Möglichkeit fällt der Kunde weg und die Entwickler schreiben ein Security Target, um von einer Prüfstelle ein Zertifikat zu erhalten, welches als Qualitätsmerkmal ihres Produktes beworben werden kann. Die Beschreibung des Erfüllen von Anforderungen ist stark produkt- bzw. systemabhängig und wird daher nicht weiter erläutert.

Protection Profile Die Erstellung eines Protection Profiles wird im folgenden mit der Erklärungs-Methode beschrieben, welche aus insgesamt sechs Teilen besteht. Das Vorgehen dieser Methode soll vor allen Dingen Verständlichkeit beim Leser schaffen. Die Informationen darüber stammen aus [49].

1. Als erstes werden Konformitätsansprüche beschrieben. Darunter fallen Ver-

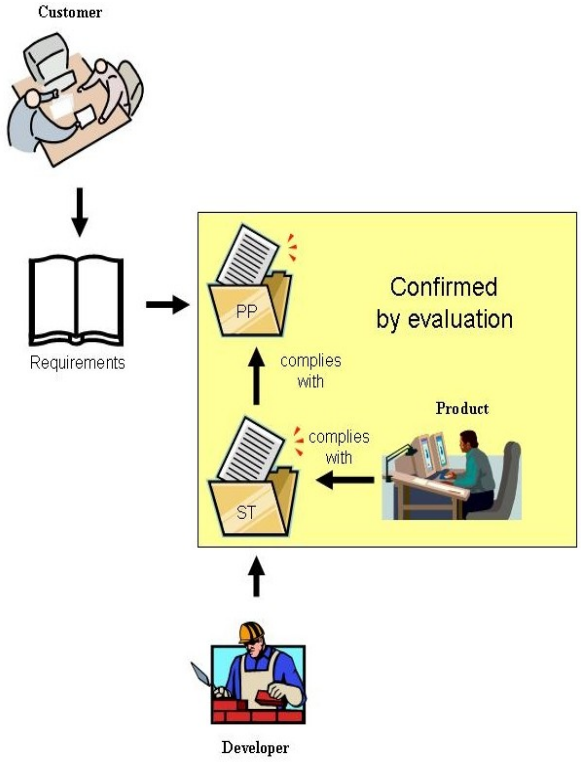

Abbildung 2.7: Common Criteria Vorgehen aus [49]

weise auf die Version des CC, abhängige Protection Profile und welche EAL-Pakete genutzt werden. Abschließend wird noch beschrieben, wie strikt sich PPs und STs, die diese PP benutzen wollen, an die Inhalte halten müssen.

2. Im zweiten Schritt werden die Sicherheitsprobleme definiert. Dabei werden in Bezug auf das zu evaluierende Ziel (Target of Evaluation–TOE) Gesetze, sonstige Regulierungen und Bedrohungen analysiert. Bei den Bedrohungen liegt der Fokus auf den zu schützenden Gütern.

3. Im dritten Schritt werden zu den Sicherheitsproblemen aus dem vorherigen Schritt abstrakte, präzise Lösungsvorschläge erarbeitet. Dabei soll sich auf das "Was" konzentriert werden und nicht beschrieben werden, "Wie" etwas zu lösen ist. Im CC-Kontext heißen diese Lösungsvorschläge Security Objects.

4. Im vierten Schritt wird für jedes Security-Object ein detailliertes Security Functional Requirement (SFR) erfasst. Die SFRs werden dabei an relevante, thematische Gruppen gekoppelt, welche im CC-Standard vorgegeben sind. Die Beschreibung als SFR umfasst die Beteiligten, die Informationsflüsse, die Operationen und die Daten. Mit Abschluss dieses Schrittes sind die Sicherheitsanforderungen an das System beziehungsweise Produkt festgelegt.

5. Im Schritt fünf werden Security Assurance Requirements (SAR) festgelegt. Diese sagen aus, wie das TOE zu evaluieren ist und ermöglichen dadurch den Vergleich von zwei Security Targets.

6. Die Einleitung kommt zum Schluss, sie fasst die Inhalte des PP in Prosa zusammen und führt den Leser in die Thematik ein.

2.2.2 Sicherheitsmodell

Ein Sicherheitsmodell bietet einen Leitfaden zur Erstellung eines Sicherheitskonzeptes. Ein ganzheitliches Modell stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem IT-Grundschutz vor.

BSI-Sicherheitsmodell

Folgende Ausführungen sind den BSI IT-Grundschutzempfehlungen entnommen [14, 15, 16, 17]. Das Ziel des Grundschutzes ist das Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus für IT-Systeme [4]. In Abbildung 2.8 sind die empfohlenen Schritte des BSI-Modells gezeigt.

Schritt eins verlangt die Erfassung aller Komponenten im Geltungsbereich. Dazu soll das Zusammenspiel zwischen Geschäftsprozessen und Anwendungen herausgearbeitet werden. Als nächstes soll der Schutzbedarf der Komponenten aus Schritt eins ermittelt werden. Der ermittelte Schutz soll gemäß der eingesetzten Informationstechnik ausreichend beziehungsweise angemessen sein. Anhand dieser Informationen werden für die Zielobjekte aus Strukturanalyse und Schutzbedarf Bausteine aus dem IT-Grundschutz gewählt. Der anschließende Basis-Sicherheitscheck soll das aktuelle Sicherheitsniveau einschätzen und liefert als Ergebnis eine Liste der relevanten Maßnahmen und ihren Umsetzungsstatus "entbehrlich", "ja", "teilweise" oder "nein". Dafür sollen Gefährdungenkataloge und Maßnahmenkataloge des BSI genutzt werden. In Schritt vier wird geprüft, ob die Standard-Sicherheitsmaßnahmen ausreichend sind, was für die meisten typischen Geschäftsfelder der Fall sein sollte. Sollten erweitere Sicherheitsmaßnahmen nötig werden, müssen für diese Risikoanalysen durchgeführt werden. Bei den Standard-Sicherheitsmaßnahmen ist dies bereits durch die IT-Grundschutz-Kataloge abgedeckt.

Ab Schritt sechs erfolgt die Durchführung der Maßnahmen. Bei der Konsolidierung wird geprüft, welche Maßnahmen aus den IT-Grundschutz-Katalogen tatsächlich in der Praxis umsetzbar sind. Teilweise müssen einige Maßnahmen noch an Gegebenheiten im Unternehmen angepasst werden. Unter Berücksichtigung des verfügbaren Budgets und des verfügbaren Personals werden die entsprechenden Maßnahmen

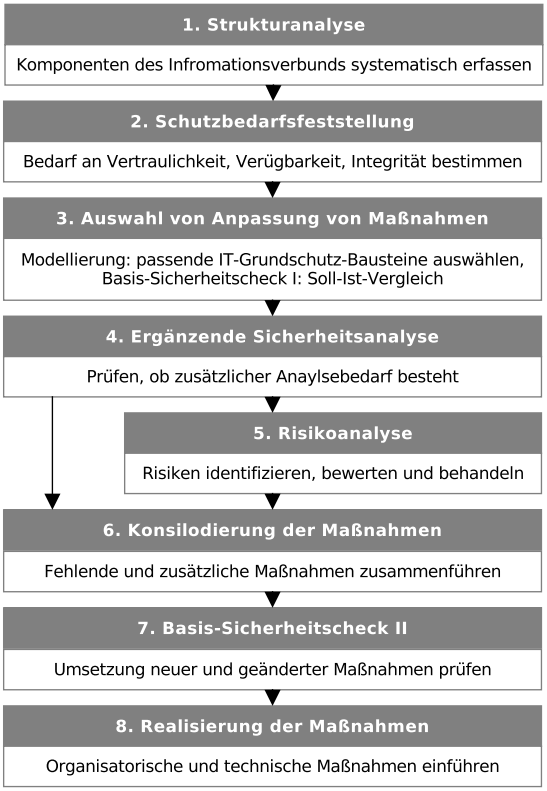

Abbildung 2.8: BSI Sicherheitskonzept[2]

für die Umsetzung geplant. Im zweiten Sicherheitscheck wird abschließend ein erneuter Soll-Ist-Vergleich durchgeführt, um die Ergebnisse der Maßnahmen zu überprüfen. Als letzter Schritt werden die Maßnahmen im Alltagsgeschäft in Betrieb genommen.

Das vom BSI vorgeschlagene Konzept und das damit verbundene Vorgehen betrachtet ein Sicherheitsmodell ausgiebig aus technischer Sicht. Es wurde entwickelt, um als internationaler Standard genutzt zu werden, hat dort jedoch aufgrund schlechter englischer Übersetzungen keinerlei Verbreitung. Auch in Deutschland ist die Verbreitung nur sehr gering [56].

2.2.3 Methoden zur Bedrohungsanalyse

Zusätzlich zum Vorgehen des BSI werden weitere Methoden für die Bedrohungsanalyse vorgestellt, die nützlich für das Erstellen eines Sicherheitskonzepts sind. Aufgrund von Finanznöten des BSI kann sich nicht darauf verlassen werden, dass die Inhalte des IT-Grundschutzes immer aktuell sind [52].

[2]Der Zeichnung [18] des BSI nachempfunden, aufgrund unangemessener Bildqualität

Soft Systems Methodology

Nachfolgende Erläuterungen beziehen sich auf [50, s. 252]. Das Lösen von Sicherheitsproblemen ist ein kniffeliges Unterfangen, da die typische Vorgehensweise von vielen Informatikern, ein Problem mit Technologien zu bewerfen, nicht funktioniert. Fragt man diese–"Wie löst man das Problem, Benutzer sicher über das Internet zu authentifizieren?"–dann werden Antworten wie OpenID, LDAP, SecurID oder ähnliches zu hören sein. Nur die wenigsten werden fragen–"Wer soll, wo, wogegen authentifiziert werden, wie benutzerfreundlich (einfach) kann der Mechanismus sein und welches Budget steht zur Verfügung?"–Um das natürliche Verlangen, die Lieblingstechnologie verwenden zu wollen, zu unterdrücken, ist es sinnvoll, Problem Structuring Methods (PSK) einzusetzen. Eine dieser PSK-Methoden ist die Soft Systems Methodology (SSM).

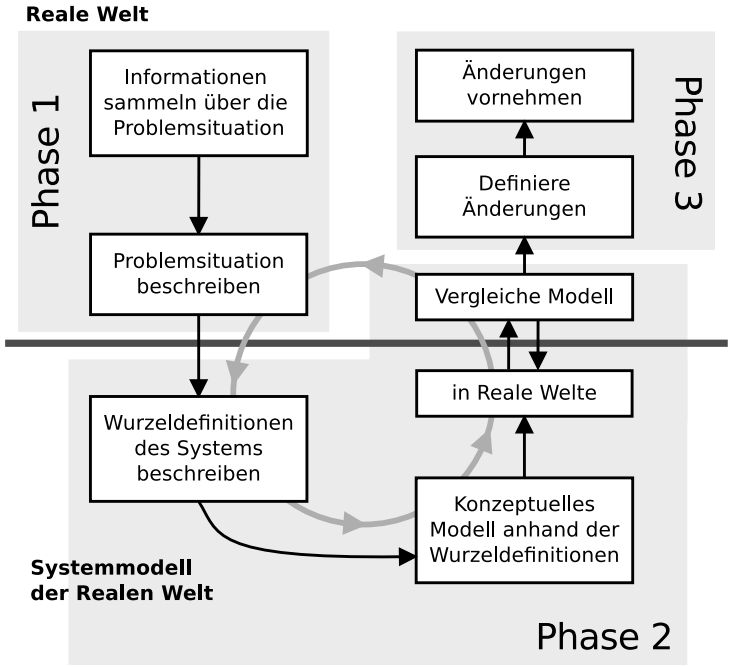

Abbildung 2.9: Soft Systems Methodologie

Die folgenden Inhalte sind den Quellen [8, 62, 59] entnommen. Die Entwicklung von SSM begann in den späten 60er Jahren an der Universität von Lancaster und wurde von Peter Checkland geleitet. Es war zunächst als Modellierungswerkzeug gedacht, wird aber hauptsächlich als Lern- und Bedeutungswerkzeug angesehen, denn SSM kann prinzipiell immer dann eingesetzt werden, wenn jemand versucht, zielgerichtet zu handeln. Das Forscherteam um Peter Checkland hat SSM, beispielsweise während des Flugzeug-Projekts Concorde, eingesetzt, bei welchem Sie beauftragt wurden zu helfen. Ein wichtiger Teil von SSM ist die Weltanschauung, welche einem

Vorgehen Sinn und Zweck verleiht. Beispielsweise ist des einen Terrorist des anderen Freiheitskämpfer. Beide Weltanschauungen betrachten jedoch dasselbe Geschehen. Durch mehrere zielgerichtete Vorgehen unterschiedlicher Weltanschauungen wird in SSM versucht, die reale Welt zu beschreiben. Diese ist jedoch viel zu komplex, um in irgendeiner Modellsprache erfasst zu werden. Daher wird das Vorgehen bewusst auf ein rein konzeptionelles Modell beschränkt. Diese Einschränkung verringert die Komplexität und vereinfacht dadurch die Problemlösung. Die Abbildung 2.9 zeigt die Schritte des SSM-Modells in drei Phasen. Die Trennung zwischen realer Welt und Systemmodell der realen Welt findet zwischen Phasen eins und zwei statt. In der ersten Phase wird die gesamte Problemsituation der realen Welt aus Sicht aller Beteiligten erörtert und unstrukturiert beschrieben. Anhand dieser Informationen wird in der zweiten Phase ein Bild, in SSM-Terminologie Rich-Picture genannt, erstellt. Dieses ist ein wichtiges Hilfsmittel zur Beschreibung der Problemsituation, welches möglichst viele Informationen in einem Bild erfassen soll. Mit dessen Hilfe sollen Grenzen, Struktur, Informationsflüsse, Kommunikationskanäle und das menschliche Aktivitätssystem eines Systems aufzeigt werden. Das Bild dient als Grundlage für die Ursachendefinitionen, welche einen festen Rahmen für die konzeptionellen Modelle ermöglichen. Die Ursachendefinitionen sorgen dafür, dass wichtige Aspekte nicht weggelassen werden. Die Gedächtnisstütze CATWOE[3] ist eine Empfehlung zur Erstellung der Ursachendefinitionen:

- **Client (Kunde)**, Wer oder was profitiert von dem Umwandlungsprozess?
- **Actor (Akteur)**, Wer ermöglicht den Kunden den Umwandlungsprozess?
- **Transformation process (Umwandlungsprozess)**, von einem Startzustand in eine Endzustand.
- **Weltanschauung**, gibt dem Umwandlungsprozess Bedeutung[4].
- **Owner (Inhaber)**, vor wem muss sich das System verantworten und/oder wer kann veranlassen, dass es nicht existiert.
- **Environmental constraints (Randbedingungen)**, was beeinflusst das System, ohne es zu kontrollieren?

Die Rollen welche Kunde, Akteur und Inhaber belegen, können in bestimmten Fällen überlappen. CATWOE ist keine willkürlich Ansammlung von Eigenschaften, sondern resultiert aus Beobachtungen der realen Welt. Bei der Ausübung von SSM

[3] Übersetzungen wurden aus dem Artikel [59] übernommen.

[4] Weltanschauung wird explizit, auch in der englischen Literatur, als Begriffsteil in CATWOE genannt. [50, s. 255]

ist aufgefallen, dass insbesondere Akteur und Inhaber oft bei der Betrachtung ausgelassen werden, da diese "zu offensichtlich" erscheinen [50, s. 255]. Die Reihenfolge, in welcher die Eigenschaften abgearbeitet werden, ist beliebig. Je nach Problemsituation sind einige Eigenschaften offensichtlicher als andere. Die konzeptionellen Modelle, welche aus den Ursachendefinitionen gebildet wurden, dienen dazu, Debatten über die Thematik zu strukturieren, indem sie mit der realen Welt verglichen werden. In einem iterativen Prozess werden die ersten beiden Phasen wiederholt, bis die Thematik klar genug ist, um Ergebnisse zu treffen. Die Ergebnisse werden abschließend, in Phase drei, in konkrete Schritte formuliert, die ausgeführt werden sollen.

Die Soft Systems Methodology ist zwar keine Methodik, die explizit zur Erstellung eines Sicherheitskonzeptes gedacht ist, ihre Vorgehensweise für die Analyse, durch Trennung von realer Welt und deren Abstraktion, jedoch gut geeignet zum Lösen beliebiger Problemstellungen. SSM nimmt bewusst Einfluss auf das menschliche Denken und Vorgehen, um dieses zu fokussieren und dadurch zu optimieren.

Data Flow Diagramme

Der nachfolgender Paragraph bezieht sich auf [50, s. 263]. Durch die Bedrohungsanalyse (Kapitel 3) mittels SSM wird geklärt, gegen welche Bedrohungen geschützt werden soll und welche Maßnahmen dafür notwendig sind. Darauf aufbauend kann die Bedrohungsmodellierung der Implementierung, unter Verwendung von Data Flow Diagrammen, angewandt werden. Data Flow Diagramme (DFD) gehen zurück auf die 70er Jahre. Ihre Aufgabe ist es, die gefährdeten Informationen der Applikation zu identifiziert, die Bedrohungen zu finden und Maßnahmen dagegen zu treffen. Es gibt mehrere Level von DFDs, welche den Detailgrad des Diagramms bestimmen. Für die Bedrohungsmodellierung reicht Level 0 aus. Es zeigt den Informationsfluss zwischen internen und externen Anwendungsgrenzen. Für die Bedrohungsmodellierung wird der Aufbau der Diagramme auf die fünf Objekte (Abbildung 2.10) beschränkt. Die Vertrauensgrenze ist ein Objekt, dass das klassische DFD erweitert, um den Aspekt der Bedrohungen eines System darstellen zu können. Generell gilt, überschreitet ein Datenfluss eine Vertrauensgrenze, ist er durch Bedrohungen verwundbar.

Anhand der Data Flow Diagramme werden Gefährdungen für Informationsflüsse gesucht. Diese werden einfachheitshalber in zunächst fünf Kategorien gegliedert:

Denial of Service (DoS) ist eine sehr allgemeine Gefährdung, weshalb diese nur bei Netzwerkzugriffen berücksichtigt wird. Auf Grundlage dieser fünf Kategorien können detaillierte Analysen durchgeführt werden.

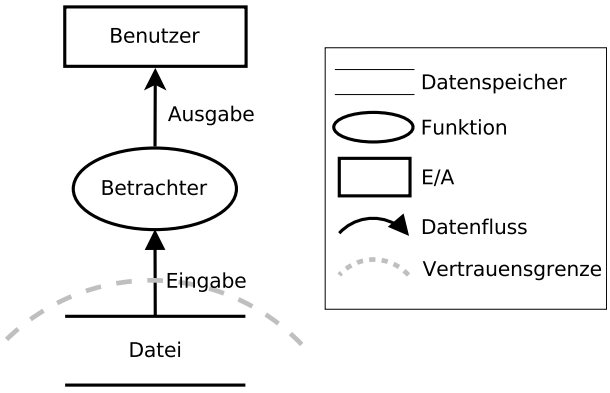

Abbildung 2.10: Data Flow Diagramm Beispiel

Sabotage	unentdeckt Daten modifizieren
Personifikation	vorgeben, jemand oder etwas Anderes zu sein
Informationspreisgabe	unberechtigter Zugriff auf Informationen
Disput	meiden der Verantwortung für ein Tun oder Nichttun
Denial of Service	einen Service an seiner Ausführung hindern

2.3 Authentifizierungsverfahren

Für die Authentifizierung gibt es verschiedene Möglichkeiten, welche sich sowohl in ihrem Aufwand als auch ihrem Nutzen unterscheiden. Zuvor wird noch der Begriff "Vertrauen" definiert.

2.3.1 Vertrauen

Vertrauen ist der Zustand, der durch Authentifizierung erreicht werden soll. Vertrauen sagt aus, dass ein Partner einem anderen Partner in Funktion, Ehrlichkeit und Zuverlässigkeit, aufgrund von eigenen Erfahrungen, glaubt [9]. Dabei unterscheidet man einseitiges und beidseitiges Vertrauen. Von einseitigem Vertrauen wird gesprochen, wenn nur ein Partner einen Nachweis seiner Identität erbracht hat. Bei beidseitigem Vertrauen haben beide Kommunikationspartner gegenseitig überprüft, dass der Andere derjenige ist, welcher er vorgibt zu sein.

2.3.2 Passwörter

Bei passwortbasierter Authentifizierung weist sich ein Kommunikationspartner über einen eindeutigen Namen und ein Passwort gegenüber einem anderen Kommunikationspartner aus. Passwortbasierende-Authentifizierung wird meistens verwendet, um einseitiges Vertrauen herzustellen. Der typische Einsatz ist die Anmeldung

an einem Server, um Zugriff auf dessen Services zu erhalten. Der Benutzer weist sich mit Name und Passwort gegenüber dem Server aus, umgekehrt gibt es oft keinen Nachweis über die Identität. Eine Möglichkeit des Identitätsnachweises von Serverseite sind Zertifikate (vgl. 2.3.4). Die Sicherheit von Passwörtern basiert auf der Annahme, dass der Benutzer ein sicheres Passwort gewählt hat und dieses stets vor fremden Zugriff schützt. Die Realität zeigt jedoch, dass diese Annahme selten zutrifft [50, s. 2].

2.3.3 Symmetrisch

Symmetrische Verfahren arbeiten mit einem Passwort oder Schlüssel, der beiden Kommunikationspartnern bekannt ist. Dieser muss vor der Kommunikation, über einen zweiten Kanal, etwa persönlich, ausgetauscht werden. Das Verfahren wird deshalb auch als Pre-Shared-Key (PSK) bezeichnet. Die verbreitetste Anwendung von PSKs sind WLAN-Netzwerk im privaten Bereich. Zugang zu einem solchen WLAN-Netzwerk kann jeder erhalten, der den Schlüssel kennt. Unter der Annahme, dass nur Berechtigte den Schlüssel kennen, wird ein Vertrauensverhältnis zwischen den Kommunikationspartnern in dem Netzwerk aufgebaut. Bei steigender Anzahl der Kommunikationspartner wird dieses System unbrauchbar, denn jeder neue Partner erhält den gleichen Schlüssel. Soll nun einem Berechtigten der Zugriff verboten werden, muss der Schlüssel gewechselt werden. Dies führt dazu, dass alle, außer demjenigen, dem die Berechtigung entzogen werden soll, einen neuen Schlüssel benötigen.

2.3.4 Asymmetrisch

Asymmetrische Verfahren arbeiten mit zwei Schlüsseln, einem öffentlichen und einem privaten (Abbildung 2.11). Der öffentliche Schlüssel wird dem Kommunikationspartner übergebenen, der private Schlüssel bleibt im eigenen Besitz und wird vor fremden Zugriff geschützt.

Der große Vorteil dieses Verfahrens gegenüber den Symmetrischen ist, das der öffentliche Schlüssel über einen nicht vertrauenswürdigen Kanal geteilt werden kann. Bei der Authentifizierung wird der private Schlüssel genutzt, um eine Nachricht zu signieren. Mit dem öffentlichen Schlüssel kann der Kommunikationspartner verifizieren, dass die Nachricht von dem Kommunikationspartner kommt, der den passenden privaten Schlüssel hat (Abbildung 2.12). Dadurch kann festgestellt werden, ob die Nachricht auf dem Transportweg manipuliert worden ist, allerdings bleibt das Problem des Vertrauens, denn ob der Schlüssel von demjenigen stammt, der der Kommunikationspartner vorgibt zu sein, ist dadurch nicht garantiert. Hier-

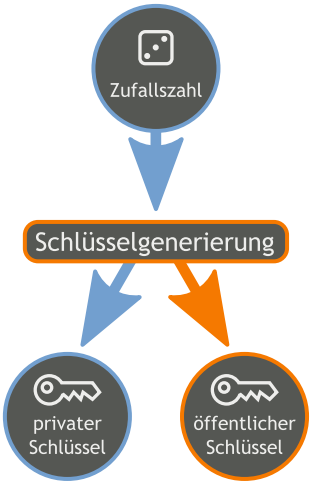

Abbildung 2.11: Public/Private Schlüsselgenerierung aus [2]

bei wurde die Notwendigkeit nach einem expliziten Austauschkanal eliminiert, da der Schlüsselaustausch, über einen unsicheren Kanal erfolgen kann. Allerdings hat man dadurch das Bedürfnis nach einen Authentifizierungskanal geschaffen, um eine Identitätsprüfung durchführen zu können.

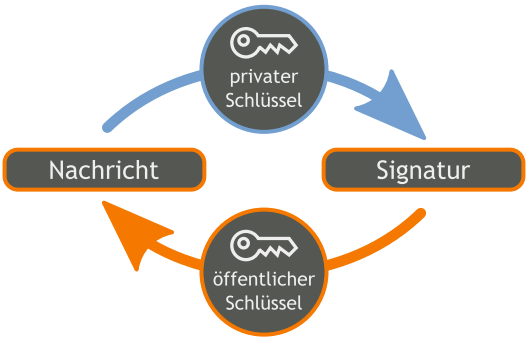

Abbildung 2.12: Public/Private Verifizierung aus [2]

Aus diesem Hintergrund wurden Zertifikate erschaffen. Der heutige verbreitetste Standard sind Zertifikate im X.509-Format. Ein Zertifikat beinhaltet Informationen über den Inhaber, die Zertifizierungsstelle, die Gültigkeit und den öffentlichen Schlüssel. Anstatt den öffentlichen Schlüssel auszutauschen, wird nun das Zertifikat gesendet. Bei der Zertifizierungsstelle kann die Echtheit verifiziert werden.

> The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.
>
> *Gene Spafford*

Kapitel 3

Bedrohunganalyse

Als erstes wird in diesem Kapitel die Zielsetzung dieser Thesis beschrieben. Die eigentliche Bedrohungsanalyse gliedert sich in die drei SSM-Phasen, die in Abschnitt 2.2.3 beschrieben sind. Zunächst wird die Problemsituation beschrieben, danach werden zwei konzeptionelle Modelle aus unterschiedlichen Weltanschauungen erstellt. Die unterschiedlichen Weltanschauungen entstammen der Betrachtung eines Beschützers und eines Angreifers des Systems. Durch den Vergleich der konzeptionellen Modelle mit der realen Welt werden konkrete Maßnahmen formuliert. Das Ergebnis der Bedrohungsanalyse soll mögliche Bedrohungen aufdecken und erste Maßnahmen hervorbringen.

3.1 Zielsetzung

Ziel dieser Thesis ist es, einen Lösungsvorschlag für die Authentifizierung und Autorisierung eines Fernzugriffes auf den Marktrechner zu unterbreiten. Abbildung 3.1 zeigt die dafür relevanten Use-Cases. Auf der linken Seite sind die Benutzer zu sehen. Diese wollen lokal oder remote bestimmte Funktionen auf dem Marktrechner aufrufen. Dazu müssen Sie vorher authentifiziert und autorisiert werden. Die Autorisierung soll auf einem Rollenmodell basieren, wobei ein Benutzer mehrere Rollen innehaben kann. Die Benutzung über den Remotezugriff soll über HTTPS und das RestGateway des Marktrechners erfolgen. Zur Überprüfung der Authentifizierungs- und Autorisierungsdaten des Nutzers soll ein Authentifizierungs- und Autorisierungs-Server (AAS) kontaktiert werden. Dieser AAS kann räumlich getrennt von den Benutzern, etwa über das Internet, erreichbar sein. Der Marktrechner soll die Möglichkeit bieten, mehrere AAS abfragen zu können.

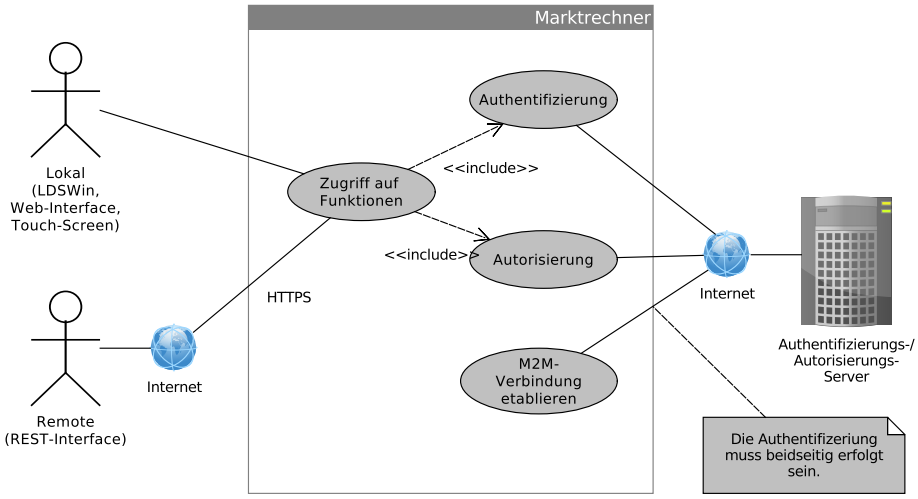

Abbildung 3.1: Zielsetzung Use-Case-Diagramm

3.1.1 Vorgehen

Im Grundlagenteil 2.2.1 wurde die Common Criteria als internationaler Sicherheitsstandard vorgestellt, welcher für die Entwicklung sicherer Systeme verwendet wird. Das für diese Thesis relevante Protection Profile analysiert die aus Kundensicht relevanten Anforderungen des zu sichernden Systems. Ein komplettes PP zu erstellen, würde den Rahmen der Thesis sprengen, deswegen werden die wichtigsten Aspekte herausgenommen und behandelt. Dazu werden zunächst die zu schützenden Güter und deren Bedrohungen analysiert. Anschließend werden Maßnahmen zu den Bedrohungen gesucht. Dabei soll zunächst vermieden werden, Bezug auf eine bestimmte Technologie oder ein bestimmtes Konzepte, zu nehmen, außer die Randbedingungen beziehungsweise Maßnahmen lassen keine alternativen Lösungen zu. Zum Schluss werden die Kriterien aufgestellt, anhand welcher die Evaluierung durchgeführt werden soll.

3.1.2 Methoden

Als Methoden für die Erkennung der Bedrohungen werden die Soft Systems Methodology und Data Flow Diagramme eingesetzt. Unterstützend werden Gefährdungenkataloge und Maßnahmenkataloge aus dem IT-Grundschutz des BSI herangezogen.

Der BSI hat Gefährdungen und Maßnahmen zu Bausteinen zusammengefasst, die sich in fünf Kategorien gliedern:

- Übergreifende Aspekte
- Infrastruktur

- IT-Systeme
- Netze
- Anwendungen

Die übergreifenden Aspekte beinhalten wichtige Bausteine, etwa Datensicherungskonzept, Sensibilisierung und Schulung zur Informationssicherheit oder Behandlung von Sicherheitsvorfällen. Mit dem Blick auf den Schwerpunkt dieser Thesis wird aus dieser Kategorie lediglich auf das Kryptokonzept eingegangen. Aus dem selben Grund werden die Bausteine aus der Kategorie Infrastruktur nicht weiter betrachtet. Ebenso werden die Gefährdungen der höheren Gewalt und die Maßnahmen der Notfallvorsorge nicht betrachtet.

Die Bedrohungsanalyse bewegt sich auf einem abstrakten generischen Level, weshalb die Kategorien IT-Systeme und Netze hier nicht betrachtet werden. In der anschließenden Bedrohungsmodellierung wird das System konkretisiert, womit diese Bausteine dann zur Geltung kommen. Jeder Abschnitt in diesen beiden Kapiteln erklärt seine relevanten Bausteine, Gefährdungen und Maßnahmen.

3.2 Beschreibung der Problemsituation

Die in Abschnitt 2.1.2 geschilderte Architektur des Marktrechnerumfeldes wird mit dem Rich-Picture in Abbildung 3.2 auf Sicherheitsmängel untersucht. Der Fokus dieser Arbeit liegt auf dem Fernzugriff, dennoch werden auch die Probleme des lokalen Zugriffes erfasst. Dadurch soll verhindert werden, dass der Fernzugriff unnötige Hindernisse für die lokale Zugriffskontrolle schafft.

3.2.1 Identifizieren der Rollen

Zunächst wird ein Überblick über alle Zugriffsberechtigten geschaffen. Diese werden anhand von Rollen zusammengefasst, welche Funktion und Zugriffsart beschreiben. Alle Rollen sind in der Abbildung 3.2 illustriert. Die Beschreibungen der Rollen sind allgemein gehalten und nehmen keinen Bezug auf aktuelle oder zukünftige technologische Begebenheiten.

Der Projektierer konzipiert und entwirft komplette Kälteanlagen. Ein Teil seiner Aufgabe kann das Erstellen der Offline-Konfiguration sein. Diese kann direkt von Werk aus aufgespielt werden. Der Inbetriebnehmer muss den vorkonfigurierten Marktrechner dann lediglich noch installieren und testen.

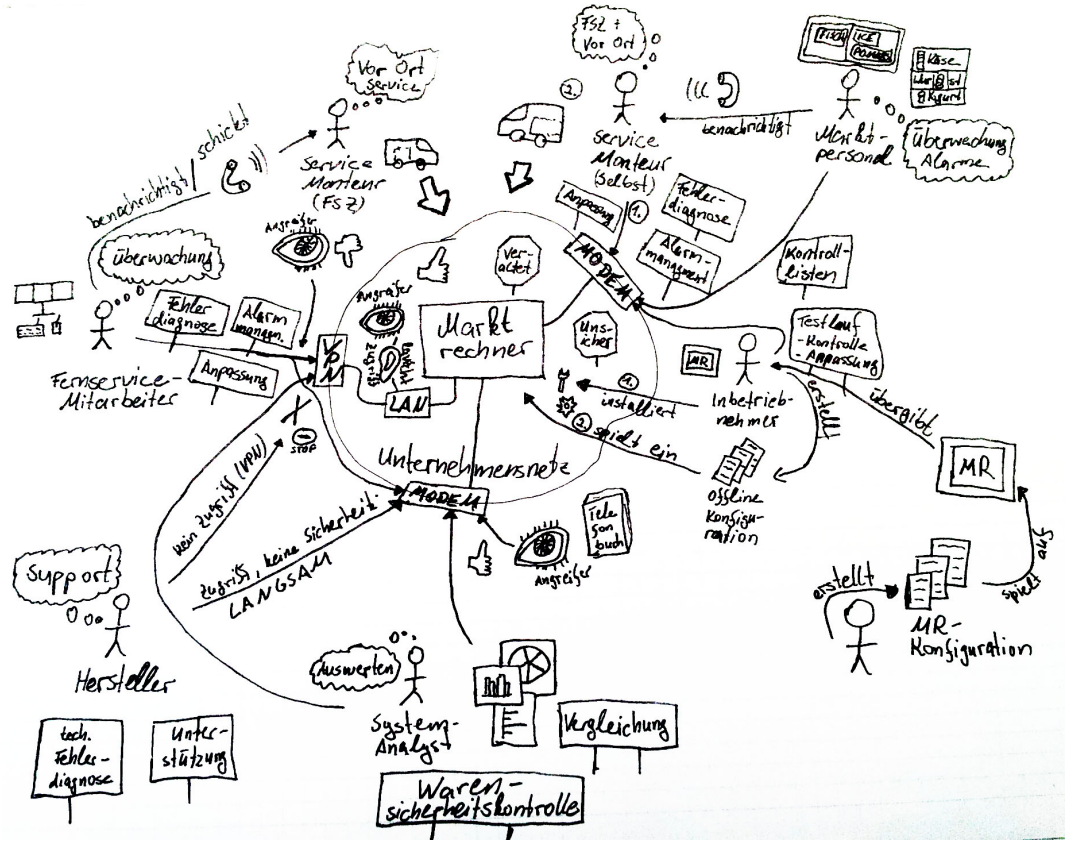

Abbildung 3.2: Problemsituation

Der Inbetriebnehmer ist die Rolle, welche das System initial zum Laufen bringt. Der Inbetriebnehmer muss vor Ort die Anlage in Betrieb nehmen. Dazu kann er bereits im Voraus eine Offline-Konfiguration anlegen, welche an die Anlage des Kunden angepasst ist. Die Konfiguration wird auf die Anlage eingespielt, sobald die Hardware installiert ist. Bevor die Anlage produktiv eingesetzt werden kann, wird ein Testlauf durchgeführt. Während des Testlaufs muss der Inbetriebnehmer die Anlage überwachen, um bei Problemen die Konfiguration, die Parameter und die Einstellungen anzupassen. Zur Überwachung des Testlaufes muss der Inbetriebnehmer nicht zwingend permanent vor Ort sein, sondern kann den Status auch aus der Ferne abrufen, damit der Inbetriebnehmer nicht etliche Stunden neben dem Marktrechner auf das Auftreten von Fehlern warten muss.

Der Service-Monteur führt Wartungen und Störungsbehebungen durch. Für den Service-Monteur gibt es zwei denkbare Ausprägungen. Als Selbständiger wird er im Fall einer Störung durch den Eigentümer der Anlage oder dessen Personal benachrichtigt. Nun hat er die Möglichkeit, aus der Ferne eine Fehlerdiagnose durchzuführen und Veränderungen an der Konfiguration und dem Alarmmana-

gement durchzuführen. Sollte er nicht in der Lage sein, die Störung aus der Ferne zu beheben, muss er dieselbe Tätigkeiten vor Ort durchführen können. Als Mitarbeiter im Außendienst einer Fernservice-Zentrale entfällt die Diagnose und die Fehlerbehebung aus der Ferne, da dies bereits durch den Fernservice-Mitarbeiter durchgeführt wurde. Wenn die Störung von dort nicht gelöst werden kann, wird der Service-Monteur zur Anlage geschickt.

Der Fernservice-Mitarbeiter überwacht mehrere Anlagen aus der Ferne. Diese Rolle führt die selben Tätigkeiten wie ein Service-Monteur durch. Allerdings erfolgt die bereits erwähnte Fehlerdiagnose, Kontrolle und Anpassung von Parametern und Einstellungen sowie das Alarm-Management ausschließlich aus der Ferne. Einige Störungen können durch Anpassen der Konfiguration hinausgezögert werden, bis ein Service-Monteur vor Ort ist. Dadurch kann zum Beispiel Warenschaden auf Kosten von Energieeffizienz verhindern werden.

Der System-Analyst wertet relevante und vergleichbare Daten zur Energieeffizienz und Warensicherheit aus. Auch er arbeitet ausschließlich aus der Ferne. Auswertbare Daten sind etwa Temperaturwerte oder Energieverbrauch. Sollten diese Werte im Vergleich mit anderen Anlagen negativ auffallen, kann er veranlassen, dass eine Anlage überprüft wird.

Der Eigentümer/Das Marktpersonal ist daran interessiert, eine Kontrolle der Parameter zur Warensicherheit durchzuführen und eine Dokumentation der Waren-Temperaturen zu erhalten. Auch soll das Marktpersonal über Alarme informiert werden, um einen Service-Monteur zu benachrichtigen und Warenschaden zu verhindern. Die Rolle des Marktpersonals kann Zugriff vor Ort benötigen, aber auch der Zugriff aus der Firmenzentrale wäre denkbar.

Der Hersteller produziert die Hardware und entwickelt die Software des Marktrechners. Nach der Installation eines Marktrechner kann er anderen Rollen Unterstützung bei der Durchführung ihrer Arbeiten geben. Damit bei Softwareproblemen schnell Hilfe geleistet werden kann, will er sich aus der Ferne verbinden können .

3.2.2 Systemumgebung

Der Marktrechner wird als Teil einer Kälteanlage beim Kunden installiert und wird dort an dessen Netzwerk angeschlossen. Der Fernzugriff auf einen Marktrechner ist prinzipiell immer möglich. Zwei Arten des Fernzugriffs sind etabliert, über VPN

oder Modem. Verbindungen über VPN kommen ausschließlich in Fernwarten zum Einsatz. Zum aktuellen Zeitpunkt sind etwa ein Viertel der Marktrechner über VPN erreichbar. Der Einsatz von VPN hat den Nachteil, dass er extrem aufwendig zu etablieren, denn hier treffen unterschiedliche IT-Infrastrukturen zusammen, was ein Garant für Probleme ist. Beispielsweise sind Überschneidungen bei IPv4-Adressen eines der Hauptprobleme, da viele Administratoren Subnetze aus der Literatur übernehmen und diese diesbezüglich größtenteils gleich ist. Außerdem beschränkt sich der Zugriff ausschließlich auf die gekoppelten Netze. Dadurch ist es dem Hersteller nicht möglich, Unterstützung aus der Ferne zu leisten. Zwar ist es durchaus möglich, einen temporären VPN-Zugriff für den Hersteller einzurichten, in der Praxis hat sich jedoch gezeigt, dass dies ein sehr langwieriger Prozess ist. Über VPN ist die Verbindung bis zum Unternehmensnetz abgesichert, sodass ein Angreifer hier wenig Möglichkeit hat einzudringen. Alle anderen Verbindungen werden über Modems ermöglicht. Deren Einsatz ist veraltet und bietet nur sehr geringe Übertragungsgeschwindigkeiten. Zudem stellen immer mehr Internet-Provider analoge ISDN-Anschlüsse auf Voice-over-IP (VoIP) Lösungen um. VoIP sorgt dafür, dass eine zuverlässige Modem-Kommunikation unmöglich wird. Durch diese VoIP-Problematik wird das Modem im Rahmen der Thesis nicht weiter berücksichtigt, da es in absehbarer Zeit abgelöst werden muss. Für das LAN, indem sich der Marktrechner befindet, gilt, dass ein Angreifer durch keine geeigneten Sicherheitsmaßnahmen aufgehalten wird.

3.3 Sichtweise der Beschützer

Anhand der in Abschnitt 3.2 beschriebenen Problemsituation wird hier die Sichtweise der Beschützer des Systems betrachtet. Zunächst legen die Ursachendefinitionen das Grundgerüst fest, in welchem sich die Beschützer bewegen. Anhand derer wird dann das konzeptionelle Modell aufgebaut, das klare Anforderungen stellt, die die Beschützer für sinnvoll halten. Dieses Systemmodell wird abschließend mit der realen Welt verglichen.

3.3.1 Ursachendefinitionen

Bei den Ursachendefinitionen der Beschützer sind die Eigenschaften für Kunden, Inhaber und Umwandlungsprozess offensichtlich. Für den Akteur, die Weltanschauung und die Randbedingungen bedarf es hingegen einer genaueren Analyse:

Kunden	Alle Rollen aus Abschnitt 3.2.1 und der Marktrechner
Inhaber	Angreifer
Umwandlungsprozess	Von einem nicht vertrauenswürdigen Zustand in einen vertrauenswürdigen Zustand wechseln.

Akteur Diese Rolle kann je nach Dienstleister und Kundenwünschen unterschiedlich besetzt sein. Die offensichtlichsten Akteure sind Hersteller und Fernservice-Zentralen. Darüber hinaus wäre es denkbar, dass ein Marktbetreiber selbst diese Rolle einnehmen möchte.

Weltanschauung Hersteller und Fernservice-Zentralen sind daran interessiert, unerwünschte Zugriffe zu verhindern und ihre jeweiligen vertraulichen Daten zu schützen.

Das zu schützende Gut des Hersteller ist sein proprietäres Protokoll, da mit dessen Kenntnis unbemerkt Schaden angerichtet werden kann. Deshalb sollen die Kommunikationsinhalte geschützt werden, um zu verhindern, dass Angreifer Kenntnisse über Programmroutinen und Protokolle erlangen. Ein kompromittiertes Protokoll könnte ein Angreifer nutzen, um Warenschaden anrichten, wofür der Hersteller und/oder die Fernservice-Zentrale haftbar sein können. Darüber hinaus kann ein Imageschaden verursacht werden, um zum Beispiel Endkunden abzuwerben.

Die Benutzer hingegen wollen ein funktionierendes System, sie haben einen Kältehintergrund und keine Ahnung von IT, Vertraulichkeit ist für sie von sekundärer Natur. Wenn der Prozess, Vertrauen zu schaffen, Dinge kompliziert, wird der Benutzer versuchen, ihn zu umgehen. Sollte das System nicht funktionieren, weil der Benutzer die Authentifizierung falsch bedient, ist trotzdem das System schuld, denn es ist seine Aufgabe, den Benutzer darauf hinzuweisen [50, s. 5].

Zusätzlich spielt die Nachvollziehbarkeit eine große Rolle, denn durch das Wissen—"Wer hat wann mit welchen Mitteln was veranlasst beziehungsweise worauf zugegriffen?" [39]—können unerlaubte Handlungen seitens der eigenen Mitarbeiter kontrolliert werden.

Randbedingungen Die Marktrechner sind im Unternehmensnetz des Endkunden installiert und haben einen Internetzugang. Die Kommunikation mit dem Benutzer findet über den unsicheren Kommunikationskanal Internet statt. Der Benutzer nutzt das RestGateway für den Fernzugriff. Die Kommunikation dabei soll über das HTTPS-Protokoll stattfinden, weil dieses meist bei restriktiven Firewallregeln Einstellungen funktioniert. Die Authentifizierung der Benutzer wird durch den

Marktrechner an einen oder mehrere AAS delegiert. Die Authentifizierung der Fernservice-Mitarbeiter obliegt der Fernservice-Zentrale, nicht dem Endkunden. Der Hersteller kann zur Unterstützung temporären Zugriff durch die FSZ oder den Endkunde bekommen. Die Zutrittskontrolle zum Marktrechner obliegt dem Endkunden.

3.3.2 Konzeptionelles Modell

Die folgende Beschreibung des konzeptionellen Modells nimmt direkten Bezug auf die Ursachendefinitionen. Das Modell darf nichts hinzufügen, das nicht in den Ursachendefinitionen aufgeführt wurde. Durch diese Einschränkung soll verhindert werden, dass Instanzen aus der realen Welt hinzugefügt werden, und damit das Modell unbrauchbar komplex wird [50, s. 256]. Aus den Ursachendefinitionen ergibt sich das folgende konzeptionelle Modell:

B1 Der Marktrechner darf Verbindungen von Kunden nur akzeptieren, wenn deren Berechtigungsnachweis von einem AAS verifiziert wurde.

B2 Der Marktrechner soll lokale Kunden ebenfalls durch einen AAS authentifizierten lassen.

B3 Der Marktrechner soll die Rollen des authentifizierten Kunden beim AAS erfragen.

B4 Der Marktrechner soll den Zugriff anhand von Rollen autorisieren.

B5 Die Kommunikation zwischen Marktrechner und Kunde muss über HTTPS verschlüsselt werden.

B6 Angreifer (Inhaber) können sich Zugang zum Unternehmensnetzwerk verschaffen.

B7 Angreifer (Inhaber) dürfen kein Wissen über Kommunikationsinhalte haben.

B8 Angreifer (Inhaber) dürfen nicht unbemerkt vorgeben, Benutzer (Kunden) zu sein.

3.3.3 Vergleich mit der realen Welt

Der Vergleich des konzeptionellen Modells mit der realen Welt soll Schwächen aufdecken, die zunächst ignoriert werden konnten. Für den Vergleich werden Gefährdungen und Maßnahmen aus den Anwendungsbausteinen 5.4 "Webserver" und

5.21 "Webanwendungen" der IT-Grundschutz-Kataloge des BSI verwendet [13, 11]. Unter Berücksichtigung auf den Umfang der Thesis werden menschliche Fehlhandlungen von Benutzern und Administratoren, sowie technisches Versagen durch Softwarefehler-Fehler als Gefährdungen ignoriert.

Zu B1-B2 Durch die Gefährdung 4.33 "Schlechte oder fehlende Authentikation[1]" [24] des BSI wird darauf hingewiesen, dass Unbefugte ohne Maßnahmen der Zugriffskontrolle jederzeit ein System kompromittieren können. Als Maßnahme empfiehlt der BSI unter 2.7 "Vergabe von Zugangsberechtigungen" [43]. Diese besagt, dass Benutzer sich mit einer Identifikation und einem Passwort oder Token gegenüber einem System ausweisen müssen, um Zugang zu erlangen. Die weiterführende Maßnahme 2.11 "Regelung des Passwortgebrauchs" trifft Regelungen, unter welchen Benutzer sichere Passwörter wählen müssen [38]. Die Maßnahme 2.7 wird vom Marktrechner erfüllt, indem der AAS zur Überprüfung des Berechtigungsnachweises kontaktiert wird. Maßnahme 2.11 obliegt allerdings dem Authentifizierungsserver, welcher in dieser Thesis lediglich als Black-Box betrachtet wird.

Zu B3-B4 Bei der Autorisierung warnt der BSI vor 2.67 "Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten" [23]. In vielen Organisationen ist die Vergabe und Verwaltung von Rechten sehr arbeitsintensiv, da diese schlecht geregelt ist und teilweise die falschen Tools eingesetzt werden. Sind die Tools nicht flexible genug, dann ist mit der Gefährdung, 5.19 "Missbrauch von Benutzerrechten" zu rechnen [30], denn Benutzer, die mehr Rechte besitzen als zur Ausübung ihrer Tätigkeiten benötigt werden, sind oft nicht verlegen auch zu nutzen. Da der Autorisierungsserver, ebenfalls als Black-Box betrachtet wird, sind diese Gefährdungen für die Thesis zu vernachlässigen.

Zu B5 In Punkt B5 soll eine Verbindung über HTTPS hergestellt werden, damit die Übertragung der Benutzer-Berechtigungsnachweise verschlüsselt stattfindet. Der BSI hat diesen Punkt in der Maßnahme 5.66 "Verwendung von TLS/SSL" [48] erfasst. TLS verwendet Zertifikate im X.509-Format, zur Verschlüsselung der Daten. Es gibt zwei Möglichkeiten TLS einzusetzen. Die erste Möglichkeit sind Zertifikate von Zertifizierungsstellen. Die Zertifikat-Branche heutzutage ist allerdings rein kommerziell getrieben [50, s. 50]. Die zwei Parteien, die hier primär agieren sind der Zertifikatbeantrager und die Zertifizierungsstelle. Zur Verifizierung, der Identität und des Wahrheitsgehaltes der Zertifikatsinhalte des Zertifikatbeantragers, gibt es keinerlei Vorgaben. Ein Benutzer, der ein erhaltenes Zertifikat bei einer Zertifizierungsstelle verifizieren möchte, hat zu dieser meist keinerlei Beziehung und muss

[1] Rechtschreibfehler des BSI, korrekt ist Authentifizierung

sich darauf verlassen, dass die Zertifizierungsstelle genügend Vorkehrungen gegen Betrugsversuche unternommen hat. Ein Zertifikat ermöglicht zwar eine Validierung des Zertifikatsinhaber, in wie weit dieser Information vertraut werden kann muss der Benutzer entscheiden. Im Zweifelsfall bescheinigt ein Zertifikat, dass der Inhaber des Zertifikates der Zertifizierungsstelle Geld transferiert hat. Von einer Entität, die Echtheit von etwas verifizieren zu lassen, zu welcher kein Vertrauen besteht, ist sinnlos. Daher sollte beim Einsatz von Zertifikaten, welche von einer öffentlichen Zertifizierungsstelle erstellt wurden, die Vertrauenswürdigkeit im Voraus geprüft werden. Die zweite Möglichkeit sind selbst-signierte Zertifikate. Hierbei entfällt die Möglichkeit einer wirkungsvolle Verifikation, durch einen Dritten, da die Zertifikate vom Zertifikatsinhaber selbst erstellt wurden. Zusätzlich können beiden Möglichkeiten durch Client-Zertifikate ergänzt werden, um neben der Serveridentität auch die des Client zu authentifizieren.

Unter Beachtung des Aufwandes und der Kosten ist TLS mit selbst-signierten Zertifikaten ausreichend sicher. In Abschnitt 3.4 wird darauf eingegangen, wie das Risiko ein gefälschtes Zertifikat zu erhalten, minimiert werden kann. Zusätzlich zur generellen Empfehlung des BSI, sollte ausschließlich die aktuelle TLS Version 1.2 mit Chiffrensammlung, die Perfekt Forward Security (PFS) nutzen, verwendet werden. Älteren Versionen haben allesamt Schwachstellen, die durch diverse Attacken verwundbar sind [58]. Deshalb wird B5 des konzeptionellen Modell durch folgenden Punkt ersetzt:

- Die Kommunikation zwischen Marktrechner und Kunde muss über HTTPS verschlüsselt werden unter Verwendung von TLS 1.2 und Verwendung einer Chiffrensammlungen, die der PFS genügt.

Für die Authentifizierung von Maschine-zu-Maschine (M2M) Kommunikation hat das BSI keine vordefinierte Maßnahme. Die M2M-Kommunikation zwischen Marktrechner und AAS ist essentiell für den Zugriffsschutz, deshalb muss hier eine beidseitige asynchrone Authentifizierung eingesetzt werden, die es ermöglicht, Vertrauen zwischen beiden Partnern aufzubauen. Folgende Punkte werden daher Teil des konzeptionellen Modell.

- Die Authentifizierung zwischen Marktrechner und AAS soll ausschließlich über ein Public/Private-Key Verfahren erfolgen.
- Die Identität des Gegenüber muss durch einen zweiten Kommunikationskanal bestätigt werden.

Für den lokalen Zugriff ergibt sich durch den Einsatz von Authentifizierungs- und Autorisierungsservern eine Besonderheit. Für den Fall, dass kein AAS erreichbar ist,

zum Beispiel durch eine Netzwerkstörung, muss es einen einmaligen Mechanismus geben, um einem lokalen Kunden den Zugriff zu erlauben. Ein Beispiel für einen solchen Mechanismus sind Einmal-Passwörter, die die Fernservice-Zentrale auf Anfrage ausstellt. Daher wird das Konzept noch ergänzt durch:

- Der Marktrechner muss lokal durch einen Einmal-Mechanismus entsperrbar sein, wenn kein AAS verfügbar ist.

Zu B6-B8 Punkt sechs ist aufgrund der Randbedingungen aus der Herstellersicht nicht regulierbar. Punkt sechs verlangt, dass die Kommunikation verschlüsselt zwischen den Kommunikationspartnern erfolgt und wird durch die bereits erläuterte BSI Maßnahme 5.66 umgesetzt. In Punkt sieben wird auf die sichere Verwaltung der Berechtigungsnachweise hingewiesen. Diese werden vom AAS verwaltet und sind daher nicht relevant für diese Thesis.

3.4 Sichtweise der Angreifer

Nach der Analyse der Gefährdungen aus Sicht der Beschützer wird nun die Sichtweise der Angreifer beleuchtet. Im wesentlichen werden fünf Angriffsarten unterschieden [50, s. 256][57][60].

- Spionage
- Cyberkrieg
- Finanziell motiviert
- Selbstbestätigung des Egos
- Frustrierte oder verärgerte Mitarbeiter

Für Spionage kommen hauptsächlich Konkurrenten des Systemherstellers in Frage. Spionage von Endkunden-Konkurrenz, um Informationen auf diesem Weg erlangen, ist eventuell denkbar, allerdings bieten sich hierzu andere Möglichkeiten an, beispielsweise das Abwerben von Mitarbeitern.

Der Cyberkrieg ist die kriegerische Auseinandersetzung im Bereich der Informationstechnik. Ein militärisch motivierter Angreifer könnte durch die massenhafte Zerstörung von Kühlgütern, die Lebensmittelversorgung eines Landes/Kontinentes stark beschädigen. Das solche Angriffe möglich sind, ist seit Bekanntwerden des

Stuxnet-Wurms gewiss, welcher die Leittechnik einer Urananreicherungsanlage eines iranischen Atomkraftwerkes stören sollte [61].

Finanziell motivierte Angreifer können bei einem Angriff auf eine Kälteanlage keinen direkten, unbemerkten finanziellen Diebstahl begehen, da dort keinerlei Zahlungsströme abgewickelt werden. Durchaus denkbar wäre, die Erpressung gegen einen Eigentümer vieler Anlagen, mit der Drohung, Warenschaden zu verursachen. Die dafür benötigte technische Expertise verlangt allerdings detailliertes Informatik- und Kältetechnikwissen. Ein Angreifer, welcher auf einen direkten Konkurrenten zurückzuführen ist, hätte dieses Wissen. Ein solcher Angreifer könnte durch seine(n) Angriff(e) Imageschaden verursachen, beispielsweise durch Verursachen von Fehlfunktionen. Dadurch ist es der Konkurrenz möglich, die eigenen Produkte unter Kunden besser zu bewerben und die eigene Marktmacht auszubauen.

Der vierte Angreifertyp ist aufgrund erforderlicher Expertise fast vollständig auszuschließen, zudem wird das Hacken einer Kälteanlage kein großes öffentliches Interesse wecken, wodurch der erfolgreiche Hack ohne Prestige beziehungsweise Ruhm bleibt, welches das Ego aufbauen würde.

Angreifer aus Mitarbeiterkreisen sind ebenso zu berücksichtigen. Das Hauptmotiv dabei ist eine aus Mitarbeitersicht ungerechtfertigte Kündigung. Durch sein Fachwissen und seine Zugriffsrechte kann der Mitarbeiter erheblichen Schaden anrichten, der im schlimmsten Fall zur Insolvenz führen kann.

3.4.1 Ursachendefinitionen

Kunden	Angreifer, beziehungsweise deren Auftraggeber
Inhaber	Beschützer
Akteur	Alle Rollen aus Abschnitt 3.2.1 und die Angreifer

Umwandlungsprozess Authentifizierung und Autorisierung ohne Wissen der Beschützer aushebeln, um geschützte Inhalte zu kompromittieren und Daten zu extrahieren oder Fehlfunktionen zu verursachen.

Weltanschauung

- Die Angreifer, respektive deren Auftraggeber, wollen durch Spionage und/oder Manipulation dem Hersteller, der Fernservice-Zentrale und dem Eigentümer Schaden zufügen.

- Ein militärisch motivierter Angreifer möchte die Infrastruktur, etwa eines Landes, zerstören oder beschädigen.
- Ein finanziell motivierter Konkurrent möchte dem Hersteller Marktanteile abnehmen und verhindern, dass dieser neue Anteile erhält. Der größte Erfolg für ihn ist es, einen Konkurrenten komplett vom Markt zu verdrängen.
- Ein verärgerter Mitarbeiter sucht Genugtuung gegenüber seinem Arbeitgeber. Sein Handeln erfolgt aus dem Affekt und verfolgt keine weiteren Ziele.

Randbedingungen Die Kommunikation erfolgt verschlüsselt durch ein geeignetes Kryptoverfahren, der Zugriff auf alle Systeme ist durch entsprechende Berechtigungsnachweise geschützt, die Zutrittskontrolle zum Marktrechner obliegt dem Endkunden.

3.4.2 Konzeptionelles Modell

A1 Angreifer (Kunden) können sich Zugriff zum LAN der Endkunden verschaffen.

A2 Alle Aktionen der Angreifer (Kunden) sollen geschehen, ohne Kenntnisnahme der Beschützer (Inhaber).

A3 Angreifer (Kunden) wollen in den Besitz von Berechtigungsnachweisen der Akteure kommen (Phishing, Social Engineering).

A4 Angreifer (Kunden) können verschlüsselte Kommunikation aufnehmen und später erneut einspielen (Replay-Attacke).

A5 Angreifer (Kunden) können eine Kommunikation kompromittieren, indem Sie zwischen den Kommunikationspartnern auftreten (MITM-Attacke).

A6 Angreifer (Kunden) können den Verbindungspool des Marktrechners erschöpfen und diesen überlasten (DOS-Attacke).

3.4.3 Vergleich mit der realen Welt

Für den Vergleich mit der realen Welt wird neben den bereits für die Beschützer benutzten Bausteine zusätzlich der Baustein 5.22 "Protokollierung" verwendet [12]. Der Aspekt des menschliches Versagens dieses Bausteines wird ebenfalls ignoriert.

Zu A1 In Punkt eins des konzeptionellen Modells gelten die selben Randbedingungen wie auch bei den Beschützern. Je nach Strenge der Zutrittskontrolle des Endkunden hat der Angreifer Zugriff auf das LAN des Marktrechners.

Zu A2 Der zweite Punkt zeigt das Verlangen der Angreifer, unentdeckt zu bleiben, um eine Schwachstelle möglichst lange auszunutzen. Diese Gefährdung führt der BSI unter 2.160 "Fehlende oder unzureichende Protokollierung" [19]. Anhand der Protokollierung können Angriffe aufgedeckt und Sicherheitslücken geschlossen werden. Darauf aufbauend wird auf die Gefährdung 2.22 "Fehlende oder unzureichende Auswertung von Protokolldaten" gelistet [22]. Diese macht darauf aufmerksam, dass vorhandene Protokolle auch ausgewertet werden müssen. Fallen allerdings zu viele Protokolldaten an, ist es aufgrund der Menge nicht mehr möglich, diese geeignet auszuwerten. Entstehen kann eine solche Menge an Informationen, beispielsweise durch falsche Filter, die im produktiven Einsatz die gleiche Informationsflut erzeugen, wie sie während der Entwicklungsphase notwendig sind. Aber auch legitim können riesige Datenmengen zustande kommen, etwa bei IT-Systemen in einem Informationsverbund, hier müssen sicherheitsrelevante Ereignisse protokolliert werden, die dabei helfen, Hard- und Softwareprobleme zu finden und zu beheben. Deshalb wird im Bezug auf die Auswertung die Gefährdung 4.89 "Fehlendes oder unzureichendes Alarmierungskonzept für die Protokollierung" erwähnt [26]. Bei der Alarmierung sollte jedoch darauf geachtet werden, dass die Quote der False-Positives (Fehlalarm) und False-Negatives (kein Alarm) möglichst gering ist. Bei den False-Positives können so fälschlicherweise Anwendungen auf eine Blacklist gesetzt beziehungsweise von einer Whitelist genommen werden. Bei den False-Negatives besteht zudem die Gefahr, dass ein Angriff unerkannt bleibt. Als grundsätzliche Maßnahme schlägt der BSI in Punkt 2.499 vor "Planung der Protokollierung" [42]. Diese Maßnahme beinhaltet die Erstellung eines Protokollierungskonzeptes, die Administration der Protokolldaten und das Einsetzen eines Frühwarnsystems. Das Protokollierungskonzept wird in der Maßnahme, 2.500 "Protokollierung von IT-Systemen" weitergehend erläutert. Hierbei wird ein mehrstufiger Prozess beschrieben, der alle wichtigen Aspekte von der Entwicklung bis zum Betrieb berücksichtigt. Zudem ist die Vertraulichkeit und die Integrität der protokollierten Ereignisse hervorzuheben, weshalb die Protokollierung vor unbefugten Zugriff geschützt werden muss. Das Erstellen eines Konzeptes für ein Frühwarnsystem wird aufgrund des Umfanges in dieser Thesis nicht weiter berücksichtigt. Das konzeptionelle Modell der Beschützer wird durch folgende Punkte erweitert:

- Unerlaubte Aktivitäten der Angreifer (Inhaber) sollen nachvollziehbar sein.
- Unerlaubte Aktivitäten der Angreifer müssen durch ein Frühwarnsystem erkannt werden.
- Angreifer (Inhaber) sollen die Protokolldaten nicht einsehen können.

Diese Punkte berücksichtigten allerdings nur die Angreifer. Unerlaubte Aktivitäten seitens der Mitarbeitern sind ebenfalls denkbar, da diese zu den möglichen Angreifertypen gehören. Für die Protokollierung wird daher folgendes gefordert:

- Jegliche Aktivität von Kunden, Inhabern und Akteuren, die einen Zugriff auf den Marktrechner zur Folge hat, muss zum Zweck der Nachvollziehbarkeit protokolliert werden.
- Jegliche unerlaubte Aktivitäten müssen durch ein Frühwarnsystem erkannt werden.
- Angreifer (Inhaber) und unbefugte Kunden sollen die Protokollierung nicht einsehen können.

Zu A3 In Punkt drei versuchen die Angreifer, in Besitz von Berechtigungsnachweisen zu kommen. Durch das Stehlen von Berechtigungsnachweisen scheint der Zugriff trotz Protokollierung legitim. Dazu gibt es mehrere Möglichkeiten, die zwei beliebtesten sind Phishing und Social Engineering. Im Gefährdungen-Katalog des BSI tauchen diese Methoden der Angreifer auf als 5.157 "Phishing und Pharming" und 5.42 "Social Engineering" [28, 33]. Beim Phishing versucht ein Angreifer gezielt, dem Opfer Passwörter oder andere vertrauliche Daten zu entlocken. Dabei gibt er vor, jemand zu sein, den das Opfer als vertrauenswürdig einstuft. Die Vielzahl solcher Angriffe findet über E-Mail statt, in der das Opfer einen Link klickt, der zu einer Webseite führt, die scheinbar zu der vertrauenswürdigen Entität in der E-Mail passt. Dort wird das Opfer dann aufgefordert, seine vertraulichen Daten preiszugeben. Um Mitarbeiter vor solchen Angriffen zu schützen, muss diesen ein Bewusstsein dieser Gefahren beigebracht werden. Die Verantwortung und das Risiko dafür liegt bei den Fernservice-Zentralen und Endkunden. Deswegen wird diese Methode nicht weiter betrachtet. Beim Social Engineering versuchen die Angreifer ebenfalls eine vertrauenswürdige Entität zu mimen. Die Angreifer nutzen hierzu meist Telefonanrufe. Dabei geben diese sich als Vorgesetzter, Administrator oder Techniker aus, um auf diese Weise an vertrauliche Informationen zu kommen. Social Engineering setzt darauf, eine Beziehung zu dem Opfer aufzubauen, dazu können im Voraus viele unwichtige Telefonate geführt werden. Auch hier liegt die Verantwortung und das Risoko bei den FSZs und den Endkunden. Die geringen Möglichkeiten, mit der Protokollierung diese Angriffe zu entdecken, werden in Abschnitt 4.1 erläutert.

Zu A4 In Punkt vier versuchen die Angreifer, durch Aufzeichnen und Wiedereinspielen von Nachrichten Schaden anzurichten. Vor dieser Gefährdung warnt der

BSI durch 5.24 "Wiedereinspielen von Nachrichten" [32]. Die Replay-Attacke kann Schaden anrichten, ohne dass die Angreifer über die Inhalte der Kommunikation wissen. Deshalb muss das konzeptionelle Modell erweitert werden, durch:

- Aufgezeichnete Kommunikation ist vom Marktrechner beim Wiedereinspielen zu erkennen und zu verwerfen.

Zu A5 Der fünfte Punkt besagt, dass ein Angreifer sich als Man-in-the-Middle zwischen zwei Kommunikationspartner bringt. In dieser Rolle leitet er die Nachrichten an den eigentlichen Empfänger weiter, sodass es für diesen so aussieht, als kommt die Nachricht von dem eigentlichen Sender. In diesem Zug kann der Angreifer die Nachrichten mitlesen und manipulieren. Über die beiden Gefährdungen, 5.48 "IP-Spoofing" und 5.78 "DNS-Spoofing", weist der BSI auf MITM-Attacken hin [34, 35]. Beim IP-Spoofing wird der Absender eines IP-Paketes gefälscht, sodass der Empfänger glaubt, die Nachricht stammt von einem anderen Teilnehmer. Im Zusammenhang mit leicht fälschbaren Sequenznummern des TCP-Protokolls lassen sich auf diese Weise Angriffe durchführen. Jedoch muss der Angreifer berücksichtigen, dass der keine Antworten von dem Opfer bekommt. Beim DNS-Spoofing gelingt es einem Angreifer, die Zuordnung zwischen Rechnername und zugehöriger IP-Adresse zu fälschen. Einige Dienste nutzen DNS zur Authentifizierung, indem sie beim DNS-Dienst die korrekte IP-Adresse erfragen, wenn diese manipuliert wurde, kann ein Angreifer unbefugt Zugriff erlangen. Eine erweiterte Form ist das Web-Spoofing, dort werden Domain-Name einer falschen IP-Adresse zugeordnet, sodass ein Client bei der Eingabe einer Adresse im Browser auf die Webseite des Angreifers geleitet wird. Wie einfach ein DNS-System zu kompromittieren ist, hängt von der verwendeten Software und Konfiguration ab. Zum Schutz vor DNS-Spoofing schlägt der BSI mit der Maßnahme 5.59 "Schutz vor DNS-Spoofing bei Authentisierungsmechanismen" vor, komplett auf DNS zu verzichten und IP-Adressen statt Domainnamen zu nutzen [47]. Gegen IP-Spoofing helfen besser Algorithmen zur Authentifizierung und zur Berechnung der TCP-Sequenznummern.

- Der Marktrechner soll darauf verzichten, AAS-Server über Domainnamen anzusprechen.

Zu A6 Punkt sechs kann ebenfalls durchgeführt werden ohne Wissen über Kommunikationsinhalte oder Berechtigungsnachweise. Der Marktrechner wird hierbei durch eine Vielzahl von Verbindungsanfragen überlastet. Dadurch wird verhindert, dass sich legitime Akteure verbinden können. DoS-Attacken aus dem LAN des Endkunden sind aufgrund der Randbedingungen nicht zu unterbinden, da die

Zugriffskontrolle dem Endkunden obliegt. Im Falle eines Schadens kann dieser keine Ansprüche geltend machen. Sollte eine DoS-Attacke über das Internet möglich sein, könnte der Hersteller durchaus zur Verantwortung gezogen werden. Das BSI berücksichtigt die Gefährdung von DoS-Attacken nur bei der Überlastung eines DNS-Server, 5.151 "DNS-Flooding - Denial-of-Service" [27], um die Namensauflösung von Domains zu unterbinden. Um einen kleinen Rechner, wie den Marktrechner zu überlasten, dürfte eine kleine Anzahl von Angreifern genügen. Dieser Angriff im Verbund nennt sich Distributed-Denial-of-Service (DDoS). Im Gegensatz zu DDoS-Attacken gibt es auch Low-rate-Denial-of-Service (LDoS) Attacken [50, s. 303]. Deren Ziel ist es, alle Threads eines Server zu erschöpfen und diese möglichst lange am Leben zu halten. Kontrolliert ein Angreifer alle Threads, ist nur er noch in der Lage, mit dem System zu kommunizieren. Um Angriffe dieser Art zu entdecken, wird Spezialhardware benötigt. Aus diesem Grund sollte der Marktrechner niemals direkt aus dem Internet zu erreichen und damit lahm zu legen sein. Anhand dieser Einsichten wird das konzeptionelle Modell der Beschützer um folgende Eigenschaft ergänzt:

- Direkte beliebige Verbindungsversuche aus dem Internet auf den Marktrechner sind zu unterbinden.

3.5 Maßnahmen

Die Sichtweise der Beschützer und der Angreifer haben jeweils ein konzeptionelles Modell hervorgebracht, welches mit der realen Welt verglichen wurde. Die praktikablen Inhalte werden zu Funktionensgruppen zusammengefasst, ähnlich der Security Objects aus dem Protection Profile der CC.

3.5.1 Logging & Audit

Das Verlangen nach *Nachvollziehbarkeit* der Beschützer und das Verlangen der Angreifer, unentdeckt zu bleiben, zieht sich durch alle Eigenschaften der konzeptionellen Modelle. Daraus folgt die wichtigste Maßnahme der Beschützer, einen *Logging- und Audit-Mechanismus* zu etablieren.

M1 Jegliche Aktivität von Kunden, Inhabern und Akteuren, die einen Zugriff auf den Marktrechner zur Folge hat, muss zum Zweck der Nachvollziehbarkeit protokolliert werden.

M2 Jegliche unerlaubte Aktivitäten müssen durch ein Frühwarnsystem erkannt werden.

M3 Angreifer (Inhaber) und unbefugte Kunden sollen die Protokollierung nicht einsehen können.

Die genaue Planung der Protokollierung ist sehr wichtig. Da dieser Mechanismus zudem komplex ist, wird in Kapitel 4 diese Maßnahme mit geeigneten Techniken weiterführend unter die Lupe genommen.

3.5.2 M2M-Kommunikation

Der AAS ist für die Überprüfung von Berechtigungsnachweisen und deren Rollenzuordnung zuständig. Die technische Umsetzung eines AAS ist keine Maßnahme, die in dieser Thesis Beachtung finden soll. Es wird angenommen, dass diese Problematik bereits gelöst ist. Die folgenden Maßnahmen wurden für die M2M-Kommunikation festgelegt:

M4 Die Authentifizierung zwischen Marktrechner und AAS soll über ein Public-/Private-Key Verfahren erfolgen.

M5 Die Identität des Gegenüber muss durch einen zweiten Kommunikationskanal bestätigt werden.

M6 Eine Verbindung darf erst aufgebaut werden, wenn M4 und M5 erfüllt wurden.

M7 Der AAS (Akteur) soll dem Marktrechner die Rolle(n) des zu authentifizierten Kunden verifizieren, falls diese gesendet werden.

M8 Der AAS (Akteur) soll dem Marktrechner die Rolle(n) des zu authentifizierten Kunden mitteilen, falls diese nicht gesendet wurden.

Die Kommunikation zwischen Marktrechner und AAS ist Grundlage für Authentifizierung und Autorisierung. Deshalb werden die Informationsflüsse in Kapitel 4 an einer konkreten Architektur auf Gefährdungen hin untersucht.

3.5.3 Benutzer-Kommunikation

Die nächste Maßnahme widmet sich der Kommunikation zwischen Marktrechner und Kunde. Als Voraussetzung wird angenommen, dass die M2M-Kommunikationsmaßnahmen erfolgreich umgesetzt wurden. Um Vertrauen herzustellen, wie das bei der M2M-Kommunikation der Fall ist, benötigt es einer gegenseitigen Authentifizierung. Da die gegenseitige Authentifizierung mit hohem administrativen Aufwand

einhergeht, wird zwischen Marktrechner und Kunde lediglich eine einseitige Authentifizierung durchgeführt. Dadurch wird eine ausreichend sichere Authentifizierung geschaffen, die gleichzeitig praktikabel und in einem angemessenem Budget umsetzbar ist.

M9 Der Marktrechner darf Verbindungen von Kunden nur akzeptieren, wenn deren Berechtigungsnachweise von einem AAS verifiziert wurde.

M10 Der Marktrechner soll lokale Kunden ebenfalls durch einen AAS authentifizierten lassen.

M11 Die Kommunikation zwischen Marktrechner und Kunde soll über HTTPS verschlüsselt werden, unter der Verwendung von TLS 1.2.

Auch hier werden die Datenflüsse in Kapitel 4 erbracht weitergehend betrachtet.

3.5.4 Autorisierung

Nicht jeder Benutzer soll vollen Zugriff auf alle Funktionen am System haben. Für einen Analysten beispielsweise genügt es, wenn er lesend auf Energie- und Temperaturdaten zugreifen kann. Der AAS ist verantwortlich, die ihm bekannten Rollen eines Benutzers dem Marktrechner beim Verbindungsaufbau mitzuteilen.

M12 Der Marktrechner soll den Zugriff anhand der vom AAS verifizierten oder mitgeteilten Rolle(n) autorisieren.

M13 Die verfügbaren Rollen sind jene, die anhand des Rich-Picture identifiziert wurden.

3.5.5 Verschlüsselung

Damit ein Angreifer nicht die Kommunikationsinhalte abhören kann, müssen diese ausreichend verschlüsselt werden. Ausreichend nimmt Bezug auf Möglichkeiten, welche der Marktrechner aufgrund seiner Hardware leisten kann. Folgende Maßnahmen sollen bei der Auswahl eines geeigneten Verschlüsselungsalgorithmus helfen:

M14 Die Verschlüsselung soll unabhängig von der Authentifizierungsmethode asynchron sein.

M15 Das Verschlüsselungsverfahren muss Perfekt Forward Security (PFS) einsetzen.

M16 Aufgezeichnete, verschlüsselte Kommunikation ist vom Marktrechner beim Wiedereinspielen zu erkennen und zu verwerfen. (Nonce)

3.5.6 Verbindungen

Verbindungen zu und vom Marktrechner unterliegen potentiellen Gefährdungen, welche ein Angreifer ausnutzen kann. Dem sollen die folgenden Maßnahmen Einhalt gebieten:

M17 Der Marktrechner soll darauf verzichten, AAS-Server über Domainnamen anzusprechen. (Spoofing)

M18 Direkte beliebige Verbindungsversuche aus dem Internet auf den Marktrechner sind zu unterbinden. (DoS)

3.5.7 Notentriegelung

Für den Fall des Verbindungsausfalles zum AAS, beispielsweise während eines Netzwerkausfalls oder einer Netzwerkstörung, muss weiterhin der Zugriff vor Ort auf das System gewährleistet werden. Dazu sollen nach Bedarf, beispielsweise Einmalkennwörter vom Eigentümer oder von der Fernservice-Zentrale ausgestellt werden.

(M19) Der Marktrechner muss lokal durch einen Einmal-Mechanismus entsperrbar sein, wenn kein AAS vefügbar ist.

Diese Notentriegelungsmaßnahme ist Teil des kompletten Authentifizierungs- und Autorisierungskonzeptes, ist jedoch unabhängig vom Fokus der Thesis auf den Fernzugriff und wird daher hier im weiteren Verlauf nicht weiter betrachtet.

Kapitel 4

Bedrohungsmodellierung

In der Bedrohungsanalyse wurden Gefährdungen auf abstrakter, konzeptioneller Ebene mit der Problem Structuring Method SSM betrachtet. Es wurde absichtlich darauf verzichtet, die eigentliche Implementierung zu berücksichtigen. Anhand von Data Flow Diagrammen werden in diesem Kapitel die Architektur und die Implementierung analysiert, um die gefährdeten Informationsflüsse auf Bedrohungen hin zu untersuchen. Betrachtet werden die wichtigsten Informationsflüsse für Authentifizierung und Autorisierung: Logging und Audit, M2M-Kommunikation und Benutzer-Kommunikation.

4.1 Log-/Auditdateien

In Abschnitt 3.5 wurden die Maßnahmen aus der Bedrohungsanalyse festgehalten. Eine der Wichtigsten ist der Logging-/Audit-Mechanismus. Damit dieser korrekt funktioniert und nicht seinerseits zur Sicherheitslücke wird, werden dessen Informationsflüsse genauer betrachtet. Dieser Abschnitt geht auf Gefährdungen und Bedrohungen aus dem Baustein 5.22 "Protokollierung" und 3.102 "Server unter Unix" ein.

4.1.1 Informationsfluss

Der Informationsfluss berücksichtigt Log- und Auditdaten von Anwendungen des Marktrechners, die auf dessen permanenten Speicher protokolliert wurden. In der Abbildung 4.1 ist der Informationsfluss von Log- und Auditdaten zu sehen. Ausschließlich Administratoren sollen in der Lage sein, über eine Betrachtungsfunktion die Daten einzusehen, da dort sensitive Daten, etwa Passwörter, beinhaltet sein können. Unter keinen Umständen soll es möglich sein, die Daten zu verändern.

Für die Inhalte ist anzunehmen, dass diese nur von vertrauenswürdigen Anwendungen des Systems geschrieben werden. Die Inhalte selbst können aber von nicht vertrauenswürdigen Quellen kommen, daher muss dort mit Schadcode gerechnet werden.

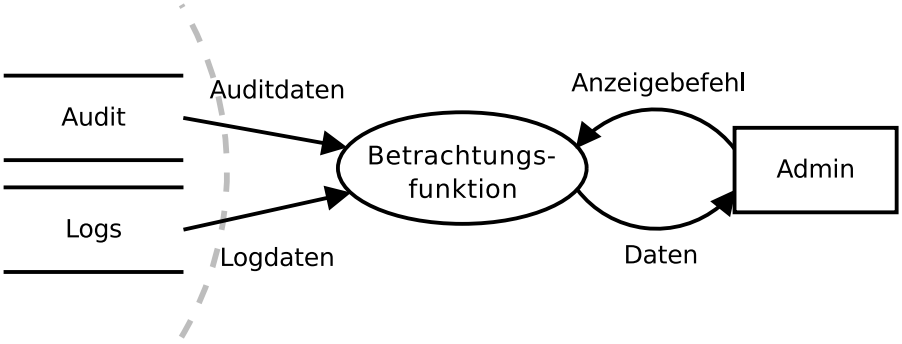

Abbildung 4.1: DFD Log-/Audit-Datenfluss

4.1.2 Gefährdungen identifizieren

Die Protokollierung auf dem Marktrechner findet lokal statt, sodass die Aspekte der zentralen Protokollierung aus dem Baustein "Protokollierung" nicht betrachtet werden. Abbildung 4.2 zeigt die Gefährdungen der einzelnen Beteiligten. Sabotage ist ein Aspekt, der bei Log- und Audit-Dateien gegeben ist, denn diese enthalten Informationen, die auf unerlaubte Aktivitäten schließen lassen. Versucht ein Angreifer, beispielsweise per Bruteforce-Angriff, das Passwort eines Benutzers herauszufinden, dann sind im Audit die fehlgeschlagenen Authentifizierungsversuche aufgezeichnet. Sollte dieser geglückt sein und der Benutzer hat Rechte, das Audit zu verändern, kann der Angreifer seine Spuren verwischen. Ein anderer Angreifer könnte versuchen, Schwachstellen in der Implementierung zu finden. Im Log würden dadurch zahlreiche Fehlermeldungen entstehen. Durch Entfernen dieser kann er sicherstellen, dass eine eventuelle Sicherheitslücke unentdeckt bleibt. Der zweite Aspekt für Log- und Audit-Daten ist die Informationspreisgabe, da in beiden sensitive Daten enthalten sein können, welche Unberechtigte nicht einsehen dürfen. Der BSI hat diese Gefährung unter 2.161 "Vertraulichkeits- und Integritätsverlust von Protokolldaten" [20] gelistet. Vertrauliche sensitive Informationen sind, beispielsweise Benutzername, IP-Adresse oder E-Mail. Falls Unberechtigte diese Daten einsehen können, entsteht dadurch eine neue Gefährdung, die der BSI unter 5.18 "Systematisches Ausprobieren von Passwörtern" benennt [29]. Sollte ein Angreifer den Benutzernamen aus den vertraulichen Daten der Protokollierung erlangen, kann er diesen dazu nutzen, gezielt das Passwort zu erraten. Informationspreisgabe ist auch für die Betrachtungsfunktion zu berücksichtigen, diese darf Daten nur für

Administratoren anzeigen. Zudem unterliegt sie der Personifikation, indem die eigentliche Betrachtungsfunktion mit Schadcode modifiziert wurde und nun vorgibt, die Ursprüngliche zu sein. Der BSI weist in 5.2 "Manipulation an Informationen oder Software" auf diese Gefährdung hin [31]. Auch der Administrator unterliegt der Personifikation, indem ein Angreifer in Besitz der Berechtigungsnachweise kommt. Eine weitere Gefährdung bei Inhalten von Log- und Auditdaten wird durch die Bedrohungstunnelung verursacht [50, s. 265]. Dabei wird Schadcode durch einen oder mehrere Instanzen getunnelt. Beispielsweise eine Anwendung, die bei jedem Anmeldeversuch den Benutzernamen protokolliert, kann zu einer Tunnelinstanz werden, indem ein Angreifer statt eines Benutzernamens Javascript-Schadcode angibt. Das Opfer des Angriffes ist eine Betrachtungsfunktion für die Protokollierung, welche die Inhalte in einer Web-Anwendung darstellt. Da die Web-Anwendung der protokollierenden Anwendung vertraut, werden die Inhalte nicht auf der Schadcode geprüft. Deshalb muss beachtet werden, dass die Daten zwar von vertrauenswürdigen Quellen kommen, die Inhalte allerdings aus nicht vertrauenswürdigen Quellen stammen. Unter diesem Gesichtspunkt muss eine Web-Anwendung in den Daten nach JavaScript-Inhalten suchen, auch wenn diese scheinbar von vertrauenswürdigen Quellen stammen.[1]

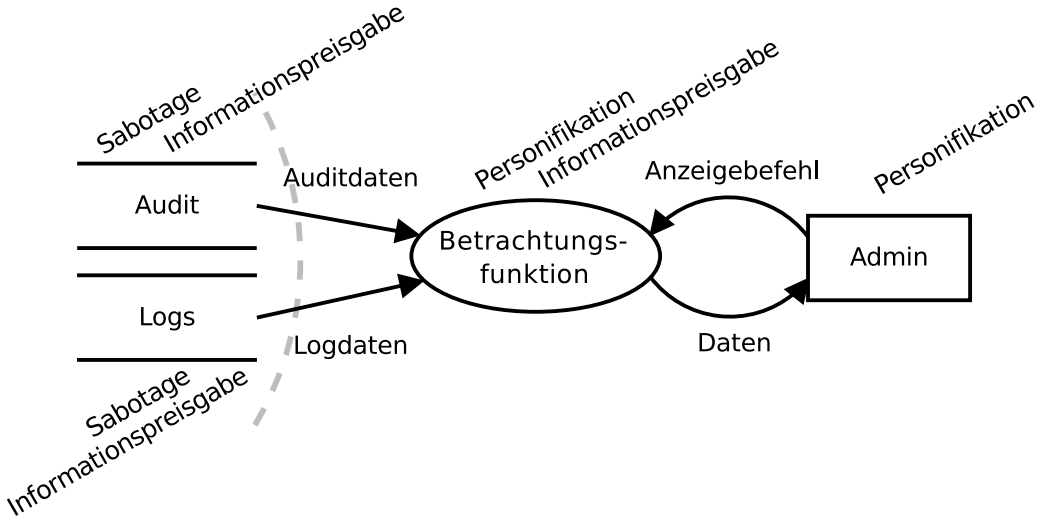

Abbildung 4.2: DFD Logdaten Gefährdungen

4.1.3 Maßnahmen

Aus den Gefährdungen ergeben sich folgende Maßnahmen, welche zur Sicherung der Informationsflüsse durchgeführt werden müssen. Für Unix Systeme, unter

[1] Ein solcher Angriff wurde erfolgreich an https://github.com/nlaplante/syslogng-web durchgeführt

welche Linux aus der Sicht des BSI fällt, gibt es die Maßnahme 4.25 "Einsatz der Protokollierung im Unix-System" [45]. Diese weist darauf hin, dass die Protokolldateien möglichst von Systemtools zu erstellen sind. Log- und Audit-Daten dürfen in einer Datei oder Datenbank abgelegt werden. Dabei weist der BSI darauf hin, dass die Datei-Attribute ausschließlich dem Systembenutzer für Logging und Auditing modifizierende Rechte geben soll. Dabei wird angenommen, dass Datei-/Datenbankzugriffsmechanismus sowie Systemauthentifizierung nicht komprimiert sind. Der BSI empfiehlt für die Protokollierung mindestens folgende Ereignisse zu berücksichtigen: Logins (auch Fehlversuche), Aufruf von su, Fehlerprotokollierungsdatei / Protokollierung wichtiger Vorgänge (errorlog) und Administratortätigkeiten (insbesondere von root ausgeführte Befehle). Für die Alarmierung verweist das BSI zusätzlich noch auf halbautomatische Logfileparser des Systems, beispielsweise swatch, logsurfer oder checksyslog. Das Betrachten der Daten darf nur durch einen Administrator geschehen, der durch die Datei-Attribute ausschließlich lesenden Zugriff erhält. In der Maßnahme 2.33 "Aufteilung der Administrationstätigkeiten unter Unix" weißt der BSI daraufhin, dass unter Linux Administratoren meist mit Super-User Rechten versehen werden [41]. In diesem Fall ist es einem Benutzer möglich, alle Dateien zu lesen, schreiben und auszuführen. Als eine mögliche Lösung werden daher Linux-Systembenutzer vorgeschlagen. Diese sind Eigentümer, der für ihre Prozesse benötigten Programmen und Dateien. Darüber hinaus haben diese keine weiteren Rechte. Für das Betrachten der Protokolldaten bedeutet dies, dass es einen Benutzer gibt, der das alleinige Leserecht auf diese Daten hat. Durch das Vermeiden von vielen Benutzern mit Super-User Rechten wird zudem das Risiko gesenkt, dass die Betrachtungsfunktion von einem Angreifer modifiziert wurde, da die potentiellen Opferkandidaten reduziert wurden. Bei der Auswahl eines Administrators muss trotzdem mit besonderer Sorgfalt vorgegangen werden. Der BSI empfiehlt dies in der Maßnahme 3.10 "Auswahl eines vertrauenswürdigen Administrators und Vertreters" [44]. Dort wird zudem darauf aufmerksam gemacht, dass der Administrator eine wichtige Schlüsselrolle ist und daher in seiner Abwesenheit genügend qualifizierte und natürlich auch vertrauenswürdige Vertreter vorhanden sein müssen. Ist die Betrachtungsfunktion eine Web-Anwendung, benötigt sie eine Authentifizierung, die mit der Systemauthentifizierung integriert ist. Log- und Audit-Daten müssen vor der Darstellung durch einen Sanitizer von schadhaften Inhalten befreit werden. Wurden solche Daten entfernt, muss der Administrator darauf hingewiesen werden. Der Administrator weist sich durch seinen Berechtigungsnachweis aus, dieser wird von ihm vor fremden Zugriff geschützt. Weiterhin erfolgt erneut die Annahme, dass die Systemauthentifizierung nicht komprimiert wurde. Als letzten Punkt der Maßnahme 4.25 empfiehlt der BSI die Sicherung der Protokollierung und verweist dabei auf gesetzliche und vertragliche Fristen.

4.2 Benutzer-Kommunikation

Eingehende Benutzerverbindungen sollen ausschließlich über HTTPS erfolgen. Zu diesem Zweck wurde das RestGateway entwickelt, über welches auf den Marktrechner zugegriffen werden kann.

4.2.1 Informationsfluss

In Abbildung 4.3 wird der Informationsfluss über das RestGateway gezeigt. Dabei fließen die Daten durch drei Vertrauensgrenzen. Sowohl RestGateway als auch LanGateway fungieren dabei als Datenproxy. Beide leiten die Anfragedaten ohne Validierung der Inhalte weiter. Deswegen muss darauf geachtet werden, dass ein Angreifer keine Bedrohungstunnelung durchführen kann. Das RestGateway arbeitet als Wrapper, unterschiedliche Abfragen werden anhand der URL unterschieden und in entsprechende TCP-CAN-Telegramme übersetzt. Die URL-Parameter einer Anfrage werden vom RestGateway auf einen gültigen Wertebereich überprüft. Die Antwort auf eine solche Anfrage sind menschenlesebare interpretierte Inhalte.

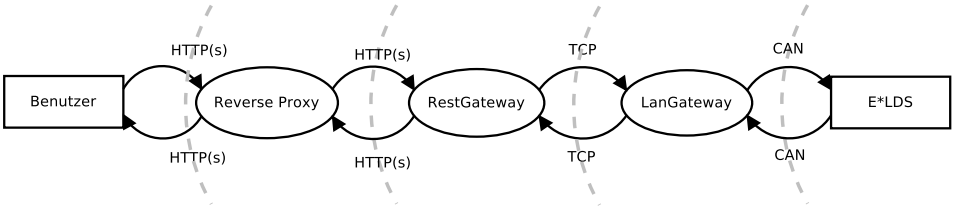

Abbildung 4.3: DFD HTTP-Anfrage

4.2.2 Gefährdungen identifizieren

In Abbildung 4.4 sind die Bedrohungen in den fünf Kategorien aufgezeigt. Der Benutzer unterliegt der Gefahr der Personifizierung durch das Stehlen seines Berechtigungsnachweises. Dazu werden Phishing-Attacken genutzt, die bereits in Abschnitt 3.4 ausführlich erläutert wurden. Ein Gefährdung durch Disput ist für den Benutzer ausgeschlossen, da die Log- und Audit-Daten nicht verändert werden können und der Zugriff zur Nachvollziehbarkeit im Audit dokumentiert ist.

Auf dem Weg, den eine Benutzeranfrage zurücklegen muss, unterliegt diese an zwei Stellen der Möglichkeit einer Man-in-the-Middle-Attacke. Zunächst zwischen Benutzer und RestGateway und anschließend zwischen RestGateway und LanGateway. Durch einen MITM können an beiden Gateways Informationen preisgegeben werden, die der MITM mitliest. Zudem ist dieser auch in der Lage, die Inhalte zu sabotieren, anstatt die Informationen nur passiv mitzulesen. Auf Seiten des RestGateway

sind die Informationen einfach zu interpretieren und daher einfach zu manipulieren. Ein MITM zwischen den beiden Gateways benötigt für die gleichen Aufgaben ein detailliertes Wissen über das Herstellerprotokoll. Ein dritter Möglichkeit für den MITM ist es, personifizierend aufzutreten. In der Personifikation als RestGateway kann der Angreifer eine Anfrage direkt an das LanGateway weiterleiten, wodurch eventuelle Sanatizer übergangen werden. Die Antwort des LanGateway kann er zudem beliebig sabotieren. Als LanGateway-Personifizierung ist er zwar nicht in der Lage, eine Nachricht an den CAN-Bus weiterzuleiten, kann jedoch dem Benutzer die Illusion einer erfolgreichen Kommunikation geben. Die Voraussetzungen sind hierbei die gleichen wie bei der Informationspreisgabe und Sabotage. Die verschiedenen Möglichkeiten, eine MITM-Attacke durchzuführen, wurden in Abschnitt 3.4 durch die verschiedenen Spoofing-Verfahren bereits detailliert erläutert.

Die Funktionen RestGateway und LanGateway unterliegen durch ihre Netzwerkschnittstellen der Gefahr einer DoS-Attacke. Während das RestGateway über das Internet kontaktiert werden kann, ist das LanGateway nur über das LAN zu erreichen. Das LAN obliegt der Kontrolle der Endkunden, daher liegt das Risiko alleine beim Endkunden und wird nicht weiter betrachtet. Auf die Gefährdungen durch DoS-Attacken wurde bereits ausführlich in Abschnitt 3.4 eingegangen. Ziele, die ein Angreifer durch die Überlastung des Marktrechners verfolgen kann, sind Verhinderung der Datenarchivierung, der Alarmierung und der Überwachung der Anlage. Anlagenschaden kann er damit nicht anrichten, da alle Komponenten der Kälteanlage über einen Notmodus, ohne den Marktrechner arbeiten können. Bei der Beschreibung einer Kälteanlage wurde zudem gesagt, dass die Prozesse, um Warenschaden anzurichten, nur langsam voranschreiten. Aus diesem Grund wird ein Monteur die Anlage höchstwahrscheinlich wieder instand setzen, bevor Schaden entsteht, da der Angriff auf jeden Fall entdeckt wird.

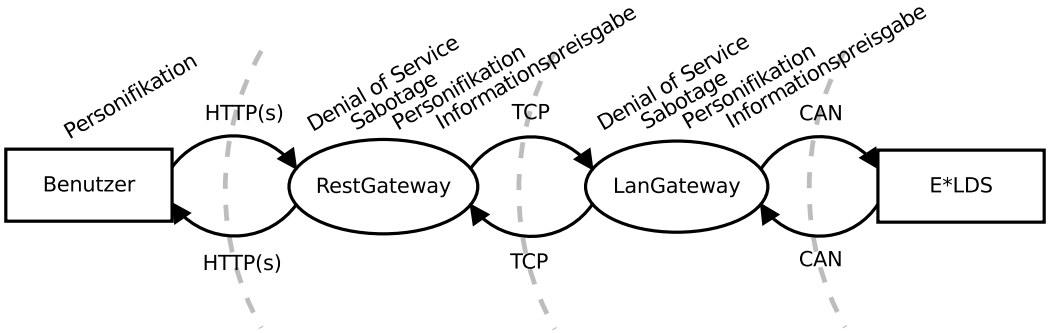

Abbildung 4.4: DFD HTTP-Gefährdungen

4.2.3 Maßnahmen

An Berechtigungsnachweise von Benutzern zu gelangen, ist für einen motivierten Angreifer durch Phishing-Attacken möglich. Unter dieser Annahme wird festgelegt, dass ungewöhnliche Login-Muster in den Audit-Daten erkannt werden müssen, beispielsweise wenn sich ein Benutzer innerhalb weniger Minuten von unterschiedlichen physikalischen Orten verbindet. Um RestGateway und LanGateway durch einen Man-in-the-Middle zu schützen, wurde bereits in Abschnitt 3.4 festgelegt, auf DNS-Adressen zu verzichten [47]. Diese Anforderung ist jedoch problematisch, wenn es um die Flexibilität einer IT-Infrastruktur geht. Deshalb können DNS-Adressen eingesetzt werden, wenn bei der Konfiguration des DNS-Servers sorgfältig vorgegangen wird. Die Gefährdung durch eine Fehlkonfiguration wird durch eine menschliche Fehlhandlung verursacht und deshalb in diesem Rahmen nicht weiter betrachtet. Ein 100-prozentiger Schutz gegen einen MITM ist daher nicht zu gewährleisten. Der Authentifizierungsmaßnahmen des BSI für einen Schutz gegenüber Phishing-Attacken, ist leider nicht existent. Damit ein Angreifer, der über eine Phishing-Attacke an den Berechtigungsnachweis eines Benutzers gelangt ist, trotzdem keinen Zugriff auf das System erlagen kann, soll eine Zwei-Faktor-Authentifizierung (2FA) eingesetzt werden. Eine 2FA benötigt zur erfolgreichen Authentifizierung eines Benutzers zwei Komponenten. Zum einen etwas, was der Benutzer weiß und zum andern etwas, was der Benutzer besitzt. Die erste Anforderung wird durch das Wissen von Benutzername und Passwort bereits erfüllt. Für die zweite Anforderung muss sich der Benutzer durch ein Client-Zertifikat ausweisen. Bei der 2FA findet zunächst eine Zertifikatsüberprüfung statt, dabei überprüft der Client das Server-Zertifikat und vice versa. Aus Gründen der Benutzerfreundlichkeit wird das Client-Zertifikat auf den Endgeräten der Benutzer installiert, wodurch die Überprüfung für diese transparent funktioniert. Im nächsten Schritt weist sich der Benutzer aktiv durch seinen Berechtigungsnachweis aus. Auf diesem Weg wird verhindert, dass von unautorisierten Geräten auf den Marktrechner zugegriffen werden kann. Dadurch wird das Risiko einer MITM-Attacke, verglichen mit Aufwand und Kosten, auf ein akzeptables Niveau gesenkt. Durch den Einsatz von Zertifikaten entsteht allerdings das Risiko durch die Gefährdung 5.84 "Gefälschte Zertifikate" [37]. Hier muss darauf geachtet werden, dass Zertifikate auch geprüft werden und das kein Mitarbeiter absichtlich oder fälschlicherweise beliebig Zertifikate generieren kann. Weitere Details zur Schlüsselverwaltung werden im nächsten Abschnitt, anhand der Schlüsselkontinuität, erläutert.

Die Authentifizierung, welche in Abschnitt 3.5 gefordert wird, muss über drei Vertrauensgrenzen sichergestellt werden. Bei jedem Durchschreiten einer Vertrauensgrenze besteht das Risiko, attackiert zu werden. Um die Quellen für Gefährdungen durch zu viele Vertrauensgrenzen zu reduzieren, sollte die Funktionalität des Lan-

Gateway in das RestGateway integriert werden. Ein externes RestGateway würde anstatt des LanGateway mit dem internen RestGateway kommunizieren, welches dann lediglich als Proxy fungiert. Alternativ muss sichergestellt werden, dass das LanGateway ausschließlich lokal über die Loopback-Adresse (127.0.0.1) erreichbar ist. Aufgrund der Gefahr durch Bedrohungstunnelung muss jede Funktion die für sich relevanten Eingaben von einem Sanatizer prüfen lassen.

4.3 M2M-Kommunikation

Die Authentifizierung und Autorisierung wird vom Marktrechner an einen AAS-Server ausgelagert. Für diesen Abschnitt ist der Baustein 1.7 "Kryptokonzept" aus der Kategorie Übergreifende Aspekte von Bedeutung [10].

4.3.1 Informationsfluss

In Abbildung 4.5 wird der Informationsfluss zwischen Marktrechner und AAS dargestellt. Eingeleitet wird der Informationsfluss stets vom Marktrechner, wenn dieser eine Benutzeranfrage erhält und den Berechtigungsausweis validieren möchte. Als Antwort erhält er das Validierungsergebnis und für den Erfolgsfall die Rollen des Benutzers. Alternativ kann der Marktrechner den Berechtigungsnachweis in Verbindung mit einer Rolle an den AAS senden. Ein positives Validierungsergebnis sagt dann aus, dass der Berechtigungsnachweis gültig ist und der Benutzer die geforderte Rolle inne hat. Dies kann beispielsweise für eine mehrstufige Autorisierung lokal am Marktrechner genutzt werden, da hier die Einstellungen über die GUI in mehreren Ebenen organisiert sind. Die eigentlichen Module, beispielsweise das RestGateway, wurden in der Abbildung 4.5 der Einfachheit wegen in Marktrechner und AAS abstrahiert. Bevor die Validierung erfolgen kann, muss zunächst eine authentifizierte Verbindung vom Marktrechner zum AAS hergestellt werden.

4.3.2 Gefährdungen identifizieren

Die Gefährdungen werden in Abbildung 4.6 visualisiert. Sowohl Marktrechner als auch AAS unterliegen der Gefährdung der Personifikation. Die Verbindung zwischen den beiden Teilnehmern ist über ein Public/Private-Key Verfahren abgesichert. Dabei weist der BSI auf die Gefährdung 4.35 "Unsichere kryptographische Algorithmen" hin [25]. Hierbei muss darauf geachtet werden, dass ein Angreifer nicht mit vertretbaren Ressourcen das kryptographische Verfahren brechen kann. Des Weiteren besteht die Gefahr 2.19 "Unzureichendes Schlüsselmanagement bei

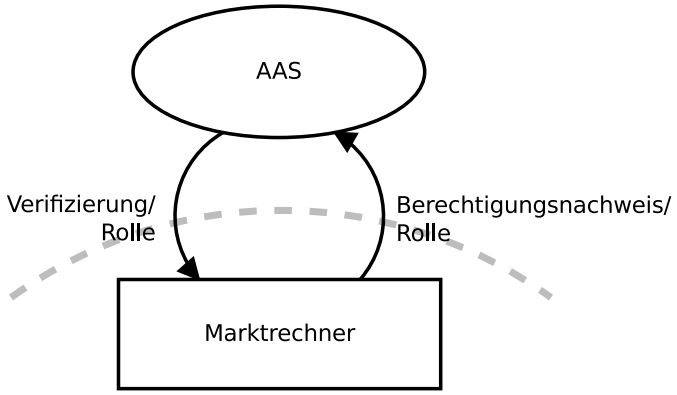

Abbildung 4.5: DFD Authentifizierung-Autorisierung

Verschlüsselung" [21]. Ein ungeeignetes Schlüsselmanagement identifiziert der BSI an:

- kryptographischen Schlüssel, die in einer ungesicherten Umgebung erzeugt oder aufbewahrt werden,
- ungeeignete, oder leicht erratbare Schlüssel,
- zur Verschlüsselung bzw. Entschlüsselung eingesetzten Schlüssel, die den Kommunikationspartner nicht auf einem sicheren Weg erreichen.

Davon abgeleitet wird die Gefährdung 5.83 "Kompromittierung kryptographischer Schlüssel" [36]. Bei Verfahren mit kryptographischen Schlüsseln hängt die Sicherheit maßgebend davon ab, dass diese geheim bleiben. Ein Beispiel der Kompromittierung, neben dem Schlüsselmanagement, ist das Entwenden der als Backup hinterlegten Schlüssel. Dadurch entsteht die Gefährdung der Informationspreisgabe am AAS. Ein Angreifer könnte sich als Marktrechner ausgeben und versuchen, über Bruteforce oder sonstige Verfahren das Passwort eines Nutzers herauszufinden.

Der Marktrechner unterliegt zudem der Gefährdung einer DoS-Attacke. Da er jedoch derjenige ist, der die Verbindung initialisiert, und eingehende Verbindungen nicht zugelassen werden, ist das Risiko bei der M2M-Kommunikation zu vernachlässigen.

4.3.3 Maßnahmen

Die Kryptographie von Authentifizierungslösungen wurde vor Jahrzehnten entworfen und ist dementsprechend erprobt. Die Auswahl eines geeigneten Verfahrens beschreibt das BSI in der Maßnahme 2.164 "Auswahl eines geeigneten kryptographischen Verfahrens" [40]. Bei symmetrischen Verfahren, wie AES oder SERPENT,

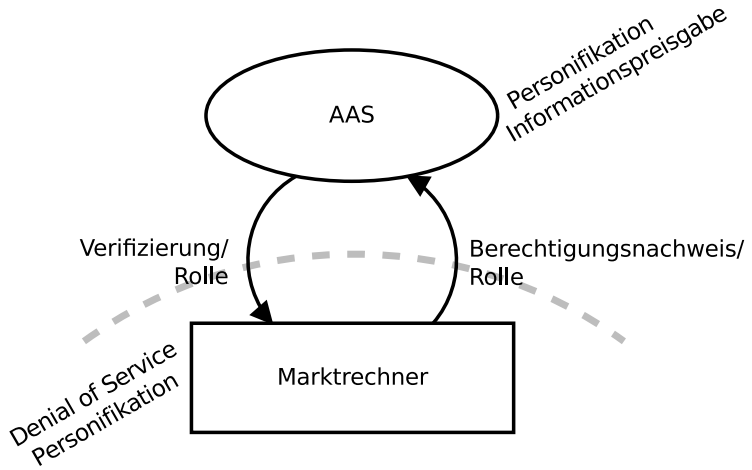

Abbildung 4.6: DFD Authentifizierung-Autorisierung

soll eine Mindestschlüssellänge von 100-Bit gewählt werden. Bei asymmetrischen Verfahren eignet sich RSA oder auf elliptischen Kurven basierende Verschlüsselungsverfahren. Als Schlüssellänge für RSA wird mindestens 1536-Bit gefordert. Damit die Kryptographie funktioniert, müssen Schlüssel ausgetauscht werden. Das BSI hat in der Maßnahme 2.46 "Geeignetes Schlüsselmanagement" sinnvolle Hinweise für die einzelnen Aufgaben des Schlüsselmanagements zusammengestellt. Zunächst müssen die Schlüssel generiert werden, das soll in einer sicheren Umgebung und unter dem Einsatz geeigneter Schlüsselgeneratoren erfolgen. Die primäre Problemstellung bei der Schlüsselverwaltung ist allerdings: Wie gelangt ein Schlüssel vom Erzeuger zu den vorgesehenen Empfängern? Das populärste Modell der Schlüsselverteilung ist das "Schlüssel fallen aus dem Himmel"-Modell. Es ist deshalb so weit verbreitet, weil durch die Komplexität des Problems, Entwickler von Sicherheitsprotokollen es gerne ignorieren und jemand anderem die Lösungsfindung zuschieben. Das BSI macht hierzu keinen Lösungsvorschlag, es gibt lediglich den banalen Hinweis, die Schlüssel nicht unverschlüsselt zu übertragen, sondern entsprechende Verfahren, beispielsweise Key Encryption Key (KEK) bei X.509-Zertifikaten, zu verwenden. Ein Konzept, das nicht dem "Schlüssel fallen aus dem Himmel"-Modell unterliegt, ist das der Schlüsselkontinuität [51]. Implementiert wird dieses beispielsweise in SSH oder PGP. Ihm zugrunde liegt das Konzept der Beständigkeit, dass bedeutet, anhand des Schlüssel kann überprüft werden, ob die Entität, mit welcher gestern kommuniziert wurde, auch heute noch dieselbe ist. Die Schlüsselkontinuität unterliegt allerdings einer Schwachstelle, denn beim initialen Austausch ist eine MITM-Attacke möglich. Ein Angreifer hat dementsprechend exakt eine Chance, die Verbindung zu kompromittieren. Wenn er zu diesem Zeitpunkt die Attacke nicht durchführen kann, hat er seine Chance vertan. Ein derartiger Angriff ist nicht auszuschließen, jedoch ist die Wahrscheinlichkeit sehr gering und daher das Risiko für die M2M-Kommunikation

akzeptabel. Sollte in Zukunft entschieden werden, dass das Risiko eines MITM während des initialen Schlüsselaustausches nicht tragbar ist, können Fingerprints der öffentlichen Schlüssel oder Zertifikate ausgetauscht werden. Der Austausch von Fingerprints muss natürlich auf einem alternativen Kommunikationskanal erfolgen. Hierzu empfiehlt sich der Versandweg per Post oder Kurier. Beim Versand des verifizierenden Datenträgers gilt jedoch Vorsicht. Der BSI hat für die Versendung von Datenträgern eine Maßnahme verfasst. Unter 5.23 "Auswahl einer geeigneten Versandart für Datenträger" listet der BSI vier Möglichkeiten für den Versand [46]: Post, Kurierdienste, persönlicher Kurier oder persönliche Übergabe. Für den Austausch von Datenträgern, die die Identität von AAS und Marktrechner bescheinigen, sollte die persönliche Übergabe gewählt werden. Hierbei wird ein vertrauenswürdiger Kurier, etwa ein Mitarbeiter, mit dem Datenträger gesendet und übergibt diesen persönlich dem dafür bestimmten Empfänger. Während der Übergabe bekommt der Kurier auch den Datenträger des Anderen, wodurch eine gegenseitige Authentifizierung möglich wird. Diese Maßnahme ist die sicherste, aber auch die teuerste. Ob eine FSZ statt eines persönlichen Kuriers die Post einsetzt, hängt von der eigenen Risikobewertung ab, der Hersteller kann hier nur eine Empfehlung aussprechen. Nach dem initialen Schlüsselaustausch besteht für den MITM eine weitere Möglichkeit die Verbindung zu komprimierten und zwar während eines Schlüsselwechsels. In einer Sicherheitsrichtlinie muss festgelegt werden, in welches Zeitabständen ein Wechsel stattfinden soll. Von Seiten des BSI gibt es hierzu keine Richtwerte. Ein ausgetauschter Schlüssel muss gespeichert werden. Unter dem Punkt Schlüsselinstallation und -speicherung, weist das BSI daraufhin, dass zumindest Zeitweise die Schlüssel im Klartext verfügbar sind. Kann dem System nicht vertraut werden, empfiehlt sich die Auslagerung auf Hardware-Verschlüsselungskomponenten. Letzter Teil der Schlüsselverwaltung ist die Schlüsselvernichtung. Hierbei muss sichergestellt werden, dass ein Schlüssel wirklich entfernt wurde, etwa durch wiederholtes überschreiben der Speicherzellen auf einem Datenträger.

Kapitel 5

Prototypische Implementierung

In diesem Kapitel wird eine prototypische Implementierung anhand der in den vorherigen Kapiteln besprochenen Maßnahmen, gezeigt. Zunächst werden Kriterien festgelegt, die die prototypische Implementierung erfüllen soll. Als Leitfaden dienen die Security Assurance Requirements (SAR) aus dem Protection Profile der Common Criteria. Diese definieren in einer standardisierten Sprache die notwendigen Aufgaben für die verschiedenen Stufen der Vulnerability Analysis (AVA_VAN).

5.1 Schlüsselwörter

In diesem Abschnitt werden die folgenden Schlüsselwörter definiert, welche als Hilfe zur Bewertung bei der Evaluierung dienen. Die Schlüsselwörter und deren Bedeutung orientieren sich an dem Request For Change (RFC) 2119 der Internet Engineering Task Force (IETF) [7]:

"MUSS", "SOLL", "ERFORDERLICH", "DARF" "EMPFOHLEN", "NICHT", "KANN" und "OPTIONAL"

1. **MUSS** Dieses Wort oder der Term "SOLL" und "ERFORDERLICH" bedeuten, dass eine Definition unverzichtbarer Teil einer Spezifikation sein soll.

2. **SOLL NICHT** Diese Phrase bedeutet ein Verbot einer Definition als Teil einer Spezifikation.

3. **DARF** Dieses Wort oder das Adjektiv "EMPFOHLEN" bedeuten, dass es Gründe gibt, warum unter besonderen Umständen auf diese Definition als Teil einer Spezifikation verzichtet werden darf.

4. **DARF NICHT** Diese Phrase bedeutet, dass auf ein Verbot einer Definition als Teil einer Spezifikation unter besonderen Umständen verzichtet werden darf.

5. **KANN** Dieses Wort oder der Term "OPTIONAL" bedeuten, dass diese Definition als Teil einer Spezifikation nach Belieben umgesetzt werden darf.

5.2 Anforderungen

Die folgenden Anforderungen werden an die prototypische Implementierung gestellt. Die Anforderungen werden dabei aus den Maßnahmen der Kapitel 3 und 4 zusammengestellt.

5.2.1 Log-/Audit-Mechanismus

Das System *MUSS* einen Audit-Mechanismus, zur Erfüllung der Maßnahme M1 (vgl. 3.5), implementieren, der zum Zweck der Nachvollziehbarkeit jegliche Benutzeraktivitäten protokolliert. Aus der BSI Maßnahme 4.33 (vgl. 4.1.3) folgt, der Zugriff auf die Protokolldaten *SOLL* ausschließlich dem Systembenutzer für Logging und Auditing möglich sein. Sonstige Rechte *MUSS* dieser Benutzer entzogen bekommen. Des Weiteren *DARF* das System *NICHT* Informationen protokollieren, die sensitive Daten oder datenschutzrechtlich illegal Inhalte beinhalten, welches in Maßnahme 4.25 (vgl. 4.1.3) empfohlen wird. Das System *KANN* ein Frühwarnsystem haben, das durch die Maßnahme M3 (vgl. 3.5) gefordert wird. Ist dies nicht der Fall *MUSS* die Möglichkeit bestehen die Audit-Daten in Echtzeit mitzuverfolgen, um ein eigenes Frühwarnsystem zu etablieren. Es wird durch die BSI Maßnahme 4.25 (vgl. 4.1.3) *EMPFOHLEN*, ein eigenes Frühwarnsystem mittels halbautomatische Logfileparser des Systems umzusetzen.

5.2.2 M2M-Kommunikation

Das System *MUSS* sich bei der Auswahl eines geeigneten kryptographischen Verfahren an die Empfehlungen der BSI Maßnahme 2.164 (vgl. 4.3.3) halten. Bei symmetrischen Verfahren *MUSS* eine Mindestschlüssellänge von 100-Bit gewählt werden und bei asymmetrischen Verfahren werden mindestens 1536-Bit gefordert. Durch die Maßnahme M4 (vgl. 3.5) wird *EMPFOHLEN*, asymmetrische Verfahren den symmetrischen vorzuziehen. Die dabei genutzte Kryptographie *DARF* der, durch Maßnahme M15 (vgl. 3.5) geforderten, Perfect Forward Security genügen. Für das

gewählte Verfahren *MUSS* ein geeignetes Schlüsselmanagement, nach BSI Maßnahme 2.46 (vgl. 4.3.3), vorgewiesen werden. Dabei *MUSS* die Generierung von Schlüsseln in einer sicheren Umgebung stattfinden. Die Distribution von geteilten Schlüsseln bei den symmetrischen Verfahren sowie Client-Zertifikaten bei den asymmetrischen Verfahren *DARF NICHT* unverschlüsselt erfolgen. Bei asymmetrischen Verfahren *DARF* der öffentliche Schlüssel durch einen Fingerprint verifiziert werden (Maßnahme M5, vgl. 3.5). Beim Austausch der Fingerprints ist es *ERFORDERLICH*, dass der Austauschkanal ein anderer ist, wie der Kommunikationskanal (vgl. 4.3.3). Die Distribution *MUSS* die BSI Maßnahme 5.23 (vgl. 4.3.3) berücksichtigten. Des Weiteren *MUSS* das System nach Maßnahme M7 und M8 (vgl. 3.5) eine rollenbasierte Autorisierung, der erfolgreich authentifizierten Benutzer, durchführen. Optional *KANN* das System die Schlüsselkontinuität implementieren.

5.2.3 Benutzer-Kommunikation

Für das Zustandekommen einer Verbindung, zwischen Benutzer und Marktrechner, ist es *ERFORDERLICH*, dass eine Two-Factor-Authentication (vgl. 4.2.3) erfolgreich durchgeführt wurde. Der Verbindungsaufbau *MUSS* immer über einen Reverse Proxy erfolgen, der als Gegenmaßnahme zu Denial-of-Service Attacken (vgl. 4.2.3) Pflicht ist. Die erste Authentifizierung des Benutzers *MUSS* gegenüber dem Reverse Proxy, anhand eines Client-Zertifikats (vgl. 4.2.3), erfolgen, bevor dieser die Anfrage an den Marktrechner weitergeleitet. Die Kommunikation zwischen Benutzer und Reverse Proxy *SOLL*, laut Maßnahme M11 (vgl. 3.5), ausschließlich über HTTPS, unter Verwendung von TLS 1.2 und Perfekt Forward Security, stattfinden. Über die Anfrage *SOLL* der Benutzer seinen Berechtigungsnachweis an den Marktrechner übermitteln. Kommt die zweite Authentifizierung durch den AAS zu dem Ergebnis "Berechtigungsnachweis gültig", *SOLL* die Anfrage durchgeführt werden. Im umgekehrten Fall "Berechtigungsnachweis ungültig", *MUSS* die Anfrage mit dem HTTP Fehlercode 403 (Verboten wegen mangelnder Berechtigung) beantwortet werden.

5.3 Beurteilung der AAS-Kandidaten

Für die prototypische Implementierung wurden vor Beginn der Thesis zwei Softwareprodukte herausgesucht, die anhand ihrer Beschreibungen zu dem Thesis-Thema gepasst haben. In diesem Abschnitt sollen die beiden Produkte anhand der Anforderungen auf Umsetzbarkeit geprüft werden. Zunächst wird die Middleware CodeMeter der Wibu-Systems AG betrachtet und anschließend der Open-Source RADIUS-Server des FreeRADIUS Projektes.

5.3.1 CodeMeter

CodeMeter ist die Middleware der Wibu-Systems AG, deren Hauptaufgabe der Softwareschutz und das Lizenzmanagement ist. Auf speziell geschützten USB-Sticks, den sogenannten Wibu-Keys, werden daher hauptsächlich Schlüssel für die Softwarelizenzensierung verteilt. Es ist allerdings möglich, beliebige Daten sicher durch die Wibu-Keys zu verteilen, beispielsweise Client-Zertifikate für die Benutzer-Kommunikation. Für WAN-Verbindungen sieht die Entwickler-Dokumentation folgende Architektur vor:

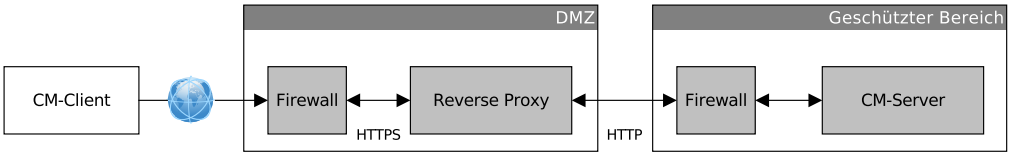

Abbildung 5.1: CodeMeter WAN-Architektur

Über HTTPS stellt ein CodeMeter-Client eine Anfrage. Diese muss von einem Reverse Proxy entgegengenommen werden. Dieser liefert daraufhin ein Server-Zertifikat aus, das der Client überprüft. Optional kann der Reverse Proxy den Kunden durch Benutzername und Passwort authentifizieren. Client-Zertifikate werden zum Zeitpunkt des Schreibens dieser Thesis nicht von der CodeMeter-Software unterstützt. Des Weiteren gehört der Reverse-Proxy sowie die Art und Weise der Benutzerauthentifizierung nicht zum Funktionsumfang der CodeMeter-Software.

5.3.2 FreeRADIUS

RADIUS ist ein Authentifizierungsdienst für sich einwählende Benutzer (engl. Remote Authentication Dial-In User Service). Er besteht aus einem Client-Server-Protokoll zur Authentifizierung, Autorisierung und Buchhaltung (engl. Accounting). Dieses sogenannte Triple-A-System wird hauptsächlich bei VPN, WLAN oder DSL genutzt. Beispielsweise wird das weltweite eduroam-Netzwerk, das Studierenden und Mitarbeitern von Hochschulen erlaubt einen WLAN-Internetzugang an allen Standorten teilnehmender Organisationen anhand ihres eigenen Berechtigungsnachweises zu erhalten. Der Accounting-Aspekt von RADIUS ist nicht Teil dieser Thesis und wird deshalb vernachlässigt. RADIUS selbst besitzt nur eine sehr einfach Konfigurationsdatenbanken zur Authentifizierung, mit welcher keine komplexen Unternehmensstrukturen dargestellt werden können. Aus diesem Grund können moderne RADIUS-Server diese Funktionalität an gängige Authentifizierungsserver, beispielsweise SQL-Datenbanken, Kerberos, LDAPs oder Active Directories, delegieren. Ein RADIUS-Server kann daher als Multiplexer eingesetzt werden, um

verschiedene externe Authentifizierungsserver mit einem Protokoll anzusprechen.

Das RADIUS-Protokoll zur Authentifizierung läuft in zwei Phasen ab (Abbildung 5.2). Zunächst sendet ein RADIUS-Client einen Access-Request, welcher von einem RADIUS-Server entweder mit Access-Accept für eine erfolgreiche Authentifizierung oder Access-Reject für eine fehlerhafte Authentifizierung beantwortet wird. Die dritte Möglichkeit Access-Challange wird für komplexere Authentifizierung genutzt, um zusätzliche Informationen abzufragen, beispielsweise ein zweites Passwort oder einen Token. Für den Rahmen der prototypischen Implementierung wird diese Möglichkeit nicht weiter betrachtet. Alle Attribute einer RADIUS-Nachricht, beispielsweise Benutzer oder Passwort, bestehen aus Attribute-Value-Pairs (AVP). Neben im Protokoll vorgeschriebenen gibt es herstellerspezifische und benutzerdefinierte Attribute. RADIUS-Client und RADIUS-Server verschlüsseln die AVPs anhand eines beider bekannten Geheimnisses.

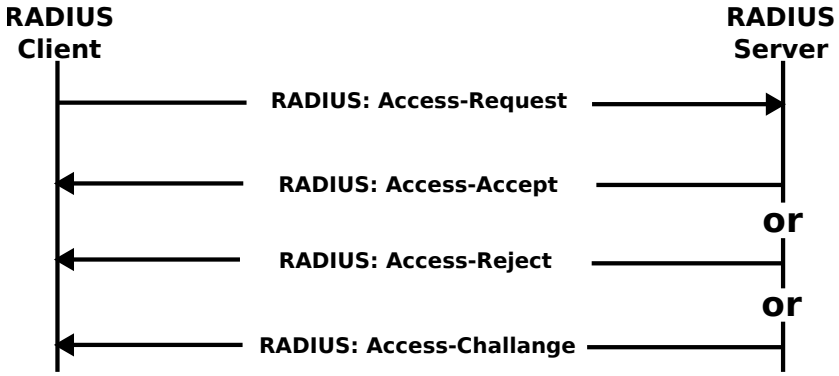

Abbildung 5.2: RADUIS Access-Protokoll

Der FreeRADIUS-Server besitzt zudem eine Richtliniensprache, welche zur Umsetzung einer rollenbasierten Autorisierung genutzt werden kann. Damit ist er in der Lage, Attribute-Value-Pairs auszuwerten und das Ergebnis der Authentifizierung zu manipulieren. Der FreeRadius-Server kann unter Windows, Mac, Linux und BSD Systemen aufgesetzt werden. Die Client-Library kann unter Linux genutzt werden, was für den Einsatz auf dem Marktrechner ausreichend ist.

5.3.3 Schlussfolgerung

CodeMeter Die Wibu-Keys können für die sichere Verteilung der Client-Zertifikate genutzt werden, die für die Benutzer-Kommunikation nötig sind. Die CodeMeter-Software ist allerdings, zum Zeitpunkt des Schreibens dieser Thesis, im Sinne der Aufgabenstellung unbrauchbar, da keine Client-Zertifikate unterstützt werden, was die Anforderung an die Benutzer-Kommunikation verletzt. Ob der Einsatz von Wibu-Keys zur Verteilung von Client-Zertifikaten wirtschaftlich ist, muss gesondert

von der Eckelmann AG evaluiert werden. Für die prototypische Implementierung wird CodeMeter daher nicht eingesetzt.

FreeRADIUS Der Marktrechner ist in der Lage, mit Hilfe der Client-Library den FreeRADUIS-Server zur Authentifizierung und Autorisierung zu kontaktieren. Durch die Multiplexer Funktionalität sind zudem die meisten Authentifizierungsserver abgedeckt, welche eine Fernservice-Zentrale zur Verwaltung ihrer Benutzer nutzen könnte. Die Authentifizierung und Verschlüsselung findet über ein symmetrisches Verfahren auf der Basis eines geteilten Geheimnisses statt, was die Anforderungen zunächst erfüllt, doch aus der Projektdokumentation ist nicht ersichtlich welche Algorithmen dafür verwendet werden. Durch die Multiplexer Funktionalität ist der FreeRADIUS-Server sehr praktikabel, deshalb soll dieser, im Rahmen der prototypischen Implementierung, aufgesetzt werden.

5.4 Prototyp

In diesem Abschnitt wird zunächst das Konzept für die prototypische Implementierung beschrieben. Anschließend werden die beteiligten Komponenten und deren Implementierung beschrieben.

5.4.1 Konzept

Das Konzept der prototypischen Implementierung ist zweigeteilt: Auf der einen Seite die Benutzer-Kommunikation zum Marktrechner hingehend und auf der anderen Seite die Authentifizierung und Autorisierung vom Marktrechner ausgehend. In der Abbildung 5.3 sind alle Komponenten gezeigt.

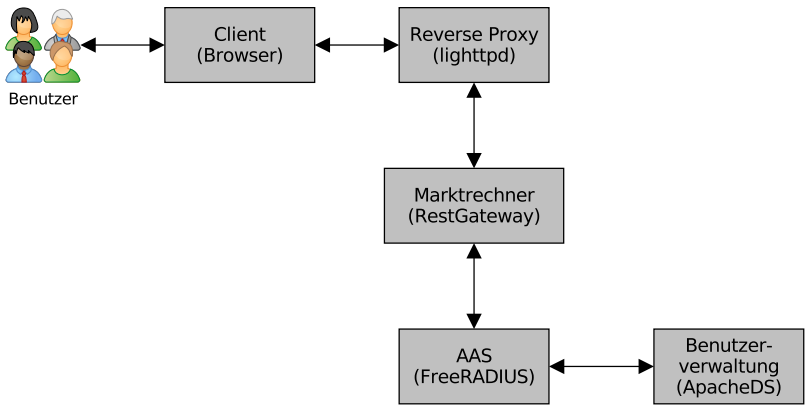

Abbildung 5.3: Konzept prototypische Implementierung

Für die Benutzer-Kommunikation wird als Client der Firefox-Browser eingesetzt. Dieser stellt seine Anfrage gegen den Reverse Proxy, welcher durch einen lighttpd-Webserver realisiert wird. Nach erfolgreicher Zertifikatsprüfung wird eine Anfrage an den Marktrechner weitergeleitet. Das RestGateway-Modul entnimmt Benutzername und Passwort aus den Anfrageparametern. Mit Hilfe der FreeRADIUS-Client-Library sendet das Modul eine Access-Request-Nachricht an den FreeRADIUS-Server. Der RADIUS-Server delegiert die Authentifizierung an den LDAP-Server ApacheDS und führt anschließend eine rollenbasierte Autorisierung durch. Im Erfolgsfall sendet er eine Access-Accept-Nachricht, ansonsten eine Access-Reject-Nachricht. Dementsprechend beantwortet der Marktrechner die Benutzeranfrage mit dem Anfrage-Ergebnis oder dem HTTP-Fehlercode 503 (Forbidden).

5.4.2 Umsetzung

In diesem Abschnitt werden die einzelnen Komponenten aus dem Grobkonzept erklärt und ihre Umsetzung in der prototypischen Implementierung beschrieben.

Reverse Proxy

Der Reverse Proxy ist das Bindeglied zwischen Benutzer und Marktrechner. Zunächst werden die Anforderungen der Verschlüsselung durch TLS 1.2 umgesetzt. Dazu wird ein serverseitiges selbst signiertes X.509-Zertifikat genutzt. Für die folgenden Schritte wird das OpenSSL Kommandozeilen-Tool (openssl) verwendet. Als erstes wird ein Certificate Signing Request (CSR) erzeugt, welcher alle Zertifikatsinformationen inklusive des öffentlichen Schlüssels beinhaltet. Zu diesem öffentlichen wird im selben Schritt auch ein passender privater Schlüssel angelegt. Anschließend wird der CSR zu einem X.509-Zertifikat, indem er mit dem privaten Schlüssel signiert wird. Der private Schlüssel wird nun mit dem Zertifikat zu einer PEM-Datei konkateniert und in der Serverkonfiguration bekannt gemacht. Zusätzlich wird in der Konfiguration die Chiffrenliste angepasst, sodass nur Chiffren erlaubt sind, die Perfekt-Forward-Security nutzen. Außerdem werden die veralteten TLS Versionen SSLv2 und SSLv3 verboten. Da laut Anforderung, nur Anfragen über HTTPS möglich sein sollen, werden die Anfragen, die lediglich das HTTP-Protokoll benutzen nach HTTPS weitergeleitet.

Die Anforderungen legen fest, dass der lighttpd den ersten Teil der Two-Factor-Authentication durchführen muss. Für die Authentifizierung der Benutzer mittels Client-Zertifikaten wird eine Certificate Authority (CA) benötigt. Diese wird im Kontext des lighttpd-Servers angelegt. Für den Client wird nun eine eigener CSR erzeugt. Dieser wird mit dem Zertifikat des Servers und dessen privaten Schlüssel

signiert. Das Ergebnis daraus ist ein X.509-Client-Zertifikat im CRT-Format. Dieses wird für den Import im Browser abschließend in das p12-Format konvertiert. Des Weiteren wird dadurch das Zertifikat durch ein Passwort geschützt, wodurch die Anforderung, Zertifikate nicht unverschlüsselt zu versenden, erfüllt wird.

Benutzer und Client

Die Voraussetzung für eine Kommunikation seitens des Benutzer ist der Besitz des Client-Zertifikates. Über den Versand dieses muss sich für die prototypische Implementierung keine Gedanken gemacht werden, da der Firefox-Browser und der Reverse Proxy auf der selben Maschine laufen. Im Firefox-Browser kann das verschlüsselte p12-Zertifikat durch die Eingabe des Passwortes importiert werden. Über den folgenden Aufruf kann ein Benutzer nun eine Anfrage an den Reverse-Proxy senden.

Auflistung 5.1: HTTPS-Anfrage an Reverse Proxy

```
1 https:// marktrechner.eckelmann.de/rest/1.0/controller?user=ksapp&pass=123456
```

Der Reverse Proxy liefert daraufhin sein selbst signiertes Server-Zertifikat aus und fordert das mit diesem signierte Client-Zertifikat an. Bei der ersten Anfrage wird der Benutzer aufgefordert das relevante Client-Zertifikat auszuwählen. Anschließend geschieht dies vollkommen transparent für den Benutzer. Im Falle einer erfolgreichen Verifizierung des Client-Zertifikates wird die Anfrage an den Marktrechner weitergeleitet. Die Anforderung, mit der Anfrage den Berechtigungsnachweis zu senden, wird über die GET-Parameter *user* und *pass* erfüllt.

Marktrechner

Die Installation der FreeRADIUS-Client-Library ist Vorraussetzung für die Erweiterung des RestGateways. Bei der Installation tritt zunächst das Problem auf, dass auf der Projektwebseite nur der Programmcode der letzten offiziellen Version 1.1.6, welche 2007 veröffentlicht wurde, zu finden ist. Durch gründliches suchen und mit etwas Glück findet man den aktuellen Quellcode auf github. In der Projektgeschichte aus den letzten Jahren ist zu sehen, dass die Client-Library seitdem weiter gepflegt wurde. Der Quellcode lässt sich dank GNU autotools reibungslos kompilieren und installieren. Die Dokumentation ist allerdings sehr spärlich und zudem verstreut. Es ist notwendig, die relevanten Teile aus diversen README-Dateien und Quellcode-Kommentaren zusammenzufügen, bis das Gesamtgefüge einen Sinn ergibt. Zudem sind die API-Zusammenhänge nur mit Hilfe von Beispielcode zu verstehen.

Der erste notwendige Bibliotheksaufruf ist *rc_read_config*. Dieser liest die Konfigurationsdatei ein, welche mit Standardwerten installiert worden ist. In der Konfigurationsdatei müssen zwei Anpassungen getätigt werden. Zum einen muss die IP-Adresse oder Domain des FreeRADIUS-Servers angegeben werden und zum anderen muss das geteilte Geheimnis gesetzt werden. Dieses darf eine Maximallänge von 31-Buchstaben haben. Das in der Konfiguration gesetzte Geheimnis hat die Maximallänge und wurde mit dem Linux-Kommandozeilenprogramm apg generiert. Für die prototypische Implementierung wurde keine sichere Umgebung für die Generierung gewählt, auch die Distributionsmaßnahmen nach 5.23 wurden nicht weiter beachtet. Wurde die Konfiguration erfolgreich geladen, wird über den Aufruf *rc_read_dictionary* das Wörterbuch geladen, das Attributen Datentypen zuordnet. Für die Autorisierung wird der Service, nach welchem die Anfrage verlangt, an den FreeRADIUS-Server übermittelt. Dazu wird das Wörterbuch um das string-Attribut *REST_SERVICE* erweitert. Anschließend können alle nötigen Attribute-Value-Pairs einer Anfrage mit *rc_avpair_add* hinzugefügt werden. Für die Access-Request-Nachricht sind diese:

- Benutzername (USER_NAME),
- Passwort (USER_PASSWORD) und
- RestService (REST_SERVICE)

Abschließend wird über *rc_auth* die Anfrage versendet. Der Rückgabewert 0 zeigt eine erfolgreiche Authentifizierung und Autorisierung an. Die Anfrage wird nun vom RestGateway weiterverarbeitet. Mit dem Rückgabewert 1 wird eine Ablehnung seitens des FreeRADIUS-Servers ausgedrückt und der Rückgabewert 2 sagt aus, dass keine Verbindung zum Server aufgebaut werden konnte. In beiden Fällen wird die Anfrage abgebrochen und mit dem HTTP Fehlercode 403 quittiert.

Die Anforderungen an Logging und Auditing wurden für das RestGateway-Modul nur rudimentär umgesetzt. Anfragen von Benutzern werden mit Benutzername und Zeitstempel sowie dem Authentifizierungsergebnis in eine Datei geschrieben. Dies geschieht mit Qt Standardmechanismen. Für eine Erweiterung die den syslog-ng-Dienst nutzt, war die Zeit zu knapp.

Die hier beschriebene Erweiterung des RestGateway-Moduls konnte leider nicht auf dem Marktrechner getestet werden, da das verwendete Webframework mit der aktuellen ARM-Toolchain von ptxdist (vgl. 2.1.2) nicht kompilierbar ist. Aus diesem Grund wurden das RestGateway von extern, auf einer Ubuntu 12.04 Installation, gegen das LanGateway des Marktrechners eingesetzt (vgl. 2.1.3), um authentifizierte Anfragen durchzuführen.

Benutzerverwaltung

Zur Benutzerauthentifizierung wird eine externe Benutzerverwaltung benötigt. Dazu wurde exemplarisch ApacheDS gewählt, welches das Lightweight Directory Access Protocol (LDAP) unterstützt. Die Wahl einer Benutzerverwaltungen mit LDAP Unterstützung wurde getroffen, weil dieses in den meisten Unternehmensbenutzerverwaltungen verfügbar ist. LDAP legt Daten in einer Baumstruktur ab. Für eine Benutzerverwaltung gibt es jedoch keine Vorgaben, wie die Baumstruktur anzulegen ist. Jeder Knoten kann von beliebig vielen Objekt-Klassen erben. Anhand der Objekt-Klassen sind Attribute verfügbar, die teilweise verpflichtend sind. In Abbildung 5.4 ist die Struktur dargestellt, die für die prototypische Implementierung gewählt wurde. Vom root-Knoten, mit den Domain Components *dc=eckelmann,dc=de*, ausgehend, wurden drei Kinderknoten, die von der Objekt-Klasse *organizationalUnit* erben, erzeugt. Diese Objekt-Klasse verpflichtet zur Angabe des Namens der Unternehmenseinheit (*ou*). Zunächst wurde die Abteilung *kgl* gewählt, welche die Untereinheiten *users* und *admins* hat. Diese Untereinheiten beinhalten jeweils Benutzerknoten.

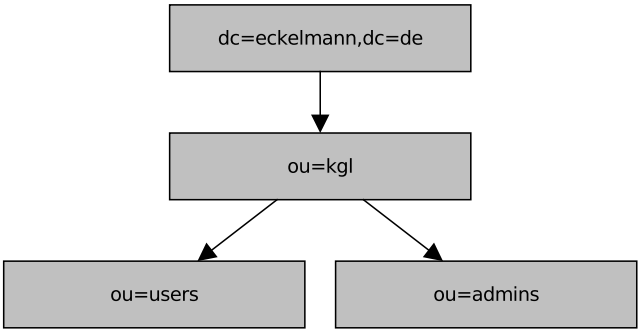

Abbildung 5.4: LDAP Struktur

Der Benutzerknoten, in Auflistung 5.2 im LDIF-Format dargestellt, erbt von zwei Objekt-Klassen. Der Distinguished Name (*dn*) erlaubt es, einen Knoten eindeutig im Baum zu finden. Über die Objekt-Klasse *person* wird verpflichtend das Attribut Common-Name (*cn*) verfügbar sowie weitere optionale Attribute für Vorname, Nachname, Benutzername und Passwort. Der Benutzername wird über *uid* angegeben und spielt eine wichtige Rolle für die FreeRADIUS-Konfiguration. Die Objekt-Klasse *radiusProfile* ermöglicht das Hinzufügen von Rollen, die der FreeRADIUS-Server als *radiusGroupName*-Attribute kennt und auslesen kann.

Auflistung 5.2: Benutzerbeschreibung im LDIF-Format

```
1 dn: cn=Kevin Sapper,ou=users,ou=kgl,dc=eckelmann,dc=de
2 objectClass: top
```

```
3  objectClass: radiusProfile
4  objectClass: person
5  cn: Kevin Sapper
6  givenName: Kevin
7  sn: Sapper
8  uid: ksapp
9  userPassword:: e3NoYX1mRXFOQ2NvM1lxOWg1WlVnbEQzQ1pKVDRsQnM9
10 radiusGroupName: analyst
11 radiusGroupName: fernservice
```

In der Praxis wird statt *person* oft die Objekt-Klasse *inetOrgPerson* gewählt, da diese es ermöglicht deutlich detaillierte Informationen über einen Nutzer zu erfassen. Alternativ werden die beide Klassen gerne auch kombiniert. Der komplette Inhalt des LDAP-Servers, im LDIF-Format, ist im Anhang A.2 zu finden.

AAS

Die Installation des FreeRADIUS-Server auf einem Ubuntu System erfolgt ganz einfach über das Paketverwaltungssystem APT. Alternativ ist die Installation über die Quellen ohne Probleme zu bewerkstelligen. Die FreeRADIUS-Dokumentation führt den Benutzer Schritt für Schritt, mit ausführlichen Erklärungen, durch diesen Prozess. Die Basiskonfiguration des Servers wird in der Dokumentation sehr gut erläutert. Zunächst erfolgt die Einrichtung der Clients. Bevor ein Marktrechner eine Anfrage an den FreeRADIUS-Server stellen kann, muss dieser als Client konfiguriert werden. Clients werden anhand einer IP-Adresse oder Domain unterschieden und bekommen ein Geheimnis zugeordnet. Im Fall der prototypischen Implementierung wird das Geheimnis genutzt, welches über apg bei der Client-Library Konfiguration generiert wurde. Dieses Geheimnis wird (laut Projekt-Wiki [6]) genutzt, um die übertragenen Attribute einer Anfrage zwischen Server und Client zu verschlüsseln.

So gut wie die Basiskonfiguration beschrieben ist, so sehr fehlen nötige Beschreibungen bei den Modulkonfigurationen, darunter auch beim LDAP-Modul. Beispielsweise ist die Funktionalität zum Auslesen der LDAP-Gruppen nur sehr vage gehalten. Bei der LDAP-Konfiguration werden zunächst die Verbindungsdaten des LDAP-Server eingetragen. Dies geschieht über die Angabe der IP-Adresse und des TCP-Ports. Diese Verbindung ist ohne weitere Konfiguration komplett unverschlüsselt. Mittels der STARTTLS Funktionalität, wie sie auch bei E-Mail Servern und Clients genutzt wird, kann die Verbindung verschlüsselt werden. Falls diese Verschlüsselung nicht ausreichend ist, können zusätzlich Client-Zertifikate zur Authentifizierung des LDAP-Servers eingesetzt werden, wie dies bei der Benutzer-

kommunikation der Fall ist. Für die prototypische Implementierung soll STARTTLS genügen. Für die Benutzerauthentifizierung wird sich der FreeRADIUS-Server beim LDAP-Server einloggen. Dazu nutzt er den Berechtigungsnachweis eines Benutzers der Unternehmenseinheit *admins*. Über das *identity*-Attribute wird dieser Benutzer angegeben. Für die prototypische Implementierung wurde hierzu der Benutzer *cn=binduser* angelegt. Damit die Admin-Benutzer nicht für die allgemeine Authentifizierung genutzt werden können, wird die Unternehmenseinheit *users* als Basisknoten für die Benutzersuche eingetragen. Valide Benutzerknoten erben von der *radiusprofile* Objekt-Klasse und besitzen das *uid*-Attribute für den Benutzernamen. Findet der FreeRADIUS-Server einen übereinstimmenden Benutzernamen, liest er dessen Passwort aus und vergleicht es mit dem übermittelten. Ist dies erfolgreich, markiert der FreeRADIUS-Server den Access-Request mit *accept* und liest die Rollen des Benutzers über das *radiusGroupName*-Attribute aus.

Um die rollenbasierte Authentifizierung durchführen zu können, muss zusätzlich das Wörterbuch des FreeRADIUS-Server um das *REST_SERVICE*-Attribut erweitert werden, wie es auch bei der Client-Library geschehen ist. In einer Richtliniendatei kann der FreeRADIUS-Server anhand des übermittelten *REST_SERVICE*-Attributes nachschauen, ob der Benutzer die erforderliche Rolle, zum Aufruf dieses Services, besitzt. Ist dies nicht der Fall, manipuliert der RADIUS-Server das Authentifizierungsergebnis auf *reject*. Auflistung 5.3 zeigt einen Auszug der Richtlinien für die Autorisierung. Hier für den Service *controller*, der die Gruppen *hersteller* und *fernservice* erlaubt. Alle anderen werden abgelehnt.

Auflistung 5.3: Richtlinie für den controller-Service

```
1 if ("%{request:rest_service}" == "controller ") {
2     if (Ldap-Group == "hersteller" || Ldap-Group == "fernservice") {
3         noop
4     }
5     else {
6         reject
7     }
8 }
```

Neben den funktionalen Anforderungen muss der FreeRADIUS-Server auch die Anforderungen an den Log- und Audit-Mechanismus erfüllen. Zum Zweck der Nachvollziehbarkeit werden Access-Request-Nachrichten mit Benutzername, IP-Adresse, Zeitstempel und Authentifizierungsergebnis protokolliert. Dazu wird der syslog-ng-Dienst genutzt, um die Daten in einer MongoDB abzulegen. Zum Betrachten der Daten wird das Web-Tool syslogng-web genutzt. Dieses Tool ermöglicht jedoch uneingeschränkt die Daten zu Betrachten, wodurch die Anforderung an

Vertraulichkeit verletzt wird. Alle Daten und Prozesse sind einem speziellen Systembenutzer zugeordnet, sodass zumindest die Protokolle nicht unerlaubt manipuliert werden können. Die Anforderungen an ein Frühwarnsystem wurden aufgrund fehlender Systemtools nicht umgesetzt.

Wisdom consists in being able to
distinguish among dangers and
make a choice of the least harmful.
Niccolo Machiavelli, The Prince

Kapitel 6

Evaluation

In diesem Kapitel soll herausgefunden werden, ob der FreeRADIUS-Server für die Authentifizierung und Autorisierung von Fernzugriffen auf eine Automatisierungsanlage geeignet ist. Dazu werden die Aspekte Installation & Dokumentation, Sicherheit und Wartung betrachtet.

6.1 Installation & Dokumentation

Die Installation des FreeRADIUS-Server geht sehr einfach von statten. Auch die Basiskonfiguration ist ohne Probleme zu bewältigen. Je mehr man jedoch ins Detail geht, desto spärlicher werden die Informationen. Durch die große Verbreitung des FreeRADIUS Projektes, lassen sich die Informationen mehr oder weniger leicht aus verschiedenen Internetquellen zusammensuchen. Zudem besteht die Möglichkeit, sich Support von der Firma Network RADIUS SARL zu kaufen, welche die Entwicklung des Projektes vorantreibt. Diese bietet Supportleistungen, in unterschiedlichen Umfängen, ab 2000 € bis 5000 € pro Jahr an. Die Literatur über den FreeRADIUS-Server ist mit zwei Büchern überschaubar. Das Buch FreeRADIUS for Beginner's war bei der Konfiguration des LDAP-Moduls unerlässlich und behandelt alle Bereiche der FreeRADIUS-Server Konfiguration zumindest oberflächlich [1].

Die Client-Library ist zwar einfach zu installieren, allerdings erfordert die Konfiguration und Nutzung erfahrene C-Entwickler, die die Zusammenhänge aus dem Quellcode herauslesen können.

6.2 Sicherheit

Die Authentifizierung und Autorisierung von Fernzugriffen durch den Marktrechner sollte in zwei getrennten Problemstellungen betrachtet werden. Die Benutzer-Kommunikation zum Marktrechner und die M2M-Kommunikation mit dem AAS.

Der Funktionsumfang der M2M-Kommunikation zwischen Marktrechner und FreeRADIUS-Server hat sich in der prototypischen Implementierung als äußerst komfortabel erwiesen. Durch die Möglichkeit zur Anbindung externer Benutzerverwaltungen stellt der FreeRADIUS-Server eine praktikable Lösung als Multiplexer für die meisten Kunden dar. Die Anbindung eines LDAP-Servers kann hierbei durch Client-Zertifikate auf dem gleichen Niveau abgesichert werden, wie dies bei der Benutzer-Kommunikation der Fall ist. Für die Evaluierung der Sicherheit der M2M-Verbindung wurde der Datenverkehr zwischen FreeRADIUS-Client und FreeRADIUS-Server mit dem wireshark Netzwerkprotokoll-Analysierprogramm untersucht. In Abbildung 6.1 ist der Inhalt einer RADIUS Access-Request-Nachricht von wireshark dargestellt.

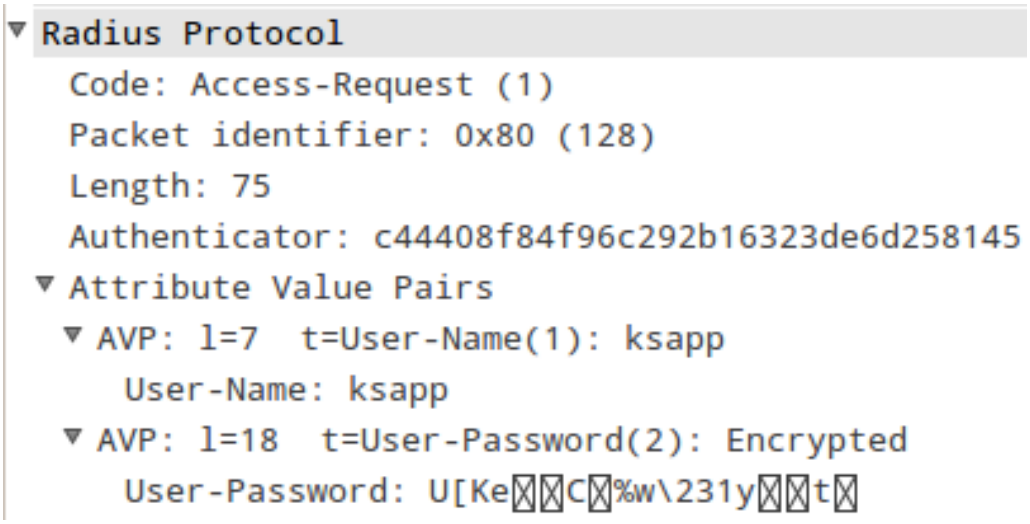

Abbildung 6.1: RADIUS Access-Request in wireshark

Dort ist zusehen, dass außer dem Wert des Benutzerpasswortes nichts verschlüsselt wird. Ein Angreifer kann also ohne Hindernisse die Metadaten der Nachricht mitlesen. Die Sicherheit des verschlüsselten Passwortes hängt zudem von einem gut gewählten Geheimnis ab. Des Weiteren geht weder aus der Dokumentation noch aus einer sonstigen Quelle hervor, wie das Passwort mit dem Geheimnis verschlüsselt wird. Diese Methode wird in der Kryptographie auch obfuscation genannt, also Verschleierung, und unterliegt der Sicherheitsannahme, dass niemand weiß wie die Kryptographie funktioniert. Dieses Vorgehen ist hochgradig riskant, weshalb

der FreeRADIUS-Server ohne zusätzliche Vorkehrungen niemals über das Internet Anfragen entgegennehmen sollte. Der Wunsch den AAS auch über das Internet erreichbar zu machen, könnte beispielsweise unter der Nutzung eines SSH-Tunnels realisiert werden.

Die LDAP-Anbindung über STARTTLS oder Client-Zertifikate ist gegenüber der FreeRADIUS-Client/Server Anbindung komplett verschlüsselt. Dadurch ist das Risiko ein LDAP über eine Internetverbindung anzubinden durchaus überschaubar. Hierbei sind Client-Zertifikate der STARTTLS Funktionalität vorzuziehen, da diese das Risiko einer MITM-Attacke deutlich senken. Im Unternehmensnetzwerk muss die Fernservice-Zentrale entscheiden, welche Lösung bevorzugt wird.

Die Benutzer-Kommunikation hat laut der Eckelmann AG die Anforderung, über das Internet auf den Marktrechner zugreifen zu können. Diese Anforderung wird in der prototypischen Implementierung erfüllt, denn die Anforderungen an die Benutzer-Kommunikation wurden alle ohne Kompromisse erfüllt. Dadurch ist das Risiko der Gefährdungen auf dem Kommunikationsweg in einen vertretbaren Rahmen gepackt worden.

Das größte bestehende Problem ist die Verteilung von Zertifikaten, Schlüsseln und Geheimnissen. Alle Umsetzungen in der prototypischen Implementierung wählen das "Schlüssel fallen vom Himmel"-Modell und kümmern sich nicht weiter um deren Distribution. Der Versand auf einem Datenträger ist dabei eine gute und sichere Möglichkeit, welche durch die Maßnahme 5.23 des BSI ausführlich erläutert wurde. Von anderen Arten der Distribution, etwa E-Mail, sollte abgesehen werden, da diese nicht das nötige Vertrauensniveau schaffen können. Ein weiteres Problem ist die nicht Existenz eines Früherkennungssystem für den Logging- und Auditing-Mechanismus. Da die Daten bereits in einer Datenbank vorliegen muss noch ein Tool gefunden werden, dass diese in Echtzeit auswerten kann. Des Weiteren benötigt das RestGateway eine Erweiterung, um mit syslog-ng zu interagieren und der Betrachter für die Protokolledaten, darf diese nicht allen Nutzern zugänglich machen.

6.3 Wartung

Die Wartung der Fernservice-Benutzer über die firmeneigene Benutzerverwaltung sollte jeder Administrator begrüßen, da er dadurch nicht mit der Aufgabe konfrontiert wird, Redundanzen pflegen zu müssen. Deutlichen Aufwand hingegen bedeutet die Installation der Client-Zertifikate auf den Benutzersystemen. Neben der Installation müssen diese auch regelmäßig, etwa alle zwei Jahre, erneuert werden, da diese ein Ablaufdatum besitzen. Dieser Aufwand bedeutet allerdings gleichzeitig eine deutliche Reduzierung des Angriffsrisikos, was durchaus in einem fairen Ver-

hältnis zu den daraus entstehenden Kosten liegt. Das gleiche gilt beim Einsatz von Client-Zertifikaten bei LDAP-Servern. STARTTLS ist zwar in der Wartung einfacher, kann jedoch keine Authentifizierung des LDAP-Servers durchführen.

Die Wartung der Geheimnisse zwischen FreeRADIUS-Client und FreeRADIUS-Server ist dagegen eine kleine Katastrophe. Obwohl diese Geheimnisse kein Ablaufdatum, wie die Zertifikate, besitzen, ist es durchaus sinnvoll diese in bestimmten Intervallen zu wechseln. Dies darf nicht über einen unsicheren Kommunikationskanal, beispielsweise das Internet, erfolgen. Da die meisten Anlagen mehrfach im Jahr gewartet werden, könnte hierbei ein neues Geheimnis aufgespielt werden, welches der Service-Monteur zuvor von der Firmenzentrale erhalten hat. Ist der Austauschmechanismus einfach zu handhaben sind die dadurch anfallenden Kosten überschaubar. Trotzdem besteht hier das Risiko einer totalen Komprimierung aller Marktrechner, beispielsweise durch einen Softwarefehler im Marktrechner oder in der FreeRADIUS-Server Implementierung. Wenn zu einem Zeitpunkt alle Geheimnisse ausgetauscht werden müssen, ist dies zum einen extrem teuer und zum anderen über einen kurzen Zeitraum nicht zu bewältigen, da es deutlich mehr Marktrechner als Service-Monteure gibt. Wurden VLAN- oder SSH-Vorkehrungen getroffen, ist das Risiko durch eine solche Komprimierung, nicht in einen kritischen Zustand zu verfallen, überschaubar.

Kapitel 7

Zusammenfassung

Im Rahmen dieser Thesis sollte ein Entwurf eines Sicherheitskonzeptes zur Authentifizierung und Autorisierung von Fernzugriffen erstellt werden. Dabei wurde die Steuerungstechnik für Kälteanlagen der Eckelmann AG und deren Anbindung an Fernservice-Zentralen betrachtet. Durch die Industrie 4.0 Bewegung wurde angeregt, Daten auch in Unternehmensnetzwerken nicht mehr unverschlüsselt zu übertragen. Des Weiteren sollte es möglich werden, Systeminteraktionen der Mitarbeiter nachzuvollziehen. Zudem sollte die Flexibilität der Infrastruktur erweitert werden, um dem Hersteller vereinfachten Support zu ermöglichen. Denn zur Zeit müssen sich zunächst zwei IT-Abteilung zusammensetzten und eine VPN-Verbindung zwischen den Unternehmensnetzen einrchten, was in den meisten Fällen zu viel Zeit in Anspruch nimmt. Ein Wunsch an die Authentifizierung war es, dem Benutzer, unabhängig von seinem Standort, einen möglichst komfortablen Login zu ermöglichen.

Durch die Bedrohungsanalysen in den Kapiteln 3 und 4 wurden viele Gefährdungen des aktuellen Systems und des Konzeptes für die prototypische Implementierung gefunden. Einen starken Einfluss hierauf hatten die Sicherheitskataloge des Bundesamtes für Sicherheit in der Informationstechnik. Durch die Kataloge konnte auf eine breite Basis von möglichen Gefährdungen zurückgegriffen werden. Anhand der gefundenen Gefährdungen wurden viele Maßnahmen formuliert, die in die Anforderungen der prototypischen Implementierung eingeflossen sind. Für den Benutzerlogin wurde eine Two-Factor-Authentication etabliert. Die erste Authentifizierung findet durch Client-Zertifikate statt, wodurch diese für den Benutzer fast transparent abläuft. Gleichzeitig wird möglichen Angreifern dadurch ein großes Hindernis in den Weg gestellt. Der Einsatz eines Reverse Proxy Servers verhindert zudem, dass DoS-Attacken die Steuerungstechnik der Kälteanlage überlasten können. Für die zweite Authentifizierung des Benutzers werden dessen Benutzername

und Passwort benötigt. Diese Daten liegen bereits in den Benutzerverwaltungen der Fernservice-Zentralen vor, deshalb wurde mit dem FreeRADIUS-Server ein Authentifizierungsserver aufgesetzt, der als Multiplexer für alle gängigen Benutzerverwaltungen eingesetzt werden kann.

Einige Probleme hat die prototypische Implementierung dennoch aufzuweisen. Die Kommunikation zum FreeRADIUS-Server, durch die Client-Bibliothek des FreeRADIUS Projektes, verschlüsselt, trotz eines geteilten Geheimnisses, die Kommunikationsdaten nur unzureichend. Weitere Probleme liegen gibt es bei der Nachvollziehbarkeit, durch eine unvollständige Umsetzung der Protokollierung von Benutzerinteraktionen. Des Weiteren konnte die Anforderung an ein Frühwarnsystem nicht umgesetzt werden. Eine große Lücke klafft zudem in der Distribution von Schlüsseln, Geheimnissen und Zertifikaten, welche für die Kommunikation der Komponenten untereinander benötigt werden.

Sollte in Betracht gezogen werden das Konzept der prototypische Implementierung in einer produktiven Umgebung umzusetzen, müssen vorher die bestehenden Probleme gelöst werden. Für die Kommunikation zum FreeRADIUS-Server ist eine einfache Lösung die Einrichtung eines SSH-Tunnels. Die Protokollierung muss auf allen Komponenten anhand der gegeben Anforderungen umgesetzt werden und zudem muss ein Frühwarnsystem gefunden werden, das die Daten der Protokollierung in Echtzeit auswerten kann. Für die Distribution der Schlüssel, Geheimnisse und Zertifikate müssen, in Zusammenarbeit mit den Fernservice-Zentralen, Prozesse definiert werden, die einen sicheren Austausch ermöglichen.

Der Umfang der Bachelorarbeit hat es lediglich ermöglicht einen Entwurf eines Sicherheitskonzept zu erstellen, der als Orientierungshilfe dienen kann. Viele Aspekte, wie etwa die IT-Infrastruktur, Datensicherung, höhere Gewalt und Notfallversorgung wurden nur unzureichend oder überhaupt nicht betrachtet. Dazu wurde mehrfach das menschliche Versagen als Gefährdungsgrund vernachlässigt. Ein ganzheitliches Sicherheitskonzepts muss alle Aspekte berücksichtigen und ein höheres Maß an Detailreichtum bieten. In Anbetracht der angewandten Zeit und des daraus resultierenden Ergebnisses, scheint es nicht wirtschaftlich die eigenen Mitarbeiter auf diese Thematik anzusetzen, da diese durch die Aufgabe mindesten ein halbes Jahr an eine Tätigkeit gebunden werden, die in erster Linie keinen Profit erwirtschaftet. Abschließend muss bedacht werden, dass Sicherheit zwangsläufig einen Mehraufwand bedeutet, der durch Mehrkosten abgedeckt werden muss.

Kapitel 8

Literaturverzeichnis

Literaturquellen

[1] Dirk van der Walt. FreeRADIUS Beginner's Guide. Packt Publishing, Birmingham B2 2PB, UK, 2011.

Online-Quellen

[2] Asymetrische, kryptographie - wikipedia. http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem. [letzter Zugriff: 26.08.14].

[3] Eckelmann: Produkte für das steuern und regeln von kälteanlagen. http://www.eckelmann.de/produkte-loesungen/kaeltetechnik/elds-produkte. [letzter Zugriff: 17.Jul.2014].

[4] It-grundschutz - wikipedia. http://de.wikipedia.org/wiki/IT-Grundschutz. [letzter Zugriff: 26.08.14].

[5] Representational state transfer - wikipedia. http://de.wikipedia.org/wiki/Representational_State_Transfer. [letzter Zugriff: 08.Aug.2014].

[6] Wiki freeradius. http://wiki.freeradius.org. [letzter Zugriff: 10.Okt.2014].

[7] S. Bradner. Key words for use in rfcs to indicate requirement levels. http://www.rfc-base.org/txt/rfc-2119.txt. [letzter Zugriff: 09.Sep.2014].

[8] Peter Checkland. Systems explained by peter checkland. http://www.open.edu/openlearn/money-management/management/leadership-and-

management/managing/systems-explained-peter-checkland. [letzter Zugriff: 22.Jul.2014].

[9] Liang Chen. Authentifizieren und vertrauen schaffen. http://www.ipd.uni-karlsruhe.de/~damast/seminar/FAS2007/pdfs/FAS2007_Chen_Authentifizierung_Ausarbeitung.pdf. [letzter Zugriff: 18.Aug.2014].

[10] Bundesamt für Sicherheit in der Informationstechnik. B 1.7 kryptokonzept. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01007.html. [letzter Zugriff: 22.Sep.2014].

[11] Bundesamt für Sicherheit in der Informationstechnik. B 5.21 webanwendungen. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05021.html. [letzter Zugriff: 16.Sep.2014].

[12] Bundesamt für Sicherheit in der Informationstechnik. B 5.22 protokollierung. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05022.html. [letzter Zugriff: 16.Sep.2014].

[13] Bundesamt für Sicherheit in der Informationstechnik. B 5.4 webserver. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05004.html. [letzter Zugriff: 16.Sep.2014].

[14] Bundesamt für Sicherheit in der Informationstechnik. Bsi-standard 100-1: Managementsysteme für informationssicherheit (isms). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile. [letzter Zugriff: 28.Jul.2014].

[15] Bundesamt für Sicherheit in der Informationstechnik. Bsi-standard 100-2: It-grundschutz-vorgehensweise. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile. [letzter Zugriff: 28.Jul.2014].

[16] Bundesamt für Sicherheit in der Informationstechnik. Bsi-standard 100-3: Risikoanalyse auf der basis von it-grundschutz. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/

ITGrundschutzstandards/standard_1003_pdf.pdf?__blob=publicationFile. [letzter Zugriff: 28.Jul.2014].

[17] Bundesamt für Sicherheit in der Informationstechnik. Bsi-standard 100-4: Notfallmanagement. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile. [letzter Zugriff: 28.Jul.2014].

[18] Bundesamt für Sicherheit in der Informationstechnik. Das ism des bsi, it-grundschutz. https://www.bsi.bund.de/SharedDocs/Bilder/DE/BSI/Themen/grundschutzdeutsch/Webkurs/pic2 [letzter Zugriff: 22.Jul.2014].

[19] Bundesamt für Sicherheit in der Informationstechnik. G 2.160 fehlende oder unzureichende protokollierung. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02160.html. [letzter Zugriff: 02.Sep.2014].

[20] Bundesamt für Sicherheit in der Informationstechnik. G 2.161 vertraulichkeits- und integritätsverlust von protokolldaten. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02161.html. [letzter Zugriff: 02.Sep.2014].

[21] Bundesamt für Sicherheit in der Informationstechnik. G 2.19 unzureichendes schlüsselmanagement bei verschlüsselung. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02019.html. [letzter Zugriff: 22.Sep.2014].

[22] Bundesamt für Sicherheit in der Informationstechnik. G 2.22 fehlende oder unzureichende auswertung von protokolldaten. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02022.html. [letzter Zugriff: 02.Sep.2014].

[23] Bundesamt für Sicherheit in der Informationstechnik. G 2.67 ungeeignete verwaltung von zugangs- und zugriffsrechten. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g02/g02067.html. [letzter Zugriff: 02.Sep.2014].

[24] Bundesamt für Sicherheit in der Informationstechnik. G 4.33 schlechte oder fehlende authentikation. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g04/g04033.html. [letzter Zugriff: 01.Sep.2014].

[25] Bundesamt für Sicherheit in der Informationstechnik. G 4.35 unsichere kryptographische algorithmen. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g04/g04035.html. [letzter Zugriff: 22.Sep.2014].

[26] Bundesamt für Sicherheit in der Informationstechnik. G 4.89 fehlendes oder unzureichendes alarmierungskonzept bei der protokollierung. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g04/g04089.html. [letzter Zugriff: 02.Sep.2014].

[27] Bundesamt für Sicherheit in der Informationstechnik. G 5.151 dns-flooding - denial-of-service. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05151.html. [letzter Zugriff: 03.Sep.2014].

[28] Bundesamt für Sicherheit in der Informationstechnik. G 5.157 phishing und pharming. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05157.html. [letzter Zugriff: 03.Sep.2014].

[29] Bundesamt für Sicherheit in der Informationstechnik. G 5.18 systematisches ausprobieren von passwörtern. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05018.html. [letzter Zugriff: 02.Sep.2014].

[30] Bundesamt für Sicherheit in der Informationstechnik. G 5.19 missbrauch von benutzerrechten. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05019.html. [letzter Zugriff: 02.Sep.2014].

[31] Bundesamt für Sicherheit in der Informationstechnik. G 5.2 manipulation an informationen oder software. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05002.html. [letzter Zugriff: 19.Sep.2014].

[32] Bundesamt für Sicherheit in der Informationstechnik. G 5.24 wiedereinspielen von nachrichten. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05024.html. [letzter Zugriff: 03.Sep.2014].

[33] Bundesamt für Sicherheit in der Informationstechnik. G 5.42 social engineering. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/

ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html. [letzter Zugriff: 03.Sep.2014].

[34] Bundesamt für Sicherheit in der Informationstechnik. G 5.48 ip-spoofing. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05048.html. [letzter Zugriff: 03.Sep.2014].

[35] Bundesamt für Sicherheit in der Informationstechnik. G 5.78 dns-spoofing. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05078.html. [letzter Zugriff: 03.Sep.2014].

[36] Bundesamt für Sicherheit in der Informationstechnik. G 5.83 kompromittierung kryptographischer schlüssel. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05083.html. [letzter Zugriff: 01.Sep.2014].

[37] Bundesamt für Sicherheit in der Informationstechnik. G 5.84 gefälschte zertifikate. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05084.html. [letzter Zugriff: 22.Sep.2014].

[38] Bundesamt für Sicherheit in der Informationstechnik. M 2.11 regelung des passwortgebrauchs. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html. [letzter Zugriff: 01.Sep.2014].

[39] Bundesamt für Sicherheit in der Informationstechnik. M 2.110 datenschutzaspekte bei der protokollierung. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02110.html. [letzter Zugriff: 01.Sep.2014].

[40] Bundesamt für Sicherheit in der Informationstechnik. M 2.164 auswahl eines geeigneten kryptographischen verfahrens. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02164.html. [letzter Zugriff: 22.Sep.2014].

[41] Bundesamt für Sicherheit in der Informationstechnik. M 2.33 aufteilung der administrationstätigkeiten unter unix. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02033.html. [letzter Zugriff: 19.Sep.2014].

[42] Bundesamt für Sicherheit in der Informationstechnik. M 2.499 planung der protokollierung. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02499.html. [letzter Zugriff: 02.Sep.2014].

[43] Bundesamt für Sicherheit in der Informationstechnik. M 2.7 vergabe von zugangsberechtigungen. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02007.html. [letzter Zugriff: 01.Sep.2014].

[44] Bundesamt für Sicherheit in der Informationstechnik. M 3.10 auswahl eines vertrauenswürdigen administrators und vertreters. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03010.html. [letzter Zugriff: 04.Sep.2014].

[45] Bundesamt für Sicherheit in der Informationstechnik. M 4.25 einsatz der protokollierung im unix-system. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04025.html. [letzter Zugriff: 19.Sep.2014].

[46] Bundesamt für Sicherheit in der Informationstechnik. M 5.23 auswahl einer geeigneten versandart für datenträger. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05023.html. [letzter Zugriff: 08.Sep.2014].

[47] Bundesamt für Sicherheit in der Informationstechnik. M 5.59 schutz vor dns-spoofing bei authentisierungsmechanismen. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05059.html. [letzter Zugriff: 02.Sep.2014].

[48] Bundesamt für Sicherheit in der Informationstechnik. M 5.66 verwendung von tls/ssl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05066.html. [letzter Zugriff: 01.Sep.2014].

[49] Bundesamt für Sicherheit in der Informationstechnik. The pp/st guide. [letzter Zugriff: 28.Aug.2014].

[50] Peter Gutmann. Engineering security. https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf. [letzter Zugriff: 10.Jul.2014].

[51] Peter Gutmann. Key management through key continuity (kcm). https://tools.ietf.org/id/draft-gutmann-keycont-01.txt. [letzter Zugriff: 22.Sep.2014].

[52] Till Hoppe-Handelsblatt. It-sicherheitsbehörde in finanznot. http://www.handelsblatt.com/politik/deutschland/bsi-it-sicherheitsbehoerde-in-finanznot/10286414.html. [letzter Zugriff: 29.Aug.2014].

[53] Common Criteria Recognition Arrangement Members. Common criteria for information technology security evaluation - part 1: Introduction and general model. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf. [letzter Zugriff: 28.08.14].

[54] Common Criteria Recognition Arrangement Members. Common criteria for information technology security evaluation - part 2: Security functional requirements. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf. [letzter Zugriff: 28.08.14].

[55] Common Criteria Recognition Arrangement Members. Common criteria for information technology security evaluation - part 3: Security assurance requirements. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf. [letzter Zugriff: 28.08.14].

[56] Markus Reppner. Bsi-grundschutz: zu komplex, zu aufwändig, zu deutsch. http://www.zdnet.de/41525300/bsi-grundschutz-zu-komplex-zu-aufwaendig-zu-deutsch/3/. [letzter Zugriff: 29.Aug.2014].

[57] Achim Sawall. Netzwerktechniker legt it von Ölfirma lahm - vier jahre haft. http://www.golem.de/news/it-sabotage-netzwerktechniker-legt-it-von-oelfirma-lahm-vier-jahr-haft-1405-106695.html. [letzter Zugriff: 02.Sep.2014].

[58] Remy van Elst. Stong ssl security on lighttpd. https://raymii.org/s/tutorials/Strong_SSL_Security_On_lighttpd.html. [letzter Zugriff: 01.Sep.2014].

[59] Peter Weeks. Soft systems methodologie (checkland). http://www.12manage.com/methods_checkland_soft_systems_methodology_de.html. [letzter Zugriff: 22.Jul.2014].

[60] Wikipedia. Cyberkrieg. http://de.wikipedia.org/wiki/Cyberkrieg. [letzter Zugriff: 16.09.14].

[61] Wikipedia. Stuxnet. http://de.wikipedia.org/wiki/Stuxnet. [letzter Zugriff: 16.09.14].

[62] Bob Williams. Soft systems methodology. http://users.actrix.co.nz/bobwill/ssm.pdf. [letzter Zugriff: 22.Jul.2014].

Anhang A

Ergänzendes Material

A.1 Anforderungscheckliste

Auflistung aller Anforderungen und deren Ergebnisse aus der prototypischen Implementierung.

A.1.1 Logging & Audit

- □ Jegliche Aktivität von Kunden, Inhabern und Akteuren, die einen Zugriff auf den Marktrechner zur Folge hat, muss zum Zweck der Nachvollziehbarkeit protokolliert werden.
- □ Jegliche unerlaubte Aktivitäten müssen durch ein Frühwarnsystem erkannt werden.
- □ Logging und Audit Betrachter müssen die Daten durch einen Sanitizer reinigen lassen.
- □ Angreifer (Inhaber) und unbefugte Kunden sollen die Protokollierung nicht einsehen können.

A.1.2 M2M-Kommunikation

- □ Die Authentifizierung zwischen Marktrechner und AAS soll über ein Public/Private-Key Verfahren erfolgen.
- □ Die Identität des Gegenüber muss durch einen zweiten Kommunikationskanal bestätigt werden.

- ☒ Der AAS (Akteur) soll dem Marktrechner die Rolle(n) des zu authentifizierten Kunden verifizieren, falls diese gesendet werden.
- ☒ Der AAS (Akteur) soll dem Marktrechner die Rolle(n) des zu authentifizierten Kunden mitteilen, falls diese nicht gesendet wurden.
- □ Das Verschlüsselungsverfahren muss Perfekt Forward Security (PFS) einsetzen.
- □ Die Verschlüsselung soll unabhängig von der Authentifizierungsmethode asynchron sein.

A.1.3 Benutzer-Kommunikation

- ☒ Der Reverse Proxy darf Anfragen von Kunden nur an den Marktrechner weiterleiten, wenn dessen Client-Zertifikate verifiziert wurde.
- ☒ Der Marktrechner darf Verbindungen von Kunden nur akzeptieren, wenn dessen Berechtigungsnachweis von einem AAS verifiziert wurde.
- □ Der Marktrechner soll lokale Kunden ebenfalls durch einen AAS authentifizierten lassen.
- ☒ Die Kommunikation zwischen Marktrechner und Kunde soll über HTTPS verschlüsselt werden, unter der Verwendung von TLS 1.2.
- ☒ Das Verschlüsselungsverfahren muss Perfekt Forward Security (PFS) einsetzen.
- ☒ Die Verschlüsselung soll unabhängig von der Authentifizierungsmethode asynchron sein.

A.1.4 Autorisierung

- ☒ Der Marktrechner soll den Zugriff anhand der vom AAS verifizierten oder mitgeteilten Rolle(n) autorisieren.
- □ Die verfügbaren Rollen sind jene, die anhand des Rich-Picture identifiziert wurden.

A.1.5 Verschlüsselung

- □ Aufgezeichnete, verschlüsselte Kommunikation ist vom Marktrechner beim Wiedereinspielen zu erkennen und zu verwerfen. (Nonce)

A.1.6 Verbindungen

- ☐ ~~Der Marktrechner soll darauf verzichten, AAS-Server über Domainnamen anzusprechen. (Spoofing)~~
- ☒ Direkte beliebige Verbindungsversuche aus dem Internet auf den Marktrechner sind zu unterbinden. (DoS)

A.2 LDAP-Inhalt

Auflistung A.1: LDAP-Inhalt im LDIF-Format

```
1  version: 1
2
3  # Top-level
4  dn: dc=eckelmann,dc=de
5  objectclass: top
6  objectclass: domain
7  dc: eckelmann
8
9  # KGL-Abteilung
10 dn: ou=kgl,dc=eckelmann,dc=de
11 objectClass: top
12 objectClass: organizationalUnit
13 ou: people
14 ou: radius
15
16 # admins Organisation
17 dn: ou=admins,ou=kgl,dc=eckelmann,dc=de
18 objectClass: top
19 objectClass: organizationalUnit
20 ou: people
21 ou: admins
22
23 # Benutzer zum Anmelden am LDAP
24 dn: cn=binduser,ou=admins,ou=kgl,dc=eckelmann,dc=de
25 objectClass: top
26 objectClass: person
27 cn: binduser
28 sn: freeradius
```

```
29 userPassword:: e1NTSEF9U0F1c1UvcFZVaVhBb2lHUlhXR01lRWpFYURhcGw
30
31 #   users Organisation
32 dn: ou=users,ou=kgl,dc=eckelmann,dc=de
33 objectClass: top
34 objectClass: organizationalUnit
35 ou: radius
36 ou: users
37
38 #   Benutzer zur Authentifizierung  und Autorisierung
39 dn: cn=Kevin Sapper+sn=Sapper,ou=users,ou=kgl,dc=eckelmann,dc=de
40 objectClass: top
41 objectClass: inetOrgPerson
42 objectClass: radiusProfile
43 objectClass: person
44 objectClass: organizationalPerson
45 cn: Kevin Sapper
46 sn: Sapper
47 givenName: Kevin
48 mail: k.sapper@eckelmann.de
49 uid: ksapp
50 userPassword:: e3NoYX1mRXFOQ2NvM1lxOWg1WlVnbEQzQ1pKVDRsQnM9
51 radiusGroupName: analyst
52
53 dn: cn=John Doe+sn=Doe,ou=users,ou=kgl,dc=eckelmann,dc=de
54 objectClass: top
55 objectClass: inetOrgPerson
56 objectClass: radiusProfile
57 objectClass: person
58 objectClass: organizationalPerson
59 cn: John Doe
60 sn: Doe
61 givenName: John
62 mail: j.doe@fsz.de
63 uid: jdoe
64 userPassword:: e3NoYX1mRXFOQ2NvM1lxOWg1WlVnbEQzQ1pKVDRsQnM9
65 radiusGroupName: fernservice
66
67 dn: cn=Matthias Wolf+sn=Wolf,ou=users,ou=kgl,dc=eckelmann,dc=de
68 objectClass: top
```

```
objectClass: inetOrgPerson
objectClass: radiusProfile
objectClass: person
objectClass: organizationalPerson
cn: Matthias Wolf
sn: Wolf
givenName: Matthias
mail: m.wolf@eckelmann.de
uid: mwolf
userPassword:: e3NoYX1mRXFOQ2NvM1lxOWg1WlVnbEQzQ1pKVDRsQnM9
radiusGroupName: hersteller
```