Endbericht
PG555: Cloud-basiertes Internetbanking System

30. März 2012
<table>
<thead>
<tr>
<th>Autoren</th>
<th>Cai</th>
<th>(CW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wei</td>
<td>Hellwig</td>
<td>(RH)</td>
</tr>
<tr>
<td>Richard</td>
<td>Kexel</td>
<td>(JK)</td>
</tr>
<tr>
<td>Johann</td>
<td>Mucha</td>
<td>(VM)</td>
</tr>
<tr>
<td>Viktor</td>
<td>Seeland</td>
<td>(TS)</td>
</tr>
<tr>
<td>Thorben</td>
<td>Spasovski</td>
<td>(DS)</td>
</tr>
<tr>
<td>Daniel</td>
<td>Stoklossa</td>
<td>(VS)</td>
</tr>
<tr>
<td>Viktor</td>
<td>Vasileva</td>
<td>(AV)</td>
</tr>
<tr>
<td>Anna</td>
<td>Waqas</td>
<td>(MW)</td>
</tr>
<tr>
<td>Muhammad</td>
<td>Yang</td>
<td>(YD)</td>
</tr>
</tbody>
</table>
Inhaltsverzeichnis

0. Einleitung 1
   0.1. Problemstellung 1
   0.2. Aufbau des Dokuments 2

I. Dokumentationen und Compliance 3
   1. Technische Dokumentation 5
      1.1. Cloud 5
         1.1.1. Verwendete Cloudtechnologie 5
         1.1.2. Banking-Umgebung 6
         1.1.3. Anwendung 7
      1.2. Datenbank 10
         1.2.1. Vorbetrachtung 10
         1.2.2. Zugriff auf die Datenbank 12
         1.2.3. Aufbau 14
      1.3. Glassfish 20
         1.3.1. Java Database Connectivity (JDBC) 20
         1.3.2. Sicherheitsrealm 22
      1.4. Komponenten 24
         1.4.1. Architektur 24
      1.5. Sicherheit 28
         1.5.1. Aufbau der Dokumentation 28
         1.5.2. Planung der Sicherheit 28
         1.5.3. Implementierung der Sicherheitsmaßnahmen 30
         1.5.4. Verwaltung der RSA-Schlüssel 38
      1.6. GUI Testen durch Selenium 39
         1.6.1. Einführung 39
         1.6.2. Selenium IDE 39
         1.6.3. Selenium RC 39
         1.6.4. Problem mit SSL-Zertifikate 39
         1.6.5. Selenium Testen in Form von JUnit 41
      1.7. Log-System mit Log4J 42
         1.7.1. Komponenten 43
         1.7.2. Besondere Konfiguration mit JSF und Spring unter Glassfish 45
         1.7.3. LogDaten 45
2. Compliance

2.1. Gesetze

2.1.1. Behandlung der Gesetze nach dem Projektplan
2.1.2. Betrachtete Gesetze
2.1.3. Analyse und Dokumentation der Gesetze
2.1.4. Anforderungen durch Gesetze

2.2. Security Policy

2.2.1. IT-Sicherheitsleitlinie (Security Policy Schicht 1, BSI 100-1)
2.2.2. BSI-Grundschatz (Security Policy Schicht 2, BSI 100-2)
2.2.3. Handbücher (Security Policy Schicht 3, BSI 100-3)

II. Abweichungen vom Pflichtenheft

3. Abweichungen vom Pflichtenheft

3.1. Kommunikationsanschlüsse

3.1.1. Kommunikation mit der Schufa
3.1.2. Börse und Bahn
3.1.3. Interbank

3.2. Rollen und deren Funktionalitäten

3.2.1. Kundenberater
3.2.2. Kunde
3.2.3. Geschäftsführer
3.2.4. Produktentwickler
3.2.5. Controlling-Mitarbeiter
3.2.6. Kassierer
3.2.7. Jurist
3.2.8. System
3.2.9. Systemadministrator
3.2.10. Eigenhändler
3.2.11. Marketing

3.3. Automatisierte Prozesse

III. Maßnahmen und Erfahrungen

4. Maßnahmen des Managements

4.1. Projektmanagement

4.1.1. Zusammenfassung des Projektmanagements im Projektplan
4.1.2. Vorgehen in der zweiten Projektphase

4.2. Teammanagement

4.2.1. Zusammenfassung des Teammanagements im Projektplan

4.3. Qualitätsmanagement

4.3.1. Zusammenfassung des Qualitätsmanagements im Projektplan
4.3.2. Vorgehensweise im Qualitätsmanagement während des Projektes . 74
4.4. Risikomanagement . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 77
  4.4.1. Zusammenfassung des Risikomanagements im Projektplan . . . . 77
4.5. Bewertung der Maßnahmen . . . . . . . . . . . . . . . . . . . . . . . . . . 79
  4.5.1. Projektmanagement . . . . . . . . . . . . . . . . . . . . . . . . . 79
  4.5.2. Teammanagement . . . . . . . . . . . . . . . . . . . . . . . . . . . 79
  4.5.3. Qualitätsmanagement . . . . . . . . . . . . . . . . . . . . . . . . . 81
  4.5.4. Risikomanagement . . . . . . . . . . . . . . . . . . . . . . . . . . . 81

5. Erfahrungen 85

IV. Anhang 91

A. Anwender Dokumentation 93
  A.1. Einleitung . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 93
  A.2. Voraussetzungen zur Nutzung . . . . . . . . . . . . . . . . . . . . . . . . 93
  A.3. Benutzeroberfläche . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 93
  A.4. Gemeinsame Funktionen . . . . . . . . . . . . . . . . . . . . . . . . . . . . 94
    A.4.1. Ein- und Ausloggen . . . . . . . . . . . . . . . . . . . . . . . . . . . 94
    A.4.2. Rollen-Auswahl . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 95
    A.4.3. Nachrichtenverkehr . . . . . . . . . . . . . . . . . . . . . . . . . . . 96
  A.5. Kunde . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 97
    A.5.1. Banking . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 99
    A.5.2. Börse . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 103
    A.5.3. Persönliche Daten ansehen . . . . . . . . . . . . . . . . . . . . . . . 105
    A.5.4. Nachrichten . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 106
    A.5.5. Kurse . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 106
  A.6. Kundenberater . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 107
    A.6.1. Aufgaben . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 108
    A.6.2. Kundenverwaltung . . . . . . . . . . . . . . . . . . . . . . . . . . . 108
    A.6.3. Nachrichten . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 117
    A.6.4. Kurse . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 117
  A.7. Kassierer . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 119
  A.8. Produktdirektiven . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 120
    A.8.1. Aufgaben . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 120
    A.8.2. Statistische Daten . . . . . . . . . . . . . . . . . . . . . . . . . . . . 120
    A.8.3. Nachrichten . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 120
  A.9. Marketing-Mitarbeiter . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 121
  A.10. Controlling-Mitarbeiter . . . . . . . . . . . . . . . . . . . . . . . . . . . . 121
    A.10.1. Aufgaben . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 121
    A.10.2. Kundenverwaltung . . . . . . . . . . . . . . . . . . . . . . . . . . . 122
    A.10.3. Logs einsehen . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 122
    A.10.4. Nachrichten . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 122

VII
A.10.5. Kurse einsehen ................................................................. 123
A.11. Jurist .................................................................................. 124
  A.11.1. Aufgaben einsehen ....................................................... 124
  A.11.2. Kundenverwaltung ....................................................... 124
  A.11.3. Kontodatenliste beantragen ......................................... 125
  A.11.4. Nachrichtenverkehr ..................................................... 125
A.12. Geschäftsführer ................................................................. 126
  A.12.1. Limits setzen .............................................................. 126
  A.12.2. Kundenverwaltung ....................................................... 127
  A.12.3. Log einsehen ............................................................... 127
  A.12.4. Kontodatenliste beantragen ......................................... 128
  A.12.5. Statistische Daten ....................................................... 128
  A.12.6. Einstellung der Verdächtigkeitsprüfung für Überweisung .. 128
  A.12.7. Nachrichtenverkehr ..................................................... 128
  A.12.8. Kurse einsehen ........................................................... 128
A.13. Eigenhändler .................................................................... 128
  A.13.1. Börseangelegenheit .................................................... 129
  A.13.2. Kontostand einsehen .................................................. 129
  A.13.3. Nachrichtenverkehr ..................................................... 129
A.14. Systemadministrator .......................................................... 129
  A.14.1. Systemstatus einsehen ................................................ 130
  A.14.2. Mitarbeiterverwaltung ................................................ 130
  A.14.3. Log einsehen ............................................................... 131
  A.14.4. Log auswerten ............................................................ 132
  A.14.5. Backup erstellen ........................................................ 133
  A.14.6. RSA Schlüssel verwalten ............................................. 133
  A.14.7. Nachrichtenverkehr ..................................................... 135
  A.14.8. Runterfahren .............................................................. 135

B. Datenbanktabellen ............................................................... 137
  B.1. Personen .......................................................................... 137
  B.2. Interne Konten ................................................................ 138
  B.3. Transaktionen ................................................................. 139
  B.4. Börse und Nachrichten .................................................... 140
  B.5. Vorgänge ........................................................................ 141
  B.6. Stammdaten .................................................................... 142

C. Security Policy .................................................................... 143
  C.1. IT-Sicherheitsleitlinie ........................................................ 144
  C.2. BSI-Grundschatzkataloge .................................................. 153

D. Technologieauswahl ............................................................ 221
  D.1. Technologieauswahl ........................................................ 222
Literaturverzeichnis
0. Einleitung

Autor: VM

Das Onlinebanking ist für die Banken eine wichtige Komponente zur Abwicklung ihrer Geschäftsprozesse. Die Entwicklung einer Software zur Umsetzung des Onlinebankings ist sehr komplex und stellt hohe Anforderungen an die Entwickler der Software. Im Rahmen der Projektgruppe PG555 ist ein Bankensystem mit Online-Funktionalität von den Projektteilnehmern zu entwerfen. Das vorliegende Dokument beinhaltet den Endbericht des Projekts zur Entwicklung des Bankensystems.

0.1. Problembeschreibung


Die zweite Phase hat das Ziel das Bankensystem zu entwickeln. Dazu sind die in der Spezifikation definierten Funktionen als Web-Applikation zu entwerfen und zu testen. Wichtige Aufgaben sind hierbei die Integration eines geeigneten Datenbanksystems zur Speicherung von Daten, die Implementierung der Geschäftsprozessverwaltung und der Systemschnittstellen, sowie die Erstellung von Webseiten für die Benutzeroberfläche. Das Testen der Funktionen dient der Qualitätssicherung.
0.2. Aufbau des Dokuments

Der Endbericht besteht aus drei Teilen. Im ersten Teil ist die technische Dokumentation des Bankensystems und die Umsetzung der Compliance-Anforderungen beschrieben. Im zweiten Teil wird auf die Unterschiede der Funktionen des Systems in Bezug zu den Funktionen, die im Pflichtenheft [32] definiert sind, eingegangen. Der dritte Teil enthält die Beschreibung der Maßnahmen des Managements und die Erfahrungen der Projektteilnehmer während des Projekts. Im Anhang befindet sich schließlich eine Anwenderdokumentation, in der die Nutzung des Bankensystems vorgestellt wird.


Der dritte Teil beinhaltet zum einen die Dokumentation der Maßnahmen des Managements und zum anderen Erfahrungsberichte der Projektmitglieder. Im Abschnitt über die Maßnahmen werden die im Projektplan [33] definierten Maßnahmen und ihre Umsetzung während des Projekts beschrieben. Die Maßnahmen beziehen sich auf das Projektmanagement, das Teammanagement, das Qualitätsmanagement und das Risikomanagement für die Projektgruppe. Die Erfahrungsberichte fassen die während des gesamten Projekts gemachten Erfahrungen der Projektteilnehmer zusammen.
Teil I.

Dokumentationen und Compliance
1. Technische Dokumentation

1.1. Cloud

Autor: VS

1.1.1. Verwendete Cloudtechnologie

Die Cloud wurde als eine Private Cloud mit der Open-Source Cloud Computing Software Eucalyptus Community Cloud\(^1\) (ECC) in der Version 2.0.3 realisiert. Dies ist eine Infrastructure as a Service-Cloud (IaaS) und bietet für den Anwender einen Zugriff auf das System ab der Betriebssystemebene. Das bedeutet, dass der Anwender beliebig virtuelle Server starten kann auf denen ein Betriebssystem läuft, auf welches er vollen Zugriff hat. Die ECC besteht aus den folgenden Komponenten:

- Cloud Controller (CLC)
- Walrus
- Storage Controller (SC)
- Cluster Controller (CC)
- Node Controller (NC)


\(^1\)http://open.eucalyptus.com/

### 1.1.2. Banking-Umgebung


Die Banking-Software und die dazugehörigen Komponenten wurden auf einem EBS installiert, so dass auch alle Einstellungen und Daten, die bei der Ausführung entstehen,

Abbildung 1.2.: Konkrete Umsetzung der Banksystemumgebung

1.1.3. Anwendung

Um mit der Cloud zu interagieren wurden die Euca2ools\cite{19} eingesetzt. Dies ist eine Sammlung von Komandozeilenwerkzeugen, die vom Eucalyptus Team angeboten werden. Für den Zugriff auf die Cloud, ist eine Registrierung beim Cloud-Controller notwendig. Dazu besucht man die URL des Cloudservers (https://129.217.47.70:8443/) und klickt auf “Apply for Account” und gibt seine Daten ein. Daraufhin erhält der Administrator
eine Meldung und kann den Benutzer freischalten, welcher sich dann in der Weboberfläche einloggen kann. Danach kann unter dem Punkt “Credentials” ein Zertifikat für den Benutzer heruntergeladen werden, das von den Euca2ools verwendet wird, um sich bei der Cloud zu authorisieren und über eine verschlüsselte Verbindung mit ihr zu kommunizieren. Die Euca2ools können dann verwendet werden um Ressourcen abzufragen und Instanzen hochzuladen und laufen zu lassen.

1.1.3.1. Informationen abfragen

Mit den folgenden Befehlen lassen sich Informationen über laufende Instanzen, verfügbare Images, verfügbare Ressourcen und vorhandene Backups abfragen:

- `euca-describe-images`: Zeigt verfügbare Images, Image-IDs, Bucket- und Objektname an.
- `euca-describe-availability-zones`: Zeigt die verfügbaren Cluster und deren freie Ressourcen an.
- `euca-describe-snapshots`: Zeigt die vorhandenen Backups, sowie deren IDs, Erstellungszeitpunkt und Status an.

1.1.3.2. Instanzen verwalten

Mit den folgenden Befehlen werden Instanzen gestartet, gestoppt und Adressen reserviert und zugeteilt:

- `euca-terminate-instance`: Stoppt laufende Instanzen.
- `euca-allocate-address`: Reserviert eine öffentliche IP-Adresse für den Benutzer.
- `euca-associate-address`: Weist einer Instanz eine IP-Adresse zu.

1.1.3.3. Images verwalten

Mit den folgenden Befehle werden Images in die Cloud hochgeladen und beim Cloud-Controller registriert:

- `euca-upload-bundle`: Lädt ein gebündeltes Image in die Cloud.
- `euca-register`: Registriert ein gebündeltes Image bei der Cloud.
1.1.3.4. EBS verwalten

Mit den folgenden Befehlen wird ein EBS-Volume erstellt, gelöscht, einer Instanz zugewiesen und entfernt sowie Backups davon erstellt und gelöscht:

- **euca-create-volume**: Erstellt ein EBS-Volume in dem spezifizierten Cluster.
- **euca-delete-volume**: Löscht ein EBS-Volume.
- **euca-attach-volume**: Bindet ein EBS-Volume in einer Instanz ein.
- **euca-detach-volume**: Entfernt ein EBS-Volume aus einer Instanz.
- **euca-create-snapshot**: Erstellt einen Snapshot eines Volumes.
- **euca-delete-snapshot**: Löscht einen Snapshot.

Weitere Kommandos und Informationen zur Verwendung der Eucalyptus-Cloud finden sich im Eucalyptus User’s Guide [21].
1.2. Datenbank

Autor: JK

1.2.1. Vorbetrachtung


1.2.1.1. Begriffe

In diesem Unterabschnitt sollen die wichtigsten Begriffe zu der verwendeten Datenbank vorgestellt werden, um das Verständnis des Abschnitts zu fördern. Es sei angemerkt, dass einige Begriffe sich mit denen in weiteren Kapiteln überschneiden, aber eine unterschiedliche Bedeutung besitzen [35].

**Datenbank** Eine Ansammlung von Tabellen und Views, die miteinander in Beziehungen stehen.

**Datensatz** Daten einer Tabelle, die zusammen eine Einheit bilden.

**Fremdschlüssel** Eine Referenz von einer Tabelle auf einen Datensatz einer anderen Tabelle mit dem Ziel eine Beziehung zwischen den Tabellen sicherzustellen.

**Normalisierung** Methoden, die auf eine Datenbank und ihre Tabellen angewendet werden, um eine einfache Handhabung zu gewährleisten. So können z.B. doppelte Einträge ausgeschlossen werden.

**Primärschlüssel** Eine Menge von Feldern, die den Datensatz eindeutig identifiziert.

**Tabelle** Eine Ansammlung von Daten, die gleich aufgebaut sind und zeilenweise angeordnet werden.

**Transaktion** Eine atomare Aktion innerhalb der Datenbank, die aus mehreren Anfragen bestehen kann.

**Schema** Die Festlegung, welche Form die Daten in einer Datenbank haben müssen und welche Beziehungen zwischen den Daten bestehen.
**Sicht oder View** Eine Sammlung von Datensätzen bezüglich einer bestimmten Anfrage, die gespeichert und wie in einer Tabelle eingesehen werden kann. Der Zweck ist die Wiederverwendung von Anfragen und die Einsparung häufiger Datenbankzugriffe.

### 1.2.1.2. Einordnung ins System


Abbildung 1.3.: Einordnung der Datenbank innerhalb des Cloud-Systems

Abbildung 1.3 stellt das Cloud-System abstrakt dar. Man erkennt, dass innerhalb der

1.2.2. Zugriff auf die Datenbank


1.2.2.1. Verbindung zur Datenbank

Wie in Abbildung 1.3 dargestellt, existieren eine Möglichkeit der Verbindung zur Datenbank von außen. Dies ist vor allem für den Datenbankadministrator notwendig, da dieser unabhängig vom Internetbankingsystem verschiedene Arbeiten durchführen soll. Um die Datenbank also von außen ansprechen zu können benötigt man die folgenden Verbindungsdaten:

**Host:** 129.217.47.73  
**Port:** 3306


1.2.2.2. Rollen in der Datenbank

Es existieren insgesamt drei Rollen, die auf die Datenbank zugreifen können, um mit dieser zu interagieren. Diese sind:

- BaFin und BZSt
- Banksystem
- Datenbank-Administrator

**BaFin und BZSt** benötigen einen Zugriff auf die Kundenstammdaten der Bank [32] in stammdaten über eine SQL-Schnittstelle. Der Zugriff soll für den Kunden unbemerkt
seine und passiert außerhalb des Internetbankingsystems direkt auf den Datenbankserver. Die Authentifizierung erfolgt passwortbasiert, muss aber für einen sichere Verbindung zertifikatbasiert sein.

Das **Banksystem** befindet sich auf einem Webserver **Glassfish** (siehe Abschnitt [1.3]). Dieser stellt eine sichere Verbindung zu der Datenbank her und authentifiziert sich mit Hilfe eines Benutzernamens und eines Passworts (siehe Abschnitt [1.3.1]). Dabei muss das System sowohl auf die Datenbank **stammdaten**, als auch auf **banksystem** einen Zugriff erhalten, um die Daten aktuell und konsistent zu halten. Die Rolle **Banksystem** ist also vor allem für die Verwaltung der Daten innerhalb der Datenbanken zuständig.

**Datenbank-Administrator** hat die Aufgabe die Wartung durchzuführen und damit die Verwaltung des gesamten Datenbankservers zu übernehmen. Dazu gehört nicht nur Benutzerverwaltung und Rechtevergabe, sondern auch das Anlegen neuer Tabellen oder Datenbanken, falls diese im weiteren Betrieb des Systems benötigt werden. Dazu verbindet er sich von außen direkt auf den Datenbank-Server und kann die Aufgaben unabhängig vom Banksystem erledigen.


Tabelle 1.1.: Übersicht über die Rollen und die Authentifizierungsart

<table>
<thead>
<tr>
<th>Benutzer</th>
<th>Rolle</th>
<th>Authentifizierung</th>
</tr>
</thead>
<tbody>
<tr>
<td>bafinbzst</td>
<td>BaFin und BZSt</td>
<td>passwortbasiert</td>
</tr>
<tr>
<td>system</td>
<td>Banksystem</td>
<td>passwortbasiert</td>
</tr>
<tr>
<td>root</td>
<td>Datenbank-Administrator</td>
<td>passwortbasiert</td>
</tr>
</tbody>
</table>

1.2.2.3. Rechte der Benutzer

Sind die Benutzer authentifiziert, erfolgt die Autorisierung nach einem rollenbasierten Verfahren. Tabelle 1.2 stellt dazu die Benutzer mit ihren Rechten dar. Die Rechte richten sich nach den SQL-Anfragen, die der jeweilige Benutzer ausführen darf. Es gilt zudem das Prinzip, dass alle Aktionen, die nicht explizit erlaubt, verboten sind.

Der Benutzer **bafinbzst** darf demzufolge auf die Daten in der Datenbank **stammdaten** nur lesend zugreifen, **system** erhält Schreib- und Leserechte an **stammdaten** und **banksystem**, während **root** einen Vollzugriff auf den Datenbankserver bekommt und alle verfügbaren Aktionen auf allen Datenbanken (auch Verwaltungsdatenbanken) bearbeiten darf.
Tabelle 1.2.: Übersicht über die Autorisierung der Benutzer auf verschiedenen Datenbanken

<table>
<thead>
<tr>
<th>Benutzer</th>
<th>Datenbanken</th>
<th>Rechte</th>
</tr>
</thead>
<tbody>
<tr>
<td>bafinbzst</td>
<td>stammdaten</td>
<td>SELECT</td>
</tr>
<tr>
<td>system</td>
<td>stammdaten, banksystem</td>
<td>SELECT, INSERT, UPDATE, DELETE</td>
</tr>
<tr>
<td>root</td>
<td>alle</td>
<td>alle</td>
</tr>
</tbody>
</table>

An dieser Stelle soll erwähnt sein, dass obwohl der Datenbank-Administrator (root) alle Rechte hat, dennoch das BDSG und LDSG gilt [9][5]. Der Administrator unterliegt einer Schweigepflicht nach §5 BDSG und muss im Falle einer Auftragsdatenverarbeitung nach §11 BDSG einem schriftlichen Vertrag zustimmen (siehe Kapitel 2).

1.2.3. Aufbau


Eine Tabelle bzw. Entität, die Datenfelder, Primärschlüssel oder Fremdschlüssel enthält.

Datenfeld, das als Primärschlüssel oder als Teil des Primärschlüssels dient.

Fremdschlüssel, der nicht Teil des Primärschlüssels ist.

Beziehung zwischen Tabelle A und Tabelle B. Fremdschlüssel aus A referenziert den Primärschlüssel oder Index der Tabelle B, ist aber kein Teil des Primärschlüssels in Tabelle A.
1.2.3.1. Datenbank: banksystem

Die Datenbank banksystem bietet die Grundlage für das gesamte System. Darin werden alle Daten des Systems abgelegt, die persistent gehalten werden müssen, um diese bei einem Systemabsturz wiederherstellen zu können. Die Tabellen basieren auf dem verwendeten Modell, so dass eine Abbildung der Objekte im Programm unkompliziert auf die Tabellen durchgeführt werden kann. Da es sich um relationale Datenbanken handelt, wurden die Tabellen einer Normalisierung bis zur dritten Normalform unterzogen. Im Folgenden werden einige für wichtig erachtete Ausschnitte aus der Datenbank vorgestellt.

Abbildung 1.4.: Tabellenstruktur für die Akteure der Bank

In Abbildung 1.4 werden die Akteure der Bank betrachtet. Um einen Akteur im System
Um eine Person eindeutig zu identifizieren, wurde ein zusammengesetzter Schlüssel aus vier Attributen name, vorname, geburtsdatum und geburtsort prototypisch festgelegt. Da eine Person mehrere Adressen haben kann, wurde eine n:m-Beziehung zwischen der Tabelle person und der Tabelle adresse angenommen, die wiederum eine besondere Tabelle persadr benötigt, um die Personen mit den Adressen zu verknüpfen. Man beachte, dass in diesem Fall eindeutige Indizes id_person und id_adresse als Fremdschlüssel verwendet werden und nicht die Primärschlüssel selbst. Zusätzlich zu persönlichen Daten, muss sich ein Akteur im System anmelden können. Dazu benötigt er einen Benutzernamen, einen Passwort und eine Gruppenzugehörigkeit, wonach die Autorisierung erfolgt. Der Benutzername und das Passwort wird in der Datenbank benutzer abgelegt, während sich die Gruppen eines Benutzers in der Tabelle gruppe befinden. Für die Identifikation eines Akteurs benötigt man also seine persönlichen Daten und den Benutzernamen. Dies liegt vor allem daran, dass die Mitarbeiter der Bank ebenfalls Kunden der Bank sein können und man gern eine Isolierung zwischen Kunden und Mitarbeitern hätte. Da Kunden zusätzlich noch eine Kundennummer in der Bank erhalten sollen,
wurde die Tabelle *kunde* angelegt, die alle Akteure aus der Tabelle *akteur* mit der Gruppe *Kunde* auf eine eindeutige Kundennummer abbildet. Um die Akteure der Bank mit wenigen Datenbankanfragen auslesen zu können, wurden die Views *view_kunde* und *view_akteur* angelegt.


Abbildung 1.6.: Tabellenstruktur für die Geldtransaktionen der Bank

1.2.3.2. Datenbank: stammdaten

Die Datenbank für BaFin und BZSt wurde bereits von dem Auftraggeber vorgegeben und ist so auch im System hinzugefügt worden. Es werden dabei nur Stamminformationen der Konten in dieser Datenbank gespeichert, wobei nach dem Schließen eines Kontos die Daten noch drei Jahre in dieser Datenbank gespeichert bleiben bis sie gelöscht werden.
den müssen.

Abbildung 1.7.: Tabellenstruktur für die Datenbank *stammdaten*

Abbildung 1.7 zeigt die Tabellen der Datenbank *stammdaten*. In jeder Tabelle wird das Eintragsdatum und das Löschdatum des zugehörigen Wertes gespeichert. Die Person wird dabei durch einen Primärschlüssel *PersonId* identifiziert, der auch als Fremdschlüssel in den Tabellen *persongebdat* und *personadress* gespeichert wird. Eine besondere Unterscheidung gibt es zwischen einem wirtschaftlich Berechtigten und einem Verfügungsbeschränkten eines Kontos, wobei die erste Gruppe den Inhaber und alle Personen einbehalten, die über das Konto verfügen können.

Eine vollständige Auflistung aller Tabellen der beiden Datenbanken befindet sich im Anhang [B].
1.3. Glassfish

Autor: JK


Um Glassfish konfigurieren zu können, muss dieser gestartet und die Administrationskonsole aufgerufen werden, die unter folgender Adresse im Browser zu erreichen ist:

http://129.217.47.73:4848

Die Konsole ist passwortgeschützt und die Zugangsdaten können bei dem zuständigen Administrator angefragt werden.

Die durchzuführenden Konfigurationen beziehen sich auf den Datenbankzugriff und Sicherheitsmechanismen, die angeboten werden.

1.3.1. Java Database Connectivity (JDBC)


1.3.1.1. Verbindungspool erstellen

Zusätzlich dazu muss die Datenbank-Verbindung in der Administrationskonsole von Glassfish konfiguriert werden. Dazu öffnet man die Konsole und wählt in der Navigationsleiste links Ressourcen → JDBC → JDBC-Verbindungspool aus. Anschließend werden alle vorhandenen Pools im Hauptfenster aufgelistet. Falls der zu konfigurierende Pool noch nicht vorhanden ist, wählt man die Option Neu mit folgenden Daten aus:

Poolname: MySQLPool (willkürlich wählbar)
Ressourcentyp javax.sql.DataSource

Hersteller MySQL

Im Fenster, das nach dem Auswählen von Weiter folgt, müssen folgende Eigenschaften eingetragen werden. Dabei muss auf die Groß- und Kleinschreibung geachtet werden.

Port 3306

ServerName 129.217.47.73

DatabaseName banksystem

User system

Password Aus Sicherheitsgründen entfernt

Url jdbc:mysql://129.217.47.73:3306/banksystem

URL jdbc:mysql://129.217.47.73:3306/banksystem

Sind alle Eigenschaften eingetragen, kann zusätzlich die Datenbankverbindung mit einem Ping getestet werden.

Zusätzlich muss die obere Prozedur für die weiteren, vorhandenen Datenbanken durchgeführt werden. Bevor man aber auf diese Datenbanken in der Anwendung zugreifen kann, muss je eine Datenquelle (engl. DataSource) angelegt und im System bekannt gemacht werden.

1.3.1.2. Datasource erstellen

In der Administrationskonsole von Glassfish wählt man Ressourcen → JDBC → DataSource aus. Bei der Auflistung im Hauptfenster legt man eine neue Datasource an mit folgenden Eigenschaften:

JNDI-Name jdbc/MySQLDataSource

Poolname MySQLPool (Name des Verbindungspools unter 1.3.1.1)

Aktiviert Häkchen setzen

Für jeden Pool muss eine eigene Datasource angelegt werden und unterschiedliche JNDI-Namen vergeben werden, um diese im System ansprechen zu können.

Zusätzlich zur Administrationskonsole müssen die Datasourcen im Deployment Descriptor web.xml des Projekts bekannt gemacht werden. Dazu fügt man die folgenden Zeilen (für jede Datasource) in die Datei ein.

21
Außerdem muss der Server-Deployment Descriptor `glassfish-web.xml` um die folgenden Zeilen erweitert werden:

```xml
<resource-ref>
  <res-ref-name>
    jdbc/MySQLDataSource
  </res-ref-name>
  <res-type>javax.sql.DataSource</res-type>
  <res-auth>Container</res-auth>
  <res-sharing-scope>Shareable</res-sharing-scope>
</resource-ref>
```

Nun kann auf die Datasource innerhalb der Glassfish-Anwendung zugegriffen werden.

### 1.3.2. Sicherheitsrealm

Einer der Vorteile an den Webservern bzw. Web-Containern wie Glassfish ist, dass diese bereits mit einigen Sicherheitsmechanismen ausgestattet sind, die zertifiziert sind und deshalb keine Verifikation benötigen.

Die Konfiguration des Sicherheitsrealms erfolgt in der Administrationskonsole von Glassfish. Hier wählt man in der Navigationsleiste Konfigurationen → server-config → Sicherheit → Bereiche aus. An dieser Stelle muss ein neuer Realm angelegt werden. Folgende Daten werden dabei in die Felder eingetragen und die übrigen leerlassen:

**Name** rollen-realm

**Klassename** com.sun.enterprise.security.auth.realm.jdbc.JDBCRealm

**JAAS-Kontext** jdbcRealm

**JNDI** jdbc/MySQLDataSource (Datasource aus Abschnitt 1.3.1.2)

**Benutzertabelle** benutzer

**Benutzerspalte** benutzername

**Passwortspalte** passw

**Gruppentabelle** gruppe

**Gruppenspalte** gruppe

**Digest-Algorithmus** MD5

**Codierung** Hex

Damit ist die Konfiguration des Sicherheitsrealms abgeschlossen. Die Authentifizierung und Authorisierung erfolgt über die Deployment Deskriptoren web.xml und glassfish-web.xml in Verbindung mit dem Formular auf der Seite login.xhtml (siehe Kapitel 1.5).
1.4. Komponenten

1.4.1. Architektur

Autor: JK

In Abbildung 1.3 wurde das Internetbanking-System innerhalb des Cloud-Systems in zwei Schichten dargestellt, die Internetbanking-Schicht auf dem Webserver und die Datenbankschicht. Die Benutzer greifen über einen Browser auf den Webserver zu, der die für den Benutzer wichtige Daten anzeigt. Es handelt sich also um eine Client-Server-Interaktion, weshalb sich als Architekturmodell das Client-Server-Modell anbietet. Abbildung 1.8 betrachtet das Internetbanking-System als Client-Server-Modell, wo-

Abbildung 1.8.: Banksystem in einer Client-Server Architektur mit mehreren Schichten

1.4.1.1. Präsentationsschicht

Bei der Präsentationsschicht handelt es sich um einen Teil des Entwurfsmusters Model-View-Controller (MVC) [53], wobei es sich um die View handelt [38]. Diese besteht aus zwei Teilen, den JavaServer Faces und den ManagedBeans [55].

JavaServer Faces


ManagedBeans

ManagedBeans sind normale Java-Klassen, die mit der Annotation @ManagedBean versehen werden. Damit dürfen alle JSF-Seiten auf die Methoden und Attribute der Bean zugreifen. Allerdings ist der Zugriff auf die Attribute nur über Getter- bzw. Setter-Methoden erlaubt, so dass eine Kapselung der Attribute möglich ist.

Innerhalb des Projekts wurde das PresentationModel- bzw. das ViewHelper-Muster angewandt [22], das eine Trennung von Daten, die innerhalb der View angezeigt werden und dem eigentlichen Modell (Containerklassen) fordert. Das PresentationModel (PM) besteht dabei aus mehreren ManagedBeans und befinden sich im Paket de.layout. Dazu zählen die Klassen:

- AufgabePM
- EingabeHandler
- KontoPM
- KundePM
- Navigation
- NavigationRollen
- NutzerPM
- PersonPM

1.4.1.2. Controllerschicht und Containerschicht


Controller

Das System besteht aus mehreren Controllern, die alle eine bestimmte Aufgabe haben. Der GeldtransferController zum Beispiel, der die Aufgabe hat aller Geldtransaktionen im System zu verwalten. Die verwendeten Controller sind:

- BoersenController
- GeldtransferController
- KontoController
- KommunikationsController
- KundenController
- Nutzerverwaltung
- SecurityController

Alle Anwendungsfälle, die das System enthalten muss [32], sind auf diese Controller verteilt und werden über die GUI und das PresentationModel ausgeführt.

Container

1.4.1.3. Datanzugriffsschicht

Die Datanzugriffsschicht hat die Aufgabe eine Verbindung zur Datenbank aufzubauen und die notwendigen Informationen zu speichern oder auszulesen. Dabei wurde das DataAccessObject-Muster (DAO-Muster) verwendet [22], das die Datenbankanfragen in den entsprechenden DataAccess-Objekten umhüllt und eine Trennung zwischen der spezifischen Datenbankanfrage und dem System erreicht. Als Zugriff auf die DAOs wird eine MySQLDAOFabrik verwendet, die als Singleton [38] implementiert wurde. Die einzelnen DAOs sind keine Singleton-Objekte und können deshalb mehrmals im System vorkommen. Die implementierten DAOs befinden sich im Paket de.dao und sind im einzelnen folgende Klassen:

- AkteurDAO
- AufgabeDAO
- KontoDAO
- KundeDAO
- NutzerDAO
- PersonDAO

Da das System nicht komplett implementiert werden konnte, handelt es sich um eine unvollständige Liste der DAOs, die noch erweitert werden müsste.
1.5. Sicherheit

Autor: VM

1.5.1. Aufbau der Dokumentation

Die folgenden Abschnitte beinhalten die technische Dokumentation des Themas Sicherheit im Projekt. Die Verletzung von Sicherheitsinteressen wird dabei als Sicherheitsvorfall bezeichnet [39]. Es wird zunächst eine Zusammenfassung der Planung vorgestellt, die in dem Projektplan entwickelt wurde [33]. Es werden dazu die für das Bankensystem relevanten Sicherheitsinteressen, die identifizierten Risiken für Sicherheitsvorfälle und die Sicherheitsmaßnahmen zur Vermeidung dieser vorgestellt. Daraufhin wird die Umsetzung der Planung während des Projektes vorgestellt. Für jedes einzelne Sicherheitsinteresse werden die implementierten Maßnahmen beschrieben. Im Anschluss daran folgt ein Abschnitt über die technische Umsetzung der RSA-Schlüsselverwaltung [30], die für die Verwaltung der Sicherheitsmaßnahmen digitale Signierung und Verschlüsselung benötigt wird.

1.5.2. Planung der Sicherheit

Während der Planungsphase des Projektes wurden die folgenden Sicherheitsinteressen für das Bankensystem identifiziert, die bis auf die Anonymität, aus Biskup [30] entnommen sind:

- Anonymität
- Authentizität
- Integrität
- Nachweisbarkeit
- Verfügbarkeit
- Vertraulichkeit

Des weiteren wurden die folgenden Risiken für die Verletzung der Sicherheitsinteressen ermittelt:

- Die Anonymität kann durch die Weitergabe von personenbezogenen Daten (kurz: Weitergabe) verletzt werden
- Die Authentizität kann durch Vortäuschung einer falschen Identität (kurz: Vortäuschung) verletzt werden
- Die Integrität kann durch eine fehlerhafte Übertragung von Daten oder durch Manipulation dieser (kurz: Manipulation) verletzt werden
• Die Nachweisbarkeit kann durch den Verlust von Daten zum Nachhalten von fehlerhaften und spezifizierten Ereignissen (kurz: Verlust der Nachvollziehbarkeit) verletzt werden

• Die Verfügbarkeit kann durch den Ausfall von Funktionen des Systems oder des gesamten Systems (kurz: Ausfall) verletzt werden

• Die Vertraulichkeit kann durch das bereits erwähnte Risiko der Weitergabe personenbezogener Daten verletzt werden

• Das Risiko eines nicht-spezifizierten Verhaltens des Systems (kurz: Nicht-spezifiziertes Verhalten) hat nicht absehbare Folgen, weshalb die Betroffenheit aller Sicherheitsanforderungen bis auf die Nachweisbarkeit nicht ausgeschlossen werden kann


<table>
<thead>
<tr>
<th>Kürzel</th>
<th>Risiko</th>
<th>Sicherheitsanforderung</th>
<th>Sicherheitsmechanismus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vertuschn</td>
<td>Vertuschn eines falschen Identums</td>
<td>Authentizität</td>
<td>Digitale Signierung</td>
</tr>
<tr>
<td>Manipulation</td>
<td>Fehlende Übertragung oder bewusste Manipulation von Daten</td>
<td>Integrität</td>
<td>Digitale Signierung</td>
</tr>
<tr>
<td>Weitergabe</td>
<td>Weitergabe von vertraulichen (z.B. personenbezogenen) Daten</td>
<td>Anonymität, Vertraulichkeit</td>
<td>Verschlüsselung</td>
</tr>
<tr>
<td>Ausfall</td>
<td>Ausfall von Funktionen des Systems, bzw. des kompletten Systems</td>
<td>Verfügbarkeit</td>
<td>Erstellung von Backups</td>
</tr>
<tr>
<td>Unautorisierte Nutzung</td>
<td>Unautorisierte Nutzung von Funktionen des Systems</td>
<td>Autorisation</td>
<td>Rechtevergabe</td>
</tr>
<tr>
<td>Verlust der Nachvollziehbarkeit</td>
<td>Verlust der Nachvollziehbarkeit von fehlerhaften, bzw. unerlaubten, Ereignissen</td>
<td>Nachweisbarkeit</td>
<td>Event-Logging</td>
</tr>
<tr>
<td>Nicht-spezifiziertes Verhalten</td>
<td>Nicht-spezifiziertes Verhalten der Funktionen der Software</td>
<td>Anonymität, Authentizität, Autorisation, Integrität, Verfügbarkeit, Vertraulichkeit</td>
<td>Testen (inkl. BPM)</td>
</tr>
</tbody>
</table>

Abbildung 1.9.: Übergangsmatrix
1.5.3. Implementierung der Sicherheitsmaßnahmen

In diesem Abschnitt wird die Implementierung der Sicherheitsmechanismen beschrieben. Die Beschreibung ist nach den Sicherheitsinteressen unterteilt und es werden somit die Sicherheitsmechanismen zu je einem Sicherheitsinteresse genannt. Im Anschluss der Beschreibung der Maßnahmen der einzelnen Sicherheitsinteressen wird die Vermeidung des Risikos Nicht-specifiziertes Verhalten beschrieben, welches eine Sonderstellung einnimmt, da das Risiko fast alle Sicherheitsinteressen betreffen kann.

1.5.3.1. Wahrung der Anonymität

Die Notwendigkeit der Anonymität resultiert aus der Verarbeitung personenbezogener Daten durch das Bankensystem. Im Fokus stehen hierbei zum Beispiel die personenbezogenen Daten der Kunden der Bank. Die Compliance der Bank fordert aufgrund des Bundesdatenschutzgesetzes [9], dass personenbezogene Daten nicht an Unberechtigte weitergegeben werden können. Es wird somit gefordert, dass die Kunden in Bezug zu unberechtigten Personen anonym bleiben. Die Anonymität muss sowohl für die Daten gelten, die von einem Client zum Server-System geleitet werden, als auch für die im System persistent gehaltenen Daten. So soll es nicht möglich sein, dass die Informationen der personenbezogenen Daten, die über das Internet gesendet werden und somit durch beliebige Rechner verarbeitet werden können, Unberechtigten zugänglich gemacht werden. Die Personen, auf die sich die Daten beziehen, sollen also Unberechtigten gegenüber anonym bleiben. Außerdem soll das unberechtigte Lesen der persistent gehaltenen Daten in der Datenbank des Systems vermieden werden. Auch hier gilt die Forderung nach der Anonymität der Personen auf die sich die Daten beziehen. So ist es beispielsweise notwendig, dass ein Kunde, der das Bankensystem nutzt, gegenüber weiteren Akteuren des Systems unbekannt ist, sofern dies nicht explizit erlaubt ist. Die Person soll also nicht aus den persistent gehaltenen Daten ermittelbar sein.

Die Anonymität stellt ein Sicherheitsinteresse dar, welches über das Sicherheitsinteresse der Vertraulichkeit von Daten abgedeckt wird. Aus diesem Grund entsprechen die für die Wahrung der Anonymität genutzten Sicherheitsmechanismen den Sicherheitsmechanismen für die Wahrung der Vertraulichkeit. Diese Sicherheitsmechanismen werden im Abschnitt 1.5.3.7 beschrieben, worin die Wahrung der Vertraulichkeit erläutert ist.

1.5.3.2. Wahrung der Authentizität

Die Authentizität wird für das Bankensystem gefordert, da zum einen die Benutzer des Systems korrekt identifiziert werden müssen. Das bedeutet, dass für das System eine korrekte Zuordnung des Benutzers zu einer Person notwendig ist. Zum anderen ist es für die Akteure des Systems notwendig, dass der Zugang zum System über eine bereitgestellte Verbindung authentisch ist. Hierbei muss erstens sichergestellt werden, dass eine von einem Benutzer aufgerufene Internetseite über dem Webbrowser dem Banken-


1.5.3.3. Wahrung der Autorisierung


1.5.3.4. Wahrung der Integrität

können zwei verschiedene Arten der Manipulation der systembezogenen Daten genannt werden. Zum einen können die Daten, die für die Verarbeitung an das System gesendet werden, manipuliert werden. Zum anderen können die Daten in dem System manipuliert werden. Ein Beispiel für die Notwendigkeit der Wahrung der Integrität beim Senden von Daten ist, dass die Durchführung einer Überweisung, die von einem Kunden mittels eines Client-Systems ausgelöst wurde, in der vom Kunden vorgesehenen Form durchgeführt werden soll. Es sollen dazu die vom Kunden eingegabenen Daten, wie das Quell-, das Zielkonto, der Verwendungszweck, sowie der zu überweisende Betrag unverändert zum Server-System, also zum Bankensystem, übertragen werden. Bei diesem Vorgang ist zu beachten, dass aufgrund der Übertragung der Daten über das Internet, die Daten durch beliebige Rechner zur Weiterleitung vom Client zum Server verarbeitet werden können. Somit besteht potentiell die Gefahr, dass die Daten an diesen Rechnern manipuliert werden. Zur Wahrung der Integrität sollen die Daten in der vorgesehen Form verarbeitet werden. Dies bedeutet, dass die bei der Eingabe spezifizierten Konten durch den eingegebenen Betrag aktualisiert werden und der Vorgang in der Datenbank gespeichert wird. Ein Beispiel zur Wahrung der Integrität bezüglich der Daten des Systems ist, dass der Kontostand eines Kunden, der in der Datenbank gespeichert ist, nicht auf unberechtigte Weise verändert werden soll.


1.5.3.5. Wahrung der Nachweisbarkeit


Die Einsicht der erstellten Log-Dateien in der Benutzeroberfläche konnte allerdings aus zeitlichen Gründen nicht der Spezifikation entsprechend umgesetzt werden. Beispielsweise konnte für die Rolle Geschäftsführer die Einsicht der Log-Daten nicht implementiert werden.
1.5.3.6. Wahrung der Verfügbarkeit

Verfügbarkeit bedeutet, dass das Bankensystem zu den spezifizierten Zeiten für die Benutzer genutzt werden kann. Die Nutzung bezieht sich auf die Funktionen des Systems, weshalb die Verfügbarkeit fordert, dass die Funktionen ausgeführt werden können und dass diese der Spezifikation entsprechend umgesetzt werden können. Die Funktionen müssen also nicht nur ausführbar sein, sondern müssen zudem korrekte Ergebnisse liefern. Für das Bankensystem ist die Verfügbarkeit ein sehr wichtiges Interesse, da die Geschäfte einer Bank häufig über das Internet getätigt werden. Fallen die Funktionen des Systems aus, so fallen auch potentielle Einnahmen aus Geschäften für die Bank weg. Außerdem kann durch den Ausfall der Funktionen die Reputation der Bank geschädigt werden, weshalb auch hier mit negativen finanziellen Folgen zu rechnen ist.


1.5.3.7. Wahrung der Vertraulichkeit


Die Gewährleistung der Vertraulichkeit während der Übertragung der Daten erfolgt mit Hilfe einer Verschlüsselung der Daten in der bereits im Abschnitt 1.5.3.2 beschriebenen SSL-Verbindung. Hierbei wird die symmetrische und asymmetrische Verschlüsselung in der hybriden Verschlüsselung kombiniert. Zur asymmetrischen Verschlüsselung wurde

Zur Wahrung der Vertraulichkeit für die persistent gehaltenen Daten, wurde die in Abschnitt 1.5.3.3 beschriebene rollenbezogene Rechtevergabe eingesetzt. Somit lässt sich die Einsicht der Daten derart kontrollieren, dass nur berechtigte Personen Zugang zu diesen Daten haben. Eine weitere Maßnahme zur Wahrung der Vertraulichkeit betrifft den im Abschnitt 1.5.3.4 beschriebenen SQL-Injection-Angriff. Da ein SQL-Injection-Angriff nicht nur die Daten des Systems manipulieren, sondern auch den unberechtigten Zugang zu den Daten ermöglichen kann, ist die im Abschnitt 1.5.3.4 beschriebene Maßnahme zum Schutz vor SQL-Injection-Angriffen auch für die Wahrung der Vertraulichkeit relevant. Die nicht berechtigte Einsicht der Daten wird deshalb möglich, weil bei einem Angriff nicht nur SQL-Befehle zum Schreiben, sondern auch zum Lesen von Daten eingegeben werden können.

1.5.3.8. Vermeidung von nicht-spezifiziertem Verhalten


### 1.5.4. Verwaltung der RSA-Schlüssel

Im Folgenden wird die Verwaltung der *RSA*-Schlüssel beschrieben, die für die Verwaltung der in Abschnitt 1.5.3 beschriebenen Sicherheitsmaßnahmen digitale Signierung und Verschlüsselung notwendig ist. Da der *RSA*-Algorithmus für beide Maßnahmen verwendet wird, werden in beiden Maßnahmen *RSA*-Schlüssel eingesetzt.


1.6. GUI Testen durch Selenium

Autor: CW

1.6.1. Einführung


1.6.2. Selenium IDE


1.6.3. Selenium RC

Mit Hilfe von Selenium RC(Remote Control Server) kann auch ein Test auf einer entfernten Maschine erfolgen. Die Architektur der Anwendung Selenium RCs ist in Abb. 1.11 dargestellt. Um die Oberfläche zu testen muss ein bestimmter Selenium-Core in den Browser eingebunden werden.

1.6.4. Problem mit SSL-Zertifikate


\[3\]siehe den Abschnitt 1.6.5

39
war, zeigte der Browser eine entsprechende Fehlermeldung. Diese führte letztlich dazu, dass der Test mit Selenium abgebrochen wurde. Um dieses Problem zu lösen, musste innerhalb von Firefox das verwendete Browserprofil geändert oder ein Neues erstellt werden. Im Folgenden wurde immer die Kombination aus Selenium und Firefox verwendet.

1.6.4.1. Einstellungsvorgang

Durch den Befehl “firefox.exe -ProfileManager“ ist ein neues Firefoxprofil in einem bestimmten Verzeichnis anzulegen, so dass beim nächste Mal der Selenium-Test mit dem neuen Profil gestartet wird. Dafür ist es nötig mit diesen Befehlen aus der Selenium API das neue Firefox-Profil zu konfigurieren:

“java -jar selenium-server-2.19.0.jar -trustAllSSLCertificates -firefoxProfileTemplate [Pro
filspeicherpfad]“
Das Argument "-trustAllSSLCertificates" spielt dabei eine große Rolle. Mit diesem Attribut wird auch der Zugang zu Webseiten ohne gültiges Zertifikat erlaubt.

1.6.5. Selenium Testen in Form von JUnit

Der Test der GUI der Webanwendung kann auch ohne die Selenium IDE durchgeführt werden. Dazu muss die entsprechende Library (Selenium-JAVA-API) im Projekt aufgenommen werden. Anschließend können die JUnit-Codes auch manuell erstellt werden. Dieser Code besteht aus drei Teilen, die mit der Annotation \@ gekennzeichnet werden:

@Before Zuerst werden alle für den Test nötigen Vorbereitungen getroffen werden. Darunter fällt z.B. die Instanziierung des Browser, sowie die Eingabe der Ziel-URL.

@Test Hierin befindet sich der eigentliche Test. In diesem Teil werden die aufzurufenden GUI-Seiten sowie Klicks programmiert.

@After Im After-Teil findet die Verifikation des Tests statt. Darunter fällt z.B. die Prüfung, ob die korrekte Seite aufgerufen wurde, oder ob Layout-Fehler während des Test aufgetreten sind (siehe Abbildung 1.13). Tritt ein solcher Fehler auf, wird der laufenden Test unterbrochen und die entsprechende Fehlermeldung wird in der Konsole ausgegeben. Tritt kein Fehler auf, läuft der Test bis zum Ende durch (siehe Abbildung 1.12).
1.7. Log-System mit Log4J

Autor: YD

1.7.1. Komponenten


1.7.1.1. Logger


Beispiel-Code:

```java
Logger l = Logger.getLogger("wecker");
l.setLevel(Level.ERROR);
l.debug("Jetzt wird geweckt.");
l.info("Guten Morgen.");
l.warn("Du solltest langsam aufstehen!");
l.error("Es ist ein unerwarteter Fehler aufgetreten!");
l.fatal("Das war’s. Du kommst zu spät zur Arbeit!");
```


1.7.1.2. Appender

Beispiel-Code:

```java
log4j.rootLogger=DEBUG,myapp,A1
log4j.appender.myapp=org.apache.log4j.RollingFileAppender
log4j.appender.myapp.file=/home/LogDatei.log
log4j.appender.myapp.maxFileSize=10MB
log4j.appender.myapp.maxBackupIndex=10
log4j.appender.myapp.layout ConversionPattern=%5p | %d | %F:%L | %m%n

log4j.appender.A1.layout ConversionPattern=%5p | %d | %F:%L | %m%n
```


1.7.1.3. Layouts

Die Komponente Layout bestimmt die Form der zu erstellenden Meldungen. Dazu wird vor Anzeige der Meldungen durch den Appender die Form dieser durch eine Layout-Komponente zugeordnet. Die Zuordnung wird in Konfigurationsdateien definiert. Beispiele:

- `% -5p` linksbündig mit fünf Zeichen die Priorität der Meldung ausgegeben.
- `[ % t ]` Ausgeben von welchem Thread aufgerufen ist.
- `( % F:% L )` Name und Zeilennummer der Methode.
1.7.1.4. log4j.properties

In jedem Projekt, in dem Log4j verwenden werden soll, muss zuerst eine properties-Datei erstellt werden. Diese ist für die Einstellungen von Log4j notwendig. Die properties-Datei definiert unter anderem die Komponenten, die von Log4j verwendet werden sollen, und wie die Meldungen anzuzeigen sind ([1.7.1.2] [1.7.1.3]).

1.7.2. Besondere Konfiguration mit JSF und Spring unter Glassfish


Beispiele:

log4j.logger.com.acme=DEBUG
log4j.logger.org.springframework=DEBUG
log4j.logger.jsf=DEBUG
log4j.logger.org.apache.myfaces=DEBUG
log4j.logger.com.sun.faces=DEBUG

1.7.3. LogDaten


1.7.3.1. LogDatei.log

1.7.3.2. Log-Datei in Konsole

Ein Beispiel für Meldungen, die in der Konsole der Entwicklungsumgebung angezeigt werden, ist in Abbildung 1.14 dargestellt.

Abbildung 1.14.: Anzeige von Meldungen in der Konsole der Entwicklungsumgebung
2. Compliance

Autor: TS

2.1. Gesetze


2.1.1. Behandlung der Gesetze nach dem Projektplan

Das ursprüngliche Vorgehen war folgendermaßen geplant:

1. Extraktion der wichtigsten Artikel mit Bezug zum Online-Banking-System aus diesen Texten.
3. Modellierung der Rechte und Pflichten mit Secure Tropos [33].
5. Ergänzung der Anwendungsfalldiagramme durch zusätzliche Metainformationen in Form von Tabellen (eine je Anwendungsfall).
7. Um die geltenden Gesetze im System zurückverfolgen zu können, wurde eine Notation der Gesetzesanforderungen für jeden modellierten Prozess festgelegt. Dann sollte die Notation der Prozesse in dem Architekturentwurf die Zurückverfolgbarkeit herstellen.
2.1.2. Betrachtete Gesetze


Die übrigen Gesetze sind:

- KonTraG [2]
- AktG [10]
- KWG [3]
- WpHG [4]
- HGB [15]
- AO [12]
- LDSG [5]
- TMG [1]

2.1.3. Analyse und Dokumentation der Gesetze


- Gesetz (entspricht dem Kürzel des jeweiligen Paragrafen)
- Was (entspricht dem betroffenen Objekt)
- Wer (entspricht dem handelnden Akteur)
- Anforderung (entspricht den zusätzlichen Anforderungen an das System)
- Gesetzestext (Kurze Zusammenfassung des Paragrafen)

Ebenfalls abweichend vom Projektplan wurde auf die Notation mit SecureTropos verzichtet, da keine brauchbare Entwicklungsumgebung gefunden werden konnte.

Parallel zur Erstellung der Tabelle wurde das Pflichtenheft erstellt. Dort sind die Anwendungsfalldiagramme [17] für die Rollen des Systems modelliert. Für jeden Anwendungsfall wurde eine zusätzliche Tabelle erstellt, die unter anderem die Zeile “Gesetze“
beinhaltet. In dieser Zeile sind die relevanten Gesetze und Paragrafen für den jeweils betrachteten Anwendungsfall aufgelistet. Somit konnte eine Referenzierung der Gesetze und Paragrafen in die tabellarischen Anwendungsfallsbeschreibungen integriert werden.

Zu der tabellarischen Beschreibung wurde im Pflichtenheft die Prozessmodellierung ergänzt, sodass ein Prozess pro Anwendungsfall vorhanden ist. Mit Hilfe der Referenzierung auf die relevanten Gesetze in der Anwendungsfallsbeschreibung ist also zusätzlich eine Referenzierung in der Prozessmodellierung vorhanden.

### 2.1.4. Anforderungen durch Gesetze

Durch einige Gesetze ergaben sich zusätzliche Anforderungen an das System.

So fordert das HGB bestimmte Aufbewahrungsfristen für Unterlagen, die bestimmte Vorgänge oder deren Zustandekommen dokumentieren.

Das BDSG fordert, dass personenbezogene Daten wie Name, Adresse, Geburtsdatum und Bankverbindungen nur erhoben werden dürfen, wenn ein Grund dafür vorliegt und auch nur solange gespeichert werden dürfen, wie dieser Grund besteht.

Durch das TMG wurden insbesondere Anforderungen an die Sicherheit der Datenübertragung und die Lagerung von Daten definiert.

Die MaRisk fordern das erstellen einer Security Policy, sowie im Zusammenspiel mit dem KWG einen Zugang für BaFin und BZSt.


AktG und KonTraG richten sich auf die Struktur von Aktiengesellschaften aus und hatten somit keine Auswirkungen auf unser System.

### 2.2. Security Policy


Dazu war vorgesehen sie in drei Schichten zu entwerfen:

1. Die erste Schicht (BSI 100-1) sollte Management-Prinzipien, Ressourcen, Mitarbeiter und den Sicherheitsprozess beinhalten.

2. In der zweiten Schicht (BSI 100-2) sollte die Vorgehensweise für den Betrieb der Software beschrieben werden.
3. Die dritte Schicht (BSI 100-3) sollte aus den Handbüchern für die vorgesehenen Nutzer des Systems bestehen.

In den folgenden Unterabschnitten werden die Ergebnisse zusammengefasst. Die Dokumente der Security Policy sind diesem Dokument im Anhang beigefügt.

2.2.1. IT-Sicherheitsleitlinie (Security Policy Schicht 1, BSI 100-1)

Die IT-Sicherheitsleitlinie (Anhang C.1) beschreibt, wie im Allgemeinen sichergestellt werden soll, dass im Betrieb alle nötigen Gesetze und Standards eingehalten werden. Sie behandelt unter anderem die Themen:

1. Allgemeine Ziele
2. Geltungsbereich
3. Verantwortlichkeiten und Zuständigkeiten
4. Sicherheitsmanagement
5. Sicherheitsmaßnahmen
6. Richtlinien für Mindeststandards


2.2.2. BSI-Grundschutz (Security Policy Schicht 2, BSI 100-2)


Die Bausteine sind für die folgenden Themen beschrieben:

1. Übergreifende Aspekte
2. Infrastruktur
3. IT-Systeme
4. Netze
5. Anwendungen


2.2.3. Handbücher (Security Policy Schicht 3, BSI 100-3)


Insbesondere soll die dritte Schicht der Security Policy solchem Fehlverhalten vorbeugen, das zu Sicherheitslücken oder Gesetzeswidrigkeiten führt. Die Handbücher sind deshalb so ausgelegt, dass sie auch als Nachschlagewerk dienen können.

Teil II.

Abweichungen vom Pflichtenheft
3. Abweichungen vom Pflichtenheft

Autor: AV, MW, DS

In diesem Kapitel geht es um die Abweichungen zwischen dem implementierten System und den Zielen, die sich die PG555 in dem Pflichtenheft vorgenommen hat. Es wird erklärt, was bis jetzt erreicht wurde. Die Rollen, die im Pflichtenheft beschrieben wurden, werden lediglich mit deren Funktionalitäten aufgelistet. Insbesondere werden wir darauf eingehen, welche Unterschiede es zwischen der Spezifikation und der Implementierung gibt, mit Begründung, warum es zu diesen Abweichungen gekommen ist. Schließlich werden die Funktionalitäten aufgelistet, die nicht implementiert worden sind. Anschließend werden auch die automatisierten Prozesse dargestellt und zwar die, die nicht als Anwendungsfall bei den Rollen vorgekommen und erklärt worden sind.


3.1. Kommunikationsschnittstellen

3.1.1. Kommunikation mit der Schufa


3.1.2. Börse und Bafin


3.1.3. Interbank

Die Kommunikation mit der Interbank, also das Versenden von Überweisungen und Lastschriften an andere Banken, wurde in der ersten Phase der PG geplant. Die Spezifikationen der Schnittstelle wurden erst zu Beginn der zweiten Phase der PG bekannt gegeben. Danach wurden bis Ende Januar die Spezifikationen in Zusammenarbeit mit den Betreuern auf die Anforderungen des Pflichtenhefts reduziert und angepasst.

Die Spezifikationen und die ursprüngliche Planung waren leider widersprüchlich, so dass erneute Planung notwendig wurde, zudem ging der Interbank-Server, der vom Lehrstuhl bereitgestellt werden sollte, erst in der Mitte der zweiten Phase in Betrieb. Es gab zudem Probleme den Cloud der PG555 aufzusetzen, da durch lange Verzögerung die ursprünglich ausgewählte IRB für die Bereitstellung der Server (Hardware) nicht mehr in Frage kam, wurden die Server (Hardware) vom Lehrstuhl bereitgestellt. Hieraus entstanden große Verzögerungen in der Implementierung der Interbank-Komponente.

Der letzte Stand der Interbank-Kommunikation ist, dass die EBICS-Nachrichten mit den abgesprochenen Zustands-Tags gelesen und erstellt werden können. Das Versenden und Empfangen der Nachrichten ist auch implementiert, jedoch traten immer wieder Probleme mit den Zertifikaten auf, die nicht behoben werden konnten.

Die Interbank-Nachrichten für Lastschriften (FIToFICstmrDrcftDbt), Überweisungen (FIToFICstmrCdtTrf), Retourüberweisungen und Rücklastschriften (PmtRtr) sowie Statusreports (FIToFIPmtStsRpt) können in vereinfachter Form auch gelesen, evaluiert, verarbeitet und versendet werden.

3.2. Rollen und deren Funktionalitäten

3.2.1. Kundenberater

Autor: MW

In diesem Unterkapitel werden alle Funktionen, die einem Kundenberater erlaubt sind, mit den im Pflichtenheft spezifizierten Funktionen verglichen. Wenn es eine Funktion gibt, die sowohl von Kundenberater als auch von anderen Akteuren benutzt werden kann, wird so eine Funktion nur in dem Unterkapitel beschrieben.

Dieses Unterkapitel besteht aus drei Teilen. Im ersten Teil werden die Funktionen aufgelistet, die entsprechend der Beschreibung im Pflichtenheft implementiert wurden.
Im zweiten Teil werden die Funktionen erläutert, die von der Spezifikation abweichen. In diesem Teil wird es auch begründet, wie diese Abweichungen zustande gekommen sind. Im letzten Teil werden Funktionen aufgelistet, die aus den oben genannten Gründen nicht implementiert werden können.

- Bereits implementierte Funktionen ohne Abweichung:
  - Aufgaben im Workflowsystem bearbeiten
  - Ausloggen
  - Dauerauftrag ändern
  - Dauerauftrag löschen
  - Dauerauftrag tätigen
  - Einloggen
  - Geld abbuchen
  - Geld einzahlen
  - Kontaktdaten ändern
  - Konto entsperren
  - Kontoentsperrung beantragen
  - Konto eröffnen
  - Konto schließen
  - Kontosperrung ausführen
  - Kontoparameter ändern
  - Kunden anlegen
  - Kunde löschen
  - Lastschrift stornieren
  - Lastschrift tätigen
  - Nachricht verschicken
  - Schecks einreichen
  - Überweisung tätigen

- Bereits implementierte Funktionen mit Abweichung:
  - Buchungen einsehen:
    Der Akteur kann alle verfügbaren Buchungen einsehen, aber hat keine Möglichkeit
Buchungen aus einem bestimmten Zeitraum abzurufen.

– Kontostand einsehen:

• Nicht implementierte Funktionen – Banking:
  – Internationale Überweisung tätigen:
    Da es noch keine Möglichkeit gibt, eine Transaktion mit einer internationalen Bank auszuführen, wird diese Funktion nicht implementiert.
  – Konto sperren:
    Kundenberater als Akteur kann diese Funktion ausführen, aber das System nicht.
  – Karte beantragen:
    Da dieses System nur prototypisch implementiert ist und es keine Möglichkeit Karte einzusetzen gibt, wurde diese Funktion nicht implementiert.
  – Karte sperren:
    Da keine Karte angelegt wird, wird diese Funktion auch nicht implementiert.

• Nicht implementierte Funktionen – Börse (Begründung siehe Kapitel 3.1.2)
  – Automatische Order
  – Depotinformationen einsehen
  – Finanzinstrumente kaufen
  – Finanzinstrumente verkaufen
  – Kurse einsehen
  – Order löschen

• Nicht implementierte Funktionen (Begründung siehe Kapitel 3.1.2)
  – Nachricht lesen

3.2.2. Kunde

Autor: MW

Laut Pflichtenheft gibt es eine Spezialisierung unter den Akteuren, die bewirkt, dass der spezielle Akteur (Kundenberater) alle Anwendungsfälle ausführen kann, die der generelle Akteur (Kunde) auch ausführen kann. Zusätzlich gibt es zwei Anwendungsfälle, die der Kunde ausführen kann. [32]

• Nicht implementierte Funktionen:
– Empfängerdaten auswählen
– Empfängerdaten speichern

3.2.3. Geschäftsführer

Autor: AV

Im Folgenden wird auf die Funktionen, die ein Geschäftsführer bedienen darf, eingegangen. Wie es im Pflichtenheft definiert ist, übernimmt ein Geschäftsführer alle Funktionen, die auch von einem Kundenberater, Jurist, Eigenhändler, Controlling-Mitarbeiter oder Produktentwickler ausgeführt werden. Deswegen werden die Anwendungsfälle, die bereits bei der Rolle Kundenberater (siehe Kapitel 3.2.1) betrachtet werden, nicht berücksichtigt, da sie genau so für die Rolle Geschäftsführer funktionieren. Es gibt einen Anwendungsfall, der nur von einem Geschäftsführer ausgeführt werden darf.

• Nicht implementierte Funktionen:
  – Limits setzen

3.2.4. Produktentwickler

Autor: AV

Die folgenden Anwendungsfälle – Ausloggen, Einloggen, Nachrichten lesen und Nachrichten verschicken – sind im Abschnitt 3.2.1 beschrieben und funktionieren genau so auch für die Rolle Produktentwickler. Demnach werden diese hier nicht beschrieben. Außerdem darf laut Pflichtenheft ein Produktentwickler:

• Nicht implementierte Funktionen
  – Anonymisierte Daten einsehen

3.2.5. Controlling-Mitarbeiter

Autor: AV


• Bereits implementierte Funktionen ohne Abweichung:
  – Logs einsehen
• Bereits implementierte Funktionen mit Abweichung:
  – Fachabteilung stellt Daten bereit:
    Die Daten, die von dem Jurist angefragt wurden, werden ausgewählt, extra-
    hiert und per Post an den Juristen geschickt.

• Nicht implementierte Funktionen:
  – Liste mit verdächtigen Finanzinstrumentstransaktionen prüfen

3.2.6. Kassierer

Autor: AV

Laut Pflichtenheft darf ein Kassierer sich einloggen und ausloggen, Geld auszahlen, Geld
einzahlen und den Kontostand einsehen. Diese Anwendungsfälle werden bereits im Ab-
schnitt 3.2.1 berücksichtigt und funktionieren ohne einen Unterschied. Aufgrund dessen
werden sie in diesem Abschnitt nicht weiterverfolgt.

3.2.7. Jurist

Autor: DS

Die Anwendungsfälle Nachrichten lesen und Nachrichten verschicken funktionieren ge-
nauso wie sie bei dem Kundenberater, Kapitel 3.2.1 beschrieben worden sind. Weiter
folgt eine Auflistung der

• bereits implementierten Funktionen ohne Abweichung:
  – Kontosperrung beantragen
  – Konto entsperren
  – Titel mit Pfändung und Vollstreckung eintragen
  – Liste mit verdächtigen Überweisungen prüfen
  – Antrag auf Entsperrung bestätigen bzw. ablehnen
  – Aufgaben im Workflowsystem bearbeiten

• bereits implementierten Funktionen mit Abweichung:
  – Bonität des Kunden von der Schufa einholen
    Hierfür wurde eine Dummy-Klasse erstellt, die mit einer Wahrscheinlichkeit
    von 99 % eine positive Auskunft liefert.
  – Informationen über große Kredite erhalten (siehe Bonität)

• nicht implementierten Funktionen:
  – Kontodatenliste beantragen
Dieser Anwendungsfall wurde durch die Aufgaben im Workflowsystem gelöst. Ein Jurist darf nur dann die für ihn relevanten Kunden- und Kontendaten einsehen, wenn er vorher eine Aufgabe erstellt hat und diese von einem Kunden genehmigt wurde. Der andere Fall ist, wenn vom Kundenberater eine Aufgabe, wie z.B. Bonität prüfen, erstellt wurde. Im diesem Fall werden die Daten des Kunden mitgeschickt und dem Jurist zur Einsicht freigegeben.

3.2.8. System

Autor: DS

In diesem Unterkapitel werden die von System automatisiert ausgeführten, bereits implementierten, Funktionen aufgelistet, bzw. die Funktionen die laut Spezifikation automatisiert ausgeführt werden sollten, nur als Gründe, die in der Einleitung (vgl. Kapitel 3) angegeben wurden, nicht oder mit kleinen Abweichungen, umgesetzt worden sind.

- Bereits implementierte Funktionen ohne Abweichung:
  - Logs erstellen
  - Überweisung auf Gültigkeit prüfen

- Bereits implementierte Funktionen mit Abweichung:
  - Block von Lastschrift erhalten
  - Block von Lastschrift verschicken
  - Block von Überweisung erhalten
  - Block von Überweisung verschicken
  - Internationale Überweisung auf Gültigkeit prüfen
  - Lastschrift prüfen
    Zu den oberen sechs Anwendungsfällen siehe Kapitel 3.1.3
  - Zinsen buchen
    Zinsen werden einmal pro Tag berechnet aber nicht abgebucht. Grund dafür ist, dass es kein Dispoüberziehung geprüft wird.

- Nicht implementierte Funktionen:
  (vgl. Kapitel 3 und 3.1.2)
  - Börsentransaktionen der Bank / des Kunden durchführen
  - Dispoüberziehung Prüfen
  - Gegenlastschrift Veranlassen
  - Limits prüfen
– Überweisung auf Verdächtigkeit prüfen
– Kontostammdaten historisieren

3.2.9. Systemadministrator

Autor: DS


- Bereits implementierte Funktionen ohne Abweichung:
  - Konfiguration des Systems
  - Starten
  - Nutzerrechte/Nutzer anlegen, löschen, vergeben
  - RSA Schlüssel ändern
  - Backup einspielen
  - Aktuellen Systemstatus einsehen
  - Logs einsehen
  - Backup erstellen

- Bereits implementierte Funktionen mit Abweichung:
  - Logs auswerten:

3.2.10. Eigenhändler

Autor: DS

Diese Rolle besitzt die Funktionen, die der Kundenberater auch hat (vgl. Kapitel [3.2.1]). Deswegen werden sie hier nicht detailliert beschrieben.

3.2.11. Marketing

Autor: DS

Bei dieser Rolle kommen Anwendungsfälle – Einloggen, Ausloggen, Aufgaben in Workflowsystem bearbeiten, Nachrichten lesen, Nachrichten verschicken – die in Abschnitt 3.2.1 schon beschrieben wurden. Zusätzlich gibt es einen Anwendungsfall – Anonymisierte Daten einsehen – der im Kapitel 3.2.4 erklärt wird.

Aufgrund dessen wird bei der Marketing-Abteilung nicht auf die oben genannten Funktionen weiter eingegangen.

3.3. Automatisierte Prozesse

Autor: DS


Die bankinternen automatisierten Prozesse sind:

- bereits implementierte Funktionen ohne Abweichung:
  - Retourüberweisung eintragen
  - Stornogebühren abbuchen
  - Zinsen und Kontoführungsgebühren verbuchen

- bereits implementierte Funktionen mit Abweichung:
  - System Testen:
Teil III.

Maßnahmen und Erfahrungen
4. Maßnahmen des Managements

Autor: RH

4.1. Projektmanagement

Dieses Kapitel befasst sich mit allgemeinen Problemen in einem Projekt. Entsprechende Lösungen, die während des Projektes ausgearbeitet wurden, werden vorgestellt.

4.1.1. Zusammenfassung des Projektmanagements im Projektplan

Im Projektplan werden zwei Phasen des Projektes beschrieben, wobei sich die Phasen an die Semester anordnen, in denen das Projekt stattfand. Die erste Phase betrifft die Planung des zu erstellenden Banksystems, während die zweite Phase dessen Umsetzung, also Implementierung, Test und Dokumentation berücksichtigt. Die erste Phase wurde in folgende Arbeitspakete (abgekürzt AP) eingeteilt, wobei die einzelnen Arbeitspakete voneinander abhängen [33]:

1. AP Projektplan
2. AP Anforderungsanalyse
3. AP Spezifikation
4. AP Pflichtenheft
5. AP GUI-Entwurf
6. AP Technologieauswahl
7. AP Architekturrentwurf

Die Vorgehensweise in der zweiten Phase unterscheidet sich von der Vorgehensweise in der ersten Phase dadurch, dass die Methode Extreme Programming (XP) [27] verwendet wurde, wobei nicht alle Praktiken davon vollständig durchgeführt wurden. Dies liegt daran, dass die Möglichkeit einer räumlichen Nähe fehlte und fachliche Qualifikationen nicht hinreichend vorhanden waren. Deshalb wurde vor allem auf die Praktiken Räumlich Zusammensitzen und Komplettes Team verzichtet und die Praktik Wochenzyklus etwas abgewandelt (siehe Kapitel 4.3).

Die Vorteile von Extreme Programming liegen vor allem in der inkrementellen und in der testgetriebenen Entwicklung, die die Qualität des Systems steigern sollen. Außer-
dem wird dadurch im Gegensatz zu anderen Entwicklungsmodellen, wie zum Beispiel dem Spiralmodell [31], mehr Zeit eingespart. Die Mitglieder suchen sich die Aufgaben selbstständig aus, so dass das Zuteilen von Aufgaben nicht notwendig ist. Im Falle, dass ein Mitglied keine Aufgaben bearbeitet, wird ihm eine der vorhandenen Aufgaben zugewiesen. Falls es mehr Aufgaben als Mitglieder geben sollte, werden Prioritäten festgelegt bzw. nach Möglichkeit Aufgaben gruppiert, so dass die Schwierigkeit der einzelnen Aufgaben auf einem ähnlich hohen Niveau ist [33].

4.1.2. Vorgehen in der zweiten Projektphase


4.1.2.1. 1. Teilphase

1.1 GUI
1.2 Programmskelett
1.3 Datenbank
1.4 Schnittstellen


Nach der Fertigstellung der ersten Teilphase wurde folglich ein vollständiges Gerüst des Systems angelegt. Die restlichen Teilphasen erweitern die leeren Klassen um Funktionalitäten.
4.1.2.2. 2. Teilphase

2.1 Authentifikation und Authorisierung
2.2 Kontodatenkomponente
2.3 Kundendatenkomponente


4.1.2.3. 3. Teilphase

3.1 Transaktionskomponente
3.3 Zinskomponente
3.4 Kreditkomponente


Bei der Kreditkomponente handelt es sich um die Verwaltung der Kredite, die als Konto im System angelegt werden. Hierbei prüft das System die Kreditkonten auf die Einhaltung der Konditionen und meldet notfalls Unstimmigkeiten an eine bestimmte Rolle.

4.1.2.4. 4. Teilphase

4.1 Börsenkomponeente


4.1.2.5. 5. Teilphase

5.1 Backup
5.2 Replikationsserver

Die fünfte Teilphase beinhaltet die Komponente, die für das Backup des Systems verantwortlich ist. Dazu zählt sowohl das Erstellen, als auch das Einspielen des Backups auf den Spiegelserver. Der Replikationsserver, der Kontostammdaten für die BaFin und BZSt bereitstellt wird ebenfalls in dieser Teilphase erstellt und vor allem das Übertragen der Kontostammdaten auf diesen Server verwaltet.

4.1.2.6. 6. Teilphase

6.1 Systemangelegenheiten

Unter Systemangelegenheiten fallen vor allem die Funktionen, die der Systemadministrator erledigt. Außerdem beinhaltet die Teilphase das Einbinden von Business Process Mining und das automatische Erkennen von Anomalien im System.
4.2. Teammanagement

Im Folgenden wird auf das Thema Teammanagement während der gesamten Projekts eingegangen. Hierzu werden die im Projektplan (33) genannten Maßnahmen erwähnt, die im Projekt durchgeführten Maßnahmen vorgestellt und schließlich einen Rückblick, der den Erfolg der Methoden bewertet.

4.2.1. Zusammenfassung des Teammanagements im Projektplan

Im Projektplan wurde für das Teammanagement ein Konfliktmanagement innerhalb der Gruppe geplant. Dieses beinhaltet die Maßnahmen Konflikte rechtzeitig zu erkennen, richtig zu analysieren und konstruktiv zu bearbeiten. Ziel dieser Maßnahme ist vor allem das Arbeitsklima zu verbessern und die Zufriedenheit innerhalb der Gruppe zu erhalten.


Der Projektplan sah weiterhin Konflikttypen bezüglich eines möglichen Vergehens einzelner Projektmitglieder vor, um mögliche Konsequenzen zu ermitteln. Die Konflikttypen sind:

1. Leichte Vergehen (z.B. Verspätungen zu Treffen) ohne weitere Konsequenzen, außer bei wiederholten Vergehen mit der Konsequenz einer zusätzlichen Arbeitszuteilung
2. Mittlere Vergehen (z.B. Arbeitsverweigerung) mit der Konsequenz einer Abmahnung, wobei drei Abmahnungen einem schweren Vergehen entsprechen
3. Schwere Vergehen (z.B. bei dauerhafter Arbeitsverweigerung) mit der Konsequenz, dass ein Ausschluss der Person aus der PG angestrebt wird


4.3. Qualitätsmanagement

Qualitätsmanagement sollte in der gesamten Laufzeit des Projekts angewandt werden, um so nicht nur die Qualität des zu erstellenden Systems, sondern auch die Qualität der herangezogenen Prozesse sicherzustellen.

4.3.1. Zusammenfassung des Qualitätsmanagements im Projektplan


4.3.1.1. Qualitätsziele

Die Qualitätsziele sollen für jedes Arbeitspaket (AP) die Zeitpunkte festmachen, an denen eine erfolgreiche Erreichung des Ziels vom Paket erkennbar ist. Es wurden folgende Qualitätsziele bezüglich der Arbeitspakete festgelegt [33]:

1. AP Projektplan: Vollständigkeit; Korrektheit
2. AP Anforderungsanalyse: Vollständigkeit; Einhaltung der Compliance; Betrachtung aller Sicherheitsrisiken
3. **AP Spezifikation**: Vollständigkeit; Korrektheit der Diagramme; Einhaltung der Compliance

4. **AP Prozessmodellierung**: Vollständigkeit; Korrektheit der Diagramme; Schutz der Daten; Schutz der Personen

5. **AP GUI erstellen**: Benutzbarkeit der GUI; Vollständigkeit; Korrektheit; Robustheit

6. **AP Technologieauswahl**: Vollständigkeit; Notwendigkeit; Konsistenz; Einfachheit

7. **AP Architekturentwurf**: Vollständigkeit; Korrektheit; Robustheit; Zuverlässigkeit; Schutz

8. **AP Zwischenbericht**: Vollständigkeit; Korrektheit

9. **AP Implementierung und Test**: Vollständigkeit der Tests, der Komponenten, der Dokumentation; Korrektheit; Verständlichkeit des Codes; Zuverlässigkeit; Schutz; Effizienz; Robustheit gegen Angriffe; Robustheit unter Last

10. **AP Endbericht**: Vollständigkeit des Endberichts; Korrektheit

In jedem Arbeitspaket wird das Qualitätsziel **Vollständigkeit** geprüft, wobei dieses Ziel für jedes Paket einzeln definiert werden musste, indem man einen Sollwert vorgibt. Dieser Sollwert wird beim Messen mit dem gemessenen Istwert verglichen, um den Grad der Vollständigkeit zu ermitteln.

### 4.3.1.2. Qualitätsmechanismen

Als Qualitätsmechanismen zur Sicherstellung und Überprüfung der Qualitätsziele wurden folgende Verfahren herausgestellt [33] [44]:


- **Goal-Question-Metric-Ansatz**: Anhand von Qualitätszielen, werden Fragen herausgearbeitet, die an die jeweilige Phase gestellt werden, um schließlich daraus Metriken abzuleiten und zu messen. Der Vorteil liegt in der Messung nur sinnvoller Metriken und soll Zeit und Kosten sparen.

- **Statische Codeanalyse**: Ein Programmcode wird mit Hilfe eines automatischen Tools einer Prüfung unterzogen, in der vor allem syntaktische Fehler gefunden
werden. Außerdem werden Merkmale gefunden, die häufig einen Fehler verursachen oder die Verständlichkeit des Codes beeinträchtigen.


- **Style Check**: Ein *Style Checker* soll die Verständlichkeit des Programmcodes verbessern, indem die für das Projekt definierten Konventionen auf ihre Einhaltung geprüft werden.

### 4.3.2. Vorgehensweise im Qualitätsmanagement während des Projektes

In der ersten Phase der Entwicklung, die alle Arbeitspakete vor der Implementierung enthält, wurden drei Qualitätsmechanismen Review, Inspektion und Goal-Question-Metric-Ansatz (GQM) angewandt.

#### 4.3.2.1. AP Projektplan


Die Vollständigkeit des Projektplans wurde allerdings nicht erreicht, da die angenommenen Sollwerte falsch waren, was dazu führte, dass der Projektplan dreimal überarbeitet werden musste.

#### 4.3.2.2. AP Anforderungsanalyse

Bei der Anforderungsanalyse gab es die Schwierigkeit, dass die Vollständigkeit und auch die Korrektheit der herausgestellten Anforderungen nicht klar überprüft werden konnten. Dies liegt vor allem daran, dass es wesentlich von der Eigeninterpretation abhängt.


*Qualitätsziel: Vollständigkeit*
Frage 1: Gibt es Unklarheiten, die im Lastenheft auftauchen?

Metrik 1: Anzahl Unklarheiten pro Anforderung
Falls Unklarheiten bei einer gefundenen Anforderung existieren, bedeutet das, dass eine Anforderung möglicherweise unvollständig ist. Dies hat zur Folge, dass Fragen an den Kunden formuliert werden müssen.

Qualitätsziel: Korrektheit
Frage 1: Sind die extrahierten Anforderungen auch so im Lastenheft vorhanden?
Metrik 1: Anzahl überflüssiger Anforderungen

Frage 2: Sind Anforderungen in sich stimmig? Gibt es keine Konflikte?
Metrik 1: Anzahl Anforderungen insgesamt
Metrik 2: Anzahl Inkonsistenzen zwischen den Anforderungen

Bei diesen Metriken war das Ziel die Konsistenz zu messen. Wurde mindestens eine Inkonsistenz gefunden, so mussten die Anforderungen überarbeitet und einem erneuten Inkonsistenzcheck unterzogen werden.

4.3.2.3. AP Spezifikation


Wegen Zeitmangel konnte das GQM-Verfahren nicht durchgeführt werden, was auch an der Qualität des Pflichtenheftes bemerkbar war. Die Qualitätsziele Vollständigkeit und Korrektheit konnten beim Pflichtenheft erst nach mehreren Review- und Inspektionsdurchläufen sichergestellt werden.

4.3.2.4. AP GUI-Entwurf

Beim GUI-Entwurf wurden mehrere Reviews durchgeführt und somit versucht die Qualität der GUI, vor allem im Hinblick auf die Benutzerbarkeit zu optimieren. GQM-Ansatz konnte bei diesem Qualitätsziel sinnvoll zum Einsatz gebracht werden, indem die Elemente und ihre Anordnung betrachtet wurden. Dabei wurden Sollwerte für die Anzahl

**Qualitätsziel: Benutzbarkeit**

*Frage 1:* Ist die GUI intuitiv zu bedienen?

*Metrik 1:* Anzahl Buttons pro Seite

*Metrik 2:* Anzahl Textfelder pro Seite

*Metrik 3:* Anzahl Menüeinträge in der Navigation

*Metrik 4:* Anzahl Beschreibungen pro Seite

Bei diesem Qualitätsziel gab es die Idee, dass zu viele Elemente auf einer Seite den Benutzer überfordern würden. Um dies zu verhindern messen die Metriken die Anzahl der Elemente pro Seite. Die Schwellen für die Anzahl an Elementen weichen bei unterschiedlichen Seiten von einander ab.

### 4.3.2.5. AP Zwischenbericht

Beim Zwischenbericht wurden Reviews von mindestens drei unabhängigen Personen durchgeführt, um so die Vollständigkeit und Korrektheit gewährleisten zu können. In besonders schwierigen Fällen, wie z.B. wenn ein Teiltext durch jemanden mit Migrationshintergrund geschrieben wurde, erfolgte meist ein weiteres Review durch eine weitere Person. Diese stand dann entsprechend auch bei Fragen zur deutschen Sprache bereit.

Da auch die Abgabe des Zwischenberichtes erst nach mehrmaligen hin und her schicken zwischen Projektgruppe und Betreuer erfolgen konnte, wurden die Anmerkungen seitens der Betreuer protokolliert und korrigiert. Bei den darauffolgenden erneuten Reviews wurde insbesondere auf die Einhaltung der Korrekturwünsche der Betreuer geachtet, um eine möglichst zufriedenstellende Version des Zwischenbericht abzugeben.

### 4.3.2.6. Qualitätssicherung während der Entwicklung

Die zweite Phase wurde nach dem Vorgehensmodell *eXtreme Programming (XP)* organisiert, wobei sie die Implementierung, die Dokumentation und den Test des Systems beinhaltet. Da nach *XP* der Ansatz *Test First* vorgeschlagen wird, wurden die BlackBox-Tests, die über Schnittstellen die Anforderungen testen, vor dem Code erstellt. Zusätzlich wurden Reviews durch das vier-Augen Prinzip durchgeführt. Dabei wurden die Paare, die eine Programmieraufgabe zusammen bearbeiteten, am Anfang eines Programmierabschnitts festgelegt. So könnte z.B. eine Person den Test erstellen und die Andere die Implementierung. Allerdings wurden die Reviews gegenseitig ganz nach dem Motto *check before check-in* durchgeführt, was bedeutet, dass die größten Fehler
beseitigt wurden, bevor eine Integration ins Hauptsystem erfolgte. Eine Abwandlung ist, dass die Iterationen nicht in einem Wochenzyklus angesetzt sind, da eine Woche für die meisten Iterationen zu kurz zu sein schien. Stattdessen wurden zwei- oder dreiwöchige Iterationen durchgeführt.

Nach dem lokalen Check des Programmcodes, konnte ein zentraler Integrationstest durchgeführt werden, wobei für noch unfertige Komponenten Mock-Up-Objekte erstellt wurden. Dabei dienten diese Objekte als Stellvertreter für unfertige Klassen und boten nur sehr begrenzte Funktionalität, so dass das System immer lauffähig blieb und so eine Continuous Integration durchgeführt werden konnte.

4.4. Risikomanagement

Bei Gruppen, die neu zusammengesetzt werden, wie bei einer Projektgruppe, kann es zu sehr vielen unvorhergesehenen Ereignissen kommen, die ein Risiko für die Erreichung des festgelegten Ziels darstellen. Diese Risiken zu erkennen und Strategien für die Beherrschung dieser zu entwickeln, ist das Ziel des Risikomanagements.

4.4.1. Zusammenfassung des Risikomanagements im Projektplan

Im Projektplan wurden die folgenden vier Stufen des Risikomanagements vorgestellt [33].

1. Risikoerkennung
2. Risikoanalyse
3. Risikoplanung
4. Risikoüberwachung

Diese einzelnen Phasen sollen im Weiteren Verlauf genauer betrachtet werden.

4.4.1.1. Risikoerkennung

Bei der Risikoerkennung ist die hauptsächliche Aufgabe, mögliche Risiken vor dem Eintreten zugehöriger Störungen zu erkennen. Im Projektplan wurden folgende Risiken als relevant für die Projektgruppe identifiziert.

- Personalausfall
- Konflikte zwischen den Mitgliedern
- Schlechte Moral bei den Mitgliedern
- Sprachliche Barrieren
Tabelle 4.1: Risikoanalyse: Je nach Schaden, den der Eintritt eines Risikos mit sich bringt und dessen Eintrittswahrscheinlichkeit, wird die Gefahr des Risikos durch ein Ampelsystems angezeigt.

<table>
<thead>
<tr>
<th>Schaden bei Eintritt</th>
<th>Eintrittswahrscheinlichkeit</th>
<th>Mittel (wahrscheinlich 25%-75%)</th>
<th>Hoch (Sehr wahrscheinlich &gt;75%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tolerierbar</td>
<td>Wenig wahrscheinlich (&lt;25%)</td>
<td>Grün</td>
<td>Grün</td>
</tr>
<tr>
<td>Ernst</td>
<td>Grün</td>
<td>Gelb</td>
<td>Gelb</td>
</tr>
<tr>
<td>Katastrophenal</td>
<td>Gelb</td>
<td>Rot</td>
<td>Rot</td>
</tr>
</tbody>
</table>

- Zeitverzug
- Technische Risiken

4.4.1.2. Risikoanalyse

Bei der Risikoanalyse werden die im ersten Schritt identifizierten Risiken bezüglich ihrer Eintrittswahrscheinlichkeit und bezüglich des Schadens, der durch eine risikobasierte Störung entsteht, bewertet. Dabei zog man Tabelle 4.1 heran, die ein Ampelsystem verwendet, um die Bedeutung der Risiken für den Projekterfolg zu veranschaulichen[33].


4.4.1.3. Risikoplanung

Bei der Risikoplanung ist das Ziel die erkannten und analysierten Risiken, so zu behandeln, dass die Eintrittswahrscheinlichkeit und auch die Schwere des Schadens beim Eintritt reduziert wird. Es mussten im Voraus Risikobehandlungsmaßnahmen[33] getroffen werden. Diese Maßnahmen sind:
- Risikovermeidung: Ein bestimmtes Projektrisiko beseitigen.
- Risikoverminderung: Die Eintrittswahrscheinlichkeit eines Risikos verringern.
- Risikobegrenzung: Den Schaden eines Risikos verringern.
- Risikoverlagerung: Projektrisiken auf Dritte übertragen.

4.4.1.4. Risikoüberwachung


4.5. Bewertung der Maßnahmen

4.5.1. Projektmanagement

Prinzipiell war die Einteilung in kleinere Teilphasen ein gutes Vorgehen. Auf diese Art und Weise wurden einmal am Anfang der Planung die Abhängigkeiten zwischen den einzelnen Teilphasen bestimmt und so die AP’s aufgeteilt. Befürchtungen, dass es Abhängigkeiten gibt, die nicht betrachtet wurden und so später zu Problemen führen könnten, bewahrheiteten sich nicht. Letztlich konnten leider nicht alle Arbeitspakete abgearbeitet werden. Was von den oben genannten Arbeitspaketen realisiert wurde, kann aus Teil II Abweichungen vom Pflichtenheft entnommen werden.

4.5.2. Teammanagement


Auf das strukturierte Diskutieren mit der Bildung von zwei Gruppen wurde bei Meinungsverschiedenheiten verzichtet, da sich die Diskussionen immer in einem zeitlich akzeptablen Rahmen bewegten. Als einziger Punkt der Maßnahme zum strukturierten
Diskutieren aus dem Projektplan wurde der Mehrheitsentscheid angewandt, da es sich als eine gute Entscheidungshilfe nach einer offen geführten Diskussion herausgestellt hat. Durch die völlige Akzeptanz durch die Mitglieder wurden aufwendigere Verfahren zur Abstimmung und Diskussionsführung nicht angewandt.

Die Maßnahme zum Überblicken des Gesamtkontexts des Projekts wurde während der Treffen durch die Mitglieder praktiziert. So konnte die erste Phase des Projekts in den geplanten Arbeitspaketen abgearbeitet werden, auch wenn Änderungen der Arbeitspakete nicht verhindert werden konnten.


Die Maßnahme zur Strukturierung der regelmäßigen Treffen wurde vom Projektplan angewandt. Es hat sich dabei herausgestellt, dass durch die Strukturierung eine effiziente

Innerhalb der zweiten Phase stellte sich heraus, dass die Protokollierung durch das bisher angewandte Verfahren keinen großen Nutzen mehr hatte. Über die Zeit der Entwurfsphase wurden in jedem Treffen Protokolle erstellt, die festhielten, was beschlossen wurde, und wie welche Arbeiten verteilt wurden. Dies brachte in der Phase der Implementierung nur wenig, da sich jeder selbst Aufgaben aus einem Aufgabenpool nahm und diese bearbeitete. Somit wandelten sich die Ansprüche an die Protokolle, denn es mussten auch eine technische Dokumentation erfolgen. Aus diesem Grund wurde diverse andere Protokollierungsverfahren angewandt und die bisherigen Protokolle lediglich bei Treffen mit den Betreuern weitergeführt.

4.5.3. Qualitätsmanagement


4.5.4. Risikomanagement

Das Risikomanagement erwies sich als eine der schwierigsten Aufgaben, die in einem Projektalltag durchgeführt werden müssen. Dies lag vor allem daran, dass keiner von den Teilnehmern der Projektgruppe jemals damit Erfahrungen gemacht hat.

Die Risiken wurden zwar, soweit es geht, erkannt, die Analyse und die Planung der Behandlungsmaßnahmen waren aber eine ziemlich große Herausforderung. Im Folgenden sollen die einzelnen Risiken und ihre Behandlung vorgestellt werden.
4.5.4.1. Personalausfall


4.5.4.2. Konflikte zwischen den Mitgliedern


4.5.4.3. Sprachliche Barrieren

Da von den zehn Teilnehmern der Projektgruppe, sieben einen Migrationshintergrund aufweisen und fünf davon sprachliche Probleme haben, ist die Wahrscheinlichkeit von sprachlichen Schwierigkeiten in der Kommunikation und Erstellung von Dokumenten bei etwa 50%. Der Schaden, der dadurch entsteht ist bezüglich Tabelle 4.1 katastrophal, was auch direkte Auswirkungen auf den Zeitverzug hat. Deshalb wird dieses Risiko im roten Bereich eingeschätzt. Die einzige Möglichkeit, die wir sehen ist eine Risikoverlagerung durchzuführen, wobei sprachintensive Aufgaben, wie z.B. das Verfassen von Texten, von den übrigen Teilnehmern erledigt werden.

4.5.4.4. Zeitverzug

Auch bei diesem Risiko sehen wir uns im roten Bereich. Dies führt dazu, dass wichtige Dokumente meistens mit Wochen Verspätung abgegeben werden. Die Risikobegrenzung
war die Nutzung der vorlesungsfreien Zeit als Puffer und die Einführung von *Powertagen*, an denen die Gruppe sich ganztägig trifft. Damit wird Zeit eingespart, was daran liegt, dass Fragen in der Gruppe persönlich geklärt wurden und langwieriger E-Mail-Austausch vermieden wurde. Außerdem konnten Entscheidungen so viel schneller und effizienter getroffen werden.
5. Erfahrungen

Autor: VM


Autor: CW


Autor: RH


Autor: TS

Während der Arbeit an dem umfangreichen Projekt, ein cloudbasiertes Internetbanking-System zu planen und zu implementieren, habe ich für einiges zur langfristigen Arbeit innerhalb einer Gruppe feststellen können. Besonders auffällig war in diesem Projekt die Planung, da hiermit noch niemand Erfahrungen gesammelt hatte und sie die Hälfte des Aufwandes für das Projekt ausmachte. Es kam immer wieder die Situation auf, dass etwas modelliert werden musste, von dem zu dem Zeitpunkt niemand so wirklich wusste was es war, so wurde z.B. die Struktur der Konto- und Transaktions-Klassen stark verändert, nachdem bekannt wurde, wie die Transaktionen übermittelt werden müssen. Oder dass etwas ausgewählt werden musste, das trotz hohem Zeitaufwand nicht ausreichend gestestet werden konnte. Einige der Tools, die allen unbekannt waren stellten sich als nicht oder zumindest nicht für Arbeit im Team brauchbar heraus und mussten durch andere Tools oder geschickte Organisation ersetzt werden. Insbesondere das Einarbeiten in die Gesetzestexte und die Modellierung der Gesetze war sehr aufwendig, da wir zur Extraktion wichtiger Passagen keine Hilfsmittel oder für uns verständliche Vorgehensweisen finden konnten und für deren Darstellung keine für die Bearbeitung in einer Gruppe geeignete Software vorhanden war.

Eine zweite große Problematik innerhalb der Planung bestand aus der Kommunikation

In der Implementierungsphase, die die zweite Hälfte des Projekts ausmachte, habe ich viel über das Programmieren an sich und den Einsatz von Frameworks gelernt. Das Lernen und Einarbeiten kostete viel Zeit, da zu den meisten Anforderungen und Frameworks wenig oder kein Vorwissen vorhanden war.

**Autor: JK**


Als Problem hat sich das verteilte Arbeiten herausgestellt. Das und die Komplexität des Systems stellte sich als eine große Hürde im Verlauf der Projektgruppe. Die räumliche Nähe war deshalb sehr wichtig, um Lösungen schnell auszudiskutieren zu können und Fragen in der Gruppe zu klären. Für mich hat sich herausgestellt, dass für verteiltes Arbeiten man ein sehr großes Vertrauen in die Fähigkeiten und Zuverlässigkeit der Teilnehmer benötigt, was bei einer wild zusammengewürfelten Gruppe nicht möglich ist.

Nach den Erfahrungen in der Projektgruppe bin ich zum Entschluss gekommen, dass eine lockerer und respektvoller Umgangston sehr wichtig für die Produktivität ist. Zusätzlich spielt die Erfahrung eine wichtige Rolle, denn theoretisches Wissen reicht oft nicht aus, da die Praxis oft ganz anders aussieht.

**Autor: VS**

In der PG habe ich viel über die Projektplanung und das Zeitmanagement gelernt. Circa die Hälfte der gesamten Projektzeit wurde für die Planung und Vorbereitung aufgewendet, was ich zuerst für übertrieben hielt. Im nachhinein denke ich aber, dass eine Planungsphase sehr wichtig ist, vor allem weil bei dem Projekt viele Bereiche berücksichtigt werden mussten, in denen alle PG-Teilnehmer noch keine Erfahrungen hatten, wie z.B. Compliance und Gesetze in Bezug auf Cloud-Systeme und Online-Banking. Es fand zwar am Anfang des Projektes eine Seminarphase statt, in der solche Themen vorge stellt wurden, aber hier wurde nur ein Überblick gegeben und nicht zu sehr ins Detail gegangen. Deswegen waren lange Einarbeitungen in neue Gebiete während des Projektes immer wieder nötig, durch die ein Zeitverzug entstanden ist. Auch bei der Bearbeitung von Aufgaben sind Probleme entstanden, da häufig Fragen aufgetaucht sind, die trotz

Autor: YD


Autor: MW

noch mehr zeitliche Verzögerung führen. In der Entwicklungsphase habe wir sehr viel mit neue Technologien zu tun gehabt. Es hat viel beigekommen aber hat auch zur Verzögerung geführt. Ohne irgendwelche Erfahrung mit jeweilige Technologien eine System wie dieses zu Implementieren ist sehr aufwändig gewesen, aber auf der Stand, wo wir jetzt bezüglich Implementierung als Gruppe sind, ist meiner Meinung nach sehr gut.

Autor: AV

Im Rahmen der Projektgruppe 555 hatte ich die Möglichkeit, viel über Teamarbeit und Projektplanung zu lernen. Bereits am Anfang habe ich festgestellt, dass ein gutes Zeitmanagement sehr wichtig ist, damit ein Projekt rechtzeitig und erfolgreich abgeschlossen werden kann. Das Problem des Zeitmanagements stellte innerhalb unserer Projektgruppe mit das größte Problem dar. Sowohl während der ersten, als auch während der zweiten Phase des Projekts hatte wir Probleme mit der Zeitplanung. Ein Grund dafür waren vor allem die fehlenden technischen Erfahrungen und die mangelnde Koordination des Projektes, was mit vielen Recherche-Arbeiten und Einarbeitung verbunden war.

Die Recherchen sowie den Einarbeitungsaufwand sehe ich persönlich dennoch nicht als Nachteil, da auf diese Weise ich die Möglichkeit hatte, neue Technologien kennenzulernen, praktische Erfahrung zu sammeln und zu lernen, wie eine Projektgruppe funktioniert, wo Risiken auftreten können und was dagegen unternommen werden kann.

Autor: DS

Arbeiten in einer Gruppe ist meistens eine sehr große Herausforderung, da man mit vielen, in der Regel, unterschiedlichen Personentypen mit unterschiedlichen Erfahrungen, zusammen ein Projekt erfolgreich abschließen möchte. Während dieser Projektgruppe (PG) war dies einer der Hürden, die uns ab und an ins Schwierigkeiten gebracht hatte. Aber nichtsdestotrotz war dieses vergangene Jahr eine schöne und reichliche Erfahrung und Vorbereitung fürs Berufsbild.

Während dieser PG, hatte man, neben der obebgenannten nicht technischen Erfahrung, auch mit reichlich vielen technischen Neuigkeiten zu tun gehabt, die man sicherlich mit ins Berufsleben mitnehmen könnte. Puncto Sicherheit in einer Cloud z.B. und das aufsetzen dieser oder aber auch die Vielzahl an Gesetzen, die man sich in der Planungsphase aneignen musste.

Diese erste Phase, die ein wesentlicher Teil unserer für die PG verbrauchte Zeit ausmachte, wurde meiner Meinung nach, sehr ausführlich seitens meiner Kommilitonen verfasst und erklärt. Ich kann mich nur ihrer Meinung anschließen.

Während der Implementierungsphase könnte man zwar die Fehler, die man in der ersten Phase, aufgrund mangelnder Erfahrung, gemacht hatte, vermeiden, aber gegen die Zeit konnten wir leider nicht kämpfen und deshalb waren nicht in der Lage manche Sachen so umzusetzen, wie sie Anfangs geplant waren.

Schließlich waren die Organisation, die Koordination und die Kommunikation und die Schwierigkeit mit zehn Personen sie zu beherrschen und die Ruhe dabei zu bewahren, die drei weitere wesentliche Sachen, die diese PG ausgemacht haben.
Teil IV.

Anhang
A. Anwender Dokumentation

Autor: CW,DY
Korrektor: TS,DS

A.1. Einleitung

In den folgenden Kapiteln wird für die einzelnen Rollen beschrieben, welche Vorgänge das System unterstützt und wie der Nutzer mit unserem System arbeiten soll.

A.2. Voraussetzungen zur Nutzung

Die Online-Banking-Software ist im Internet unter der folgenden Adresse verfügbar: https://129.217.47.73:8181/OnlineBankingNeu/faces/login.xhtml. Um das System zu nutzen, benötigen Sie einen Internet-Browser, der JAVA, JavaScript und SSL unterstützt. Im Prinzip sollen alle modernen Browser, z.B. Microsoft Internet Explorer oder Mozilla Firefox, die genannten Anforderungen erfüllen. Um die Sicherheit zu erhalten, ist es notwendig den Browser durch regelmäßige Updates immer auf dem aktuellen Stand zu halten.

A.3. Benutzeroberfläche

Die Benutzeroberfläche, die man nach dem Login erreicht, ist in drei Teile unterteilt:


A.4. Gemeinsame Funktionen

In diesem Abschnitt werden die Funktionen des Systems aufgeführt, die alle Nutzer ausführen können.

A.4.1. Ein- und Ausloggen

Nachdem Sie die Adresse des Online-Banking-Systems aufgerufen haben, kommen Sie auf die Login-Seite (s. Abb. A.2). Geben Sie Ihr Password und Ihren Benutzernamen in die dafür vorgesehenen Felder ein und bestätigen Sie Ihre Eingabe mit dem Login-Button.


Abbildung A.1.: Ausloggen
Unser System ist rollenbasiert, das heißt, dass es mehrere Rollen gibt, die jeweils bestimmte Funktionalitäten nutzen können.

Nachdem Sie sich eingeloggt haben, müssen Sie zuerst eine Rolle auswählen, um die ihr zugeordneten Funktionen ausführen zu können. Insgesamt sind zehn verschiedene Rollen wie folgt klassifiziert [32].

1. Kunde: Kunde der Bank
2. Kundenberater: Mitarbeiter der Bank, die als Kundenbetreuer in einer Filiale arbeiten
3. Controlling-Mitarbeiter: Mitarbeiter der Bank, die in der Controllingabteilung arbeiten
4. Eigenhändler: Mitarbeiter der Bank, die in der Eigenhandelsabteilung arbeiten
5. Geschäftsführer: Der Geschäftsführer der Bank.
10. Systemadministrator: Mitarbeiter der Bank, der als Systemadministrator arbeitet.

Das Rolle-Wechseln erfolgt durch Klick auf das Rollenmenü in der oberen rechten Ecke der Seite in Abb. A.3.
A.4.3. Nachrichtenverkehr

Das Banking-System bietet die Möglichkeit zwischen Mitarbeitern oder zwischen Mitarbeiter und Kunde Nachrichten zu verschicken.


Abbildung A.3.: Rolle wechseln

Abbildung A.4.: Nachrichten im Navigationsbereich und Nachricht lesen
A.5. Kunde

Autor: CW

Als Kunde sehen Sie nach dem Einloggen Ihre Benutzeroberfläche wie in Abb. A.7. Der Navigationsbereich zeigt die folgenden Einträge:

1. Online-Banking
   - Überweisung
   - Lastschrift
   - Dauerauftrag
   - Kontostand einsehen
   - Buchungen einsehen

2. Börseangelegenheiten
   - Finanzinstrument handeln
   - Depot einsehen

Abbildung A.5.: Nachricht verschicken für den Kunden
Abbildung A.6.: Nachrichten versenden für Mitarbeiter

Abbildung A.7.: Kunden-Portal

- Orderbuch
3. Persönliche Daten
4. Nachrichten
  - Nachrichten lesen
  - Nachrichten versenden
5. Kurse
  - Kurse einsehen

98
Die Unterpunkte in der Aufzählung sind die Unterpunkte der entsprechenden Einträge im Navigationsbereich.

Im folgenden werden die Funktionen an die Navigation angelehnt beschrieben.

**A.5.1. Banking**

In den folgenden Unterabschnitten werden alle Funktionen beschrieben, die unter **Banking** eingeordnet sind.

**A.5.1.1. Überweisung**

Über den Menüpunkt **Überweisung** gelangen Sie zur Ansicht **Überweisung tätigen** (s. Abb. [A.8]).

Die Felder dieser Ansicht haben die folgenden Funktionen:

2. Empfänger speichern: Wenn Sie hier das Häkchen setzen, wird der Empfänger für Ihren Account gespeichert.
3. Zielkonto/IBAN: Hier tragen Sie die IBAN des Zielkontos ein oder die Kontonummer für Inlandsüberweisungen.
4. BLZ/SWIFT: Hier tragen Sie die SWIFT zur IBAN oder die BLZ zur Kontonummer ein.
5. Verwendungszweck: Hier tragen Sie den Verwendungszweck ein.

**A.5.1.2. Lastschrift**

Über den Menüpunkt **Lastschrift** gelangen Sie zur Ansicht **Lastschrift tätigen** (s. Abb. [A.9]).

Die Felder dieser Ansicht haben folgende Funktionen:

1. Zahlungspflichtiger: Name des Zahlungspflichtigen
2. Zahlungspflichtigen speichern: Wenn Sie hier das Häkchen setzen, wird der Zahlungspflichtige für Ihren Account gespeichert.
3. Zielkonto/IBAN: Hier tragen Sie die IBAN des Zielkontos ein oder die Kontonummer für Inlandsüberweisungen.
4. BLZ/SWIFT: Hier tragen Sie die SWIFT zur IBAN oder die BLZ zur Kontonummer ein.

5. Verwendungszweck: Hier tragen Sie den Verwendungszweck ein.


A.5.1.3. Dauerauftrag

Über den Menüpunkt Dauerauftrag gelangen Sie zur Ansicht Dauerauftrag (s. Abb. A.10).

Die Felder dieser Ansicht haben die folgenden Funktionen:

2. Empfänger speichern: Wenn Sie hier das Hänchen setzen, wird der Empfänger für Ihren Account gespeichert.
3. Zielkonto/IBAN: Hier tragen Sie die IBAN des Zielkontos ein oder die Kontonummer für Inlandsüberweisungen.
4. BLZ/SWIFT: Hier tragen Sie die SWIFT zur IBAN oder die BLZ zur Kontonummer ein.
5. Verwendungszweck: Hier tragen Sie den Verwendungszweck ein.
10. Ausführungsintervall: Das Ausführungsintervall legt fest in welchen Abständen der Dauerauftrag gebucht wird.

A.5.1.4. Kontostand

Über den Menüpunkt Kontostand gelangen Sie zur Ansicht Kontostand einsehen (s. Abb. A.11).

Ihnen werden im oberen Teil der Ansicht Ihre Konten in tabellarischer Form angezeigt. In der Tabelle gibt es die Spalten Kontonummer, Eröffnungsdatum, Gesperrt und Kontostand. In der Spalte Gesperrt ist ein Wahrheitswert eingetragen (true für wahr, das Konto ist gesperrt oder false für falsch, das Konto ist nicht gesperrt).

Indem Sie in der Tabelle ein Konto auswählen und danach auf den Button Kontostand anzeigen klicken, wird Ihnen der Kontostand des ausgewählten Kontos detailliert angezeigt.
A.5.1.5. Buchungen einsehen

Über den Menüpunkt *Buchungen einsehen* gelangen Sie zur Ansicht *Buchungen* (s. Abb. A.12).

Ihnen werden im oberen Teil der Ansicht Ihre Konten in tabellarischer Form angezeigt. In der Tabelle gibt es die Spalten *Kontoinhaber*, *Kontonummer* und *Kontostand*.

Indem Sie in der Tabelle ein Konto auswählen und danach auf den Button *Konto auswählen* klicken, werden in einer Tabelle im unteren Teil der Ansicht die zum ausgewählten Konto gehörigen Buchungen angezeigt.
A.5.2. Börse

A.5.2.1. Finanzinstrument handeln

Über den Menüpunkt *Finanzinstrument handeln* gelangen Sie zur Ansicht *Finanzinstrument handeln* (s. Abb. [A.13]).

Die Felder dieser Ansicht haben die folgenden Funktionen:

2. WKN/ISIN:  .
3. Name: Hier wird der Name des Finanzinstruments angezeigt.
5. Anzahl: Hier tragen Sie Anzahl der Einheiten ein, die Sie handeln möchten.
7. Limit:  .
8. Gültig bis: Hier können Sie bestimmen, bis wann die Order bestehen soll.
9. Transaktionsart: Hier wählen Sie die Transaktionsart, also Verkauf oder Kauf.

Mit Betätigen des *Bestätigen* Buttons wird das Angebot an die Börse weitergeleitet. Um eine bestätigte Order zu stornieren lesen Sie im Abschnitt [A.5.2.3] nach.
A.5.2.2. Depotinformationen einsehen


Im oberen Teil der Ansicht werden in einer Tabelle Ihre Finanzinstrumente aufgelistet. Durch das Auswählen eines Finanzinstruments und anschließender Betätigung des *Handeln* Buttons gelangen Sie zur Ansicht *Finanzinstrument handeln* (s. Abschnitt A.5.2.1).
A.5.2.3. Orderbuch

Über den Menüpunkt Orderbuch gelangen Sie zur Ansicht Orderbuch (s. Abb. A.15).
Im oberen Teil der Ansicht werden Ihre aktuellen, offenen Order in einer Tabelle angezeigt.
Durch das Auswählen einer Order und anschließendes Betätigen des Stornieren Buttons können Sie eine Order stornieren.

Abbildung A.15.: Orderverwaltung

A.5.3. Persönliche Daten ansehen

In dieser Ansicht werden Ihre Kundennummer, Ihr Vorname, Nachname, Geburtsdatum, Geburtsort und Ihre Adresse mit Straße, Hausnummer, Postleitzahl und Ort angezeigt.
Mit Betätigung des Ändern Buttons erhalten Sie in der Ansicht Kontaktdaten ändern die Möglichkeit ihre Adresse zu ändern (s. Abschnitt A.5.3.1).

A.5.3.1. Kontaktdaten ändern

In der Ansicht Kontaktdaten ändern befinden sich die Felder Vorname, Nachname, Straße, Hausnummer, PLZ und Ort (s. Abb. A.17). Indem Sie die Einträge der Felder bearbeiten, ändern Sie die Kontaktdaten. Durch Betätigen des Buttons Bestätigen werden die Änderungen übernommen und gespeichert.
A.5.4. Nachrichten

Der Menüpunkt *Nachrichten* ist im Abschnitt A.4.3 beschrieben.

A.5.5. Kurse


In dieser Ansicht können Sie in dem Feld *WKN/ISIN* die WKN/ISIN eines Finanzinstruments eingeben. Daraufhin wird Ihnen der Name, der Typ, der aktuelle Kurswert, der mittlere Kurswert sowie die Durchschnittswerte der letzten Woche, des letzten Monats, des letzten Jahres und der durchschnittliche Wert seit dem ersten Kauf angezeigt.
Über den Handeln Button gelangen Sie zur Ansicht Finanzinstrument handeln, die in Abschnitt A.5.2.1 beschrieben ist.

Abbildung A.18.: Kurse einsehen

### A.6. Kundenberater

**Autor:** YD

Als Kundenberater sehen Sie nach dem Einloggen Ihre Benutzeroberfläche wie in Abb. A.19. Der Navigationsbereich zeigt die folgenden Einträge:

<table>
<thead>
<tr>
<th>Name</th>
<th>Kurs</th>
<th>Prozent</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAX</td>
<td>7.055.40</td>
<td>-12.3%</td>
</tr>
<tr>
<td>FAZ-INDEX</td>
<td>1.532.79</td>
<td>-13.2%</td>
</tr>
<tr>
<td>TecDAX</td>
<td>788.07</td>
<td>-1.97%</td>
</tr>
<tr>
<td>MDAX</td>
<td>10.528.60</td>
<td>-1.72%</td>
</tr>
<tr>
<td>SDAX</td>
<td>5.192.03</td>
<td>-0.55%</td>
</tr>
<tr>
<td>REX</td>
<td>419.95</td>
<td>-0.20%</td>
</tr>
<tr>
<td>EuroStoxx 30</td>
<td>2.583.39</td>
<td>-0.90%</td>
</tr>
<tr>
<td>P.A.Z. EURO INDEX 83.10</td>
<td>-0.93%</td>
<td></td>
</tr>
<tr>
<td>Dow Jones</td>
<td>13.239.10</td>
<td>+0.05%</td>
</tr>
<tr>
<td>Nasdaq 100</td>
<td>2.733.26</td>
<td>+0.75%</td>
</tr>
<tr>
<td>S&amp;P500</td>
<td>1.499.75</td>
<td>+0.40%</td>
</tr>
<tr>
<td>IBEX-35</td>
<td>10.419.53</td>
<td>+0.48%</td>
</tr>
</tbody>
</table>
1. Aufgaben
2. Kundenverwaltung
3. Nachrichten
   • Nachrichten lesen
   • Nachrichten verschicken
4. Kurse

Die Unterpunkte in der Aufzählung sind die Unterpunkte der entsprechenden Einträge im Navigationsbereich.

Im folgenden werden die Funktionen an die Navigation angelehnt beschrieben.

Abbildung A.19.: Kundenberaterportal

**A.6.1. Aufgaben**


Im oberen Teil der Ansicht werden unter *Im Auftrag gegebene Aufgaben*, in einer Tabelle die Aufgaben aufgelistet, die der Kundenberater erzeugt hat (z.B. die Überprüfung einer Person beim Eröffnen eines Kontos).


**A.6.2. Kundenverwaltung**

Abbildung A.20.: Aufgaben Übersicht

Abbildung A.21.: Aufgaben Details Übersicht

Im oberen Teil der Ansicht befinden sich die Felder Kontonummer, Kundennummer, Name und Vorname sowie der Filtern Button, dessen Funktion im Abschnitt A.6.2.1 beschrieben wird.

Im unteren Teil der Ansicht befindet sich eine Tabelle, in der die Kunden der Magnus Monetarun Bank aufgelistet sind und die Buttons Ändern (s. Abschnitt A.5.3.1) und Details anzeigen (s. Abschnitt A.6.2.4) in jeder Zeile und Details anzeigen (s. Abschnitt A.6.2.4), Kunde anlegen (s. Abschnitt A.6.2.2) und Bonität prüfen lassen (s. Abschnitt A.6.2.3).
Abbildung A.22.: Kundenverwaltung-Übersicht

A.6.2.1. Filtern


Abbildung A.23.: Kundenverwaltung mit Filter: ein Beispiel von Filter-Funktion mit Kontonummer 100000
A.6.2.2. Kunden anlegen

Wenn Sie in der Ansicht Kundenverwaltung Übersicht den Button Kunde anlegen betätigt haben, gelangen Sie zur Ansicht Kunden anlegen (s. Abb. A.24).

Hier tragen Sie in die entsprechenden Felder Vorname, Nachname, Titel, Geburtsdatum, Geburtsort, Straße, Hausnummer, PLZ, Ort und zweimal das Passwort des Kunden ein und legen dann den Kunden mit Betätigen des Bestätigen Buttons an.

![Abbildung A.24.: Beispiel: kundenanlegen](image)

A.6.2.3. Bonität prüfen

Wenn Sie in der Ansicht Kundenverwaltung Übersicht einen Kunden ausgewählt haben und anschließend den Button Bonität prüfen lassen betätigt haben, gelangen Sie zur Ansicht Bonität prüfen (s. Abb. A.25).

Um eine Bonitätsprüfung des im oberen Teil der Ansicht angezeigten Kunden zu veranlassen, müssen Sie die folgenden Felder ausfüllen:

- Beschreibung: eine kurze Beschreibung des Grundes der Prüfung
- Dringlichkeit: die Dringlichkeit der Prüfung ist mit einem der vorgegebenen Werte Niedrig, Mittel, Hoch oder Sehrhoch anzugeben. Ist die Dringlichkeit Sehrhoch, wird die Prüfung dieses Kunden bei Möglichkeit bevorzugt.
- Frist: der späteste Zeitpunkt, an dem das Prüfungsergebniss vorliegen muss
- Weitere Informationen: sollten zu den vorangegangenen Punkten zusätzliche Informationen relevant sein, können und müssen diese unter Weitere Informationen
eingetragen werden.

Durch betätigen des Buttons Absenden wird die Aufgabe erstellt und an die juristische Abteilung gesendet.

Abbildung A.25.: Beispiel: bonitätprüfen

A.6.2.4. Kundendetail-Ansicht

Wenn Sie in der Tabelle im unteren Teil der Ansicht Kundenverwaltung Übersicht einen Kunden auswählen und anschließend auf den Button Details anzeigen in der gleichen Zeile oder den gleichnamigen Button unterhalb der Tabelle betätigen, gelangen Sie in die Ansicht Kundendetail-Ansicht.

In der Kundentetail-Ansicht werden im oberen Teil der Ansicht die persönlichen Daten und die Kundennummer des Kunden angezeigt. Unter den persönlichen Daten befindet sich eine Tabelle mit den Konten des Kunden bei der Magnus Monetarius Bank. Durch das Auswählen eines Kontos in der Tabelle und das betätigen des Buttons Details in der gleichen Zeile oder des gleichnamigen Buttons unterhalb der Tabelle gelangen Sie zur Konto Detailansicht (s. Abschnitt A.6.2.5).

Weiter befinden sich folgende Buttons unterhalb der Konto-Tabelle:

- Durch das Betätigen des Buttons Kontosperrung beantragen wird eine Aufgabe erstellt und an die juristische Abteilung gesendet.
- Über den Button Nachricht schicken gelangen Sie zur Ansicht Nachricht versenden, die im Abschnitt A.4.3 beschrieben wird.
- Über den Button Konto eröffnen gelangen Sie zur Ansicht Konto eröffnen, in der Sie die, für die Eröffnung eines Kontos notwendigen Daten eintragen und ein neues Konto für den Kunden eröffnen können.
- Über den Button Kredit gewähren gelangen Sie zur Ansicht Kredit anlegen, in der Sie dem Kunden einen Kredit in einer bestimmten Höhe und über eine bestimmte Laufzeit mit festgelegten Raten gewähren können.
• Durch das Betätigen des Buttons Bonitätsprüfung gelangen Sie zur Ansicht Bonität prüfen, die im Abschnitt A.6.2.3 beschrieben wird.

• Der Button PuV ist für den Kundenberater deaktiviert.

• Über den Button Persönliche Daten ändern gelangen Sie zur Ansicht Kontaktdaten ändern, die im Abschnitt A.5.3.1 beschrieben wird.

• Durch betätigen des Buttons Kunde löschen wird der Kunde aus dem System gelöscht. Dies geschieht jedoch nur, wenn alle Konten des Kunden ausgeglichen sind.

• Über den Button Buchungen einsehen gelangen Sie zur Ansicht Buchungen, die im Abschnitt A.5.1.5 beschrieben wird.

• Über den Button Daueraufträge einsehen gelangen Sie zur Ansicht Daueraufträge einsehen, die im Abschnitt A.6.2.9 beschrieben wird.

• Über den Button Überweisung tätigen gelangen Sie zur Ansicht Überweisung tätigen, die im Abschnitt A.5.1.1 beschrieben wird.

• Über den Button Lastschrift tätigen gelangen Sie zur Ansicht Lastschrift tätigen, die im Abschnitt A.5.1.2 beschrieben wird.

• Über den Button Dauerauftrag tätigen gelangen Sie zur Ansicht Dauerauftrag, die im Abschnitt A.5.1.3 beschrieben wird.

Abbildung A.26.: Beispiel: kundendetailsanzeigen

A.6.2.5. Konto Detailsansicht

Zur Konto Detailansicht gelangen Sie wie Abschnitt A.6.2.4 beschrieben.

In der Unteransicht *Kundendaten* werden Ihnen Vorname, Nachname und Kundennummer des Kunden und Kontonummer, Bankleitzahl, Kontotyp und Kontostand des Kontos angezeigt (s. Abb. A.27).

Abbildung A.27.: kundendatenansicht


Abbildung A.28.: Zinsen-ansicht

Im unteren Teil der *Konto Detailansicht* befindet sich eine Tabelle, die mit *Karten*...
überschrieben ist. In dieser Tabelle werden die Karten mit *Kartennummer*, dem Gültigkeitsdatum *Gültig bis* und dem Wahrheitswert *Gesperrt* aufgelistet, die dem Kunden für das Konto ausgestellt wurden.

Unter der Tabelle befinden sich die folgenden Buttons:

- **Kontoparameter ändern**: Über den Button *Kontoparameter ändern* gelangen Sie zur Ansicht *Kontoparameter ändern*, die in Abschnitt A.6.2.6 beschrieben wird.
- **Karte beantragen**: Über den Button *Karte beantragen* wird eine Aufgabe erstellt, die für das Konto das Beantragen der Produktion einer Karte anstößt.
- **Karte sperren**: Durch das Auswählen einer nicht gesperrten Karte in der Tabelle und das anschließende betätigen des Buttons *Karte sperren* wird die ausgewählte Karte gesperrt.
- **Kontosperrung beantragen**: Über den Button *Kontosperrung beantragen* wird eine Aufgabe erstellt, und an die juristische Abteilung übermittelt.
- **Konto sperren**: Wurde durch die juristische Abteilung das Sperren des Kontos autorisiert, kann durch betätigen des Buttons *Konto sperren* das Konto gesperrt werden.
- **Konto schließen**: Wenn das Konto ausgeglichen ist, kann es durch Betätigen des Buttons *Konto schließen* geschlossen werden.
- **Geld einzahlen**: Über den Button *Geld einzahlen* gelangen Sie zur Ansicht *Geld einzahlen*, die in Abschnitt A.6.2.7 beschrieben wird.
- **Geld auszahlen**: Über den Button *Geld auszahlen* gelangen Sie zur Ansicht *Geld auszahlen*, die in Abschnitt A.6.2.8 beschrieben wird.

### A.6.2.6. Kontoparameter ändern

In der Ansicht *Kontoparameter ändern* können Sie das im oberen Teil der Ansicht mit den Feldern *Nachname*, *Vorname*, *Kontonummer*, *Kundennummer* und *Art des Kontos* beschriebene Konto verändern, indem Sie die Kontoparameter, die in Abschnitt A.6.2.5 erläutert werden, in den gleichbenannten Feldern neu setzten und die Eingaben mit dem Button *Bestätigen* bestätigen (s. Abb. A.29).

### A.6.2.7. Geld einzahlen

A.6.2.8. Geld auszahlen

A.6.2.9. Daueraufträge einsehen

In der Ansicht *Daueraufträge einsehen* befindet sich eine tabellarische Aufzählung der Daueraufträge des vorher ausgewählten Kunden und die Buttons *Bearbeiten* und *Löschen* (s. Abb. A.32).

Wenn Sie einen Dauerauftrag in der Tabelle auswählen und anschließend den Button *Bearbeiten* betätigen, gelangen Sie in die Ansicht *Dauerauftrag bearbeiten*, die in Abschnitt A.6.2.10 beschrieben wird.

Wenn Sie einen Dauerauftrag in der Tabelle auswählen und anschließend den Button *Löschen* betätigen, wird der ausgewählte Dauerauftrag gelöscht.

![Abbildung A.32.: Dauerauftrag einsehen](image)

A.6.2.10. Dauerauftrag bearbeiten

In der Ansicht *Dauerauftrag bearbeiten* können Sie den im oberen Teil der Ansicht *Dauerauftrag bearbeiten* den ausgewählten Dauerauftrag verändern.

A.6.3. Nachrichten

Der Menüpunkt *Nachrichten* entspricht Abschnitt A.4.3 für Mitarbeiter.

A.6.4. Kurse

In der Ansicht *Kurse* können die aktuellen Kursstände eingesehen werden (s. Abb. A.33).

Im oberen Teil der Ansicht können Sie in dem Feld *WKN/ISIN* die WKN (Wertpapierkennnummer) oder ISIN (International Securities Identifications Number) eingeben, woraufhin Ihnen Details zu dem entsprechenden Wertpapier angezeigt werden. Wenn Sie den Button *Handeln* betätigen, gelangen sie zur Ansicht *Finanzinstrument handeln* (s. Abschnitt A.5.2.1).
Im unteren Teil der Ansicht werden Ihnen bekannte Wertpapiere und deren aktueller Kurs aufgelistet.

Abbildung A.33.: kurseeinsehen
A.7. Kassierer

Als Kassierer sehen Sie nach dem Einloggen befindet sich im Navigationsmenü nur der Eintrag Kundenverwaltung (s. Abb. A.34), der in Abschnitt A.6.2 beschrieben wird. Jedoch ist die Ansicht des Kassierers auf die Funktionen Filtern (s. Abschnitt A.6.2.1) und Details anzeigen (s. Abschnitt A.6.2.4) eingeschränkt.

Die Ansicht Kundendetail-Ansicht ist für den Kassierer auf die Funktion der Buttons, die mit Details beschrieben sind und zur Konto Detailansicht (s. Abschnitt A.6.2.5) führen.

Die Konto Detailansicht ist auf die Funktionen Geld einzahlen (s. Abschnitt A.6.2.7) und Geld auszahlen (s. Abschnitt A.6.2.8) beschränkt.

Abbildung A.34.: kundenverwaltung
A.8. Produktentwickler

Autor: YD

Als Produktentwickler und Marketing-Mitarbeiter sehen Sie nach dem Einloggen Ihre Benutzeroberfläche wie in Abb. A.35. Der Navigationsbereich zeigt die folgenden Einträge:

1. Aufgaben
2. Statistische Daten
3. Nachrichten

Abbildung A.35.: Produktentwickler-Portal

A.8.1. Aufgaben


A.8.2. Statistische Daten


A.8.3. Nachrichten

A.9. Marketing-Mitarbeiter

Alle Funktionen, die Ihnen als Marketing-Mitarbeiter zur Verfügung stehen, entsprechen den Funktionen, die im Kapitel A.8 Produktentwickler beschrieben werden.

A.10. Controlling-Mitarbeiter

Autor: YD

Als Controlling-Mitarbeiter sehen Sie nach dem Einloggen Ihre Benutzeroberfläche wie in Abb. A.37. Der Navigationsbereich zeigt die folgenden Einträge:

1. Aufgaben
2. Kundenverwaltung
3. Logs einsehen
4. Nachrichten
5. Kurs einsehen


A.10.1. Aufgaben

Das Aufgabe-Workflow unter Controlling-Mitarbeiter sind identisch wie das Aufgabe-Workflow unter Kundenberater. (siehe Abschnitt Kundenberater A.6.1)
A.10.2. Kundenverwaltung

Die Kundenverwaltung unter Controlling-Mitarbeiter sind identisch wie die Kundenverwaltung unter Kundenberater. (siehe Abschnitt Kundenberater A.6.2)

A.10.3. Logs einsehen


A.10.4. Nachrichten

Das Nachrichtensystem unter Controlling-Mitarbeiter sind identisch wie Nachrichtensystem unter Kundenberater. (siehe Kapitel A.4.3)
A.10.5. Kurse einsehen

Die Funktion „Kurse einsehen“ unter Controlling-Mitarbeiter sind identisch wie Nachrichtensystem unter Kundenberater. (siehe Kapitel A.6.4)
A.11. Jurist

Autor: CW

In Abb. A.39 wird die Start Seite des Juristen angezeigt. Der Navigationsbereich zeigt die folgenden Einträge:

1. Aufgabenverwaltung
2. Kundenverwaltung
3. Kontodatenliste beantragen
4. Nachrichten
   - Nachrichten lesen
   - Nachrichten verschicken

Der Jurist-Mitarbeiter befasst sich mit der Überbrückungsfunktion zwischen Bank und staatlichen Behörden wie Bafin und BZST bei Anfrage von Kontodaten. Darüber hinaus lässt sich die Kundenverwaltung anhand der Sachverhalte durchführen oder mit den anderen Abteilungen (Controlling, Kundenberater) zusammenarbeiten.

Abbildung A.39.: Portal für Jurist-Mitarbeiter

A.11.1. Aufgaben einsehen

Der Jurist-Mitarbeiter kann sich durch Klick des Aufgaben Buttons sofort über juristische Aufgaben wie in Abb. A.40 informieren (siehe auch Abschnitt A.6.1).

A.11.2. Kundenverwaltung

A.11.3. Kontodatenliste beantragen

Solange der Jurist-Mitarbeiter von Bafin oder BZSt eine Anfrage zu kundenbezogenen Information von gewissen Konten bekommt, erhält er dabei eine Vorgangsnummer, um die nachfolgende Aktion *Kundendatenliste beantragen* zu bestätigen und identifizieren. Es gibt zwei Möglichkeiten die Kontodatenliste zu erstellen. Entweder auf gewisse (z.B. zeitliche, zahlungsmäßige) Bedingungen gerichtet die Buchungen eines Kontos auszusortieren oder direkt anhand der geforderten Kontonummer abzufragen und eine dementsprechende Kontodatenliste zu erstellen.

Abbildung A.41.: Kontodatenliste beantragen

A.11.4. Nachrichtenverkehr

Sehen Sie bitte den Abschnitt A.4.3.
A.12. Geschäftsführer

Autor: CW

Für Geschäftsführer hat das Online System auch die dafür benötigten Funktionen bereitgestellt. Die Ansicht von dem Geschäftsführer Portal ist wie in Abb. A.42 gezeigt. Der Navigationsbereich zeigt die folgenden Einträge:

1. Limits setzen
2. Aufgabenverwaltung
3. Kundenverwaltung
4. Logs einsehen
5. Kontodatenliste beantragen
6. Statistische Daten
7. Einstellung für verdächtige Überweisungen
8. Nachrichten
   • Nachrichten lesen
   • Nachrichten versenden
9. Kurse
   • Kurse einsehen

Abbildung A.42.: Start Seite für Geschäftsführer

A.12.1. Limits setzen

Limitsystem dient dazu, die potenziellen Widerrechtlichkeiten aus dem Eigenhandel zu vermeiden. In Bezug auf das Limitsystem sollen die in Abb. A.43 aufgelisteten Parameter (Overnight-, Intraday-, Stop-Loss-, Volumen-Limit und Maximale Verlust) in
zwei Arten (weiche und harte Grenze) ausgefüllt werden. Das Überschreiten der weichen Grenze erzeugt eine Warnung, das Überschreiten der harten Grenze wird durch das System verhindert.

Abbildung A.43.: Limits setzen

**A.12.2. Kundenverwaltung**

Sehen Sie bitte den Abschnitt A.6.2

**A.12.3. Log einsehen**

Sehen Sie bitte den Abschnitt A.14.3
A.12.4. Kontodatenliste beantragen
Sehen Sie bitte den Abschnitt A.11.3

A.12.5. Statistische Daten
Sehen Sie bitte den Abschnitt A.8.2

A.12.6. Einstellung der Verdächtigkeitsprüfung für Überweisung
Diese Einstellung hilft unser System bei der Verdächtigkeitsprüfung für Überweisung, indem ein Grenzwert wie in Abb. A.44 eingetragen wird. Dies erlaubt, die Verdächtigkeitsprüfung für Überweisung automatisiert durchzuführen.

Abbildung A.44.: Parametrisierte Einstellung der Überweisungsverdächtigkeit

A.12.7. Nachrichtenverkehr
Sehen Sie bitte den Abschnitt A.4.3

A.12.8. Kurse einsehen
Sehen Sie bitte den Abschnitt A.5.5

A.13. Eigenhändler

Autor: CW
Als Eigenhändler können Sie Ihre Finanzinstrumente online an- oder verkaufen. Zusätzlich dazusind die Funktionen für Eigenhandel in Zusammenhang mit Kundenangelegenheiten verfügbar, um die aktuellen Zustände von Finanzinstrumenten oder den aktuellen Kontostand nachzufragen. In Abb. A.45 wird die Start Seite für den Eigenhändler nach Einloggen angezeigt. Der Navigationsbereich zeigt die folgenden Einträge:

1. Börseangelegenheiten
   • Order erstellen
- Depot einsehen
- Orderverwaltung

2. Kontostand

3. Nachrichten
   - Nachrichten lesen
   - Nachrichten verschicken

4. Kurse
   - Kurse einsehen

Abbildung A.45.: Start Seite für Eigenhändler

A.13.1. Börseangelegenheit

Sehen Sie bitte den Abschnitt A.5.2.

A.13.2. Kontostand einsehen

Sehen Sie bitte den Abschnitt A.5.1.4.

A.13.3. Nachrichtenverkehr

Sehen Sie bitte den Abschnitt A.4.3.

A.14. Systemadministrator

Autor: CW

Als Kundenberater sehen Sie nach dem Einloggen Ihre Benutzeroberfläche wie in Abb. A.46. Der Navigationsbereich zeigt die folgenden Einträge:

1. Systemstatus einsehen
2. Mitarbeiterverwaltung
3. Logs einsehen
4. Logs auswerten
5. Backup erstellen
6. RSA-Schlüssel-Verwaltung
7. Nachrichten
   - Nachrichten lesen
   - Nachrichten verschicken
8. Runterfahren

Abbildung A.46.: Start Seite für Systemadministrator

A.14.1. Systemstatus einsehen

Klicken Sie den Button Systemstatus, so wird der aktuelle Systemstatus, der die Informationen über Laufzeit Speicher/CPU-Auslastung des Cloudservers enthält, wie in Abb. A.47 angezeigt wird.

A.14.2. Mitarbeiterverwaltung

A.14.3. Log einsehen

A.14.4. Log auswerten

Diese Funktion dient dazu, Systemlogs bei Bedarf katalogisch sortiert darzustellen (s. Abb. A.51). Hier haben Sie die Möglichkeit sich die Logs aus einem bestimmten Zeitraum in verkürzter Form anzeigen zu lassen. Der Button Exportieren ermöglicht es Ihnen die aktuell angezeigten Logs in eine separate Log-Datei zu exportieren. Durch Auswählen eines Log-Eintrags und Betätigen des Buttons Details anzeigen wird der gesamte Log-Eintrag angezeigt.
A.14.5. Backup erstellen


A.14.6. RSA Schlüssel verwalten

In der Ansicht *RSA Schlüssel verwalten* können Sie den RSA Schlüssel 1.5.4 des Banking-Systems ändern und neue RSA Schlüssel generieren (s. Abb. A.53) oder fremde Zertifikate importieren, denen die *Magnus Monetarius Bank* vertraut (s. Abb. A.54).
Abbildung A.52.: Backup erstellen

Abbildung A.53.: RSA-Schlüssel verwalten

Abbildung A.54.: RSA-Schlüssel verwalten
A.14.7. Nachrichtenverkehr

Sehen Sie bitte den Abschnitt A.4.3.

A.14.8. Runterfahren

Durch den Menüeintrag *Runterfahren* kann der Server heruntergefahren werden.
B. Datenbanktabellen

Folgende Tabellen werden in den beiden Datenbanken banksystem und stammdaten verwendet. Der Übersicht halber wurden sie nach unterschiedlichen Bereichen aufgeteilt, wobei einige Tabellen in mehreren Bereichen vorhanden sind und als Schnittstelle zwischen diesen Bereichen dienen sollen.

Die Syntax der Tabellen wird in Abschnitt 1.2.3 vorgestellt.

B.1. Personen
B.2. Interne Konten
B.3. Transaktionen
B.4. Börse und Nachrichten
B.5. Vorgänge
B.6. Stammdaten

**inhaber**
- Kontonummer INT(10) (FK)
- PersonGebDatId INT(10) (FK)
- Eintragsdatum VARCHAR(45)
- Loeschdatum VARCHAR(45)

**persongebdat**
- PersonGebDatId INT(10)
- PersonId INT(10) (FK)
- GebDat VARCHAR(45)
- Eintragsdatum VARCHAR(45)
- Loeschdatum VARCHAR(45)

**person**
- PersonId INT(10)
- Nachname VARCHAR(45)
- Vornamen VARCHAR(45)
- Eintragsdatum VARCHAR(45)
- Loeschdatum VARCHAR(45)

**konto**
- Kontonummer INT(10)
- Eroeffnungsdatum VARCHAR(45)
- Loeschdatum VARCHAR(45)

**verfuegungsberechtigter**
- Kontonummer INT(15) (FK)
- PersonGebDatId INT(10) (FK)
- Eintragsdatum VARCHAR(45)
- Loeschdatum VARCHAR(45)

**wirtschaftlichberechtigter**
- Kontonummer INT(10) (FK)
- PersonAdressId INT(10) (FK)
- Eintragsdatum VARCHAR(45)
- Loeschdatum VARCHAR(45)

**personadress**
- PersonAdressId INT(10)
- PersonId INT(10) (FK)
- Strasse VARCHAR(45)
- Hausnummer INT(10)
- PLZ INT(10)
- Ort VARCHAR(45)
- Land VARCHAR(45)
- Eintragsdatum VARCHAR(45)
- Loeschdatum VARCHAR(45)
C. Security Policy
IT-Sicherheitsleitlinie
Magnus Monetarus Bank
Cloud-basiertes Internetbanking System

19. Dezember 2011
Inhaltsverzeichnis

1. Ziele 2
2. Adressatenkreis 3
3. Verantwortlichkeiten und Zuständigkeiten 3
4. Verantwortlichkeit Dritter 4
5. Sicherheitsmanagement 4
6. Sicherheitsmaßnahmen 4
7. Richtlinien für Mindeststandards 5
8. Schulung und Sensibilisierung 6
9. Prüfung 6
10. Gesetze und Vorschriften 6
11. Verstöße und Sanktionierung 6
12. Inkrafttreten 7
A. Glossar 7

Literaturverzeichnis 8

Dokumentenhistorie

<table>
<thead>
<tr>
<th>Version</th>
<th>Datum</th>
<th>Editor</th>
<th>Änderung</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>12.09.2011</td>
<td>DS, TS, VS</td>
<td>Initiales Dokument</td>
</tr>
<tr>
<td>1.1</td>
<td>25.11.2011</td>
<td>TS, VS (PG555)</td>
<td>Zertifizierung referenziert</td>
</tr>
<tr>
<td>1.2</td>
<td>19.12.2011</td>
<td>TS (PG555)</td>
<td>Orthographische Korrekturen</td>
</tr>
</tbody>
</table>
Präambel

Informationen und die zu ihrer Übertragung und Verarbeitung eingesetzten Prozesse und IT-Systeme stellen grundlegende Werte für die Magnus Monetarius Bank dar. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnologie (IT) maßgeblich unterstützt. Die Informationssicherheit ist ein zunehmend wichtiger Faktor geworden, weshalb insbesondere das Sicherheitsbewusstsein hinsichtlich der vorhandenen Informationen einer der entscheidenden Erfolgsfaktoren für die Bank ist.

Der Schutz dieser Werte vor Verlust, unberechtigtem Zugriff und vor unerlaubter Änderung ist unverzichtbar, um die Leistungsfähigkeit und Wettbewerbspositionen des Unternehmens, sowie das Vertrauen bei Geschäftspartnern und Kunden zu erhalten und zu verbessern.

1. Ziele

1.1 Das oberste Ziel der IT-Sicherheitsleitlinie der Magnus Monetarius Bank ist es, die Verfügbarkeit, Vertraulichkeit und Integrität der eigenen und der ihr von Kunden und Geschäftspartnern anvertrauten Informationen und Ressourcen zu schützen. Dabei ist die Nachvollziehbarkeit, Verbindlichkeit und Ordnungsmäßigkeit von Prozessen zu garantieren, um das Erreichen der Unternehmensziele zu gewährleisten und Schaden durch den Eintritt unerwünschter Ereignisse zu verhindern oder zu begrenzen.


1.3 Verspätete oder fehlerhafte Managemententscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für das Management bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicherzustellen.

1.4 Die Aktualität der Börsendaten ist für die Eigenhändler essentiell. Es muss folglich sichergestellt werden, dass der Zugriff auf die Börsendaten schnell und zuverlässig verfügbar ist.

1.5 Die Verfügbarkeit der Kommunikation mit anderen Banken ist für die Ausübung der Geschäfte von höchster Bedeutung und ist in jedem Fall sicher zu stellen.

1.6 Der Zugriff auf das Internetbanking-System muss für den Kunden zu jeder Zeit möglich sein. Dies liegt im Interesse der Magnus Monetarius Bank, da dies für das Kern-
geschäft notwendig ist.

1.7 Ein Ausfall des Nachrichtensystems oder des Workflowsystems kann zu Verzögerungen im Arbeitsablauf führen, daher ist die Verfügbarkeit des Nachrichtensystems und des Workflowsystems sicherzustellen. Im Falle eines Ausfalls muss der Betrieb der Kerngeschäfte weiterhin möglich sein.

1.8 Die Datenschutzgesetze und die Interessen unserer Mitarbeiter verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. Die Daten und die IT-Anwendungen der Personalabteilung werden daher einem hohen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Kunden und Geschäftspartner.


2. Adressatenkreis

Diese Sicherheitsleitlinie gilt für die Magnus Moneraturs Bank sowie für ihre sämtlichen Mitarbeiter. Außerdem muss die Leitlinie für alle Geschäftsprozesse, die durch das Bankingsystem durchgeführt und unterstützt werden, umgesetzt werden.

3. Verantwortlichkeiten und Zuständigkeiten

Verantwortlich für die Einhaltung dieser Sicherheitsleitlinie und damit für die Informationssicherheit ist neben der Geschäftsleitung jede Abteilung und jeder Mitarbeiter der Magnus Monetarius Bank. Jede Abteilung und jeder Mitarbeiter ist insbesondere für die Sicherheit und einen angemessenen Schutz ihrer/seiner Informationen entsprechend ihres Wertes und des Risikos für das betreffende Geschäfts- und technische Umfeld verantwortlich.

Vor diesem Hintergrund muss es für alle Informationen einen benannten Verantwortlichen geben. Insbesondere müssen folgende Verantwortliche benannt werden:

- **Datenschutzbeauftragter**
  Verantwortlich für die Einhaltung des Datenschutzes und die Weiterentwicklung der Datenschutzrichtlinie

- **IT-Sicherheitsbeauftragter**
  Verantwortlich für das Erreichen und die Einhaltung der Informationssicherheit, sowie die Erstellung und Weiterentwicklung der IT-Sicherheitsleitlinie

- **Vertreter der Rechtsabteilung**
Berät das Unternehmen bei der Erstellung und Weiterentwicklung von Sicherheits- und Datenschutzleitlinien.

4. Verantwortlichkeit Dritter

Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden von uns konkrete Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Das Recht auf Kontrolle wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben erstellen wir ein detailliertes Sicherheitskonzept mit konkreten Maßnahmenvorgaben.

5. Sicherheitsmanagement

5.1 Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingerichtet. Es ist ein IT-Sicherheitsbeauftragter benannt worden. Der IT-Sicherheitsbeauftragte berichtet in seiner Funktion direkt an den IT-Direktor, der Mitglied der Geschäftsführung ist.

5.2 Dem IT-Sicherheitsbeauftragten und den Administratoren werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiter zu bilden und zu informieren und die vom Management festgelegten Informationssicherheitsziele zu erreichen.

5.3 Die Administratoren und der IT-Sicherheitsbeauftragte sind durch die IT-Benutzer ausreichend in ihrer Arbeit zu unterstützen.

5.4 Der IT-Sicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt Gleiches für den Datenschutzbeauftragten.

5.5 Die IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des IT Sicherheitsbeauftragten zu halten.

5.6 Es wurde ein Datenschutzbeauftragter bestellt. Der Datenschutzbeauftragte hat ein ausreichend bemessenes Zeitbudget für die Erfüllung seiner Pflichten zur Verfügung. Der Datenschutzbeauftragte ist angehalten, sich regelmäßig weiterzubilden.

6. Sicherheitsmaßnahmen

6.1 Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsbe-
rechtigungen vergibt.

6.2 Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter in der Lage sind, ihre Aufgaben zu erfüllen.

6.3 Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restrikitives Berechtigungskonzept geschützt.

6.4 Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

6.5 Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

7. Richtlinien für Mindeststandards


- Internet- und E-Mail-Nutzung
- IT-Nutzung
- Outsourcing
- Archivierung
- Datensicherung
- Notfallvorsorge

7.2 Alle aus den Sicherheitsgrundsätzen abgeleiteten Regelwerke und Anweisungen werden in regelmäßigen Abständen auf ihre Aktualität, Korrektheit, Angemessenheit und Umsetzbarkeit überprüft und bei Bedarf angepasst oder durch Folgedokumente ersetzt.
Für die Koordination dieser Überprüfungen ist das Sicherheitsmanagement verantwortlich.

8. Schulung und Sensibilisierung


9. Prüfung

Die IT-Sicherheitsleitlinie sowie die auf ihr beruhenden Richtlinien werden durch das Sicherheitsmanagement ständig aktualisiert und regelmäßig auf ihre Wirksamkeit und Einhaltung überprüft. Die auf diesen Regelungen beruhenden Maßnahmen werden regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie (noch) umsetzbar und in den (aktuellen) Betriebsablauf integrierbar sind.

Die Leitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

10. Gesetze und Vorschriften

Beim Einsatz der IT sind einschlägige Gesetze, Vorschriften sowie vertragliche und aufsichtsrechtliche Verpflichtungen und Regelungen einzuhalten.

11. Verstöße und Sanktionierung

11.1 Als Verstöße werden Handlungen gegen das Regelwerk der IT-Sicherheit verstanden. Dazu zählen insbesondere:

- die Kompromittierung der Sicherheit von Informationen,
der unberechtigte Zugriff auf Informationen,
die unberechtigte Änderung, Nutzung und/oder Veröffentlichung von Informationen.

11.2 Verstöße gegen die IT-Sicherheit werden nach den geltenden Regelungen und gesetzlichen Bestimmungen geahndet.

12. Inkrafttreten

Diese Richtlinie wird von der Unternehmensleitung der Magnus Monetarius Bank verabschiedet. Sie tritt am Tag nach ihrer Bekanntmachung durch den IT-Sicherheitsbeauftragten in Kraft.

A. Glossar

- **Administrator**: Ein Administrator ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems.
- **Datenschutzbeauftragter**: Ein Datenschutzbeauftragter ist eine von der Unternehmensleitung bestellte Person, die für den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten im Unternehmen verantwortlich ist.
- **IT-Anwendung**: Software, die angewendet wird, um eine nützliche oder gewünschte Funktionalität zu erfüllen
- **IT-Direktor**: Mitglied der Geschäftsführung, das für die Organisation der IT-Systeme verwantwortlich ist
- **IT-Sicherheitsbeauftragter**: Ein IT-Sicherheitsbeauftragter ist eine von der Unternehmensleitung ernannte Person, die im Auftrag der Leitungsebene die Aufgabe Informationssicherheit koordiniert und innerhalb des Unternehmens vorantreibt.
- **IT-System**: Jegliche Art informationsverarbeitender elektronischer Systeme, z.B.: Computer, Serversysteme, Datenbanksysteme
- **Outsourcing**: Abgabe von Unternehmensaufgaben und -strukturen an Drittanbietern
- **Service Level Agreement (SLA)**: Bezeichnet einen Vertrag bzw. die Schnittstelle, zwischen Auftraggeber und Dienstleistung für wiederkehrende Dienstleistungen
- **Sicherheitsmanagement**: Bezeichnet die Planung, Steuerung und Kontrolle der Sicherheit in einem Unternehmen
• **Verfügbarkeit**: Eigenschaft, die die korrekte Nutzung einer Funktion des Systems garantiert

• **Verlässlichkeit**: Eigenschaft einer Funktion, die die korrekte Ausführung garantiert

• **Vertraulichkeit**: Eigenschaft, die die kontrollierte Nutzung (Erhebung / Bearbeitung) einer Datei des Systems durch vorgesehene Akteure garantiert. Dies impliziert auch die Nicht-Nutzung durch unberechtigte Akteure

• **Vertreter der Rechtsabteilung**: Berater des Unternehmens bei der Erstellung und Weiterentwicklung von Sicherheits- und Datenschutzrichtlinien

**Literatur**


Bausteine, Gefährdungen und Maßnahmen des BSI-Grundschutzkataloges

Magnus Monetarus Bank
Cloud-basiertes Internetbanking System

25. November 2011
Inhaltsverzeichnis

1 Bausteine für Übergreifende Aspekte ............................................. 2
1.1 Sicherheitsmanagement (B 1.0) ................................................. 2
  1.1.1 Beschreibung .............................................................. 2
  1.1.2 Gefährdungslage ......................................................... 2
  1.1.3 Maßnahmen ............................................................... 3
1.2 Organisation (B 1.1) .............................................................. 4
  1.2.1 Beschreibung .............................................................. 4
  1.2.2 Gefährdungslage ......................................................... 4
  1.2.3 Maßnahmen ............................................................... 5
1.3 Personal (B 1.2) ................................................................. 6
  1.3.1 Beschreibung .............................................................. 6
  1.3.2 Gefährdungslage ......................................................... 6
  1.3.3 Maßnahmen ............................................................... 7
1.4 Notfallmanagement (B 1.3) ...................................................... 8
1.5 Datensicherungskonzept (B 1.4) ................................................ 8
  1.5.1 Beschreibung .............................................................. 8
  1.5.2 Gefährdungslage ......................................................... 9
  1.5.3 Maßnahmen ............................................................... 9
1.6 Datenschutz (B 1.5) .............................................................. 10
  1.6.1 Beschreibung .............................................................. 10
  1.6.2 Gefährdungslage ......................................................... 10
  1.6.3 Maßnahmen ............................................................... 11
1.7 Schutz vor Schadprogrammen (B 1.6) ......................................... 12
  1.7.1 Beschreibung .............................................................. 12
  1.7.2 Gefährdungslage ......................................................... 12
  1.7.3 Maßnahmen ............................................................... 13
1.8 Kryptokonzept (B 1.7) ........................................................... 15
  1.8.1 Beschreibung .............................................................. 15
  1.8.2 Gefährdungslage ......................................................... 15
  1.8.3 Maßnahmen ............................................................... 16
1.9 Behandlung von Sicherheitsvorfällen (B 1.8) ............................... 18
1.10 Hard- und Software-Management (B 1.9) .................................... 18
1.11 Standardsoftware (B 1.10) .................................................... 18
1.12 Outsourcing (B 1.11) ........................................................... 18
  1.12.1 Beschreibung ............................................................ 18
  1.12.2 Gefährdungslage ....................................................... 20
  1.12.3 Maßnahmen ............................................................. 21
1.13 Archivierung (B 1.12) .......................................................... 22
  1.13.1 Beschreibung ............................................................ 22
  1.13.2 Gefährdungslage ....................................................... 24
  1.13.3 Maßnahmen ............................................................. 25
1.14 Sensibilisierung und Schulung zur Informationssicherheit (B 1.13) .. 27
1.15 Patch- und Änderungsmanagement (B 1.14)  ...  27
1.16 Löschen und Vernichten von Daten (B 1.15)  ...  27
1.17 Anforderungsmanagement (B 1.16)  ...  27

2 Bausteine für Infrastruktur  ...  28
  2.1 Gebäude (B 2.1)  ...  28
      2.1.1 Beschreibung  ...  28
      2.1.2 Gefährdungslage  ...  28
      2.1.3 Maßnahmen  ...  29
  2.2 Serverraum (B 2.4)  ...  30
      2.2.1 Beschreibung  ...  30
      2.2.2 Gefährdungslage  ...  30
      2.2.3 Maßnahmen  ...  31
  2.3 Rechenzentrum (B 2.9)  ...  32
      2.3.1 Beschreibung  ...  32
      2.3.2 Gefährdungslage  ...  34
      2.3.3 Maßnahmen  ...  35

3 Bausteine für IT-Systeme  ...  37
  3.1 Allgemeiner Server (B 3.101)  ...  37
      3.1.1 Beschreibung  ...  37
      3.1.2 Gefährdungslage  ...  37
      3.1.3 Maßnahmen  ...  38
  3.2 Server unter Unix (B 3.102)  ...  40
      3.2.1 Beschreibung  ...  40
      3.2.2 Gefährdungslage  ...  41
      3.2.3 Maßnahmen  ...  42
  3.3 Sicherheitsgateway (Firewall) (B 3.301)  ...  43
      3.3.1 Beschreibung  ...  43
      3.3.2 Gefährdungslage  ...  44
      3.3.3 Maßnahmen  ...  45
  3.4 Router und Switches (B 3.302)  ...  47
      3.4.1 Beschreibung  ...  47
      3.4.2 Gefährdungslage  ...  47
      3.4.3 Maßnahmen  ...  48

4 Bausteine für Netze  ...  51
  4.1 Heterogene Netze (B 4.1)  ...  51
      4.1.1 Beschreibung  ...  51
      4.1.2 Gefährdungslage  ...  51
      4.1.3 Maßnahmen  ...  52
  4.2 Netz- und Systemmanagement (B 4.2)  ...  53
      4.2.1 Beschreibung  ...  53
      4.2.2 Gefährdungslage  ...  54
4.2.3 Maßnahmen ........................................... 55

5 Bausteine für Anwendungen 57
5.1 Webserver (B 5.4) ................................. 57
  5.1.1 Beschreibung ........................................ 57
  5.1.2 Gefährdungslage ................................. 57
  5.1.3 Maßnahmen ......................................... 58
5.2 Datenbanken (B 5.7) ............................... 60
  5.2.1 Beschreibung ........................................ 60
  5.2.2 Gefährdungslage ................................. 61
  5.2.3 Maßnahmen ......................................... 62

Literaturverzeichnis 64

Dokumentenhistorie

<table>
<thead>
<tr>
<th>Version</th>
<th>Datum</th>
<th>Editor</th>
<th>Änderung</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>12.09.2011</td>
<td>TS, VS (PG555)</td>
<td>Initiales Dokument</td>
</tr>
<tr>
<td>0.2</td>
<td>25.11.2011</td>
<td>TS, VS (PG555)</td>
<td>Präambel hinzugefügt</td>
</tr>
</tbody>
</table>
Präambel

Aufbau des Dokuments


Ziel des Dokuments

Das Dokument führt die Gefährdungen und Maßnahmen auf, die für den Betrieb und die Weiterentwicklung der Bankingsoftware relevant sind, um die IT-Sicherheitsleitlinie zu vervollständigen. Weiter soll durch dieses Dokument die Zertifizierung der Bankingsoftware mit dem BSI-Grundschutz-Zertifikat (BS 7799-2) vorbereiten, die eine Zertifizierung nach ISO 27001 einschließt.

Für die Bausteine, deren Gefährdungslage durch die PG555 nicht festgestellt werden kann, werden in dieser Version (0.2) keine Gefahren und auch keine Maßnahmen aufgeführt.
1 Bausteine für Übergreifende Aspekte

1.1 Sicherheitsmanagement (B 1.0)

1.1.1 Beschreibung


Der Begriff Informationssicherheit ist umfassender als der Begriff IT-Sicherheit und wird aufgrund dessen zunehmend verwendet. Da aber in der Literatur noch überwiegend der Begriff IT-Sicherheit zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

Dieser Baustein soll aufzeigen, wie ein funktionierendes Informationssicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu sinnvolle Schritte eines systematischen Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines umfassenden Sicherheitskonzeptes. Der Baustein baut auf dem BSI-Standard 100-1 Managementsysteme für Informationssicherheit und BSI-Standard 100-2 Vorgehensweise nach IT-Grundschutz auf und fasst die wichtigsten Aspekte zum Sicherheitsmanagement hieraus zusammen.

1.1.2 Gefährdungslage

Gefährdungen im Umfeld des Sicherheitsmanagements können vielfältiger Natur sein. Stellvertretend für diese Vielzahl der Gefährdungen werden in diesem Baustein die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel

| G 2.66 | Unzureichendes Sicherheitsmanagement |
1.1.3 Maßnahmen

Im Rahmen des Sicherheitsmanagements sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Einer der Grundpfeiler zur Erreichung eines angemessenen Sicherheitsniveaus ist, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung für Informationssicherheit bewusst ist. Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen umgesetzt wird (siehe M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene).


Nachfolgend wird das Maßnahmenbündel für den Bereich Sicherheitsmanagement vorgestellt.

**Planung und Konzeption**

<table>
<thead>
<tr>
<th>Maßnahme</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.192</td>
<td>Erstellung einer Leitlinie zur Informationssicherheit</td>
</tr>
<tr>
<td>M 2.335</td>
<td>Festlegung der Sicherheitsziele und -strategie</td>
</tr>
<tr>
<td>M 2.336</td>
<td>Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene</td>
</tr>
</tbody>
</table>

**Umsetzung**

<table>
<thead>
<tr>
<th>Maßnahme</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.193</td>
<td>Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit</td>
</tr>
<tr>
<td>M 2.195</td>
<td>Erstellung eines Sicherheitskonzepts</td>
</tr>
<tr>
<td>Code</td>
<td>Typ</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>M 2.197</td>
<td>(A)</td>
</tr>
<tr>
<td>M 2.337</td>
<td>(A)</td>
</tr>
<tr>
<td>M 2.338</td>
<td>(Z)</td>
</tr>
<tr>
<td>M 2.339</td>
<td>(Z)</td>
</tr>
</tbody>
</table>

Betrieb

<table>
<thead>
<tr>
<th>Code</th>
<th>Typ</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.199</td>
<td>(A)</td>
<td>Aufrechterhaltung der Informationssicherheit</td>
</tr>
<tr>
<td>M 2.200</td>
<td>(C)</td>
<td>Management-Berichte zur Informationssicherheit</td>
</tr>
<tr>
<td>M 2.201</td>
<td>(C)</td>
<td>Dokumentation des Sicherheitsprozesses</td>
</tr>
</tbody>
</table>

Notfallvorsorge

<table>
<thead>
<tr>
<th>Code</th>
<th>Typ</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 6.16</td>
<td>(Z)</td>
<td>Abschließen von Versicherungen</td>
</tr>
</tbody>
</table>

1.2 Organisation (B 1.1)

1.2.1 Beschreibung

In diesem Baustein werden allgemeine und übergreifende Maßnahmen im Organisationsbereich aufgeführt, die als organisatorische Standardmaßnahmen zur Erreichung eines Mindestschutzniveaus erforderlich sind. Spezielle Maßnahmen organisatorischer Art, die in unmittelbarem Zusammenhang mit anderen Maßnahmen stehen (z. B. LAN-Administration), werden in den entsprechenden Baustein aufgeführt.

1.2.2 Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel

<table>
<thead>
<tr>
<th>Code</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.1</td>
<td>Fehlende oder unzureichende Regelungen</td>
</tr>
<tr>
<td>G 2.2</td>
<td>Unzureichende Kenntnis über Regelungen</td>
</tr>
<tr>
<td>G 2.3</td>
<td>Fehlende, ungeeignete, inkompatible Betriebsmittel</td>
</tr>
<tr>
<td>G 2.5</td>
<td>Fehlende oder unzureichende Wartung</td>
</tr>
<tr>
<td>G 2.6</td>
<td>Unbefugter Zutritt zu schutzbedürftigen Räumen</td>
</tr>
<tr>
<td>G 2.7</td>
<td>Unerlaubte Ausübung von Rechten</td>
</tr>
</tbody>
</table>
Menschliche Fehlhandlungen

| G 3.6 | Gefährdung durch Reinigungs- oder Fremdpersonal |

Vorsätzliche Handlungen

| G 5.1 | Manipulation oder Zerstörung von Geräten oder Zubehör |
| G 5.2 | Manipulation an Informationen oder Software |
| G 5.3 | Unbefugtes Eindringen in ein Gebäude |
| G 5.4 | Diebstahl |
| G 5.5 | Vandalismus |
| G 5.6 | Anschlag |
| G 5.16 | Manipulation bei Wartungsarbeiten |
| G 5.68 | Unberechtigter Zugang zu den aktiven Netzkomponenten |
| G 5.102 | Sabotage |

1.2.3 Maßnahmen


Planung und Konzeption

| M 2.1 | (A) Festlegung von Verantwortlichkeiten und Regelungen |
| M 2.2 | (C) Betriebsmittelverwaltung |
| M 2.4 | (B) Regelungen für Wartungs- und Reparaturarbeiten |
| M 2.5 | (A) Aufgabenverteilung und Funktionstrennung |
| M 2.40 | (A) Rechtzeitige Beteiligung des Personal-/Betriebsrates |
| M 2.225 | (B) Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten |
| M 2.393 | (A) Regelung des Informationsaustausches |
**1.3 Personal (B 1.2)**

### 1.3.1 Beschreibung


### 1.3.2 Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

**Höhere Gewalt**

| G 1.1 | Personalausfall |
| G 1.2 | Ausfall von IT-Systemen |

**Organisatorische Mängel**
Menschliche Fehlhandlungen

<table>
<thead>
<tr>
<th>G 3.1</th>
<th>Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 3.2</td>
<td>Fahrlässige Zerstörung von Gerät oder Daten</td>
</tr>
<tr>
<td>G 3.3</td>
<td>Nichtbeachtung von Sicherheitsmaßnahmen</td>
</tr>
<tr>
<td>G 3.8</td>
<td>Fehlerhafte Nutzung von IT-Systemen</td>
</tr>
<tr>
<td>G 3.9</td>
<td>Fehlerhafte Administration von IT-Systemen</td>
</tr>
<tr>
<td>G 3.36</td>
<td>Fehlinterpretation von Ereignissen</td>
</tr>
<tr>
<td>G 3.37</td>
<td>Unproduktive Suchzeiten</td>
</tr>
<tr>
<td>G 3.43</td>
<td>Ungeeigneter Umgang mit Passwörtern</td>
</tr>
<tr>
<td>G 3.44</td>
<td>Sorglosigkeit im Umgang mit Informationen</td>
</tr>
</tbody>
</table>

Vorsätzliche Handlungen

<table>
<thead>
<tr>
<th>G 5.1</th>
<th>Manipulation oder Zerstörung von Geräten oder Zubehör</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.2</td>
<td>Manipulation an Informationen oder Software</td>
</tr>
<tr>
<td>G 5.20</td>
<td>Missbrauch von Administratorrechten</td>
</tr>
<tr>
<td>G 5.23</td>
<td>Schadprogramme</td>
</tr>
<tr>
<td>G 5.42</td>
<td>Social Engineering</td>
</tr>
<tr>
<td>G 5.80</td>
<td>Hoax</td>
</tr>
<tr>
<td>G 5.104</td>
<td>Ausspähen von Informationen</td>
</tr>
</tbody>
</table>

1.3.3 Maßnahmen

Für das in einem Unternehmen oder einer Behörde tätige Personal sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer geregelter Einarbeitung neuer Mitarbeiter, über Schulungen, bis hin zu einem geregeltten Ausscheiden eines Mitarbeiters. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

<table>
<thead>
<tr>
<th>M 2.226</th>
<th>(A) Regelungen für den Einsatz von Fremdpersonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 3.51</td>
<td>(Z) Geeignetes Konzept für Personaleinsatz und -qualifizierung</td>
</tr>
</tbody>
</table>

Beschaffung
1.4 Notfallmanagement (B 1.3)

Keine ausreichende Einschätzung möglich.

1.5 Datensicherungskonzept (B 1.4)

1.5.1 Beschreibung

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

Die Konzeption einer angemessenen und funktionstüchtigen Datensicherung bedarf allerdings aufgrund der Komplexität einer geordneten Vorgehensweise. In diesem Baustein...
wird ein Weg beschrieben, wie für ein IT-System ein Datensicherungskonzept erstellt werden kann.

1.5.2 Gefährdungslage

Für die mittels eines Datensicherungskonzepts zu schützenden Daten wird für den IT-Grundschutz folgende typische Gefährdung angenommen:

Technisches Versagen

| G 4.13 | Verlust gespeicherter Daten |

1.5.3 Maßnahmen

Um eine effektive Datensicherung einzurichten, sind eine Reihe von Schritten zu durchlaufen. Diese sind in der Maßnahme M 6.33 Entwicklung eines Datensicherungskonzepts beschrieben und werden durch die dort aufgeführten Maßnahmen erläutert. Daher sollte mit der Umsetzung der Maßnahme M 6.33 begonnen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Datensicherungskonzept" vorgestellt, das vor allem für größere IT-Systeme oder IT-Systeme mit großem Datenvolumen sinnvoll ist. Die Bearbeitung der Maßnahmen sollte in der angegebenen Reihenfolge geschehen, um systematisch ein Datensicherungskonzept zu erarbeiten.

Planung und Konzeption

| M 6.33 (B) | Entwicklung eines Datensicherungskonzepts |
| M 6.34 (B) | Erhebung der Einflussfaktoren der Datensicherung |
| M 6.35 (B) | Festlegung der Verfahrensweise für die Datensicherung |
| M 6.36 (A) | Festlegung des Minimaldatensicherungskonzepts |

Beschaffung

| M 2.137 (A) | Beschaffung eines geeigneten Datensicherungssystems |

Umsetzung

| M 2.41 (A) | Verpflichtung der Mitarbeiter zur Datensicherung |
| M 6.21 (C) | Sicherungskopie der eingesetzten Software |
| M 6.37 (A) | Dokumentation der Datensicherung |

Betrieb
1.6 Datenschutz (B 1.5)

1.6.1 Beschreibung

Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

Aufgrund der engen Verflechtung von Datenschutz und IT-Sicherheit werden in diesem IT-Grundschutz-Baustein zum Thema Datenschutz einerseits die Rahmenbedingungen für den Datenschutz praxisgerecht aufbereitet und andererseits die Verbindung zur IT-Sicherheit im IT-Grundschutz aufgezeigt.


1.6.2 Gefährdungslage

<table>
<thead>
<tr>
<th>G 6.1</th>
<th>Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 6.2</td>
<td>Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>G 6.3</td>
<td>Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>G 6.4</td>
<td>Fehlende oder unzureichende Datenvermeidung und Daten- sparsamkeit bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>G 6.5</td>
<td>Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>G 6.6</td>
<td>Fehlende oder nicht ausreichende Vorabkontrolle</td>
</tr>
<tr>
<td>G 6.7</td>
<td>Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>G 6.8</td>
<td>Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>G 6.9</td>
<td>Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen</td>
</tr>
<tr>
<td>G 6.10</td>
<td>Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>G 6.11</td>
<td>Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland</td>
</tr>
<tr>
<td>G 6.12</td>
<td>Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>G 6.13</td>
<td>Fehlende oder unzureichende Datenschutzkontrolle</td>
</tr>
</tbody>
</table>

### 1.6.3 Maßnahmen

<table>
<thead>
<tr>
<th>M 2.110</th>
<th>Datenschutzaspekte bei der Protokollierung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 7.1</td>
<td>Datenschutzmanagement</td>
</tr>
<tr>
<td>M 7.2</td>
<td>Regelung der Verantwortlichkeiten im Bereich Datenschutz</td>
</tr>
<tr>
<td>M 7.3</td>
<td>Aspekte eines Datenschutzkonzeptes</td>
</tr>
<tr>
<td>M 7.4</td>
<td>Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>M 7.5</td>
<td>Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>M 7.6</td>
<td>Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>M 7.7</td>
<td>Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>M 7.8</td>
<td>Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>M 7.9</td>
<td>Datenschutzrechtliche Freigabe</td>
</tr>
<tr>
<td>M 7.10</td>
<td>Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>M 7.11</td>
<td>Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>M 7.12</td>
<td>Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten</td>
</tr>
<tr>
<td>M 7.13</td>
<td>Dokumentation der datenschutzrechtlichen Zulässigkeit</td>
</tr>
<tr>
<td>M 7.14</td>
<td>Aufrechterhaltung des Datenschutzes im laufenden Betrieb</td>
</tr>
<tr>
<td>M 7.15</td>
<td>Datenschutzgerechte Löschung/Vernichtung</td>
</tr>
</tbody>
</table>

### 1.7 Schutz vor Schadprogrammen (B 1.6)

#### 1.7.1 Beschreibung


Um für eine Gesamtorganisation einen effektiven Schutz gegen Schadprogramme zu erreichen, wird in diesem Baustein die Vorgehensweise zur Erstellung und Realisierung eines entsprechenden Sicherheitskonzeptes erläutert. Konkrete Maßnahmenempfehlungen zum Schutz vor Schadprogrammen für einzelne IT-Systeme finden sich in den systemspezifischen Bausteinen.

#### 1.7.2 Gefährdungslage

Für den IT-Grundschutz werden bezüglich Schadprogramme die folgenden typischen Gefährdungen betrachtet:
Organisatorische Mängel

- **G 2.1** Fehlende oder unzureichende Regelungen
- **G 2.2** Unzureichende Kenntnis über Regelungen
- **G 2.3** Fehlende, ungeeignete, inkompatible Betriebsmittel
- **G 2.4** Unzureichende Kontrolle der Sicherheitsmaßnahmen
- **G 2.8** Unkontrollierter Einsatz von Betriebsmitteln
- **G 2.9** Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- **G 2.136** Fehlende Übersicht über den Informationsverbund

Technisches Versagen

- **G 4.13** Verlust gespeicherter Daten
- **G 4.22** Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen

- **G 5.2** Manipulation an Informationen oder Software
- **G 5.23** Schadprogramme
- **G 5.28** Verhinderung von Diensten
- **G 5.42** Social Engineering
- **G 5.71** Vertraulichkeitsverlust schützenswerter Informationen
- **G 5.85** Integritätsverlust schützenswerter Informationen
- **G 5.142** Verbreitung von Schadprogrammen über mobile Datenträger

1.7.3 Maßnahmen

Die wichtigsten vorbeugenden Maßnahmen gegen Schäden durch Schadsoftware sind der Einsatz von Viren-Schutzprogrammen sowie regelmäßige Datensicherungen (siehe M 6.32 Regelmäßige Datensicherung).

Nachfolgend wird das Maßnahmenbündel für den Bereich SSchutz vor Schadprogrammen vorgestellt:

**Planung und Konzeption**

<table>
<thead>
<tr>
<th>M 2.154</th>
<th>(A)</th>
<th>Erstellung eines Sicherheitskonzeptes gegen Schadprogramme</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.160</td>
<td>(A)</td>
<td>Regelungen zum Schutz vor Schadprogrammen</td>
</tr>
<tr>
<td>M 3.69</td>
<td>(W)</td>
<td>Einführung in die Bedrohung durch Schadprogramme</td>
</tr>
</tbody>
</table>

**Beschaffung**

| M 2.157  | (A) | Auswahl eines geeigneten Viren-Schutzprogramms       |

**Umsetzung**

| M 4.84   | (A) | Nutzung der BIOS-Sicherheitsmechanismen |

**Betrieb**

<table>
<thead>
<tr>
<th>M 2.34</th>
<th>(A)</th>
<th>Dokumentation der Veränderungen an einem bestehenden System</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.158</td>
<td>(A)</td>
<td>Meldung von Schadprogramm-Infektionen</td>
</tr>
<tr>
<td>M 2.159</td>
<td>(A)</td>
<td>Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen</td>
</tr>
<tr>
<td>M 2.224</td>
<td>(A)</td>
<td>Vorbeugung gegen Schadprogramme</td>
</tr>
<tr>
<td>M 4.3</td>
<td>(A)</td>
<td>Einsatz von Viren-Schutzprogrammen</td>
</tr>
</tbody>
</table>

**Notfallvorsorge**

<table>
<thead>
<tr>
<th>M 6.23</th>
<th>(A)</th>
<th>Verhaltensregeln bei Auftreten von Schadprogrammen</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 6.24</td>
<td>(A)</td>
<td>Erstellen eines Notfall-Bootmediums</td>
</tr>
<tr>
<td>M 6.32</td>
<td>(A)</td>
<td>Regelmäßige Datensicherung</td>
</tr>
</tbody>
</table>
1.8 Kryptokonzept (B 1.7)

1.8.1 Beschreibung

Dieser Baustein beschreibt eine Vorgehensweise, wie in einer heterogenen Umgebung sowohl die lokal gespeicherten Daten als auch die zu übertragenen Daten wirksam-voll durch kryptographische Verfahren und Techniken geschützt werden können. Dazu wird beschrieben, wie und wo in einer heterogenen Umgebung kryptographische Verfahren und die entsprechenden Komponenten eingesetzt werden können. Da beim Einsatz kryptographischer Verfahren sehr viele komplexe Einflussfaktoren zu betrachten sind, sollte hierfür ein Kryptokonzept erstellt werden.

In diesem Baustein wird daher beschrieben, wie ein Kryptokonzept erstellt werden kann. Beginnend mit der Bedarfsermittlung und der Erhebung der Einflussfaktoren geht es über die Auswahl geeigneter kryptographischer Lösungen und Produkte bis hin zur Sensibilisierung und Schulung der Anwender und zur Krypto-Notfallvorsorge.

Für die Umsetzung dieses Bausteins sollte ein elementares Verständnis der grundlegenden kryptographischen Mechanismen vorhanden sein. Ein Überblick über kryptographische Grundbegriffe findet sich in M 3.23 Einführung in kryptographische Grundbegriffe .

1.8.2 Gefährdungslage

Kryptographische Verfahren werden eingesetzt zur Gewährleistung von
Vertraulichkeit,
Integrität,
Authentizität und
Nichtabstreichbarkeit.

Daher werden für den IT-Grundschutz primär die folgenden Gefährdungen für krypto-graphische Verfahren betrachtet:

Organisatorische Mängel

<table>
<thead>
<tr>
<th>G 2.1</th>
<th>Fehlende oder unzureichende Regelungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.2</td>
<td>Unzureichende Kenntnis über Regelungen</td>
</tr>
<tr>
<td>G 2.4</td>
<td>Unzureichende Kontrolle der Sicherheitsmaßnahmen</td>
</tr>
<tr>
<td>G 2.19</td>
<td>Unzureichendes Schlüsselmanagement bei Verschlüsselung</td>
</tr>
</tbody>
</table>

Menschliche Fehlhandlungen

| G 3.1 | Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten |
G 3.32 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren
G 3.33 Fehlbedienung von Kryptomodulen

Technisches Versagen

<table>
<thead>
<tr>
<th>G 4.22</th>
<th>Software-Schwachstellen oder -Fehler</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.33</td>
<td>Schlechte oder fehlende Authentikation</td>
</tr>
<tr>
<td>G 4.34</td>
<td>Ausfall eines Kryptomoduls</td>
</tr>
<tr>
<td>G 4.35</td>
<td>Unsichere kryptographische Algorithmen</td>
</tr>
<tr>
<td>G 4.36</td>
<td>Fehler in verschlüsselten Daten</td>
</tr>
</tbody>
</table>

Vorsätzliche Handlungen

<table>
<thead>
<tr>
<th>G 5.27</th>
<th>Nichtanerkennung einer Nachricht</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.71</td>
<td>Vertraulichkeitsverlust schützenswerter Informationen</td>
</tr>
<tr>
<td>G 5.81</td>
<td>Unautorisierter Benutzung eines Kryptomoduls</td>
</tr>
<tr>
<td>G 5.82</td>
<td>Manipulation eines Kryptomoduls</td>
</tr>
<tr>
<td>G 5.83</td>
<td>Kompromittierung kryptographischer Schlüssel</td>
</tr>
<tr>
<td>G 5.84</td>
<td>Gefälschte Zertifikate</td>
</tr>
<tr>
<td>G 5.85</td>
<td>Integritätsverlust schützenswerter Informationen</td>
</tr>
</tbody>
</table>

1.8.3 Maßnahmen

Entwicklung eines Kryptokonzepts (siehe M 2.161 Entwicklung eines Kryptokonzepts)

Ermittlung der Anforderungen an die kryptographischen Verfahren: Es muss ein Anforderungskatalog erstellt werden, in dem die Einflussgrößen und die Entscheidungskriterien beschrieben werden, die einem Einsatz von kryptographischen Verfahren zugrunde liegen (siehe M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte und M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte). Kryptographische Verfahren können auf den verschiedenen Schichten des ISO/OSI-Schichtenmodells eingesetzt werden. Je nach den festgestellten Anforderungen oder Gefährdungen ist der Einsatz auf bestimmten Schichten zu empfehlen (siehe auch...

Auswahl geeigneter kryptographischer Verfahren (siehe M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens) Bei der Auswahl von kryptographischen Verfahren steht zunächst die Frage, ob symmetrische, asymmetrische oder hybride Algorithmen geeignet sind, im Vordergrund und dann die Mechanismenstärke. Anschließend sind geeignete Produkte zu bestimmen.


Notfallvorsorge, hierzu gehören die Datensicherung bei Einsatz kryptographischer Verfahren (siehe M 6.56 Datensicherung bei Einsatz kryptographischer Verfahren), also die Sicherung der Schlüssel, der Konfigurationen der eingesetzten Produkte, der verschlüsselten Daten, die Informationsbeschaffung über sowie die Reaktion auf Sicherheitslücken.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Kryptokonzept" vorgestellt. Auf eine Wiederholung von Maßnahmen anderer Bausteine wird hier verzichtet.

**Planung und Konzeption**

| M 2.161 (A) | Entwicklung eines Kryptokonzepts |
| M 2.162 (A) | Bedarfserschließung für den Einsatz kryptographischer Verfahren und Produkte |
| M 2.163 (A) | Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte |
| M 2.164 (A) | Auswahl eines geeigneten kryptographischen Verfahrens |
| M 2.166 (A) | Regelung des Einsatzes von Kryptomodulen |
| M 3.23 (A) | Einführung in kryptographische Grundbegriffe |
| M 4.90 (A) | Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells |
Beschaffung

| M 2.165 (A) | Auswahl eines geeigneten kryptographischen Produktes |
| M 4.85 (Z)  | Geeignetes Schnittstellendesign bei Kryptomodulen     |
| M 4.88 (A)  | Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen |

Umsetzung

| M 2.46 (A)  | Geeignetes Schlüsselmanagement                        |
| M 4.86 (A)  | Sichere Rollenteilung und Konfiguration der Kryptomodule |
| M 4.87 (Z)  | Physikalische Sicherheit von Kryptomodulen             |
| M 4.89 (Z)  | Abstrahlsicherheit                                    |

Notfallvorsorge

| M 6.56 (A)  | Datensicherung bei Einsatz kryptographischer Verfahren |

1.9 Behandlung von Sicherheitsvorfällen (B 1.8)

Keine ausreichende Einschätzung möglich.

1.10 Hard- und Software-Management (B 1.9)

Keine ausreichende Einschätzung möglich.

1.11 Standardsoftware (B 1.10)

Keine ausreichende Einschätzung möglich.

1.12 Outsourcing (B 1.11)

1.12.1 Beschreibung

sind der Betrieb eines Rechenzentrums, einer Applikation, einer Webseite oder des Wach-


Die Gründe für Outsourcing sind vielfältig: die Konzentration einer Organisation auf ihre Kernkompetenzen, die Möglichkeit einer Kostenersparnis (z. B. keine Anschaffungs- oder Betriebskosten für IT-Systeme), der Zugriff auf spezialisierte Kenntnisse und Ressourcen, die Freisetzung internen Ressourcen für andere Aufgaben, die Straffung der internen Verwaltung, die verbesserte Skalierbarkeit der Geschäfts- und Produktionsprozesse, die Erhöhung der Flexibilität sowie der Wettbewerbsfähigkeit einer Organisation sind nur einige Beispiele.


Durch die enge Verbindung zum Dienstleister und die entstehende Abhängigkeit von der Dienstleistungsqualität ergeben sich Risiken für den Auftraggeber, durch die im schlimmsten Fall sogar die Geschäftsgrundlage des Unternehmens oder der Behörde vital gefährdet werden können. (Beispielsweise könnten sensitive Organisationsinformationen gewollt oder ungewollt nach außen preisgegeben werden.) Der Betrachtung von Sicherheitsaspekten und der Gestaltung vertraglicher Regelungen zwischen Auftraggeber und Outsourcing-Dienstleister kommt im Rahmen eines Outsourcing-Vorhabens somit eine zentrale Rolle zu.

19
Den Schwerpunkt dieses Bausteins bilden daher Maßnahmen, die sich mit IT-Sicherheitsaspekten des Outsourcing beschäftigen. Dazu zählen ebenfalls geeignete Maßnahmen zur Kontrolle der vertraglich vereinbarten Ziele und Leistungen sowie der IT-Sicherheitsmaßnahmen.

1.12.2 Gefährdungslage


Die Gefährdungen können parallel auf physikalischer, technischer und auch menschlicher Ebene existieren und sind nachfolgend in den einzelnen Gefährdungskatalogen aufgeführt. Um die jeweils existierenden Risiken quantitativ bewerten zu können, müssen zuvor die organisationseigenen Werte und Informationen entsprechend ihrer strategischen Bedeutung für die Organisation beurteilt und klassifiziert werden.

Höhere Gewalt

| G 1.10  | Ausfall eines Weitverkehrsnetzes |

Organisatorische Mängel

| G 2.1   | Fehlende oder unzureichende Regelungen |
| G 2.7   | Unerlaubte Ausübung von Rechten |
| G 2.26  | Fehlendes oder unzureichendes Test- und Freigabeverfahren |
| G 2.47  | Ungesicherter Akten- und Datenträgertransport |
| G 2.66  | Unzureichendes Sicherheitsmanagement |
| G 2.67  | Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten |
| G 2.83  | Fehlerhafte Outsourcing-Strategie |
| G 2.84  | Unzulängliche vertragliche Regelungen mit einem externen Dienstleister |
| G 2.85  | Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens |
| G 2.86  | Abhängigkeit von einem Outsourcing-Dienstleister |
| G 2.88  | Störung des Betriebsklimas durch ein Outsourcing-Vorhaben |
| G 2.89  | Mangelfaht IT-Sicherheit in der Outsourcing-Einführungsphase |
| G 2.90  | Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister |
Menschliche Fehlhandlungen

| G 3.1 | Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten |

Technisches Versagen

| G 4.33 | Schlechte oder fehlende Authentikation |
| G 4.34 | Ausfall eines Kryptomoduls |
| G 4.48 | Ausfall der Systeme eines Outsourcing-Dienstleisters |

Vorsätzliche Handlungen

| G 5.10 | Missbrauch von Fernwartungszugängen |
| G 5.20 | Missbrauch von Administratorrechten |
| G 5.42 | Social Engineering |
| G 5.71 | Vertraulichkeitsverlust schützenswerter Informationen |
| G 5.85 | Integritätsverlust schützenswerter Informationen |
| G 5.107 | Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister |

1.12.3 Maßnahmen

Ein ausgelagerter IT-Verbund kann sowohl aus Komponenten bestehen, die sich ausschließlich im Einflussbereich des Outsourcing-Dienstleisters befinden, als auch aus Komponenten beim Auftraggeber. In der Regel gibt es in diesem Fall Schnittstellen zur Verbindung der Systeme. Für jedes Teilsystem und für die Schnittstellenfunktionen muss IT-Grundschutz gewährleistet sein.

Planung und Konzeption

| M 2.40  | (A) | Rechtzeitige Beteiligung des Personal-/Betriebsrates |
| M 2.42  | (B) | Festlegung der möglichen Kommunikationspartner |
| M 2.221 | (A) | Änderungsmanagement |
| M 2.226 | (A) | Regelungen für den Einsatz von Fremdpersonal |
| M 2.250 | (A) | Festlegung einer Outsourcing-Strategie |
| M 2.251 | (A) | Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben |
1.13 Archivierung (B 1.12)

1.13.1 Beschreibung

Die Archivierung ist als Teil eines Dokumentenmanagement-Prozesses zu sehen. Neben der Erzeugung, Bearbeitung und Verwaltung elektronischer Dokumente spielt die dauerhafte Speicherung (Archivierung) eine besondere Rolle, denn es wird üblicherweise erwartet, dass einerseits die Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind und andererseits deren Vertraulichkeit- und Integrität gewahrt bleibt. Unter Umständen sollen elektronische Dokumente zeitlich unbegrenzt verfügbar sein.

Die Spannweite der Realisierungsmöglichkeiten eines solchen Archivsystems umfasst:

- kleine Archivsysteme, z. B. bestehend aus einem Archivserver mit angeschlossenem Massenspeicher (wie Festplatte oder Jukebox), bis hin zu
- komplexen, gegebenenfalls weltweit verteilten Archivsystemen zur organisationsweiten Archivierung von relevanten Geschäftsdaten, bestehend aus:
  - zentralen Archivserver-Komponenten mit RAID-Systemen, Jukeboxen oder der Anbindung an Storage Area Networks (SAN) für das zentrale Speichern von Dateien,
  - WORM-Medien für die revisionssichere, unveränderbare Speicherung von Daten,
  - Komponenten zur Indizierung von Dateien, Recherche und zur Umwandlung von Speicherformaten (Rendition),
  - dezentralen Cache-Servern für den schnellen Zugriff auf häufig benötigte Daten,
  - Client-Software, die einen direkten Zugriff auf Daten des Archivs erlaubt (z. B. auch aus Office-Anwendungen heraus).


In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie ein Konzept zur elektronischen Archivierung erstellt und wie der Aufbau eines Archivsystems und dessen Einbettung innerhalb eines Unternehmens bzw. einer Behörde sichergestellt werden kann. Der Aufwand zur Erstellung und Umsetzung eines solchen Konzepts ist nicht gering. Dieser Baustein sollte immer dann angewandt werden, wenn die zu archivierenden Daten langfristig für die Behörde bzw. das Unternehmen relevant sind.
1.13.2 Gefährdungslage

Für die bei der elektronischen Archivierung zu betrachtenden Archivsysteme sowie die zugehörigen Organisationsprozesse werden im Rahmen des IT-Grundschutzes die folgenden typischen Gefährdungen angenommen:

Höhere Gewalt

| G 1.2 | Ausfall von IT-Systemen |
| G 1.7 | Unzulässige Temperatur und Luftfeuchte |
| G 1.9 | Datenverlust durch starke Magnetfelder |
| G 1.14 | Datenverlust durch starkes Licht |

Organisatorische Mängel

| G 2.7 | Unerlaubte Ausübung von Rechten |
| G 2.72 | Unzureichende Migration von Archivsystemen |
| G 2.73 | Fehlende Revisionsmöglichkeit von Archivsystemen |
| G 2.74 | Unzureichende Ordnungskriterien für Archive |
| G 2.75 | Mangelnde Kapazität von Archivdatenträgern |
| G 2.76 | Unzureichende Dokumentation von Archivzugängen |
| G 2.77 | Unzulässige Übertragung von Papierdaten in elektronische Archive |
| G 2.78 | Unzulässige Auffrischung von Datenbeständen bei der Archivierung |
| G 2.79 | Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung |
| G 2.80 | Unzureichende Durchführung von Revisionen bei der Archivierung |
| G 2.81 | Unzureichende Vernichtung von Datenträgern bei der Archivierung |
| G 2.82 | Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen |

Menschliche Fehlhandlungen

| G 3.1 | Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten |
| G 3.16 | Fehlerhafte Administration von Zugangs- und Zugriffsrechten |
| G 3.35 | Server im laufenden Betrieb ausschalten |
| G 3.54 | Verwendung ungeeigneter Datenträger bei der Archivierung |
G 3.55 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen

Technisches Versagen

<table>
<thead>
<tr>
<th>G 4.7</th>
<th>Defekte Datenträger</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.13</td>
<td>Verlust gespeicherter Daten</td>
</tr>
<tr>
<td>G 4.20</td>
<td>Datenverlust bei erschöpftem Speichermedium</td>
</tr>
<tr>
<td>G 4.26</td>
<td>Ausfall einer Datenbank</td>
</tr>
<tr>
<td>G 4.30</td>
<td>Verlust der Datenbankintegrität/-konsistenz</td>
</tr>
<tr>
<td>G 4.31</td>
<td>Ausfall oder Störung von Netzkomponenten</td>
</tr>
<tr>
<td>G 4.45</td>
<td>Verzögerte Archivauskunft</td>
</tr>
<tr>
<td>G 4.46</td>
<td>Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung</td>
</tr>
<tr>
<td>G 4.47</td>
<td>Veralten von Kryptoverfahren</td>
</tr>
</tbody>
</table>

Vorsätzliche Handlungen

<table>
<thead>
<tr>
<th>G 5.2</th>
<th>Manipulation an Informationen oder Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.6</td>
<td>Anschlag</td>
</tr>
<tr>
<td>G 5.29</td>
<td>Unberechtigtes Kopieren der Datenträger</td>
</tr>
<tr>
<td>G 5.82</td>
<td>Manipulation eines Kryptomoduls</td>
</tr>
<tr>
<td>G 5.83</td>
<td>Kompromittierung kryptographischer Schlüssel</td>
</tr>
<tr>
<td>G 5.85</td>
<td>Integritätsverlust schützenswerter Informationen</td>
</tr>
<tr>
<td>G 5.102</td>
<td>Sabotage</td>
</tr>
<tr>
<td>G 5.105</td>
<td>Verhinderung der Dienste von Archivsystemen</td>
</tr>
<tr>
<td>G 5.106</td>
<td>Unberechtigtes Überschreiben oder Löschen von Archivmedien</td>
</tr>
</tbody>
</table>

1.13.3 Maßnahmen

### Planung und Konzeption

| M 2.242 (A) | Zielsetzung der elektronischen Archivierung |
| M 2.243 (A) | Entwicklung des Archivierungskonzepts |
| M 2.244 (A) | Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung |
| M 2.245 (A) | Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung |
| M 2.246 (A) | Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung |
| M 2.259 (Z) | Einführung eines übergeordneten Dokumentenmanagements |
| M 2.262 (A) | Regelung der Nutzung von Archivsystemen |
| M 2.265 (Z) | Geeigneter Einsatz digitaler Signaturen bei der Archivierung |

### Beschaffung

| M 4.168 (A) | Auswahl eines geeigneten Archivsystems |
| M 4.169 (A) | Verwendung geeigneter Archivmedien |
| M 4.170 (A) | Auswahl geeigneter Datenformate für die Archivierung von Dokumenten |

### Umsetzung

| M 1.59 (A) | Geeignete Aufstellung von Speicher- und Archivsystemen |
| M 2.266 (C) | Regelmäßige Erneuerung technischer Archivsystem-Komponenten |
| M 3.34 (A) | Einweisung in die Administration des Archivsystems |
| M 3.35 (A) | Einweisung der Benutzer in die Bedienung des Archivsystems |

### Betrieb

| M 1.60 (A) | Geeignete Lagerung von Archivmedien |
| M 2.257 (C) | Überwachung der Speicherressourcen von Archivmedien |
| M 2.258 (A) | Konsistente Indizierung von Dokumenten bei der Archivierung |
| M 2.260 (B) | Regelmäßige Revision des Archivierungsprozesses |
| M 2.261 (B) | Regelmäßige Marktbeobachtung von Archivsystemen |
| M 2.263 (A) | Regelmäßige Aufbereitung von archivierten Datenbeständen |
| M 2.264 (B) | Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung |
| M 4.171 (A) | Schutz der Integrität der Index-Datenbank von Archivsystemen |
| M 4.172 (C) | Protokollierung der Archivzugriffe |
| M 4.173 (B) | Regelmäßige Funktions- und Recoverytests bei der Archivierung |

Notfallvorsorge

| M 6.84 (A) | Regelmäßige Datensicherung der System- und Archivdaten |

1.14 Sensibilisierung und Schulung zur Informationssicherheit (B 1.13)

Keine ausreichende Einschätzung möglich.

1.15 Patch- und Änderungsmanagement (B 1.14)

Keine ausreichende Einschätzung möglich.

1.16 Löschen und Vernichten von Daten (B 1.15)

Keine ausreichende Einschätzung möglich.

1.17 Anforderungsmanagement (B 1.16)

Keine ausreichende Einschätzung möglich.
2 Bausteine für Infrastruktur

2.1 Gebäude (B 2.1)

2.1.1 Beschreibung


2.1.2 Gefährdungslage

Für den IT-Grundschutz eines Gebäudes werden folgende typische Gefährdungen angenommen:

Höhere Gewalt

| G 1.3 | Blitz |
| G 1.4 | Feuer |
| G 1.5 | Wasser |

Organisatorische Mängel

| G 2.1 | Fehlende oder unzureichende Regelungen |
| G 2.6 | Unbefugter Zutritt zu schutzbedürftigen Räumen |

Menschliche Fehlhandlungen

| G 3.85 | Verletzung von Brandschottungen |

Technisches Versagen

| G 4.1 | Ausfall der Stromversorgung |
| G 4.2 | Ausfall interner Versorgungsnetze |
| G 4.3 | Ausfall vorhandener Sicherungseinrichtungen |
Vorsätzliche Handlungen

| G 5.3 | Unbefugtes Eindringen in ein Gebäude |
| G 5.4 | Diebstahl |
| G 5.5 | Vandalismus |
| G 5.6 | Anschlag |

2.1.3 Maßnahmen


Wenn es sich dagegen um eine Anmietung oder die Nutzung eines bestehenden Gebäudes handelt, was eventuell mit Erweiterungs- bzw. Umbaumaßnahmen verbunden sein kann, sind die Möglichkeiten zur Realisierung einer adäquaten Informationssicherheit oft viel stärker eingeschränkt.

Planung und Konzeption

| M 1.3 (A) | Angepasste Aufteilung der Stromkreise |
| M 1.4 (B) | Blitzschutzeinrichtungen |
| M 1.5 (Z) | Galvanische Trennung von Außenleitungen |
| M 1.7 (A) | Handfeuerlöscher |
| M 1.8 (A) | Raumbelegung unter Berücksichtigung von Brandlasten |
| M 1.10 (Z) | Verwendung von Sicherheitstüren und -fenstern |
| M 1.11 (A) | Lagepläne der Versorgungsleitungen |
| M 1.12 (A) | Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile |
| M 1.13 (Z) | Anordnung schützenswerter Gebäudeteile |
| M 1.14 (Z) | Selbsttätige Entwässerung |
| M 1.16 (Z) | Geeignete Standortauswahl |
| M 1.18 (Z) | Gefahrenmeldeanlage |
| M 1.19 (Z) | Einbruchsschutz |
| M 2.334 (Z) | Auswahl eines geeigneten Gebäudes |

Umsetzung

| M 1.1 (A) | Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften |
| M 1.2 (A) | Regelungen für Zutritt zu Verteilern |
| M 1.6 (A) | Einhaltung von Brandschutzvorschriften |
| M 1.17  | (Z) | Pförtnerdienst |
| M 1.51  | (A) | Brandlastreduzierung |
| M 2.17  | (A) | Zutrittsregelung und -kontrolle |

**Betrieb**

| M 1.15  | (A) | Geschlossene Fenster und Türen |
| M 2.14  | (A) | Schlüsselverwaltung |
| M 2.15  | (B) | Brandschutzbegehungen |
| M 2.391 | (B) | Frühzeitige Information des Brandschutzbeauftragten |

**Aussonderung**

| M 2.308 | (Z) | Auszug aus Gebäuden |

**Notfallvorsorge**

| M 6.17  | (A) | Alarmierungsplan und Brandschutzübungen |

### 2.2 Serverraum (B 2.4)

#### 2.2.1 Beschreibung

Der Serverraum dient in erster Linie zur Unterbringung von Servern, z. B. eines LAN-Servers, eines Unix-Zentralrechners oder eines Servers für eine TK-Anlage. Darüber hinaus können dort serverspezifische Unterlagen, Datenträger in kleinem Umfang oder weitere Hardware (Sternkoppler, Protokolldrucker, Klimatechnik) vorhanden sein.


#### 2.2.2 Gefährdungslage

Für den IT-Grundschutz eines Serverraumes werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

<p>| G 1.4 | Feuer |</p>
<table>
<thead>
<tr>
<th>G 1.5</th>
<th>Wasser</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 1.7</td>
<td>Unzulässige Temperatur und Luftfeuchte</td>
</tr>
<tr>
<td>G 1.16</td>
<td>Ausfall von Patchfeldern durch Brand</td>
</tr>
</tbody>
</table>

**Organisatorische Mängel**

<table>
<thead>
<tr>
<th>G 2.1</th>
<th>Fehlende oder unzureichende Regelungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.6</td>
<td>Unbefugter Zutritt zu schutzbedürftigen Räumen</td>
</tr>
</tbody>
</table>

**Technisches Versagen**

<table>
<thead>
<tr>
<th>G 4.1</th>
<th>Ausfall der Stromversorgung</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.2</td>
<td>Ausfall interner Versorgungsnetze</td>
</tr>
<tr>
<td>G 4.6</td>
<td>Spannungsschwankungen/Überspannung/Unterspannung</td>
</tr>
</tbody>
</table>

**Vorsätzliche Handlungen**

<table>
<thead>
<tr>
<th>G 5.1</th>
<th>Manipulation oder Zerstörung von Geräten oder Zubehör</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.2</td>
<td>Manipulation an Informationen oder Software</td>
</tr>
<tr>
<td>G 5.3</td>
<td>Unbefugtes Eindringen in ein Gebäude</td>
</tr>
<tr>
<td>G 5.4</td>
<td>Diebstahl</td>
</tr>
<tr>
<td>G 5.5</td>
<td>Vandalismus</td>
</tr>
</tbody>
</table>

**2.2.3 Maßnahmen**

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Beider Auswahl und Gestaltung eines Serverraums sind eine Reihe infrastruktureller und organisatorischer Maßnahmen umzusetzen, die in M 1.58 Technische und organisatorische Vorgaben für Serverräume beschrieben sind. Dabei sind bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen, je nachdem, ob ein Serverraum in einem neu zu errichtenden Gebäude eingerichtet werden soll oder ob es sich um eine Anmietung oder die Nutzung eines bestehenden Gebäudes handelt. In diesem zweiten Fall sind die Möglichkeiten zur Realisierung einer adäquaten IT-Sicherheit oft viel stärker eingeschränkt. Die Schritte, die bei der Gestaltung eines Serverraums durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.
2.3 Rechenzentrum (B 2.9)

2.3.1 Beschreibung

In den meisten Institutionen werden alle wesentlichen strategischen und operativen Funktionen und Aufgaben durch Informationstechnik (IT) maßgeblich unterstützt oder sind sogar ohne IT nicht auszuführen. Die IT-Systeme der Institution selbst und auch deren Anbindung an externe Netze müssen in einer angemessenen Umgebung und Infrastruktur betrieben werden. Nur so lässt sich die nötige Verfügbarkeit der IT sicherstellen. Die Anforderungen an die Leistungsfähigkeit dieser Systeme und der Netzumgebung steigen stetig an. Um diesem Leistungsbedarf gerecht zu werden, um entsprechende Reserven vorzuhalten und um die IT auch wirtschaftlich betreiben zu können, haben Behörden und Unternehmen jeglicher Größe ihre IT-Landschaft in Rechenzentren konzentriert.

Als Rechenzentrum werden die für den Betrieb von komplexen IT-Infrastrukturen (Server-


Im Gegensatz zum Schutzbedarf eines Serverraums (siehe dort) sind viele Sicherheitsmaßnahmen für ein Rechenzentrum nicht optional, sondern obligatorisch. Dazu gehören beispielsweise eine angemessene Gefahrenmeldeanlage und eine alternative Stromversorgung. Üblich und bewährt für einen sicheren IT-Betrieb ist eine Brandfrüherkennung in Raum und Doppelboden von Rechnersaal und Technikräumen und gegebenenfalls auch eine automatische Löschanlage.
### 2.3.2 Gefährdungslage

Für den IT-Grundschutz eines Rechenzentrums werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

<table>
<thead>
<tr>
<th>G 1.2</th>
<th>Ausfall von IT-Systemen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 1.3</td>
<td>Blitz</td>
</tr>
<tr>
<td>G 1.4</td>
<td>Feuer</td>
</tr>
<tr>
<td>G 1.5</td>
<td>Wasser</td>
</tr>
<tr>
<td>G 1.6</td>
<td>Kabelbrand</td>
</tr>
<tr>
<td>G 1.7</td>
<td>Unzulässige Temperatur und Luftfeuchte</td>
</tr>
<tr>
<td>G 1.8</td>
<td>Staub, Verschmutzung</td>
</tr>
<tr>
<td>G 1.11</td>
<td>Technische Katastrophen im Umfeld</td>
</tr>
<tr>
<td>G 1.12</td>
<td>Beeinträchtigung durch Großveranstaltungen</td>
</tr>
<tr>
<td>G 1.13</td>
<td>Sturm</td>
</tr>
<tr>
<td>G 1.16</td>
<td>Ausfall von Patchfeldern durch Brand</td>
</tr>
</tbody>
</table>

**Organisatorische Mängel**

<table>
<thead>
<tr>
<th>G 2.1</th>
<th>Fehlende oder unzureichende Regelungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.2</td>
<td>Unzureichende Kenntnis über Regelungen</td>
</tr>
<tr>
<td>G 2.4</td>
<td>Unzureichende Kontrolle der Sicherheitsmaßnahmen</td>
</tr>
<tr>
<td>G 2.6</td>
<td>Unbefugter Zutritt zu schutzbedürftigen Räumen</td>
</tr>
<tr>
<td>G 2.11</td>
<td>Unzureichende Trassendimensionierung</td>
</tr>
<tr>
<td>G 2.12</td>
<td>Unzureichende Dokumentation der Verkabelung</td>
</tr>
</tbody>
</table>

**Technisches Versagen**

<table>
<thead>
<tr>
<th>G 4.1</th>
<th>Ausfall der Stromversorgung</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.2</td>
<td>Ausfall interner Versorgungsnetze</td>
</tr>
<tr>
<td>G 4.3</td>
<td>Ausfall vorhandener Sicherungseinrichtungen</td>
</tr>
</tbody>
</table>

**Vorsätzliche Handlungen**

<table>
<thead>
<tr>
<th>G 5.3</th>
<th>Unbefugtes Eindringen in ein Gebäude</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.4</td>
<td>Diebstahl</td>
</tr>
<tr>
<td>G 5.5</td>
<td>Vandalismus</td>
</tr>
<tr>
<td>G 5.6</td>
<td>Anschlag</td>
</tr>
<tr>
<td>G 5.16</td>
<td>Manipulation bei Wartungsarbeiten</td>
</tr>
</tbody>
</table>
2.3.3 Maßnahmen

Bei der Auswahl und Gestaltung eines Rechenzentrums sind eine Reihe infrastruktureller und organisatorischer Maßnahmen umzusetzen, die in M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum beschrieben sind. Dabei sind bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen, je nachdem, ob ein Rechenzentrum in einem neu zu errichtenden Gebäude eingerichtet werden soll oder ob es sich um eine Anmietung oder die Nutzung eines bestehenden Gebäudes handelt. In diesem zweiten Fall sind die Möglichkeiten zur Realisierung einer adäquaten Informationssicherheit oft viel stärker eingeschränkt. Die Schritte, die bei der Gestaltung eines Rechenzentrums durchlaufen sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

<table>
<thead>
<tr>
<th>M 1.3</th>
<th>(A)angled</th>
<th>Angepasste Aufteilung der Stromkreise</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 1.7</td>
<td>(A)</td>
<td>Handfeuerlöscher</td>
</tr>
<tr>
<td>M 1.10</td>
<td>(C)</td>
<td>Verwendung von Sicherheitstüren und -fenstern</td>
</tr>
<tr>
<td>M 1.12</td>
<td>(A)</td>
<td>Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile</td>
</tr>
<tr>
<td>M 1.13</td>
<td>(Z)</td>
<td>Anordnung schützenswerter Gebäudeteile</td>
</tr>
<tr>
<td>M 1.18</td>
<td>(B)</td>
<td>Gefahrenmeldeanlage</td>
</tr>
<tr>
<td>M 1.24</td>
<td>(C)</td>
<td>Vermeidung von wasserführenden Leitungen</td>
</tr>
<tr>
<td>M 1.25</td>
<td>(B)</td>
<td>Überspannungsschutz</td>
</tr>
<tr>
<td>M 1.26</td>
<td>(W)</td>
<td>Not-Aus-Schalter</td>
</tr>
<tr>
<td>M 1.27</td>
<td>(B)</td>
<td>Klimatisierung</td>
</tr>
<tr>
<td>M 1.31</td>
<td>(Z)</td>
<td>Fernanzeige von Störungen</td>
</tr>
<tr>
<td>M 1.47</td>
<td>(B)</td>
<td>Eigener Brandabschnitt</td>
</tr>
<tr>
<td>M 1.48</td>
<td>(B)</td>
<td>Brandmeldeanlage</td>
</tr>
<tr>
<td>M 1.49</td>
<td>(A)</td>
<td>Technische und organisatorische Vorgaben für das Rechenzentrum</td>
</tr>
<tr>
<td>M 1.50</td>
<td>(C)</td>
<td>Rauchschutz</td>
</tr>
<tr>
<td>M 1.52</td>
<td>(W)</td>
<td>Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur</td>
</tr>
<tr>
<td>M 1.53</td>
<td>(Z)</td>
<td>Videoüberwachung</td>
</tr>
<tr>
<td>M 1.54</td>
<td>(Z)</td>
<td>Brandfrühsterkennung / Löschtechnik</td>
</tr>
<tr>
<td>M 1.55</td>
<td>(Z)</td>
<td>Perimeterschutz</td>
</tr>
</tbody>
</table>
### Umsetzung

<table>
<thead>
<tr>
<th>M 1.57</th>
<th>(A)</th>
<th>Aktuelle Infrastruktur- und Baupläne</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.21</td>
<td>(A)</td>
<td>Rauchverbot</td>
</tr>
<tr>
<td>M 2.212</td>
<td>(B)</td>
<td>Organisatorische Vorgaben für die Gebäudereinigung</td>
</tr>
<tr>
<td>M 2.213</td>
<td>(A)</td>
<td>Inspektion und Wartung der technischen Infrastruktur</td>
</tr>
</tbody>
</table>

### Betrieb

<table>
<thead>
<tr>
<th>M 1.15</th>
<th>(A)</th>
<th>Geschlossene Fenster und Türen</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 1.23</td>
<td>(A)</td>
<td>Abgeschlossene Türen</td>
</tr>
<tr>
<td>M 1.71</td>
<td>(C)</td>
<td>Funktionstests der technischen Infrastruktur</td>
</tr>
<tr>
<td>M 1.72</td>
<td>(Z)</td>
<td>Baumaßnahmen während des laufenden Betriebs</td>
</tr>
<tr>
<td>M 1.73</td>
<td>(A)</td>
<td>Schutz eines Rechenzentrums gegen unbefugten Zutritt</td>
</tr>
</tbody>
</table>

### Notfallvorsorge

<table>
<thead>
<tr>
<th>M 6.17</th>
<th>(A)</th>
<th>Alarmierungsplan und Brandschutzübungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 6.74</td>
<td>(Z)</td>
<td>Notfallarchiv</td>
</tr>
</tbody>
</table>
3 Bausteine für IT-Systeme

3.1 Allgemeiner Server (B 3.101)

3.1.1 Beschreibung


3.1.2 Gefährdungslage


Höhere Gewalt

| G 1.1 | Personalausfall |
| G 1.2 | Ausfall von IT-Systemen |

Organisatorische Mängel

| G 2.7 | Unerlaubte Ausübung von Rechten |
| G 2.9 | Mangelhafte Anpassung an Veränderungen beim IT-Einsatz |
| G 2.36 | Ungeeignete Einschränkung der Benutzerumgebung |

Menschliche Fehlhandlungen

<p>| G 3.2 | Fahrlässige Zerstörung von Gerät oder Daten |
| G 3.3 | Nichtbeachtung von Sicherheitsmaßnahmen |
| G 3.5 | Unbeabsichtigte Leitungsbeschädigung |</p>
<table>
<thead>
<tr>
<th>G 3.6</th>
<th>Gefährdung durch Reinigungs- oder Fremdpersonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 3.8</td>
<td>Fehlerhafte Nutzung von IT-Systemen</td>
</tr>
<tr>
<td>G 3.9</td>
<td>Fehlerhafte Administration von IT-Systemen</td>
</tr>
</tbody>
</table>

### Technisches Versagen

<table>
<thead>
<tr>
<th>G 4.1</th>
<th>Ausfall der Stromversorgung</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.6</td>
<td>Spannungsschwankungen/Überspannung/Unterspannung</td>
</tr>
<tr>
<td>G 4.7</td>
<td>Defekte Datenträger</td>
</tr>
<tr>
<td>G 4.10</td>
<td>Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen</td>
</tr>
<tr>
<td>G 4.13</td>
<td>Verlust gespeicherter Daten</td>
</tr>
<tr>
<td>G 4.20</td>
<td>Datenverlust bei erschöpftem Speichermedium</td>
</tr>
<tr>
<td>G 4.22</td>
<td>Software-Schwachstellen oder -Fehler</td>
</tr>
<tr>
<td>G 4.39</td>
<td>Software-Konzeptionsfehler</td>
</tr>
</tbody>
</table>

### Vorsätzliche Handlungen

<table>
<thead>
<tr>
<th>G 5.1</th>
<th>Manipulation oder Zerstörung von Geräten oder Zubehör</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.2</td>
<td>Manipulation an Informationen oder Software</td>
</tr>
<tr>
<td>G 5.7</td>
<td>Abhören von Leitungen</td>
</tr>
<tr>
<td>G 5.9</td>
<td>Unberechtigte IT-Nutzung</td>
</tr>
<tr>
<td>G 5.15</td>
<td>Neugierige Mitarbeiter</td>
</tr>
<tr>
<td>G 5.18</td>
<td>Systematisches Ausprobieren von Passwörtern</td>
</tr>
<tr>
<td>G 5.19</td>
<td>Missbrauch von Benutzerrechten</td>
</tr>
<tr>
<td>G 5.20</td>
<td>Missbrauch von Administratorrechten</td>
</tr>
<tr>
<td>G 5.21</td>
<td>Trojanische Pferde</td>
</tr>
<tr>
<td>G 5.23</td>
<td>Schadprogramme</td>
</tr>
<tr>
<td>G 5.26</td>
<td>Analyse des Nachrichtenflusses</td>
</tr>
<tr>
<td>G 5.40</td>
<td>Abhören von Räumen mittels Rechner mit Mikrofon</td>
</tr>
<tr>
<td>G 5.71</td>
<td>Vertraulichkeitsverlust schützenswerter Informationen</td>
</tr>
<tr>
<td>G 5.75</td>
<td>Überlastung durch eingehende E-Mails</td>
</tr>
<tr>
<td>G 5.85</td>
<td>Integritätsverlust schützenswerter Informationen</td>
</tr>
</tbody>
</table>

### 3.1.3 Maßnahmen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Model-
lierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines Servers sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Ein besonderes Gewicht ist dabei auf die konzeptionellen Planungsmaßnahmen zu legen, wenn der Server im Rahmen des Aufbaus eines neuen servergestützten Netzes installiert wird. Sofern die Installation dagegen als Ausbau eines schon existierenden Netzes erfolgt, können sich die Planungsmaßnahmen häufig darauf beschränken, auf die Konformität des neuen Servers mit den schon vorhandenen Strukturen zu achten. Die Maßnahmen zur Beschaffung und zum Betrieb des Servers sind dagegen in jedem Fall umzusetzen. Die Schritte, die zum Schutz eines Servers zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

<table>
<thead>
<tr>
<th>Maßnahme</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 1.28 (B)</td>
<td>Lokale unterbrechungsfreie Stromversorgung</td>
</tr>
<tr>
<td>M 2.314 (Z)</td>
<td>Verwendung von hochverfügbaren Architekturen für Server</td>
</tr>
<tr>
<td>M 2.315 (A)</td>
<td>Planung des Servereinsatzes</td>
</tr>
<tr>
<td>M 2.316 (A)</td>
<td>Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server</td>
</tr>
<tr>
<td>M 4.250 (Z)</td>
<td>Auswahl eines zentralen, netzbasierten Authentisierungsdiens tes</td>
</tr>
<tr>
<td>M 5.10 (A)</td>
<td>Restriktive Rechtevergabe</td>
</tr>
<tr>
<td>M 1.138 (Z)</td>
<td>Einsatz von RADIUS-Servern</td>
</tr>
</tbody>
</table>

**Beschaffung**

<table>
<thead>
<tr>
<th>Maßnahme</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.317 (C)</td>
<td>Beschaffungskriterien für einen Server</td>
</tr>
</tbody>
</table>

**Umsetzung**

<table>
<thead>
<tr>
<th>Maßnahme</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.32 (Z)</td>
<td>Einrichtung einer eingeschränkten Benutzerumgebung</td>
</tr>
<tr>
<td>M 2.204 (A)</td>
<td>Verhinderung ungesicherter Netzzugänge</td>
</tr>
<tr>
<td>M 2.318 (A)</td>
<td>Sichere Installation eines Servers</td>
</tr>
<tr>
<td>M 4.7 (A)</td>
<td>Änderung voreingestellter Passwörter</td>
</tr>
<tr>
<td>M 4.15 (A)</td>
<td>Gesichertes Login</td>
</tr>
<tr>
<td>M 4.16 (A)</td>
<td>Zugangsbeschränkungen für Accounts und / oder Terminals</td>
</tr>
<tr>
<td>M 4.17 (A)</td>
<td>Sperren und Löschen nicht benötigter Accounts und Terminals</td>
</tr>
<tr>
<td>M 4.40 (C)</td>
<td>Verhinderung der unautorisierten Nutzung des Rechnermikrofons</td>
</tr>
<tr>
<td>M 4.237 (A)</td>
<td>Sichere Grundkonfiguration eines IT-Systems</td>
</tr>
</tbody>
</table>
### Betrieb

<table>
<thead>
<tr>
<th>M 2.22</th>
<th>(A) Hinterlegen des Passwortes</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.273</td>
<td>(A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates</td>
</tr>
<tr>
<td>M 4.24</td>
<td>(A) Sicherstellung einer konsistenten Systemverwaltung</td>
</tr>
<tr>
<td>M 4.93</td>
<td>(Z) Regelmäßige Integritätsprüfung</td>
</tr>
<tr>
<td>M 4.238</td>
<td>(A) Einsatz eines lokalen Paketfilters</td>
</tr>
<tr>
<td>M 4.239</td>
<td>(A) Sicherer Betrieb eines Servers</td>
</tr>
<tr>
<td>M 4.240</td>
<td>(Z) Einrichten einer Testumgebung für einen Server</td>
</tr>
<tr>
<td>M 5.8</td>
<td>(B) Regelmäßiger Sicherheitscheck des Netzes</td>
</tr>
<tr>
<td>M 5.9</td>
<td>(B) Protokollierung am Server</td>
</tr>
</tbody>
</table>

### Aussonderung

<table>
<thead>
<tr>
<th>M 2.319</th>
<th>(C) Migration eines Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.320</td>
<td>(A) Geregelte Außerbetriebnahme eines Servers</td>
</tr>
</tbody>
</table>

### Notfallvorsorge

<table>
<thead>
<tr>
<th>M 6.24</th>
<th>(A) Erstellen eines Notfall-Bootmediums</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 6.96</td>
<td>(A) Notfallvorsorge für einen Server</td>
</tr>
</tbody>
</table>

### 3.2 Server unter Unix (B 3.102)

#### 3.2.1 Beschreibung


- klassischen Unix-Systemen oder Unix-Derivaten,
- zertifizierten UNIX-Systemen (UNIX ist ein Warenzeichen der Open Group, das nur zertifizierte Systeme tragen dürfen, die die entsprechende Spezifikation erfüllen) und
- funktionellen Unix-Systemen oder unix-ähnlichen Systemen.
Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Linux ist kein klassisches Unix (der Kernel basiert nicht auf dem ursprünglichen Quelltext, aus dem sich die verschiedenen Unix-Derivate entwickelt haben), sondern ein funktionelles Unix-System. In diesem Baustein werden alle Betriebssysteme der Unix-Familie betrachtet, also auch Linux als funktionelles Unix-System. In diesem Baustein werden ausschließlich die für einen Unix-Server spezifischen Gefährdungen und Maßnahmen beschrieben, daher sind zusätzlich noch diejenigen für allgemeine Server aus Baustein B 3.101 zu betrachten.

### 3.2.2 Gefährdungslage

Für den IT-Grundschutz eines Unix-Servers werden folgende Gefährdungen angenommen:

**Organisatorische Mängel**

<table>
<thead>
<tr>
<th>G 2.15</th>
<th>Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.36</td>
<td>Ungeeignete Einschränkung der Benutzerumgebung</td>
</tr>
</tbody>
</table>

**Menschliche Fehlhandlungen**

<table>
<thead>
<tr>
<th>G 3.10</th>
<th>Falsches Exportieren von Dateisystemen unter Unix</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 3.11</td>
<td>Fehlerhafte Konfiguration von sendmail</td>
</tr>
</tbody>
</table>

**Technisches Versagen**

<table>
<thead>
<tr>
<th>G 4.11</th>
<th>Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.12</td>
<td>Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client</td>
</tr>
</tbody>
</table>

**Vorsätzliche Handlungen**

<table>
<thead>
<tr>
<th>G 5.41</th>
<th>Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.89</td>
<td>Hijacking von Netz-Verbindungen</td>
</tr>
</tbody>
</table>

41
3.2.3 Maßnahmen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines Servers unter Unix sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb dieses Servers. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

<table>
<thead>
<tr>
<th>Maßnahme</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.33</td>
<td>Aufteilung der Administrationstätigkeiten unter Unix</td>
</tr>
<tr>
<td>M 4.13</td>
<td>Sorgfältige Vergabe von IDs</td>
</tr>
<tr>
<td>M 4.18</td>
<td>Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus</td>
</tr>
<tr>
<td>M 5.16</td>
<td>Übersicht über Netzdienste</td>
</tr>
<tr>
<td>M 5.34</td>
<td>Einsatz von Einmalpasswörtern</td>
</tr>
<tr>
<td>M 5.64</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>M 5.83</td>
<td>Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN</td>
</tr>
</tbody>
</table>

**Umsetzung**

<table>
<thead>
<tr>
<th>Maßnahme</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 4.9</td>
<td>Einsatz der Sicherheitsmechanismen von X-Window</td>
</tr>
<tr>
<td>M 4.14</td>
<td>Obligatorischer Passwortschutz unter Unix</td>
</tr>
<tr>
<td>M 4.19</td>
<td>Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen</td>
</tr>
<tr>
<td>M 4.20</td>
<td>Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen</td>
</tr>
<tr>
<td>M 4.21</td>
<td>Verhinderung des unautorisierten Erlangens von Administratorrechten</td>
</tr>
<tr>
<td>M 4.22</td>
<td>Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System</td>
</tr>
<tr>
<td>M 4.23</td>
<td>Sicherer Aufruf ausführbarer Dateien</td>
</tr>
<tr>
<td>M 4.105</td>
<td>Erste Maßnahmen nach einer Unix-Standardinstallation</td>
</tr>
<tr>
<td>M 4.106</td>
<td>Aktivieren der Systemprotokollierung</td>
</tr>
<tr>
<td>M 5.17</td>
<td>Einsatz der Sicherheitsmechanismen von NFS</td>
</tr>
<tr>
<td>M 5.18</td>
<td>Einsatz der Sicherheitsmechanismen von NIS</td>
</tr>
<tr>
<td>M 5.19</td>
<td>Einsatz der Sicherheitsmechanismen von sendmail</td>
</tr>
<tr>
<td>M 5.20</td>
<td>Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp</td>
</tr>
<tr>
<td>M 5.21</td>
<td>Sicherer Einsatz von telnet, ftp, tftp und rexec</td>
</tr>
</tbody>
</table>
Einsatz der Sicherheitsmechanismen von UUCP

Deaktivieren nicht benötigter Netzdienste

Betrieb

Einsatz der Protokollierung im Unix-System

Regelmäßiger Sicherheitscheck des Unix-Systems

Notfallvorsorge

Verhaltensregeln nach Verlust der Systemintegrität

### 3.3 Sicherheitsgateway (Firewall) (B 3.301)

#### 3.3.1 Beschreibung


Die Verwendung des Begriffs Sicherheitsgateway anstatt des üblicherweise verwendeten Begriffs „Firewall“ soll verdeutlichen, dass zur Absicherung von Netzübergängen heute oft nicht mehr ein einzelnes Gerät verwendet wird, sondern eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. Paketfilterung, Schutz vor Viren oder die Überwachung des Netzverkehrs („Intrusion Detection“).

3.3.2 Gefährdungslage

Für den IT-Grundschutz eines Sicherheitsgateways werden die folgenden Gefährdungen angenommen:

**Organisatorische Mängel**

<table>
<thead>
<tr>
<th>G 2.24</th>
<th>Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.101</td>
<td>Unzureichende Notfallvorsorge bei einem Sicherheitsgateway</td>
</tr>
</tbody>
</table>

**Menschliche Fehlhandlungen**

<table>
<thead>
<tr>
<th>G 3.3</th>
<th>Nichtbeachtung von Sicherheitsmaßnahmen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 3.9</td>
<td>Fehlerhafte Administration von IT-Systemen</td>
</tr>
<tr>
<td>G 3.38</td>
<td>Konfigurations- und Bedienungsfehler</td>
</tr>
</tbody>
</table>

**Technisches Versagen**

<table>
<thead>
<tr>
<th>G 4.8</th>
<th>Bekanntwerden von Softwareschwachstellen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.10</td>
<td>Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen</td>
</tr>
<tr>
<td>G 4.11</td>
<td>Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client</td>
</tr>
<tr>
<td>G 4.12</td>
<td>Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client</td>
</tr>
<tr>
<td>G 4.20</td>
<td>Datenverlust bei erschöpftem Speichermedium</td>
</tr>
<tr>
<td>G 4.22</td>
<td>Software-Schwachstellen oder -Fehler</td>
</tr>
<tr>
<td>G 4.39</td>
<td>Software-Konzeptionsfehler</td>
</tr>
</tbody>
</table>

**Vorsätzliche Handlungen**

<table>
<thead>
<tr>
<th>G 5.2</th>
<th>Manipulation an Informationen oder Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.9</td>
<td>Unberechtigte IT-Nutzung</td>
</tr>
<tr>
<td>G 5.18</td>
<td>Systematisches Ausprobieren von Passwörtern</td>
</tr>
<tr>
<td>G 5.24</td>
<td>Wiedereinspielen von Nachrichten</td>
</tr>
<tr>
<td>G 5.25</td>
<td>Maskerade</td>
</tr>
<tr>
<td>G 5.28</td>
<td>Verhinderung von Diensten</td>
</tr>
<tr>
<td>G 5.39</td>
<td>Eindringen in Rechnersysteme über Kommunikationskarten</td>
</tr>
<tr>
<td>G 5.48</td>
<td>IP-Spoofing</td>
</tr>
<tr>
<td>G 5.49</td>
<td>Missbrauch des Source-Routing</td>
</tr>
</tbody>
</table>
### 3.3.3 Maßnahmen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Sicherheitsgateway schützt nicht vor Angriffen, die innerhalb des internen Netzes erfolgen. Um das interne Netz gegen Angriffe von Innenländern zu schützen, müssen auch beim Einsatz eines Sicherheitsgateways alle erforderlichen Sicherheitsmaßnahmen umgesetzt sein. Wenn es sich bei dem internen Netz beispielsweise um ein Unix-bzw. PC-Netz handelt, sind die in den jeweiligen Bausteinen beschriebenen Sicherheitsmaßnahmen umzusetzen.


#### Planung und Konzeption

| M 2.70 (A) | Entwicklung eines Konzepts für Sicherheitsgateways |
| M 2.71 (A) | Festlegung einer Policy für ein Sicherheitsgateway |
| M 2.301 (Z) | Outsourcing des Sicherheitsgateway |

#### Beschaffung

| M 2.73 (A) | Auswahl geeigneter Grundstrukturen für Sicherheitsgateways |
| M 2.74 (A) | Geeignete Auswahl eines Paketfilters |
| M 2.75 (A) | Geeignete Auswahl eines Application-Level-Gateways |
| M 2.299 (A) | Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway |
### Umsetzung

<table>
<thead>
<tr>
<th>M 2.76</th>
<th>(A)</th>
<th>Auswahl und Einrichtung geeigneter Filterregeln</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.77</td>
<td>(A)</td>
<td>Integration von Servern in das Sicherheitsgateway</td>
</tr>
<tr>
<td>M 3.43</td>
<td>(C)</td>
<td>Schulung der Administratoren des Sicherheitsgateways</td>
</tr>
<tr>
<td>M 4.224</td>
<td>(Z)</td>
<td>Integration von VPN-Komponenten in ein Sicherheitsgateway</td>
</tr>
</tbody>
</table>

### Betrieb

<table>
<thead>
<tr>
<th>M 2.78</th>
<th>(A)</th>
<th>Sicherer Betrieb eines Sicherheitsgateways</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.302</td>
<td>(Z)</td>
<td>Sicherheitsgateways und Hochverfügbarkeit</td>
</tr>
<tr>
<td>M 4.47</td>
<td>(A)</td>
<td>Protokollierung der Sicherheitsgateway-Aktivitäten</td>
</tr>
<tr>
<td>M 4.100</td>
<td>(C)</td>
<td>Sicherheitsgateways und aktive Inhalte</td>
</tr>
<tr>
<td>M 4.101</td>
<td>(C)</td>
<td>Sicherheitsgateways und Verschlüsselung</td>
</tr>
<tr>
<td>M 4.222</td>
<td>(B)</td>
<td>Festlegung geeigneter Einstellungen von Sicherheitsproxies</td>
</tr>
<tr>
<td>M 4.223</td>
<td>(B)</td>
<td>Integration von Proxy-Servern in das Sicherheitsgateway</td>
</tr>
<tr>
<td>M 4.225</td>
<td>(Z)</td>
<td>Einsatz eines Protokollierungsservers in einem Sicherheitsgateway</td>
</tr>
<tr>
<td>M 4.226</td>
<td>(Z)</td>
<td>Integration von Virensannern in ein Sicherheitsgateway</td>
</tr>
<tr>
<td>M 4.227</td>
<td>(C)</td>
<td>Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation</td>
</tr>
<tr>
<td>M 5.39</td>
<td>(A)</td>
<td>Sicherer Einsatz der Protokolle und Dienste</td>
</tr>
<tr>
<td>M 5.46</td>
<td>(A)</td>
<td>Einsatz von Stand-alone-Systemen zur Nutzung des Internets</td>
</tr>
<tr>
<td>M 5.59</td>
<td>(A)</td>
<td>Schutz vor DNS-Spoofing</td>
</tr>
<tr>
<td>M 5.70</td>
<td>(A)</td>
<td>Adressumsetzung - NAT (Network Address Translation)</td>
</tr>
<tr>
<td>M 5.71</td>
<td>(Z)</td>
<td>Intrusion Detection und Intrusion Response Systeme</td>
</tr>
<tr>
<td>M 5.115</td>
<td>(Z)</td>
<td>Integration eines Webserver in ein Sicherheitsgateway</td>
</tr>
<tr>
<td>M 5.116</td>
<td>(Z)</td>
<td>Integration eines E-Mailserver in ein Sicherheitsgateway</td>
</tr>
<tr>
<td>M 5.117</td>
<td>(Z)</td>
<td>Integration eines Datenbank-Servers in ein Sicherheitsgateway</td>
</tr>
<tr>
<td>M 5.118</td>
<td>(Z)</td>
<td>Integration eines DNS-Servers in ein Sicherheitsgateway</td>
</tr>
<tr>
<td>M 5.119</td>
<td>(Z)</td>
<td>Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway</td>
</tr>
<tr>
<td>M 5.120</td>
<td>(A)</td>
<td>Behandlung von ICMP am Sicherheitsgateway</td>
</tr>
</tbody>
</table>

### Aussonderung

| M 2.300 | (C) | Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways |
Notfallvorsorge

M 6.94 (C) Notfallvorsorge bei Sicherheitsgateways

3.4 Router und Switches (B 3.302)

3.4.1 Beschreibung

Netze spielen eine immer wichtigere Rolle als Teile der IT-Infrastruktur, weil Anwendungen heutzutage vermehrt über lokale Netze oder Weitverkehrsnetze betrieben werden. Die Verfügbarkeit, Integrität und Vertraulichkeit der Netze muss sichergestellt sein und mindestens den Anforderungen der Anwendungen an den Schutz dieser drei Grundwerte der IT-Sicherheit entsprechen.


3.4.2 Gefährdungslage

Neben den Gefährdungen, die generell für den Großteil der IT-Systeme gelten, existieren für aktive Netzkomponenten eine Reihe spezieller Gefährdungen.


Aktive Netzkomponenten werden oft mit einer unsicheren Default-Konfiguration ausgeliefert (siehe G 4.49 Unsichere Default-Einstellungen auf Routern und Switches), die bei der Inbetriebnahme der Geräte geprüft werden sollte. Für die sichere Trennung von Teilnetzen mit unterschiedlichem Schutzbedarf wird gelegentlich die Nutzung von virtuellen Netzen (VLANs) vorgeschlagen. Es sind jedoch einige Angriffsmethoden bekannt, die es ermöglichen, die Grenzen zwischen VLANs zu überwinden und unberechtigt auf andere VLANs zuzugreifen (siehe G 5.115 Überwindung der Grenzen zwischen VLANs).
Nachfolgend ist die Gefährdungslage beim Einsatz von Routern und Switches als Übersicht dargestellt:

Organisatorische Mängel

<table>
<thead>
<tr>
<th>G 2.1</th>
<th>Fehlende oder unzureichende Regelungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.3</td>
<td>Fehlende, ungeeignete, inkompatible Betriebsmittel</td>
</tr>
<tr>
<td>G 2.4</td>
<td>Unzureichende Kontrolle der Sicherheitsmaßnahmen</td>
</tr>
<tr>
<td>G 2.22</td>
<td>Fehlende Auswertung von Protokolldaten</td>
</tr>
<tr>
<td>G 2.27</td>
<td>Fehlende oder unzureichende Dokumentation</td>
</tr>
<tr>
<td>G 2.44</td>
<td>Inkompatible aktive und passive Netzkomponenten</td>
</tr>
<tr>
<td>G 2.54</td>
<td>Vertraulichkeitsverlust durch Restinformationen</td>
</tr>
<tr>
<td>G 2.98</td>
<td>Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches</td>
</tr>
</tbody>
</table>

Menschliche Fehlhandlungen

<table>
<thead>
<tr>
<th>G 3.64</th>
<th>Fehlerhafte Konfiguration von Routern und Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 3.65</td>
<td>Fehlerhafte Administration von Routern und Switches</td>
</tr>
</tbody>
</table>

Technisches Versagen

<table>
<thead>
<tr>
<th>G 4.8</th>
<th>Bekanntwerden von Softwareschwachstellen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.49</td>
<td>Unsichere Default-Einstellungen auf Routern und Switches</td>
</tr>
</tbody>
</table>

Vorsätzliche Handlungen

<table>
<thead>
<tr>
<th>G 5.4</th>
<th>Diebstahl</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.51</td>
<td>Missbrauch der Routing-Protokolle</td>
</tr>
<tr>
<td>G 5.66</td>
<td>Unberechtigter Anschluss von IT-Systemen an ein Netz</td>
</tr>
<tr>
<td>G 5.112</td>
<td>Manipulation von ARP-Tabellen</td>
</tr>
<tr>
<td>G 5.113</td>
<td>MAC-Spoofing</td>
</tr>
<tr>
<td>G 5.114</td>
<td>Missbrauch von Spanning Tree</td>
</tr>
<tr>
<td>G 5.115</td>
<td>Überwindung der Grenzen zwischen VLANs</td>
</tr>
</tbody>
</table>

3.4.3 Maßnahmen

Die diesem Baustein zugeordneten Sicherheitsmaßnahmen orientieren sich an dem Lebenszyklus der aktiven Netzkomponenten.
### Planung und Konzeption

| M 2.276 (Z) | Funktionsweise eines Routers |
| M 2.277 (Z) | Funktionsweise eines Switches |
| M 2.278 (Z) | Typische Einsatzszenarien von Routern und Switches |
| M 2.279 (A) | Erstellung einer Sicherheitsrichtlinie für Router und Switches |

### Beschaffung

| M 2.280 (C) | Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches |

### Umsetzung

| M 1.43 (A) | Gesicherte Aufstellung aktiver Netzkomponenten |
| M 3.38 (B) | Administratorenschulung für Router und Switches |
| M 4.201 (A) | Sichere lokale Grundkonfiguration von Routern und Switches |
| M 4.202 (A) | Sichere Netz-Grundkonfiguration von Routern und Switches |
| M 4.203 (A) | Konfigurations-Checkliste für Router und Switches |
| M 5.111 (C) | Einrichtung von Access Control Lists auf Routern |

### Betrieb

| M 2.281 (A) | Dokumentation der Systemkonfiguration von Routern und Switches |
| M 2.282 (A) | Regelmäßige Kontrolle von Routern und Switches |
| M 2.283 (B) | Software-Pflege auf Routern und Switches |
| M 4.204 (C) | Sichere Administration von Routern und Switches |
| M 4.205 (C) | Protokollierung bei Routern und Switches |
| M 4.206 (C) | Sicherung von Switch-Ports |
| M 5.112 (C) | Sicherheitsaspekte von Routing-Protokollen |

### Aussonderung

| M 2.284 (C) | Sichere Außerbetriebnahme von Routern und Switches |

### Notfallvorsorge

| M 6.91 (C) | Datensicherung und Recovery bei Routern und Switches |
| M 6.92 | (C) | Notfallvorsorge bei Routern und Switches |
4 Bausteine für Netze

4.1 Heterogene Netze (B 4.1)

4.1.1 Beschreibung


4.1.2 Gefährdungslage

Für den IT-Grundschtutz eines heterogenen Netzes werden die folgenden Gefährdungen angenommen:

<table>
<thead>
<tr>
<th>Höhere Gewalt</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>G 1.2</td>
<td>Ausfall von IT-Systemen</td>
</tr>
<tr>
<td>G 1.3</td>
<td>Blitz</td>
</tr>
<tr>
<td>G 1.4</td>
<td>Feuer</td>
</tr>
<tr>
<td>G 1.5</td>
<td>Wasser</td>
</tr>
<tr>
<td>G 1.7</td>
<td>Unzulässige Temperatur und Luftfeuchte</td>
</tr>
<tr>
<td>G 1.8</td>
<td>Staub, Verschmutzung</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organisatorische Mängel</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.7</td>
<td>Unerlaubte Ausübung von Rechten</td>
</tr>
<tr>
<td>G 2.9</td>
<td>Mangelhafte Anpassung an Veränderungen beim IT-Einsatz</td>
</tr>
<tr>
<td>G 2.22</td>
<td>Fehlende Auswertung von Protokolldaten</td>
</tr>
<tr>
<td>G 2.27</td>
<td>Fehlende oder unzureichende Dokumentation</td>
</tr>
<tr>
<td>G 2.32</td>
<td>Unzureichende Leitungskapazitäten</td>
</tr>
<tr>
<td>G 2.44</td>
<td>Inkompatible active und passive Netzkomponenten</td>
</tr>
<tr>
<td>G 2.45</td>
<td>Konzeptionelle Schwächen des Netzes</td>
</tr>
<tr>
<td>G 2.46</td>
<td>Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße</td>
</tr>
</tbody>
</table>
Menschliche Fehlhandlungen

| G 3.2 | Fahrlässige Zerstörung von Gerät oder Daten |
| G 3.3 | Nichtbeachtung von Sicherheitsmaßnahmen |
| G 3.5 | Unbeabsichtigte Leitungsbeschädigung |
| G 3.6 | Gefährdung durch Reinigungs- oder Fremdpersonal |
| G 3.8 | Fehlerhafte Nutzung von IT-Systemen |
| G 3.9 | Fehlerhafte Administration von IT-Systemen |
| G 3.28 | Ungeeignete Konfiguration der aktiven Netzkomponenten |
| G 3.29 | Fehlende oder ungeeignete Segmentierung |

Technisches Versagen

| G 4.1 | Ausfall der Stromversorgung |
| G 4.10 | Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen |
| G 4.31 | Ausfall oder Störung von Netzkomponenten |

Vorsätzliche Handlungen

| G 5.1 | Manipulation oder Zerstörung von Geräten oder Zubehör |
| G 5.2 | Manipulation an Informationen oder Software |
| G 5.4 | Diebstahl |
| G 5.5 | Vandalismus |
| G 5.6 | Anschlag |
| G 5.7 | Abhören von Leitungen |
| G 5.8 | Manipulation an Leitungen |
| G 5.9 | Unberechtigte IT-Nutzung |
| G 5.18 | Systematisches Ausprobieren von Passwörtern |
| G 5.20 | Missbrauch von Administratorrechten |
| G 5.28 | Verhinderung von Diensten |
| G 5.66 | Unberechtigter Anschluss von IT-Systemen an ein Netz |
| G 5.67 | Unberechtigte Ausführung von Netzmanagement-Funktionen |
| G 5.68 | Unberechtigter Zugang zu den aktiven Netzkomponenten |

4.1.3 Maßnahmen

Planung und Konzeption
**Umsetzung**

| M 4.7  | (A) | Änderung voreingestellter Passwörter |
| M 4.80 | (B) | Sichere Zugriffsmechanismen bei Fernadministration |
| M 4.82 | (A) | Sichere Konfiguration der aktiven Netzkomponenten |
| M 5.7  | (A) | Netzverwaltung |

**Betrieb**

| M 4.81 | (B) | Audit und Protokollierung der Aktivitäten im Netz |
| M 4.83 | (C) | Update/Upgrade von Soft- und Hardware im Netzbereich |

**Notfallvorsorge**

| M 6.52 | (A) | Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten |
| M 6.53 | (Z) | Redundante Auslegung der Netzkomponenten |
| M 6.54 | (B) | Verhaltensregeln nach Verlust der Netzintegrität |
| M 6.75 | (Z) | Redundante Kommunikationsverbindungen |

### 4.2 Netz- und Systemmanagement (B 4.2)

#### 4.2.1 Beschreibung

Ein Managementsystem für ein im Allgemeinen lokales Rechnernetz (LAN, VLAN) dient dazu, möglichst alle im lokale Netz angesiedelten Hard- und Software-Komponenten...


4.2.2 Gefährdungslage

Für den IT-Grundschutz eines Managementsystems werden die folgenden Gefährdungen angenommen:

Höhere Gewalt

| G 1.1 | Personalausfall |
| G 1.2 | Ausfall von IT-Systemen |

Organisatorische Mängel

| G 2.27 | Fehlende oder unzureichende Dokumentation |
| G 2.32 | Unzureichende Leitungskapazitäten |
| G 2.59 | Betreiben von nicht angemeldeten Komponenten |
| G 2.60 | Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement |
| G 2.61 | Unberechtigte Sammlung personenbezogener Daten |

Menschliche Fehlhandlungen

| G 3.9 | Fehlerhafte Administration von IT-Systemen |
| G 3.28 | Ungeeignete Konfiguration der aktiven Netzkomponenten |
| G 3.34 | Ungeeignete Konfiguration des Managementsystems |
| G 3.35 | Server im laufenden Betrieb ausschalten |

54
### Fehlinterpretation von Ereignissen

**G 3.36** Fehlinterpretation von Ereignissen

### Technisches Versagen

<table>
<thead>
<tr>
<th>G 4.31</th>
<th>Ausfall oder Störung von Netzkomponenten</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 4.38</td>
<td>Ausfall von Komponenten eines Netz- und Systemmanagementsystems</td>
</tr>
</tbody>
</table>

### Vorsätzliche Handlungen

<table>
<thead>
<tr>
<th>G 5.2</th>
<th>Manipulation an Informationen oder Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 5.8</td>
<td>Manipulation an Leitungen</td>
</tr>
<tr>
<td>G 5.9</td>
<td>Unberechtigte IT-Nutzung</td>
</tr>
<tr>
<td>G 5.18</td>
<td>Systematisches Ausprobieren von Passwörtern</td>
</tr>
<tr>
<td>G 5.28</td>
<td>Verhinderung von Diensten</td>
</tr>
<tr>
<td>G 5.66</td>
<td>Unberechtigter Anschluss von IT-Systemen an ein Netz</td>
</tr>
<tr>
<td>G 5.67</td>
<td>Unberechtigte Ausführung von Netzmanagement-Funktionen</td>
</tr>
<tr>
<td>G 5.86</td>
<td>Manipulation von Managementparametern</td>
</tr>
</tbody>
</table>

### 4.2.3 Maßnahmen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.


Da Managementsysteme von einem zentralistischen Ansatz ausgehen, kommt der zentralen Managementstation eine besondere Bedeutung unter Sicherheitsgesichtspunkten zu und ist daher besonders zu schützen. Zentrale Komponenten eines Managementsystems
sollten daher in Räumen aufgestellt werden, die den Anforderungen an einen Serverraum (vergleiche Baustein B 2.4 Serverraum) entsprechen.

**Planung und Konzeption**

<table>
<thead>
<tr>
<th>M 2.143 (A)</th>
<th>Entwicklung eines Netzmanagementkonzeptes</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.144 (A)</td>
<td>Geeignete Auswahl eines Netzmanagement-Protokolls</td>
</tr>
<tr>
<td>M 2.168 (A)</td>
<td>IT-System-Analyse vor Einführung eines Systemmanagement-Systems</td>
</tr>
<tr>
<td>M 2.169 (A)</td>
<td>Entwickeln einer Systemmanagementstrategie</td>
</tr>
</tbody>
</table>

**Beschaffung**

<table>
<thead>
<tr>
<th>M 2.145 (B)</th>
<th>Anforderungen an ein Netzmanagement-Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.170 (A)</td>
<td>Anforderungen an ein Systemmanagementsystem</td>
</tr>
<tr>
<td>M 2.171 (A)</td>
<td>Geeignete Auswahl eines Systemmanagement-Produktes</td>
</tr>
</tbody>
</table>

**Umsetzung**

| M 4.91 (A) | Sichere Installation eines Systemmanagementsystems |

**Betrieb**

<table>
<thead>
<tr>
<th>M 2.146 (A)</th>
<th>Sicherer Betrieb eines Netzmanagementsystems</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 4.92 (A)</td>
<td>Sicherer Betrieb eines Systemmanagementsystems</td>
</tr>
</tbody>
</table>

**Notfallvorsorge**

| M 6.57 (C) | Erstellen eines Notfallplans für den Ausfall des Managementsystems |
5 Bausteine für Anwendungen

5.1 Webserver (B 5.4)

5.1.1 Beschreibung

Das Internet ist eines der zentralen Medien der heutigen Informationsgesellschaft. Die Informationsangebote im Internet werden von Servern bereitgestellt, die Daten, meist Dokumente in Form von HTML-Seiten, an entsprechende Clientprogramme ausliefern. Dies erfolgt typischerweise über die Protokolle HTTP (Hypertext Transfer Protocol) oder HTTPS (HTTP über SSL bzw. TLS, d. h. HTTP geschützt durch eine verschlüsselte Verbindung). Neben dem Einsatz im Internet werden Webserver auch in zunehmendem Maße für interne Informationen und Anwendungen in Firmennetzen (Intranet) eingesetzt. Ein Grund dafür ist, dass sie eine einfache und standardisierte Schnittstelle zwischen Server-Anwendungen und Benutzern bieten und entsprechende Client-Software (Webbrowser) für praktisch jede Betriebssystemumgebung kostenlos verfügbar ist.

Die Bezeichnung Webserver (oder auch WWW-Server) wird meist sowohl für das Programm benutzt, welches die HTTP-Anfragen beantwortet, als auch für den Rechner, auf dem dieses Programm läuft. Bei Webservern sind verschiedene Sicherheitsaspekte zu beachten.


5.1.2 Gefährdungslage

Für den IT-Grundschutz werden bezüglich Schadprogramme die folgenden typischen Gefährdungen betrachtet:

<table>
<thead>
<tr>
<th>G 2.1</th>
<th>Fehlende oder unzureichende Regelungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>G 2.4</td>
<td>Unzureichende Kontrolle der Sicherheitsmaßnahmen</td>
</tr>
<tr>
<td>G 2.7</td>
<td>Unerlaubte Ausübung von Rechten</td>
</tr>
<tr>
<td>G 2.9</td>
<td>Mangelhafte Anpassung an Veränderungen beim IT-Einsatz</td>
</tr>
<tr>
<td>G 2.28</td>
<td>Verstöße gegen das Urheberrecht</td>
</tr>
</tbody>
</table>
5.1.3 Maßnahmen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die sichere Anbindung eines Webservers an öffentliche Netze (z. B. das Internet) ist Baustein B 3.301 Sicherheitsgateway (Firewall) zu betrachten, ebenso wie für den Zusammenschluss mehrerer Intranets zu einem übergreifenden Intranet.

Ein Webserver sollte in einem separaten Serverraum aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in Baustein B 2.4 Serverraum beschrieben.

**Planung und Konzeption**

| M 2.172 | (A) | Entwicklung eines Konzeptes für die Web-Nutzung |
| M 2.173 | (A) | Festlegung einer Web-Sicherheitsstrategie |
| M 2.175 | (A) | Aufbau eines Webservers |
| M 2.271 | (A) | Festlegung einer Sicherheitsstrategie für den WWW-Zugang |
| M 2.272 | (A) | Einrichtung eines WWW-Redaktionsteams |
| M 2.298 | (Z) | Verwaltung von Internet-Domainnamen |
| M 4.34  | (Z) | Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen |
| M 4.176 | (B) | Auswahl einer Authentisierungsmethode für Webangebote |
| M 5.64  | (Z) | Secure Shell |
| M 5.66  | (B) | Verwendung von TLS/SSL |
| M 5.69  | (A) | Schutz vor aktiven Inhalten |

**Beschaffung**

| M 2.176 | (B) | Geeignete Auswahl eines Internet Service Providers |

**Umsetzung**

| M 4.94  | (A) | Schutz der WWW-Dateien |
| M 4.95  | (A) | Minimales Betriebssystem |
| M 4.96  | (Z) | Abschaltung von DNS |
| M 4.98  | (A) | Kommunikation durch Paketfilter auf Minimum beschränken |
Betrieb

| M 2.174 (A) | Sicherer Betrieb eines Webservers |
| M 2.273 (A) | Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates |
| M 4.33 (A)  | Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung |
| M 4.64 (C)  | Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen |
| M 4.78 (A)  | Sorgfältige Durchführung von Konfigurationsänderungen |
| M 4.177 (B) | Sicherstellung der Integrität und Authentizität von Softwarepaketen |
| M 5.59 (A)  | Schutz vor DNS-Spoofing |

Notfallvorsorge

| M 6.88 (B) | Erstellen eines Notfallplans für den Webserver |

5.2 Datenbanken (B 5.7)

5.2.1 Beschreibung

Datenbanksysteme (DBS) sind ein weithin genutztes Hilfsmittel zur rechnergestützten Organisation, Erzeugung, Veränderung und Verwaltung großer Datensammlungen und stellen in vielen Unternehmen und Organisationen die zentrale Informationsbasis zu ihrer Aufgabenerfüllung bereit. Ein DBS besteht aus dem so genannten Datenbankmanagement-System (DBMS) und einer oder mehrerer Datenbanken.

Eine Datenbank ist eine Zusammenstellung von Daten samt ihrer Beschreibung (Metadata), die persistent im DBS abgelegt werden.

Das DBMS bildet die Schnittstelle zwischen den Datenbanken und dient den Benutzern zur Daten-Verwaltung und Veränderung. Die zentralen Aufgaben eines DBMS sind im Wesentlichen die Bereitstellung verschiedener Sichten auf die Daten (Views), die Konsistenzprüfung der Daten (Integritätssicherung), die Autorisationsprüfung, die Behandlung gleichzeitiger Zugriffe verschiedener Benutzer (Synchronisation) und das Bereitstellen einer Datensicherungsmöglichkeit, um im Falle eines Systemausfalls zeitnah Daten wiederherstellen zu können.
5.2.2 Gefährdungslage

Neben den grundlegenden Gefährdungen, die prinzipiell für IT-Systeme gelten, existieren Gefährdungen, die speziell die Verfügbarkeit von Datenbanken sowie die Vertraulichkeit oder die Integrität der gespeicherten Daten bedrohen.


Ein weiterer Aspekt ergibt sich aus der steigenden Komplexität des DBMS, der sich unter anderem auch in örtlich weit voneinander getrennter Datenhaltung und den damit einhergehenden Anforderungen an sichere Kommunikationswege und konsistente Daten-Synchronisation begründet.

Für den IT-Grundschutz von Datenbanken werden die folgenden Gefährdungen angenommen:

**Organisatorische Mängel**

| G 2.22 | Fehlende Auswertung von Protokolldaten |
| G 2.26 | Fehlendes oder unzureichendes Test- und Freigabeverfahren |
| G 2.38 | Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen |
| G 2.39 | Mangelhafte Konzeption eines DBMS |
| G 2.40 | Mangelhafte Konzeption des Datenbankzugriffs |
| G 2.41 | Mangelhafte Organisation des Wechsels von Datenbank-Benutzern |
| G 2.57 | Nicht ausreichende Speichermedien für den Notfall |
| G 2.110 | Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken |

**Menschliche Fehlhandlungen**

| G 3.6 | Gefährdung durch Reinigungs- oder Fremdpersonal |
| G 3.16 | Fehlerhafte Administration von Zugangs- und Zugriffsrechten |
| G 3.23 | Fehlerhafte Administration eines DBMS |
| G 3.24 | Unbeabsichtigte Datenmanipulation |
| G 3.80 | Fehler bei der Synchronisation von Datenbanken |

**Technisches Versagen**

| G 4.26 | Ausfall einer Datenbank |
Vorsätzliche Handlungen

| G 5.9    | Unberechtigte IT-Nutzung                                      |
| G 5.10   | Missbrauch von Fernwartungszugängen                         |
| G 5.18   | Systematisches Ausprobieren von Passwörtern                 |
| G 5.64   | Manipulation an Daten oder Software bei Datenbanksystemen   |
| G 5.65   | Verhinderung der Dienste eines Datenbanksystems             |
| G 5.131  | SQL-Injection                                                |

5.2.3 Maßnahmen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.


Planung und Konzeption

| M 2.80 (A) | Erstellung eines Anforderungskatalogs für Standardsoftware |
| M 2.126 (A) | Erstellung eines Datenbanksicherheitskonzeptes          |
| M 2.132 (A) | Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen |
| M 2.134 (B) | Richtlinien für Datenbank-Anfragen                      |
| M 2.363 (B) | Schutz gegen SQL-Injection                              |
| M 5.58 (B)  | Auswahl und Installation von Datenbankschnittstellen-Treibern |

Beschaffung

| M 2.124 (A) | Geeignete Auswahl einer Datenbank-Software               |

Umsetzung
<table>
<thead>
<tr>
<th>Code</th>
<th>Einteilung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>M 2.125</td>
<td>(A)</td>
<td>Installation und Konfiguration einer Datenbank</td>
</tr>
<tr>
<td>M 2.135</td>
<td>(C)</td>
<td>Gesicherte Datenübernahme in eine Datenbank</td>
</tr>
<tr>
<td>M 4.7</td>
<td>(A)</td>
<td>Änderung voreingestellter Passwörter</td>
</tr>
<tr>
<td>M 4.71</td>
<td>(C)</td>
<td>Restriktive Handhabung von Datenbank-Links</td>
</tr>
<tr>
<td>M 4.73</td>
<td>(C)</td>
<td>Festlegung von Obergrenzen für selektierbare Datensätze</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Betrieb</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M 2.31</td>
<td>(A)</td>
<td>Dokumentation der zugelassenen Benutzer und Rechteprofile</td>
</tr>
<tr>
<td>M 2.34</td>
<td>(A)</td>
<td>Dokumentation der Veränderungen an einem bestehenden System</td>
</tr>
<tr>
<td>M 2.65</td>
<td>(B)</td>
<td>Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System</td>
</tr>
<tr>
<td>M 2.127</td>
<td>(B)</td>
<td>Inferenzprävention</td>
</tr>
<tr>
<td>M 2.128</td>
<td>(A)</td>
<td>Zugangskontrolle einer Datenbank</td>
</tr>
<tr>
<td>M 2.129</td>
<td>(A)</td>
<td>Zugriffskontrolle einer Datenbank</td>
</tr>
<tr>
<td>M 2.130</td>
<td>(A)</td>
<td>Gewährleistung der Datenbankintegrität</td>
</tr>
<tr>
<td>M 2.131</td>
<td>(C)</td>
<td>Aufteilung von Administrationstätigkeiten bei Datenbanksystemen</td>
</tr>
<tr>
<td>M 2.133</td>
<td>(A)</td>
<td>Kontrolle der Protokolldateien eines Datenbanksystems</td>
</tr>
<tr>
<td>M 3.18</td>
<td>(A)</td>
<td>Verpflichtung der Benutzer zum Abmelden nach Aufgabenерfüllung</td>
</tr>
<tr>
<td>M 4.67</td>
<td>(B)</td>
<td>Sperren und Löschen nicht benötigter Datenbank-Accounts</td>
</tr>
<tr>
<td>M 4.68</td>
<td>(A)</td>
<td>Sicherstellung einer konsistenten Datenbankverwaltung</td>
</tr>
<tr>
<td>M 4.69</td>
<td>(B)</td>
<td>Regelmäßiger Sicherheitscheck der Datenbank</td>
</tr>
<tr>
<td>M 4.70</td>
<td>(C)</td>
<td>Durchführung einer Datenbanküberwachung</td>
</tr>
<tr>
<td>M 4.72</td>
<td>(Z)</td>
<td>Datenbank-Verschlüsselung</td>
</tr>
<tr>
<td>M 5.117</td>
<td>(Z)</td>
<td>Integration eines Datenbank-Servers in ein Sicherheitsgateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Notfallvorsorge</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M 6.48</td>
<td>(A)</td>
<td>Verhaltensregeln nach Verlust der Datenbankintegrität</td>
</tr>
<tr>
<td>M 6.49</td>
<td>(A)</td>
<td>Datensicherung einer Datenbank</td>
</tr>
<tr>
<td>M 6.50</td>
<td>(Z)</td>
<td>Archivierung von Datenbeständen</td>
</tr>
<tr>
<td>M 6.51</td>
<td>(B)</td>
<td>Wiederherstellung einer Datenbank</td>
</tr>
</tbody>
</table>
Literatur

D. Technologieauswahl
Technologieauswahl
Magnus Monetarus Bank
Cloud-basiertes Internetbanking System

12. März 2012
Inhaltsverzeichnis

1 Ziele 2
2 Cloud-Umgebung 3
3 Model-View-Control Prinzip 5
4 Server-Software (Backend) 6
5 Entwicklung und Darstellung des Frontend 7
6 Sichere Kommunikation unter Servern und zu externen Services 8
7 Frameworks und Extensions 10
8 Business Process Mining 11
9 Testumgebung 12
10 Entwicklungsumgebung 13

Dokumentenhistorie

<table>
<thead>
<tr>
<th>Version</th>
<th>Datum</th>
<th>Editoren</th>
<th>Änderung</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>29.09.2011</td>
<td>AV, RH</td>
<td>Initiales Dokument</td>
</tr>
<tr>
<td>2.0</td>
<td>19.12.2011</td>
<td>AV, RH</td>
<td>Korrekturen aus dem externen Bericht</td>
</tr>
</tbody>
</table>
1 Ziele

Dieses Dokument beschreibt die Technologieauswahl der PG555 zur Umsetzung einer Internetbanking-Lösung für die Magnus Monetarius Bank.


2 Cloud-Umgebung

Für die Auswahl der Cloud-Software standen nach ausführlicher Recherche der PG555
drei Lösungen zur Auswahl:

- Eucalyptus (2.0.3) \(^1\), \(^2\)
- OpenNebula (3.0) \(^3\), \(^4\)
- OpenStack (Diablo) \(^5\), \(^6\)

<table>
<thead>
<tr>
<th>Kompatibilität</th>
<th>Eucalyptus</th>
<th>OpenStack</th>
<th>OpenNebula</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>hervorragende Kompatibilität (Amazon EC, S3 etc.)</td>
<td>befriedigend (einige kleinere Anbieter)</td>
<td>gering</td>
</tr>
<tr>
<td>Updates</td>
<td>mehrmals pro Jahr</td>
<td>unregelmäßig</td>
<td>mehrmals pro Jahr</td>
</tr>
<tr>
<td>Community</td>
<td>sehr gut</td>
<td>sehr gut</td>
<td>gut</td>
</tr>
<tr>
<td>kommerzielle Version</td>
<td>verfügbar</td>
<td>nicht verfügbar</td>
<td>nicht verfügbar</td>
</tr>
</tbody>
</table>

Tabelle 2: Vergleich der Cloud-Software


\(^1\)http://open.eucalyptus.com/wiki/FAQ
\(^2\)http://open.eucalyptus.com/participate/wiki/community
\(^3\)http://wiki.openstack.org/Releases
\(^4\)http://www.openstack.org/community/
\(^5\)http://opennebula.org/software:release
\(^6\)http://opennebula.org/community:community
Aufgrund der hervorragenden Community, regelmäßigen Updates und die Kompatibilität zu den großen Public-Cloud-Anbietern ist Eucalyptus die beste, und daher die von der PG555 gewählte, Cloud-Umgebung.
3 Model-View-Control Prinzip

Das Model-View-Control (MVC) Prinzip ist ein bereits bewährtes Architekturmuster in der Softwareentwicklung. Im Wesentlichen wird die Software in 3 Betandteile mit unterschiedlichen Aufgaben zerlegt:

- **Model**
  
  Das Model stellt das Datenmodell bereit. In den Klassen der Model-Komponente werden lediglich Daten gehalten und verwaltet. Entsprechend hängt diese Komponente von der Steuerung (Control) und der Ansicht (View) ab.

- **View**
  
  Die View-Komponente enthält lediglich das Frontend, also die Benutzeroberfläche, die der Nutzer beim endgültigen Produkt sieht und bedient. In dem Fall der durch die PG555 zu entwickelnden Software stellt die Weboberfläche des Systemes die View-Komponente dar. **Sowohl die Kunden, als auch die Mitarbeiter werden sich über diese Weboberfläche einloggen.**

- **Control**
  
  Der Controller ist zuständig für sämtliche Logik und Steuerung der Abläufe und Prozesse innerhalb der Software. Er wird unter anderem durch die GUI (View-Komponente) dazu instruiert diverse Abläufe zu steuern.


\(^8\)Die Vor- und Nachteile dieser Architekturmuster hier näher zu beleuchten, würde den Rahmen dieses Dokumentes sprengen. Daher wird an dieser Stelle darauf verzichtet.
4 Server-Software (Backend)

Die Server, die innerhalb der Cloud laufen, werden vor Angriffen sicher geschützt. Die Wahl der Programmiersprache zur Implementierung der Serversoftware spielt hier eine wesentliche Rolle.


- Die Java Cryptography Extension (JCE) definiert Programmierschnittstellen für diverse Verschlüsselungsverfahren.
- Der Java Authentication and Authorization Service (JAAS) definiert Programmierschnittstellen für die sichere Feststellung der Identität eines Anwenders.
- Die Java Secure Socket Extension (JSSE) ermöglicht sichere Kommunikation über SSL.

Um die Daten sinnvoll und effizient verwalten zu können, wird auf den Servern eine Datenbank benötigt. Bei der Auswahl wurden lediglich kostenlose Open-Source Lösungen betrachtet, um keine unnötigen Kostenstellen zu eröffnen. Diese stehen kommerziellen Datenbank-Lösungen in nichts nach. Im Wesentlichen gibt es hier die großen und bekannten Datenbanken, die zur Wahl stehen:

- MySQL (5.5.19) 9
- PostgreSQL (9.1.2) 10


9http://www.mysql.de/
10http://www.postgresql.de/
Tabelle 3: Vergleich der Datenbank-Systeme

<table>
<thead>
<tr>
<th>Database</th>
<th>Performance</th>
<th>Kompabilität</th>
<th>Community</th>
<th>kommerzielle Version</th>
<th>Verfügbarkeit bei externen Anbietern</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>schnell</td>
<td>teils starke Abweichungen vom ANSI-Standard</td>
<td>sehr groß</td>
<td>verfügbar</td>
<td>nahezu überall verfügbar</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>teilweise schnell, teilweise eher langsam</td>
<td>weitgehend konform mit dem SQL-Standard ANSI-SQL 92</td>
<td>eher klein</td>
<td>nicht verfügbar</td>
<td>seltener</td>
</tr>
</tbody>
</table>

5 Entwicklung und Darstellung des Frontend


Um der Weboberfläche ein interessantes Design zu geben, werden übliche Techniken zum Design einer Webseite, wie z.B. CSS verwendet. Dies dient lediglich zur Darstellung und stell somit kein Sicherheitsrisiko dar.

---

12http://www.w3.org/Style/CSS/
6 Sichere Kommunikation unter Servern und zu externen Services


Abbildung 1: Übersicht über die externen Schnittstellen

In der Grafik (Abb. 1) ist eine Übersicht der Schnittstellen zu externen Services zu sehen. An den Kanten stehen jeweils die Verschlüsselungsverfahren, die genutzt werden, um eine sichere Kommunikation zu gewährleisten. Im Folgenden soll auf diese Kommunikationsmethoden näher eingegangen werden:

- **SSL (TLS)**


- **HTTPS**

  HTTPS ist die verschlüsselte Variante des HTTP-Protokolls. Das TLS-Verschlüsselungsprotokoll ist im TCP/IP-Modell oberhalb der Transportschicht und unterhalb der Anwendungsprotokolle, wie z.B. HTTP, angesiedelt (HTTP over SSL/TLS). HTTPS ist somit die zusammengefasste/kombinierte Version von HTTP und SSL/TLS.
Um die Verschlüsselung anzudeuten wird der Name HTTPS verwendet. Durch diese Verschlüsselung wird der Datenverkehr, der z.B. zwischen Kunde und Internetbanking-Server stattfindet, vor Angriffen (z.B. Abhören der Netzwerkdaten) Dritter geschützt.

- **IPSec**

IPSec dient zur sicheren Kommunikation unter Gewährleistung von Vertraulichkeit, Authentizität und Integrität. Im Gegensatz zu SSL/TLS arbeitet IPSec direkt auf der Vermittlungsschicht der TCP/IP-Modells.

- **FinTS**


- **EBICS**

7 Frameworks und Extensions

Zur Entwicklung des Bankingsystems werden mehrere Frameworks verwendet. Diese bieten den Vorteil, dass auf diverse bereits implementierte Funktionen zurückgegriffen werden kann. Abhängig davon, welches Framework man für einen bestimmten Zweck einsetzt, sind die enthaltenen Funktionen sehr weit entwickelt und mehrfach erprobt. Im Folgenden werden die von der PG555 verwendeten Frameworks vorgestellt:

- **Spring (3.0.6)**

- **Java Cryptography Extension (JCE)**
  Die JCE ist, wie der Name schon sagt, eine Extension für Java, welche diverse kryptographische Implementierungen beinhaltet. Im Wesentlichen bietet die JCE Lösungen für Aufgaben aus den Bereichen Verschlüsselung, KommunikationsAuthentifizierung und Schlüsselverwaltung. Genauer bietet die JCE folgende Dienste, die für die Entwicklung von sicherheitskritischen Systemen relevant sind:
  
  - **Cypher**
    Cypher bietet sowohl symmetrische, als auch asymmetrische kryptographische Algorithmen zur Verschlüsselung an.
  
  - **Key Management**
    Key Management bietet Lösungen für die Schlüsselgenerierung zum sicheren Aushandeln von Schlüsseln und zum Zerlegen der Schlüssel in ihre Bestandteile.
  
  - **Message Authentication Codes**
    Die Message Authentication Codes dienen zur Berechnung von Authentifizierungen für Kommunikationen

13http://www.springsource.org/
8 Business Process Mining

Um den sicheren Ablauf des Systems zu gewährleisten, werden sämtliche Vorgänge und Prozesse protokolliert. Um die Prozesse innerhalb des Onlinebanking-System auf Anomalien zu prüfen, müssen die erhobenen Daten mit einem Referenzmodell verglichen werden.


Damit ProM die protokollierten Daten verarbeiten kann, müssen diese in dem XML XES Format vorliegen. Dazu wurde die OpenXES-Library verwendet um entsprechende Logging-Methoden zu implementieren.
9 Testumgebung

Das Testen der Software stellt einen wesentlichen Bestandteil des Entwicklungszyklus dar. Somit ist es unverzichtbar und insbesondere im Rahmen einer cloudbasierten Internetbankinglösung ein Aspekt mit sehr hoher Priorität.

Je nach Anwendungsdomain werden unterschiedliche Testumgebungen und Werkzeuge benötigt:

- **Tests auf Korrektheit**

  Grundlegend eignet sich JUnit (4.10) als Testumgebung für Java Projekte, in denen man Komponenten- und Integrationstests durchführt. Da wir zusätzlich Bestandteile von Java EE durch JSF verwenden, wird zusätzlich das Tool Cactus (1.8.1) eingesetzt. Bei Cactus handelt es sich um eine speziell angepasste Version von JUnit für Java EE. Da auch die Oberfläche auf Korrektheit geprüft werden soll, kommt zusätzlich Selenium (2.11.0) zum Einsatz. Selenium bietet z.B. die Möglichkeit das Durchklicken der Oberfläche (z.B. um die Korrektheit dieser zu prüfen) zu automatisieren.

- **Tests auf Sicherheit**

  Sicherheitstests sind sehr vielseitig. Daher werden auch eine Vielzahl von Werkzeugen eingesetzt, um eine bestehende Sicherheit zu garantieren und nachzuweisen.

  - Application Vulnerability Scanner


  - Web Vulnerability Scanner

    Sensible Daten wie z.B. Kundendaten müssen optimal geschützt sein. Damit Dritte nicht unbefugt über Schwachstellen innerhalb der Webseite auf Datenbanken z.B. über SQL-Injection zugreifen können, wird das Webportal der Internetbankinglösung manuell und unterstützt durch Tools, auf Schwachstellen untersucht.

---

15 http://www.junit.org/
16 http://jakarta.apache.org/cactus/
17 http://seleniumhq.org/
18 http://metasploit.com/
19 http://de.wikipedia.org/wiki/SQL-Injection
20 w3af ist solch eine Tool: http://w3af.sourceforge.net/
10 Entwicklungsumgebung

Zur Entwicklung des Projektes wird die integrierte Entwicklungsumgebung (IDE) Eclipse (3.7) verwendet. Der wesentliche Vorteil ist, dass diese Entwicklungsumgebung hauptsächlich zur Entwicklung von Java-Anwendungen entworfen wurde (inzwischen unterstützt diese diverse andere Programmiersprachen) und sie sich durch eine Vielzahl von Plugins ergänzen lässt. Im Wesentlichen soll die Entwicklungsumgebung folgende Punkte gewährleisten:

- **Maximale Unterstützung des Entwicklers**
  Dies wird bei Eclipse unter anderem durch die automatische Code-Vervollständigung geleistet. Eine weitere Erleichterung ist, dass Projekte direkt aus der IDE kompiliert und getestet werden können.

- **Anbindung an eine Versionsverwaltung**
  Durch diverse Plugins kann eine Anbindung an das SVN der PG555 erfolgen. Somit werden aktuelle Entwicklungsfortschritte zentral gespeichert und dem Rest des Teams zugänglich gemacht. Dies bietet gleich mehrere Vorteile, wie die Funktion eines Backups oder des Wiederherstellens von älteren Versionen einer Datei. Darüber hinaus kann jederzeit nachvollzogen werden, was, wann, von wem geändert wurde.

- **Qualitätskontrolle**
  Um eine für alle Teammitglieder akzeptable Qualität des geschriebenen Quellcodes zu gewährleisten, ist eine Konvention erstellt worden, die beschreibt, wie geschriebener Quellcode auszusehen hat. Dies bringt diverse Vorteile, wie z.B. eine erhöhte Lesbarkeit und Wartbarkeit des Quellcodes, was das Arbeiten für andere Teammitglieder erheblich erleichtert. Auch dies kann durch ein Plugin für Eclipse sichergestellt werden. Sollte die Konvention nicht eingehalten worden sein, kann der Quellcode nicht ins SVN eingechekt werden.

\[21\text{http://www.eclipse.org/}\]
\[22\text{http://subversion.tigris.org/}\]
Literaturverzeichnis


[40] Ralph Peters GFT Technologies AG. Ebics detailed specification, 13.05.2011.


