HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

COMPASS SECURITY

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Diplomarbeit

FileBox Appliance

Abteilung Informatik

Herbstsemester 2009

Diplomand:	Roger Blum
Betreuer:	Ivan Bütler
Projektpartner:	Compass Security AG, Rapperswil SG
Experte:	Daniel Frei, Swiss Re
Gegenleser:	Walter Sprenger
Dauer:	28.09.2009 - 20.11.2009

1 Aufgabenstellung

Titel:	FileBox Appliance
Semester:	Herbstsemester 2009
Dauer:	28.09.2009 - 20.11.2009
Diplomand:	Roger Blum
Betreuer:	Ivan Bütler
Projektpartner:	Compass Security AG, Rapperswil SG
Experte:	Daniel Frei, Swiss Re
Gegenleser:	Walter Sprenger

1.1 Einleitung

Die Compass Security AG hat ein Produkt für den sicheren Dateiaustausch zwischen unabhängigen Parteien entwickelt. Hauptbestandteil dieser Lösung ist eine Webapplikation, welche auf einem Server im Internet betrieben wird. Die Clients brauchen für die Verwendung lediglich einen aktuellen Webbrowser und Zugang zum Internet. Um die Sicherheit gewährleisten zu können, erfolgt die Kommunikation zwischen Server und Client ausschliesslich über eine verschlüsselte Verbindung (SSL) und erfordert eine starke Authentisierung mittels SMS Token.
Die FileBox ist mandantenfähig, das heisst ein Kunde kann seine eigene FileBox betreiben und deren Aussehen (CI) selbst gestalten. Zum jetzigen Zeitpunkt wird das Produkt ausschliesslich bei Compass gehostet. Einige Kunden haben nun das Bedürfnis nach einer unabhängigen FileBox angemeldet, weshalb nun eine Appliance für die FileBox entwickelt werden soll. Ziel dieser Diplomarbeit ist es diese Appliance zu entwickeln.

1.2 Aufgabenstellung

Folgende Kriterien sind Bestandteil und Ziele der Aufgabenstellung:

- Auf einer vorgegebenen Compass Hardware soll auf Basis der Linux Distribution „CentOS" eine FileBox Appliance entwickelt werden.
- Die FileBox Appliance soll in einen zu entwickelnden Life-Cycle-Management-Prozess eingebettet sein um den Initialen Setup, die laufende Wartung, grössere Updates und Katastrophen Recovery Prozeduren (Ausfall Hardware und ähnliches) verwalten zu können.
- Es soll ein Prototyp entwickelt und zum DA Abschluss präsentiert werden, welcher alle oben erwähnten Anforderungen erfüllt.

1.3 Voraussetzungen

Die Diplomarbeit erhebt zu Beginn die Anforderungen an den Appliance Live-Cycle-Prozess und setzt diese in einen Anforderungskatalog und Use Cases um. Die Use Cases sind mit Compass abzustimmen und definieren den detaillierten Leistungsumfang. Die Use Cases werden in der Testphase der DA aktiv getestet und protokolliert, als auch Aussagen über die Zielerreichung werden verlangt.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

1.4 Begriffsdefinitionen

Die Diplomarbeit benützt folgende Begriffe gemäss der Compass Notation.

Begriff Updates	Bedeutung
FileBox Release	Als Release wird ein FileBox Image bezeichnet, das gemäss FileBox Roadmap neue FileBox Features, FileBox Bugfixes und OSS Security Updates enthält
FileBox Feature	Neue Features sind gemäss FileBox Roadmap geplant und werden immer in FileBox Releases ausgeliefert
FileBox Bugfixes	Ein Bugfix ist ein Patch der FileBox Anwendung, welche das Fehlverhalten der FileBox korrigiert. Darin enthalten sind applikatorische Probleme. Ein FileBox Bugfix wird einzeln ausgeliefert (und ist im nächsten FileBox Release enthalten)
OSS Security Update	Ein OSS Security Update enthält aktualisierte Teile von eingesetzten Open Source Komponenten (CentOS, Apache, MySQL, Tomcat, OpenSSL, ...)

Begriff Life Cycle	Bedeutung
Appliance Life-Cycle-Deployment	Wenn man beispielsweise 1000 Appliances verteilt hat, dann sind bestimmte Appliances als Test Appliances für Updates gedacht und erhalten dementsprechend die Updates zuerst. Nach einer konfigurierbaren Testzeit werden dann weitere Updates an weitere Appliances verteilt. Eine Appliance kann somit einer Update Klasse zugeordnet sein die bestimmt, wann das Update verteilt wird.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

1.5 Funktionale Mindestanforderungen

Der Appliance Life-Cycle erfüllt folgende minimale Anforderungen:

- Automatische Updates & Patches (siehe oben) der Appliance ohne User Interaktion, jedoch in einem frei konfigurierbaren Wartungsfenster über das Internet
- Manuelles Einspielen von Updates & Patches für Appliances ohne Internet Anschluss
- Sicherstellung der Update Integrität um sich gegen die Installation von Trojaner zu schützen
- Einführung einer Definition für die Verteilung der Updates
- Server Hardening
  - Services laufen mit least Privileges
  - Logfiles sind „Append-only", idealerweise digital signiert (unveränderbar)
  - SSH-Zugang ausschliesslich für Compass mit PublicKey Methode
- Disaster Recovery
  - Die FileBox wird durch den Appliance Hersteller in 24h Stunden ersetzt
  - Sicherstellung in dieser DA, dass die FileBox in weiteren 24h von der defekten auf die neue HW migriert wird.
- Monitoring
  - Erkennung von Disk Problemen, Disk 99% Full
  - Erkennung von weiteren HW und SW Problemen (Logfile kann nicht rotiert werden, ...)

Die Systemgrenze von diesem Projekt besteht aus einem Server-Teil (Update Server) und einer beliebigen Anzahl von Appliances (Clients). Jede Appliance ist eindeutig erkennbar. Die Appliance wird bei Compass in einem Staging Prozess einmalig vorbereitet (für alle Staging Appliances gleich), erhält eine Compass Uniqe-ID und wird dem Endkunden ausgeliefert. Dort macht der End-Kunde die Einstellungen für die Nutzung. Diese Prozedur soll an das Setup Verfahren von ISDN Routern, WLAN Access Points für End-User angelehnt und möglichst einfach sein.

1.6 Unterschriften

_____ _____

Ivan Bütler Roger Blum

Rapperswil, _____

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

2 Erklärung des Studenten

Hiermit bestätige ich, dass diese Diplomarbeit durch eigenes Wissen und eigenes Recherchieren, ohne irgendwelche Mitarbeit von anderen Personen geschrieben wurde. Die genutzten Quellen sind auf der jeweiligen Seite in der Fussnote referenziert und im Quellenverzeichnis nachgeführt.

Fragen die während der Diplomarbeit entstanden sind, wurden durch folgende Personen beantwortet:

- Philipp Oesch, Compass Security AG: Als Entwickler der FileBox konnte er bei einem Problem mit dem Datenbankschema der FileBox Hilfe leisten.
- Daniel Röthlisberger, Compass Security AG: Als Mitentwickler des Apache Moduls „mod_but" konnte er beim Kompilieren des Programmcodes weiterhelfen.

_____
Roger Blum

Rapperswil, _____

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Inhaltsverzeichnis

1 AUFGABENSTELLUNG 2
1.1 Einleitung 2
1.2 Aufgabenstellung 2
1.3 Voraussetzungen 2
1.4 Begriffsdefinitionen 3
1.5 Funktionale Mindestanforderungen 4
1.6 Unterschriften 4

2 ERKLÄRUNG DES STUDENTEN 5

3 ABSTRACT 9

4 MANAGEMENT SUMMARY 10
4.1 Ausgangslage 10
4.2 Vorgehen 10
4.3 Ergebnisse 10
4.4 Ausblick 12

5 EINLEITUNG 13

6 ANFORDERUNGEN 14
6.1 Anforderungskatalog 14
6.1.1 Initial-Setup 14
6.1.2 Fortlaufende Wartung 15
6.1.3 Disaster Recovery 15
6.2 Funktionale Anforderungen 15
6.3 Use Cases 16
6.3.1 Use Case Übersicht 17
6.3.2 UC1 – Vorbereitung 17
6.3.3 UC2 – Inbetriebnahme 18
6.3.4 Betrieb 19
6.3.5 UC3 - OS Updates 19
6.3.6 UC6 - Backup Daten 20
6.3.7 UC7 - Restore Daten 21
6.3.8 UC8 - Austausch defekter Festplatten 21
6.3.9 UC9 – Ausserbetriebnahme 22

7 STAND DER TECHNIK 23
7.1 Verwendete Software 23
7.1.1 CentOS 23
7.1.2 FileBox 23
7.1.3 Apache HTTP Server 24
7.1.4 Apache Tomcat 27
7.1.5 MySQL 27
7.2 Hardware 27

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

8 IMPLEMENTIERUNG 28
8.1 Prototypen 28
8.2 Lösungsansätze 30
8.3 RPM Paketmanagement 30
8.4 Entwicklungsumgebung 30
8.5 Harddisk Partitionierung 31
8.5.1 Risikoabschätzung 31
8.5.2 Definitives Layout 31
8.6 Release-Fahrplan 32
8.7 Compass Repository 34
8.7.1 Repository bereitstellen 35
8.7.2 FileBoxRepo-Servlet 37
8.8 Management Interface 37

9 TESTS UND QUALITÄTSKONTROLLE 38
9.1 Inbetriebnahme 38
9.2 Austausch Harddisk 39

10 ERGEBNISSE 41

11 AUSBLICK 42

12 PERSÖNLICHER BERICHT 43

13 GLOSSAR 44
13.1 Technische Begriffe 44
13.2 Dokumentspezifische Begriffe 45

14 VERZEICHNISSE 46
14.1 Literaturverzeichnis 46
14.2 Abbildungsverzeichnis 47
14.3 Tabellenverzeichnis 47

15 ANHANG 48
15.1 Projektmanagement 48
15.1.1 Meilensteine 48
15.2 Risikoanalyse 49
15.3 Geleistete Stunden 50
15.4 Sitzungsprotokolle 50
15.4.1 Sitzung vom 13.10.2009 50
15.4.2 Sitzung vom 22.10.2009 51
15.4.3 Sitzung vom 30.10.2009 51
15.4.4 Sitzung vom 16.11.2009 52
15.5 Setup Betriebssystem 53
15.5.1 LVM - Logical Volume Manager 55
15.5.2 Software RAID 56
15.5.3 Grub 56
15.5.4 Grub und RAID 56

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.5.5 Chattr 57
15.6 Setup Software 57
15.6.1 RPM Pakete 57
15.6.2 YUM 60
15.6.3 Apache HTTP Server Module kompilieren 61
15.7 Problem: Firefox akzeptiert Cookies nicht 62
15.8 Quelldateien 63
15.8.1 RPM Spezifikationen 63
15.8.2 Management Webinterface 66
15.8.3 FileBoxRepo-Servlet 70
15.9 Mitgelieferte CD 76

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

3 Abstract

Titel	FileBox Appliance
Abteilung	Informatik
Themengebiet	Sicherheit
Studienjahr	Herbstsemester 2009
Name des Studenten	Roger Blum
Betreuer	Ivan Bütler
Projektpartner	Compass Security AG, Rapperswil SG
Experte	Daniel Frei, Swiss Re

Beschreibung

Die Compass Security AG, ein Unternehmen im Bereich IT-Security, entwickelt und betreibt seit mehreren Jahren den webbasierten Dienst „FileBox", der zum sicheren Austausch von Daten über das Internet dient. Die Webanwendung wurde in der Programmiersprache Java entwickelt und wird auf einem Apache Tomcat Applikationsserver betrieben.

Seitens Compass Security besteht das Bedürfnis, die FileBox als Produkt in Form einer Hardware-Appliance auf dem Markt anbieten zu können. Das Ziel dieser Diplomarbeit ist es, ein Konzept für die Appliance auszuarbeiten und einen Prototyp zu entwickeln.

Die Herausforderung bei der Entwicklung der Appliance liegt in der kontinuierlichen Pflege der darauf enthaltenen Software und der Erkennung von Hardware-Problemen im laufenden Betrieb. Nur wenn dies gewährleistet werden kann, ist es möglich ein Produkt wie die FileBox stabil und sicher zu betreiben. Um diesen Anforderungen langfristig gerecht zu werden, muss die Appliance in einem Life-Cycle-Prozess eingebettet sein, der diese Bedürfnisse vollständig abdeckt.

Um die Aktualisierung der Software zu ermöglichen, wurde ein Update-Prozess entworfen, welcher verschiedene Release-Phasen umfasst. Neue Softwareversionen werden zunächst auf Test-Systemen installiert und geprüft, um allfällige Fehler erkennen zu können. Sofern keine Probleme auftreten, werden solche Updates auch auf produktive Appliances übertragen.

Um im Falle eines Defektes einer Festplatte den Verlust von Daten zu vermeiden, wurde ein spezielles Harddisk-Schema entworfen, welches diese Problematik berücksichtigt. Somit ist es möglich, im Fehlerfall eine defekte Festplatte auszutauschen und den regulären Betrieb - ohne Datenverlust - wieder aufzunehmen.

In Zukunft sind Erweiterungen für die Überwachung der Hard- und Software und für die Integration in bestehende Firmen-Infrastrukturen vorgesehen. Dank dem modularen Aufbau mittels ausgeklügelter Softwarepaketierung und dem umgesetzten Update-Konzept sind solche Änderungen problemlos möglich.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4 Management Summary

4.1 Ausgangslage

Die Compass Security AG, ein Unternehmen im Bereich IT-Security, entwickelt und betreibt seit mehreren Jahren den webbasierten Dienst „FileBox", der den sicheren Austausch von Daten über das Internet ermöglicht. Dabei handelt es sich um eine Webanwendung, welche ausschliesslich über verschlüsselte Verbindungen erreichbar ist und zudem für den Login eine starke Authentisierung anhand von Benutzernamen, Passwort und einem zusätzlichen SMS-Token via Mobiltelefon erfordert.

Momentan ist die FileBox nur als Dienstleistung von Compass Security, welche auf deren eigenen Servern betrieben wird, verfügbar. Um die Produktpalette von Compass zu erweitern, soll die FileBox nun in Form einer Hardware-Appliance angeboten werden können.

Im Rahmen dieser Diplomarbeit wurde sowohl ein Prototyp einer solchen Appliance entwickelt als auch die notwendigen Voraussetzungen für den Betrieb geschaffen. Als Vorgabe dazu diente eine bestehende FileBox Installation auf einem Testsystem und die von Compass festgelegte Server-Hardware. Die Appliance musste so aufgesetzt und konfiguriert werden, dass ein zuverlässiger Betrieb der FileBox möglich ist. Um diesen Anforderungen langfristig gerecht zu werden, wurde ein Update-Konzept entwickelt. Jede Appliance kann individuell mit Softwareupdates versorgt werden, so dass es beispielsweise möglich ist, auf Test-Systemen bereits vorgängig neue Releases einzuspielen, um anhand dessen Qualitätsprüfungen durchführen zu können.

4.2 Vorgehen

In einer ersten Phase wurde das Produkt „FileBox" und dessen Abhängigkeiten analysiert. Aus diesen Abhängigkeiten, diversen funktionalen und nicht-funktionalen Anforderungen des Auftragsgebers wurden Bedingungen für die Meilensteine definiert.

Die Bedingungen wurden weiter untersucht, wodurch die kritischen Technologien identifiziert werden konnten. Es wurde versucht für jede Bedingung einen Prototyp zu erstellen, um die Machbarkeit zu prüfen und gleichzeitig das notwendige Know-how aufzubauen. Ein grosser Teil der eingeplanten Zeit wurde für die Aneignung tiefgründiger Linux-Kenntnisse verwendet.

Für die eigentliche Implementation konnten die Prototypen direkt verwendet und erweitert werden. Da die einzelnen Teile jeweils voneinander abhängig sind, war es nicht möglich fortlaufend zu testen. Erst gegen Ende der Implementierungsphase konnten alle Komponenten miteinander verbunden und die resultierende Appliance ausgiebig getestet werden.

4.3 Ergebnisse

In dieser Diplomarbeit konnte die Installation der FileBox weitgehend automatisiert werden. Dies war nötig, damit sich die Appliance später selbständig aktualisieren kann und keine manuellen Eingriffe durch den Kunden nötig sind. Diese Automatisierung wurde durch die Erstellung von Softwarepaketen möglich, die kompatibel zum Paket Management System des Betriebssystem-Herstellers sind. So wurden aus der FileBox und deren Abhängigkeiten Pakete erstellt, die über ein sogenanntes Software Repository auf die einzelnen Appliances verteilt werden. Dieses Repository wird sowohl die aktuellen Softwarepakete des Betriebssystems als auch die der FileBox enthalten.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

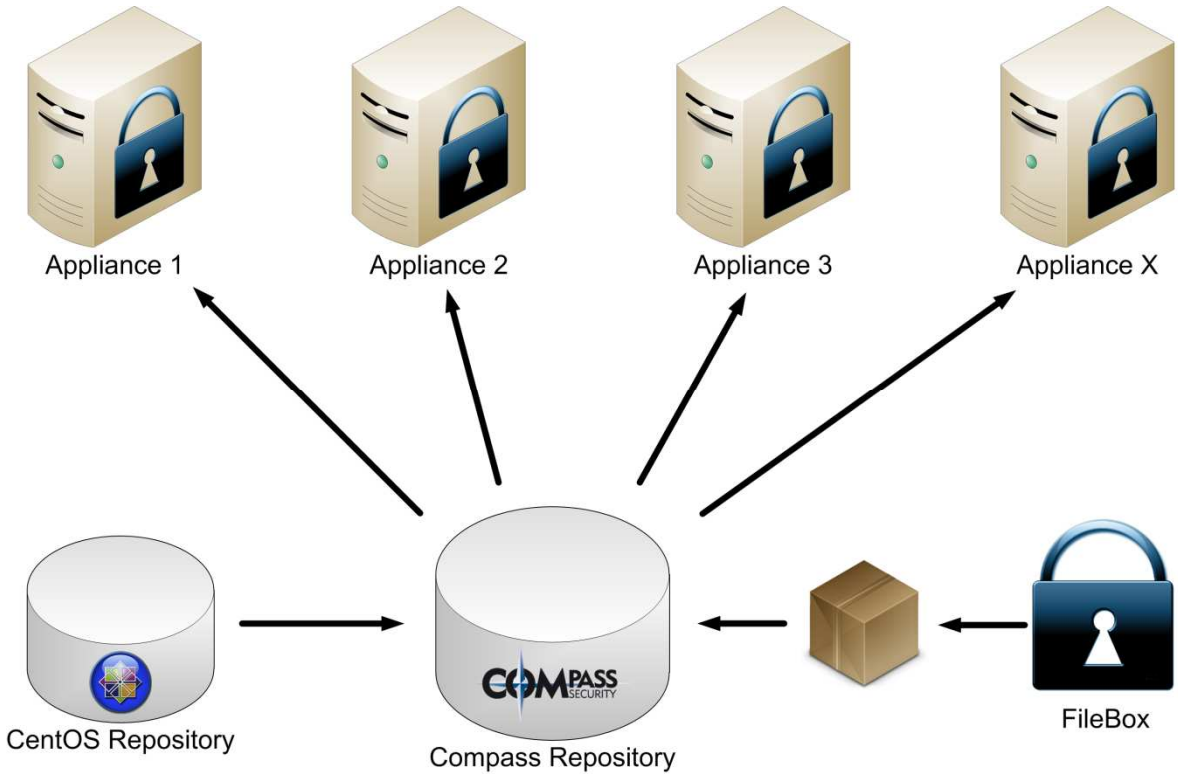

Abbildung 4-1: Update-Konzept

Das Update-Konzept wurde in der Diplomarbeit weiter ausgebaut. So kann jetzt jede Appliance anhand einer Lizenznummer eindeutig identifiziert werden. Folgende Vorteile wurden dadurch geschaffen:

- Die Gültigkeit der Lizenz kann überprüft werden: Wurde ein Aktualisierungs-Vertrag nicht verlängert, soll der Kunde keine Updates in Form von funktionserweiterten Releases mehr erhalten.
- Anhand der Lizenznummer kann dem Kunden ein individuelles Software Repository zugeordnet werden. Die Aktualisierung einzelner Appliances kann so vorgezogen oder eine andere FileBox-Version ausgeliefert werden.
- Das Update-Verhalten jeder Appliance kann protokolliert werden. Arbeitet ein Kunde mit einer veralteten Version ist es möglich ihn darauf hinzuweisen.

Einige Einstellungen der Appliance müssen für jeden Kunden individuell angepasst werden. Dazu sind Linux-Kenntnisse erforderlich. Da aber der Kunde die Appliance selbständig in Betrieb nehmen soll, wurde ein Webinterface entwickelt, welche diese Arbeit wesentlich vereinfacht. So können zum Beispiel Netzwerk-Parameter direkt über die Web-Schnittstelle konfiguriert werden.

Aus zeitlichen Gründen war es nicht möglich, alle Anforderungen aus der Aufgabenstellung umzusetzen. Vor allem auf Anforderungen, welche während der Projektplanung mit niedriger Priorität versehen wurden, musste verzichtet werden. Dank der Automatisierung der Softwareinstallation ist es jedoch möglich, solche Features auch im Nachhinein einzupflegen.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

4.4 Ausblick

Das Resultat dieser Diplomarbeit ist ein Prototyp einer Appliance. Bevor diese verkauft werden kann, sollten nebst ausführlichen Tests einige Punkte verbessert werden. Insbesondere muss das webbasierte Management-Interface sicherer gestaltet werden. Zum jetzigen Zeitpunkt könnte das System durch Fehleingaben falsch konfiguriert werden, so dass ein manueller Eingriff durch Compass unumgänglich ist.

Um die FileBox Appliance noch attraktiver zu gestalten wären folgenden Erweiterungen denkbar:

- Lokale Überwachung von Hard- und Software: Die Appliance prüft in regelmässigen Abständen ob die Hard- beziehungsweise Software richtig funktioniert. Im Fehlerfall wird der Betreiber mittels E-Mail oder SMS benachrichtigt.

- Integration in die Firmen-Infrastruktur: Die FileBox Appliance kann in die bestehende Firmen-Infrastruktur integriert werden. Denkbar wäre hier die Überwachung mittels gängigen Monitoring-Programmen oder die Nutzung von zentralen Speicherablagen.

- Compass Software Repository Management: Das Compass Software Repository wird weiter ausgebaut, sodass die Appliances aktiv überwacht werden können. Prüft eine Appliance über einen längeren Zeitraum nicht, ob neue Aktualisierungen vorliegen, wird der Kunde automatisch benachrichtigt.

- Prozesse für den Austausch von defekter Hardware: Es werden Prozesse definiert wie bei einem Defekt der Hardware vorgegangen wird.

Mit dem erarbeiteten Update Konzept können solche Features auch im Nachhinein ohne Probleme implementiert werden.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

5 Einleitung

Die Compass Security AG entwickelt und betreibt das Produkt „FileBox" für den sicheren Austausch von Dateien über das Internet. Die FileBox ist eine in Java geschriebene und auf einem Apache Tomcat Applikationsserver betriebene Webapplikation. Dank der verschlüsselten Verbindung zwischen Browser und Webserver und der sicheren Authentisierung mittels Benutzername, Passwort und einem SMS-Token über das Mobiltelefon können unabhängige Parteien so Dokumente miteinander austauschen.
Im Moment wird die FileBox als Service betrieben und auf den Systemen von Compass Security gehostet. In Zukunft soll das Produkt auch als Hardware-Appliance angeboten werden.

Im Rahmen dieser Diplomarbeit wurde ein Prototyp für eine solche Appliance entwickelt. Die folgenden Kapitel führen durch diesen Prozess. Angefangen bei der Aufnahme und Analyse der Anforderungen, der Einarbeitung in die benötigten Komponenten, bis hin zu den Ergebnissen und einem Ausblick für die Zukunft.

Technische Begriffe wurden in *kursiver* Schrift gedruckt und können im Glossar am Ende der Dokumentation nachgeschlagen werden.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6 Anforderungen

Im Rahmen dieser Diplomarbeit wird eine Prototyp für eine FileBox Appliance auf Basis von *CentOS* entwickelt. Die Hardware für diese Appliance wurde im Voraus durch Compass Security evaluiert und stand zu Beginn der Diplomarbeit bereit.

Die FileBox Appliance soll in einen Life-Cycle-Prozess eingebettet werden welcher folgende Punkte umfasst:

- Initial-Setup und Auslieferung an den Kunden
- Fortlaufende Wartung der Software
- Disaster Recovery bei einem Ausfall der Hardware

Diese Anforderungen müssen auf einander abgestimmt sein, damit die Appliance später beim Kunden optimal funktioniert.

Abbildung 6-1: Life-Cycle-Prozess

Der zu entwickelnde Prototyp erfüllt die oben erwähnten Anforderungen und wird zum Schluss der Diplomarbeit präsentiert.

6.1 Anforderungskatalog

Damit der verlangte Life-Cycle-Prozess eingehalten werden kann, muss die Appliance einige Kriterien erfüllen. Diese Kriterien werden im Folgenden aufgeführt und genauer beschrieben.

6.1.1 Initial-Setup

Eine FileBox Appliance muss vor der Auslieferung an den Kunden mit einem Initialen Setup versehen werden. Dies beinhaltet einerseits die Installation des Betriebssystems und der FileBox sowie die Grundkonfiguration damit der Kunde die Appliance in Betrieb nehmen kann.

Um einen möglichst effizienten Initial-Setup durchführen zu können, muss ein Staging-Prozess definiert werden. Eine neue Appliance soll mit einem fertigen Image bespielt werden, sodass nicht jedes Mal eine

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

manuelle Installation des Betriebssystems nötig ist. Im Anschluss wird über eine *SSH*-Konsole die Grundkonfiguration der Parameter gemacht, welche für jeden Kunden individuell sind. Dies wären:

- Netzwerk Einstellungen
- Mailserver Einstellungen
- SSL-Zertifikat für den Webserver
- Konfiguration eines Mobiltelefons für den Versand der SMS-Token

Grundsätzlich sollte der Kunde die Möglichkeit haben diese Einstellungen im Nachhinein auch selbständig anpassen zu können. Dies ist nötig, wenn beispielsweise die Netzwerk-Topologie umgestellt wird oder ein SSL-Zertifikat abläuft.
Denkbar wäre hier ein webbasiertes Management Interface, wie man es von Wireless AccessPoints oder ADSL-Routern her kennt.

Im Anschluss an die Konfiguration wird die Appliance an den Kunden ausgeliefert. Ob die Installation durch Compass Security erfolgt oder ob der Kunde diese selbständig tätigt wurde nicht definiert.

6.1.2 Fortlaufende Wartung

Die fortlaufende Wartung der Software ist eine enorm wichtige Anforderung an eine Appliance. Es kann immer vorkommen, dass in einem Produkt eine Schwachstelle entdeckt wird, welche bei der Ausnützung fatale Folgen mit sich bringt. Denkbar wären hier Szenarien wie der Diebstahl von vertraulichen Daten oder die Ausnützung der Appliance für weitere Angriffe im Firmen-Netzwerk.

Aus diesem Grund soll ein Update-Konzept erarbeitet werden, welches es ermöglicht die Appliances regelmässig mit Aktualisierungen zu versorgen. Die Updates können dabei direkt über das Internet oder in Form einer CD, für eine Offline-Installation, ausgeliefert werden.

Vor der Installation von Aktualisierungen auf produktiven Systemen müssen diese ausgiebig getestet werden. Dazu wird ein Release-Fahrplan entwickelt der mehrere Release-Phasen berücksichtigt. Ausgewählte Appliances bekommen die neuen Updates verfrüht eingespielt. Sofern keine Probleme auftreten werden auch die restlichen Geräte mit der Aktualisierung versorgt. Damit dies möglich ist, müssen die einzelnen Appliances bei Aktualisierungs-Anfrage identifiziert werden können. Dies ist im Update-Konzept zu berücksichtigen.

6.1.3 Disaster Recovery

Beim Betrieb von Informatik-Systemen muss immer damit gerechnet werden, dass ein Defekt von Hardware-Komponenten auftritt. Heikel wird es aber vor allem, wenn es sich dabei um die Festplatte handelt und alle Daten unwiderruflich verloren gehen.

Die Server-Hardware, welche für den FileBox Appliance Prototyp zur Verfügung steht ist mit zwei Festplatten ausgestattet. Dieser Vorteil sollte ausgenutzt und bei der Planung das Harddisk-Layouts berücksichtig werden.

Bei einem Defekt einer Festplatte sollte diese – ohne Datenverlust – ersetzt werden können.

6.2 Funktionale Anforderungen

Zusätzlich zu den oben stehenden Zielen im Appliance Life-Cycle wurden einige funktionale Anforderungen festgelegt, welche es ebenfalls zu erfüllen gilt:

- Automatische Updates und Patches: Die Appliances mit einer Verbindung zum Internet sollen ohne Interaktion durch den Kunden mit Aktualisierungen versorgt werden können. Das Zeitfenster für diesen Vorgang kann dabei festgelegt werden.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

- Updates und Patches für Appliances ohne Zugang zum Internet.
- Sicherstellung der Integrität von Aktualisierungen, um sich gegen die Installation von *Trojanern* zu schützen.
- Einführen einer Definition für die Verteilung der Updates.
- Server Hardening:
    - Dienste laufen mit eingeschränkten Benutzerrechten.
    - Logfiles sind „Append-only" und idealerweise digital signiert.
    - SSH-Zugang ausschliesslich für Compass Security mittels PublicKey Methode.
- Disaster Recovery:
    - Appliance wird durch den Hersteller innert 24 Stunden ersetzt.
    - Sicherstellen, dass die Appliance innerhalb weiterer 24 Stunden auf die neue Hardware migriert werden kann.
- Monitoring:
    - Frühzeitiges Erkennen von Harddisk Problemen, beispielsweise Harddisk zu 99% belegt.
    - Erkennen von weiteren Hard- beziehungsweise Softwareproblemen (Logfile kann nicht rotiert werden, …)

6.3 Use Cases

Die Aufgabenstellung und die funktionalen Anforderungen wurden in Use Cases abgebildet. Dabei konnte der Appliance Life-Cycle in zwei Phasen aufgeteilt werden.
Phase 1 enthält die Prozesse welche benötigt werden um die Appliance bereitzustellen, auszuliefern und in Betrieb zu nehmen. In Phase 2 sind die Prozesse welche die Appliance „am Leben" erhalten, also die Wartung, Aktualisierung und der Betrieb.

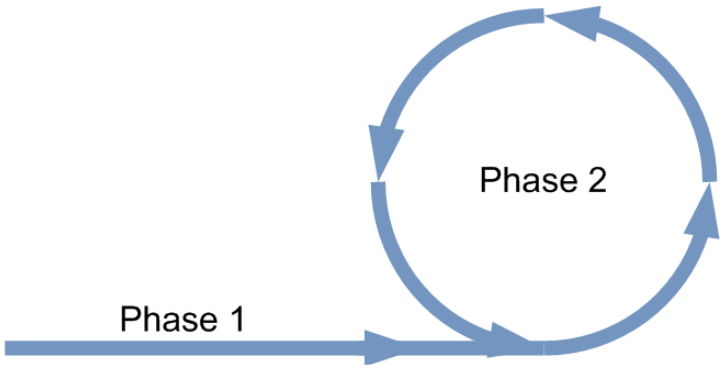

Abbildung 6-2: Life-Cycle Phasen

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.3.1 Use Case Übersicht

Folgende Tabelle zeigt eine Übersicht mit allen Use Cases. Diese wurden den zwei Life-Cycle Phasen zugeordnet und in zwei Kategorien priorisiert. Dies sind einerseits die Umsetzung in dieser Diplomarbeit und andererseits die Priorität für Compass Security.

Nr.	Titel	Phase	Priorität Compass	Priorität DA
UC1	Vorbereitung	1	1	1
UC2	Inbetriebnahme	1	1	1
UC3	Betrieb - OS Updates	2	1	1
UC4	Betrieb - FileBox Bugfixes	2	1	1
UC5	Betrieb - FileBox Features	2	1	1
UC6	Backup Daten	2	2	3
UC7	Restore Daten	2	2	3
UC8	Austausch Hardware	2	2	2
UC9	Ausserbetriebnahme	1	3	3

Tabelle 6-1: Übersicht Use Cases

6.3.2 UC1 – Vorbereitung

Dieser Use Case behandelt den Prozess von der Bestellung der Hardware bis zur Auslieferung an den Kunden.

Precondition	✦ Hardware beim Lieferanten verfügbar
Postcondition	✦ Appliance ist fertig für die Auslieferung
Actors	Compass Security
Steps	1. Anforderungen des Kunden aufnehmen (Appliance Spezifikation) 2. Hardware beim Lieferanten bestellen 3. Hardware auf technische Funktion überprüfen 4. Staging der FileBox Appliance 5. Grundkonfiguration vornehmen o Mobiltelefon für SMS-Versand 6. Updates einspielen 7. Kundenspezifische Konfiguration o Netzwerk Einstellungen o Mailserver Einstellungen o SSL Zertifikat 8. Funktion der FileBox überprüfen

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

	9. Hardware verpacken und versenden
Variationen	✦ Schritt 9: Appliance wird durch Compass direkt beim Kunden installiert
Non Functional Requirements	✦ Lieferung der Hardware durch Lieferanten in maximal zwei Wochen ✦ Auslieferung an den Kunden spätestens 4 Wochen nach Bestellung ✦ Vorbereitungszeit bei Compass dauert maximal 0.5 PT
Mögliche Probleme bei Umsetzung in DA	✦ Staging Prozess ✦ Grundkonfiguration

Tabelle 6-2: UC1 - Vorbereitung

6.3.3 UC2 – Inbetriebnahme

Der UC2 beschreibt die Inbetriebnahme der Appliance durch den Kunden oder Compass Security.

Precondition	✦ Hardware wurde durch Compass geliefert
Postcondition	✦ Appliance ist bereit für den Betrieb
Actors	Kunde, (Compass Security)
Steps	1. Appliance an Standort installieren und mit Netzwerk und Strom versorgen 2. System wird gestartet 3. Grundkonfiguration über ein Webinterface 4. Einloggen in die FileBox (Enterpriseadmin) 5. Testen von E-Mail, SMS, FastExchange
Variationen	✦ Schritt 1: Installation und Inbetriebnahme durch Compass Security ✦ Schritt 3: Grundkonfiguration durch Compass Security bereits vorgenommen
Non Functional Requirements	✦ Konfiguration soll über ein Webinterface möglich sein
Mögliche Probleme bei Umsetzung in DA	✦ Programmierung des Webinterface
Kritisch	✦ Kunde installiert die vorkonfektionierte FileBox, hat aber bei Problemen keine Möglichkeit für die Fehlersuche

Tabelle 6-3: UC2 - Inbetriebnahme

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.3.4 Betrieb

6.3.5 UC3 - OS Updates

Dieser Use Case behandelt die Aktualisierung des Betriebssystems.

Precondition	✦ Appliance bei Kunde in Betrieb ✦ Verbindung ins Internet bzw. zu Compass Server möglich ✦ Es sind neue Betriebssystem-Updates verfügbar
Postcondition	✦ Betriebssystem-Updates wurden eingespielt
Actors	Appliance, Compass Security
Steps	1. Appliance prüft in einem definierten Wartungsfenster, ob Betriebssystem-Updates vorhanden sind 2. Updates werden heruntergeladen und installiert
Variationen	✦ Appliances ohne Zugang zum Internet müssen über eine CD aktualisiert werden ✦ Je nach Updates muss das System neu gestartet werden
Mögliche Probleme bei Umsetzung in DA	✦ Erkennen von Probleme im Updateprozess

Tabelle 6-4: UC3 - OS Updates

6.3.5.1 UC4 - FileBox Bugfixes

Der UC4 beschreibt die Installation von FileBox Patches.

Precondition	✦ Es gibt eine Schwachstelle in der FileBox
Postcondition	✦ Schwachstelle bei allen Kunden behoben
Actors	Appliance, Compass Security, Kunde
Steps	1. FileBox Update wird durch Compass Security erstellt 2. Information der Kunden durch Compass Security über Schwachstelle 3. Update-Prozess wird manuell durch den Kunden gestartet 4. Funktionstest durch Kunden
Variationen	✦ Schritt 2: Kunden ohne Online-Update bekommen den Patch auf CD geliefert
Non Functional Requirements	✦ Kunden müssen über Schachstellen informiert werden
Mögliche Probleme bei Umsetzung in DA	✦ Erkennen von Problemen im Installations-Prozess

Tabelle 6-5: UC4 - FileBox Bugfixes

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.3.5.2 UC5 - FileBox Features

Dieser Use Case behandelt die Installation von zusätzlichen FileBox Features.

Precondition	✦ Feature wurde speziell für Kunde entwickelt
Postcondition	✦ Personalisierte FileBox Version wurde installiert
Actors	Compass Security, Kunde, Appliance
Steps	1. Compass stellt neues Feature als FileBox-Update bereit 2. Information an Kunde über neues Feature 3. Update-Prozess wird manuell durch den Kunden gestartet 4. Funktionstest durch Kunde
Variationen	✦ Schritt 2: Kunden ohne Online-Update bekommen das FileBox-Update auf CD geliefert
Non Functional Requirements	✦ Nur Kunden mit speziellem Vertrag erhalten die neuen Features
Mögliche Probleme bei Umsetzung in DA	✦ Erkennen von Problemen im Installations-Prozess ✦ Wie werden Features für einzelne Kunden aktiviert

Tabelle 6-6: UC5 - FileBox Features

6.3.6 UC6 - Backup Daten

Der UC6 beschreibt das Erstellen von Backups der Datenbank.

Precondition	✦ Appliance in Betrieb
Postcondition	✦ Backup des Appliance vorhanden
Actors	Kunde, Appliance
Steps	1. Kunde startet Backup über das Webinterface 2. Services werden gestoppt 3. Datenbank-Dump wird erstellt 4. Datenbank-Dump wird in ein Backup-Verzeichnis verschoben 5. Services werden wieder gestartet
Variationen	✦ Automatisierte Backups mittels Cronjob
Non Functional Requirements	✦ Die Backup-Dateien könnten zusätzlich verschlüsselt werden ✦ Sicherung auf externes Gerät
Mögliche Probleme bei Umsetzung in DA	✦ Erkennen von Fehlern ✦ Wie kann der Kunde die Backups möglichst einfach von dem Appliance herunterladen ✦ Wie gross kann ein solcher Dump werden?

Tabelle 6-7: UC6 - Backup Daten

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

6.3.7 UC7 - Restore Daten

Dieser Use Case behandelt die Wiederherstellung eines Backups.

Precondition	✦ Appliance in Betrieb ✦ Es wurde vorgängig ein Backup erstellt
Postcondition	✦ Datenbestand wieder hergestellt
Actors	Kunde, Appliance
Steps	1. Kunde wählt das zu wiederherstellende Backup aus 2. Kunde startet Restore-Prozess 3. Services werden gestoppt 4. Datenbank-Dump wird in die Datenbank übernommen 5. Services werden wieder gestartet 6. Funktionstest durch Kunden
Variationen	✦ Datenbank-Dump kommt von externem Medium
Mögliche Probleme bei Umsetzung in DA	✦ Erkennen von Fehlern ✦ Wie kann der Kunde Dumps von externen Medien einspielen ✦ Was passiert wenn sich das Datenbankschema in der Zwischenzeit durch ein Update verändert hat

Tabelle 6-8: UC7 - Restore Daten

6.3.8 UC8 - Austausch defekter Festplatten

Dieser Use Case behandelt den Austausch einer defekten Festplatte.

Precondition	✦ Harddisk ist defekt ✦ Harddisk defekt wurde festgestellt ✦ Compass Security wurde informiert
Postcondition	✦ Harddisk wurde ausgetauscht
Actors	Appliance, Compass Security, Kunde
Steps	1. Appliance wird heruntergefahren 2. Defekte Harddisk wird ausgetauscht 3. System wird gestartet 4. Konfiguration der neuen Festplatte 5. Start der Synchronisation 6. Überprüfen ob die neue Festplatte ordnungsgemäss funktioniert
Variationen	✦ Kunde tauscht defekte Harddisk selber aus
Non Functional Requirements	✦ Austausch von defekter Hardware sollte innerhalb von zwei Arbeitstagen möglich sein
Mögliche Probleme bei	✦ Erkennen von Hardware Problem

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Umsetzung in DA	✦ Informieren der zuständigen Person ✦ Konfiguration der Festplatte

Tabelle 6-9: UC8 - Austausch defekter Festplatten

6.3.9 UC9 – Ausserbetriebnahme

Der UC9 beschreibt die Ausserbetriebnahme einer FileBox Appliance.

Precondition	✦ Kunde möchte keine FileBox Appliance mehr
Postcondition	✦ Daten wurden gelöscht ✦ Appliance wurde ausser Betrieb genommen
Actors	Kunde, Compass Security , Appliance
Steps	1. Kunde meldet sich bei Compass Security, dass er keine Appliance mehr will: o Compass Security vereinbart einen Termin mit dem Kunden o Compass Security fährt vor Ort 2. Appliance wird heruntergefahren und von mit einem *Live Linux* gestartet 3. Festplatten werden unwiderruflich gelöscht 4. Compass Security nimmt Appliance zurück
Variationen	✦ Schritt 2: Appliance wird durch Kunden selbst gelöscht
Non Functional Requirements	✦ Kunde sendet im Anschluss die Appliance an Compass zurück

Tabelle 6-10: UC9 - Ausserbetriebnahme

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7 Stand der Technik

Dieses Kapitel beschreibt die Produkte und Technologien welche bei der FileBox Appliance zum Einsatz kommen. Die Abhängigkeiten zur Applikation „FileBox" konnten anhand einer Testinstallation ausgemacht werden.

7.1 Verwendete Software

7.1.1 CentOS

CentOS[1] (Community Enterprise Operating System) ist eine frei erhältliche Linux-Distribution welche auf den Quellen des kommerziellen RedHat Enterprise Linux basiert.
Bei einem Enterprise Linux[2] ist die Philosophie möglichst lange auf ein und derselben Softwareversion zu bleiben. Dies ist insbesondere für Unternehmen interessant, die nicht ständig auf eine neue Version wechseln wollen. Im Falle von *CentOS* bzw. RedHat Enterprise Linux wird zudem für jede Release-Version eine Lebensdauer von sieben Jahren garantiert. In diesem Zeitraum werden ständig neue Sicherheits-Updates zur Verfügung gestellt. Bei einer Desktop-Distribution wird der Support für eine Version in der Regel für maximal zwei Jahre angeboten.

Für die Softwarepaketierung verwendet CentOS das bewährte *RPM* Format. Jedes Programm ist als Paket abgebildet und kann Abhängigkeiten zu anderen Paketen besitzen
CentOS bezieht dies *RPM* Pakete aus einem *YUM* Software *Repository*. Mit Hilfe des *YUM*-Clients können neue Pakte installiert, aktualisiert oder deinstalliert werden. Allfällige Abhängigkeiten werden miteinbezogen. Wurden mehrere Pakete aktualisiert, kann mittels *YUM* auch direkt das ganze System aktualisiert werden. Genauere Informationen zu *YUM* und dem Software *Repository* folgen später.

Das *CentOS* als Basis der FileBox Appliance genommen wird, war eine Vorgabe von Compass Security. Für diese Distribution ist in der Firma bereits ein fundiertes Wissen vorhanden und kann somit direkt angewendet werden.

Die gegenwärtige *CentOS* Version ist 5.4.

7.1.2 FileBox

Wie bereits mehrfach beschrieben, handelt es sich bei der FileBox um eine Webapplikation für den sicheren Austausch von Daten über das Internet.
Der Begriff „FileBox" bezeichnet einerseits die Webapplikation selbst als auch die virtuellen Dateiablagen innerhalb der Software. Nur die Benutzer welche einer gemeinsamen FileBox zugewiesen sind, können miteinander Dateien austauschen. Ist im folgenden Abschnitt die virtuelle Datenablage gemeint, wird dies speziell gekennzeichnet.

Für den Betrieb sind im Wesentlichen ein Webserver, ein Applikationsserver und ein Datenbankserver erforderlich. Die Applikation selbst ist in sechs einzelne Kontexte aufgeteilt:

- Login: Login Applikation, authentisiert den Benutzer.
- Upload: User Bereich, listet verfügbare FileBoxen (Datenablagen) und ermöglich das Hochladen von Dateien in eine FileBox (Datenablage).
- Uploadadmin: Administration der FileBoxen (Datenablagen), Benutzerverwaltung für die Mandanten.

[1] Informationen basierend auf Wikipedia, http://de.wikipedia.org/wiki/CentOS
[2] Informationen basierend auf Wikipedie, http://de.wikipedia.org/wiki/Red_Hat_Enterprise_Linux#Enterprise_OS

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

- Internal: Diese Hilfsapplikation ist für den Benutzer nicht sichtbar. Sie wird für die automatisierte Bereinigung der FileBoxen (Datenablagen) benötigt.
- Enterpriseadmin: Verwaltung von Mandanten. Zugang auf diese Unterapplikation wird in der Regel durch eine Konfiguration am Webserver auf das Intranet eingeschränkt.
- FastExchange: Anonymer Teil der FileBox für den FastExchange. Optional Authentisierung über SMS Token möglich.

7.1.3 Apache HTTP Server

Als Webserver kommt ein Apache HTTP Server zum Einsatz.
Dieser wird als Reverse Proxy vor den Applikationsserver geschaltet und mit zahlreichen zusätzlichen Modulen bestückt. So übernimmt er das Sessionhandling und das erweiterte Logging für forensische Zwecke.

Folgende Module werden dem HTTP Server zugeschaltet und konfiguriert. Ein grosser Teil davon sind im CentOS Release enthalten. Die restlichen Module müssen manuell kompiliert und installiert werden.

7.1.3.1 mod_ssl

Funktion	✦ Erweitert Apache HTTP Server um OpenSSL ✦ Sichere Kommunikation über HTTPS
Beschreibung	Mit mod_ssl unterstützt der Apache HTTP Server SSL/TLS Verbindungen. In der Konfiguration wird dazu ein Private-Key und ein x509 konformes Zertifikat hinterlegt, welche dann für die sichere Kommunikation zwischen Client und Server verwendet werden.
Im CentOS Release	Ja

Tabelle 7-1: Beschreibung mod_ssl

7.1.3.2 mod_but

Funktion	✦ Entry Server mit Cookie Store ✦ Prüft Authentisierung ✦ Redirect auf Login-Applikation bei ungültiger Authentisierung
Beschreibung	Mod_but ist ein Entry Server Modul für den Apache, welches von Ivan Bütler entwickelt wurde. Ein Entry Server nimmt die Requests entgegen und überprüft die Authentisierung bzw. Autorisierung. Greift der Client auf einen Teil der Webapplikation zu, für welchen er nicht berechtigt ist, wird er entweder auf eine Fehlerseite oder auf die Login-Applikation weitergeleitet. Die Cookie Store Funktion behält alle Cookies die von der Webapplikation kommen zurück und gibt ein einzelnes, eigenes Cookie an den Client weiter. Dieses Cookie identifiziert den Client gegenüber dem Entry Server. Bei einem Request des Clients werden die Cookies der Applikation erst durch mod_but wieder eingesetzt und an die Applikation weitergeleitet. Der Benutzer hat somit nicht die Möglichkeit die Cookies einzusehen oder zu manipulieren.
Im CentOS Release	Nein

Tabelle 7-2: Beschreibung mod_but

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.1.3.3 mod_proxy

Funktion	✦ Verbindung zwischen Web- und Applikationsserver
Beschreibung	Mod_proxy stellt die Verbindung zwischen dem HTTP Server und dem Applikationsserver. Die Requests werden von dem vorgeschalteten Webserver entgegengenommen, verarbeitet und schliesslich an den Applikationsserver weitergeleitet.
Im CentOS Release	Ja

Tabelle 7-3: Beschreibung mod_proxy

7.1.3.4 mod_rewrite

Funktion	✦ Umschreiben von URLs ✦ Umleitung auf andere Ressource
Beschreibung	Mit mod_rewrite können Request-URLs umgeschrieben werden. So kann z.B. eine URL vereinfacht- oder eine Umleitung auf eine andere Ressource gemacht werden. ✦ http://host/admin → http://host/administrationsinterface ✦ http://www.filebox-solution.com/info → http://www.csnc.ch/filebox Im Falle der FileBox wird mod_rewrite genau für diese beiden Zwecke eingesetzt.
Im CentOS Release	Ja

Tabelle 7-4: Beschreibung mod_rewrite

7.1.3.5 modsecurity2

Funktion	✦ Web Application Firewall ✦ Filtern von Request ✦ Erweitertes Logging
Beschreibung	Modsecurity2 ist eine Web Application Firewall, die alle Requests gegen den Webserver filtert und gegebenenfalls blockt. Die mitgelieferten Filterregeln können beliebig angepasst werden. Zudem werden die Requests für forensische Zwecke geloggt.
Im CentOS Release	Nein

Tabelle 7-5: Beschreibung modsecurity2

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.1.3.6 mod_headers

Funktion	✦ Manipulation des HTTP Headers
Beschreibung	Mit dem Modul mod_headers können HTTP Header manipuliert werden. Es können einzelne Parameter überschrieben, hinzugefügt oder gelöscht werden. Bei der FileBox werden mit Hilfe von mod_headers die SSL Parameter von der Client-Server-Verbindung an die Webapplikation auf dem Applikationsserver übergeben. Diese Informationen werden an den Header jedes Requests angefügt.
Im CentOS Release	Ja

Tabelle 7-6: Beschreibung mod_headers

7.1.3.7 mod_replace

Funktion	✦ Ersetzen von Text im HTTP Request bzw. Response ✦ Wird meistens zusammen mit mod_proxy benötigt
Beschreibung	Mit dem Modul mod_replace kann anhand regulärer Ausdrücke im Request- bzw. Response Body nach bestimmten Mustern gesucht und ersetzt werden. Durch die Verwendung von mod_proxy können die Pfade zu Stylesheets oder Bilddateien nicht mehr korrekt sein, was mit diesem Modul umgeschrieben werden kann.
Im CentOS Release	Nein

Tabelle 7-7: Beschreibung mod_headers

7.1.3.8 mod_log_forensic

Funktion	✦ Schreibt pro Request zwei Log-Einträge ✦ Einen Eintrag vor der Verarbeitung (Zeile startet mit „+“) ✦ Einen weiteren nach der Verarbeitung (Zeile startet mit „-“) ✦ Zeigt ob ein Request komplett verarbeitet wurde
Beschreibung	Mod_log_forensic schreibt für jeden Request zwei Log-Einträge. Ein Erster vor der Verarbeitung und einen Zweiten danach. Anhand einer einzigartigen ID können diese Einträge einander zugeordnet werden. Mit Hilfe dieses Logfiles können so Requests herausgefiltert werden, die vom Server nicht verarbeitet wurden.
Im CentOS Release	Ja

Tabelle 7-8: Beschreibung mod_log_forensic

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

7.1.3.9 mod_unique_id

Funktion	✦ Erzeugt pro Request eine eindeutige Identifikationsnummer ✦ Wird benötigt um Log-Einträge vergleichen zu können
Beschreibung	Dieses Modul erzeugt für jeden Request eine eindeutige Identifikationsnummer. Diese kann dann z.B. in ein Log geschrieben- und über den HTTP Header an die Webapplikation weitergegeben werden. So können die Log-Einträge in den einzelnen Logfiles miteinander korreliert werden.
Im CentOS Release	Ja

Tabelle 7-9: Beschreibung mod_unique_id

7.1.4 Apache Tomcat

Apache Tomcat ist ein Applikationsserver, welcher für Java-Webapplikationen verwendet werden kann. Mit dem integrierten Webserver könnte ein Tomcat auch standalone betrieben werden, jedoch ist dies nur für Testzwecke zu empfehlen.
Die FileBox verwendet derzeit die Version 5.5 des Tomcat Applikationsservers.

7.1.5 MySQL

MySQL ist ein bekannter Server für relationale Datenbanken. Für die FileBox wird die Programmversion 5 verwendet.

7.2 Hardware

Die Appliance wird auf Basis eines DELL PowerEdge R200 Server gebaut. Diese Hardware wurde bereits vorgängig von Compass Security evaluiert und bestellt.
Besondere Eigenschaften sind der geringe Platzbedarf und die langfristige Verfügbarkeit beim Lieferanten.

Folgende Komponenten sind in diesem Server verbaut:

Prozessor	Dual Core Intel Xeon E3120, 3.16GHz, 1333MHz FSB
RAM	4GB (2 x 2GB DIMMs, 800MHz)
Festplatten	2 x 250GB Serial ATA 7200U/min
Netzwerk	2 x 1Gbit/s, Broadcom

Tabelle 7-10: Appliance Hardware

Abbildung 7-1: Dell PowerEdge R200

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

8 Implementierung

8.1 Prototypen

Zu Beginn der Implementierungsphase wurden die kritischen Methoden und Technologien aus den Anforderungen und Use Cases extrahiert. Pro Punkt wurde dann ein Prototyp dazu entwickelt. Mit Hilfe dieser Prototypen konnte einerseits die Machbarkeit geprüft und das nötige Know-how aufgebaut werden.

Nr.	Titel	Beschreibung	Ergebnis	Kapitel
1.	Apache Module	✦ Die Apache Module mod_but, modsecurity2 und mod_replace liegen nur im Quellcode vor. ✦ Module für Apache Version von CentOS kompilieren und testen.	✦ Module können mit Hilfe von *„apxs"* kompiliert werden. ✦ Pro Modul wird später ein *RPM* Paket gebildet.	7.1.3
2.	*RPM* Packet	✦ Damit die FileBox und deren Abhängigkeiten aktualisiert werden können, müssen daraus eigene *RPM* Pakete gebildet werden. ✦ Know-how über *RPM* fehlt noch ganz und muss erarbeitet werden.	✦ *RPM* Pakete können mit Entwicklungsprogrammen von CentOS erzeugt werden. ✦ Automatisierte Konfiguration nach der Installation ist mit Skriptaufrufen in der Installationsroutine möglich aber relativ aufwendig. ✦ Abhängigkeiten der einzelnen Pakete werden in der Spezifikation des *RPM* Paketes definiert.	15.6
3.	*YUM* Software *Repository*	✦ CentOS und andere Linux-Distributionen verwenden ein *YUM* Software *Repository* für die Softwareverteilung. ✦ Wie wird ein solches Repository nachgebaut? ✦ Können die einzelnen Clients identifiziert werden?	✦ Ein *YUM* Software *Repository* kann auf einem Web-, FTP Server oder auf dem lokalen Filesystem abgebildet werden. ✦ Der Client sucht an dieser Stelle nach einem Inhaltsverzeichnis, welches die enthaltenen Softwarepakete aufführt. ✦ Mit dem Programm „createrepo" wird ein solcher Index erstellt. ✦ Die Authentisierung kann im Falle von HTTP mit Basic oder Digest Auth gemacht werden. ✦ Anstelle eines fixen Update Servers kann auch ein Fastestmirror-URL eingetragen werden. Der	15.6.2

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Nr.	Titel	Beschreibung	Ergebnis	Kapitel
			Client ruft diesen URL auf und erhält als Antwort eine Liste mit aktuellen Repositories. Diese Funktionalität ist durch das *YUM* Plug-In Fastestmirror gegeben.	
4.	*Snapshot*	✦ Vor jedem Software Update könnte ein *Snapshot* des Filesystems gemacht werden, damit im Fehlerfall die letzte funktionierende Version wiederhergestellt werden kann. ✦ Denkbar ist eine Lösung mit *ZFS* oder *LVM*.	✦ *ZFS* gibt es aus lizenztechnischen Gründen nicht für Linux-Distributionen. ✦ Mit *LVM*-Snapshots kann das aktuelle Filesystem gesichert werden. ✦ Für einen Restore gibt es kein fertiges Kommando. Datenbestand muss aus dem *Snapshot* in das Live-System zurückkopiert werden. ✦ Systemstart ab einem *Snapshot* theoretisch möglich, jedoch noch nicht verifiziert.	15.5.1
5.	Bootkonfiguration	✦ Der Server soll auch noch starten wenn eine Festplatte defekt ist.	✦ Das Software RAID von Linux unterstützt Mirroring. Die beiden Festplatten werden dabei gespiegelt. ✦ Der Bootmanager *Grub* kann so installiert werden, dass das System auch nur noch von der zweiten Harddisk startet. ✦ Einbau einer Ersatz-Festplatte muss noch verifiziert werden.	15.5.1 15.5.2 15.5.3
6.	Logfiles	✦ Logfiles sollen nur im *Append-only* Modus geöffnet werden. ✦ Die Logfiles können somit nicht verändert- oder gelöscht werden.	✦ Mit „chattr" können die Dateiattribute dementsprechend gesetzt werden. ✦ Auch der Benutzer *root* kann die Dateien nicht mehr verändern. ✦ Vor der *Logrotation* müssen die Attribute wieder zurückgesetzt werden.	15.5.1

Tabelle 8-1: Prototypen

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

8.2 Lösungsansätze

Im Folgenden wurden aus den Anforderungen einige Stichworte herausgenommen und mögliche Lösungen dazu überlegt:

Appliance Identifizierung	✦ Appliance sendet MAC-Adresse des internetseitigen Netzwerkadapters mit ✦ Eindeutige ID die in einer Konfigurationsdatei steht und bei einem Request zu Compass mitgeschickt wird ✦ Source IP Adresse des Requests dient als Identifizierung des Kunden
Infrastruktur Compass	✦ Compass betreibt ein YUM Repository über welches die Softwareupdates verteilt werden ✦ Pro Kunden oder Wartungsvertrag wird eine eigenes Repository betrieben, damit das Updateverhalten der Appliance kontrolliert werden kann ✦ Compass liefert auch Betriebssystem Updates über das eigene Repository aus, damit der stabile Betrieb der Appliance gewährleistet werden kann
Software Deployment (Fahrplan)	✦ Unterschiedliche Repository für die einzelnen Phasen ✦ Die Appliances aus der ersten Phase müssen gezielt ausgewählt werden, damit ein breites Band von Kunden abgedeckt werden kann
Recovery bei fehlerhaftem Update	✦ Am „Ende" der Festplatte wird ein minimales Linux installiert, welches im Fehlerfall gestartet werden kann ✦ Eine Repair-Prozedur stellt den ursprünglichen Stand (vor dem Update) wieder her. Damit dies möglich ist, muss vor dem Update eine Art *Snapshot* erstellt werden. ✦ *Snapshot* mittels *LVM*

8.3 RPM Paketmanagement

Damit die FileBox automatisiert installiert und aktualisiert werden kann, muss diese in Form eines *RPM* Paketes ausgeliefert werden.
Das *RPM* Paket für die FileBox enthält nebst der Webapplikation auch diverse Skripte die nach der Installation gestartet werden und Konfigurationsdateien für die FileBox und den Webserver generieren. Theoretisch ist es möglich beliebige Konfigurationsänderungen am System über ein einziges Paket vorzunehmen. Dies kann auch nötig sein, wenn die Appliance im Nachhinein mit zusätzlichen Features erweitert werden soll.

Die funktionale Anforderung, dass die Integrität von Softwarepaketen gewährleistet werden muss, kann durch das Signieren der selbst erstellten Pakete abgedeckt werden. Bei der Installation des Paketes wird die Signatur gegen einen vorgängig importierten Public Key geprüft und nur sofern diese gültig ist, wird das Paket installiert.

Genaue Informationen zur Erzeugung von *RPM* Paketen können im Kapitel 15.6.1 nachgelesen werden.

8.4 Entwicklungsumgebung

Für die Entwicklung der *RPM* Pakete und des *YUM Repository* wurde in einer virtuellen Maschine ein Entwicklungssystem aufgesetzt. Ein enormer Vorteil einer *VM* gegenüber einer physischen Installation ist die Möglichkeit *Snapshots* im laufenden Betrieb zu erstellen. So können Tests beliebig oft wiederholt werden,

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

ohne dass das System neu aufgesetzt werden muss. Vor einem kritischen Abschnitt wurde jeweils ein *Snapshot* erstellt, zu welchem, im Falle von Problemen, später wieder zurückgesprungen werden konnte.

Details zur Installation der virtuellen Maschine sind dem Kapitel 0 zu entnehmen.

8.5 Harddisk Partitionierung

Die Partitionierung der beiden Festplatten der Appliance spielen eine entscheidende Rolle für den sicheren Betrieb der Appliance. Das System muss gegen allfällige Hardwaredefekte geschützt sein.
Eine Idee für die Zukunft wäre es, vor einem Software-Update ein *Snapshot* des Filesystems zu erstellen. So könnte im Fehlerfall zur letzten funktionierende Version zurückgesprungen werden. Dieser Gedanke wurde bei der Planung bereits berücksichtigt.

8.5.1 Risikoabschätzung

Risiko	Folge	Gegenmassnahmen	Risiko
Defekt einer Harddisk (ohne RAID)	✦ Datenverlust ✦ Defekte Harddisk muss ausgetauscht werden	✦ Hard- oder Software RAID ✦ Überwachung der Festplatten	mittel
Defekt beider Harddisk (mit RAID)	✦ Totaler Datenverlust ✦ Defekte Harddisks müssen ausgetauscht werden	✦ Datensicherung auf externes Gerät	niedrig
Softwareproblem nach einen Update	✦ FileBox funktioniert nicht mehr	✦ Snapshot des Filesystems vor dem Update ✦ Restore im Fehlerfall	hoch
Datei in FileBox wird unabsichtlich gelöscht	✦ Datei nicht mehr vorhanden ✦ Verärgerter Kunde	✦ Datensicherung auf externes Gerät	mittel

Tabelle 8-2: Risikoabschätzung Harddisks

8.5.2 Definitives Layout

Aufgrund der Risikoabschätzung und der Rücksprache mit dem Betreuer, Ivan Bütler, wurde ein Disklayout gewählt, welches durch den Einsatz von Software RAID redundant ist und dank der Verwendung von *LVM* mit *Snapshots* gesichert werden kann.

Die zwei 250GB Festplatten werden dazu zuerst in jeweils zwei Partitionen aufgeteilt: sda1, sda2 bzw. sdb1, sdb2. Diese werden mittels „Multiple Devices", dem Treiber für Laufwerkverbunde, zu einem RAID1 (Mirroring) zusammengefasst. Es entstehen die logischen Laufwerke md0 und md1. Da die Boot-Partition nicht auf einer *LVM* Volume Group liegen darf, wird md0 direkt formatiert und später als */boot* gemountet.
Die logische Partition md1 wird zu einer Volume Group „vg0" umgewandelt und in Logical Volumes aufgeteilt.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Im Folgenden wird dass definitive Layout noch einmal grafisch Dargestellt.

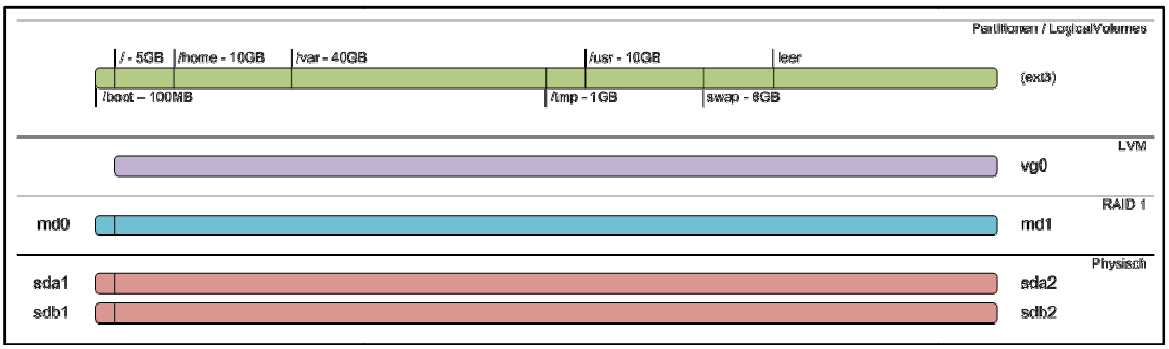

Abbildung 8-1: Layout Harddisks

8.6 Release-Fahrplan

Eine Anforderung in dieser Diplomarbeit ist die Ausarbeitung eines Release-Fahrplans. Es soll definiert werden, in welchem Zyklus die Appliances aktualisiert werden und wie dabei zwischen den einzelnen Release-Versionen unterschieden wird.

Grundsätzlich wäre es möglich, dass die Appliance die Betriebssystem-Updates über das *YUM-Repository* von CentOS bezieht und die FileBox-Releases über ein eigenes Compass *Repository* eingespielt werden. Gibt es aber eine Unverträglichkeit zwischen dem FileBox Release und den CentOS Updates, hat Compass keine Möglichkeit in das Geschehen einzugreifen.
Aus diesem Grund wurde entschieden, dass Compass Security auch für die CentOS Updates verantwortlich sein wird. Das heisst, Compass Security stellt ein eigenes *YUM* Software *Repository* zur Verfügung, welches in regelmässigen Abständen mit dem CentOS *Repository* synchronisiert wird. Die Updates werden jedoch nicht direkt an die Kunden ausgeliefert, sondern immer zusammen mit dem aktuellen FileBox Release getestet. Hat sich diese Kombination bewährt, werden die Test-Appliances aktualisiert. Sofern bei diesen keine Problem auftreten, werden auch die restlichen Kunden-Appliances mit dem Release versorgt.
Die Kombination zwischen CentOS Updatestand und FileBox Release bilden einen Appliance-Release.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Folgende Grafik soll den Ablauf im Detail veranschaulichen:

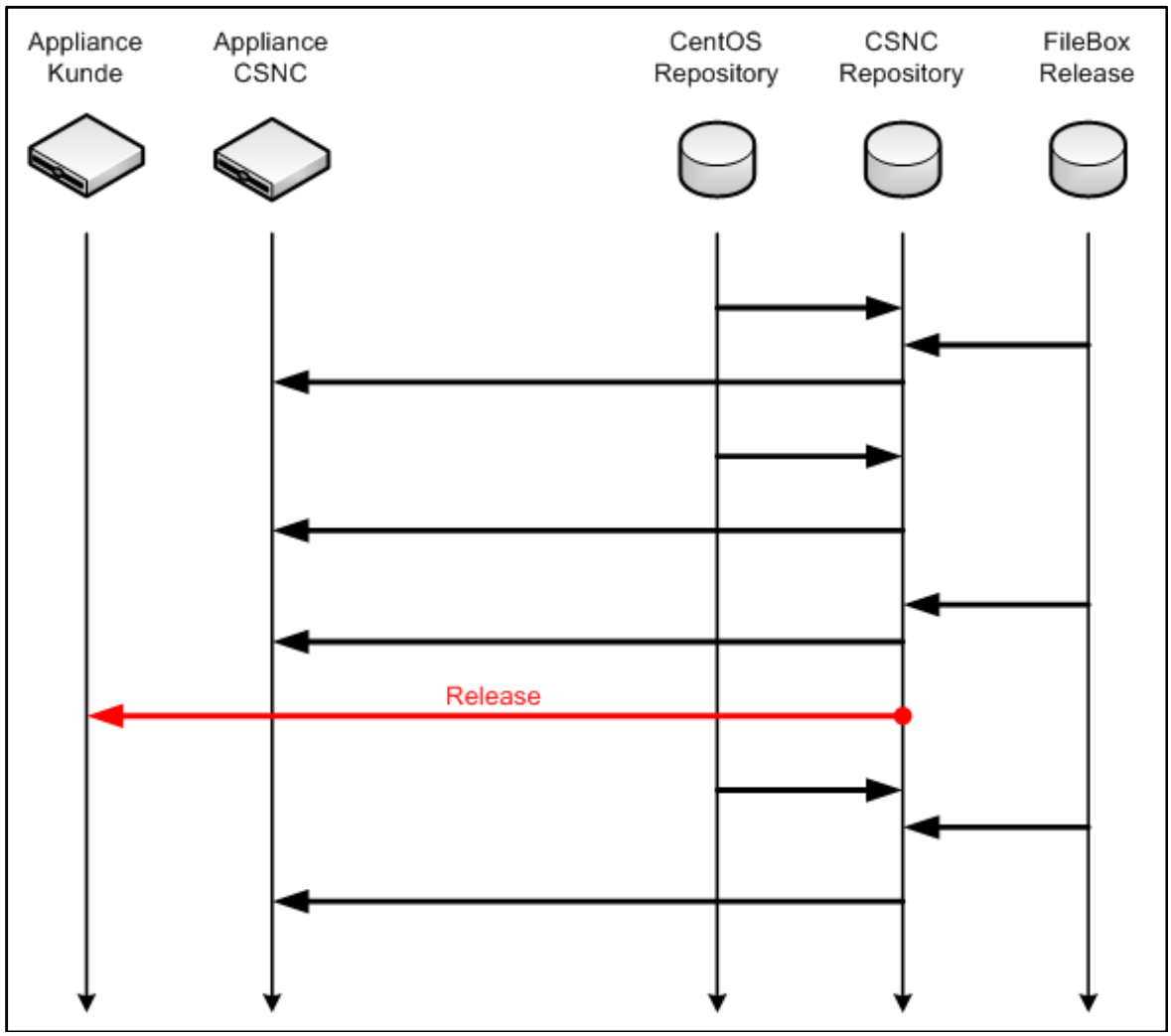

Abbildung 8-2: Release Fahrplan 1

Später im produktiven Betrieb wird es drei Software *Repositories* geben: Unstable, RC (Release Candidate) und Stable.

Das „Unstable" *Repository* wird täglich vom *CentOS Repository* her aktualisiert und mittels *Snapshot*-Technologie „eingefroren". Gibt es zudem noch ein neuer FileBox-Release wird dieser ebenfalls eingespielt. In einem regelmässigen Zyklus, z.B. wöchentlich, wird ein solcher *Snapshot* in das „RC" *Repository* übernommen. Dieser Release wird dann auf die Test-Appliances verteilt und über eine bestimmte Dauer getestet. Sofern sich die Kombination zwischen FileBox Release und dem *CentOS* Updates bewährt hat, wird diese in das „Stable" *Repository* übernommen und auf die restlichen Kunden-Appliances verteilt.

Compass sollte pro *Repository* mindestens eine Appliance selber betreiben, damit allfällige Probleme rechtzeitig erkannt- und behoben werden können.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Im Folgenden ist dieser Ablauf nochmals grafisch verdeutlicht:

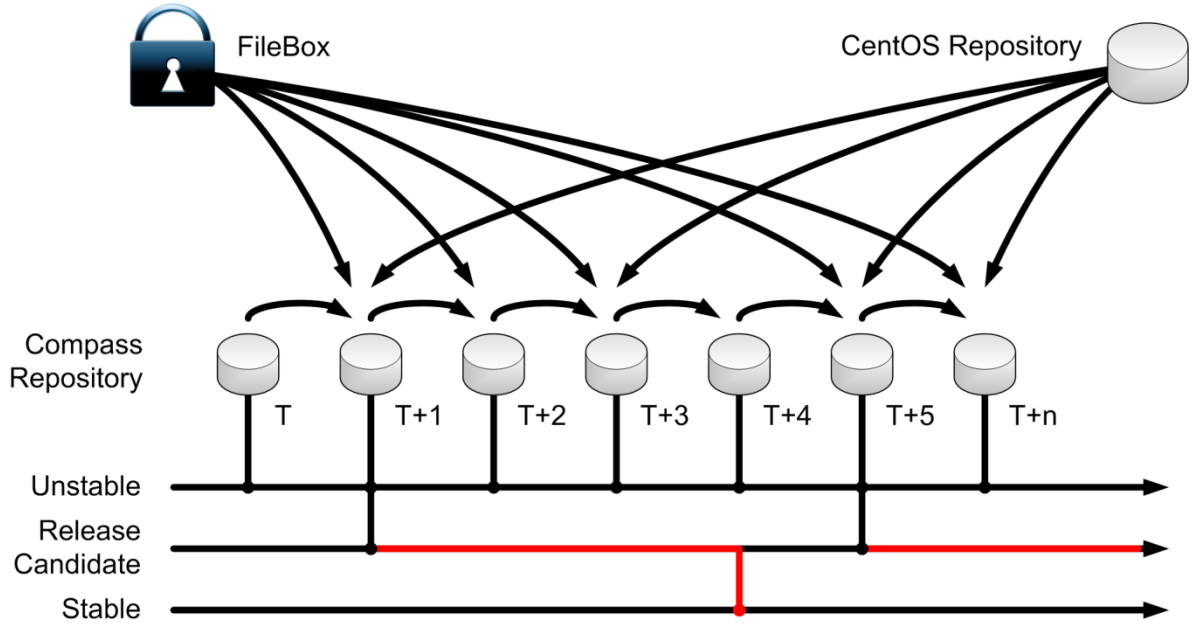

Abbildung 8-3: Release Fahrplan 2

8.7 Compass Repository

Compass Security wird für die Software-Updates pro Release-Typ (Unstable, RC, Stable) eigene *YUM* Software *Repositories* betreiben. Damit den Appliances individuelle Repositories zugeordnet werden können, wurde ein Java Servlet namens „FileBoxRepo" programmiert mit welchem dies möglich ist.
Als Basis für diesen Prozess dient mir das *YUM* Plug-In „fastestmirror". Anstatt bei jedem Update ein statisch zugeordnetes Software *Repository* zu wählen, wird zuerst ein Request an eine Fastestmirror-URL abgesetzt und als Antwort erhält der Client eine Liste von geographisch nahen und vor allem aktuellen Repositories. In der Anfrage sendet der Client ebenfalls seine CentOS Release Version und die dessen Hardware-Architektur mit. So kann das entsprechende *Repository* zugeordnet werden.

Dieser Mechanismus wurde nun weiter ausgebaut und um einen Parameter „key" erweitert. Über diesen Schlüssel muss eine eindeutige Identifikationsnummer mitgeschickt werden, damit Gültigkeit der Lizenz geprüft und zugleich die Appliance identifiziert werden kann. Anhand dieser Identifikation wird entschieden von welchem Repository (Unstable, RC, Stable) die Appliance ihre Updates beziehen soll.
Ist die Lizenznummer ungültig oder wurde sie durch Compass widerrufen, erhält die Appliance kein Mirror-URL und kann sich somit nicht mehr aktualisieren.
Denkbar wäre, dass die Kunden welchen einen Aktualisierungs-Vertrag mehr wollen zwar noch mit Betriebssystem Updates versorgt werden, jedoch keine neuen FileBox Features und Patches mehr erhalten.

Die Mirrorlist-URL ist nach folgendem Schema aufgebaut:

```
http://mirror.csnc.ch/mirror?releasever=5.4&basearch=x86_64&key=111
```

Die Antwort des FileBoxRepo-Servlets sieht in diesem Fall so aus:

```
http://mirror.csnc.ch/centos/5.4/unstable/x86_64/
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

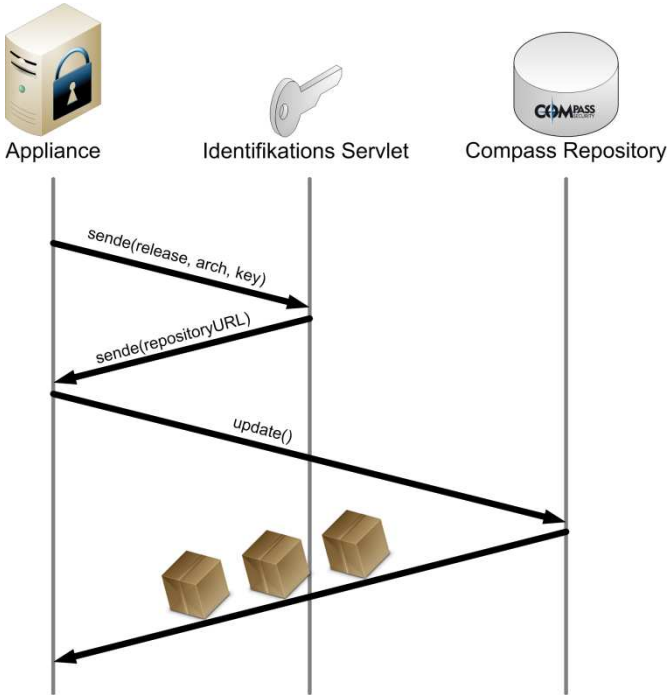

Abbildung 8-4: FileBoxRepo Servlet

8.7.1 Repository bereitstellen

Das Verzeichnis „/opt/repo" in der Entwicklungsumgebung ist die Basis für das *YUM* Software *Repository*. In dieses Verzeichnis müssen alle Softwarepakete, welche im gegenwärtigen *CentOS* Release vorhanden sind kopiert werden. Dies geschieht mit Hilfe von *Rsync*. Da die Appliance auf der *CentOS* Version 5.4 basiert, ist es nicht nötig das gesamte Repository zu synchronisieren. Das Unterverzeichnis „5.4" genügt in diesem Fall.

```
# yum install rsync
# rsync -aqzH --delete eu-msync.centos.org::CentOS/5.4 /opt/repo
```

Der aktuelle *CentOS* Release besteht aus ca. 30GB Daten. Die Synchronisation kann also mehrere Stunden dauern.

Im Anschluss findet man im Verzeichnis „/opt/repo" folgende Ordnerstruktur vor:

```
/opt/
`-- repo
    `-- 5.4
        |-- addons
        |   |-- i386
        |   `-- x86_64
        |-- centosplus
        |   |-- i386
        |   `-- x86_64
        |-- contrib
        |   |-- i386
        |   `-- x86_64
        |-- extras
        |   |-- i386
        |   `-- x86_64
        |-- fasttrack
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
        |   |-- i386
        |   `-- x86_64
        |-- os
        |   |-- i386
        |   `-- x86_64
        `-- updates
            |-- i386
            `-- x86_64
```

Damit der Entworfene Release-Fahrplan umgesetzt werden kann muss nun noch einiges angepasst werden:

1) Die Verzeichnisse für die i386-Architektur können gelöscht werden, da die Appliance Hardware auf 64Bit basiert.
2) Es wird ein zusätzliches Verzeichnis „filebox" mit dem Unterordner „x86_64" angelegt. An dieser Stelle werden später die FileBox-Releases platziert.
3) Unterhalb des Verzeichnisses „5.4" werden die Ordner unstable, rc und stable angelegt.
4) Schliesslich werden die Ordner addons, centosplus, contrib, extras, fastcrack, os und updates in die Ordner unstable, rc, und stable kopiert.

Die Verzeichnisstruktur sieht im Anschluss folgendermassen aus:

```
/opt/
`-- repo
    `-- 5.4
        |-- rc
        |   |-- addons
        |   |   `-- x86_64
        |   |-- centosplus
        |   |   `-- x86_64
        |   |-- contrib
        |   |   `-- x86_64
        |   |-- extras
        |   |   `-- x86_64
        |   |-- fasttrack
        |   |   `-- x86_64
        |   |-- filebox
        |   |   `-- x86_46
        |   |-- os
        |   |   `-- x86_64
        |   `-- updates
        |       `-- x86_64
        |-- stable
        |   |-- addons
        |   |   `-- x86_64
        |   |-- centosplus
        |   |   `-- x86_64
        |   |-- contrib
        |   |   `-- x86_64
        |   |-- extras
        |   |   `-- x86_64
        |   |-- fasttrack
        |   |   `-- x86_64
        |   |-- filebox
        |   |   `-- x86_46
        |   |-- os
        |   |   `-- x86_64
        |   `-- updates
        |       `-- x86_64
        `-- unstable
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
            |-- addons
            |   `-- x86_64
            |-- centosplus
            |   `-- x86_64
            |-- contrib
            |   `-- x86_64
            |-- extras
            |   `-- x86_64
            |-- fasttrack
            |   `-- x86_64
            |-- filebox
            |   `-- x86_64
            |-- os
            |   `-- x86_64
            `-- updates
                `-- x86_64
```

8.7.2 FileBoxRepo-Servlet

Das FileBoxRepo Java Servlet welches die Lizenzprüfung übernimmt und die entsprechende Antwort liefert ist für den Prototyp extrem einfach gehalten:

Anhand der übergebenen Parameter wird eine URL zusammengesetzt und dem Client als Antwort zurückgesendet.

Die gültigen Lizenzen sind in einer Konfigurations-Datei erfasst und können angepasst werden, ohne dass das Servlet neu kompiliert werden muss.

Dieses Servlet sollte für den produktiven Betrieb weiter ausgebaut werden. Mögliche Erweiterungen wären:

- Datenhalten in einer relationalen Datenbank
- Auswerten des Update-Verhaltens der einzelnen Appliances
- Benachrichtigung des Kunden wenn eine Appliance über einen längeren Zeitraum keine Updates mehr bezogen hat
- Sammeln von Statusinformationen der einzelnen Appliances

Der Quellcode dieses Servlets ist unter dem Kapitel 15.8.3 angefügt.

8.8 Management Interface

Das webbasierte Management Interface für die Appliance wurde in der Skriptsprache Perl programmiert und mittels CGI über den Webserver verarbeitet.

Aus zeitlichen Gründen wurde das Interface nicht fertiggestellt. Zum jetzigen Zeitpunkt kann lediglich die Netzwerk-Konfiguration der Appliance angepasst werden.
Damit dies möglich ist, mussten dem Apache-Benutzerkonto spezielle Privilegien gegeben werden. Da derselbe Webserver aber auch für die FileBox verwendet wird, kann diese Lösung nicht für ein produktives System übernommen werden.

Eine ideale Lösung wäre die Verwendung eines zweiten Webservers mit mehr Privilegien, der aber ausschliesslich über ein separates Management-Netzwerkinterface erreichbar ist.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

9 Tests und Qualitätskontrolle

9.1 Inbetriebnahme

Annahme	✦ Ein Kunde hat eine Appliance bestellt und diese gilt es vorzubereiten ✦ Hardware wurde beim Lieferanten bestellt und ist bereit für den Einsatz
Vorbereitung	✦ Es wurde vorgängig ein *Diskdump* von einer bestehenden Appliance gemacht ✦ Der *Diskdump* befindet sich auf einer externen Festplatte

Vorgehen	Der Server wird mit einem Live Linux, z.B. Backtrack. gestartet.
	Die externe Festplatte wird gemountet
	`# mount /dev/sdd1 /mnt/usb`
	Mit Hilfe von „dd" wird das Image von der externen Festplatte auf die erste Festplatte zurückgespielt.
	`# dd if=/mnt/usb/filebox_initial.dd of=/dev/sda bs=2048k`
	Der Parameter für die Blocksize (bs) ist nicht zwingend, jedoch kann so der Datendurchsatz wesentlich gesteigert werden.
	Nachdem das Image zurückgespielt wurde, wird der Server heruntergefahren, die Live CD und die externe Festplatte entfernt und anschliessend wieder neu gestartet.
	Nun muss die zweite Harddisk partitioniert- und in den Diskverbund aufgenommen werden. Dazu kann direkt das Layout der ersten Festplatte übernommen werden.
	`# sfdisk -d /dev/sda | sfdisk /dev/sdb`
	`# mdadm --add /dev/md0 /dev/sdb1`
	`# mdadm --add /dev/md1 /dev/sdb2`
	Als letztes wird der Bootmanager *Grub* auf die zweite Festplatte installiert.
	`# grub`
	`grub> device (hd0) /dev/sdb`
	`grub> root (hd0,0)`
	`grub> setup (hd0)`
	`grub> quit`

Testergebnis	erfolgreich

Tabelle 9-1: Testprotokoll Inbetriebnahme

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

9.2 Austausch Harddisk

Annahme	✦ Erste Harddisk des Servers (sda) ist defekt ✦ Server startet nach wie vor von der zweiten Festplatte (sdb)
Vorbereitung	✦ Server mit Live Linux (Backtrack) gestartet ✦ Alle Partitionen auf der ersten Harddisk gelöscht `# dd if=/dev/zero of=/dev/sda bs=512 count=1` ✦ Reboot → System wird von der zweiten Harddisk gestartet

Vorgehen	Nach dem Reboot startet der Server ohne Probleme, jedoch ist die erste Festplatte leer.
	
	`# [root@luigi ~]# fdisk -l`
	
	`Disk /dev/sda: 250.0 GB, 250000000000 bytes`
	`255 heads, 63 sectors/track, 30394 cylinders`
	`Units = cylinders of 16065 * 512 = 8225280 bytes`
	
	`Disk /dev/sda doesn't contain a valid partition table`
	
	`Disk /dev/sdb: 250.0 GB, 250000000000 bytes`
	`255 heads, 63 sectors/track, 30394 cylinders`
	`Units = cylinders of 16065 * 512 = 8225280 bytes`
	
	`   Device Boot      Start         End      Blocks   Id  System`
	`/dev/sdb1   *           1          13      104391   fd  Linux`
	`raid autodetect`
	`/dev/sdb2              14       30394   244035382+  fd  Linux`
	`raid autodetect`
	
	Das Partitionslayout muss von der noch intakten Festplatte gesichert- und auf die neue, ersetzte, Festplatte übernommen werden.
	
	`// Partitonstabelle in Textfile schreiben`
	`# sfdisk -d /dev/sdb > sdb.dump`
	
	`// Partitionstabelle auf ersetzte Festplatte übernehemen`
	`# sfdisk /dev/sda < sdb.dump`
	
	Das Partitionslayout ist nun wieder hergestellt
	
	`# [root@luigi ~]# fdisk -l /dev/sda`
	
	`Disk /dev/sda: 250.0 GB, 250000000000 bytes`
	`255 heads, 63 sectors/track, 30394 cylinders`
	`Units = cylinders of 16065 * 512 = 8225280 bytes`
	
	`   Device Boot      Start         End      Blocks   Id  System`
	`/dev/sda1   *           1          13      104391   fd  Linux`
	`raid autodetect`
	`/dev/sda2              14       30394   244035382+  fd  Linux`
	`raid autodetect`
	
	Das Software RAID kennt diese Platte noch nicht und man muss diese wieder in den

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

	Diskverbund aufnehmen:
	
	`# mdadm --add /dev/md0 /dev/sda1`
	`# mdadm --add /dev/md1 /dev/sda2`
	
	Die Synchronisation dauert je nach Festplattengrösse einige Stunden.
	
	Als letzter Schritt, muss der Bootmanager Grub wieder in dem MBR der ersten Festplatte installiert werden.
	
	`# [root@luigi ~]# grub`
	`Probing devices to guess BIOS drives. This may take a long time.`
	
	`GNU GRUB version 0.97 (640K lower / 3072K upper memory)`
	
	`[ Minimal BASH-like line editing is supported. For the first word, TAB`
	`lists possible command completions. Anywhere else TAB lists the possible`
	`completions of a device/filename.]`
	`grub> device (hd0) /dev/sda`
	`device (hd0) /dev/sda`
	`grub> root (hd0,0)`
	`root (hd0,0)`
	`Filesystem type is ext2fs, partition type 0xfd`
	`grub> setup (hd0)`
	`setup (hd0)`
	`Checking if "/boot/grub/stage1" exists... no`
	`Checking if "/grub/stage1" exists... yes`
	`Checking if "/grub/stage2" exists... yes`
	`Checking if "/grub/e2fs_stage1_5" exists... yes`
	`Running "embed /grub/e2fs_stage1_5 (hd0)"... 15 sectors are embedded.`
	`succeeded`
	`Running "install /grub/stage1 (hd0) (hd0)1+15 p (hd0,0)/grub/stage2 /grub/grub.conf"... succeeded`
	`Done.`
	`grub> quit`

Testergebnis	erfolgreich

Tabelle 9-2: Testprotokoll Harddiskaustausch

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

10 Ergebnisse

Der Initial-Setup der Appliance und die Auslieferung an den Kunden (Phase 1) kann mit den Resultaten aus dieser Diplomarbeit weitestgehend abgedeckt werden. Auch die Grundkonfiguration über ein webbasiertes Management Interface ist teilweise möglich, jedoch beschränkt sich dieses im Moment noch auf die Netzwerk Einstellungen.
Da der Webserver mit normalen Benutzerrechten gestartet wird, wäre es grundsätzlich gar nicht möglich, dass Systemeinstellungen über ein Webinterface geändert werden können. Die Konfiguration des Webservers musste also bewusst geschwächt werden, damit dies überhaupt möglich ist. Für den produktiven Betrieb ist eine solche Lösung nicht akzeptabel. Als Alternative könnte eine zweite Webserver-Instanz erzeugt werden. Die muss zwar auch mit Administrationsrechten gestartet werden, jedoch könnte diese an eine zweite Netzwerkkarte gebunden werden, welche nur aus dem lokalen Netzwerk- oder sogar nur von einem einzelnen System erreichbar ist. Aus zeitlichen Gründen konnte dies jedoch nicht mehr umgesetzt werden.

Dank der Ausarbeitung eines Update-Konzeptes und der Abbildung der FileBox und deren Abhängigkeiten in Form von *RPM* Paketen, kann auch die zweite Phase des Appliance Life-Cycle erfüllt werden.

Die Integrität von Aktualisierungen kann mit Hilfe einer digitalen Signatur sichergestellt werden. Compass Security wird also einen Private-Key haben, mit welchem jedes erstellte *RPM* Pakete digital unterschrieben wird. Die Appliance prüft vor der Installation eines Paketes, ob diese Signatur gültig ist und verweigert unter Umständen die Annahme.

Das Disaster Recovery bei dem Ausfall einer Festplatte konnte erfolgreich simuliert werden, in dem eine Festplatte während dem Betrieb gelöscht wurde. Dank dem erarbeiteten Harddisk Layout war es innert kürzester Zeit möglich die Daten von der noch funktionierenden Festplatte auf eine „neue" Festplatte zurückzuspielen.

Einige Anforderungen konnten aus zeitlichen Gründen nicht mehr umgesetzt werden. Davon betroffen waren unter anderem das Backup beziehungsweise der Restore der Datenbank und die aktive Überwachung von Hardware-Komponenten.
Dank den geschaffenen Voraussetzungen können solche Features aber auch zu einem späteren Zeitpunkt noch eingebaut werden.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

11 Ausblick

Der Prototyp der FileBox Appliance, welcher im Rahmen dieser Diplomarbeit erarbeitet wurde, erfüllt bereits einen grossen Teil der Anforderungen die durch Compass Security gestellt wurden.

Damit die Appliance schon baldmöglichst bei Kunden zum Einsatz kommen kann, sollten die restlichen Anforderungen rasch implementiert und ausgiebige Tests gestartet werden.

Dank dem modularen Aufbau und dem Update-Konzept, kann die Appliance auch in Zukunft ständig mit neuen Funktionen erweitert werden. Folgende Features wären beispielsweise durchaus denkbar:

- Integration in die bestehende Firmen-Infrastruktur: Die Appliance kann bestehende Ressourcen wie Datenablage, Backupkonzepte, Monitoring, usw. nutzen.
- Erkennen von Hard- und Software Problemen im laufenden Betrieb mit automatischer Benachrichtigung an die zuständige Person.
- Paralleler Betrieb mehrerer Appliances mit automatischer Lastverteilung.

Wer weiss, vielleicht ist die FileBox Appliance schon bald so selbstverständliche wie heutzutage ein Mailserver. Es wäre auf jeden Fall interessant einen entscheidenden Beitrag dazu geleistet zu haben.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

12 Persönlicher Bericht

Das Thema dieser Diplomarbeit hat mich von Anfang an fasziniert, da mir die Kombination von Hard- und Software sehr abwechslungsreich erschien. Ich wurde nicht enttäuscht, der Titel hielt was er versprach.

Bei der Entwicklung des Update-Konzeptes und dem Harddisk Layout hatte ich tiefgehende Einblicke in das Betriebssystem CentOS und konnte so meine bisherigen Linux-Kenntnisse erweitern. Technologien wie *RPM* oder *YUM* habe ich zwar früher regelmässig verwendet, mir aber nie grosse Gedanken darüber gemacht was für ein Aufwand hinter der Erzeugung von Softwarepaketen und deren Verteilung steckt. Ich denke ich werde in Zukunft die Arbeit der vielen, freiwilligen, Open-Source Entwickler noch mehr schätzen und ich könnte mir durchaus vorstellen auch privat mehr Zeit mit solchen Projekten zu verbringen.

Bei der Konfiguration des Apache HTTP Server und dem Applikationsserver Tomcat hatte ich zum ersten Mal praktische Einblicke in eine Multi-Tier-Applikation wie dies auch bei grösseren Anwendungen wie einem eBanking der Fall ist. Die Theorie war mir zwar aus dem Unterricht an der HSR bekannt, jedoch ist die Praxis noch interessanter.

Dass ich diese Diplomarbeit in einer Einzelgruppe geschrieben habe, sehe ich im Nachhinein als einen kleinen Nachteil. Ich konnte zwar immer alles so umsetzen wie ich es wollte, jedoch hatte ich nicht die Möglichkeit eine zweite Meinung einzuholen wenn ich Mal irgendwo angestossen bin. Auch das Verfassen von wichtigen Texten wie zum Beispiel dem Management Summary fällt einem alleine etwas schwerer.

Alles in allem hat mir diese Diplomarbeit sehr grossen Spass bereitet und ich würde mich sehr freuen, wenn die FileBox Appliance schon bald bei Kunden im Einsatz steht.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

13 Glossar

13.1 Technische Begriffe

Abkürzung	Beschreibung
Appliance	Dedizierte Hardware die einen spezifischen Service zur Verfügung stellt
apxs	APache eXtenSion Tool
CentOS	Community Enterprise Operating System
CI	Corporate Identity
CSNC	Compass Security Network Computing AG
Diskdump	Abbild einer Festplatte in einer einzelnen Datei
GCC	Die GNU Compiler Collection[3] ist eine Sammlung von Compilern aus dem GNU-Projekt. Spricht man von „gcc" wird meistens der C-Kompiler gemeint.
Live Linux	Linux Distribution die ab einer CD oder USB-Laufwerk gestartet wird und keine Änderungen am System vornimmt.
Logrotation	Log-Dateien von Applikationen werden in regelmässigen Abständen rotiert. Das heisst, dass die aktuelle Datei archiviert- und mit einer leeren Datei begonnen wird.
LVM[4]	Logical Volume Manager, Abstraktionsebene zwischen der Festplatte und dem Filesystem.
MBR	Der Master Boot Record ist der erste Block auf einer Festplatte in welchem der Bootmanager und das Partitionslayout gespeichert sind.
OS	Operating System, Betriebssystem
RFC	Request for Comments, definieren einen Standard
RPM	RPM Package Manager
Snapshot	Abbild der Festplatte
SSH	Secure Shell, verschlüsselte Verbindung auf die Konsole eines Systems.
SSL	Secure Socket Layer, Verschlüsselungsprotokoll
Trojaner	Bösartige Software, welche beispielsweise Daten vom System wegkopiert oder die interaktive Kontrolle eines Systems ermöglicht
VM	Virtual Machine, virtualisierte Betriebssystem-Instanz

[3] Informationen basierend auf Wikipedia: http://de.wikipedia.org/wiki/GNU_Compiler_Collection
[4] Informationen basierend auf Wikipedia: http://de.wikipedia.org/wiki/Logical_Volume_Manager

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

WAR	Web Archive, komprimierte Java-Webapplikation
Wrapper	Ein Wrapper erweitert die Funktion eines Programmes in dem er dieses aufruft und zusätzlich eigene Manipulationen an einem Objekt vornimmt.
ZFS[5]	Filesystem mit RAID Funktionalität welches von SUN Microsystems entwickelt wurde.

13.2 Dokumentspezifische Begriffe

Begriff	Erklärung
DA	Diplomarbeit
MS	Meilenstein
PT	Personentag

[5] Informationen basierend auf Wikipedia: http://de.wikipedia.org/wiki/ZFS_%28Dateisystem%29

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

14 Verzeichnisse

14.1 Literaturverzeichnis

Der Literaturverweis ist jeweils in der Fussnote der aktuellen Seite ersichtlich. Im Folgenden sind alle Nachweise noch einmal zusammengefasst.

	Titel, URL	Autor, Typ
1.	CentOS http://de.wikipedia.org/wiki/CentOS	Wikipedia Web
2.	RedHat Enterprise Linux http://de.wikipedia.org/wiki/Red_Hat_Enterprise_Linux#Enterprise_OS	Wikipedia Web
3.	GNU Compile Collection http://de.wikipedia.org/wiki/GNU_Compiler_Collection	Wikipedia Web
4.	LVM http://de.wikipedia.org/wiki/Logical_Volume_Manager	Wikipedia Web
5.	ZFS Dateisystem http://de.wikipedia.org/wiki/ZFS_%28Dateisystem%29	Wikipedia Web
6.	Software RAID http://dev.riseup.net/grimoire/storage/software-raid/	Riseup Labs Web
7.	RPM-Pakete erstellen http://www.linuxhaven.de/dlhp/HOWTO/DE-RPM-HOWTO-7.html	Marco Budde Web
8.	Createrepo http://createrepo.baseurl.org/	Unbekannt Web
9.	RFC2965 - HTTP State Management Mechanism http://www.faqs.org/rfcs/rfc2965	Unbekannt Web

Tabelle 14-1: Literaturverzeichnis

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

14.2 Abbildungsverzeichnis

Abbildung 4-1: Update-Konzept 11
Abbildung 6-1: Life-Cycle-Prozess 14
Abbildung 6-2: Life-Cycle Phasen 16
Abbildung 7-1: Dell PowerEdge R200 27
Abbildung 8-1: Layout Harddisks 32
Abbildung 8-2: Release Fahrplan 1 33
Abbildung 8-3: Release Fahrplan 2 34
Abbildung 8-4: FileBoxRepo Servlet 35
Abbildung 15-1: Geleistete Stunden 50
Abbildung 15-2: Installation Harddisk Layout 53
Abbildung 15-3: Installation Bootmanager 54
Abbildung 15-4: Installation Netzwerk Einstellungen 54
Abbildung 15-5: Installation Paket Auswahl 55

14.3 Tabellenverzeichnis

Tabelle 6-1: Übersicht Use Cases 17
Tabelle 6-2: UC1 - Vorbereitung 18
Tabelle 6-3: UC2 - Inbetriebnahme 18
Tabelle 6-4: UC3 - OS Updates 19
Tabelle 6-5: UC4 - FileBox Bugfixes 19
Tabelle 6-6: UC5 - FileBox Features 20
Tabelle 6-7: UC6 - Backup Daten 20
Tabelle 6-8: UC7 - Restore Daten 21
Tabelle 6-9: UC8 - Austausch defekter Festplatten 22
Tabelle 6-10: UC9 - Ausserbetriebnahme 22
Tabelle 7-1: Beschreibung mod_ssl 24
Tabelle 7-2: Beschreibung mod_but 24
Tabelle 7-3: Beschreibung mod_proxy 25
Tabelle 7-4: Beschreibung mod_rewrite 25
Tabelle 7-5: Beschreibung modsecurity2 25
Tabelle 7-6: Beschreibung mod_headers 26
Tabelle 7-7: Beschreibung mod_headers 26
Tabelle 7-8: Beschreibung mod_log_forensic 26
Tabelle 7-9: Beschreibung mod_unique_id 27
Tabelle 7-10: Appliance Hardware 27
Tabelle 8-1: Prototypen 29
Tabelle 8-2: Risikoabschätzung Harddisks 31
Tabelle 9-1: Testprotokoll Inbetriebnahme 38
Tabelle 9-2: Testprotokoll Harddiskaustausch 40
Tabelle 15-1: Literaturverzeichnis 46
Tabelle 16-1: Projektplaung Risikoanalyse 49
Tabelle 16-2: Sitzung vom 13.10.2009 50
Tabelle 16-3: Sitzung vom 22.10.2009 51
Tabelle 16-4: Sitzung vom 30.10.2009 52
Tabelle 16-5: Sitzung vom 16.11.2009 52
Tabelle 16-6: Entwicklungsserver 53
Tabelle 16-7: Grub Stages 56
Tabelle 16-8: RPM Spezifikation 59

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15 Anhang

15.1 Projektmanagement

15.1.1 Meilensteine

15.1.1.1 Meilenstein 1

Im ersten Meilenstein werden die Anforderungen an die Appliance aufgenommen und analysiert. Zudem wird die FileBox Testinstallation studiert, um alle Abhängigkeiten zu anderen Softwarekomponenten kennen zu lernen.

Anhand dieser Bedürfnisse werden Use Cases definiert und priorisiert, welche im Verlauf dieser Diplomarbeit umgesetzt werden.
Für jeden Use Case werden die kritischen Methoden und Technologien aufgenommen und dazu Prototypen entwickelt. So kann einerseits die Machbarkeit geprüft und das nötige Know-how aufgebaut werden.

Sollten es Anforderungen geben, die nicht umgesetzt werden können, werden diese mit dem Betreuer besprochen und nach Alternativen gesucht.

Der erste Meilenstein sollte bis zum 23. Oktober 2009 umgesetzt werden.

15.1.1.2 Meilenstein 2

Im zweiten Meilenstein werden die Use Cases mit der Priorität „1" umgesetzt. Folgende Reihenfolge wurde dabei gewählt:

- UC3-5: Betrieb - Installation von OS Updates, FileBox Bugfixes und FileBox Features.
  - RPM Pakete und Installationsroutinen erstellen
  - YUM Repositories einrichten
  - Lizenzüberprüfung implementieren
  - Testen ob die Anforderungen aus dem Use Case abgedeckt werden

- UC2: Inbetriebnahme und Konfiguration durch den Kunden über ein Webinterface.
  - Management Webinterface auf Basis von CGI/Perl entwickeln
  - Konfigurations-Templates erstellen
  - Staging Prozess entwickeln und dokumentieren
  - Testen ob die Anforderungen aus dem Use Case abgedeckt werden

- UC1: Vorbereitung der Appliance bis zur Auslieferung
  - Staging Prozess entwickeln und dokumentieren
  - Testen ob die Anforderungen aus dem Use Case abgedeckt werden

Ziel ist es diese Arbeiten bzw. diesen Meilenstein bis zum 6. November 2009 abzuschliessen.

15.1.1.3 Meilenstein 3

Im dritten Meilenstein werden die Use Cases mit niedrigerer Priorität umgesetzt:

- UC6: Backup Daten
  - Skript für ein Backup der Datenbank
  - Integration in das Management Interface

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

- Testen

- UC7: Restore Daten
  - Skript für den Restore einer gesicherten Datenbank
  - Integration in das Management Interface
  - Testen

- UC8: Austausch defekter Hardware
  - Prozess einer defekten Hardware durchspielen

- UC9: Ausserbetriebnahme
  - Appliances wipen

Sollten die Arbeiten im zweiten Meilenstein mehr Aufwand erfordern als ursprünglich kalkuliert, werden diese auf Kosten des dritten Meilensteines vorgezogen.

Das Ziel wäre es, diesen Meilenstein per 13. November 2009 abzuschliessen.

15.2 Risikoanalyse

Risiko Bewertungen								
Risk ID	Risiko	Auswirkung	Massnahme	Kosten der Massnahmen in h	Max. Schaden in h	Wahrschein-lichkeit des Eintreffens	Gewichteter Schaden in h	Priorität
R01	Automatisches Update der Appliance ist nicht möglich.	Mehraufwand im Projekt	Alternative Lösung muss gesucht werden: z.B. manuelles Update durch Betreiber	40	80	15%	12	Hoch
R02	Datenverlust im SVN Repository	Verzögerung im Projekt	Restore eines Backups, Überstunden	2	8	5%	0	Niedrig
R03	Mitarbeiter wird Krank oder hat einen Unfall	Verzögerung im Projekt, zurzeit des Ausfalls Projektstillstand	Reserven einplanen, Überstunden	24	240	10%	24	Mittel
R04	Missverständnisse zwischen Auftraggeber und Auftragnehmer	Mehraufand durch Sitzungen und Präsentationen	Sitzungen	12	30	15%	5	Hoch
	Total Kosten in Arbeitspaketen enthalten			78				
	Total Rückstellungen						41	

Tabelle 15-1: Projektplanung Risikoanalyse

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.3 Geleistete Stunden

Folgende Grafik zeigt die geleisteten Stunden pro Woche. Insgesamt sind bei dieser Diplomarbeit etwas mehr als 400 Arbeitsstunden zusammengekommen.

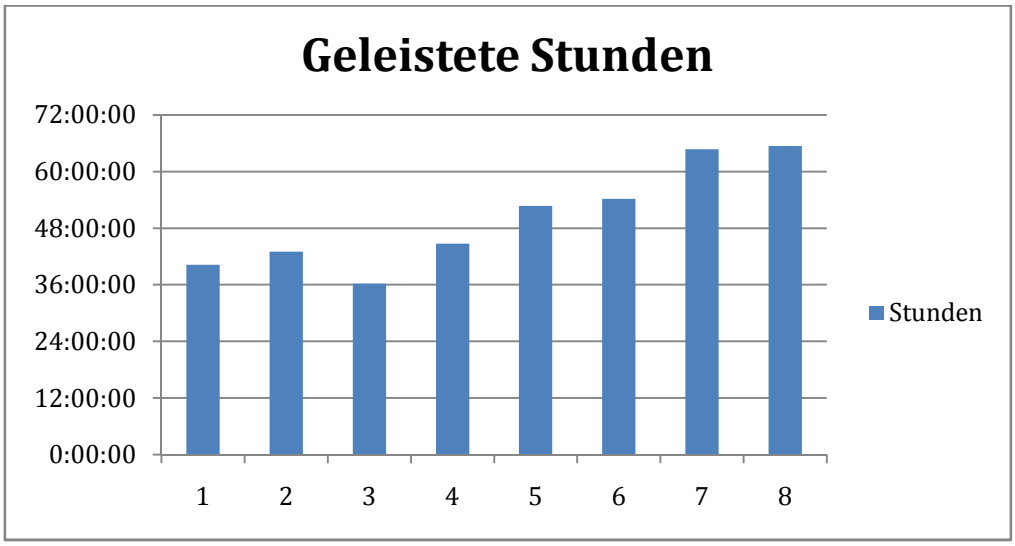

Abbildung 15-1: Geleistete Stunden

15.4 Sitzungsprotokolle

15.4.1 Sitzung vom 13.10.2009

Teilnehmer	Ivan Bütler, Roger Blum
Zeit	11:30 bis 12:00 Uhr
Themen	✦ Bisherige Arbeiten ✦ Besprechung der Aufgabenstellung ✦ Besprechung der Hardware für die Appliance ✦ Iterative Projektplanung ✦ Definition Meilensteine o MS1: Prototyp pro kritischem Punkt in Aufgabenstellung o MS2: Use-Cases mit hoher Priorität umgesetzt o MS3: Use-Cases mit Priorität < 1 umgesetzt
Deliverables	-
Nächste Sitzung	-

Tabelle 15-2: Sitzung vom 13.10.2009

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.4.2 Sitzung vom 22.10.2009

Teilnehmer	Ivan Bütler, Roger Blum
Zeit	14:30 bis 16:30 Uhr
Themen	✦ Use Cases besprochen o Aufgliederung in zwei Prozesse (Bestellung/Installation und Betrieb) o Priorisierung für FileBox ✦ FileBox Roadmap in DA einfliessen lassen ✦ Anforderungen an Kunden: Was müssen wir von ihm wissen um eine Appliance vorzubereiten ✦ Harddisk Konzept Appliance ✦ YUM Repository Konzept
Deliverables	✦ Übersicht Use Cases mit Priorität ✦ UC Betrieb aufteilen in verschiedene Update-Typen o OS o FileBox Bugfix o FileBox Feature ✦ Tabelle mit Prototypen o Nummerierung o Titel o Beschreibung o Ergebnis o Verweis/Link zu aufgebautem Know-how ✦ Bewertung / Konklusion für Meilenstein 2 o Was wird in MS2 umgesetzt o Definition MS2 o Termin bis wann MS2 umgesetzt wird
Nächste Sitzung	Mittwoch, 28.10.2009, 14:00 Uhr

Tabelle 15-3: Sitzung vom 22.10.2009

15.4.3 Sitzung vom 30.10.2009

Teilnehmer	Ivan Bütler, Roger Blum
Zeit	14:00 bis 15:30 Uhr
Themen	✦ Sitzungsprotokoll soll in Zukunft im Anschluss an die Sitzung an Betreuer gesendet ✦ Dokumentation wöchentlich an Betreuer senden ✦ Diskussion über die automatisierte Repository-Zuteilung mittels Fastestmirror-Plug-In o Daraus ist der Release Fahrplan entstanden (siehe Kapitel 8.6) o Appliance wird so vorbereitet, dass der Fahrplan umgesetzt werden kann ✦ Harddisk Layout präsentiert und begründet:

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Teilnehmer	Ivan Bütler, Roger Blum
	o Die Partition für die Datenbank-Daten (/var) ist für die DA genügend, soll jedoch später grösser sein o Unterschiedliche Partitionen für Applikationsdaten und Logfiles wurden gewählt
Deliverables	✦ Sitzungsprotokoll ✦ Aktuelle Version der Dokumentation
Nächste Sitzung	-

Tabelle 15-4: Sitzung vom 30.10.2009

15.4.4 Sitzung vom 16.11.2009

Teilnehmer	Ivan Bütler, Roger Blum
Zeit	08:30 bis 09:30 Uhr
Themen	✦ Abstract o Abstract kann noch interessanter gestaltet werden o Vergleichbar mit dem Werbeflyer zu einem Produkt ✦ Management Summary o Text soll mehr technisch gehalten werden o Keine unnötigen Informationen o Formulierung teilweise zu kompliziert ✦ A0-Poster o Gute Bilder o Text kann noch weiter gekürzt werden
Deliverables	-
Nächste Sitzung	-

Tabelle 15-5: Sitzung vom 16.11.2009

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.5 Setup Betriebssystem

Für die Entwicklung der FileBox Appliance wurde eine VMware Virtual Machine vorbereitet und folgendermassen konfiguriert:

Betriebssystem	CentOS 5.4
Architektur	64Bit (x86_64)
RAM	512MB
Harddisk	50GB

Tabelle 15-6: Entwicklungsserver

Die Harddisk der virtuellen Maschine wird in mehrere logische Laufwerke (Volumes) aufgeteilt. Dies hat den Vorteil, dass die einzelnen Volumes unterschiedlich gemountet und so die Sicherheit des Systems erhöht werden kann.
Im späteren Betrieb wird das Verzeichnis */opt* als Hauptverzeichnis für das Software Repository verwendet. Aus diesem Grund wird es ebenfalls als separates, logisches Volume angelegt.

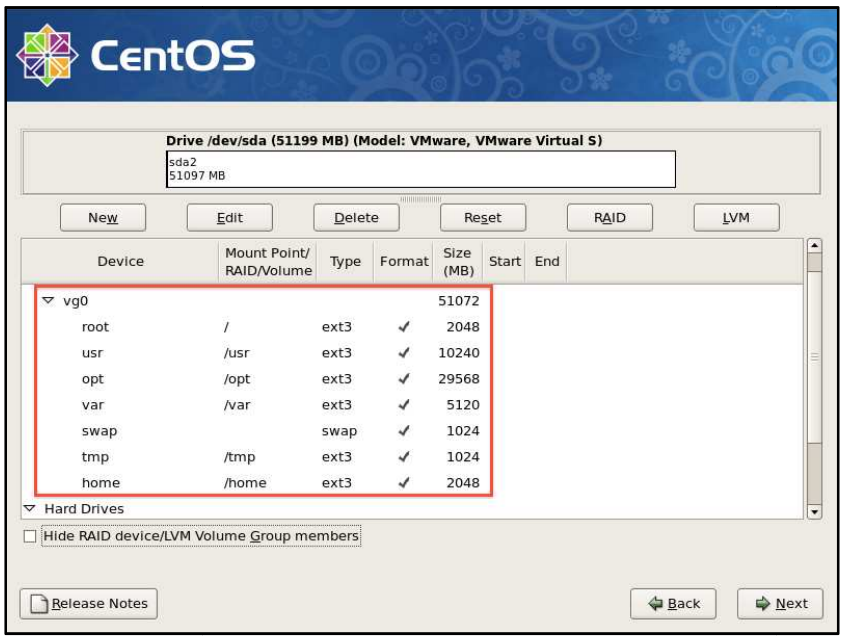

Abbildung 15-2: Installation Harddisk Layout

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Der Bootmanager *GRUB* wird in den *MBR* (Master Boot Record) der primären Festplatte „/dev/sda" installiert.

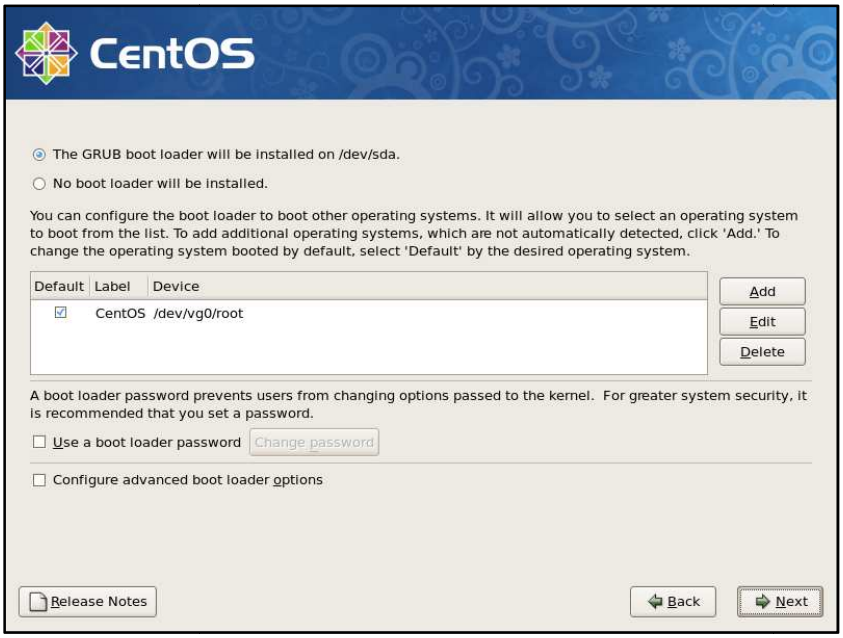

Abbildung 15-3: Installation Bootmanager

Die IP Adresse für den Server wurde statisch auf 172.16.122.31 mit dem Subnetz 255.255.255.0 konfiguriert. Der Gateway und gleichzeitig auch DNS Server für dieses System ist der Host mit der IP Adresse 172.16.122.2.

Abbildung 15-4: Installation Netzwerk Einstellungen

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Um eine möglichst minimale Betriebssystem-Installation zu erhalten, muss die erweiterte Paketauswahl genutzt werden. Nur so können auch wirklich alle unnötigen Softwarepakete von der Auswahl entfernt werden.

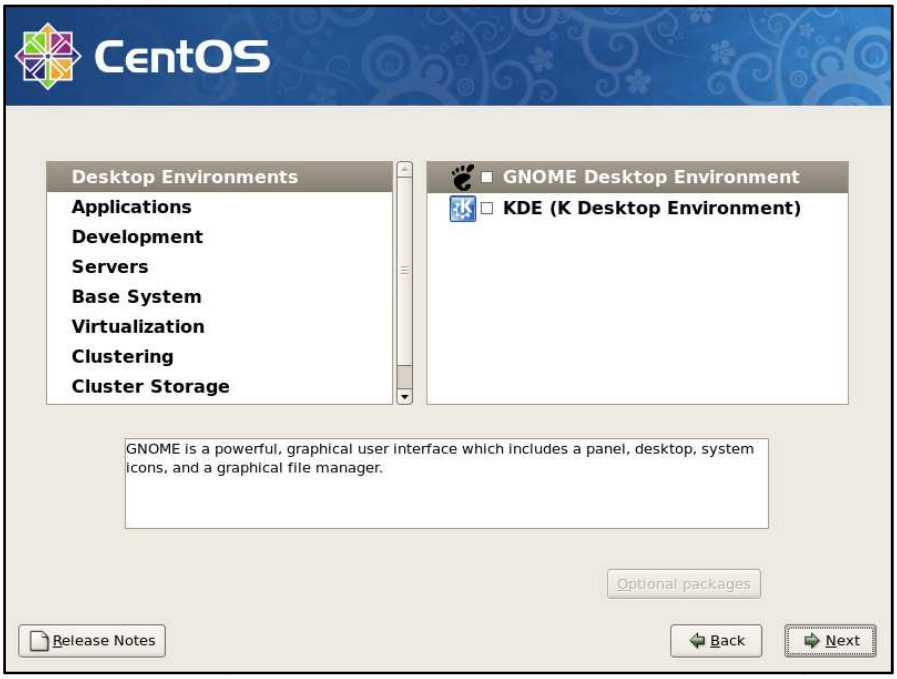

Abbildung 15-5: Installation Paket Auswahl

Schliesslich wird die Installation gestartet.
Bereits nach wenigen Minuten kann das System verwendet werden.

15.5.1 LVM - Logical Volume Manager

Mit LVM (Logical Volume Management) können Festplatten unter Linux abstrahiert werden. Das heisst, es werden keine eigentliche Partitionen mehr angelegt. Die Harddisk oder Teile davon werden in einen Diskpool, einer Volume Group (VG), gemappt und bilden so einen grossen Pool von Speicherplatz. Nun werden Logical Volumes (LV) erstellt, welche mit den bisher bekannten Partitionen vergleichbar sind. Der Vorteil dieser Abstrahierung ist, dass die logischen Volumes, abhängig vom Filesystem, zur Laufzeit verändert werden können. Es ist auch möglich Snapshots von einem LV zu machen. Dabei wird der aktuelle Stand eines LV's in einem neuen LV eingefroren und kann so z.B. gesichert, oder als alternative Startpartition verwendet werden.

Nachfolgend werden die wichtigsten Systembefehle für *LVM* kurz erklärt.

Volume Group erstellen:
```
# vgcreate <vg_name> /dev/sda1 /dev/sdb1
```

Logical Volume erstellen:
```
# lvcreate –n <lv_name> -L<groesse> <vgname>
```

Ein logisches Volume nach dem Erstellen mounten:
```
# mount /dev/<vg_name>/<lv_name> /mnt/<mountpoint>
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.5.2 Software RAID

Mit folgendem Befehl [6]kann eine Harddisk nach dem Austausch wieder in einen Diskverbund aufgenommen werden:

```
# mdadm --manage /dev/mdX --add /dev/sdaX
```

15.5.3 Grub

Der Bootmanager *Grub* wird zum Starten des Betriebssystems verwendet. Normalerweise belegt ein Bootmanager die ersten 512 Bytes der ersten Festplatte und startet daraus das installierte Betriebssystem. Da *Grub* aber über wesentlich mehr Funktionen als ein gewöhnlicher Bootmanager verfügt, reichen diese 512 Bytes nicht aus, weshalb der Bootmanager in drei Teile aufgeteilt wurde. Diese werden als Stage 1, 1.5 und 2 bezeichnet.

Stage	Funktion
Stage 1	✦ Wird im Bootsektor der Festplatte installiert und belegt die ersten 512 Bytes. ✦ Dient nur dazu Stage 1.5 oder 2 zu laden.
Stage 1.5	✦ Liegt zwischen Bootsektor und dem ersten Block der ersten Partition. ✦ Enthält Treiber für das Filesystem auf welchem Stage 2 liegt.
Stage 2	✦ Befindet sich auf einer beliebigen Partition der Festplatte. ✦ Zeigt das Bootmenü welches aus einer Konfigurationsdatei geladen wird. ✦ Startet schliesslich das selektierte Betriebssystem.

Tabelle 15-7: Grub Stages

Grub verwendet andere Namen für Festplatten und Partitionen. Die von Linux bekannten Bezeichnungen wie „hda" für IDE Festplatten und „sda" für SCSI oder S-ATA Festplatten gibt es unter *Grub* nicht. Er benennt alle Disk nach dem Schema *„(hd0)"*, „(hd1)", usw.
Die erste Partition auf der ersten Festplatte heisst somit nicht „sda1" sondern „(hd0,0)".

15.5.4 Grub und RAID

Wird Grub zusammen mit einem Software RAID 1 (Mirroring) verwendet, muss ein kleiner Trick angewendet werden, damit ein System auch noch startet, selbst wenn die erste Festplatte defekt ist. In diesem Fall wird die Festplatte die ursprünglich „sdb" hiess, zu „sda". Der *Grub* Bootmanager auf der zweiten Festplatte ist aber so konfiguriert, dass er Stage 2 aus der zweiten Harddisk, also „sdb" lädt. Er würde Stage 2 also nicht finden.
Mit einem manuellen Eingriff kann dem aber entgegengewirkt werden, indem man dem *Grub* der zweiten Festplatte vorgibt, dass er sich auf der Ersten Festplatte befindet.

```
# grub
grub> device (hd0) /dev/sdb
grub> root (hd0,0)
grub> setup (hd0)
```

Mit dem Kommando „device (hd0) /dev/sdb" wird die zweite Harddisk auf den Namen „(hd0)" gemappt. Grub wird so auf der zweiten Festplatte installiert, jedoch mit einer Konfiguration die er für die erste Festplatte verwenden würde.

[6] Software RAID, http://dev.riseup.net/grimoire/storage/software-raid/, Riseup Labs

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.5.5 Chattr

Eine Anforderung für die Appliance ist, dass Logfiles vom Web- und Applikationsserver nur angefügt, jedoch nicht überschrieben oder gelöscht werden können. Mit dem Programm „chattr" können spezielle Attribute für eine Datei auf einem Ext2/Ext3 Filesystem gesetzt werden.
Mit folgendem Befehl wird die angegebene Datei gegen das Verändern und Löschen geschützt. Der Benutzer kann dann nur noch Text an das Dokument anfügen.

```
# chattr +a <filename>
```

Nur der Benutzer *root* kann diese Attribute wieder entfernen.

15.6 Setup Software

15.6.1 RPM Pakete

CentOS verwendet für die Softwareinstallation das RPM Paketsystem. Dieses wurde ursprünglich von RedHat entwickelt, wird heutzutage aber von sehr vielen Distributionen eingesetzt.
RPM Pakete können sowohl Software Quellcode als auch binäre Dateien enthalten. Im ersten Fall wird das Programm bei der Installation kompiliert und an die entsprechende Stelle kopiert.
Der Vorteil von RPM Paketen ist, dass für jedes Paket Abhängigkeiten definiert werden können. So kann ein Paket erst installiert werden, wenn diese alle erfüllt sind. Gibt es eine neuere Version der Software, kann das Paket aktualisiert werden, ohne dass bestehenden Konfigurationsdateien überschrieben werden.

Einige von der FileBox benötigte Apache Module sind nicht im regulären CentOS Release enthalten. Damit diese später auf den neuesten Stand gebracht werden können, ohne dass ein manueller Eingriff erforderlich ist, wurden für diese Module RPM Pakete erstellt.

Dateinamen von RPM Paketen sind standardisiert und werden aus folgenden Elementen zusammengesetzt:

```
<name>-<version>-<release>-<architektur>.rpm

Optional kann zwischen dem Release und der Architektur noch das OS angegeben
werden. Bei CentOS 5.4 wäre die „el5" für Enterprise Linux 5.
```

Nachfolgend einige wichtige Befehle für RPM Pakete:

Paket installieren bzw. updaten:

```
# rpm –Uvh mod_but-3.3-1.i386.rpm
```

-U Update aktualisieren (Update). Falls das Paket noch nicht auf dem System vorhanden ist: Paket installieren
-v Detailliertere Ausgabe (Verbose)
-h Hash des Paketes ausgeben

Paket deinstallieren:

```
# rpm –e mod_but
```

-e Pakete vom System entfernen (Erase)

Alle installierten Pakete auflisten und nach Namen filtern:

```
# rpm –qa | grep <name>
```

-q Suche nach Paket (Query)
-a Alle Pakete auflisten (Filtern gegebenenfalls mittels „grep")

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.6.1.1 Erstellung von RPM Paketen

Schritt 1: Entwicklungsumgebung vorbereiten

Zum Erstellen von RPM Paketen muss das Hilfsprogramm „rpmbuild" installiert werden. Dies erfolgt mit folgendem Kommando:

```
# yum install rpmbuild
```

Nachfolgend kann die Entwicklungsumgebung vorbereitet werden. Diese besteht aus einer vorgegebenen Ordnerstruktur die vorzugsweise im Home-Verzeichnis eines Benutzers angelegt wird. RPM Pakete sollten immer mit normalen Benutzerprivilegien erzeugt werden. Der Root-Account sollte nicht für die Erstellung von Paketen genutzt werden.

```
# cd ~
# mkdir –-parents rpm/{BUILD,RPMS,SOURCES,SPECS,SRPMS}
```

Die Konfiguration für „rpmbuild" kann wahlweise im Home-Verzeichnis des Benutzers oder global im Verzeichnis „/etc" angelegt werden. Nachfolgend ein Beispiel für eine saubere Konfiguration im Home-Verzeichnis eines Benutzers.

```
# cd ~
# vi .rpmmacros
```

~/.rpmmacros:

```
%_topdir /home/rblum/rpm
%_builddir %{_topdir}/BUILD
%_rpmdir %{_topdir}/RPMS
%_sourcedir %{_topdir}/SOURCES
%_specdir %{_topdir}/SPECS
%_srcrpmdir %{_topdir}/SRPMS
```

Soll ein Paket mit GPG signiert werden können, müssen zusätzlich folgende Zeilen angefügt werden. Der Parameter „%_gpg_name" definiert dabei die ID des zu verwendenden Private Keys.

```
%_signature gpg
%_gpg_name DXXXXXX
```

Schritt 2: Paket erzeugen

Für jedes *RPM* Paket das man erzeugt werden soll, muss eine Spezifikation [7]angelegt werden. Dabei handelt es sich um eine Textdatei die Parameter und Makros enthält. Die Makros können anhand eines vorgestellten Prozent-Zeichen (%) erkannt werden.

Summary:	Kurzbeschreibung der Software, maximal eine Zeile
Name:	Name der Software, ohne Leerzeichen, bildet Dateinamen
Version:	Versionsnummer
Release:	Ändert sich bei minimalen Anpassung am Quellcode

[7] RPM-Pakete erstellen, http://www.linuxhaven.de/dlhp/HOWTO/DE-RPM-HOWTO-7.html, Marco Budde

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Packager:	Name / E-Mail Adresse des Paketerzeugers
License:	Lizenztyp der Software
Group:	Gruppe / Kategorie in welche die Software gehört, vergleichbar mit einer Verzeichnisstruktur
Source:	URL zum Hersteller
%description	Beschreibung zu der Software in Prosatext. Kann mehrere Zeilen umfassen.
%files	Auflistung der Dateien die zum Paket gehören. Wird vor den Dateiname ein „%config" gesetzt handelt es sich um eine Konfigurationsdatei. Diese werden bei einem Update nicht überschrieben, sondern zu der bestehenden Datei gelegt und mit der Erweiterung „rpmnew" versehen. Mit „%dir" wird ein ganzes Verzeichnis angegeben.
%pre %post %preun %postun	Hier können Skripte angegeben werden, die jeweils vor- oder nach der Installation bzw. Deinstallation ausgeführt werden.

Tabelle 15-8: RPM Spezifikation

mod_but.spec:

```
Summary: <Kurzbeschreibung, eine Zeile>
Name: <Späterer Name des Paketes>
Version: <Versionsnummer>
Release: <Releasenummer>
Packager: <Name / E-Mail Adresse des Erzeugers>
License: <Lizenzart>
Group: <Gruppe, wichtig für Paketverwaltungssysteme>
Source: <URL zu Webseite des Programmes>

%description
<Beschreibung in Prosa, mehrere Zeilen möglich>

%files
<Auflistung der Dateien die ins Paket gepackt werden sollen>
```

Bei dem Parameter „Group" wird ein Gruppenname angegeben, vergleichbar mit einem Verzeichnispfad. Dieser dient dazu, dass bei einem grafischen Paketverwaltungsprogramm das Paket in eine Kategorie eingegliedert werden kann.
Folgende Namen sind von RPM vorgegeben und sollten nach Möglichkeit eingehalten werden:

/usr/share/doc/rpm-4.4.2.3/GROUPS:

```
Amusements/Games
Amusements/Graphics
Applications/Archiving
Applications/Communications
Applications/Databases
Applications/Editors
Applications/Emulators
Applications/Engineering
Applications/File
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
Applications/Internet
Applications/Multimedia
Applications/Productivity
Applications/Publishing
Applications/System
Applications/Text
Development/Debuggers
Development/Languages
Development/Libraries
Development/System
Development/Tools
Documentation
System Environment/Base
System Environment/Daemons
System Environment/Kernel
System Environment/Libraries
System Environment/Shells
User Interface/Desktops
User Interface/X
User Interface/X Hardware Support
```

Das Paket wird schliesslich mit folgendem Befehl erstellt und befindet sich im Anschluss im Verzeichnis „~/rpmbuild/RPMS/x86_64":

```
# rpmbuild –bb –-sign <file>.spec
```

-b Es wird ein binary Paket erzeugt
-- sign Das Paket wird digital signiert

15.6.2 YUM

YUM steht für Yellow Update Modified. Es ist ein Paket-Management-System für *RPM* Pakete welches von vielen Linux-Distributionen, unter anderem auch CentOS, verwendet wird. Mit *YUM* können Software-Pakete gesucht, installiert, aktualisiert und deinstalliert werden.
Im Wesentlichen besteht *YUM* aus zwei Teilen: - Dem Kommandozeilenprogramm als Client und aus einem Serverteil, dem sogenannten *YUM* Software *Repository*.

15.6.2.1 YUM Client

Der *YUM* Client ist ein Kommandozeilenprogramm welches diverse Optionen unterstützt. Im Folgenden werden diese kurz erläutert:

Nach *RPM* Paketen suchen:

```
# yum search <name>
```

RPM Paket installieren:

```
# yum install <name>
```

Installierte Pakete aktualisieren (wenn nötig):

```
# yum update
```

Installiertes Paket entfernen (inkl. deren Abhängigkeiten):

```
# yum remove <name>
```

YUM setzt auf den bereits bekannten Funktionen der RPM Pakete auf. So werden z.B. die Abhängigkeiten überprüft und bei der Installation gleich mit einbezogen.

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Grundsätzlich ist es möglich, beliebig viele *Repositories* nach *RPM* Paketen zu durchsuchen. Im Verzeichnis „/etc/yum.repos.d/" muss pro *Repository* eine Konfigurationsdatei erstellt werden. In solche einer Datei wird definiert, wie das Repository zu erreichen ist.
Die einzelnen Repositories können auch priorisiert werden. So können z.B. Pakete aus dem Distributions-Release den Paketen eines Drittherstellers vorgezogen werden.

Der YUM Client ist modular aufgebaut. So gibt es Plug-Ins die den Funktionsumfang des Clients erweitern. Zwei Beispiele wären sind die Plug-Ins „fastestmirror" welches jeweils den geographisch nächstgelegenen Updateserver heraussucht oder das „yum-updatesd" welches in regelmässigen Abständen nach neuen Updates sucht.

15.6.2.2 YUM Repository

Ein *YUM Repository* ist eine Sammlung von *RPM* Paketen die entweder auf dem lokalen Dateisystem, einer CD, einem Web- oder FTP Server abgelegt sind. In jedem Repository gibt es ein Inhaltsverzeichnis, welches die Namen und Versionen der Software Pakete enthält. Der *YUM* Client muss so nicht das ganze Repository durchsuchen, sonder kann diesen Index herunterladen.
Will man ein eigenes *YUM Repository* im Internet aufbauen, benötigt man nur einen Web- oder FTP Server und eigene *RPM* Pakete. Der Index wird mit Hilfe des Programms „createrepo[8]" erstellt.

```
# createrepo /pfad/zum/software/verzeichnis
```

15.6.3 Apache HTTP Server Module kompilieren

Einige Apache Module sind nicht im CentOS Release enthalten uns müssen deshalb vorgängig kompiliert werden. Solche Arbeiten werden auf dem Entwicklungsserver „fbdev64" gemacht.
Die Module werden mit Hilfe von *apxs*, dem APache eXtenSion tool kompiliert. Dieses Programm ist ein *Wrapper* um den Compiler „GCC", der dafür sorgt, dass das Modul mit denselben Parametern kompiliert wird, welche bereits bei dem Apache HTTP Server verwendet wurden. So wird sichergestellt, dass die Module später auch auf den installierten HTTP Server Version abgestimmt sind.

Apxs ist im Paket „httpd-devel" enthalten. Dieses Paket wird nun zusammen mit weiteren Abhängigkeiten für die Apache Module heruntergeladen und installiert.

```
# yum install make httpd-devel pcre-devel libxml2-devel
```

Das System ist nun bereit für das Kompilieren der Apache Module.

15.6.3.1 modsecurity2

Das Modul wird von der Webseite des Herstellers heruntergeladen und entpackt.

```
# wget http://downloads.sourceforge.net/project/mod-security/modsecurity-
apache/2.5.11/modsecurity-apache_2.5.11.tar.gz?use_mirror=sunet
# tar xfz modsecurity-apache_2.5.11.tar.gz
# cd modsecurity-apache_2.5.11/apache2/
```

Anschliessend werden die Abhängigkeiten überprüft und das Modul kompiliert bzw. installiert.

```
# ./configure
# make
# make install
```

Das Modul befindet sich im danach im Verzeichnis */usr/lib64/httpd/modules/mod_security2.so*.

[8]Createrepo, http://createrepo.baseurl.org/, Unbekannt

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.6.3.2 mod_replace

Bei mod_replace wird nicht die aktuellste Version aus dem Internet verwendet, sondern eine durch Compass leicht modifizierte Variante.
In diesem Fall wird das Modul direkt mit *apxs* kompiliert und installiert.

```
# cd mod_replace
# apxs -c -i mod_replace.c
```

Im Anschluss befindet sich das Modul im Verzeichnis */usr/lib64/httpd/modules/mod_replace.so*.

15.6.3.3 mod_but

Dieses Modul wird ausschliesslich durch Compass Security gepflegt und ist somit auch nur über das interne Repository erhältlich. Das Modul kann aus den Quelldateien mittels nachfolgendem Befehl erstellt werden.

```
# cd mod_but
# make
```

Im Anschluss befindet sich das Modul im Verzeichnis „/usr/lib64/httpd/modules/mod_but.so".

15.7 Problem: Firefox akzeptiert Cookies nicht

Folgendes Problem ist bei einem Test der FileBox Appliance aufgetreten:

Um die FileBox und deren Abhängigkeiten besser kennenzulernen, wurde in einer VM die komplette Umgebung nachgebaut. Zu Beginn funktionierte alles bestens, doch als eine Woche später die VM wieder verwendet wurde, war der Zugriff auf die Login-Applikation der FileBox nicht mehr möglich. Stattessen wurde man auf eine Fehlerseite von „mod_but" weitergeleitet, welche besagte, dass der Browser (Firefox) keine Cookies akzeptiert.
Mit Hilfe des Tools Paros Proxy wurde das Problem weiter analysiert. Dazu wird der Proxy zwischen Browser und Webserver geschaltet. So kann der Verkehr (Requests und Responses) analysiert- und ein Fehler erkannt werden.
In diesem Fall war es so, dass die Applikation zwar eine Session Cookie sendet, der Browser dieses aber bei einer erneuten Anfrage nicht mehr mitsendete. Das Problem wurde schliesslich beim Browser vermutet, weshalb ein anderes Produkt (Safari) gewählt wurde. Mit diesem Browser funktionierte der Login ohne weitere Probleme.
Die Rekonstruierung aller Änderungen an dieser virtuellen Maschine brachte schliesslich die Lösung. In der Zwischenzeit wurde der Host von ursprünglich „fbdev.local" zu „fbdev" umbenannt. Genau diese Endung bzw. das Fehlen derer war der Grund weshalb der Browser das Session Cookie nicht mehr mitsendete.

Recherchen im Internet ergaben, dass der RFC2965[9], HTTP State Management Mechanism, der Grund für dieses Verhalten war:
Dieser besagt unter anderem, dass nur Cookies für Webseiten akzeptiert werden dürfen, die einen Punkt im Hostnamen haben. Firefox scheint der einzige Browser zu sein, welcher die Vorgaben des RFC strikt umgesetzt hat.
Die Vermutung liegt nahe, dass gerade Webentwickler welche häufig mit dem Hostnamen „localhost" arbeiten, schon oft über dieses Problem gestolpert sind.

[9] RFC2965 - HTTP State Management Mechanism, http://www.faqs.org/rfcs/rfc2965

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

15.8 Quelldateien

15.8.1 RPM Spezifikationen

15.8.1.1 mod_but

```
Summary: entry server module for httpd
Name: mod_but
Version: 3.3
Release: 1
Packager: Roger Blum <rblum@hsr.ch>
License: Other
Group: Applications/Internet
Requires: httpd >= 2.2.3

%description
mod_but is a module for Apache HTTP server to create an entry server with a
cookie store

%files
/usr/lib/httpd/modules/mod_but.so
```

15.8.1.2 mod_replace

```
Summary: filter module for apache http server
Name: mod_replace
Version: 0.1
Release: 1
Packager: Roger Blum <rblum@hsr.ch>
License: GPL
Group: Application/Internet
Source: http://downloads.sourceforge.net/project/mod-replace/mod-
replace/mod_replace-0.1.0.tar.gz/mod_replace-0.1.0.tar.gz
Requires: httpd >= 2.2.3

%description
Filter and replace strings in HTTP requests and responses. This can be done in
the header and in the body too.

%files
/usr/lib/httpd/modules/mod_replace.so
```

15.8.1.3 modsecurity2

```
Summary: web application firewall for apache http server
Name: modsecurity2
Version: 2.5.10
Release: 1
Packager: Roger Blum <rblum@hsr.ch>
License: GPLv2
Group: Application/Internet
Source: http://www.modsecurity.org/download/modsecurity-apache_2.5.10.tar.gz
Requires: httpd >= 2.2.3

%description
Web application firewall with advanced logging capabilities for Apache HTTP
server.
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
%files
/usr/lib/httpd/modules/mod_security2.so
```

15.8.1.4 FileBox

```
Summary: FileBox
Name: filebox
Version: 2.8
Release: 1
Packager: Roger Blum <rblum@hsr.ch>
License: Other
Group: Application/Internet
Source: http://www.filebox-solution.com/
Requires: java-1.6.0-sun >= 1.6.0.11, tomcat5 >= 5.5.23, unzip >= 5.52, mysql-
server >= 5.0.77, httpd >= 2.2.3, mod_ssl >= 2.2.3, mod_but >= 3.3, mod_replace
>= 0.1, modsecurity2 >= 2.5.10, sudo >= 1.6.9p17

%description
FileBox for secure file exchange

%define _fb_root /usr/share/filebox
%define _fb_conf /etc/filebox
%define _fb_mgmt /var/www/mgmt
%define _fb_app /usr/share/tomcat5/webapps

%files
%_fb_root
%_fb_conf
%_fb_mgmt

%post
source %_fb_conf/filebox.conf
source %_fb_conf/network.conf
source %_fb_conf/database.conf

service httpd stop
rm -rf /etc/httpd/conf.d/*
%_fb_root/script/confgen.sh %_fb_root/templates/httpd/filebox.11.httpd.conf.tmpl
/etc/httpd/conf.d/filebox.11.httpd.conf
%_fb_root/script/confgen.sh %_fb_root/templates/httpd/filebox.12.httpsd.conf.tmpl
/etc/httpd/conf.d/filebox.12.httpsd.conf
%_fb_root/script/confgen.sh %_fb_root/templates/httpd/filebox.30.mgmt.conf.tmpl
/etc/httpd/conf.d/filebox.30.mgmt.conf
cp %_fb_root/templates/httpd/filebox.10.general.conf /etc/httpd/conf.d/
cp %_fb_root/templates/httpd/filebox.20.error.conf /etc/httpd/conf.d/
cp -r %_fb_root/templates/httpd/filebox_modsecurity /etc/httpd/conf.d/
openssl req -new -newkey rsa:2048 -nodes -subj "/CN=${SERVER_NAME}/O=Compass
Security AG/C=CH/ST=St. Gallen/L=Rapperswil" -keyout
/etc/pki/tls/private/filebox.key -out /etc/pki/tls/certs/filebox.csr
openssl x509 -in /etc/pki/tls/certs/filebox.csr -out
/etc/pki/tls/certs/filebox.crt -req -signkey /etc/pki/tls/private/filebox.key -
days 730
service httpd start
chkconfig httpd on

service mysqld start

mysql -u root -h localhost < %_fb_root/templates/filebox/upload.sql
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
%_fb_root/script/confgen.sh %_fb_root/templates/filebox/sqluser.sql.tmpl
%_fb_root/templates/filebox/sqluser.sql
mysql -u root -h localhost < %_fb_root/templates/filebox/sqluser.sql
mysql -u root -h localhost < %_fb_root/templates/filebox/initial.sql

chkconfig mysqld on


service tomcat5 stop
rm -rf /usr/share/tomcat5/webapps/*
unzip %_fb_root/war/enterpriseadmin.war -d
/usr/share/tomcat5/webapps/enterpriseadmin
unzip %_fb_root/war/event.war -d /usr/share/tomcat5/webapps/event
unzip %_fb_root/war/fastexchange.war -d /usr/share/tomcat5/webapps/fastexchange
unzip %_fb_root/war/internal.war -d /usr/share/tomcat5/webapps/internal
unzip %_fb_root/war/login.war -d /usr/share/tomcat5/webapps/login
unzip %_fb_root/war/uploadadmin.war -d /usr/share/tomcat5/webapps/uploadadmin
unzip %_fb_root/war/upload.war -d /usr/share/tomcat5/webapps/upload

%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/BaseConfig.properties.tmpl
%_fb_app/enterpriseadmin/WEB-INF/classes/ch/csnc/BaseConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/BaseConfig.properties.tmpl %_fb_app/event/WEB-
INF/classes/ch/csnc/BaseConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/BaseConfig.properties.tmpl %_fb_app/fastexchange/WEB-
INF/classes/ch/csnc/BaseConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/BaseConfig.properties.tmpl %_fb_app/internal/WEB-
INF/classes/ch/csnc/BaseConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/BaseConfig.properties.tmpl %_fb_app/login/WEB-
INF/classes/ch/csnc/BaseConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/BaseConfig.properties.tmpl %_fb_app/upload/WEB-
INF/classes/ch/csnc/BaseConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/BaseConfig.properties.tmpl %_fb_app/uploadadmin/WEB-
INF/classes/ch/csnc/BaseConfig.properties

%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/enterpriseadmin_UploadConfig.properties.tmpl
%_fb_app/enterpriseadmin/WEB-INF/classes/ch/csnc/UploadConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/event_UploadConfig.properties.tmpl
%_fb_app/event/WEB-INF/classes/ch/csnc/UploadConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/fastexchange_UploadConfig.properties.tmpl
%_fb_app/fastexchange/WEB-INF/classes/ch/csnc/UploadConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/internal_UploadConfig.properties.tmpl
%_fb_app/internal/WEB-INF/classes/ch/csnc/UploadConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/login_LoginConfig.properties.tmpl %_fb_app/login/WEB-
INF/classes/ch/csnc/LoginConfig.properties
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/upload_UploadConfig.properties.tmpl
%_fb_app/upload/WEB-INF/classes/ch/csnc/UploadConfig.properties
%_fb_root/script/confgen.sh
%_fb_root/templates/filebox/uploadadmin_UploadConfig.properties.tmpl
%_fb_app/uploadadmin/WEB-INF/classes/ch/csnc/UploadConfig.properties

cp %_fb_root/war/local_policy.jar /usr/lib/jvm-private/java-1.6.0-
sun/jce/vanilla/
cp %_fb_root/war/US_export_policy.jar /usr/lib/jvm-private/java-1.6.0-
sun/jce/vanilla/

service tomcat5 start
chkconfig tomcat5 on


mkdir -p /var/spool/sms/outgoing
chmod 777 /var/spool/sms/outgoing
cp %_fb_root/templates/filebox/splash.xpm.gz /boot/grub
```

15.8.2 Management Webinterface

index.html:

```
<html>
    <head>
        <title>FileBox Management</title>
    </head>
    <body>
        <h1>FileBox Management</h1>
        <table width="100%" border="1">
            <tr>
                <td><a href="network.cgi">Network</a></td>
                <td>Database</td>
                <td>Maintenance</td>
                <td><a href="system.cgi">System</a></td>
                <td>Logout</td>
            </tr>
        </table>
    </body>
</html>
```

network.cgi:

```
#!/usr/bin/perl -w

use strict;
use CGI;

my $cgi = new CGI;
my $method="POST";
my $action=$cgi->url(-relative=>1);
my $encoding="";

my $eth0_ip = $cgi->param('_ETH0_IP');
my $eth0_netmask = $cgi->param('_ETH0_NETMASK');
my $eth1_ip = $cgi->param('_ETH1_IP');
my $eth1_netmask = $cgi->param('_ETH1_NETMASK');

if($cgi->param('apply')
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
    && $eth0_ip=~/^((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-
5]|2[0-4][0-9]|[01]?[0-9][0-9]?))*$/
    && $eth0_netmask=~/^((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-
9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))*$/
    && $eth1_ip=~/^((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-
5]|2[0-4][0-9]|[01]?[0-9][0-9]?))*$/
    && $eth1_netmask=~/^((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-
9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))*$/) {

    print $cgi->header();
    print <<"END";

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US" xml:lang="en-US">
    <head>
        <title>Untitled Document</title>
    </head>
    <body>
        <h1>Network</h1>
        <p>Settings successfull applied!</p>
        <a href="network.cgi">Back</a>
    </body>
</html>
END

    &writeConfig;
    system("sudo /usr/share/filebox/script/confgen.sh /var/www/mgmt/network.conf
/usr/share/filebox/config/network/ifcfg-eth0.tmpl /etc/sysconfig/network-
scripts/ifcfg-eth0");
    system("sudo /usr/share/filebox/script/confgen.sh /var/www/mgmt/network.conf
/usr/share/filebox/config/network/ifcfg-eth0.tmpl /etc/sysconfig/network-
scripts/ifcfg-eth1");
    #system("sudo service network restart");

} else {
    my %config;
    &readConfig("network.conf", \%config);
    print $cgi->header();
    print <<"END";
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US" xml:lang="en-US">
    <head>
        <title>FileBox Management - Network</title>
    </head>
    <body>
        <h1>Network</h1>
        <form method="post" action="network.cgi" enctype="multipart/form-data" >
            <fildset>
                <legend>Basic</legend>
                <table border="0">
                    <colgroup>
                        <col width="200" />
                        <col />
                    </colgroup>
                    <tr>
                        <td>Hostname:</td>
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
                        <td><input type="text" name="_HOSTNAME"
value="$config{"HOSTNAME"}" /></td>
                    </tr>
                    <tr>
                        <td>Default Gateway:</td>
                        <td><input type="text" name="_GW" value="$config{"GW"}"
/></td>
                    </tr>
                    <tr>
                        <td>DNS 1:</td>
                        <td><input type="text" name="_DNS1"
value="$config{"DNS1"}" /></td>
                    </tr>
                    <tr>
                        <td>DNS 2:</td>
                        <td><input type="text" name="_DNS2"
value="$config{"DNS2"}" /></td>
                    </tr>
                    <tr>
                        <td>DNS 3:</td>
                        <td><input type="text" name="_DNS3"
value="$config{"DNS3"}" /></td>
                    </tr>
                </table>
            </fieldset>
            <br />
            <fildset>
                <legend>Internet Facing Interface (eth0)</legend>
                <table border="0">
                    <colgroup>
                        <col width="200" />
                        <col />
                    </colgroup>
                    <tr>
                        <td>IP Adress:</td>
                        <td><input type="text" name="_ETH0_IP"
value="$config{"ETH0_IP"}" /></td>
                    </tr>
                    <tr>
                        <td>Netmask:</td>
                        <td><input type="text" name="_ETH0_NETMASK"
value="$config{"ETH0_NETMASK"}" /></td>
                    </tr>
                </table>
            </fieldset>
            <br />
            <fildset>
                <legend>Management Interface (eth1)</legend>
                <table border="0">
                    <colgroup>
                        <col width="200" />
                        <col />
                    </colgroup>
                    <tr>
                        <td>IP Adress:</td>
                        <td><input type="text" name="_ETH1_IP"
value="$config{"ETH1_IP"}" /></td>
                    </tr>
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
                    <tr>
                        <td>Netmask:</td>
                        <td><input type="text" name="_ETH1_NETMASK"
value="$config{"ETH1_NETMASK"}" /></td>
                    </tr>
                </table>
            </fieldset>
            <br />
            <input type="submit" name="apply" value="Apply" />
        </form>
        <br />
        <br />
        <br />
        <a href="index.html">Back</a>
    </body>
</html>
END
}

sub writeConfig() {
    open(CONFIG, ">network.conf");
    print CONFIG "HOSTNAME=",$cgi->param('_HOSTNAME'),"\n",
        "GW=",$cgi->param('_GW'),"\n",
        "DNS1=",$cgi->param('_DNS1'),"\n",
        "DNS2=",$cgi->param('_DNS2'),"\n",
        "DNS3=",$cgi->param('_DNS3'),"\n",
        "ETH0_IP=",$cgi->param('_ETH0_IP'),"\n",
        "ETH0_NETMASK=",$cgi->param('_ETH0_NETMASK'),"\n",
        "ETH1_IP=",$cgi->param('_ETH1_IP'),"\n",
        "ETH1_NETMASK=",$cgi->param('_ETH1_NETMASK'),"\n";
    close(CONFIG);
}

sub readConfig {
    my $config_line;
    my $name;
    my $value;
    my $config;
    my $filename;

    ($filename, $config) = @_;

    if (!open (CONFIG, "$filename")) {
        print "ERROR: Config file not found : $filename\n";
        exit(0);
    }

    foreach (<CONFIG>) {
        $config_line=$_;
        chop ($config_line);                                    # Get rid of
the trailling \n
        $config_line =~ s/^\s*//;                               # Remove
spaces at the start of the line
        $config_line =~ s/\s*$//;                               # Remove
spaces at the end of the line
        if ( ($config_line !~ /^#/) && ($config_line ne "") ) {     # Ignore
lines starting with # and blank lines
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
            ($name, $value) = split (/=/, $config_line);            # Split each
line into name value pairs
            $$config{$name} = $value;                               # Create a
hash of the name value pairs
        }
    }

    close(CONFIG);
}
```

system.cgi

```
#!/usr/bin/perl -w

use strict;
use CGI;

my $cgi = new CGI;
my $method="POST";
my $action=$cgi->url(-relative=>1);
my $encoding="";

if($cgi->param('reboot')) {
    &rebootServer;
} elsif($cgi->param('shutdown')) {
    &shutdownServer;
} else {
    print $cgi->header(),
        $cgi->start_html(),
        $cgi->h1("System"),
        "\n";

    print $cgi->start_form($method,$action,$encoding),
        $cgi->submit(-name=>'reboot',-value=>'Reboot'),
        "<br />",
        $cgi->submit(-name=>'shutdown',-value=>'Shutdown');
    print $cgi->end_form();

    print "<br />",
        "<br />",
        $cgi->a({-href=>'index.html'},"Back");

    print $cgi->end_html();
}

sub rebootServer() {
    system("sudo shutdown -r now");
}

sub shutdownServer() {
    system("sudo shutdown -h now");
}
```

15.8.3 FileBoxRepo-Servlet

Mirror.java:

```
package ch.csnc.filebox.mirror;

import java.io.IOException;
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
import java.io.PrintWriter;

import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

/**
 * Servlet implementation class Mirror
 */
public class Mirror extends HttpServlet {
	private static final long serialVersionUID = 1L;
	private RepoUrlBuilder rub;

	/**
	 * Default constructor.
	 */
	public Mirror() {
		rub = new RepoUrlBuilder();
	}

	/**
	 * @see HttpServlet#doGet(HttpServletRequest request, HttpServletResponse
	 *      response)
	 */
	protected void doGet(HttpServletRequest request,
			HttpServletResponse response) throws ServletException,
IOException {
		PrintWriter out = response.getWriter();

		String licenseKey = (String) request.getParameter("key");
		String releasever = (String) request.getParameter("releasever");
		String basearch = (String) request.getParameter("basearch");
		String repo = (String) request.getParameter("repo");

		response.setContentType("text/plain");

		out.print(rub.buildUrl(releasever, basearch, repo, licenseKey));

		out.close();
	}
}
```

RepoUrlBuilder.java

```
package ch.csnc.filebox.mirror;

import java.util.Iterator;
import java.util.ResourceBundle;
import java.util.StringTokenizer;
import java.util.Vector;

public class RepoUrlBuilder {
	private Vector<String> architectures;
	private Vector<String> repos;
	private Vector<Release> releases;
	private LicenseValidator lv;
	private ResourceBundle res;
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
	public RepoUrlBuilder() {
		res = ResourceBundle.getBundle("ch.csnc.filebox.mirror.Mirror");
		lv = new LicenseValidator();
		releases = new Vector<Release>();

		StringTokenizer stVersions = new StringTokenizer(res
				.getString("osVersions"), ";");
		StringTokenizer stMapping;
		while (stVersions.hasMoreTokens()) {
			stMapping = new StringTokenizer(stVersions.nextToken(), "-
>");
			releases.add(new Release(stMapping.nextToken(), stMapping
					.nextToken()));
		}

		StringTokenizer stArchitectures = new StringTokenizer(res
				.getString("osArchs"), ";");
		architectures = new Vector<String>();
		while (stArchitectures.hasMoreTokens()) {
			architectures.add(stArchitectures.nextToken());
		}

		StringTokenizer stRepos = new StringTokenizer(res
				.getString("repoTypes"), ";");
		repos = new Vector<String>();
		while (stRepos.hasMoreTokens()) {
			repos.add(stRepos.nextToken());
		}
	}

	public String buildUrl(String osVersion, String osArch, String repo,
			String licenseKey) {

		String url = new String(res.getString("baseURL"));
		int release = lv.validate(licenseKey);

		Iterator<Release> it = releases.iterator();
		boolean osOk = false;
		while (it.hasNext()) {
			Release r = it.next();
			if (r.getMajor().equals(osVersion)) {
				url += r.getMinor();
				osOk = true;
			}
		}

		if(!osOk){
			return "Unknown release version. Allowed: " +
releasesToLine(releases);
		}

		switch (release) {
		// invalid license
		case 0: {
			return "Invalid license key!";
		}
			// unstable
		case 1: {
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
                        url += "/unstable";
                        break;
                }
                        // RC
                case 2: {
                        url += "/rc";
                        break;
                }
                        // stable
                case 3: {
                        url += "/stable";
                        break;
                }
                }

                if (repos.contains(repo)) {
                        url += "/" + repo;
                } else {
                        return "Unknown repository type. Allowed: " +
vectorToLine(repos);
                }

                if (architectures.contains(osArch)) {
                        url += "/" + osArch + "/";
                } else {
                        return "Unknown architecture. Allowed: "
                                        + (architectures);
                }

                return url;
        }

        private String vectorToLine(Vector<String> input) {
                String line = new String();

                Iterator<String> it = input.iterator();
                while (it.hasNext()) {
                        line += it.next() + " ";
                }

                line = line.trim();

                return line;
        }

        private String releasesToLine(Vector<Release> input) {
                String line = new String();

                Iterator<Release> it = input.iterator();
                while(it.hasNext()) {
                        line += it.next().getMajor() + " ";
                }

                line = line.trim();

                return line;
        }
}
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Release.java

```
package ch.csnc.filebox.mirror;

public class Release {
	public static int UNSTABLE = 1;
	public static int RC = 2;
	public static int STABLE = 3;

	private String major;
	private String minor;

	public Release(String major, String minor) {
		super();
		this.major = major;
		this.minor = minor;
	}

	public String getMajor() {
		return major;
	}

	public void setMajor(String major) {
		this.major = major;
	}

	public String getMinor() {
		return minor;
	}

	public void setMinor(String minor) {
		this.minor = minor;
	}

	public String toString() {
		return major;
	}
}
```

LicenseValidator.java

```
package ch.csnc.filebox.mirror;

import java.util.Iterator;
import java.util.ResourceBundle;
import java.util.StringTokenizer;
import java.util.Vector;

public class LicenseValidator {
	private Vector<License> licenses;
	private ResourceBundle res;

	public LicenseValidator() {
		licenses = new Vector<License>();

		res = ResourceBundle.getBundle("ch.csnc.filebox.mirror.Mirror");
		StringTokenizer stLicenses = new StringTokenizer(res
				.getString("licenseMapping"), ";");
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
		StringTokenizer stMapping;

		while (stLicenses.hasMoreTokens()) {
			stMapping = new StringTokenizer(stLicenses.nextToken(), "-
>");
			licenses.add(new License(stMapping.nextToken(), Integer
					.parseInt(stMapping.nextToken())));
		}
	}

	public int validate(String licenseKey) {
		Iterator<License> it = licenses.iterator();

		while (it.hasNext()) {
			License l = it.next();
			if (l.getLicenseKey().equals(licenseKey)) {
				return l.getRelease();
			}
		}
		return 0;
	}
}
```

License.java

```
package ch.csnc.filebox.mirror;

public class License {
	private int release;
	private String licenseKey;

	public License(String licenseKey, int release) {
		super();
		this.release = release;
		this.licenseKey = new String(licenseKey);
	}

	public int getRelease() {
		return release;
	}

	public void setRelease(int release) {
		this.release = release;
	}

	public String getLicenseKey() {
		return licenseKey;
	}

	public void setLicenseKey(String licenseKey) {
		this.licenseKey = licenseKey;
	}
}
```

Mirror.properties:

```
baseURL=http://mirror.csnc.ch/centos/
osVersions=4->4.8;5->5.4
osArchs=i386;x86_64
repoTypes=os;updates;addons;extras;centosplus;contrib;filebox
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

```
# 1->unstable, 2->RC, 3->stable
licenseMapping=111->1;222->2;333->3
```

15.9 Mitgelieferte CD

Die erarbeiteten Dokumente sind ebenfalls auf der mitgelieferten CD in elektronischer Form vorhanden.

```
+---01_Dokumentation
+---02_Projektmanagement
+---03_Sourcen
|   +---FileBoxRepo_Servlet
|   |   \---FileBoxRepo
|   |       +---.settings
|   |       +---res
|   |       |   \---ch
|   |       |       \---csnc
|   |       |           \---filebox
|   |       |               \---mirror
|   |       +---src
|   |       |   \---ch
|   |       |       \---csnc
|   |       |           \---filebox
|   |       |               \---mirror
|   |       \---WebContent
|   |           +---META-INF
|   |           \---WEB-INF
|   |               \---lib
|   +---Mgmt_Interface
|   +---RPM_Spezifikationen
|   \---YUM_Repository
+---04_Grafiken
|   +---Bootloader
|   +---FileBox_Icon
|   \---Visio
\---05_A0_Poster
```


Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch