

Domänencontroller in einer Schule

to be announced

2008

Inhaltsverzeichnis

1	Ausgangssituation	1
2	Projektplanung	2
2.1	Istanalyse	2
2.2	Sollkonzept	2
2.3	Entscheidungen	4
3	Lösungsmöglichkeiten	6
4	Angebotserstellung	8
4.1	Prüfung an Anforderungen	8
4.2	Angebote von Lieferanten	8
4.3	Angebot für den Kunden	9
4.4	Angebotsbesprechung	10
5	Durchführung	11
5.1	Vorkonfiguration im Betrieb	11
5.2	Aufbau beim Kunden	11
5.3	Training der Administratoren	12
6	Abschluß des Projektes	13
6.1	Systemabnahme und Übergabe	13
6.2	Rechnungsstellung	13
6.3	Projektstunden	14
6.4	Fazit	14
7	Anhang	15
7.1	Dokumente	15
7.1.1	Nicht in der Abschlußprojektdokumentation aufgeführte Dokumente . . .	15
7.1.2	Kenndaten	15
7.1.3	Hinweise	15
7.1.4	Bei Netzwerkproblemen	15
7.2	Serverkonfiguration	16
7.2.1	Der Domain- und Dateiserver	16
7.2.2	Die Firewall	18
7.3	Benutzerdokumentation	21
7.3.1	Zentrales Benutzerverwaltungsprogramm	21
7.3.2	Einstellungen am Kinderschutzfilter	21
7.3.3	Integration neuer Windowsrechner	22
7.3.4	Integration neuer Linuxrechner	22
7.3.5	Ausschnitt aus der dhcpd.conf Datei	22
8	Pflichtenheft	24
8.1	Unterzeichnende	24

8.2	Ziele	24
8.3	Hardwareausbau	24
8.4	Testanforderungen	24
9	Quellen	26
9.1	Quellenangaben	26

1 Ausgangssituation

Der Schule „KGS-Kleinstadt“ wurden 40 Computersysteme von folgendem Typ gespendet.

Tabelle 1.1: Rechnerdetails

Hersteller	Maxdata
Prozessortyp	Intel Pentium IV mit 1,6GHz Taktung
RAM	512 MB
Festplattenspeicher	20 GB
Betriebssystem	Keines
Monitor	Belinea 15,, TFT
Weitere Komponenten	Netzwerkkarte Soundkarte Tastatur Maus

Diese sollen in das bestehende Schulnetz eingegliedert und dieses dabei ausgebaut werden. Derzeit besuchen rund 1600 Schüler die Schule, welche als Ganztagschule eingerichtet ist. Das Lehrangebot umfasst alle Klassen und Schulformen von der Grundschule bis hin zum Abitur. Der Auftrag zum Aufbau und Einrichten der Rechner wurde von der Schule an mich vergeben, Ansprechpartner für mich sind: Herr Meenen, der Schulassistent, der auch die Administration des Schulnetzes zusammen mit Herrn Meints, dem Lehrer für Informatik, übernimmt. Weiterhin ist der Leiter der Schule, Herr Mars als Entscheider über die finanziellen Mittel ein wichtiger Ansprechpartner.

2 Projektplanung

2.1 Istanalyse

Herr Meenen stellte mir im Verlauf eines Gespräches und anschließender Begehung der Räumlichkeiten die benötigten Daten für die Istanalyse zur Verfügung.

Die KGS-Kleinstadt verfügt über einen Rechnerraum mit 20 Plätzen. Die Geräte sind identisch ausgestattet und verfügen über eine Internetverbindung, die über einen Router realisiert wird. Jeder Schüler benutzt die gleiche Kombination aus Benutzernamen und Passwort, um sich an den Computern anzumelden. Bei der Anmeldung verbindet sich der Rechner mit einem Dateiserver und richtet ein Netzlaufwerk ein. Auf diesem Netzlaufwerk befinden sich in nach den Lehrernamen benannten Verzeichnissen wiederum Unterverzeichnisse, welche nach den einzelnen Klassen benannt sind und darin Unterverzeichnisse, welche sich die Schüler selbst anlegen, um darin ihre jeweiligen Arbeitsergebnisse speichern zu können.

Da jeder Schüler sich mit dem gleichen Benutzernamen am Dateiserver anmeldet, kann auch jeder Schüler überall auf dem Dateiserver die Daten verändern. So kommt es täglich vor, dass die Ordner der Lehrkräfte, Klassen oder Schüler umbenannt oder gelöscht werden. Im schlimmsten Falle werden die Arbeitsergebnisse gefälscht und mit ungültigen Daten gefüllt.

Die Rechner selbst verfügen über eine Wächterkarte, die jegliche Änderungen am Dateisystem des Rechners unterbindet und den Rechner bei jedem Neustart in seinen Ursprungszustand zurückversetzt. Dies gilt auch für die auf dem Rechner installierten Virens Scanner. Der Virens Scanner muss bei jedem Neustart die aktuellen Virusdefinitionen aus dem Internet neu laden.

Der Internetrouter selbst bietet keine Kontrolle über die Inhalte, welche die Schüler sich im Internet ansehen oder auf die lokalen Rechner laden. So kommt es immer wieder vor, dass Schüler sich eindeutig pornographische Inhalte ansehen und ganze Computerspiele aus dem Internet herunterladen. Beides ist unerwünscht und sorgt im Fall des Spieleherunterladens auch dafür, dass die 2 MBit/s DSL Leitung der Schule schnell an ihre Grenzen stößt und anderen ein sinnvolles Arbeiten mit dem Internet unmöglich macht.

2.2 Sollkonzept

Nach dem Gespräch mit Herrn Meenen habe ich noch mit Herrn Meints, dem Lehrer für Informatik und Herrn Mars, dem Schulleiter gesprochen. In diesem Gespräch wurden der finanzielle Rahmen für den Kauf von Hard- und Software sowie die Wünsche der Schule an der Lösung besprochen.

Basierend auf diesen Informationen habe ich folgendes Sollkonzept entwickelt:

Das Problem mit dem Dateiserver wird durch das Einrichten einer Accountverwaltung gelöst. Jeder Schüler erhält danach einen eigenen Account, bestehend aus Benutzernamen und Passwort sowie einen eigenen Speicherbereich von 50 Megabyte Größe. Dieser Speicherbereich wird als Netzlaufwerk für den Schüler eingerichtet. Für Unterrichtsmaterial, welches die Lehrkräfte den Schülern zur Verfügung stellen wollen, wird ein weiteres Netzlaufwerk eingerichtet, auf dem die Schüler nur lesend Zugriff haben. Damit die Internetleitung besser ausgenutzt wird und Inhalte nicht vierzig mal gleichzeitig geladen werden, wird ein Proxy eingerichtet. Dieser ermöglicht auch eine Kontrolle über die aufgerufenen Inhalte und wird gleichzeitig auch zum

Überprüfen der ladenden Inhalte auf Viren genutzt.

Die bestehenden Rechner werden in die Accountverwaltung eingebunden, die Wächterkarten bleiben dabei aktiv. Durch das Einrichten des Proxys werden die Zeiten des Herunterladens der Virendefinitionsdateien so stark verkürzt, dass dieses System so bestehen bleibt. Beide Räume erhalten einen eigenen Netzwerkschwitch, welcher die Verbindung zum Accountserver und dem Internet ermöglicht.

Das weitere Vorgehen leitet sich aus dem Sollkonzept wie folgt ab:

1. Recherche der möglichen Lösungen
2. Wahl der zu installierenden Lösung nach Entscheidungstabelle
3. Wahl der Server und Drucker
4. Erstellung eines Angebotes
5. Annahme des Angebotes durch die Schule
6. Veranlassung des Netzwerkaufbaus
7. Aufbau der Server und Drucker
8. Installation der Serverbetriebssysteme
9. Einrichten des Accountservers
10. Einrichten der Webproxys
11. Einrichten der Inhaltsprüfungssoftware
12. Einrichten der Virens Scanner
13. Einrichten der Drucker
14. Veranlassung des Aufbaus der gespendeten Rechner
15. Einrichten der gespendeten Rechner
16. Einbinden der bestehenden Systeme in das Accountsystem
17. Test des Gesamtsystems
18. Erstellen der Benutzerdokumentation
19. Erstellen der Administrationsdokumentation
20. Inbetriebnahme und Übergabe der Systeme
21. Einweisen der Administratoren in das System

2.3 Entscheidungen

Es gibt schon fertige Softwarelösungen für die Problemstellung, welche unterschiedliche Stärken und Schwächen haben. Um eine eindeutige Entscheidung treffen zu können, welche Lösung an der KGS-Kleinstadt installiert wird, habe ich mit Herrn Meints, Herrn Mars und Herrn Meenen zusammen einen Katalog von Kriterien und deren Gewichtung angefertigt.

Tabelle 2.1: Entscheidungskriterien

Kriterium	Gewichtung	Erklärung
Preis:	2	10 Punkte Maximal, je ein Punkt pro angefangene Einhundert Euro Anschaffungskosten Abzug. Minimum 0 Punkte.
Dokumentation:	3	5 Punkte für mitgelieferte gedruckte Anleitung, 4 Punkte für als PDF verfügbare Installationsanleitung, 3 für Hilfestellungen in Form von Webforen des Herstellers, 2 für allgemeine Webforen, 0 für „googlen“ oder nicht verfügbare Dokumentation.
Support:	2	5 Punkte für kostenlosen technischen Support, 4 Punkte für begrenzten kostenlosen Support, 3 für ausschließlich kostenpflichtigen Support, 0 für keinen Support.
Verfügbarkeit von Verwaltungsprogrammen	5	5 Punkte für ein zentrales Verwaltungstool, 4 Punkte für verschiedene Verwaltungstools für unterschiedliche Bereiche, 3 Punkte für Verwaltungstools, die nur einen Dienst konfigurieren. 1 Punkt für eigene Konfiguration je Rechner, 0 Punkte für Verwaltung durch das händische Ändern von Konfigurationsdateien.
Verfügbarkeit:	1	5 Punkte für freies Herunterladen von Installationsimages, 4 Punkte für käuflich erwerbbar Installationsmedien, 3 Punkte für kostenpflichtiges Herunterladen von Installationsmedien.
Vorliebe der Schuladministratoren:	1	Dieser Punkt wurde eingeführt, um den Vorlieben des Schuladministrators, der die Lösung nach der Installation und Übergabe verwalten muss, Rechnung zu tragen. Maximale Punktzahl entspricht der Anzahl an vorgestellten Lösungen, minimale Punktzahl ist 1 für die am wenigsten favorisierte Lösung.

3 Lösungsmöglichkeiten

Es gibt unterschiedlichste vorgefertigte Server für Schulen, darunter Lösungen von Microsoft, aber auch Open Source Lösungen. Im Folgenden stelle ich die von mir geprüften Lösungen vor.

Windows Small Business Server

Der Windows Small Business Server ist speziell auf die Anforderungen von kleinen bis mittelständischen Unternehmen abgestimmt. Es werden Domänenverwaltung und Dateiserver zur Verfügung gestellt. Zudem noch Email und Datenbankserver. Für den Einsatz in der Schule spricht, dass er kompatibel zu dem bestehenden Netzwerk ist.

OSS

Der Open School Server ist hervorgegangen aus SuSE Linux 9.0 und bietet neben der Domänenverwaltung und Dateiserver alle weiteren unter Linux möglichen Serverdienste an.

Arktur

Der Arktur Schulserver ist ebenfalls aus SuSE Linux hervorgegangen und bietet die gleichen Dienste wie der OSS. Er wird von Lehrkräften gepflegt, die dieses in ihrer Freizeit unternehmen.

Skolelinux

Skolelinux ist ein aktiv gepflegter Schulserver, welcher aus dem Debianprojekt hervorgeht. Entwickelt wurde er in Norwegen, wird aber mittlerweile weltweit genutzt. Er bietet neben allen Diensten, die OSS und Arktur bringen auch den Vorteil einer einfachen Installation und Verwaltung.

Edubuntu

Edubuntu ist eine Installationsvariante von Ubuntu Linux. Es ist möglich, jeden Konfigurationswunsch für Schulen mit Edubuntu zu erfüllen, besonders hervorzuheben ist die Unterstützung für Thin-Client Systeme.

SLIXS

Solutions for Linux & XFREE in schools (SLIXS) ist eine in Österreich entwickelte Lösung für Schulen. Sie bietet nur die Domänenverwaltung und Dateiserver.

Ausgeschiedene Systeme

Der Arktur Schul Server ist in der Version 3.5 und 4.5 verfügbar. Die Webseite der Arkturverwalter weist auf die Versionsunterschiede hin. Beide Versionen werden gleichermaßen weiterentwickelt, basieren aber im Kern auf Suse 7.0 und sind zu lange nicht gepflegt werden, um noch als aktuell zu gelten. Aus diesem Grund wurde auch OSS schon von vornherein nicht in die Prüfung mit einbezogen, es basiert jedoch auch auf Suse 9.0.

Die einzelnen Werte für die Tabelle ergaben sich aus Internetrecherchen, mit Schwerpunkt auf Vorstellungen der einzelnen Produkte. Da diese an unterschiedlichen Tagen durchgeführt wurden, kam es zu einer Differenz bei SLIXS, welches in diesem Zeitraum ein Update erhielt. Dabei wurden die alten Dokumentationen von SLIXS nicht mehr verfügbar, die neuen waren

noch nicht eingestellt, wodurch die geringe erreichte Punktzahl von SLIXS zu erklären ist.

Tabelle 3.1: Die gewichtete Entscheidungstabelle

Produkt		SLIXS	Edubuntu	Skolelinux	Windows SBS
Kriterium	Gewichtung				
Preis	2	10	10	10	0
Dokumentation	3	0	3	4	5
Support	2	0	3	3	4
Verwaltungstools	5	0	1	5	5
Verfügbarkeit	1	0	5	5	4
Vorliebe	1	1	3	2	4
Summe		21	48	70	51

Nachdem die Ergebnisse klar waren und der Windows Small Business Server aus Kostengründen nicht mehr in Betracht gezogen werden konnte, wurde beschlossen, eine gemischte Lösung aufzubauen. Der Server sollte auf Basis von Skolelinux aufgebaut werden. Für die Firewall habe ich vorgeschlagen, Ubuntu Linux zu verwenden, da Herr Meenen diese Linuxvariante bereits kennt. Der Vorschlag wurde angenommen. Die gespendeten Rechner werden ebenso mit Skolelinux in der Clientvariante ausgerüstet, da dies den Konfigurationsaufwand minimiert. Die Möglichkeit, Windows anstelle von Linux auf den Clients zu installieren, wurde zwar diskutiert, aber aus reinen Kostengründen wieder verworfen.

4 Angebotserstellung

4.1 Prüfung an Anforderungen

Um ein Angebot erstellen zu können, habe ich zunächst geprüft, welche Hardwareausstattung mindestens nötig ist, um einen störungsfreien Betrieb zu ermöglichen und anschließend Angebote von verschiedenen Lieferanten eingeholt. Diese habe ich verglichen und das günstigste gewählt. Die wichtigste Kenngröße ist das Vorhandensein einer Netzwerkkarte im Dateiserver, die mindestens 1 Gbit/s Übertragungskapazität erreichen kann. Ich konnte feststellen, dass kein Server mehr vertrieben wird, der nicht mit einer solchen Netzwerkkarte ausgestattet ist. 1 Gbit/s Übertragungskapazität erlauben eine Übertragung von 125 Mbyte Daten pro Sekunde. Geteilt durch die 40 Clients sind das pro Client 3,125 Mbyte pro Sekunde, wenn jeder Client gleichzeitig Daten anfordert. Sollten alle Benutzer die maximale Größe ihres Profils ausnutzen und dieses beim Anmelden zum Client übertragen, so dauert diese Übertragung 16 Sekunden, wenn jeder Client gleichzeitig sein Profil anfordert.

4.2 Angebote von Lieferanten

Tabelle 4.1: Angebotsgrundlage

Zweck	Einheit	Hersteller	Preis (Euro) ohne MWSt
Domänencontroller und Dateiserver	Servertower mit Dualcoreprozessor @1,8 GHz 1024 MB RAM 3 Festplatten mit je 200GB Speicher und optischen Laufwerk	Pyramid	1161,00
		Bechtle	900,15
		Thomas Krenn	1396,10
Firewall	Servertower mit Singlecoreprozessor @1,8 GHz 512 MB RAM 1 Festplatte mit 160 GB Speicher und optischem Laufwerk	Pyramid	970,00
		Bechtle	606,20
		Thomas Krenn	697,70
Netzwerk Raumswitche	3 * 25 Port Switches mit 100 Mbit/Port und einem 1 Gbit Uplink Port	Reichelt	641,52
		Bechtle	587,70
		Thomas Krenn	890,40
Hauptverteiler	1 * 8 Port Switch jeder Port kann bis 1 Gbit übertragen	Reichelt	88,16
		Bechtle	81,80
		Thomas Krenn	249,80

Da alle Angebote technisch gleichwertig waren, habe ich den günstigsten Hersteller (Bechtle) gewählt, um auf diesen Preisen basierend mein Angebot zu erstellen, welches ich der Schule vorgelegt habe. Kostenaufschläge für Gemeinkosten und Gewinn wurden nicht in diese Dokumentation aufgenommen. Damit dennoch eine Berechnung sichtbar ist, habe ich dafür 30% vom Kaufpreis auf den Preis für den Kunden aufgeschlagen.

4.3 Angebot für den Kunden

Die wesentlichen Punkte des Angebotes waren:

Tabelle 4.2: Angebotstabelle

Zweck oder Dienstleistung	Einheit	Menge	Preis (Euro) ohne MWSt
Domänenkontroller und Dateiserver	Servertower mit Dualcoreprozessor @1,8 GHz 1024 MB RAM 3 Festplatten mit je 200GB Speicher und optischen Laufwerk	1	1170,16
Firewall	Servertower mit Singlecoreprozessor @1,8Ghz 512 MB RAM 1 Festplatte mit 160 GB Speicher und optischem Laufwerk	1	788,06
		Servergesamt:	1958,22
Netzwerk Raumswitche	25 Port Switch mit 100 Mbit/Port und einem 1 Gbit Uplink Port	3	254,67
Hauptverteiler	8 Port Switch jeder Port kann bis 1 Gbit übertragen	1	81,80
Kleinteile	Netzwerkdosen, Kabel, Stecker Pauschalpreis je Anschluss 25 Euro	50	25,00
		Netzwerkgesamt:	2095,80
	Gesamtpreis ohne Arbeitsstunden für Serverkonfiguration		4054,03
	+ Mehrwertsteuer 19%		770,27
	Gesamtpreis ohne Arbeitsstunden für Serverkonfiguration inkl. Mehrwertsteuer		4824,30

4.4 Angebotsbesprechung

Die Schule war der Ansicht, dass sie den Einbau der Netzwerkkomponenten in Eigenleistung günstiger erreichen könnte und bot an, uns den Auftrag zu übergeben, den Netzerkausbau allerdings selbst zu übernehmen. Ich habe Herrn Meenen, welcher den Einwand brachte und Herrn Mars darauf hingewiesen, dass die Übertragungsbandbreite von den Raumverteilern zum Hauptverteiler mindestens 1 GBit/s sein sollte, da durch die Menge der Clients das nötige Laden der Benutzerprofile sonst länger dauert. Meine Anmerkung wurde festgehalten, der entsprechende Posten wurde aus dem Angebot gestrichen und die Schule hat den Auftrag mit den entsprechenden Änderungen gestellt. Das Pflichtenheft dazu befindet sich in Auszügen im Anhang unter **Pflichtenheft**

5 Durchführung

5.1 Vorkonfiguration im Betrieb

Nachdem mir Herr Meenen mitgeteilt hatte, dass der Ausbau des Netzwerkes vor dem Ende stünde, habe ich die Hardware bestellt und nach Lieferung mit der Installation begonnen. Die Installation des Server gestaltete sich denkbar einfach, die exzellente Schritt-für-Schritt Anleitung des Skolelinuxprojektes befolgend war die Grundinstallation rasch beendet. Die Anpassungen für die Serverdienste nahmen danach aber die meiste Zeit in Anspruch. Anschließend habe ich die Firewall konfiguriert. Hier muss nur beachtet werden, dass einzig der Domänen- und Dateiserver Zugriff auf Internetdienste hat. Die entsprechende Vorgehensweise für beide Server ist im Anhang unter Punkt **Serverkonfiguration** zu finden.

5.2 Aufbau beim Kunden

Nachdem ich die Grundkonfiguration der Server beendet hatte, wurden sie ausgeliefert und beim Kunden aufgestellt.

Beim Kunden wurden dann die Drucker eingerichtet und an das Netzwerk angeschlossen. Die Drucker wurden beim Accountserver angemeldet, damit dieser die Zugriffe auf die Drucker verwalten kann. Es wurde auf dem Server eine Dateifreigabe eingerichtet, auf welche sämtliche Inhalte der Dateifreigabe des alten Servers kopiert wurden. Anschließend wurde der alte Dateiserver deaktiviert und vom Netz genommen. Nachdem die benötigte Infrastruktur eingerichtet war, konnten die Clientsysteme integriert werden. Zunächst wurden die gespendeten Rechner mit Hilfe der Installations-CDs eingerichtet. Dabei gingen Herr Meenen, Herr Meints und ich gemeinsam vor, wodurch Zeit gespart wurde. Wichtig bei diesem Schritt war, dass die MAC Adressen der Rechner festgehalten wurden. Bei jedem Rechner wurde der Drucker, welcher im selben Raum war, eingerichtet. Damit war die nötige Einrichtung für die Linuxrechner beendet, und die Windowsrechner wurden eingerichtet. Dies funktionierte nur in zwei getrennten Schritten, da dem Accountserver die MAC Adressen der Clients bekannt sein müssen.¹ Zunächst wurden die MAC Adressen der Windowsclients ausgelesen. Anschließend wurden alle MAC Adressen (Linux, Windows und Drucker) am Domänencontroller (Accountserver) mit Hilfe des grafischen „Iwat“ Tools eingetragen und per Texteditor in die Konfigurationsdatei des DHCP-Servers. Ein Auszug der Konfigurationsdatei befindet sich im Anhang unter **Ausschnitt aus der dhcpd.conf**.

Nachdem die MAC-Adressen eingetragen waren konnte der zweite Teil der Windowsclientintegration von Statten gehen. Zunächst wurden die Windowsrechner mit deaktivierter Wächterkarte neu gestartet. Anschließend wurden sie der Domäne beigefügt und der Drucker im Raum wurde über die Druckerfreigabe des Domänenkontrollers als Standarddrucker eingetragen. Die Virens Scanner auf den Rechnern wurden aktualisiert und sie wurden so eingestellt, dass sie nach einer Aktualisierung der Virendefinitionsdateien keinen vollständigen Systemscan mehr durchführen, wohl aber alle Dateien beim Öffnen und Schließen scannen. Auf jedem Rechner wurde der Benutzer „Raum412“ als automatisch angemeldeter Benutzer eingerichtet. Damit

¹ Dies ist nicht analog zur Einrichtung der Linuxclients, da diese Besonderheit dort nicht auftritt.

wird über den Zeitraum von den Osterferien bis zu den Sommerferien die Kompatibilität zum alten Verhalten bewahrt. Gleichzeitig gibt es Herrn Meenen Zeit, um die nötigen Accounts für die Schüler zu erstellen und es gibt keinen Bruch in der Nutzung der Rechnern im aktuellen Schuljahr. Mit Beginn des neuen Schuljahres soll dieses Verhalten wieder deaktiviert werden. Zum Schluß wurden alle Einstellungen gesichert und die Wächterkarten wieder aktiviert. Anschließend wurden die ersten Accounts eingerichtet. Das Vorgehen dazu ist im Anhang unter dem Punkt **Accounteinrichtung** beschrieben.

5.3 Training der Administratoren

Das Training für Herrn Meenen und Herrn Meints fand in den neu eingerichteten Räumen statt. Inhalte waren die Einrichtung neuer Clients, die Einrichtung von neuen Druckern und neuen Accounts, unterschiede zwischen Nutzergruppen und deren Einrichtung. Die Konfiguration des Inhaltsfilters und der Firewall wurden zum Abschluß des Trainings gezeigt.

6 Abschluß des Projektes

6.1 Systemabnahme und Übergabe

Die Einhaltung der Anforderungen wurde geprüft, indem von je einem Windows- und einem Linuxclient aus die Anmeldung mit verschiedenen Benutzeraccounts getestet wurde, das Sperren des Internetzugangs getestet wurde und die Funktionalität der Virens Scanner getestet wurde. Zur Prüfung der Virens Scanner wurden die Testdateien von EICAR (<http://www.eicar.org>) herangezogen, die Prüfung des Inhaltsfilters wurde geprüft in dem die Webseiten <http://www.youporn.com> <http://www.playboy.com> aufgerufen wurden. Die Prüfung galt als erfolgreich, wenn die Seiten gesperrt waren.

Die korrekte Einrichtung der Drucker wurde geprüft, indem von jedem Raum aus je ein Druckauftrag an den Raumdrucker gesendet wurde, und je ein Druckauftrag an fremde Drucker. Letztere sollten abgewiesen werden, erstere mussten erfolgreich sein.

6.2 Rechnungsstellung

Da Unternehmensinterna nicht in dieser Dokumentation veröffentlicht werden sollen, werden auch hier Gemeinkostenaufschläge auf die Arbeitsstunden nicht ausgewiesen. Ausgegangen wird von folgenden Kenngrößen:

Kosten für Auszubildenden je Stunde Arbeitszeit betriebsintern: 17,00 Euro

Kosten für Auszubildenden je Stunde Arbeitszeit betriebsextern: 35,00 Euro

Für die Einrichtung der Server, die im Betrieb und nicht beim Kunden vorgenommen wurde, wird eine Pauschale von 200 Euro je Server berechnet. Für Planungsarbeiten wird dem Kunden eine Arbeitsstunde berechnet, für die Erstellung der Dokumentation 2 Stunden. Restliche Arbeitsstunden sind für den Kunden prüfbar beim Kunden vor Ort entstanden.

Tabelle 6.1: Rechnungsgrundlage

Position	Bezeichnung	Menge	Preis (Euro)
1	Server für Domänenkontroller	1	1170,16
2	Server für Firewall	1	788,06
3	Einrichtung von Servern	2	200,00
6	Arbeitsstunden (Azubi)	17	35,00
	Gesamtpreis ohne MwSt		2954,22
	+ MwSt 19%		561,11
	Endpreis		3514,33

6.3 Projektstunden

Es wurden 17 Stunden beim Kunden verbracht, die restlichen 18 Stunden des Projektes teilen sich auf in 10 Stunden für die Servereinrichtung, welches somit eine Stunde länger dauerte als ursprünglich geplant. Dafür konnte ich die Benutzerdokumentation innerhalb von 2 Stunden statt der geplanten 3 Stunden erstellen. Die restlichen 6 Stunden wurden für Istanalyse, Soll-konzept, Hardwarebedarfsberechnung, Anforderung der Angebote und die Angebotserstellung benötigt.

6.4 Fazit

Im Verlauf des Projektes konnte ich zeigen, dass eine Lösung eines Problems mit Open Source Mitteln möglich ist, zum Preis des geringfügig erhöhten Aufwandes bei der Einrichtung. Um eine einheitlichere Anwendung für die Benutzer zu ermöglichen, wäre es meiner Meinung nach besser gewesen, alle Clients mit Windows einzurichten, was aber aus Kostengründen nicht möglich war. Der Mischbetrieb von Linux und Windows im Anwenderbereich, wie er hier gezeigt ist, wird zwar durch Nutzen von den selben Anwendungsprogrammen wie z.B. OpenOffice als Office-Lösung auf beiden Plattformen ermöglicht. Jedoch erfordert dieser Ansatz ein Erlernen des Umgangs mit beiden Systemen, welches für die Lehrkräfte vermutlich als nachteilig empfunden wird. Gleichzeitig ist dieser Punkt ein Vorteil für die Schüler, da sie so eine Qualifikation für beide Systeme erhalten und, wenn die derzeitigen Prognosen von vermehrtem Einsatz von Linux in der Arbeitswelt sich als korrekt erweisen, einen Vorteil bei der späteren Berufswahl haben.

7 Anhang

Im Anhang befindet sich die Betriebsdokumentation und die Benutzerdokumentation. Die Betriebsdokumentation setzt sich dabei aus allen Teilen des Anhangs zusammen, die Benutzerdokumentation nur aus dem **Benutzerdokumentation** genannten Teil.

7.1 Dokumente

7.1.1 Nicht in der Abschlußprojektdokumentation aufgeführte Dokumente

Es wurden Dokumente aus der Abschlussprojektdokumentation bewusst ausgelassen. Das sind die Kopien der Rechnungen der Lieferer und die Kopien der Rechnungen für die Schule. Mir ist bewusst, dass diese Dokumente in einer Betriebsdokumentation Eingang finden, aber sie sind nicht für die Öffentlichkeit bestimmt.

7.1.2 Kenndaten

Administrationspasswörter aller Systeme während der Installation:

Benutzer root 1Ron5T0rm

lwat user: admin

lwat password: 1Ron5T0rm

Es wurde den Administratoren der Schule mitgeteilt, dass diese Passwörter zu ändern sind. Es wurde ein weiterer Account für uns eingerichtet, über den wir Servicearbeiten durchführen können:

Benutzer: HelpData

Passwort: 1492-KliA

7.1.3 Hinweise

Achtung, die Konfiguration der Virens Scanner ist genau wie beschrieben durchzuführen, insbesondere auf dem Firewallrechner! Andere Vorgehensweisen, mögen sie auch richtig erscheinen, führen nicht zum gewünschten Ergebnis.

7.1.4 Bei Netzwerkproblemen

Der Kunde hat die Netzwerkkonfiguration selbst übernommen, Probleme mit der Netzwerkhardware und den Leitungen sind nicht in unserer Gewährleistung!

7.2 Serverkonfiguration

7.2.1 Der Domain- und Dateiserver

Der Domänencontroller wurde nach der Standartinstallation wie folgt angepasst:

Anpassungen am Dateiserver

Damit der Dateiserver „SAMBA“ Dateien auf Viren prüfen kann, muss das entsprechende Modul aktiviert werden. Wie später bei der Firewall selbst, wird auch auf dem Dateiserver der ClamAV Virens scanner diesen Dienst übernehmen. Das Modul „vscan-clamd“ muss konfiguriert werden. Dies geschieht zum einen in der Konfigurationsdatei von „SAMBA“ in „/etc/samba/smb.conf“ sowie die Konfiguration des Scanmoduls selbst in „/etc/samba/vscan-clamav.conf“. In der smb.conf wird festgelegt, welche Freigaben gescannt werden, in der vscan-clamav.conf wird festgelegt, wie gescannt wird. Die Anpassungen in der smb.conf ist hier beispielhaft eingetragen:

```
[Name der Freigabe]
vfs objects = vscan-clamav
vscan-clamav: config-file = /etc/samba/vscan-clamav.conf
Es folgen die üblichen SAMBA-Optionen für die Freigabe
```

Es folgt der gesamte Inhalt der Datei /etc/samba/vscan-clamd.conf:

```
#
# /etc/samba/vscan-clamav.conf
#

[samba-vscan]
; run-time configuration for vscan-samba using
; clamd
; all options are set to default values

; do not scan files larger than X bytes. If set to 0 (default),
; this feature is disabled (i.e. all files are scanned)
max file size = 0

; log all file access (yes/no). If set to yes, every access will
; be logged. If set to no (default), only access to infected files
; will be logged
verbose file logging = no

; if set to yes (default), a file will be scanned while opening
scan on open = yes
; if set to yes, a file will be scanned while closing (default is yes)
scan on close = yes

; if communication to clamd fails, should access to file be denied?
; (default: yes)
deny access on error = no
```

```

; if daemon failes with a minor error (corruption, etc.),
; should access to file denied?
; (default: yes)
deny access on minor error = no

; send a warning message via Windows Messenger service
; when virus is found?
; (default: yes)
send warning message = yes

; what to do with an infected file
; quarantine: try to move to quarantine directory
; delete: delete infected file
; nothing: do nothing (default)
infected file action = quarantine

; where to put infected files - you really want to change this!
quarantine directory = /opt/clamav/quarantine
; prefix for files in quarantine
quarantine prefix = vir-

; as Windows tries to open a file multiple time in a (very) short time
; of period, samba-vscan use a last recently used file mechanism to avoid
; multiple scans of a file. This setting specified the maximum number of
; elements of the last recently used file list. (default: 100)
max lru files entries = 100

; an entry is invalidad after lru file entry lifetime (in seconds).
; (Default: 5)
lru file entry lifetime = 5

; exclude files from being scanned based on the MIME-type! Semi-colon
; seperated list (default: empty list). Use this with care!
exclude file types =

; socket name of clamd (default: /var/run/clamd). Setting will be ignored if
; libclamav is used
clamd socket name = /tmp/clamd

; limits, if vscan-clamav was build for using the clamav library (libclamav)
; instead of clamd

; maximum number of files in archive (default: 1000)
libclamav max files in archive = 1000

; maximum archived file size, in bytes (default: 10 MB)
libclamav max archived file size = 5242880

; maximum recursion level (default: 5)
libclamav max recursion level = 5

```

Änderungen am auf dem Domänencontroller installierten SQUID Proxy

Üblicherweise wird beim Skolelinux-Konzept davon ausgegangen, dass der Hauptserver auch als Firewall tätig ist. Da die Virenkontrolle des Internetverkehrs und die Prüfung auf unerwünschte Inhalte den Server stark belasten, wurde diese Funktion auf eine externe Firewall ausgegliedert. Um den Konfigurationsaufwand für den Kunden gering zu halten, wurde der auf dem Hauptserver installierte Squid Proxy, den alle Clients als Proxyserver zugewiesen bekommen, über die `neighbor-cache-peer` Option umgestellt. Der Squid Proxy des Domänencontrollers greift nun über den Squid Proxy der Firewall auf das Internet zu. Der Weg ist dabei folgender:

Squid (Firewall) <-> Dansguardian Kinderschutz <-> HAVP Virenschanner <-> Squid (Hauptserver)

Dazu wurde in der Datei `/etc/squid/squid.conf` folgende Zeile hinzugefügt:

```
cache_peer 10.0.1.1 parent 3128 default, no-delay
```

Weitere Änderungen am Server waren nicht nötig.

7.2.2 Die Firewall

Auf dem Firewallcomputer wird ein Webproxy (Squid), ein Kinderschutzproxy (Dansguardian) und ein Virenschanner für Webseiten (HAVP) installiert.

Vorbereitungen

Damit HAVP installiert werden kann, muss die „Mandatory Access“ Option für das Dateisystem aktiviert werden. Die Option erlaubt es, Zugriffe auf Dateien nur für bestimmte Programme zuzulassen. HAVP stellt so sicher, dass nur der Virenschanner auf die zu scannenden Daten zugreifen kann.

In Datei `/etc/fstab`

Ändern der Zeile:

```
UUID=[...] / defaults,errors=remount-ro 0
```

in:

```
UUID=[...] / defaults,mand,errors=remonut-ro 0
```

Als Verzeichnis für temporäre Dateien für HAVP wird `/havtmp` angelegt:

```
mkdir /havtmp
```

Als Verzeichnis für aktuell gescannte Dateien wird `/havp` angelegt:

```
mkdir /havp
```

Man kann entweder den Rechner neu starten oder mit dem Befehl: `mount / -o remount` erreichen, dass die neuen Optionen für das Dateisystem geladen werden.

Installation der Firewallsoftware

Zuerst: *ClamAV*

```
apt-get install clamd clamav-dev freshclam clamd-daemon
```

Dann *Squid*

```
apt-get install squid
```

Dann *dansguardian*

```
apt-get install dansguardian
```

Dann *havp*

```
apt-get install havp
```

Konfiguration der Firewallsoftware

Damit der HAVP funktioniert, muss der Virenschanner CLAMAV auf Betrieb am Netzwerksocket eingestellt werden. Dazu ändert man die Datei `/etc/clamd/clamd.conf` wie folgt ab:

```
LocalSocket /var/run/clamd/clamdctl
In:
# LocalSocket /var/run/clamd/clamdctl
#AllowSupplementaryGroups no
In
AllowSupplementaryGroups yes
Und
# TCPSocket 3310
In
TCPSocket 3310
```

Anschließend startet man clamav neu: `/etc/init.d/clamav-daemon restart`

Der Squid Webproxy ist schon von sich aus so eingestellt, dass er nur Verbindungen vom Rechner entgegennimmt, auf dem er installiert ist. Diese Einstellungen werden beibehalten. Dansguardian muss so eingestellt werden, dass die Software auf einem anderen als den Standardnetzwerkport lauscht. Dazu muss die Datei `/etc/dansguardian/dansguardian.conf` wie folgt geändert werden:

```
Filterip =
In
Filterip = 127.0.0.1
Und
Filterport = 8080
In
Filterport = 8282
```

Zum Schluss kann HAVP konfiguriert werden. Dazu muss man die Datei `/etc/havp/havp.config` wie folgt geändert werden:

```
# DAEMON false
In
DAEMON true
# TEMPDIR /var/run/havp
In
TEMPDIR /havptmp
PARENTPORT 3128
In
PARENTPORT 8282
ENABLECLAMLIB true
In
ENABLECLAMLIB false
ENABLECLAMD false
In
ENABLECLAMD true
CLAMDSOCKET /tmp/clamd
In
#CLAMDSOCKET
Die Zeilen: # CLAMDSERVER
# CLAMDPOR
In
```

```
CLAMDSERVER 127.0.0.1
CLAMPDPORT 3310
```

Nachdem die Software konfiguriert ist, muss noch der Benutzer havp der Gruppe clamav und der Benutzer clamav der Gruppe havp hinzugefügt werden.

```
addgroup havp clamav
addgroup clamav havp
```

Die Verzeichnisse `/havp` und `/havptmp` müssen dem Benutzer havp gehören:

```
chown havp /havp
chown havp /havptmp
```

Jetzt können die Dienste neu gestartet werden:

```
/etc/init.d/squid restart
/etc/init.d/havp restart
/etc/init.d/dansguardian restart
```

Die Dienste sind nun eingerichtet.

Das Firewallskript findet sich unter `/etc/network/firewall.sh`. Es ist eine übliche IPtables Konfiguration und erlaubt ausgehenden Verkehr nur vom Accountserver aus. Andere Versuche vom internen Netz der Schule auf das Internet zuzugreifen werden abgewiesen. Vom Internet aus wird die Firewall als Statefull Inspection Firewall betrieben, welche neue Verbindungen nur vom Netz der Schule aus ins Internet zulässt, nicht umgekehrt.

7.3 Benutzerdokumentation

Dieses Dokument dient dazu, Sie bei der Pflege des Datenbestandes und der Server zu unterstützen. Es ist als Ergänzung zur Dokumentation von Skolelinux und Ubuntu gemacht, die Sie stets aktualisiert im Internet finden:

Tabelle 7.1: Hilfsurls

System	Adresse (URL)	Sprache
Skolelinux	http://wiki.debian.org/DebianEdu/Documentation/Etch	Englisch
	http://maintainer.skolelinux.no/debian-edu-doc/de/release-manual.html	Deutsch
Ubuntu	https://help.ubuntu.com/	Englisch
	https://wiki.ubuntu.com/GermanDocumentation	Deutsch

7.3.1 Zentrales Benutzerverwaltungsprogramm

Das zentrale Benutzerverwaltungsprogramm kann vom Server aus über die Desktopverknüpfung `/textit/wat` erreicht werden und von allen anderen Arbeitsplätzen aus mit dem Webbrowser über den Link: <https://www/wat:999>. Damit man das Programm benutzen kann, muss man sich dort mit seinem Benutzernamen und Passwort anmelden. Je nach Berechtigung können anschließend Änderungen vorgenommen werden. Die höchsten Berechtigungen hat der Benutzer **admin**, danach Benutzer der Gruppe **jr-admins**, welche Benutzer anlegen und verwalten können.

7.3.2 Einstellungen am Kinderschutzfilter

Die Dansguardian Filtersoftware wird über mehrere Dateien konfiguriert. Jede Datei befindet sich im Verzeichnis `/etc/dansguardian` auf dem Firewallrechner. Jede Datei bringt eine eigene

Erklärung mit. Dateien, die mit dem Kürzel *banned* beginnen, definieren dabei eindeutig nicht erlaubte Inhalte, Dateien die mit *exception* beginnen definieren eindeutig erlaubte Inhalte.

Inhalte, welche die gewichtete Prüfung durchlaufen, werden im Stammverzeichnis `/etc/dansguardian/phraselists` und dann in je nach Bereich bezeichneten Unterverzeichnissen definiert. Ab welchen Gewichtungen der Zugang zu den gewünschten Inhalten gesperrt wird legt die Datei `/etc/dansguardian/dansguardianf1.conf` festgelegt. Insbesondere ist dabei auf den Eintrag `naughtynesslimit = ...` zu achten. Jede gefundene unerwünschte Phrase erhöht einen Zähler und sollte dieser Zähler den Wert dieser Variable überschreiten, wird die Seite nicht angezeigt.

Zwei weitere Einstellungsmöglichkeiten sind gerade zum Einrichten des Filters nützlich: `bypass = 1` sorgt dafür, das auf der Meldungsseite, ein Link auf die gesperrte Seite angeboten wird, welcher nach Eingabe des Passwortes welches mit `bypasskey=Passwort` definiert wird, den Zugang zur gesperrten Seite erlaubt.

7.3.3 Integration neuer Windowsrechner

Um neue Rechner mit dem Windowsbetriebssystemen in das Schulnetz zu integrieren, muss die MAC Adresse der Netzwerkkarte des neuen Rechners mit dem „Iwat“ Programm am Server eingetragen werden, damit dieser Rechner sich an der Domäne anmelden kann. Zudem muss die MAC Adresse auch in die Datei `/etc/dhcp/dhcpd.conf` eingetragen werden. Anschließend kann der Rechner am Netzwerk angeschlossen und gestartet werden. Nach dem Start des Rechners muss er an der Domäne Skole angemeldet werden. Sie werden dazu nach einem Benutzernamen und Passwort gefragt, welcher die Berechtigung hat, neue Rechner der Domäne hinzuzufügen. Dieser Benutzername ist **root**. Sie müssen die Anmeldung zwei Mal durchführen. Beim ersten Mal wird sie zwingend fehlschlagen, da der Server erst nach diesem Schritt dem neuen Rechner eine interne Identitätsnummer zuweisen konnte. Beim zweiten Versuch wird der Rechner in die Domäne aufgenommen. Nach einem Neustart des Rechners können alle Benutzer der Domäne sich an diesem Rechner anmelden.

7.3.4 Integration neuer Linuxrechner

Um neue Rechner mit dem Betriebssystem Linux in das Schulnetz zu integrieren müssen sie die MAC Adresse der Netzwerkkarte des Linuxclients mit dem „Iwat“ Programm am Server eintragen. Zudem müssen sie die MAC Adresse in der Datei `/etc/dhcp/dhcpd.conf` eintragen. Anschließend benutzen Sie die Skolelinux Installations-CD, um ein fertig vorkonfiguriertes Linux auf dem Rechner zu installieren. Wählen Sie als zu installierendes Profil „Workstation“ aus. Sobald die Installation fertig ist und der Rechner am Netzwerk angeschlossen ist, können sich Benutzer mit ihrem Benutzernamen und Passwort an dem Rechner anmelden und arbeiten. Vergessen Sie nicht, die CD wieder aus dem Laufwerk zu entfernen!

7.3.5 Ausschnitt aus der dhcpd.conf Datei

Alle Rechner haben einen eigenen Eintrag in der `dhcpd.conf` Datei. Ein Eintrag ist wie folgt aufgebaut:

```
host static00 {  
hardware ethernet 00:00:00:00:00:00;  
fixed-address 10.0.0.0;  
}
```

static00 steht dabei für den zu vergebenen Hostnamen.
00:00:00:00:00:00 Ist der Platzhalter für die MAC Adresse des Hosts.
10.0.0.0 ist der Platzhalter für die zu vegebene IP-Adresse, hier muss die entsprechende IP-Adresse welche der Host erhalten soll eingetragen werden.

8 Pflichtenheft

Es wird der Inhalt des Pflichtenheftes wiedergegeben, es ist keine Kopie des Pflichtenheftes.

8.1 Unterzeichnende

Das Pflichtenheft wurde von mir als Ausführender und der Schule als Kunden unterschrieben.

8.2 Ziele

Ziel des Projektes „Einrichtung eines zentralen Anmeldeservers“ ist es, einen Domänencontroller für die im Laufe des Projektes einzurichtenden Computer der neuen Computerräume einzurichten und die Computer aus dem bestehenden System in das neue System zu integrieren. Der alte Datenbestand wird vom alten Dateiserver übernommen und auf den einzurichtenden neuen Dateiserver aufgespielt. Um einen Virenschutz zu gewährleisten, wird eine Internetfirewall mit integriertem Virenschutz eingerichtet. Zusätzlich muss diese Firewall aufgerufene Webinhalte prüfen und den Zugriff auf unerwünschte Inhalte sperren. Die Definition von unerwünschten Inhalten muss jederzeit änderbar sein. Weiterhin muss ein Virens Scanner auf dem Dateiserver eingerichtet werden, der die Dateien beim Öffnen und Speichern auf Viren überprüft. Die bestehende Anti-Virus-Lösung auf den bestehenden Rechnern wird beibehalten, der derzeitige Konfigurationsstand so abgeändert, dass kein kompletter Systemscan nach einem Update mehr durchgeführt wird. Der Anmeldeserver muss für jeden Schüler 50 Megabyte Speicher bereitstellen. Ein Zugriff auf diesen Speicherbereich muss für den Schüler von jedem Rechner aus dem alten Rechnerraum sowie den neuen Rechnerräumen möglich sein.

8.3 Hardwareausbau

Die benötigte Hardware für Server und Firewall wird vom Ausführenden gekauft und konfiguriert. Den Ausbau des Netzwerkes inklusive Kauf und Einrichtung von Switchen sowie der Verkabelung der Räume wird von der Schule durchgeführt.

8.4 Testanforderungen

Um die Möglichkeit der Benutzeranmeldung zu testen wird eine Anmeldung eines Benutzers nacheinander aus jedem Raum vorgenommen. Die Virens Scanner werden mit der EICAR Testsignatur getestet. Der Test gilt als fehlgeschlagen, wenn der EICAR Testvirus erfolgreich auf einen Rechner in einem der Rechnerräume geladen werden kann. Um die Filterung von unerwünschten Inhalten zu testen wird von einem der Rechner aus den Rechnerräumen versucht die Internetseiten <http://www.youporn.com> und <http://www.playboy.com> aufzurufen. Wenn der Aufruf gelingt, gilt dieser Test als fehlgeschlagen.

Tabellenverzeichnis

1.1	Rechnerdetails	1
2.1	Entscheidungskriterien	5
3.1	Die gewichtete Entscheidungstabelle	7
4.1	Angebotsgrundlage	8
4.2	Angebotstabelle	9
6.1	Rechnungsgrundlage	13
7.1	Hilfsurls	21

9 Quellen

9.1 Quellenangaben

Webseiten:

<http://www.skolelnux.no>

<http://www.ubuntu.com>

<http://www.edubuntu.org>

<http://www.slixs.at>

<http://www.linux-schulserver.de>

<http://www.microsoft.com>

<http://www.reichelt.de>

<http://www.pyramid.de>

<http://www.bechtle.de>

<http://www.thomas-krenn.de>