

Open Source Migration der Monopolkommission

Beispiel einer Migration von Windows2000 auf Open Source Software

von Thomas Sprickmann Kerkerinck

Die Ausschreibung des BSI

Im Juni vergangenen Jahres wurde seitens des Bundesinnenministers die Initiative ergriffen Open Source Projekte in Bundesbehörden zu initiieren, um die Einsatzfähigkeit von Open Source Software und im speziellen Linux zu evaluieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) suchte daraufhin Behörden, die im Rahmen eines Pilotprojektes bereit waren, eine entsprechende Umstellung durchzuführen. Die Monopolkommission war dazu bereit.

Die Aufgaben der Monopolkommission als Determinante für die IT-Struktur

In der Monopolkommission arbeiten Wissenschaftler als Gutachter für die Bundesregierung an der Erstellung von Gutachten zur regelmässigen Beurteilung des jeweiligen Standes und der absehbaren Entwicklung der Unternehmenskonzentration in Deutschland unter wirtschafts-, insbesondere wettbewerbspolitischen Gesichtspunkten, der Würdigung der Vorschriften über die Zusammenschlusskontrolle und der Stellungnahme zu aktuellen wettbewerbspolitischen Fragen. Die Kommission besitzt gegenüber Unternehmen kein Auskunftsrecht. Amtliche Daten unterliegen den jeweils für sie geltenden Vertraulichkeits- und Geheimhaltungsvorschriften.

Im Zusammenhang mit diesen Aufgaben nutzen die wissenschaftlichen Mitarbeiter den Arbeitsplatzrechner um Texte zu erstellen, Daten auszuwerten und Daten zu präsentieren und Daten mit andern per eMail auszutauschen. Die Daten werden aus unterschiedlichen Bereichen und in unterschiedlichen Formaten zur Verfügung gestellt oder über Internetrecherche erhoben. Neben den wissenschaftlichen Mitarbeitern und ihren Aufgaben hat die Monopolkommission weitere Mitarbeiter, die unterschiedliche Aufgaben wie Bibliotheksverwaltung und Sekretariat und die Aufgaben der Geschäftsstelle der Monopolkommission übernehmen. Auch diesen Mitarbeitern sind in der Hauptfunktion Textverarbeitung und Tabellenkalkulation und eMail zuzuordnen. Darüber hinaus sind jedoch auch die Zusammenstellung von Zeitungsquellen, CD-Archivierung, allgemeine Funktionen wie Terminkalender, scannen, Webseiten erstellen, farbig drucken u.v.m. im Bereich der Mitarbeiter zu finden. Diese bereits bestehenden Aufgaben aller Mitarbeiter der Monopolkommission waren durch die Migration der Arbeitsplatzrechner und der Server auf Open Source Software unbehindert weiterzuführen.

Die Auswahl der Distribution

Im Rahmen der Bieterkonferenz zum Auftrag standen 8 verschiedene Firmen vor der Aufgabe den Projektverantwortlichen des BSI als auch der Monopolkommission eine Aussage über Präferenzen für die einzusetzende GNU/Linux Distribution zu geben. Die überwiegende Mehrheit der Unternehmensvertreter sprachen sich für Debian aus, da das Thema Softwareverteilung und Stabilität für die PC-Arbeitsplätze (Clients) mit besonderer Bedeutung versehen war.

Ziel der Migration

Ziel der Servermigration war eine harmonische Client/Server Landschaft, welche flexibel einsetz- und erweiterbar sein sollte und die Gesichtspunkte Wartbarkeit, Verfügbarkeit und Wiederherstellbarkeit berücksichtigte. So wurden sämtliche Serverkomponenten bzw. Dienste auf die Anforderungen der Clients angepasst, insbesondere hinsichtlich zentraler Administration, Datenhaltung, Update-Fähigkeit der Clients und dynamischer Benutzerkonfiguration.

Im Feinkonzept wurde festgelegt, dass die Konfiguration der einzelnen Arbeitsplatzrechner ausnahmslos von zentraler Stelle über einen Administrationsserver, die *INFRApliance* Administration Console, erfolgt. Als Hardware für die Serverkomponenten sollte der vorhandene Hardware (Dell Poweredge 2500) genutzt werden.

Sämtliche Funktionalitäten sollten übersichtlich und einfach zu administrieren sein, um einen schnellen Umstieg für die Administratoren zu ermöglichen.

Ziel der Client-Migration war der Austausch der vorhandenen Applikationen durch gleichwertige OSS-Applikationen oder Applikationen, die auf dem OSS-Betriebssystem GNU/Linux lauffähig sind. Die

Nutzer sollten sich dabei so einfach und so schnell wie möglich an die veränderte Umgebung gewöhnen und alle wesentlichen Funktionen ihres bisherigen Arbeitsplatzrechners wiederfinden. Dabei sollte eine „Vor-Ort-Administration“ weitgehend unterbleiben können. Gleichzeitig sollte für die sensiblen Daten eine zentrale Datensicherung und eine den hohen Sicherheitsanforderungen der Monopolkommission gerecht werdenden Zutrittsbeschränkung zu den Daten implementiert werden. Die Anschaffung von neuer Client Hardware sollte soweit als möglich unterbleiben.

Das Konzept

Als Clients sollten handelsübliche PC zum Einsatz kommen, auf denen als Betriebssystem die Debian-Distribution des GNU/Linux mit Namen „Woody“ installiert wird. Die Clients selbst halten die Applikationen vor und setzen ihre Prozessorleistung zur Ausführung der Applikationen ein. Daher sollten Clients mindestens mit Pentium II oder Celeron (500 MHz) oder AMD K6-2 ausgestattet sein. Die Druckaufbereitung, das Scannen von Daten, die Webcam, u.v.m. werden vom PC übernommen. Alle Applikationen der Monopolkommission die auf dem Betriebssystem Windows2000 lauffähig waren, wurden durch Open-Source-Software (OSS) oder OSS-lauffähige Applikationen ersetzt. Einzige Ausnahme ist ein von der Firma Hoppenstedt erstellte CD-ROM für Firmendaten, deren Applikation Einträge in die Windows Registry vornimmt. Jedoch auch hier konnten durch Mitarbeiter eines anderen Pilotprojektes (Bundeskartellamt) erfreuliches berichtet werden und auch diese Applikation steht unter Linux (mit WINE) zur Verfügung.

Im Unterschied zu Windows2000 steht mit GNU/Linux eine Auswahl verschiedener Windowmanager zur Verfügung, die zum Einsatz kommen könnten. Bereits im Angebot wurde der IceWM als Windowmanager berücksichtigt, da sich die Optik sehr an bereits bekannte „Desktop“ anlehnt, jedoch als Applikation auf dem Client moderat mit den Systemressourcen umgeht. Die „Desktop“-Funktionalität, d.h. das Programm-Icons auf der Oberfläche liegen und per Mausklick die damit verbundenen Programme gestartet werden können, wird nicht über den IceWM zur Verfügung gestellt, sondern durch den Filebrowser GNOME Midnight Commander.

Als Office-Applikation wurde StarOffice 6.0 ausgewählt. Ausschlaggebend für den Einsatz von StarOffice 6.0, alternativ zu OpenOffice.org, war die Rechtschreibprüfung, da in der Monopolkommission kein anders Office-Produkt mehr vorhanden sein würde, kam einer möglichst guten Rechtschreibprüfung eine besondere Bedeutung zu. Einigen Benutzern wurde alternativ die Möglichkeit gegeben, wie bisher mit Latex Texte zu verfassen und zu layouten.

Für das Suchen von Dateien ist mit dem Windows Explorer ein Produkt im Windows-Umfeld zur Verfügung, das in der intuitiven Bedienbarkeit auch für den Einsatz in der Monopolkommission als Maßstab für Filebrowser-Funktionen benannt wurde. Der GNOME Midnight Commander (GMC) bietet ebenfalls Linux-basiert die gewünschten Funktionen und ermöglicht darüber hinaus das „Öffnen“ und „Ansehen“ von Archiven (z.B. .zip oder .tar), ohne auf ein entsprechendes Archivierungswerkzeug zurückgreifen zu müssen.

Für die Mailfunktionalität standen zu Beginn des Projektes drei OSS-Produkte zur Auswahl. Kmail, Sylpheed und Mozilla. Da im Zusammenhang mit der Umstellung der Arbeitsplatzrechner auch die bereits vorgesehene Digitale Signatur eingeführt werden sollte, wurde ein einfach zu bedienender Mail-Client gesucht, der neben der leicht zu bedienenden graphischen Oberfläche auch die Unterstützung für GNUUpG als Digitaler Signatur bot. Die Entscheidung für einen Standardarbeitsplatz fiel auf Sylpheed.

Als Browser standen ebenfalls einige Applikationen zur Auswahl: Konquerer, Mozilla, Galeon. Da die Funktionen zum Durchsuchen von Internetseiten mindestens den Umfang der bisher zur Verfügung stehenden Applikation haben sollte, war Mozilla aufgrund der umfangreichen Funktionen auch in Bezug auf Plug-Ins schon ein Favorit als Browser, da jedoch die Mailfunktionen von einer anderen Applikation übernommen würde wurde bei den Testnutzern Galeon eingesetzt. Schnell fanden sich die Testnutzer zurecht und somit wurde Galeon, der auf der „Rendering-engine“ von Mozilla basiert, gewählt.

Bisher kam ein vom Scannerhersteller mitgeliefertes Programm Adobe Photoshop LE (Limited Edition) und der entsprechende Windows-Treiber zum Einsatz. Da für den Scanner ein Treiber für Linux zur Verfügung stand, wurde nur noch nach einer Scanner-Software unter Linux gesucht. SANE (Scanner Access Now Easy, Frontend Xsane) wurde den Testbenutzern zur Verfügung gestellt und nachdem die bisher genutzten Funktionen über SANE ebenfalls zur Verfügung stehen, konnte sichergestellt werden, dass die Benutzer die erforderlichen Aufgaben erledigen können. Um eine

leichte Weiterverarbeitung der Daten zu ermöglichen, wurde das Scannerprogramm auch zum Aufruf aus StarOffice und GIMP eingerichtet. Dort kann man unter einem entsprechenden Menüpunkt ein Bild vom Scanner „anfordern“.

Für die Erstellung von .pdf-Dokumenten wurde auf Basis des Betriebssystems Windows2000 der Adobe Acrobat in der Version 5.0 eingesetzt. Von den verschiedenen Funktionen wurde im wesentlichen der Acrobat Distiller benutzt, um aus .doc-Dokumenten entsprechende .pdf-Dokumente zu erstellen. Da die weitergehenden Funktionen des Adobe Acrobat nicht benutzt wurden, war es möglich die im StarOffice 6.0 und OpenOffice.org integrierte Funktion des Erstellens eines .pdf-Dokumentes über den Druckdialog und die Auswahl des „PDF-Konverter“ zu nutzen. Für das Öffnen von .pdf-Dokumenten zum Lesen und Drucken steht der Acrobat Reader in der Version 5.0 als Freeware auch für Linux zur Verfügung.

Integration besonderer Sicherheitsmerkmale am Arbeitsplatz

Als Wunsch der Monopolkommission stand von Anfang an fest, dass für die Anmeldung am Client eine Kombination von zwei Merkmalen zur Authentifizierung am Arbeitsplatz zum Einsatz kommen sollte, da die Kombination von zwei Sicherheitsmerkmalen zu einer Erhöhung der Fälschungssicherheit einer Authentifizierung führt. Ergebnis war die Kombination von Chipkarte und Fingerabdruck.

Für die Erstellung von Chipkarten, zum Enrollment von Fingerabdrücken und zur Erstellung der Digitalen Signatur-Daten wurde eine integrierte Applikation erstellt. Hiermit kann sehr leicht über eine graphische Oberfläche eine Chipkarte erstellt werden, die bis zu zehn Finger eines Benutzers enrollt werden und die GnuPG-Schlüssel für die Digitale Signatur erzeugt werden. Die Gewinnung der Biometriedaten wird dabei über ein Produkt der Siemens AG durchgeführt, welches nicht quelloffen zur Verfügung steht. Die Daten, die per Minuzien-Verfahren aus einem gescannten Fingerabdruck gewonnen werden, liegen verschlüsselt auf dem Webserver.

Über die Chipkarte sollte den Nutzern ermöglicht werden, die Authentifizierung ohne Passwort durchzuführen und Platz für die Aufnahme der Daten für die Digitale Signatur zu bieten. Verblieben wäre jedoch die Bestätigung der Authentizität durch Eingabe einer „Persönlichen Identifikationsnummer“ (PIN) auf der Chipkarte. Diese Eingabe wurde für die „Online“-Umgebung durch die Nutzung eines biometrischen Verfahrens ersetzt.

Die Chipkarte wird jetzt zur Authentifizierung in beiden möglichen Umgebungen („Online“ und „Offline“) auf gleiche Art, jedoch mit unterschiedlicher Ausprägung genutzt.

Für die Mitarbeiter der Monopolkommission ist als Regelfall das Arbeiten im Netzwerk der Monopolkommission vorgesehen. Für diesen Fall sind alle Dienste und Applikationen für die Mitarbeiter zugänglich. Der Benutzer authentifiziert sich mit Chipkarte und Fingerabdruck. Die Integration der Chipkarte in das System erfolgt über eine PAM (Pluggable Authentication Module) Schnittstelle, so dass die Authentifizierung für den Displaymanager (verantwortlich für den Anmeldebildschirm) sowie auch für die Bildschirmschoner zur Verfügung steht. Nach Einschub der Chipkarte werden die verschlüsselten Biometriedaten vom Server geladen und mittels Fingerprintschlüssel entschlüsselt. Im Anmeldebildschirm und per LED Anzeige der Maus erscheint dann die Aufforderung, einen Finger auf den Sensor zu legen. Die Biometriedaten werden extrahiert und mit den entschlüsselten Daten verglichen (matchen). Ist der Benutzer am System angemeldet und wird die Karte entfernt, wird die Arbeitsstation per Bildschirmschoner gesperrt. Nach Wiedereinschub der Karte, werden wiederum die Biometriedaten verglichen und ggf. der Zugriff auf die Arbeitsstation gewährt.

Unter der „Online“ Umgebung wird die Netzwerkumgebung verstanden bei der folgende Voraussetzungen gelten. Zum einen muss ein Client eine physische Verbindung zum Netzwerk haben (Netzwerkkabel). Zum zweiten müssen dann im Netzwerk folgende Dienste zur Verfügung stehen: Nameservice, Adminservice (LDAP-Service), Fileservice.

Für den Fall, dass die Netzwerkverbindung gestört ist und die Arbeitsplatzrechner keinen Zugriff zu den Servern haben ist keine normale Anmeldung am Arbeitsplatz möglich. Der Benutzer erkennt dies an der Anmeldemaske. Er findet dann nicht die gewohnte Anmeldemaske vor, sondern eine spezielle „Offline“-Anmeldemaske.

In solchen Fällen kann sich ein Benutzer nur „Offline“ anmelden. Dafür wird ausschließlich die Chipkarte benötigt, da die Biometriedaten bei einer Anmeldung mit den Daten des LDAP-Directory verglichen werden müssten, die aber nur über das Netzwerk zu erreichen wären.

Da die vom Benutzer erstellten Daten nicht auf dem zentralen Fileserver abgelegt werden können, wird bei der ersten „Offline“-Anmeldung an einem Arbeitsplatz ein „Home“-Verzeichnis für den Benutzer angelegt, in dem er seine Daten speichern kann. Zu diesem „Home“-Verzeichnis hat nur der Benutzer und der Administrator Zugriff. Sollte sich an dem Rechner ein anderer Mitarbeiter anmelden, wird auch für ihn ein eigenes „Home“-Verzeichnis angelegt.

Wenn der Benutzer sich an diesem Arbeitsplatz später wieder „Online“ anmeldet, wird sein „Home“-Verzeichnis mit gemountet, d.h. er kann auf seine lokal gespeicherten Daten wieder zugreifen. Dabei hat er für den Datenabgleich selbst zu sorgen. Wenn er „Online“ ist, kann er Daten vom Fileserver in sein lokales „Home“-Verzeichnis kopieren oder verschieben und auch umgekehrt Daten aus dem „Home“-Verzeichnis auf dem Server ablegen. Ein Abgleich der Dateien ist manuell zu tätigen.

Als Applikationen stehen dem Benutzer dann StarOffice und Sylpheed als Mail-Client zur Verfügung. Da alle anderen Dienste und Applikationen nur für den Netzwerkgebrauch vorgesehen sind, kann der Benutzer diese im „Offline“-Modus nicht nutzen.

Digitale Signatur

Im Rahmen der Migration der Monopolkommission sollte die Einführung der digitalen Signatur für den gesicherten Mailverkehr erfolgen. Da das BSI mit dem Projekt Ägypten¹ über ein Open-Source-Projekt verfügt, das den Standard nach Sphinx² zur Erstellung einer Public-Key-Infrastruktur (PKI) erfüllt, sollte wenn möglich die digitale Signatur aufgrund der dort getätigten Entwicklung mit dem Mail-Client Kmail umgesetzt werden. Da zum Entscheidungszeitpunkt die Arbeiten im Projekt Ägypten noch nicht in Form eines einsatzreifen Produktes abgeschlossen waren, wurde als die digitale Signatur in Form von GnuPG-Schlüsseln realisiert. Dabei werden die GnuPG-Daten verschlüsselt auf der Chipkarte abgelegt.

Die Serverumgebung

Angeboten war im Bereich der Server die INFRAppliances der Firma SFI Technology Services AG, die als Open-Source-Software (OSS) im Rahmen des Projektes Anpassungen erfordern oder erstellt wurden, um den Anforderungen an die zentrale Administration der gesamten Client- und Serverlandschaft zu entsprechen. Die Serverfunktionen sollten sich im Rahmen des Projektes auf einem Server installieren lassen.

Bei der INFRAppliance Administration Console handelt es sich um ein webbasiertes Werkzeug, mit dem alle wesentlichen Parameter für die Server, Clients, Applikationen und Benutzer administriert werden können. Die Daten werden dabei in einem LDAP-Server mit openLDAP abgelegt. Von dort können Sie bei Bedarf auch wieder hergestellt werden.

Die Administration Console unterstützt in der IT- Umgebung die zentrale Verwaltung von

- Benutzerkonten und -einstellungen
- Druckern
- Softwarepaketen für die Softwareverteilung
- Client-Hardwarekonfiguration

Damit wurde die Administration Console zentraler Angelpunkt für die umfangreichen zentralen Funktionen, die in dem Konzept zur Verfügung stehen. Die auf der Administrationskonsole eingestellten Parameter werden serverseitig durch den 'sfi-director' Daemon im Hintergrund verarbeitet. Dadurch ist es möglich, die getätigten Einstellungen auch auf mehrere Server zu replizieren, um so eine einheitliche Administrationsoberfläche für verschiedene Linux-Server, zur Verfügung zu stellen.

Der INFRAppliance Fileserver hält in der Monopolkommission alle von den Benutzern erstellten Daten in deren „Home“-Verzeichnissen vor. Gleichzeitig sind für den Austausch von Daten oder das Zusammenarbeiten von Mitarbeitern Gruppenverzeichnisse angelegt, in die die Mitglieder einer

¹ www.bsi.de/aufgaben/projekte/sphinx/aegypten/opensour.htm

² www.bsi.de/aufgaben/projekte/sphinx/index.htm

Gruppe Dateien legen und aus denen sie auch lesen können. Integriert ist ein Backup-Modul, mit dem die Daten des Fileserver nach einstellbaren Parametern gesichert und rückgesichert werden können.

Der *INFRApliance* Webserver ist die für eine Reihe von Funktionen eingesetzt. Zuerst dient er als Webserver für die zentralen Webapplikationen. Dann werden die Intranetseiten der Monopolkommission über den Webserver zur Verfügung gestellt. Gleichzeitig stehen die Softwarepakete für Clients über den Webserver zur Verfügung. Für die Webapplikationen jedoch auch für andere Applikationen sind auch die Datenbanken (PostgreSQL, MySQL) hier implementiert. Zuletzt nimmt der Webserver mit dem *INFRApliance* PHP-Groupware- und Webfilespace die Aufgaben für Datenaustausch und Groupware über die Webapplikation PHP-Groupware wahr. Integriert ist hierbei ein Backup-Modul für die Sicherung und Rücksicherung der entsprechenden Datenbestände.

Die drei Server und die ergänzenden Module wurden innerhalb des Projektes so erstellt bzw. angepasst, dass die gesamte Client- und Serverlandschaft von der Administration Console aus zu administrieren ist. Dabei basiert das Frontend der Administration Console auf der Open-Source-Software (OSS) Webmin. Die Weboberfläche gestattet die Administration der Clients und Server unabhängig vom Standort des Administrators, von jedem im Netzwerk befindlichen Arbeitsplatzrechner.

Als zentraler Verzeichnisdienst kommt openLDAP zum Einsatz, wo letztlich alle Einstellungen, die zu Benutzern Software oder Hardware administriert werden, abgelegt werden. Damit sind die Daten für die Wiederherstellung von Benutzerprofilen besonders leicht zu erhalten. Gleichzeitig werden die Benutzerprofile auch in den jeweiligen „Home“-Verzeichnissen der Benutzer hinterlegt, so dass bei der Anmeldung eines Benutzers die entsprechenden individuellen Einstellungen für den beliebigen Arbeitsplatz zur Verfügung stehen.

Zentraler Ansatz

Für die Kosten des Betriebs einer IT-Infrastruktur sind eine ganze Reihe von Faktoren von Bedeutung. Neben den Lizenzkosten für Betriebssystem und Applikationen auf Servern und Clients sind die laufenden Kosten des Betriebs der wesentliche Faktor.

Der zentrale Ansatz wurde grundsätzlich für alle Funktionen zum Betrieb der IT-Struktur in der Monopolkommission und für die zu erstellenden Webapplikationen gewählt, da dadurch die Administrationskosten wesentlich gesenkt werden können. Wenn Administration vor Ort entfallen kann, die Benutzer grundsätzlich nicht in der Lage sind die auf dem LDAP-Server liegenden Einstellungen zu ändern, die aktuellen Konfigurationen jederzeit eingesehen werden können, d.h. das System jederzeit definiert ist und letztlich auch noch die „Fernwartung“ systemeigenen mit Linux möglich ist, dann kommt mit der zentralen Administration und Datenhaltung bei dezentraler Verfügbarkeit von Rechenleistung lokal am Arbeitsplatz derzeit ein Optimum an kostensenkenden Faktoren zusammen.

Auf dem Administrationsserver war bereits RedHat Version 7.2 installiert. Die *INFRApliance* Administration-Console basiert auf verschiedenen Filesystemen: ext3 für das 'eigentliche Betriebssystem', xfs für die 'Nutzdaten', wie Web, Administration (LDAP), Datenbanken und NFS-Exporte.

Die Benutzerdaten (z.B. Name, User ID, Group IDs) und Benutzereinstellungen für Applikationen werden über die Administration Console angelegt und administriert. Die Daten werden über die Administration Console im LDAP-Server abgelegt, aus dem die Daten jederzeit wiederhergestellt werden können. Gleichzeitig werden Benutzereinstellungen auf dem *INFRApliance* Fileserver mit in den jeweiligen Homeverzeichnissen deponiert. Die Zuweisung von im Netzwerk befindlichen Druckern -letztlich werden alle Drucker als Netzwerk in das Netzwerk eingebunden - erfolgt ebenfalls über die Administration Console. Die entsprechenden Informationen werden in den Homeverzeichnissen abgelegt und stehen den Benutzern mit der Anmeldung automatisch zur Verfügung.

Ebenfalls werden weitere Einstellungen der Hardwarekonfiguration der Clients über den Administration Console auf dem LDAP-Server abgelegt. Die Daten werden automatisch bei Installation der Clients oder über das entsprechende Modul der Administration Console manuell registriert. Dabei wird die MAC-Adresse der Netzwerkkarten als Client bezeichnendes Merkmal verwendet. Die vom Client automatische erkannten Hardwaredaten (Grafikkarte, Grafikkartentreiber

und Monitoreinstellungen) werden nach Angabe es Host-Administrator-Passwortes im LDAP-Tree abgelegt.

Der Administrationsserver stellt auch die Verwaltung der für die Clients vorgesehenen Softwarepakete zur Verfügung. Dabei findet die Installation von Software (Patches, Updates oder Applikationen) über die in der Administration Console definierten Client-Gruppen statt. So können Updates oder Release-Wechsel zunächst auf einzelnen Clients getestet werden, ohne die Produktivumgebung zu beeinflussen. Natürlich sind so auch unterschiedliche Client-Konfigurationen möglich, wobei dann jedoch die Roaming-Funktion eingeschränkt oder gar aufgehoben wird.

Die Daten der Benutzer werden zentral auf dem Server im INFRA*Appliance* Fileserver mit Backup gehalten. Damit ist gewährleistet, dass die sensiblen Daten in das bestehende Sicherungskonzept für den Server eingebunden werden und eine Delegation der Verantwortlichkeiten der individuellen Sicherung der Daten auf dem Client - mit den damit verbundenen Schwierigkeiten der Kontrolle - unterbleiben kann. Der Zugriff auf die Daten auf dem Server ist durch User- und Gruppenrechte gesteuert, wobei die „Home“-Verzeichnisse der Benutzer für andere Benutzer nicht zugänglich sind. Lediglich dem Administrator sind Zugriffsrechte gewährt.

Die zentrale Softwareverteilung ermöglicht die automatische, schnelle und einfache Verteilung von Betriebssystem Updates, Applikationen und Security-Patches. Dabei wird die zu verteilende Software in systemkonforme Pakete für die Debian-Distribution (apt-get-Schnittstelle) gepackt, die den Clients zur automatischen Installation zur Verfügung gestellt werden. Beim Booten des Rechners wird der Softwarestand des Clients überprüft und eventuell zur Verfügung stehende Softwarepakete automatisch heruntergeladen und installiert. Die Möglichkeit, auch manuell Softwarepakete auf die Clients zu laden bleibt dabei erhalten. Durch Zuordnung von Clients zu Clientklassen können einzelne Softwarepakete diesen Clientklassen zugewiesen werden.

Spezielle Aufgaben

Neben den für den Client und auf der Serverseite entwickelten Lösung sollten im Rahmen der Migration noch weitere Funktionalitäten erstellt oder aus dem Microsoft-Umfeld ersetzt werden.

Da eine Reihe von Funktionen von mehreren Arbeitsplätzen aus genutzt werden sollte, entstanden im Rahmen des Projektes Webapplikationen, die über den INFRA*Appliance* Web und Groupware-Server allen Mitarbeitern der Monopolkommission per Webbrowser zur Verfügung stehen.

Bibliotheksverwaltung

Da die Monopolkommission eine eigene Bibliothek besitzt, wurde zur Verwaltung des Bücherbestandes der Bibliothek ein Katalog mit Webinterface erstellt, mit dem jeder berechnigte Mitarbeiter von seinem Arbeitsplatz aus die Liste der verfügbaren Bücher einsehen und nach Büchern mit bestimmten Attributen durchsuchen kann. Das Webinterface bietet dabei für Mitarbeiter mit Verwalterbefugnissen zusätzlich die Möglichkeit, neue Bücher aufzunehmen, die Daten bereits aufgenommener Bücher zu verändern oder aus dem Katalog zu entfernen.

Alle Daten wurden aus Gründen der Performanz und der Datensicherheit in einer auf dem Administrationsserver befindlichen PostgreSQL-Datenbank abgelegt. Die Administration der Applikation, die sich auf das Setzen einiger grundlegender Parameter beschränkt (z.B. Festlegung der Gruppennamen für die Recherche- und Verwalterbefugnisse), wurde in die Administration Console integriert. Folgende Funktionalitäten stehen dem Benutzer demnach über die Intranet Seite zur Verfügung.

- Suche nach Büchern
- Anzeige der Neuerwerbungen
- Hinzufügen eines neuen Buches (falls der Benutzer der Gruppe angehört, der die Verwalterbefugnisse eingeräumt wurden)
- Anzeige der Ausleihen eines Benutzers

Dem Administrator der Bibliotheksverwaltung stehen weitere Funktionen zur Verfügung, die ihm die Verwaltung der Buchbestände und der Ausleihen durch Mitarbeiter der Monopolkommission ermöglichen.

CD-Archivierung

Bei der Monopolkommission wurden abgeschlossene Projekte, z.B. in der Vergangenheit erstellte Gutachten, auf CD archiviert.

Zur Verwaltung dieser CDs wurde ein CD-Katalog mit Webinterface erstellt, mit dem jeder berechtigte Mitarbeiter von seinem Arbeitsplatz aus die Liste der verfügbaren CDs einsehen und nach Dateien mit bestimmten Attributen (Name, Änderungsdatum, Größe) durchsuchen kann. Das Webinterface bietet für Mitarbeiter mit Editorbefugnissen ferner die Möglichkeit, beliebige neue CDs in den Katalog aufzunehmen sowie die Daten von existierenden CDs zu modifizieren bzw. aus dem Katalog zu entfernen. Alle Daten sind aus Gründen der Performanz und Datensicherheit in einer auf dem Administrationsserver befindlichen PostgreSQL-Datenbank abgelegt. Die Administration des Systems, die sich auf das Setzen einiger weniger grundlegender Parameter beschränkt (z.B. Festlegung der Gruppennamen für die Recherche- und Editorbefugnisse), wurde in die Administration Console integriert. Folgende Funktionen wurden in der Applikation verwirklicht:

- Stöbern durch den CD-Bestand nach diversen Kriterien (z.B. nach Kategorie oder Entstehungsjahr)
- Suche im CD-Bestand nach CD-Attributen
- Suche nach Dateien (Ermitteln der CDs, die bestimmte Dateien enthalten)
- Hinzufügen einer neuen CD (falls der Benutzer der Gruppe angehört, der die Editorbefugnisse eingeräumt wurden)

Kalender

In der Monopolkommission wurden zur Abstimmung von Terminen mit der OSS PHP-Groupware ein Terminkalender per Webapplikation zur Verfügung gestellt, der über die Intranetseite durch die Benutzer aufgerufen werden kann. Hier können die Mitarbeiter ihre eigenen Termine und Gruppentermine eingeben und organisieren. Dabei verfügt der Terminkalender über die Funktion Termine mit anderen Mitarbeitern abgleichen zu können, d.h. Überschneidungen entsprechend anzuzeigen.

Adressbuch

Die Aufgabenstellung im Zusammenhang mit dem Adressbuch war geprägt von unterschiedlichen Anforderungen und unterschiedlichsten Datenquellen für die Mitarbeiter der Monopolkommission. Auch hier wurde im Rahmen des Feinkonzeptes entschieden den Anforderungen durch die Entwicklung einer Webapplikation zu entsprechen. Zum späteren Zeitpunkt wurde die Integration der Funktionen in PHP-Groupware beschlossen und realisiert. Den Mitarbeitern steht eine Auswahl verschiedener „Adressbücher“ zur Verfügung, die über die Datenbankbindung von StarOffice auch für Serienbrieffunktionen genutzt werden können.

Migration Fragebogen-Workflow und Statistikdatenauswertung

Die Vorgaben zu diesen beiden Punkten waren im Rahmen der Ausschreibung und auch bei der Erstellung des Feinkonzeptes im Wesentlichen auf die Anforderungen der beiden betroffenen Mitarbeiter zugeschnitten. Für beide Teilprojekte gab es keine von vornherein fest definierten Applikationen, die migriert werden mussten. Statt dessen stützten sich die Aufgaben, die von den wissenschaftlichen Mitarbeitern im Zusammenhang mit der Auswertung von Statistikdaten für die Gutachten und im Zusammenhang mit der Datenerhebung mittels an Firmen gesandter Fragebögen zu erledigen sind, im Wesentlichen auf Funktionen, die von dem Softwareprodukt Microsoft Office abgedeckt wurden. Dabei wurden vor allem dessen Teilkomponenten Access (Datenbank), Excel (Tabellenkalkulation) und Visual Basic (Makro- bzw. Skriptsprache zur Prozeßautomatisierung) eingesetzt. Da das im Zuge der Migration als Ersatz für Microsoft Office eingeführte StarOffice diese Funktionalitäten nicht vollständig anbietet -- so ist zwar mit StarCalc eine mit Excel vergleichbare Tabellenkalkulation vorhanden, es fehlen jedoch die Datenbank und eine zu Visual Basic vollständig kompatible Programmiersprache -- musste für die fehlenden Funktionalitäten anderweitig Ersatz beschafft werden. Es war also notwendig, die Aufgaben der beiden Mitarbeiter zu analysieren, wiederkehrende Problemstellungen zu identifizieren und dann Methoden und Werkzeuge auszuwählen, mit denen die Mitarbeiter ihre Aufgaben auch nach der Umstellung auf Linux und Open-Source-Software würden erledigen können. Zuletzt waren die Mitarbeiter in der Anwendung dieser Methoden und Werkzeuge zu unterweisen.

Da sich die Funktionalitäten von StarOffice, wie oben bereits angedeutet, auf die grundlegenden Office-Bereiche Textverarbeitung, Tabellenkalkulation und Präsentationserstellung konzentrieren, war zunächst Ersatz für die Datenbankkomponente von Microsoft Access zu finden (die Datenzugriffskomponente von Access, also Funktionen zum Zugriff auf und zur Arbeit mit externen Datenquellen, ist in StarOffice überwiegend vorhanden). Hierbei fiel die Wahl wiederum auf PostgreSQL, aus demselben Gründen, aus denen dieses RDBMS auch für die Webapplikationen ausgewählt worden war, und um nicht unnötigerweise ein zusätzliches System einzuführen. Als Programmiersprache wurde ebenfalls Perl gewählt, wobei hier die herausragenden Fähigkeiten zur Textextraktion (wichtig bei der Verarbeitung von Daten aus externen Quellen), die Vielfalt an hochwertigen, frei verfügbaren Modulen für alle denkbaren Anwendungszwecke, die gute Datenbankbindung durch das Datenbankinterface DBI sowie die Möglichkeit zur objektorientierten Programmierung und strukturierten Fehlerbehandlung (Exceptions) den Ausschlag gaben. Dazu kamen noch diverse kleinere Open-Source-Applikationen und Hilfsprogramme, um verschiedene spezifische Anforderungen der beiden Teilbereiche abzudecken, z.B. Software zur Datenvisualisierung (Ploticus) sowie diverse Datenbank-Hilfsprogramme. Mit dem Open-Source-Tool pgadminII und dessen "Database Migration Wizard" stand ein komfortables Hilfsmittel zur Verfügung, um bestehende Datenbanken von Microsoft Access nach PostgreSQL zu migrieren.

Die beiden Teilprojekte wurden also in einem interaktiven Prozeß, d.h. in direkter Zusammenarbeit mit den betroffenen Mitarbeitern angegangen. Hierbei war von Vorteil, dass beide Mitarbeiter bei ihrer Arbeit mit dem bisherigen System bereits an prinzipbedingte Grenzen gestoßen waren, deren Überwindung sie sich als Nebeneffekt der Migration erhofften, so dass ihre Motivation und Bereitschaft zur Kooperation entsprechend hoch waren und das angestrebte Ziel erreicht werden konnte.

Der Ablauf der Migration

Die Migration der Arbeitsplätze und der Serverumgebung konnte aufgrund der vielen Vorarbeiten erst sehr spät im Projekt zwei Wochen vor Projektende erfolgen. Die Migration der Serverumgebung ging in zwei Schritten vonstatten. Zuerst wurde ein INFRApliance Fileserver und ein INFRApliance Webserver in der Testumgebung aufgestellt. Der bisherige Fileserver wurde parallel im Netz betrieben.

Die Mitarbeiter wurden aufgefordert Ihre Daten, die eventuell noch lokal auf den PC Arbeitsplätzen vorhanden waren auf den zentralen Fileserver zu verschieben. Für den eigentlichen Migrationstag wurde ein Freitag ausgesucht, da die Mitarbeiter im Zusammenhang mit der Migration zum Enrollment der Fingerprintdaten einbestellt werden mussten. Das Enrollment und die Ausgabe der Chipkarten wurde soweit die Mitarbeiter vor Ort sein konnten durchgeführt. Danach wurde auf den PC die Client-CD installiert. Dabei ergaben sich bei der automatischen Hardwareerkennung Probleme mit den LWL-Netzwerkkarten. Die Karten sind von einem Hersteller und haben die identischen Bezeichnungen, jedoch wurden verschiedene Bausteine verwendet. Ergebnis dieses Umstandes war die Erstellung einer zweiten Client-CD die mit einem anderen Treiber für die Netzwerkkarten ausgerüstet wurden.

Die enrollten Mitarbeiter konnten darauf hin an ihren Arbeitsplätzen arbeiten. Für die Mitarbeiter wurde eine kurze Einweisung für die Anmeldung mit Chipkarte und Biometrie gegeben. Am folgenden Montag standen Mitarbeiter zur Verfügung, um eventuell auftretenden Problemen schnell begegnen zu können. Gleichzeitig setzten die Benutzerschulungen für die Mitarbeiter in ihren speziellen Aufgabenfeldern ein. Ursprünglich wurde die Schulung der Mitarbeiter in Gruppen vorgesehen. Aufgrund unterschiedlichster Anforderungen der einzelnen Mitarbeiter wurde jedoch auf die individuelle Schulung der Mitarbeiter für eine ganze Reihe von Funktionen umgestellt. Dies kam bei den Mitarbeitern gut an, ließ sich jedoch nur umsetzen weil einige Mitarbeiter nicht vor Ort waren. Dabei wurde ein modularer Aufbau für die Schulung gewählt. Es wurden kleine Abschnitte gewählt, um dem Mitarbeiter Zeit für Tagesgeschäft zu lassen und die Mitarbeiter konnten mitentscheiden, welche Module von ihnen benötigt wurden. Die wissenschaftlichen Mitarbeiter brauchten zum Beispiel keine Formatierungsdetails für Texte, da eine Kollegin die Formatierung der „offiziellen“-Texte übernimmt, zum anderen wurde nur für das Sekretariat der Umgang mit Serienbriefen als wichtig eingestuft. Der Aufwand der Schulungen wuchs jedoch damit auch an. Zusätzlich wurde die Übernahme der „Altdaten“ aufwendiger als erwartet, da die Datenvolumina der einzelnen Arbeitsplatzrechner („Laufwerk C“) im Vorfeld nur geschätzt werden konnte.

Erst nachdem die Clients migriert waren, wurde der bisherige Fileserver zum zentralen INFRApliance Server mit den oben genannten Funktionen. Da für die Migration des Fileservers keine Testmöglichkeit existierte entschloss man sich eine Woche nach der Client-Migration an einem Samstag auch den Server zu migrieren. Für den Fall das dabei Probleme auftreten würden, hätte man auf die bereits vorhandenen INFRApliance Umgebung in der Testumgebung zurückgreifen können. Doch die Migration lief im wesentlichen Problemlos, so dass bis auf die Backup-Funktion alle Funktionalitäten zur Verfügung gestellt wurden.

Das Backup-Problem wurde noch mal stark in den Vordergrund gerückt, als bei einem Backupversuch zum Wochenende der Server mit der verwendeten RedHat-Version abstürzte. Das Aufspielen eines neuen Kernels behob die Probleme des Betriebssystems mit der zur Verfügung stehenden Hardware. Seit dem läuft der Server im Produktivsystem.

Fazit

Die Migration IT-Struktur der Monopolkommission auf Open-Source-Software (OSS) wurde mit Erfolg abgeschlossen. Die geforderten Funktionen konnten mit nachvollziehbarem Aufwand erstellt werden.

Dabei lag der Schwerpunkt der Umstellung im Wesentlichen in der Abstimmung von vorhandenen Open-Source-Software-Komponenten, der Erstellung der zentralen Administrationsmöglichkeiten und der Implementierung der Sicherheitsfunktionalitäten sowie der Ablösung von Funktionen, die über die Applikation MS Access abgewickelt wurden.

Die größte Herausforderung bestand jedoch in der zeitlichen Definition der Arbeiten innerhalb von nur drei Monaten. Einige Funktionen wurden neu entwickelt und angepasst und solche Arbeiten waren mit einem extrem engen Zeitplan nur unter größten Schwierigkeiten zu bewerkstelligen.

Eine der Veränderungen die den Mitarbeitern die neue Arbeitsumgebung täglich präsent werden lassen ist die Integration der Chipkarte und Biometrie-Anmeldung. Die Funktionalität ist in der Art der Umsetzung leicht zu bedienen ist und im Tagesgeschäft nicht störend zu Tage tritt. Die Akzeptanz der neuen Arbeitsumgebung und der neuen Applikationen konnte über die besonders angepassten Schulungen hergestellt werden.

Das Ergebnis der Arbeiten ist eine in fast allen Bereichen unter General Public License (GPL) stehende Arbeitsumgebung die die vor der Migration vorhandenen Funktionalitäten wieder zur Verfügung stellt und an zahlreichen Punkten durch zusätzliche Funktionen ergänzt werden.

Die erstellte Lösung ist geeignet bei gleichgelagerten Anforderungen für eine schnelle Implementierung einer Open-Source-Software (OSS)-Lösung zu dienen. Bei andersartigen Anforderungen kann sie als Basis dienen, um Implementierungsschwellen von Open-Source-Software (OSS) zu senken oder Migrationsprojekte zu beschleunigen.

Kontakt:

natural computing GmbH
Martener Str. 535
44379 Dortmund
Tel.: +49 231 61048-50
Fax: +49 231 61048-40
info@natural-computing.de
www.natural-computing.de