

Beispiel einer Migration von Windows 2000 auf Open-Source-Software

THOMAS SPRICKMANN KERKERINCK

1. Die Ausschreibung des BSI

Im Juni 2002 wurde seitens des Bundesinnenministers die Initiative ergriffen Open-Source-Projekte in Bundesbehörden zu initiieren, um die Einsatzfähigkeit von Open-Source-Software (OSS) 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, seitens der Monopolkommission war man dazu bereit. Die Ausschreibung wurde mit einer Bieterkonferenz durchgeführt, in der alle namhaften Unternehmen aus der Open-Source-Software-Szene vertreten waren. Am 31. Juli wurde der natural computing GmbH, Dortmund, und ihren Partnern, der SFI Technology Service AG, Schweiz, sowie der Quelltext AG, ebenfalls Dortmund, der Zuschlag erteilt, und am 1. August begann das Projekt.

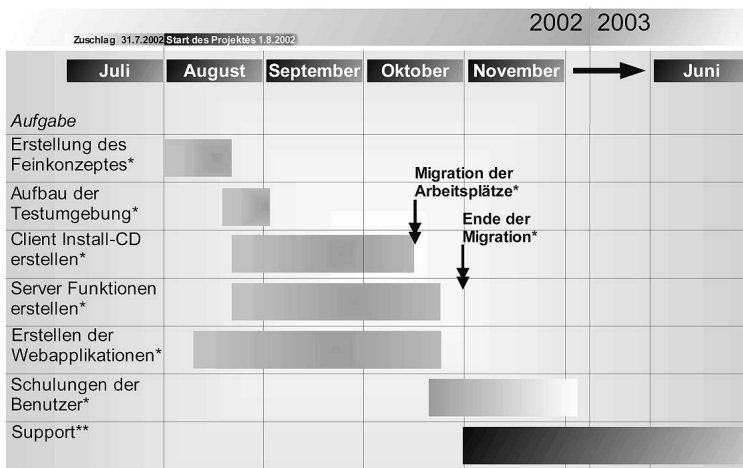


Abbildung 1: Zeitplan des Projektes der Migration der Monopolkommission

1.1. Die Aufgaben der Monopolkommission als Determinante für die IT-Struktur

Um im Rahmen des Projektes eine gute Leistung abgeben zu können, war es uns wichtig zu verstehen, welche Aufgaben die Monopolkommission hat. 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 zu präsentieren und sie mit anderen per E-Mail 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 sowie E-Mail zuzuordnen. Darüber hinaus sind jedoch auch die Zusammenstellung von Zeitungsquellen, CD-Archivierung, allgemeine Funktionen wie Terminkalender, scannen, Webseiten erstellen, Handouts erstellen 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.

1.2. Die Auswahl der Distribution

Im Rahmen der Bieterkonferenz zum Auftrag standen acht 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 (7 von 8) der Unternehmensvertreter sprach sich für Debian aus, da das Thema Softwareverteilung und Stabilität für die PC-Arbeitsplätze (Clients) mit besonderer Bedeutung versehen war. Die automatische Verteilung von Software-Paketen ist in einem Netzwerk von Computern eine der Zeit sparenden Methoden, um die jeweiligen Arbeitsplatzrechner mit der aktuellsten Software zu versorgen. Bisher waren dafür teure Werkzeuge notwendig, oder die Aktualisierung und das Neuinstallieren von Software wurde mittels Datenträger (Disketten oder CDs) von einem qualifizierten Mitarbeiter am einzelnen Arbeitsplatz vorgenommen.

1.3. Ziel der Migration

Ziel der Server-Migration war ein harmonisch aufeinander abgestimmtes Funktionieren der Clients und Server, also eine Client/Server-Landschaft, welche flexibel einsetz- und erweiterbar sein sollte und die Gesichtspunkte Wartbarkeit, Verfügbarkeit und Wiederherstellbarkeit berücksichtigte. So wurden sämtliche Server-Komponenten bzw. -Dienste auf die Anforderungen der Clients angepasst, insbesondere hinsichtlich zentraler Administration, Datenhaltung, Update-Fähigkeit der Clients und dynamischer Benutzerkonfiguration. Bei der dynamischen Benutzerkonfigura-

tion werden dem Arbeitsplatzrechner erst bei der Anmeldung eines Benutzers (Users) bestimmte Konfigurationsparameter (z.B. ob ein Benutzer ein Zugriffsrecht auf ein CD-ROM-Laufwerk hat oder nicht) übergeben.

Im Feinkonzept wurde festgelegt, dass die Konfiguration der einzelnen Arbeitsplatzrechner ausnahmslos von zentraler Stelle über einen Administrationsserver erfolgt, also keine Administration (Einstellen von Druckertreiber, Grafikauflösung, auf dem Rechner vorhandene Software) lokal am Arbeitsplatz zu tätigen ist. Deshalb sollte auch das Administrationswerkzeug entsprechend einfach bedienbar sein, denn die Administratoren sollten ja nicht in kürzester Zeit zu Linux-Profis ausgebildet werden, sondern mit einfachen Mitteln alle notwendigen und wünschenswerten Aufgaben erledigen können. Ziel der Client-Migration war der Austausch der vorhandenen Applikationen durch gleichwertige OSS-Applikationen oder solchen, 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“ per qualifiziertem Mitarbeiter am jeweiligen Arbeitsplatz weitgehend unterbleiben können. Gleichzeitig sollten für die sensiblen Daten eine zentrale Datensicherung und eine den hohen Sicherheitsanforderungen der Monopolkommission gerecht werdende Zutrittsbeschränkung zu den Daten implementiert werden. Die Anschaffung von neuer Client-Hardware sollte soweit als möglich unterbleiben.

2. Das Konzept

2.1. Der Client als Basis

In den ersten zwei Wochen des Projektes trafen sich die Projektbeteiligten, um aus dem „2-Seiter“ der Ausschreibungsunterlagen und dem angebotenen Konzept der ausführenden Firmen ein Feinkonzept zu erstellen, das die weiteren Arbeiten bestimmen sollte. Bereits in der Ausschreibung war definiert, dass die Migration eine Migration von so genannten FatClients¹ sein sollte, denn als Clients sollten die handelsüblichen PCs zum Einsatz kommen, die bereits seit ca. 2 Jahren im Einsatz waren. Die Clients selbst sollten die Applikationen vorhalten und ihre Prozessorleistung zur Ausführung dieser einsetzen. Auch die Druckaufbereitung, das Scannen von Daten, die Webcam u. v. m. sollten vom PC übernommen werden. Alle Applikationen der Monopolkommission, die auf dem Betriebssystem Windows 2000 lauffähig waren, wurden durch Open-Source-Software (OSS) oder OSS-lauffähige Applikationen ersetzt. Einzige Ausnahme ist eine von der Firma Hoppenstedt erstellte CD-ROM für Firmendaten, deren Applikation Einträge in eine Windows-Registry², der zentralen Datei für die Registrierung von Programmen im Windows-Betriebssystem, vornimmt, damit die Programme unter anderem alle Betriebssystemfunktionen nutzen können. Jedoch auch hier konnten die Erfahrungen der Mitarbeiter

¹ FatClient ist ein voll ausgestatteter PC, im Gegensatz dazu ist ein ThinClient ein Gerät ohne Festplatte und lokale Applikationen.

² Mehr zur Registry unter http://www.zdnet.de/downloads/weekly/7/weekly_143-wc.html.

eines anderen Pilotprojektes (Bundeskartellamt³) genutzt werden, um diese Applikation unter WINE⁴ (einer Emulation, die auf einem Linux-System einer für Windows entwickelten Software eine entsprechende Umgebung zur Verfügung stellt) verfügbar zu machen.

Im Unterschied zu Windows 2000 stehen unter GNU/Linux verschiedene Fenstermanager zur Auswahl, die zum Einsatz kommen könnten. Bereits im Angebot wurde der IceWM⁵ als Fenstermanager vorgeschlagen, da sich die Optik sehr an Windows 9x, NT und 2000 anlehnt und auch die gewohnten Tastaturbefehle, wie ALT-F4 für das Schließen eines Fensters, vorbestimmt sind. Als Applikation geht er auf dem Client moderat mit den Systemressourcen, wie z.B. Prozessor oder Arbeitsspeicher, um. Die „Desktop“-Funktionalität, d. h., dass Programm-Icons auf der Oberfläche liegen und per Mausklick die damit verbundenen Programme gestartet werden können, wird nicht über den IceWM bereit gestellt, sondern durch den Filebrowser GNOME Midnight Commander⁶.

Als Office-Applikation wurde Staroffice 6.0 ausgewählt, welches zwar auf dem Open-Source-Produkt Openoffice basiert, jedoch selbst nicht Open-Source-Software ist, da lizenzpflichtige Produkte wie eine Datenbank oder eine Rechtschreibprüfung hinzugefügt wurden. Ausschlaggebend für den Einsatz von Staroffice 6.0, alternativ zu Openoffice, war die Rechtschreibprüfung. Da in der Monopolkommission kein anderes 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 Latex⁷, einem auf dem Textsatzsystem TeX⁸ basierenden Werkzeug, um Texte zu verfassen und zu layouten, zu arbeiten.

Für das Suchen von Dateien steht 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) sowie das Öffnen der darin befindlichen Dateien, ohne auf ein entsprechendes Archivierungswerkzeug zurückgreifen zu müssen.

Für die Mail-Funktionalität 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 Signatur⁹ zur eindeutigen und rechtssicheren Unterschrift von Dokumenten oder auch E-Mails eingeführt werden sollte, wurde ein einfach zu bedienender Mail-Client gesucht, der neben der leicht zu bedienenden grafischen Oberfläche auch die Unterstützung für

³ Vgl. <http://www.bundeskartellamt.de>.

⁴ Vgl. <http://www.winehq.com/>.

⁵ Vgl. <http://www.icewm.org>.

⁶ Vgl. <http://www.ibiblio.org/mc/>.

⁷ Vgl. <http://www.dante.de>.

⁸ Vgl. <http://www-cs-faculty.stanford.edu/~knuth/>.

⁹ Vgl. <http://www.bund.de/Gut-zu-Wissen/Kommunikation-und-Medien/Internet/Elektronische-Signatur-.7482.htm>.

GNUpG¹⁰ als digitaler Signatur bot. Die Entscheidung für einen Standardarbeitsplatz fiel auf Sylpheed¹¹.

Als Browser standen ebenfalls einige Applikationen zur Auswahl: Konquerer, Mozilla, Galeon. Da die Funktionen zum Durchsuchen von Internetseiten mindestens den Umfang der bisher (MS Internet Explorer) zur Verfügung stehenden Applikation haben sollte, war Mozilla auf Grund der umfangreichen Funktionen auch in Bezug auf Plug-Ins, wie z.B. Macromedia Flash, schon ein Favorit als Browser, da jedoch die Mail-Funktionen von einer anderen Applikation übernommen würde, wurde bei den Testnutzern Galeon eingesetzt. Schnell fanden sich die Testnutzer zurecht, und somit wurde Galeon¹², der auf der „Rendering-engine“, der Grafikdarstellungs-Software von Mozilla, basiert, gewählt.

Bisher kamen ein vom Scanner-Hersteller mitgeliefertes Programm Adobe Photoshop LE (Limited Edition) und der entsprechende Windows-Treiber zum Einsatz. Da für den Scanner ein Treiber für Linux bereitstand, wurde nur noch nach einer Scanner-Software unter Linux gesucht. SANE (Scanner Access Now Easy, Frontend Xsane)¹³ wurde den Testbenutzern zur Verfügung gestellt, und nachdem die bisher genutzten Funktionen über SANE ebenfalls verfügbar waren, 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 GIMP¹⁴ eingerichtet. Dort kann man wie gewohnt unter dem entsprechenden Menüpunkt ein Bild scannen.

Für die Erstellung von pdf-Dokumenten wurde auf Basis des Betriebssystems Windows 2000 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 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.

Mit den hier beschriebenen Elementen war der Arbeitsplatz-PC in seiner Grundausstattung als Linux-PC erstellt. Dass die Arbeiten damit nicht abgeschlossen waren, sondern lediglich die Basis der Lösung erstellt wurde, zeigen die im Folgenden geschilderten Details der Lösung.

2.2. 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 Si-

¹⁰ Vgl. <http://www.gnupg.de/>.

¹¹ Vgl. <http://www.sylpheed.org>.

¹² Vgl. <http://www.gnome.org/gnome-office/galeon.shtml>.

¹³ Vgl. <http://www.sane-project.org/>.

¹⁴ Vgl. <http://www.gimp.de/>.

cherheitsmerkmalen zu einer Erhöhung der Fälschungssicherheit einer Authentifizierung führt. Ergebnis war die Kombination von Chipkarte und Fingerabdruck.

Für die Erstellung von Chipkarten, zum Erfassen von Fingerabdrücken und zur Erstellung der Digitalen-Signatur-Daten wurde eine integrierte Applikation erstellt. Mit der Applikation kann man über eine grafische Oberfläche sehr leicht eine Chipkarte erstellen, die für die digitale Signatur und zur Authentifizierung bei der Anmeldung am Arbeitsplatz genutzt wird. Die Gewinnung der Biometriedaten wird dabei über ein Produkt der Siemens AG¹⁵ durchgeführt, welches nicht quelloffen zur Verfügung steht. Die Daten, die per Minuzien-Verfahren¹⁶ aus einem gescannten Fingerabdruck gewonnen werden, liegen verschlüsselt auf dem Webserver.

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

Unter der „Online“-Umgebung wird die Netzwerkumgebung verstanden, bei der folgende Voraussetzungen gelten. Zum einen muss ein Arbeitsplatzrechner eine physische Verbindung zum Netzwerk haben (Netzwerkkabel). Zum anderen 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 Netzwerkanmeldung am Arbeitsplatz möglich. Der Benutzer erkennt dies an der Anmeldemaske. Er findet dann nicht die gewohnte Anmeldemaske mit grünem Schriftzug vor, sondern eine spezielle „Offline“-Anmeldemaske mit rotem Schriftzug „offline“.

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.

Als Client ist also auch ein Laptop einsetzbar, der ja nicht immer im Netz sein muss, der jedoch über die Administration zentral mit allen Diensten und Applikationen versorgt wird, sobald er sich im Netzwerk befindet.

2.3. 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 Ägypten¹⁷ über ein Open-Source-Projekt verfügt, das den Standard nach Sphinx¹⁸ zur Erstellung einer Public-Key-Infrastruktur (PKI) erfüllt, sollte wenn möglich die digitale Signatur auf Grund 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

¹⁵ Seit 1.10. 2003 hat die Firma Bromba GmbH (<http://www.bromba.de>) die Technik von der Siemens AG übernommen.

¹⁶ Vgl. <http://www.fraunhofer.de/german/publications/df/df1998/198-30.htm>.

¹⁷ Vgl. <http://www.bsi.de/aufgaben/projekte/sphinx/aegypten/opensour.htm>.

¹⁸ Vgl. <http://www.bsi.de/aufgaben/projekte/sphinx/index.htm>.

waren, wurde die digitale Signatur in Form von GnuPG-Schlüsseln realisiert. Dabei werden die GnuPG-Daten verschlüsselt auf der Chipkarte abgelegt.

2.4. Die Serverumgebung

Das Konzept beinhaltetete von Beginn an einen zentralen Ansatz für die wesentlichen Komponenten. Erst durch die zentralen Komponenten, die auf den reibungslosen Einsatz der Linux-PC-Arbeitsplätze abgestimmt wurden, konnte die leicht zu administrierende Umgebung die gesteckten Ziele (einfache Administration bei höherer Sicherheit der Arbeitsumgebungen) erreichen. Dabei wurden die grundsätzlich auf verschiedenen Servern liegenden Funktionen so angepasst, dass sie sich im Rahmen des Projektes auch auf einem einzigen Server installieren lassen.

Bei der INFRApliance Administration Console¹⁹ handelt es sich um ein webbasiertes Werkzeug, mit dem alle wesentlichen Parameter für die Server, Clients, Applikationen und Benutzer administriert werden können. Die Administration Console unterstützt in der IT-Umgebung die zentrale Verwaltung von

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

Damit wurde die Administration Console Angelpunkt für die umfangreichen zentralen Funktionen, die in dem Konzept zur Verfügung stehen. Der INFRApliance Fileserver²⁰ speichert in der Monopolkommission alle von den Benutzern erstellten Daten in deren „Home“-Verzeichnissen ab. Gleichzeitig sind für den Austausch von Daten oder das Zusammenarbeiten von Mitarbeitern Gruppenverzeichnisse angelegt, in die die Mitglieder einer Gruppe Dateien legen und aus denen sie sie auch lesen können. Integriert ist ein Backup-Modul, mit dem die Daten des Fileservers gesichert und rückgesichert werden können.

Der INFRApliance Webserver²¹ hat verschiedene Aufgaben. Zuerst dient er als Webserver für die zentralen Webapplikationen, die im Rahmen des Projektes entstanden sind. Zusätzlich werden die Intranetseiten der Monopolkommission über den Webserver zur bereitgestellt. Im Zusammenhang mit der Softwareverteilung stellt der Webserver die Softwarepakete zur Verfügung. Für die Webapplikationen jedoch auch für andere Applikationen sind auch die Datenbanken (PostgreSQL, MySQL) hier implementiert. Die drei Server und die ergänzenden Module wurden innerhalb des Projektes so erstellt bzw. ergänzt, dass die gesamte Rechnerlandschaft (Clients und Server) von der Administration Console aus zu administrieren ist. Dabei basiert die Oberfläche der Administration Console auf der Open-Source-Software (OSS) Webmin²². Die Weboberfläche gestattet die Administration der Clients und Server unabhängig vom Standort des Administrators von jedem im Netzwerk befindlichen Arbeitsplatzrechner.

¹⁹ Vgl. <http://www.sfi-director.org>.

²⁰ Vgl. <http://www.sfi.ch>.

²¹ S.o.

²² Vgl. <http://www.webmin.de/>.

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, sodass bei der Anmeldung eines Benutzers die entsprechenden individuellen Einstellungen für den beliebigen Arbeitsplatz zur Verfügung stehen.

2.5. Zentraler Ansatz

Für die Kosten des Betriebs einer IT-Infrastruktur sind eine ganze Reihe von Faktoren von Bedeutung. Neben den Lizenzkosten für Betriebssysteme 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 erst 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, und die aktuellen Konfigurationen jederzeit eingesehen werden können, d. h., das System jederzeit definiert ist, und letztlich auch noch die „Fernwartung“ über systemeigene Mechanismen mit Linux möglich ist, dann kommt mit der zentralen Administration und Datenhaltung bei dezentraler Verfügbarkeit von Rechenleistung lokal am Arbeitsplatz derzeit ein Optimum an Kosten senkenden Faktoren zusammen.

Die Benutzerdaten (z.B. Name, User ID, Group IDs) und Benutzereinstellungen für Applikationen werden über die Administration Console angelegt und administriert. Ebenfalls werden weitere Einstellungen der Hardwarekonfiguration der Clients über die Administration Console auf dem LDAP-Server²³ abgelegt. Die Daten werden automatisch bei Installation der Clients oder über das entsprechende Modul der Administration Console manuell registriert. Die vom Client automatisch erkannten Hardwaredaten (Grafikkarte, Grafikkartentreiber und Monitoreinstellungen) werden gespeichert.

Der Administrationsserver stellt auch die Verwaltung der für die Clients vorgesehenen Softwarepakete zur Verfügung. Die Daten der Benutzer werden zentral auf dem Server im INFRAppliance 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.

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 gepackt, die den Clients zur automatischen Installation zur Verfügung gestellt werden. Beim Starten des Rechners werden der Softwarestand des Clients

²³ Vgl. <http://verzeichnisdienst.de/ldap/>.

überprüft, und eventuell zur Verfügung stehende Softwarepakete automatisch heruntergeladen und installiert. Die Möglichkeit, auch manuell Softwarepakete auf die Clients zu laden, bleibt dabei erhalten.

2.6. Spezielle Aufgaben

Neben der 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 allen Mitarbeitern der Monopolkommission per Webbrowser zur Verfügung stehen.

2.6.1. Bibliotheksverwaltung

Da die Monopolkommission eine eigene Bibliothek besitzt, wurde zur Verwaltung des Bücherbestandes der Bibliothek ein Katalog mit Weboberfläche erstellt, mit dem jeder berechtigte Mitarbeiter von seinem Arbeitsplatz aus die Liste der verfügbaren Bücher einsehen und nach Büchern mit bestimmten Attributen durchsuchen kann. Die Weboberfläche 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.

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.

2.6.2. 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 Weboberfläche 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. Die Weboberfläche 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. Folgende Funktionen wurden in der Applikation verwirklicht:

- Durchsuchen des CD-Bestands 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).

2.6.3. Kalender

Vor der Migration wurde in der Monopolkommission kein elektronischer Kalender mit seinen verschiedenen Möglichkeiten, z.B. der Terminabstimmung, eingesetzt. Im Rahmen der Migration wurde zur Abstimmung von Terminen mit der PHP-Groupware²⁴ ein Terminkalender per Weboberfläche 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.

2.6.4. Adressbuch

Die Aufgabenstellung im Zusammenhang mit dem Adressbuch war geprägt von unterschiedlichen Anforderungen und unterschiedlichsten Datenquellen für die Mitarbeiter der Monopolkommission. Der Informationsverbund der Bundesbehörden (IVBB²⁵) sollte berücksichtigt werden – genauso wie der hauseigene Adressbuchansatz des Bundeskartellamtes. 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 damit eine Auswahl verschiedener „Adressbücher“ zur Verfügung, die über die Datenbankanbindung von Staroffice auch für Serienbrieffunktionen genutzt werden kann.

2.6.5. 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. Stattdessen 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 Problem

²⁴ Vgl. <http://phpgroupware.org/>.

²⁵ Vgl. <http://www.ivbb.de>.

stellungen zu identifizieren und dann Methoden und Werkzeuge auszuwählen, mit denen die Mitarbeiter ihre Aufgaben, unter anderem der Datenauswertung und -zusammenstellung, 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 MS 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 denselben Gründen, aus denen dieses relationale Datenbanksystem auch für die Webapplikationen ausgewählt worden war und um nicht unnötigerweise ein zusätzliches System einzuführen. Als Programmiersprache wurde wie bei den Webapplikationen Perl gewählt, wobei hier die herausragenden Fähigkeiten zur Textextraktion (wichtig bei der Verarbeitung von Daten aus externen Quellen), die Vielfalt an hochwertigen und 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 MS 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, sodass ihre Motivation und Bereitschaft zur Kooperation entsprechend hoch waren und das angestrebte Ziel weitgehend erreicht werden konnte.

3. Der Ablauf der Migration

Bereits bei der Bieterkonferenz waren Mitarbeiter, also spätere „User“ der Lösung, anwesend. Im Rahmen des Projektes wurden sehr schnell (innerhalb der ersten vier Wochen) einzelne Mitarbeiter mit Linux-Arbeitsplätzen ausgestattet, die von den Applikationen her dem finalen Client sehr nahe kamen. Dabei konnten die Mitarbeiter die Applikationen sehr früh testen und entsprechende Anregungen geben. Die im Rahmen des Feinkonzeptes ausgewählten Applikationen waren bereits sehr auf die Eignung hin geprüft und ausgewählt worden. Die gewählten Sicherheitsmechanismen des Einsatzes der Biometrie und der Chipkarte waren der deutlichste Beleg für die Umstellung an sich.

Die eigentliche Umstellung der Arbeitsplätze (Clients) und der Serverumgebung konnte auf Grund der vielen Vorarbeiten erst sehr spät im Projektablauf erfolgen, genau gesagt, zwei Wochen vor Projektende. Die Migration der Serverumgebung ging dabei in zwei Schritten vonstatten. Zuerst wurden 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 dem zentralen Fileserver abzulegen. Für den eigentlichen Migrationstag wurde ein Freitag ausgesucht, da die Mitarbeiter im Zusammenhang mit der Migration zum Erfassen der Fingerprintdaten einbestellt werden mussten. Die mit Fingerabdruck erfassten Mitarbeiter konnten daraufhin an ihren Arbeitsplätzen arbeiten. Für die Mitarbeiter wurde eine kurze Einweisung für die Anmeldung mit Chipkarte und Biometrie gegeben. Am folgenden Montag standen Mitarbeiter von natural computing 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. Auf Grund 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 der Monopolkommission nicht vor Ort waren. Dabei wurde ein modularer Aufbau für die Schulung gewählt. Es wurden kleine Abschnitte gewählt, um dem Mitarbeiter Zeit fürs 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“ aufwändiger als erwartet, da die Datenvolumen der einzelnen Arbeitsplatzrechner („Laufwerk C“) im Vorfeld nur geschätzt werden konnten.

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 Sonnabend auch den Server zu migrieren. Für den Fall, dass dabei Probleme auftreten würden, hätte man auf die bereits vorhandene INFRApliance-Umgebung in der Testumgebung zurückgreifen können. Doch die Migration lief im Wesentlichen problemlos, sodass 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 Backup-Versuch 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. Seitdem läuft der Server im Produktivsystem.

Die Nutzer arbeiten bereits seit dem 28. Oktober 2002 im Produktivsystem. Die bei der Anmeldung für den E-Mail-Verkehr zur Verfügung gestellte GnuPG-Signa-

tur wird von der Chipkarte über die per USB angeschlossene Tastatur dem Client zur Verfügung gestellt. Dieser Vorgang dauert ca. zehn bis 15 Sekunden. Nicht jeder Mitarbeiter war mit dieser Komforteinbuße zufrieden.

Das Projekt beinhaltete auch den Support der Lösung bis zum 30. Juni 2003. In dieser Zeit standen den Mitarbeitern Hotline- und E-Mail-Support zur Verfügung sowie eine Anzahl von Tagen vor Ort, um eventuell auftretende Probleme und Anforderungen bearbeiten zu können. Die Mitarbeiter nahmen alle Arten des angebotenen Supports wahr. Gegenstand der Supportanfragen war dabei nur zum kleineren Teil auf das System an sich bezogen, zum größeren auf Funktionalitäten aus den eingesetzten Applikationen.

Selbstverständlich konnte auch während des Projektes nicht jeder Prozess in der Monopolkommission so untersucht und aufgenommen werden, wie man sich das wünschen würde, dazu stand für das gesamte Projekt viel zu wenig Zeit zur Verfügung. Also kamen im Rahmen des Supports auch Dinge ans Licht, die nicht berücksichtigt waren. Doch die Anfragen konnten in der Regel sehr schnell und auch fast durchweg mit einer Lösung beantwortet werden.

Die Anfrage nach speziellen Programmen, die einzelne Mitarbeiter einsetzen wollten, konnte nicht immer positiv beantwortet werden, da leider nicht jede Applikation für Linux existiert bzw. nicht jede Applikation mithilfe von Emulatoren unter Linux funktioniert. Doch konnten einige Alternativen angeboten werden.

Was interessanterweise nicht zu einer Supportanfrage führte, war zu Beginn des Jahres der Stromausfall im Haus der Monopolkommission. Die Systeme starteten nach dem Stromausfall ohne Probleme.

Die nächsten Schritte sind die Implementierung der VPN-Lösung (Virtual-Private-Network), mit der die Mitarbeiter über eine sichere Verbindung auch von außen über das Internet auf ihre Daten in den Räumen der Monopolkommission zugreifen können, das Update der Office-Umgebung oder eine Implementierung der Funktion „Faxen aus Staroffice“ oder anderen Applikationen heraus.

4. Fazit

Der Autor sieht sich hier nicht im Stande, die Zufriedenheit aus Sicht der Benutzer wiederzugeben. Diese können nur die Mitarbeiter der Monopolkommission selbst darstellen. Jedoch können die Häufigkeit der Anfragen und die Tiefe der Fragestellungen einen sicheren Hinweis darauf geben, dass die Migration der Monopolkommission auf Open-Source-Software (OSS) gelungen ist.

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 und tritt im Tagesgeschäft nicht störend zu Tage.

Das Ergebnis der Arbeiten ist eine in fast allen Bereichen unter der *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.

Die Ergebnisse der Migration wurden nach Abschluss der Arbeiten bei der Erstellung des Migrationsleitfadens durch die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt.) verwendet.

Bei dem Projekt ist herauszuheben, dass es sich zum ersten Mal um die Komplettmigration einer Bundesbehörde handelt, die exemplarisch nachweisen sollte, dass auch eine komplette Arbeitsumgebung auf Open-Source-Software migriert werden kann. Doch sollte man nicht übersehen, dass auf Grund der außerordentlichen zeitlichen Restriktionen nicht jeder Prozess in der Monopolkommission simuliert werden konnte und auch zukünftige Entwicklungen nur in begrenztem Maß einbezogen werden konnten. So ist nicht auszuschließen, dass in Zukunft die eine oder andere Applikation, die nicht für Linux zur Verfügung steht, auf einer anderen Plattform genutzt werden muss.

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

Eine weitere Implementierung für 95 Arbeitsplätze hat inzwischen beim Landesrechnungshof Mecklenburg-Vorpommern stattgefunden. In 15 Arbeitstagen konnte dort die Lösung mit einigen Anpassungen implementiert werden. Die Umstellung der Clients und die Schulung der Mitarbeiter auf die neuen Arbeitsplätze wurden von den Mitarbeitern des Landesrechnungshofes in Eigenregie durchgeführt und dauerten rund 6 Wochen.

Vorstellung Natural Computing GmbH:

Die Natural Computing GmbH wurde 2001 von fünf Personen mit unterschiedlichen Schwerpunkten im Bereich der IT-Branche gegründet, um mit dem Fokus auf den Einsatz von Linux am Arbeitsplatz am Markt tätig zu sein. Langjährige Erfahrungen aus verschiedensten Bereichen von IT-Systemen und Dienstleistungen wurden gebündelt, um Kunden integrierbare Lösungen auf Basis von Debian GNU/Linux anzubieten.

Natural Computing bietet seinen Kunden aus Mittelstand und öffentlicher Beratung die Entwicklung sowie Implementierung von Linux-Arbeitsplatzlösungen.und

Beispiel einer Migration von Windows 2000 auf Open-Source-Software

ist Mitglied des LIVE Linuxverband e.V., der Autor ist Mitglied des Vorstandes des LIVE.