

Das Windows-Netzwerk der Verwaltung

Irene Neumann
irene.neumann@cms.hu-berlin.de

Boris Masinovsky
boris.masinovsky@cms.hu-berlin.de

Vorbemerkungen

In diesem Artikel wird die Lösung vorgestellt, mit der seit April 2005 das bisherige Netzwerkbetriebssystem Banyan VINES der Verwaltung der HU abgelöst wird. Das Vorhaben ist alternativlos und dringend, da die Herstellerfirma nicht mehr existiert und damit keinerlei Support und auch keine Weiterentwicklungen möglich sind.

Die Projektgruppe für die Ablösung des Netzwerkbetriebssystems Banyan VINES der Verwaltung setzte sich das Ziel, nicht nur den Ersatz, sondern gleichzeitig eine Verbesserung des IT-Services zu erreichen. Folgende Ziele wurden definiert:

- Gewährleistung der erforderlichen Sicherheitsstandards,
- Bereitstellung von ausreichendem Speicherplatz für alle Benutzer im Netzwerk und Einbeziehung möglichst aller Benutzerdaten in die Datensicherung,
- Einführung der weitgehenden Austauschbarkeit der Arbeitsplatzrechner,
- Einführung aktueller netzbasierter IT-Lösungen und Nutzung aktueller Software,
- hohe Verfügbarkeit der IT-Systeme und der Netzlaufwerke und
- Verbesserungen der abteilungsübergreifenden Arbeiten innerhalb der Verwaltung, der Arbeitsfähigkeit – auch bei Netz- bzw. Serverstörungen – und der gemeinsamen Druckernutzung.

Diese Ziele sollen auf der Basis moderner und zukunftssicherer Technologien erreicht werden.

Der Artikel beschreibt die Komponenten des Verwaltungsnetzes der HU, ohne die in Zukunft kaum eine Anwendung funktionieren wird. Die überfällige Ablösung des alten Netzwerkbetriebssystems wird genutzt, um ein neues Gesamtkonzept, basierend auf aktuellen Technologien, zu erarbeiten und umzusetzen. Kern der neuen Lösung ist ein Windows-Netzwerk.

Warum ein eigenes Windows-Netzwerk für die Verwaltung?

Welches Netzwerkbetriebssystem?

Im Rahmen des CMS-Projektes »VINES-Ablösung in der HU« wurde nach umfangreicher Prüfung von Alternativen entschieden, ein Windows-Server-Netzwerk als zentralen Service in der HU einzusetzen. Zum Zeitpunkt der Entscheidung stand kein anderes geeignetes System für ein großes Netzwerk, wie das der HU, zur Verfügung. Seit Oktober 2003 befindet sich das Windows-Netzwerk der HU in Produktion.

Diese Entscheidung wurde für die besonderen Bedingungen der Verwaltung, beispielsweise durch Testinstallationen von UNIX und Samba, verifiziert. Folgende Kriterien führten zur Entscheidung für den Einsatz eines Windows-Netzwerkes in der Verwaltung:

- Für die überwiegende Mehrzahl der ca. 80 verwaltungsspezifischen Anwendungen existieren nur Systeme, die Windows als Betriebssystemgrundlage verlangen,
- die Kernsysteme der Verwaltung – Datenbankanwendungen der HIS GmbH [1] für ca. 150 Mitarbeiter – wurden durch den Hersteller auf Windows-basierte Versionen umgestellt,
- bei Einsatz anderer Technologien hätte eine Windows-Umgebung, z. B. für den Einsatz von Windows-Terminalservern, in jedem Fall mit zusätzlichen Ressourcen aufgebaut werden müssen,
- andere Netzwerkbetriebssysteme hätten Eigenentwicklungen, z. B. für die Benutzer- und Rechteverwaltung, erfordert, waren noch nicht ausgereift

oder erfüllten die Anforderungen nicht, und

- durch den Einsatz gleichartiger Technologien ergeben sich Synergieeffekte im CMS.

Durch Testarbeiten zeigte sich, dass das Nachfolgesystem von Windows 2000, Windows Server 2003, inzwischen ausreichend stabil war und deutliche Vorteile beim beabsichtigten Einsatz von Terminalservern, Systemrichtlinien, VPN-Technologien und von Smartcards als Authentifizierungsmöglichkeit bot.

Es wurde entschieden, im Verwaltungsnetz das Netzwerkbetriebssystem Windows Server 2003 einzusetzen.

Warum ein eigenes Netzwerk?

Die Datenverarbeitung der Universitätsverwaltung (UV) unterliegt besonderen Sicherheitsanforderungen. Sie muss zum Beispiel den Erfordernissen der Verarbeitung von vertraulichen und personenbezogenen Daten (Datenschutzgesetz) Rechnung tragen. Es ist unabdingbar, die Daten und Dienste vor Kompromittierung, Missbrauch und Datenverlust zu schützen.

Ein Weg, der ebenfalls in Hochschulen gegangen wird, ist die völlige Trennung der IT-Infrastruktur der Verwaltung von Außennetzen. Das bedeutet aber auch Verzicht auf Informationen und moderne Formen der Zusammenarbeit. Das war für die HU auf Dauer nicht akzeptabel.

In zwei Forschungsprojekten, die der DFN-Verein im Zeitraum von 1997 – 2003 förderte, wurde ein Konzept für den Anschluss einer modernen Verwaltung unter sicheren Bedingungen an das Internet erarbeitet. Lösungen wurden entwickelt, mit denen im geschlossenen sicheren Verwaltungsbereich externe Dienste genutzt oder mit denen Dienste der Verwaltung externen Benutzern bereitgestellt werden können.

Leider konnte diese Projektreihe trotz positiver Evaluierung nicht fortgesetzt werden, da das Förderungssystem umgestellt wurde und es bisher nicht gelang, andere Förderträger zu gewinnen.

Innerhalb der Forschungsprojekte wurde das vorher lokale Verwaltungsnetz mit dem Netzwerkbetriebssystem Banyan

VINES über eine vielschichtige Server- und Kommunikationsstruktur (mit dem Firewall-System als Kern) an das Netz der HU angeschlossen.

Es musste nun entschieden werden, ob sich die Verwaltung in das Windows-Netzwerk der HU mit eigenen Domänen integrieren kann oder ob ein eigenes Windows-Netzwerk erforderlich ist, damit die Sicherheit des Verwaltungsnetzwerkes gewährleistet werden kann.

Dazu wurden Windows-Server-Testsysteme implementiert, sichere Verbindungen zwischen Domänen über Virtual Private Networks (VPN) getestet und eine Prinziplösung für ein neues Firewall-System entwickelt. Die Lösung erwies sich als ausgesprochen komplex und aufwändig, aber prinzipiell einsetzbar.

Leider musste Microsoft gegen Ende des Testzeitraums offiziell bestätigen, dass Domänen als Teile von Windows-Netzwerken nicht vor administrativen Zugriffen aus anderen Domänen geschützt werden können. Da an der HU Domänen nicht – wie in Firmen üblich – nur zentral, sondern auch dezentral verwaltet werden, kam eine Integration der Verwaltungsdomäne in den Baum der HU nicht mehr infrage. Die Fakultäten und Institute unterliegen aufgrund der anderen Zielsetzung ihrer Tätigkeit in den meisten Fällen nicht den strengen Sicherheitsrestriktionen wie die Verwaltung. Das notwendige Sicherheitsniveau kann so nicht mehr gewährleistet werden. Für die Verwaltung wurde deshalb ein getrenntes Windows-Netzwerk eingerichtet.

Was wird abgelöst?

Folgende Dienste des Netzwerkbetriebssystems Banyan VINES sind gegenwärtig noch im Einsatz und werden abgelöst:

- *Benutzerverwaltung*

Das neue Konzept der Benutzerverwaltung integriert die Verwaltung von Benutzeraccounts der UV in das Konzept des CMS. Die Benutzeraccounts der UV werden in der zentralen Account-Datenbank des CMS verwaltet. Ziel ist es, langfristig die Teilnahme der UV an einem künftigen zentralen Identitätsmanagement der HU zu ermöglichen. Die interne Struktur wird nach den ge-

meinsam entwickelten Prinzipien des HU-Windows-Netzwerkes entworfen. Sie wird so konzipiert, dass neue Anforderungen der Verwaltung, wie die integrierte Zusammenarbeit über Referats- und Abteilungsgrenzen hinweg, leichter realisiert werden können. Teile der Benutzerverwaltung werden automatisiert.

- *VINES-Filedienste*

Die Struktur der VINES-Filedienste wird vollständig überarbeitet. Durch den Einsatz der modernen Technologie eines Storage Area Network (SAN)[2] ist es möglich, im Wesentlichen inhaltlich und unabhängig von technischen Restriktionen zu planen. Die Speicherkapazität der ersten Ausbaustufe umfasst ca. 1,5 Terabyte. Die persönlichen Daten der Benutzer werden auf Netzlaufwerken gespeichert und zusätzlich automatisiert verschlüsselt lokal abgelegt. Damit stehen sie auch bei Zugangsproblemen zur Verfügung. Wichtige nutzerbezogene Systemdaten werden auf Netzlaufwerke umgeleitet und erleichtern die Weiterarbeit an anderen PCs. Die komplizierte Rechtestruktur der bisherigen Filesysteme wird in Zusammenarbeit mit den Referaten und Abteilungen mit dem Ziel überarbeitet, übersichtlichere und effektivere Strukturen zu erhalten. Durch die Verlagerung der lokalen Daten auf die Netzlaufwerke ist es möglich, Benutzerdaten automatisiert zu sichern.

- *netzwerkbasierte Anwendungen*

Sofern möglich, werden netzwerkbasierte Anwendungen zentral bereitgestellt. Die Anwendungen werden nur noch auf den Terminalservern einer Serverfarm installiert. Auf den Arbeitsplatzrechnern muss lediglich ein Zugangsclient administriert werden. Nur mit dieser Technologie ist es noch möglich, die erforderlichen Änderungen in den Anwendungen zu bewältigen. Den Schwerpunkt bilden dabei die Kernsysteme der Verwaltung, die Datenbankanwendungen der HIS GmbH für ca. 150 Mitarbeiter.

- *Netzwerkdruckdienste*

Für die Netzwerkdruckdienste existieren zwei Lösungen. Für kleine Arbeitsgruppen sind Drucker vorgesehen, die direkt an das Netzwerk angeschlossen werden. Hochleistungsdrucker, Dru-

cker für spezielle Formate oder Drucker für einen größeren Benutzerkreis werden über einen Printserver zentral verwaltet und den berechtigten Benutzern bereitgestellt.

• **NetBIOS-Dienst**

Der NetBIOS-Dienst wird für eine veraltete Spezialanwendung benötigt. Hier ist es sinnvoller, die Anwendung abzulösen, als eine Sonderlösung zu entwickeln.

Welche Dimensionen hat das Vorhaben?

Das Projekt

Nachdem das Konzept für die notwendige Ablösung der Banyan-VINES-Dienste feststand, wurde der Projektplan erstellt. Aufgrund des Umfangs des Projektes wurde für die Projektplanung und die Dokumentation der Projektrealisierung eine neue Technologie eingesetzt – das Web-basierte Wiki [3]. Die Projektbeteiligten nutzen das Wiki als Projektdokumentation, damit der aktuelle Stand für alle online verfügbar ist.

Im Projekt werden 550 Arbeitsplatzrechner ersetzt, ein Großteil der Server auf neue Versionen gebracht oder neue Serversysteme eingeführt. Basisdienste, ohne die das Windows-Netzwerk nicht funktionieren kann, müssen eingerichtet und über 80 betreute Anwendungen überprüft und im neuen System wieder funktionsfähig bereitgestellt werden.

Das bestehende Servernetzwerk unter Banyan VINES mit den notwendigen Ba-

sisdiensten wurde über Jahre aufgebaut. Jetzt ist es notwendig, den Austausch mit neuen Technologien neben dem Betrieb der Produktionssysteme und ohne größere Unterbrechungen zu bewältigen. Parallel dazu werden fast alle Datenbankanwendungen der HIS GmbH abgelöst sowie neue umfangreiche Systeme (siehe Artikel »Prüfungsanmeldung per Internet«) eingeführt.

Das Gesamtprojekt vorzustellen, würde den Rahmen des Artikels sprengen. An dieser Stelle sollen Schwerpunkte der Teilprojekte genannt werden.

Teilprojekt Planung und Leitung

Neben der Steuerung des Gesamtprojektes sind folgende Schwerpunkte im Teilprojekt enthalten:

- das Sicherheitskonzept,
- das Umstellungskonzept,
- das Schulungskonzept und
- die Dokumentationen.

Das Sicherheitskonzept musste durch den Einsatz neuer IT-Systeme und neuer Technologien völlig überarbeitet werden. Neue Funktionsprinzipien ergeben anders geartete Gefährdungen und erfordern spezielle Sicherheitslösungen, Backup-Lösungen und Produktionsabläufe.

Das Umstellungskonzept muss eine sanfte Migration in die neue Umgebung ermöglichen. Um den Datenaustausch innerhalb und zwischen den Abteilungen zu ermöglichen, wird bis zum Abschluss

der Umstellungsarbeiten neben dem Windows-Netzwerk auch das Banyan-VINES-Netz zur Verfügung stehen. Das Banyan-VINES-Netz wurde deshalb durch zwei StreetTalk-for-NT-Server erweitert. Die Umstellung der Benutzerzugänge und der Arbeitsplatzrechner erfolgt gruppenweise, um Beeinträchtigungen durch Arbeit in unterschiedlichen Umgebungen möglichst gering zu halten.

Für die Schulungen der Benutzer wurde eine Testumgebung eingerichtet. Die Schulungen werden durch Dozenten der Beruflichen Weiterbildung nach einem von der Projektgruppe ausgearbeiteten Schulungskonzept durchgeführt. Zusätzlich erfolgen arbeitsplatzbezogene Einweisungen bei der PC-Übergabe.

Teilprojekt Windows-Server

Das Teilprojekt Windows-Server umfasst neben dem Aufbau der Server und ihrer technischen Umgebung auch Teilbereiche wie:

- Entwurf der Domänenstruktur,
- Festlegung der Struktur und der Rechte der Filesysteme,
- das Betreuungskonzept mit der Benutzerverwaltung,
- Beschaffungen und Klärung von Standortfragen und
- den Aufbau von Testsystemen.

Teilprojekt Rechner-Installation

Im Teilprojekt Rechner-Installation werden die Arbeitsplatzrechner für das Windows-Servernetz aufgebaut, auch mit dem Ziel, den enormen Betreuungsaufwand zu senken. Dazu gehören:

- zentrale Beschaffungen einheitlich ausgestatteter Arbeitsplatzrechner,
- Entwicklung einer einheitlichen Standardinstallation und einer weitgehend automatisierten Lösung für die Installation der Arbeitsplatzrechner,
- Installationen von Zusatzsoftware erst nach Funktionsprüfung und nur durch geschultes IT-Personal,
- Einführung der serverbasierten automatischen Verteilung und Überwachung von Virens Scanner-Updates, Windows- und Office-Updates,
- Weiterentwicklung der Fernbetreuung,

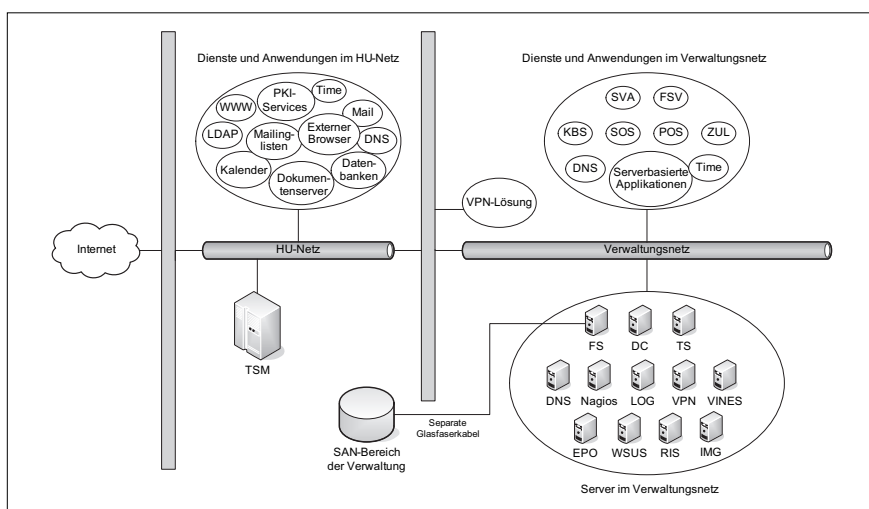


Abb. 1: Im Verwaltungsnetz benutzte Dienste und Anwendungen und dafür benötigte Server.

- Integration von serverbasierten Systemrichtlinien und
- Ablösung veralteter Anwendungen.

Jeder Benutzer, der in das Windows-Netz aufgenommen wird, erhält einen Arbeitsplatzrechner mit der Standardinstallation der Verwaltung. Näheres dazu finden Sie im Artikel »PC-Betreuung und Installation heute«.

Teilprojekt Terminalserver/HIS

Im Teilprojekt Terminalserver/HIS wird die Terminalserverfarm der Verwaltung mit allen erforderlichen Anwendungen bereitgestellt. Im Artikel »Verwaltungssoftware auf einer zentralen Terminalserverfarm« wird das Teilprojekt vorgestellt.

Im Rahmen des Teilprojektes wurden zusätzlich Terminalserverzugänge zur zentralen Farm des HU-Netzes für Benutzer des Verwaltungsnetzes bereitgestellt. Sie ermöglichen den Zugang zu einem unbeschränkten »externen Browser« und den Zugang zu CD-ROM-Recherchen.

Teilprojekt Vernetzungsstruktur/Sicherheit

Im Teilprojekt Vernetzungsstruktur/Sicherheit werden die übergreifenden Basisdienste weiterentwickelt bzw. konzipiert. Es umfasst Aufgaben wie:

- Anbindung des Verwaltungsnetzes an das zentrale Backup-System der HU und Einführung einer Verschlüsselungslösung im Backup-System,
- Konzept für die Namensauflösung (DNS) im Verwaltungsnetz,
- Einführung einer zentralen Serverüberwachung,
- Schaffung einer VPN-Lösung für Benutzer des HU-Netzes, die dedizierte Anwendungen des Verwaltungsnetzes benötigen,
- Austausch des Firewall-Systems, um den erweiterten Anforderungen gerecht werden zu können,
- neue Lösung für den Datenaustausch zwischen Benutzern des inneren Verwaltungs- und des äußeren HU-Netzes über Firewall-Grenzen hinweg und
- Überarbeitung der Vernetzungsstruktur des Verwaltungsnetzes und Installation aktueller Kommunikationstechnik.

Näheres zu einigen Themen wird in den Artikeln »Sicher auf die Datenautobahn« und »Von Einheit und Mannigfaltigkeit« in diesem Heft beschrieben.

Relativ schnell wurde klar, dass dieses Projekt die Kapazität der Projektgruppe übersteigt. Ein Einsatz von Fremdfirmen, wie in Unternehmen üblich, kam aus Kostengründen nicht infrage.

Dazu kam, dass bereits im April 2005 die Teile des Windows-Netzwerkes in Produktion gehen mussten, die für die Inbetriebnahme des neuen Anwendungssystems »Studierendendatenverwaltung (HISSOS-GX)« unabdingbar waren. Es war wirtschaftlich nicht tragbar und personell auch nicht möglich, nur für das Verwaltungsnetz ein Windows-Spezialistenteam mit 3 Mitarbeitern vorzuhalten, um auch bei Urlaub oder Krankheit die erforderliche hohe Verfügbarkeit des Windows-Netzwerkes zu gewährleisten. Neue Wege mussten gefunden werden.

Erstens wurde die Zusammenarbeit der Spezialisten des CMS für das Windows-Netzwerk, das SAN, das Backupsystem (TSM) [4] und die Kommunikationstechnik intensiviert.

Zweitens wurde die zentrale Windowsgruppe des CMS befristet verstärkt, so dass sie zusätzlich die Basisbetreuung der Domänencontroller und der Fileserver übernehmen konnte. Alles Übrige, wie die Benutzerverwaltung, die Anwendungsbetreuung, die Betreuung der Terminalserver, um nur einige Teile zu nennen, blieb weiterhin in der Projektgruppe für die Verwaltung.

Wie sieht es hinter den Kulissen aus?

Das Windows-Netzwerk der Verwaltung ist ein komplexes System, organisiert in einer Root-Domäne. Es wird durch eine Firewall gesichert und ist damit von den übrigen Windows-Netzen der HU getrennt. Zur Reduzierung von Ausfallzeiten durch mögliche Störungen von Hard- oder Software werden alle wichtigen Systeme redundant (mindestens 2-fach) aufgebaut. Es werden folgende Technologien/Dienste und Windows-Server-Komponenten eingesetzt:

- 2 Domain Controller (DC),

- 2 Fileserver (FS),
- 4 Terminalserver (TS),
- 2 interne DNS-Server,
- 2 Nagios-Überwachungssysteme,
- 2 Log-Server,
- VPN-Infrastruktur,
- Banyan-VINES-Dateidienste (Ablösung Ende 2006 bzw. Anfang 2007 geplant),
- McAfee ePolicy Orchestrator Server (EPO),
- Windows Server Update Service (WSUS) und
- Remote Installation Server (RIS).

Die Abbildung 1 zeigt eine Prinzipdarstellung des Verwaltungsnetzes.

Die Server befinden sich im Serverraum des CMS, Standort Mitte. Der Serverraum ist mit USV und Klimaanlage ausgestattet, die Server sind in 19"-Schränken untergebracht. Die Administration erfolgt über Konsolenswitches, die eine netzunabhängige Möglichkeit des Remote-Managements von Servern bieten.

Die Kernkomponenten des Windows-Netzwerkes sind die Domain Controller und File- bzw. Terminalserver, basierend auf Windows Server 2003. Die Domain Controller sind primär für die Anmeldung der Benutzer zuständig. Bei Ausfall eines Domain Controller sind Anmeldungen weiterhin möglich.

Auf einem Domain Controller läuft das Active Directory, der Verzeichnisdienst von Microsoft. Das Active Directory ordnet verschiedenen Netzwerkobjekten wie Benutzern, Servern und Arbeitsplatzrechnern unter anderem Eigenschaften zu und verwaltet diese.

Weitere Aufgaben der Domain Controller sind die Zuweisung von Netzlaufwerken und die Einstellung der Benutzerumgebung anhand von Systemrichtlinien für Computer und Benutzer.

Die von Microsoft gebotenen Möglichkeiten werden folgendermaßen umgesetzt:

- Für die Zuweisung von Netzlaufwerken werden Skripte eingesetzt, die durch eine Systemrichtlinie, je nach Abteilungszugehörigkeit und Mitgliedschaft in besonderen Benutzergruppen, die differenzierten Anforderungen der Verwaltung an gemeinsame Laufwerke erfüllen.

- Die Benutzerumgebung wird mit einem einheitlichen Profil für alle Abteilungen eingestellt, um eine effiziente und produktive Arbeitsweise zu ermöglichen.
- Die Systemrichtlinien für Arbeitsplatzrechner sind auf die größtmögliche Betriebssicherheit und Fehlerfreiheit hin optimiert.
- Für die Domäne und für einzelne Server wurden spezielle Systemrichtlinien definiert.

Der Verzeichnisdienst – Active Directory

Im Active Directory des Verwaltungsnetzes wird für jede Abteilung der Verwaltung eine Struktur, die so genannte OU (Organization Unit), eingerichtet. In der OU befinden sich jeweils die Unterstrukturen für Arbeitsplatzrechner, Gruppen und Benutzer. Zusätzlich sind mehrere administrative Strukturen eingerichtet.

Durch Replikation des Active Directory werden administrative Änderungen der Benutzer- und Computer-Struktur der Domäne bzw. der Richtlinien auf einem Domain Controller sofort auf andere Domain Controller übertragen.

Um einzelne Objekte des Active Directory besser verwalten zu können, wurde ein spezielles Namenskonzept entwickelt.

Terminalserver

Die Terminalserver, basierend auf der Windows Server 2003 Enterprise Edition und der Terminalserver-Software Citrix MetaFrame XP, sind unter anderem die Grundlage für die Nutzung der aktuellen Programme (GX-Serie) der HIS GmbH, die von der Verwaltung genutzt werden. Durch die Terminalserver-Technologie können Spezialprogramme mit einheitlichen Einstellungen einer großen Benutzergruppe zur Verfügung gestellt werden, ohne sie auf jedem Arbeitsplatzrechner installieren und warten zu müssen. Redundanz wird durch die Vereinigung mehrerer Terminalserver in einem Citrix-Cluster und die Nutzung des Citrix-Load-Balancing erreicht. Die Benutzer werden über einen Browserdienst mit dem jeweils am wenigsten ausgelasteten Server verbunden, wobei die Auslas-

tungskriterien vom Terminalserver-Administrator festgelegt werden.

Weiterhin können die Benutzer mit Hilfe der Ordnerumlenkung sowohl im Terminalserver-Fenster als auch auf dem lokalen Desktop auf denselben Ordner »Eigene Dateien« zugreifen und damit Daten zwischen den beiden Arbeitsumgebungen austauschen. Der Systemordner »Anwendungsdaten« wird ebenfalls umgelenkt, jedoch in einem eigenen Ordner für die jeweilige Arbeitsumgebung gespeichert, um eine saubere Trennung zu gewährleisten. Für die umgelenkten Ordner wurde die Technologie der Offlinedateien aktiviert, um deren Verfügbarkeit auch bei Netzwerk- bzw. Fileserverstörungen sicherstellen zu können.

Fileserver

Die Grundlage jeder Gruppenzusammenarbeit sind gemeinsame Netzlaufwerke. Sie müssen permanent verfügbar sein, eine gute Performance bieten, ausreichend dimensioniert sein und eine verlässliche Datensicherung ermöglichen. Diesen Zweck erfüllen unsere Fileserver im Zusammenspiel mit einem Storage Area Network (SAN) und dem Backupssystem Tivoli Storage Manager (TSM). Die Fileserver sind in einem Cluster organisiert, auf denen sich mehrere Freigaben für Netzlaufwerke befinden. Bei Ausfall eines Servers im Cluster erfolgt ein automatisches Failover auf andere Fileserver. Auch bei der Anbindung an das SAN ist mehrfache Redundanz gegeben. Jeder Fileserver ist durch eine Fibre-Channel-Netzwerkkarte mit jeweils zwei Verbindungen an ebenfalls redundanten SAN-Switches angeschlossen, die ihrerseits zweifach an SAN-Virtualisierungsserver angeschlossen sind. Auch die Virtualisierungsserver sind redundant an die eigentlichen Platten-Arrays angeschlossen, so dass eine hohe Verfügbarkeit gewährleistet werden kann.

Disk Quota und Rechteeregungen

Als Disk Quota werden Techniken zur Begrenzung des für Benutzer eines Computersystems maximal verfügbaren Speicherplatzes bezeichnet. Diese Grenzen werden im Verwaltungsnetz durch

Microsoft-Quota-Mechanismen beziehungsweise die Software SpaceGuard SRM [5] der Firma tools4ever verwaltet. Zur Vereinfachung der Verwaltung von Zugriffsrechten für Netzlaufwerke wurde ein wohl durchdachtes Konzept entwickelt.

Datensicherung

Die Datensicherung der Netzlaufwerke und des Systemstatus der Domain Controller erfolgt mit Hilfe des zentralen Backup-Systems (TSM) der HU. Für die Verwaltung wurde ein zusätzliches Feature der verschlüsselten Datenübertragung und Speicherung eingeführt. Die Daten werden mit AES 128bit [6] verschlüsselt vom SAN über die Fileserver auf das TSM übertragen und in einem eigenen Bereich (auf eigenen Bändern) abgelegt, so dass die Vertraulichkeit der Daten gewährleistet bleibt. Innerhalb eines bestimmten Zeitraums (momentan 3 Monate) können Daten wiederhergestellt werden.

Weitere Server und Dienste

Zusätzlich zu den Kernkomponenten waren folgende Aktivitäten hinsichtlich der Dienste bzw. der Server erforderlich:

- Es wurden interne DNS-Server eingerichtet.
- Durch die zentrale Serverüberwachung werden Server und Dienste zentral von einem Monitor-System überwacht. Serverprotokolle werden von einem eigenen Protokoll-Server gesammelt, gefiltert und ausgewertet. Bei kritischen Ereignissen werden die Administratoren automatisch benachrichtigt.
- Die verfügbaren und vom Administrator freigegebenen Updates für Windows und Office werden durch den Windows Server Update Service (WSUS) automatisch auf die Rechner verteilt und installiert.
- Die aktuellen Viren-Signaturen werden vom McAfee ePolicy Orchestrator Server (EPO) auf die Rechner verteilt und automatisch installiert.
- Für spezielle Änderungen auf den Arbeitsplatzrechnern wurde ein eigens entwickelter Update-Service auf jedem Rechner installiert.

- Für eine schnelle Installation von Arbeitsplatzrechnern wird ein Remote-Installation Service (RIS) Server verwendet.
- Kopien von Datenträgern (Images) bzw. andere wichtige Daten können auf einem dedizierten Image-Server abgelegt werden.
- Für den Zugriff auf HIS-Systeme vom HU-Netz aus wurde eine spezielle VPN-Lösung entwickelt.

Was hängt für den Benutzer vom Funktionieren der Windows-Umgebung ab?

Ganz einfach – alles, was Benutzer der Universitätsverwaltung mit Hilfe ihres PCs machen wollen, hängt davon ab. Die Anmeldung am Windows-Netzwerk ermöglicht den Zugang zu den Diensten der Universitätsverwaltung.

Die Profile für die Mailoberfläche und den WWW-Browser befinden sich auf Netzlaufwerken. Der Zugang zu Anwendungen erfolgt über Windows-Server. Dazu gehören beispielsweise die Studierendendatenverwaltung, das Personalsystem oder die Finanzsysteme. Bis auf immer weniger ausschließlich lokale Anwendungen einzelner Benutzer sind die Anwendungen der Verwaltung vom Funktionieren des Windows-Netzwerkes abhängig.

Damit ergibt sich ein neues Problem. Leider gibt es kein »100 % sicheres« Windows-System. Auch die Rechner der HU sind Angriffen durch Würmer, Viren und anderen folgenschweren Attacken ausgesetzt. In der Regel bemerken Besitzer bereits befallener Rechner nicht, dass ihr Rechner Angriffe startet, Spam-Mails verteilt oder seine Nutzerdaten an Dritte sendet. Das ist kein Schreckensszenario, sondern Alltag.

Was wäre, wenn das im Windows-Netz der Verwaltung passieren würde? Wie lange können Mitarbeiter der Verwaltung ohne Mail, ohne Zugang zu Netzlaufwerken, ohne Zugang zu fachspezifischen Anwendungen arbeiten? Was passiert, wenn Daten Unbefugten zugänglich werden?

Durch eine Vielzahl zusätzlicher Maßnahmen wurde das Sicherheitsrisiko für

die IT des Verwaltungsnetzes minimiert. Eine absolute Sicherheit kann es allerdings nicht geben. Die bisherigen Konzepte verhinderten in den vergangenen Jahren im Verwaltungsnetz derartige »Erfolge« von Angreifern. Das soll auch so bleiben.

Erfahrungen und Stand der Realisierung

Die Ablösung von Banyan VINES in der Verwaltung wurde immer wieder verschoben, weil die personellen Kapazitäten des CMS für diese sehr aufwändigen und komplizierten Arbeiten nicht ausreichten. Zusätzlich wurde die Lockerung bestehender Sicherheitsmaßnahmen aufgrund fehlender Kapazitäten als inakzeptabel bewertet. Durch die befristete Bereitstellung von personellen Ressourcen für den CMS hat sich die Situation nun dergestalt verändert, dass mit der VINES-Ablösung im Jahr 2005 begonnen werden konnte und diese 2007 abgeschlossen werden soll. Erst diese personelle Verstärkung ermöglicht es dem CMS, das Projekt erfolgreich zum Abschluss zu bringen.

Besonders bewährt hat sich die Teilung der Administrationsaufgaben. Die Basisbetreuung erfolgt sehr effizient durch das hochspezialisierte zentrale Windows-Team des CMS. Die vier Mitarbeiter gewährleisten die erforderliche Verfügbarkeit der Windows-Server des Verwaltungsnetzes. Leider ist einer dieser Administratoren nur für die Dauer der Einführung des Windows-Systems angestellt. Wie die Betreuung der Windows-Server der Verwaltung nach Ablauf der Einführungsphase weitergeführt werden kann, ist derzeit noch ungeklärt.

Es wird eingeschätzt, dass alle weiteren Betreuungsaufgaben durch die DV-Mitarbeiter des CMS für die Verwaltung nach Abschluss des Projektes zu übernehmen sind. Die Auslieferung neuer Rechner mit der Windows-XP-Standardinstallation erfolgt abteilungs- bzw. gruppenweise. Bis Februar 2006 werden etwa 80 Rechner ausgeliefert und damit zwei Abteilungen der Verwaltung mit neuen Rechnern versorgt. Die weitere

Auslieferung erfolgt in Abstimmung mit den jeweiligen Abteilungsleitern.

Die Benutzer neu ausgelieferter Rechner verfügen bereits über Home-Verzeichnisse im Windows-Netzwerk. Im nächsten Schritt werden weitere VINES-Dienste abgelöst. Mit der Inbetriebnahme des neuen Firewall-Systems wurde 2005 begonnen.

Bis Ende des ersten Quartals 2006 werden die HIS-Anwendungen SOS, ZUL, SVA und KBS durch die Terminalserver-basierten GX-Versionen abgelöst.

Zusätzlich befinden sich die Systeme POS-GX und Komponenten von FSV-GX in der Einführung. Damit nutzt die überwiegende Zahl der Benutzer der Kernsysteme der Verwaltung aktuelle Systeme der HIS GmbH über die Terminalserver des Windows-Netzwerkes.

Ausblick

Es ist ein steiniger Weg, sowohl für die Teilnehmer des Verwaltungsnetzes als auch für die Projektgruppe, bei laufender Produktion die Basistechnologie zu ersetzen. Der sich dadurch ergebende technologische Sprung bringt jedoch Vorteile für alle Beteiligten.

Die Entscheidung für die Nutzung von Windows als Netzwerkbetriebssystem ist nicht endgültig. Die Projektgruppe ist weiterhin für andere Lösungen offen, wenn sie beispielsweise hinsichtlich der Kosten, der Administrierbarkeit, eines Zuwachses an Sicherheit und natürlich für unsere Benutzer Vorteile bieten.

Literatur

- [1] HIS GmbH. <http://www.his.de/>.
- [2] FRANK SITTEL: Institute ans SAN. *cms-journal*. 2004, 25.
- [3] TWiki: <http://twiki.org/>.
- [4] CHRISTOPH WEICKMANN: Backup – Datensicherheit für alle. *cms-journal*. 2004, 25.
- [5] tools4ever: <http://www.tools4ever.com/products/spaceguard>.
- [6] JIM SCHAAD: *Advanced Encryption Standard (AES)*. <http://www.ietf.org/rfc/rfc3565.txt>.