

PC-Installation und PC-Betreuung heute

Ingo Rauschenberg
ingo.rauschenberg@cms.hu-berlin.de

Überblick

Im Folgenden wird ein Überblick über verschiedene Technologien und Voraussetzungen gegeben, die es den Administratoren ermöglichen, über 500 Computer des Verwaltungsnetzes effektiv zu betreuen und den Aufwand zur Problemlösung zu reduzieren.

Die eingesetzten Technologien sind dem Kostenrahmen (personeller Aufwand und Beschaffungskosten) und den derzeitigen Möglichkeiten angepasst. Die Voraussetzungen sind teilweise Idealvorstellungen von Administratoren, aber unverzichtbar, wenn die PC-Betreuung effektiver werden soll.

Folgende Voraussetzungen sind wesentlich und werden näher betrachtet:

- *Gleiche Hardwarebasis*

Der Vorteil gleicher Hardwarebasis für die Nutzer des Verwaltungsnetzes besteht darin, dass sie problemlos andere Rechner der Verwaltung benutzen können und Ersatz bei Hardwareausfall bereitsteht. Für die Administratoren hat die gleiche Beschaffenheit der Rechner den Vorteil, dass sie nicht die Treiber, Updates und Ersatzteile einer unüberschaubaren Anzahl unterschiedlicher Hardware vorhalten müssen, sondern nur die einer geringen Anzahl von Hardwarevariationen. Durch den großflächigen Einsatz gleicher Hardware nehmen Installation, Fehlerfindung und Beseitigung nur einen Bruchteil der Zeit in Anspruch, die bei exotischer Hardware aufgewendet werden müsste.

- *Identische Softwareinstallation*

Bei identischer Softwareinstallation ist es dem Administrator wesentlich leichter möglich, Probleme zu lösen, da sich

im Prinzip jeder Rechner gleich verhält. Auch dies ist – wie eingangs schon erwähnt – eine Idealvorstellung, der man sich in der Realität nur annähern kann. Nachdem entschieden wurde, Windows als Betriebssystem in der Universitätsverwaltung einzusetzen, wurden Hardwareklassen definiert und für diese jeweils ein geeignetes Betriebssystem festgelegt. Gegenwärtig werden noch Windows 98 für sehr alte Rechner, Windows 2000 und für alle Neuinstallationen Windows XP eingesetzt. Damit die Betreuung der Rechner mit unterschiedlichen Betriebssystemen von Microsoft für den Administrator trotzdem möglich ist, muss jedes dieser Betriebssysteme und jede darauf installierte Anwendungssoftware identisch installiert und konfiguriert sein.

- *Automatisches Update und Fehlerüberwachung*

Hierbei soll ein Automatismus jeden einzelnen Rechner im Verwaltungsnetz auf Fehler überwachen, die Software des Rechners auf dem neuesten Stand halten und bei Problemen den zuständigen Administrator des CMS informieren. Dieser kann sich anhand der ermittelten technischen Daten eine Übersicht verschaffen und das Problem schneller lösen. Die automatische Fehlerüberwachung hat den Vorteil, dass damit Probleme erkannt werden können, die den Anwender nicht beeinträchtigen und die er deshalb nicht bemerkt. Auch dies ist eine Idealvorstellung. Bisher ist es nicht möglich, die Fehlerüberwachung und das Update jedes Rechners und jeder Software durch einen einzigen Automatismus zu realisieren. Im Verwaltungs-

Dieser Artikel beschreibt, wie es den Administratoren in der Universitätsverwaltung heutzutage möglich ist, eine größere Zahl von Rechnern zu administrieren und welche Techniken bzw. Programme dabei zur Anwendung kommen. Es wird auf die aktuelle Methode der Windows-XP-Installation mit Hilfe eines Remote Installation Service Server, auf die Fehlerüberwachung und das Update von Rechnern aus der Ferne durch einen Windows Server Update Service und einen ePolicy Orchestrator Server eingegangen. Die Möglichkeiten der Fernbetreuung von Mitarbeitern der Universitätsverwaltung durch Virtual Network Computing werden beschrieben.

netz der Humboldt-Universität sind die Fehlerüberwachung und das Updaten von Software aufgrund der geringen Personalkapazität auf die wichtigsten Komponenten beschränkt.

• Fernwartung

Die Standorte der Verwaltung sind über die Stadt verteilt und nicht immer lassen sich die Probleme am Telefon lösen. So blieb dem Administrator früher oft nichts anderes übrig, als sich auf den Weg zu machen. Dabei war die Wegezeit oft größer als die Problemlösungszeit. Daher stammt auch der Begriff »Turnschuhadministrator«, der das Problem sehr treffend beschreibt. Durch den Einsatz neuer Technologien ist es möglich, bei Rechnern im Verwaltungsnetz, die mit Windows 2000 oder XP ausgestattet sind, einen Teil der administrativen Arbeiten aus der Ferne zu erledigen.

Gleiche Hardwarebasis – wie realisiert?

Da Computer zu unterschiedlichen Zeitpunkten, bei unterschiedlichen Firmen und auch von unterschiedlichen Mitarbeitern der Humboldt-Universität beschafft werden, kann die Ausstattung der Rechner variieren. Um dem Ziel der gleichen Hardwarebasis näher zu kommen, werden spezielle Hardwareanforderungen für Rechner, die für die Universitätsverwaltung beschafft werden, definiert. Die Beschaffungsstelle der HU beschafft nach diesen Vorgaben PCs für die Verwaltung. Auch aus Kostengründen hat sich die zentrale Beschaffung größerer Rechnerposten, die nach diesen Anforderungen ausgestattet sind, für die Verwaltung bewährt.

Die Anforderungen, die an neu beschaffte Rechner gestellt werden, ergeben sich aus dem aktuellen Stand der Technik, aus Erfahrungen, die mit Rechnern gemacht worden sind und aus speziellen technischen Anforderungen, die für eine reibungslose Installation und den problemlosen Einsatz der Rechner nötig sind.

Aktueller Stand der Technik

Die Anforderungen an einen Arbeitsplatzrechner nach dem aktuellen Stand der Technik sind:

- Prozessortakt 2 GHz,
- 512 MByte RAM,
- Festplatte ab 40 GByte,
- DVD-Laufwerk,
- Diskettenlaufwerk,
- Grafikkarte mit VGA- und DVI-Ausgang und mindestens 32 MByte Grafikspeicher,
- eine Soundkarte,
- USB- und Firewire-Anschlüsse und
- eine 100 MBit/s Netzwerkkarte.

Diese Anforderungen werden regelmäßig aktualisiert. Neue Anforderungen werden hinzukommen, je nachdem welche neuen Technologien in Zukunft Einzug in die PCs der Verwaltung halten. Ein Beispiel dafür ist der Smartcard-Reader.

Spezielle Anforderungen

Spezielle technische Anforderungen sind derzeit für Rechner der Verwaltung ein Front-USB-Anschluss, für Mitarbeiter die mobile USB-Geräte benutzen müssen, und spezielle Netzwerkkarten, um die automatische Installation der Rechner zu ermöglichen.

Aus allen genannten Anforderungen wurde ein Profil erarbeitet, das bei der Beschaffung der Rechner berücksichtigt werden muss. In der Vergangenheit sind jedoch nicht alle Rechner der Verwaltung zentral beschafft bzw. nicht bei allen Beschaffungen ist auf die Anforderungen geachtet worden. Rechner, die nicht diesem Profil entsprechen, machen dem Administrator in der Regel mehr Arbeit. Das umfasst sowohl Erstinstallation als auch Betreuung und Reparatur.

Identische Softwareinstallation – wie realisiert?

Die identische Installation betrifft vor allem das Betriebssystem und die Standardsoftware, die einheitlich auf jedem in der Verwaltung eingesetzten Rechner vorhanden sein muss. Davon ausgenom-

men sind Programme, die nur in speziellen Bereichen bzw. bei speziellen Tätigkeiten benötigt werden. Aufgrund der Lizenzkosten kann Software nicht prophylaktisch auf jedem Rechner installiert werden. Hinzu kommt der zeitliche Aufwand für das Erzeugen der automatischen Installation, was nicht mit jeder Software funktioniert.

Bisheriges Herangehen

Früher wurde die identische Grundinstallation dadurch realisiert, dass ein Rechner installiert und konfiguriert wurde und der fertige Rechner mit Hilfe eines Imageprogramms (PowerQuest Drive Image) dupliziert wurde. Nach dem Kopieren waren nur noch minimale Änderungen nötig. Diese Installationen waren aufgrund der Einschränkungen des Betriebssystems nur gering vor Änderungen geschützt.

Mit den Betriebssystemen Windows 2000 und Windows XP ist das Herstellen identisch installierter Rechner etwas komplizierter geworden, da nicht mehr einfach ein Rechner genommen und dessen Installation auf einen anderen kopiert werden kann. Eine Kopie würde nur bei Rechnern mit ähnlicher Hardware funktionieren, da sonst das Betriebssystem aufgrund fehlender Treiber oder eines falschen *Hardware Abstraction Layers* (HAL) nicht mehr startet. Weiterhin muss das Kopieren speziell vorbereitet werden, da es sonst möglich ist, dass die Kopie des Originalbetriebssystems die gleiche Identifizierungsnummer (SID) wie das Original hat. Diese muss jedoch eindeutig sein, um Windows-Installationen unterscheidbar zu machen. Auch die Änderungen, die nach dem Kopieren durchzuführen sind, sind im Vergleich zu Windows 95/98 und der darauf eingesetzten Software umfangreicher geworden. Da das Kopieren eines Rechners mit Windows 2000 oder XP und die Nachbereitung fast so umfangreich wie eine eigene Installation geworden sind, ist auch die Fehleranfälligkeit einer solchen Installation gestiegen. Daher ist mit der Einführung von Windows XP im Verwaltungsnetz eine automatische Installation der Rechner eingeführt worden, die jeden Rechner nach vorge-

gebenem Muster installiert und bei der die Anpassungen im Nachhinein minimal sind.

Zeitgemäß installieren – der RIS-Server

Die Installation von Windows XP im Verwaltungsnetz wird über einen *Remote Installation Service Server* (RIS-Server) von Microsoft realisiert.

Bei dieser Methode liegt alles, was für die Installation eines Client-Rechners gebraucht wird, im Netz auf dem RIS-Server und der Rechner holt sich das Benötigte über das Netzwerk.

Voraussetzungen dafür sind ein Verwaltungsnetzanschluss und die Fähigkeit des Rechners, vom Netzwerk zu booten.

Installation des Betriebssystems

Zu Beginn der Installation bootet der Client-PC vom Netzwerk. Vom Dynamic Host Configuration Protocol Server (DHCP-Server) auf dem RIS-Server wird ihm eine IP-Adresse zugewiesen. Danach lädt er das Boot Image via Trivial File Transfer Protocol (TFTP) vom RIS-Server herunter und bootet mit dem Image. Nach diesem Prozess steht eine rudimentäre Textmenüumgebung mit einer Netzwerkverbindung zum RIS-Server zur Verfügung. Nach der Authentifizierung wird eine der auf dem RIS-Server bereitgestellten Installationen ausgewählt. Es erfolgt der Start der ausgewählten Installation mit der Angabe der Partition, wohin Windows installiert werden soll, dem Herunterladen der benötigten Daten vom RIS-Server und der eigentlichen automatischen Installation.

Die Installation muss vorher entwickelt, getestet und auf dem RIS-Server bereitgestellt werden. Dazu gehören Dateien, Skripte und Treiber für eine bestimmte Windows-Installation und die Anpassung der Skripte und Konfigurationen an die vorher festgelegten Spezifikationen der Windows-Installation.

Microsoft selbst bietet die Möglichkeit, die Bereitstellung mit einer Antwortdatei zu beeinflussen. In dieser kann festgelegt werden, wie Windows installiert werden soll, im Fall der Verwaltungsnetzinstallation also vollautomatisch. Es kann ausgewählt werden, welche Komponenten installiert und welche nicht installiert

```
[ data]
floppyless="1"
msdosinitiated="1"
OriSrc="\\%SERVERNAME%\RemInst\%INSTALLPATH%"
OriTyp="4"
LocalSourceOnCD=1
DisableAdminAccountOnDomainJoin=0
AutoPartition=0
UnattendedInstall="Yes"

[ SetupData]
OsLoadOptions="/noguiboot /fastdetect"
SetupSourceDevice="\ Device\ LanmanRedirector\ %SERVERNAME%\RemInst\
%INSTALLPATH%"

[ GuiUnattended]
OemSkipWelcome=1
OemSkipRegional=1
TimeZone=110
ProfilesDir="D:\Dokumente und Einstellungen"
AutoLogon=Yes
AutoLogonCount=2
```

Abb. 1: Auszug aus einer Antwortdatei für Windows XP.

werden sollen. Es wird zum Beispiel der standardmäßig installierte Windows Messenger abgewählt. Die Netzwerkeinstellungen der späteren Windows-Installation werden hier festgelegt, ebenso wie die Einstellung, dass das Verzeichnis »Dokumente und Einstellungen« auf die 2. Partition gelegt werden soll.

Generell haben alle neu ausgelieferten Rechner für die Verwaltung (Windows 2000 und XP) zwei Partitionen; eine, auf der das Betriebssystem und die Programme installiert sind und eine, auf der die Nutzerdaten liegen. Somit ist es bei einem Rechnertausch eines Nutzers leicht, die Daten zu retten und bei einem Systemfehler kann die Betriebssystempartition unabhängig von der Datenpartition repariert werden.

In der Antwortdatei für die automatische Installation durch den RIS-Server können auch Verzeichnisse angegeben werden, die Plug'n'Play-Treiber enthalten, die bei der normalen Windows-Installation nicht enthalten sind. Wenn bekannt ist, dass spezielle Rechner diese benötigen, werden sie aus den Installations-CDs extrahiert und im RIS-Server eingebunden. Nach der Windows-Installation, also der reinen Betriebssysteminstallation, werden automatisch Skripte aufgerufen. Auch diese müssen vorher auf dem RIS-Server vorbereitet und in der Antwortdatei eingetragen sein. Mit Hilfe dieser Skripte kann neben der Windows-Installation auch die Installation der Standardsoftware automatisch erfolgen.

Installation der Standardsoftware der Verwaltung und Einstellungen des Betriebssystems

In der Windows-XP-Installation wird neben dem Betriebssystem folgende Software automatisch installiert:

- Microsoft Office 2003 (inkl. Updates von Microsoft),
- Acrobat Reader 7,
- GhostScript und GhostView (zur Anzeige von Postscriptdateien),
- FilZip (ein kostenloses Packprogramm, das mehr Archivtypen unterstützt als das interne Packprogramm von Windows XP),
- Rückenfit (ein Programm der Charité zur Erhaltung der Rückengesundheit bei sitzenden Tätigkeiten),
- Mozilla (Internet-Browser und Mail-Client),
- McAfee ePO-Agent (eine Software für die Installation und Überwachung der Antivirensoftware von McAfee),
- FreePDF XP (ein Programm, das die Generierung von PDF-Dateien ermöglicht),
- Java Runtime Environment,
- Quicktime,
- Netscape Calendar,
- Citrix ICA Client und
- TightVNC.

Da sich nicht jedes dieser Programme ohne Benutzereingabe installieren lässt, muss auch hier für jedes eine Methode zur automatischen Installation gefunden werden.

Nach der zusätzlichen Softwareinstallation werden in einem Skript verschie-

dene Einstellungen von Windows vorgenommen, die nicht über die Antwortdatei der Windowsinstallation einstellbar, die jedoch für das problemlose Arbeiten mit Windows XP sinnvoll sind (zum Beispiel das Aktivieren der NUM-Lock-Taste beim Systemstart, das Aussehen und Verhalten der *Start-Leiste* oder das Erscheinungsbild des Windows-Explorers).

Nachdem die Windows-Installationsdateien, die zusätzlichen Plug'n'Play-Treiberdateien, die zusätzliche Software, die Antwortdatei und die eigenen Skripte auf dem RIS-Server hinterlegt und eingebunden sind, kann die oben beschriebene Installation automatisch durchgeführt werden.

Die Nacharbeiten

Die Nacharbeiten, die nach einer solchen automatischen Installation nötig sind, sind minimal. Sie bestehen aus der Zuweisung der IP-Adresse und des korrekten Rechnernamens, dem Aktivieren des Windows Update Services, gegebenenfalls der Installation von Banyan VINES und der Vergabe von Passwörtern für die lokalen Accounts. Bei der Auslieferung eines neuen Rechners an einen Benutzer müssen dann noch die Daten von einem eventuell vorhandenen alten Rechner auf den neuen kopiert werden.

Der Vorteil dieser Installationsmethode besteht in der sauberen, standardisierten Installation, bei der nicht die umfangreichere Nachbereitung einer Imageinstallation nötig ist. Kleine Änderungen an der Installation sind nicht so aufwendig wie bei einer Imageinstallation, da diese direkt auf dem RIS-Server gemacht werden und kein komplett neues Image erstellt werden muss.

Es ist sichergestellt, dass jeder Computer gleich installiert ist, weil bei dieser Installationsart der größte Teil automatisch abläuft und wenig Nachbereitung benötigt wird. Die automatische Installation ermöglicht es auch dezentralen Administratoren, eine Standardinstallation für das Verwaltungsnetz durchzuführen.

Seit dem Einsatz von Windows 2000 und Windows XP im Verwaltungsnetz ist die Forderung nach gleich installierten Rechnern auch Monate nach der Auslieferung erfüllt, da es dem normalen Benutzer nicht mehr möglich ist, unab-

sichtlich oder beabsichtigt zusätzliche Software zu installieren. Zusätzliche Software kann nur noch nach ausreichenden Tests durch einen Mitarbeiter des CMS installiert werden. Dadurch ist der Betreuungsaufwand enorm gesunken.

Automatische Updates und Fehlerüberwachung – wie realisiert?

Durch die Standardisierung der Computer der Verwaltung ist es sinnvoll, diese auch aus der Ferne auf Fehler zu überwachen und mit Updates zu versorgen. Es ist entschieden worden, dies nur für die wichtigsten Komponenten der neu ausgelieferten Rechner zu realisieren, da das Verwaltungsnetz durch ein Firewall-System geschützt wird.

Eine dieser Komponenten ist der Virens Scanner, da ein aktueller Virens Scanner und eine frühe Erkennung eines Virenbefalls sehr wichtig für die hohe Verfügbarkeit des Verwaltungsnetzes sind. Weiterhin erscheinen bei Microsoft monatlich Updates, die Sicherheitslücken in den Betriebssystemen und der Microsoft-Anwendungssoftware beheben. Andere Komponenten sind die automatische Verteilung der Updates und die automatische Überwachung des Patchstandes der Rechner in der Universitätsverwaltung.

In der Abbildung 2 zur *Fehlerüberwachung und Updateversorgung im Verwaltungsnetz* sind die eingesetzten Techniken skizziert.

Windows-Updates

Optimal ist es, wenn ein Rechner alle verfügbaren Updates installiert hat, denn wenn eine Sicherheitslücke, die durch ein Update geschlossen wird, einmal bekannt ist, dauert es nicht lange bis es Programme gibt, die diese Sicherheitslücke ausnutzen.

Zur Überwachung und Verteilung der Updates für die Betriebssysteme und Software von Microsoft ist im Verwaltungsnetz ein »Windows Server Update Service«-Server (WSUS-Server) im Einsatz. Dieser Server lädt Updates, sobald diese verfügbar sind, von Microsoft herunter. Danach hat ein Administrator

die Möglichkeit, die Updates für verschiedene Rechner freizugeben. In der Regel werden die Updates zuerst für eine Gruppe von Testrechnern und erst nach Prüfung für die Rechner im Verwaltungsnetz freigegeben. Auf dem WSUS-Server wird überwacht, welche Rechner Updates benötigen, welche Updates auf den Rechnern installiert sind, wann das letzte Mal eine Updateprüfung stattfand und ob es Fehler bei automatischen Updates gab. Durch dieses Vorgehen kann sichergestellt werden, dass jeder Rechner des Verwaltungsnetzes, bei dem der Windows Update Service eingestellt ist, auf dem neuesten Patchstand ist und somit die Gefahr für diesen Rechner, Opfer eines Angriffs zu werden, drastisch reduziert wird. Weiterhin können Rechner identifiziert werden, bei denen Fehler auftreten. Sie werden gezielt repariert, sodass die Gefahr für das Verwaltungsnetz weiter gemindert wird.

Da der WSUS-Server auch Updates für die Serverbetriebssysteme bereitstellt, werden auch die im Verwaltungsnetz eingesetzten Windows-Server, zum Beispiel die Terminalserverfarm, über den WSUS-Server versorgt und auf Fehler beim Update überwacht.

Das Virens Scannerupdate

Die zweite wichtige Komponente, die bei neu ausgelieferten Rechnern, aber auch bei Servern im Verwaltungsnetz überwacht wird, ist der Virens Scanner. Es kommt immer wieder vor, dass für eine Sicherheitslücke im Betriebssystem noch kein Update von Microsoft existiert, es aber schon einen Virus dafür gibt. Sollte es für diesen Virus jedoch schon eine Signatur für die Antivirensoftware geben, so muss diese umgehend auf die Rechner verteilt werden.

Für die Verteilung wird im Verwaltungsnetz ein *electronic Policy Orchestrator* Server (ePO-Server) für Produkte der Firma McAfee eingesetzt. Dieser lädt die aktuellen Virensignaturen und Scanmodule sowie Patches der Scansoftware von McAfee herunter und verteilt sie an die Rechner im Verwaltungsnetz. Weiterhin überwacht der Server den Status und die Einstellungen der Virens Scanner auf den Rechnern. Sollte auf einem mit dem

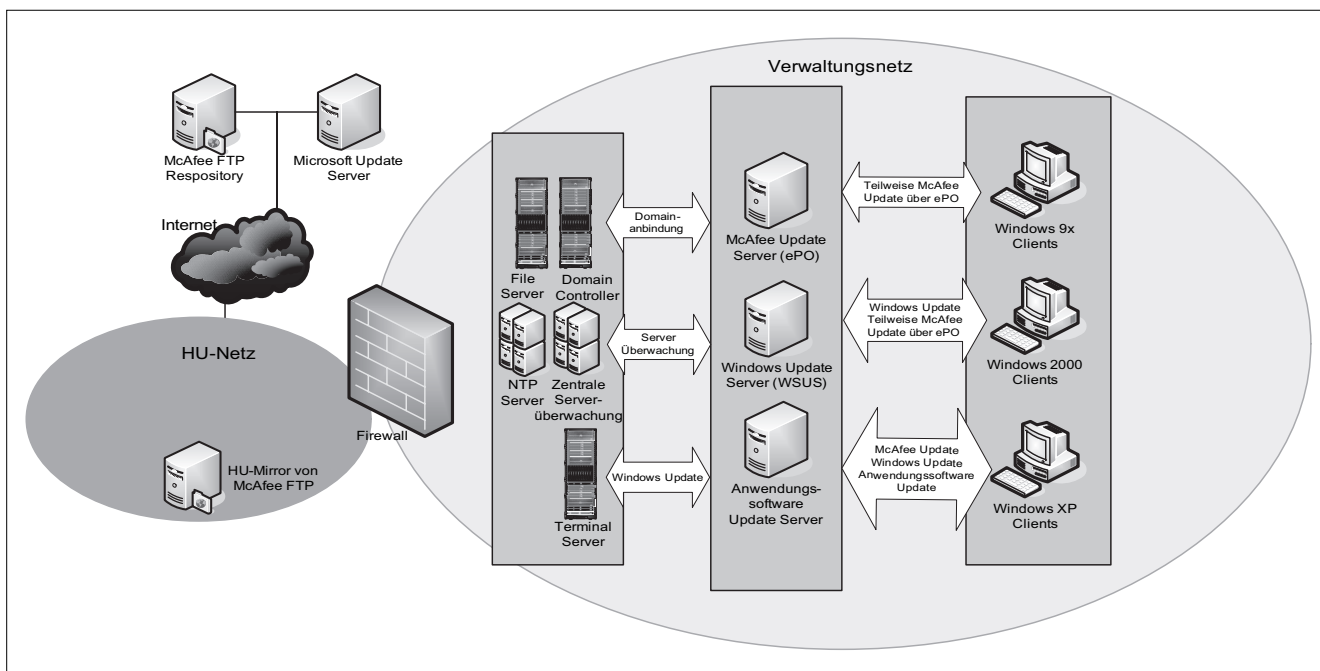


Abb. 2: Fehlerüberwachung und Updateversorgung im Verwaltungsnetz

ePO-Agenten ausgestatteten Rechner kein oder ein veralteter Virens Scanner gefunden werden, so wird der alte ggf. deinstalliert und der neue Virens Scanner installiert. Sobald der Server entdeckt, dass ein Rechner keine aktuellen Virensignaturen herunterlädt oder dass auf einem Rechner der Verwaltung ein Virus gefunden wurde, sendet er an den verantwortlichen Mitarbeiter des CMS eine E-Mail, in der auf das Ereignis hingewiesen wird.

Da jeder so ausgestattete Rechner des Verwaltungsnetzes alle 5 bis 10 Minuten die Einstellungen des Virens Scanners überprüft und den Vorgaben des ePO-Servers anpasst, kann durch eine zentrale Änderung der Einstellungen am ePO-Server direkt und schnell auf eine Bedrohung reagiert werden, für die es zum Beispiel noch keine Signatur gibt.

Andere Anwendungssoftware

Ein ebenfalls wichtiger Punkt ist das Überwachen und Updaten der Software, die nicht von Microsoft oder McAfee stammt. Dafür gibt es verschiedene kommerzielle und auch frei verfügbare Möglichkeiten, von denen jede ihre Vor- und Nachteile hat. Bisher wird in der Verwaltung ein Skript genutzt, das sich bei jedem Start des Rechners mit einem

Server verbindet und dort nach bisher noch nicht auf dem Rechner ausgeführten Skripten sucht und diese ausgeführt. Diese Methode funktioniert nur bei einfachen Änderungen. Eine der zukünftigen Aufgaben wird es daher sein, ein System zu finden, das im Verwaltungsnetz die Überwachung und das Updaten der Software, die bisher noch nicht überwacht wird, zulässt.

Serverüberwachung

Es ist nötig, das korrekte Funktionieren von Servern zu überwachen. Die Überwachung dieser und auch anderer Server erfolgt durch eine redundant ausgelegte zentrale Serverüberwachung im Verwaltungsnetz, die bei Ausfall oder Problemen bei einem Server den jeweils verantwortlichen Mitarbeiter mit einer E-Mail informiert. Somit kann eine hohe Verfügbarkeit der Server garantiert und die Sicherheit des Verwaltungsnetzes gewährleistet werden.

Fernwartung – wie realisiert?

Die Administratoren des CMS betreuen die Benutzer der Universitätsverwaltung bei allen IT-Problemen. Es ist eine Hotline geschaltet und es wird bei Anrufen

zunächst versucht, das Problem über das Telefon zu lösen. Seit der Einführung von Windows 2000 und Windows XP besteht für den Mitarbeiter des CMS die Möglichkeit, über eine Remoteverbindung den Rechner zu bedienen und ihn somit aus der Ferne zu warten. Natürlich gibt es Fälle, in denen die Verbindung zu Rechnern nicht mehr aufgebaut werden kann oder das Problem nicht durch Fernwartung lösbar ist. Es bleiben den Mitarbeitern des CMS daher nicht alle, aber ein großer Teil der Wege zu den Problemrechnern erspart.

In einem Bereich wie dem Verwaltungsnetz, in dem mit vertraulichen Daten umgegangen wird, darf die Möglichkeit, den Bildschirminhalt eines fernen Rechners über das Netzwerk einzusehen, nur stark kontrolliert und eingeschränkt bestehen. Die Einschränkung besteht darin, dass die Fernwartungssoftware TightVNC so konfiguriert ist, dass nicht ohne Mithilfe und Wissen des Verwaltungsmitarbeiters eine Verbindung zu seinem Rechner aufgebaut werden kann. Der Mitarbeiter muss gezielt den Dialog eröffnen. Weiterhin ist durch ein optisch verändertes Symbol deutlich sichtbar, ob derzeit der eigene Rechner mit einem anderen Rechner verbunden ist oder nicht. Die so erreichte Fernwartung gibt den Administratoren die Mög-

lichkeit, Fehler direkt zu sehen und schneller zu beheben.

Erfahrungen und Zusammenfassung

Die hier vorgestellte Installation von Windows-XP-Rechnern mithilfe eines RIS-Servers wird seit August 2005 in der Verwaltung eingesetzt, wobei die Entwicklung einer einheitlichen, automatischen Installation für das Verwaltungsnetz etwa sechs Monate gedauert hat.

Bis Ende November 2005 wurden über 30 Rechnerinstallationen mit dieser Methode vorgenommen. Die reine Rechnerinstallation dauert ca. 75 Minuten und erfolgt nach einer Anleitung in etwa 20 Schritten. Die parallele Installation von mehreren Rechnern ist möglich. Der dadurch erhöhte Netzwerkverkehr be-

einträchtig jedoch nicht die Nutzer des Verwaltungnetzes.

Der hier vorgestellte WSUS-Server hat im Oktober 2005 den Vorgänger, den SUS-Server, abgelöst. Seitdem werden ca. 200 Rechner problemlos von diesem Server mit Updates für Microsoft-Produkte versorgt. Die Updates, die dieser Server für Windows 2000, XP, 2003 und Office-Produkte in englischer und deutscher Sprache bereithält, haben derzeit eine Gesamtgröße von etwa 8 GByte.

Der ePO-Server ist seit etwa acht Monaten in Betrieb und versorgt bisher ca. 100 Rechner mit Virenskannern und Virensignaturupdates.

Der Anwendungssoftware-Update-server ist zeitgleich mit dem RIS-Server in Produktion gegangen und hat bisher fünf verschiedene Updates an die Rechner, die diesen Server nutzen, verteilt.

Die Notwendigkeit der Einführung dieser neuen Technologien ist vor allem durch die zunehmende Bedrohung aktueller Microsoft-Betriebssysteme durch Sicherheitslücken, Viren und Spyware und durch die Notwendigkeit des Schutzes des Verwaltungsnetzes vor diesen Bedrohungen begründet.

Die Einführung und der Einsatz dieser Technologien erfordern einen erheblichen zusätzlichen Aufwand an Ressourcen und technisches Know-how im CMS.

Zusammenfassend kann gesagt werden, dass durch den Einsatz neuer Technologien auf dem Gebiet der Betreuung und Administration der Rechner

- die Sicherheit des Verwaltungsnetzes,
- die Inbetriebnahme neuer Rechner und
- die schnelle Problembehebung im Fehlerfall

in höherer Qualität und rationeller gewährleistet werden können.