Sicherheit an öffentlichen Computerarbeitsplätzen des CMS

Silvio Uth | Computer- und Medienservice, Hard- und Softwareservice | s.uth@cms.hu-berlin.de;
Sascha Demon | Computer- und Medienservice, Hard- und Softwareservice | sascha.demon@cms.hu-berlin.de;
Willi Petrov | Computer- und Medienservice, Hard- und Softwareservice | petrov@cms.hu-berlin.de

In diesem Artikel werden einige Lösungen und Vorgehensweisen vorgestellt, die zur Gewährleistung der Sicherheit im Bereich der öffentlichen Computerarbeitsplätze beitragen. Das Thema Sicherheit wird dabei unter verschiedenen Gesichtspunkten betrachtet. Zum einen ist es sowohl für die Nutzer als auch für das ÖCAP-Team selbstverständlich, dass die angebotenen Dienste immer verfügbar sind und dass auch die Arbeitsumgebung auf einem öffentlichen Desktop immer gleich und wiedererkennbar bleibt. Zum anderen – unter Berücksichtigung der Tatsache, dass sämtliche ÖCAP-Rechner in der globalen HU-Domänen-Struktur eingebunden sind – sollen von den Arbeitsstationen und Servern keine Gefahren für die HU-Computerinfrastruktur ausgehen. Für zusätzliche Informationen oder einem weiteren Erfahrungsaustausch können sich interessierte Leser gern an die Autoren wenden.

Einleitung

Die Aufgaben des Bereichs „Öffentliche Computerarbeitsplätze“ (ÖCAP) am CMS sind schon seit mehreren Jahren klar definiert: Studierenden und Mitarbeitern an der Humboldt-Universität soll die Möglichkeit gegeben werden, die für ihre studienbegleitenden, wissenschaftlichen und organisatorischen Tätigkeiten notwendigen Computerressourcen der Universität nutzen zu können. Dabei sollen sich diese Nutzer so wenig wie möglich um die technische Realisierung dieser Anforderung kümmern – ein wichtiges Ziel ist, dass an allen Computerarbeitsplätzen eine gewohnte und leicht verständliche Arbeitsumgebung vorzufinden ist, die auch alle notwendigen Werkzeuge – Software wie Hardware – enthält. Diese Aufgaben werden auch in der Zukunft von primärer Bedeutung für unseren Bereich sein. Dabei ändern sich Umfang, Qualität und Quantität der angebotenen Leistungen immer weiter, ohne dass die Arbeit der Nutzer dabei beeinträchtigt wird. So werden inzwischen nicht nur die CMS-eigenen PC-Säle und Ausbildungspools vom ÖCAP-Team betreut, sondern Terminalserver-Dienstleistungen auch universitätsweit angeboten. Wir betreiben derzeit über 530 Terminalarbeitsplätze, ca. 60 PCs, 12 MACs und 80 Mitarbeiterclients. Auch der Betrieb diverser Lizenzserver (Windows-Terminalserver-Lizensierung, Windows Vista und Server- 2008-Aktivierung, SPSS, Mathematica, ArcGis) wird vom ÖCAP-Team realisiert.

Die Terminalserver-Client-Technologie

Über die Terminalserver-Client-Technologie wurde schon mehrmals ausführlich berichtet, insofern wird an dieser Stelle nur ein kurzer Überblick über diese technische Lösung gegeben.

Auf mehreren identisch installierten Windows-Servern wird die gleiche User-Software installiert (z. B. Microsoft-Office, SPSS, TeX usw.). Diese Server werden dann logisch in einer Serverfarm zusammengefasst und es wird ein zentraler Eingangspunkt (Loadbalancer) für diese Farm definiert. Ein Client (i.d.R. ein Terminal) verbindet sich mit dem Loadbalancer und wird von diesem zum am wenigsten ausgelasteten Server in der Farm weitergeleitet. Am Terminal wird nur der für den Nutzer angepasste Desktop des Servers dargestellt – sämtliche Softwareaktionen werden im Hauptspeicher des Terminalservers virtuell ausgeführt und bidirektional verschlüsselt an das Terminal übertragen. Dieses Verfahren erlaubt es, an öffentlichen (oder auch an bestimmten Mitarbeiter-) Computerarbeitsplätzen sog. Thinclients einzusetzen – Terminals, die ohne Festplatte von einem nicht veränderbaren Flash gebootet werden und zum Server nur die Tastatur- und Mauseingaben bzw. vom Server die Monitorausgabe übertragen. Die Administration dieser Geräte erfolgt zentral und wird mit Hilfe einer Managementsoftware bewerkstelligt.
Die Terminals verfügen über nur wenig Schnittstellen (USB ist vorhanden) und keine lokalen Laufwerke, was aber bei der Verbreitung der USB-Speichermedien nicht mehr als Nachteil zu empfinden ist.

Bezüglich Sicherheit und Administration ist diese Lösung von großem Vorteil. Zum einen ist das „schlanke“ Betriebssystem der Terminals sehr robust, bietet wenige bis gar keine versehentliche oder absichtliche Veränderungs- oder Angriffsmöglichkeiten und ist nach einem Neustart des Systems in den Ursprungszustand zurückversetzt. Zum anderen werden die Thinclients nur einmal bei der ersten Inbetriebnahme konfiguriert (wenn überhaupt) – die IP-Adresse wird normalerweise über DHCP zugewiesen, es muss lediglich der Loadbalancer eingetragen werden (kann jedoch auch über DHCP erfolgen). Das einfachste Installationsszenario sähe dann so aus: Gerät wird ausgepackt, an das Netzwerk angeschlossen, auf dem DHCP-Server registriert und gebootet. Danach können sich die Nutzer sofort am Server anmelden und arbeiten.

Die Netz-Infrastruktur und der Serverfarmaufbau

Zurzeit befinden sich 30 Server in der Terminalserver-Farm. Als Betriebssystem dient Windows 2003 Server R2 Enterprise; die neue Version „2008“ wird derzeit getestet und demnächst eingeführt. Die beiden Xeon-Prozessoren mit 3 GHz und der (relativ kleine) 2GB-Arbeitspeicher pro Server erlauben das gleichzeitige Arbeiten von ca. 25-30 Nutzern. Jeder dieser Server besitzt eine öffentliche IP-Adresse aus dem Humboldt-Netz und eine private, nicht „geroutete“ IP-Adresse. Auch hier haben Sicherheitsüberlegungen eine Rolle gespielt: Die an der Serverfarm angeschlossenen Terminals haben ebenfalls nur private IP-Adressen, sind somit für die „Außenwelt“ nicht sichtbar; sie müssen nur die Verbindung zum Server herstellen, von dort aus geht es über die öffentliche Adresse des Servers weiter. Alle Server sind Mitglieder einer Domäne und in einer ‚Organisationseinheit‘ zusammengefasst - für diese gelten restriktive Sicherheitsrichtlinien. Als Loadbalancer fungiert ein entsprechendes Produkt der Firma ‚2X‘ – dieser hat sich als robust und zuverlässig erwiesen. Hier wird allerdings überlegt, mit der Einführung des Windows-Servers 2008 auch dessen Netzwerkausgleich-Dienst zu nutzen. Weiterhin ist ein windowseigener „Sitzungsmanager“ in der Farm konfiguriert – dieser sorgt dafür, dass bei einem beabsichtigten oder technisch bedingten Verbindungsabbruch getrennte Sitzungen der Nutzer ohne Datenverlust wiederhergestellt werden.

Skalierbarkeit und Administration

Sowohl client- als auch serverseitig ist die bestehende Infrastruktur jederzeit erweiterbar. Wie bereits erwähnt, ist es äußerst einfach, neue Terminals in Betrieb zu nehmen um beispielsweise einen neuen Pool mit Arbeitsplätzen auszustatten. Ab etwa 30 neuen Clients wird ein neuer Server der Farm hinzugefügt. Zwar nicht so einfach wie Terminals, aber ähnlich routiniert werden auch die Server installiert. Da deren Festplatten an einem konfigurierten RAID1-Controller angeschlossen sind, wird die zweite Festplatte eines komplett eingerichteten Image-Servers in den zu installierenden Server eingesteckt und gespiegelt. Das System kann sofort (während der Spiegelung) gestartet und konfiguriert werden (IP-Adresse, Rechnername, Domänenzugehörigkeit usw.). Dieser Vorgang dauert etwa 20 Minuten, sodass es durchaus möglich wäre, im Notfall eine komplette Farm in wenigen Stunden wiederherzustellen. Aus administrativer Sicht ist diese Lösung sehr günstig. Zwar sind es immerhin zurzeit 30 Server, die gepflegt werden müssen, doch im Vergleich zu den ca. 600 Thinclient-Arbeitsplätzen, die damit versorgt werden, reduziert sich der Aufwand um ein Vielfaches, denn Software- und Systemupdates stehen nach der Installation auf den Servern sofort allen Clients zur Verfügung. Auch gibt es diverse Möglichkeiten, die Admin-Aufgaben zu automatisieren: WSUS (Windowsupdate-Server), Skripte und Richtlinien sind hier nützliche Werkzeuge.

Die Ausfallsicherheit in einer Serverfarm ist hoch. Für den Fall, dass ein oder mehrere Server gleichzeitig ausfallen, wird die logische Farm durch den Loadbalancer weiterhin funktionsfähig bleiben – die Nutzer würden sich weiterhin an den restlichen Maschinen anmelden können. Kritisch wird es, wenn mehr als die Hälfte der Server nicht verfügbar ist (ist jedoch auch von der jeweiligen Nutzerlast abhängig), doch in diesem Fall hat ein Administrator wahrscheinlich sowieso Probleme anderer Natur.

Risiken und Sicherheitsaspekte (Warum sind ÖCAP besonders anfällig?)

Internetseiten bestehen heute im Allgemeinen nicht mehr nur aus reinem HTML-Code, sie enthalten mehr und mehr aktive Inhalte wie Java, ActiveX oder Flash. Das bedeutet, dass der Programmcode vom Internet geladen und auf dem lokalen PC ausgeführt wird. Natürlich gibt es Sicherheitsvorkehrungen im Browser und seitens des Betriebssystems, die festlegen, dass dieser Code in einem vom System abgegrenzten, geschützten Bereich – einer Laufzeitumgebung (z. B. Java VirtualMachine) – ausgeführt wird. Betriebssysteme, Browser und Laufzeitumgebungen sind komplexe Computer-Programme, die Fehler enthalten. Immer wieder kommt es vor, dass diese Fehler von findigen Spezialisten und böswilligen Hackern ausgemacht und für Angriffe auf das System oder zum Ausspionieren von Daten benutzt werden. Kürzlich, bei einem Wettbewerb an der CanSecWest, einer Sicherheitskonferenz in Vancouver im März 2008, wurden ein Mac OS X und ein Windows XP-System so in kürzester Zeit kompromittiert. Die „Angreifer“ konnten über eine manipulierte Webseite Zugang zum System und auf alle Daten erhalten. Die von ihnen ausgenutzten Sicherheitslücken waren den Betriebssystemherstellern bis dahin nicht bekannt.

Um Viren, bösartigen Skripten, Passwortgrabbern, Rootkits und Co entgegenzuwirken, ist es oft notwendig, ein ganzes Arsenal an Sicherheitsvorkehrungen zu treffen. Speziell PCs und Server, die rund um die Uhr erreichbar sind, begegnen oft einem enormen Gefahrenpotenzial. Angreifer haben, anders als

bei kurzlebigen Sitzungen, viel Zeit, um an systemkritische Informationen, wie Passwörter oder mittelkritische Informationen, wie nach außen geöffnete Ports und die dort angebotenen Serverdienste, zu kommen. Käme jemand, zum Beispiel mit Hilfe einer Bruteforce-Attacke, an Passwort-Informationen, hätte der Angreifer die Möglichkeit, innerhalb kürzester Zeit den Server oder aber die gesamte Farm unter seine Kontrolle zu bekommen. Wie kann man z. B. den über den RDP-Port angebotenen Terminalserverdienst schützen? Man könnte den Port verlegen, aber einen versierten Angreifer wird dies sicher nicht lange aufhalten können. Und doch ist es sinnvoll, unterschiedliche Hürden im System einzubauen, auch solche, die auf den ersten Blick als unwichtig erscheinen. Sichere (komplexe) Passwörter, das schnelle Schließen von möglichen Sicherheitslöchern durch den Betriebssystemhersteller und das damit verbundene umgehende Einspielen von System- und Softwareupdates sind Aufgaben von höchster Priorität.

Da an einem Terminalserver zwischen 20 und 30 Nutzer arbeiten, ist es wichtig, dass die einzelnen Sitzungen die Sicherheit des Betriebssystems nicht gefährden und sich untereinander nicht beeinflussen. Zudem ist der Datenschutz zu beachten, d. h. kein Nutzer darf unberechtigt die Daten eines anderen zu sehen bekommen. Durch fremde Daten (Diskette, USB-Stick) potenziert sich auf einem Terminalserver die Bedrohung durch Viren, Skripte, ActiveX&Co. Dabei darf man sich nicht nur auf zu bearbeitende Dokumente beschränken, sondern muss sich außerdem auch auf mögliche Eingriffe ins Betriebsystem (Skripte, verbotene Programme) einstellen.

Gegenwärtige Lösungen

Um die Sicherheit an den öffentlichen Computerarbeitsplätzen zu erhöhen, wurde seit März 2003 die personalisierte Anmeldung eingeführt. Alle Studierenden einer Hochschule sowie Mitarbeiter der HU sind berechtigt, die ÖCAP des CMS zu nutzen. Zum Anmelden am Computer wird ein Windows-Account aus dem Verzeichnisdienst Active-Directory benötigt, der nach einer Online-Beantragung sofort benutzbar ist. Dieser Account gilt für alle öffentlichen Computerarbeitsplätze der Universität. Für die Nutzer ist darüber hinaus die Anmeldung, Verlängerung und/oder Reaktivierung des Accounts auch in Selbstbedienung über ein entsprechendes Web-Formular möglich.

Zentrale Nutzerdatenbank (ADS) und Gruppenrichtlinien

Der Zugang zu den Computerarbeitsplätzen wird zentral über den Verzeichnisdienst Active Directory (ADS) verwaltet. Sowohl die Benutzer-, als auch die Terminalserver- und PC-Konten im ADS sind logisch in sogenannten „Organisationseinheiten“ (organizational units, OUs) gruppiert. Dadurch wird die Verzeichnisstruktur hierarchisch gegliedert, was die Administration der einzelnen Konten sehr vereinfacht. Ein großer Vorteil dieser Technologie ist auch, dass für jede OU (und für jedes darin enthaltenes Konto) eigene Sicherheitsrichtlinien (Gruppenrichtlinien) definiert werden können, wodurch unter anderem festgelegt ist, dass die Nutzer keine Fremdsoftware installieren oder ausführen dürfen, dass die Systemlaufwerke ausgeblendet sind oder dass keine Registry-Bearbeitungstools gestartet werden dürfen. Diverse Einträge aus dem Startmenü und auf dem Desktop, die die Sicherheit des Systems betreffen, wurden auch entfernt.

Die eingestellten Gruppenrichtlinien wurden sowohl zentral auf dem Domaincontroller als auch lokal auf jedem Terminalserver aktiviert, um die Offline-Verbreitung der Richtlinien zu sichern.

Das „Default User“-Profil

Für jeden Nutzer, der sich an einem Windowsrechner (Workstation oder Server) anmeldet, wird ein eigener Profilordner mit dem Anmeldenamen des Nutzers auf der lokalen Festplatte erstellt. In diesem Ordner, der eine Kopie der Ordner „%windrive%\dokumente und einstellungen\default user“ darstellt, werden sämtliche für die jeweilige Sitzung notwendigen Daten gespeichert. Hierzu zählen z. B. das Aussehen des Desktops, die Links im Startmenü, das Verhalten des Windows-Explorers und die Einstellungen des Internet-Explorers. Es bietet sich also beim Betrieb von öffentlichen Arbeitsplätzen an, dass der Inhalt des „Default User“-Profils vor der ersten Nutzeranmeldung am Rechner bearbeitet und den Anforderungen des Arbeitsplatzes angepasst wird. Ein Hauptaugenmerk gehört dabei der Datei ‚ntuser.dat’. Diese stellt für die Dauer der Sitzung eine Abbildung der User-Registry dar und bietet somit sehr viele Anpassungsmöglichkeiten. Ein Beispiel dafür ist, dass dadurch das Anzeigen bestimmter Laufwerke im Windows-Explorer unterbunden wird. Der Vorteil bei der Anpassung des „Default User“-Profils liegt darin, dass dessen Inhalt immer gleich bleibt und nur vom Administrator geändert werden kann. So finden angemeldete Nutzer – egal von wo aus sie sich anmelden und an welchem Server sie arbeiten – immer die gleiche Arbeitsumgebung vor. Allerdings gibt es bei diesem Verfahren auch Nachteile: Zum einen kann unterschiedlichen Nutzergruppen kein vom Standard abweichendes Profil zugewiesen werden (dies muss durch Anmeldeskripte abgefangen werden), zum anderen können Programmeinstellungen, die durch die Nutzer selbst vorgenommen werden, nur für die jeweilige Sitzung gespeichert werden, da nach einem Ab- und erneutem Anmelden die Sitzung mit hoher Sicherheit auf einem anderen Server gestartet wird – und auf diesem wird eben wieder ein neues, ‚sauberes’ Profil angelegt.

Antivirensoftware und Firewall

Obwohl, wie oben beschrieben, die Gruppenrichtlinien sehr restriktiv definiert worden sind, wird auch Antivirensoftware an den Terminalservern eingesetzt. Dabei wird die Virendefinitionsdatei täglich automatisch aktualisiert. Allerdings hat der Einsatz von Antivirensoftware auf einem Terminalserver auch einen Nachteil: So viele Nutzer auf einem Ser-

ver angemeldet sind, so viele Instanzen des Virenscanners laufen auch gleichzeitig. Dies beeinträchtigt in geringem Maße die Leistung des Gesamtsystems, durch die Verbesserung von Serverkomponenten wird diese Auswirkung jedoch immer weiter reduziert.

Da die Terminalserverfarm im Hochverfügbarkeitsmodus läuft und ständig im Netz präsent ist, könnte diese sehr leicht zum Angriffsziel werden. Um das zu verhindern, ist auch eine Firewall aktiv. Die Firewalleinstellungen sind so definiert worden, dass der Benutzerzugriff auf die Terminaldienste nur bestimmten Gruppen aus dem Netz der Humboldt-Universität möglich ist und alle nicht benötigten Ports gesperrt sind.

Skripte zur Erhöhung der Sicherheit

Bei der Sicherheitsgewährleistung werden nicht nur betriebssystemeigene Hilfsmittel verwendet, sondern auch eigens für diesen Zweck entwickelte Skripte. Die Ausführung dieser Skripte wird sowohl über Gruppenrichtlinien als auch lokal über jeden der Server gesteuert. Mit Hilfe dieser Skripte wird z. B. erreicht, dass die temporär auf der Festplatte angelegten Profile der Nutzer gelöscht werden, da es ansonsten unter Umständen zur Überfüllung der Systemfestplatte und infolgedessen zum Ausfall des betroffenen Servers kommen könnte. Auch die Anmeldezeiten, zu welchen sich Nutzer auf den Servern einloggen können, werden durch Skripte gesteuert, wobei die jeweiligen Öffnungszeiten berücksichtigt werden.

Proxyserver

Nutzer an den öffentlichen Computerarbeitsplätzen surfen über einen Proxyserver im Internet. Dieser ist im jeweiligen Profil des Benutzers hinterlegt und kann nicht geändert werden. Auf dem Proxyserver werden keine Daten über besuchte Webseiten eines einzelnen Benutzers gespeichert, er leitet alle Anfragen ohne Zwischenspeicherung ins Internet durch. Der Proxyserver dient vor allem dazu, Internetseiten mit systemgefährdendem Code und Internetseiten mit gewaltverherrlichenden oder pornografischen Inhalten auszufiltern. Das Hinzufügen einer Zeile in der Konfigurationsdatei des Proxyservers reicht oft aus, um die Sicherheit der Serverfarm in diesem Bereich zu erhöhen.

Virtuelle Maschinen als Arbeitsplätze

Die Virtualisierung von Betriebssystemen samt installierter Software eröffnet administrativ und sicherheitstechnisch ganz neue Wege. So wurden die PCs in einem unserer PC-Pools mit einem „nackten“ Windows XP und nur dem VMWare-Player installiert. Über diesen Player haben Nutzer die Möglichkeit, sich zwischen mehreren virtuellen Maschinen zu entscheiden: Windows XP, Vista, Linux. In diesen VMs ist wiederum die komplette Software installiert. Leistungsmäßig sind so gut wie keine Unterschiede zu merken – selbst bei solchen Anwendungen wie Photoshop oder SPSS. Ein Problem stellt manchmal das Abspielen von DVDs dar – hier sollte auf einen auf dem Hostsystem installierten Medien-Player zurückgegriffen werden. Die virtuellen Maschinen sind ähnlich restriktiv konfiguriert wie die „normalen“: Domänenzugehörigkeit, Richtlinien, Firewall, Virenscanner usw. sind auf dem gleichen Niveau; die Nutzer haben nur „Benutzer“-Rechte. Allerdings sind die virtuellen Festplatten auf „independent“ eingestellt – nach einem Aus- und Einschalten (nicht Neustart) werden sämtliche Änderungen im System verworfen. Auf diese Weise wird gesichert, dass sich die Arbeitsplatzinstallation immer auf dem gleichen vom Administrator definierten Zustand befindet. Beim Windows update oder bei neuer Software wird nur die Master-VM bearbeitet und dann geklont. Per Knopfdruck wird dieser Klon auf den einzelnen PC-Pool-Rechner übertragen.

Auch besteht manchmal die Anforderung seitens der Nutzer, eigene Software auf einem öffentlichen PC zu installieren und zu testen. Auch für diesen Fall befinden sich virtuelle Maschinen mit „independent“-Festplatten auf den Rechnern. Hier hat der Nutzer sinnvollerweise volle Admin-Rechte und keine Restriktionen, jedoch keine Netzwerkanbindung. Diese Lösung wird gern in Anspruch genommen und ist für beide Seiten – Nutzer und Administratoren – ein praktikabler Weg, Sicherheit und Funktionalität zu verbinden.

Aber auch Server laufen auf virtueller Basis – insbesondere solche, die Dienste anbieten, die zwar immer verfügbar sein müssen, jedoch ressourcensparend sind, wie etwa Lizenz-, Druck-, DHCP-, Skript- oder Proxyserver. Hier werden zum einen die Anfangsinstallation und zum anderen regelmäßig (wöchentlich nachts) Kopien der VM-Ordner auf einem Fileserver gesichert. Auf diese Weise konnten Serverkapazitäten gespart und auch die Reaktionszeiten bei Serverausfällen reduziert werden.

Schlussbemerkung

Bedenkt man, dass sich die Terminalserver-Client-Technologie als sinnvolle Lösung beim Betrieb standardisierter Computerarbeitsplätze durchgesetzt hat und vom ÖCAP-Bereich weitestgehend beherrscht und zukünftig weiterhin eingesetzt wird, so ist es nahe liegend, dass die verfügbaren (und auch jederzeit erweiterbaren) Kapazitäten universitätsweit angeboten werden. DV-Beauftragten wird die Möglichkeit geboten, mit sehr geringem Aufwand PC- und Terminal-Pools oder auch „normale“ Mitarbeitercomputer in Betrieb zu nehmen. Im günstigsten Fall beschränkt sich der persönliche Einsatz auf die Aufstellung von Thinclients: Gleich danach können Nutzer – einen gültigen Windows-Account vorausgesetzt – mit der Arbeit beginnen. Da die Terminals praktisch wartungsfrei sind und die Server- und Softwarepflege vom ÖCAP-Team übernommen wird, ist dies zudem eine, auch aus sicherheitstechnischer und administrativer Sicht, komfortable Lösung.