inforum

Zentrum für Informationsverarbeitung der Universität Münster
Jahrgang 31, Nr. 1 – Februar 2007 ISSN 0931-4008

Inhalt

Impressum

infoWWW
ISSN 0931-4008

Westfälische Wilhelms-Universität
Zentrum für Informationsverarbeitung (Universitätsrechenzentrum)
Röntgenstr. 9–13
48149 Münster

E-Mail: ziv@uni-muenster.de
WWW: http://www.uni-muenster.de/ZIV/
Redaktion: E. Sturm (✆ 83-31679, ✉ sturm@uni-muenster.de
Fax: 83-31553)
Satz: B. Schultze
Satzssystem: StarOffice 8
Druck: Drucktechnische Zentralstelle

Auflage dieser Ausgabe: 1300

Editorial

E. Sturm

Obwohl ich schon gut einen Monat nach Erscheinen des letzten infoWWW meine Kollegen wieder nach Artikeln für die nächste Ausgabe gefragt hatte, wurde ich mit solchen geradezu überschüttet. Die Anzahl Artikel in der Rubrik „ZIV-Aktuell“ blieb in etwa konstant, aber für „ZIV-Präsentation“ gab es einen neuen Rekord.

Dazu trug zum einen R. Perske mit seiner Serie über unseren neuen Webserverpark bei. Wir hoffen, damit besonders den Fachbereichen zu dienen, die bisher Webseiten selbst betrieben haben. Der Webserverpark schont die Ressourcen und entspricht den Empfehlungen des Landesrechnungshofs.

Aber dort ist auch ein weiterer versteckt, den ich Ihrer Aufmerksamkeit empfehlen möchte, nämlich der Bericht der IV-Kommission über die Fortentwicklung des Münsteraner Modells der Aufgabenverteilung zwischen ZIV und IVVen.

Das Thema des Monats ist ansonsten, ob man das gut findet oder nicht, Windows Vista. Im Prinzip war ich schon beeindruckt, dass diesmal die Sicherheit deutlich verbessert schien, und überlegte, welchen meiner Rechner ich als Ersten aufrüsten sollte – eine Neuinstallation wollte ich mir auf keinen Fall antun. Glücklicherweise schickte mir mein Kollege W. Lange vorher die folgende Webadresse zu:

`rtsp://real.swr.de/swr/ratgeber/multimedia/134978.rm`

Wenn man einen Realplayer oder „Real Alternative“ installiert hat, sieht man einen sehr optimistischen Film über den Versuch, Vista über XP zu installieren. Obwohl der Protagonist an alles zu denken scheint und auch den „Windows Vista Upgrade Advisor“ vorher zu Rate zieht, scheitert das Ganze an fehlenden Vista-Treibern – schon der Drucker funktioniert nicht mehr, vom lokalen Netz ganz zu schweigen.

Die Quintessenz ist jedenfalls, bei einem alten Rechner noch ein halbes Jahr zu warten oder aber einen neuen Rechner zu kaufen, der dann wohl mit passenden Treibern versehen sein sollte (den neuen Drucker nicht zu vergessen!). Der Film ist einfach empfehlenswert!

Übrigens gibt es mit Windows Vista demnächst ganz neue Viren: Wenn Sie bei eingeschalteter Spracherkennung eine dafür präparierte Webseite angezeigt haben, kann es sein, dass eine Stimme beginnt, Windows-Kommandos zu sprechen. Zumindest sollte es so möglich sein, den PC herunterzufahren, die Übertragung eines Schadprogramms würde wohl etwas dauern.

ZIV-Aktuell

Neue SPAM- und Virenerkennung im Regelbetrieb

D. Bucher

Hier soll noch einmal dafür geworben werden, Spam- und Virenmails zentral löschen zu lassen.

Das ZIV hat zur Verbesserung der SPAM- und Virenerkennung ein neues Produkt getestet und es am 19.01.2007 in den Regelbetrieb überführt. Damit steht ein nun effektives Werkzeug im Umgang mit SPAM zur Verfügung. Die SPAM-Erkennungsrate liegt bei etwa 90 % mit einem extrem geringen Fehlerkennungswert von 1:1 Million. Durch den Einsatz dieser Geräte ergeben sich einige Änderungen und neue Möglichkeiten für die Nutzerinnen und Nutzer.

SPAM-Erkennung

Es besteht nun die zu empfehlende Möglichkeit, erkannte SPAM direkt löschen zu lassen. Die erforderliche Genehmigung können Sie uns unter dieser URL erteilen:

`http://www.uni-muenster.de/ZIV/Service/ironport-email.html`

Hier finden Sie auch detailliertere Informationen zur SPAM- und Virenfilterung. Falls Sie uns die Genehmigung nicht erteilen, wird SPAM weiter in Ihr Postfach ausgeliefert. Es ändert sich aber die Art der Markierung erkannter SPAM. Sie wird mit der Kopfzeile:

```
X-Spam-Symantec: YES
```

gekennzeichnet. Lokale SPAM-Filter müssen ggf. von Ihnen angepasst werden.

Viren-Filterung

Erkannte Viren werden entfernt und die Mail mit einer Ergänzung im Betreff/Subject markiert. Die Mails werden dann zugestellt. Es besteht analog zur SPAM-Behandlung die Möglichkeit, erkannte Virenmails ohne weitere Benachrichtigung löschen zu lassen.

Vollwertige Nutzerkennungen für Erst-Immatrikulierte

R. Mersch

Erst-immatrikulierte Studierende erhalten seit Ende Januar 2007 unmittelbar eine vollwertige und bis (mindestens) zur Exmatrikulation gültige Nutzerkennung. Die vormals erforderliche initiale Freischaltung braucht somit nicht mehr durchgeführt zu werden.

Der HR-Feed (Einspeisung der Personendaten aus den maßgeblichen Datenbanken der Universitätsverwaltung in die Nutzerverwaltung) der Studierenden-Daten führte in der Vergangenheit zur Erzeugung einer vorläufigen Nutzerkennung in der Nutzergruppe `u1stud`. Erst mit der Freischaltung über ein Web-Formular (MeinZIV) wurde diese Kennung der Nutzergruppe `u0dawin` zugeordnet und erhielt somit elementare Rechte wie

- Benutzung des E-Mail-Systems des ZIVs,
- Eintragung in die Windows-Domäne `uni-muenster` und somit Benutzung vieler Windows-Arbeitsplätze in der Universität,
- Benutzung der Netzzugangs-Systeme, also insbes. Nutzung des Funk-LANs.

Das alte Verfahren führte zu häufigen Rückfragen und somit langen Warteschlangen am Service-Schalter des ZIVs zu Semesterbeginn. Außerdem erfordern die immer breitere Verbreitung findenden Online-Verfahren, dass Studierende von Anfang an via E-Mail erreichbar sind. Aus diesen Gründen wurde das Verfahren nun dahin gehend verändert, dass die mit dem HR-Feed übermittelten Nutzerkennungen der neu immatrikulierten Studierenden unmittelbar in der Nutzergruppe `u0dawin`, und somit mit vollen Rechten, erzeugt werden. Außerdem werden die Kennungen automatisch in bestimmte Fachbereichs-Gruppen eingetragen, wenn die Voraussetzungen erfüllt sind (Studium in einem passenden Fachbereich bzw. Studiengang). Dies sind die Gruppen `h0stud` (Psychologie), `o0stud` (Mathematik), `p0stud` (Physik), `q0stud` (Chemie), `r0stud` (Biologie), `s0studm` (Mineralogie) und `t0stud` (Sport).

Voraussetzung für das neue Verfahren war die Änderung des Anschreibens an die Studierenden. Mit der Mitteilung der Nutzerkennung und des Anfangspasswortes werden die Studierenden nun auf die Nutzungsordnung und datenschutzrechtliche Belange hingewiesen.

Die zu dieser Nutzerkennung gehörende E-Mail-Adresse im ZIV (*nutzerkennung@*uni-muenster.de) wird von der Universitätsverwaltung als Kontaktadresse betrachtet. Die Universität erwartet, dass der/die Studierende unter dieser Adresse erreichbar ist. Dieses E-Mail-Konto sollte also regelmäßig bearbeitet werden.

Schon seit einiger Zeit werden die Studierenden-Kennungen automatisch verlängert, so dass die Verlängerung via Online-Formular ebenfalls nicht mehr nötig ist. Erst mit der Exmatrikulation erlischt der Zugang zu den Studierendengruppen und damit auch die Kennung selbst, wenn sie nicht inzwischen anderen dauerhaften Gruppen, wie etwa der Mitarbeitergruppe, zugeordnet wurde.

Nicht betroffen von dem neuen Verfahren sind Studierende, die bereits eine nach dem alten Verfahren erzeugte vorläufige Kennung besitzen, diese aber noch nicht freigeschaltet haben. Für sie ist die einmalige Freischaltung weiterhin erforderlich.

Neue Service-Rufnummern des ZIV

W. Kaspar, M. Speer

Einige wichtige Service-Rufnummern des ZIV wurden auf prägnante, auf „00“ endende Nummern umgestellt.

Folgende, größtenteils neue Service-Rufnummern wurden eingerichtet (dabei handelt es sich jeweils um die Durchwahl; bei externen Anrufen bitte 83 vorwählen):

- 31100 Benutzerverwaltung
- 31200 NTC (Netz-Technik-Center, Rechnernetz-Technik)
- 31400 NIC (Netz-Informations-Center, Rechnernetz-Verwaltung)
- 31500 NOC (Netz-Operating-Center, Rechnernetz-Betrieb und -Störungsmeldung)
- 31600 Zentrale Servicestelle „ZIVline“ (Hotline)
- 31700 Service-Schalter in der Einsteinstr. 60
- 31900 Benutzerberatung in der Einsteinstr. 60

Auch die in der Vergangenheit für die oben genannten Dienste veröffentlichten Rufnummern funktionieren noch bis auf Weiteres.

Neues vom Parallelrechner ZIVcluster

Martin Leweling

Es gibt bereits jetzt mehr Plattenplatz für die Benutzer und ab März 2007 ein neues Batchsystem.

Am Dienstag, den 12. Dezember 2006, wurde der Plattenplatz im GPFS (General Parallel Filesystem) des ZIVClusters morgens um ca. 9 Uhr routinemäßig überprüft. Innerhalb von wenigen Tagen war der freie Bereich von etwa 120 GB auf etwa 7 GB geschrumpft, und er verringerte sich weiter um etwa 10 MB pro Minute. Eine Notfallmaßnahme musste also her, wobei möglichst keine Beeinträchtigung der Benutzer stattfinden sollte, da man diese ja nicht mehr vorwarnen konnte.

Zufälligerweise war am Vortag die Hardware für das neue Raidsystem des ZIVclusters in Betrieb genommen worden und musste nur noch als RAID5 für das GPFS konfiguriert werden. Es handelt sich hierbei um ein IBM System Storage DS4700 mit 16 Fibre Channel SCSI-Platten (je 136 GB, 15000 RPM). Diese wurden in 3 RAID5-Arrays mit je 5 Platten (4 plus Parity) und eine Hot-Spare-Platte aufgeteilt, wobei jedes RAID5 noch in zwei logische Laufwerke partitioniert wurde. Insgesamt ergibt das 6 logische Laufwerke der Größe 272,5 GB. Bisher bestand nun das GPFS ebenfalls aus 6 lo-

gischen Laufwerken der Größe 93,6 GB, die optimal ausbalancierte Konfiguration bei 3 Fileservern und 2 RAID-Controllern. Für eine reibungslose Migration stellt das GPFS einen Mechanismus bereit, einzelne logische Laufwerke im laufenden Betrieb zu ersetzen, also ohne das Dateisystem „unmounten" zu müssen. Dabei darf das neue Laufwerk auch größer sein; das Dateisystem wird dabei automatisch angepasst. Innerhalb eines Vormittages konnte so ohne Beeinträchtigung der Benutzer das GPFS-Dateisystem von etwa 570 GB auf 1,6 TB erweitert werden, mit deutlich schnelleren Festplatten und einem vielfach schnelleren RAID-System. So stieg die maximale Schreib-Performance gegenüber dem alten Zustand von etwa 37 MB/s auf etwa 118 MB/s.

Natürlich bedeutet der vergrößerte Plattenplatz auf dem ZIVcluster nicht, dass Benutzer nun verschwenderischer damit umgehen sollten. Der Benutzer ist weiterhin selbst für regelmäßiges Aufräumen und ein langfristiges Archivieren seiner Daten verantwortlich. Vom ZIVcluster selbst werden nur verhältnismäßig kurzfristige Backups angelegt. Insbesondere Nutzer, die ihre zentrale Nutzungsberechtigung verlieren, sollten rechtzeitig ihre ZIVcluster-Daten sichern, da die Daten abgelaufener Benutzerkennungen bei Bedarf nach frühestens drei Monaten ohne Archivierung gelöscht werden.

Eine weitere Neuerung kommt auf die Benutzer im März zu (voraussichtlich zweite Märzwoche, Ankündigung erfolgt in den HotNews): Das alte Batchsystem PBS Pro, das im letzten Jahr nach neuen Versionen einige wirklich lästige Bugs eingeführt und vormals funktionierende Features fallen gelassen hat, wird durch die kostenlose Open Source-Alternative Torque/Maui ersetzt (siehe `http://www.clusterresources.com/pages/products.php`). Bei den besonders störenden Bugs bzw. „Features" im PBS Pro sind hier fehlende Unterstützung von SSH-X11-Forwarding, nicht funktionierende Zeitreservierungen in dedizierten Queues, unzuverlässige Hilfeleistung bei „verhungernden" Rechenjobs, sowie zusätzlich erforderliche Lizenzen bei Hyperthreading-Aktivierung zu nennen. Man bekommt die fehlenden Features zwar nicht garantiert mit dem neuen System, aber wenigstens muss dann kein Geld für teure Jahreslizenzen ausgeben werden. Leider sind die Binärformate der Jobdateien von PBS Pro und Torque nicht zueinander kompatibel, so dass die Queues des ZIVclusters entweder vor der Einführung des neuen Batchsystems leerlaufen müssen, oder nach der Neuinstallation von Torque nicht gestartete Jobs gelöscht und neu abgeschickt werden müssen. In jedem Fall sollten sich die Benutzer mit der Dokumentation von Torque auseinandersetzen, die rechtzeitig (etwa ab Ende Februar) auf den Dokumentations-Webseiten des ZIVclusters zu finden sein wird (`http://www.uni-muenster.de/ZIV/Server/ZIVcluster/dokumentation.html`). Prinzipiell sind die Befehle von PBS Pro und Torque einander sehr ähnlich, da sich beide aus dem gleichen Vorgänger – der sich nun OpenPBS nennt – entwickelt haben.

Neue Lizenzperiode für die Statistiksoftware SPSS

Chr. Schild

SPSS erfreut sich großer Beliebtheit, Preis bleibt unverändert.

Vergangenen Dezember ist SPSS mit einer neuen Lizenzperiode an den Start gegangen. Wie üblich kann beim ZIV wieder eine frische Lizenz mit der Laufzeit Dezember 2006 bis November 2007 erworben werden. Der Preis hat sich nicht geändert und liegt für die Einzelplatzlizenz wie gehabt bei 50 €.

Der im letzten Jahr hinzugekommene zentral installierte Lizenzserver, der statt einer Einzelplatzlizenz genutzt werden kann, hat sich in letzter Zeit großer Beliebtheit erfreut und wurde rege genutzt. Hunderte von Nutzern haben dieses Angebot des ZIV aufgegriffen und den – im Gegensatz zur Einzelplatzlizenz – kostenlosen Lizenzserver verwendet. Der Lizenzserver hat dabei die Einzelplatzlizenz-Installationen aber nicht komplett ablösen können. Hierfür bestand immer noch Nachfrage, da der Lizenzserver nicht in jedem Szenario verwendet werden kann.

Interessanterweise hat sich im letzten Jahr der Bedarf an Einzelplatzlizenzen trotzdem mit fast 300 verkauften Exemplaren zum Vorjahr fast verdoppelt. Unsere Vermutung ist, dass aufgrund des Labels „kostenlos" das Produkt SPSS stark beworben wurde und so

mehr Nutzer auf das mit 50 € immer noch sehr günstige Angebot des ZIV aufmerksam wurden.

Aktuell ist immer noch SPSS in der Version 14 (verfügbar in deutsch und englisch). Im Laufe des Jahres kommt Version 15 hinzu. Für ganz Eilige ist bereits die Version 15 auf englisch vorhanden. Leider nicht mehr als Einzelplatzlizenz verfügbar ist SPSS 13, hier wurden keine Lizenzen mehr von SPSS geliefert. Ausnahme ist der Lizenzserver, verwendet man diesen, so sind dort noch SPSS-13-Lizenzen abrufbar. In diesem Jahr ist letztmalig ausnahmsweise noch eine Lizenz für SPSS 12 mitgeliefert worden, dies wird im kommenden Jahr nicht mehr der Fall sein. Wir empfehlen dringend allen Nutzern, auf die jeweils neueste Version aufzurüsten. Jeder, der bereits eine Lizenz erworben hat, kann mit Erscheinen der neuen Version beim ZIV die neue Software und eine neue Lizenz abholen, die Lizenzkosten sind gültig für das laufende Lizenzjahr für die komplette Produktpalette von SPSS, also auch neuere Software-Versionen.

Die über das ZIV beziehbare Lizenz für SPSS umfasst die folgenden SPSS-Module:

- Base
- Advanced Models
- Regressive Models Trends
- Categories
- Conjoint
- Missing Values
- Exact Test
- Tables

Hinzu kommen die Produkte Amos (aktuell Version 6.0, bald 7.0), sowie AnswerTree 3.1 und Data Entry Builder 4.0.

Weitere Informationen zu SPSS und zum Bestellverfahren finden Sie auf folgender Webseite:

`http://www.uni-muenster.de/ZIV/Software/SoftwareVerteilungSPSS.html`

Neues von perMail

R. Perske

Unser Webmail-Programm perMail wird ständig weiter entwickelt. Aber auch ein Blick in frühere Veröffentlichungen lohnt sich – nicht nur für neuere Nutzer.

Für neuere perMail-Nutzer empfehlen wir unsere Seite `http://www.permail.uni-muenster.de`. Diese enthält alle Anleitungen, Artikel, Hinweise, Dokumentationen und Online-Hilfen, die wir in den letzten Jahren über perMail veröffentlicht haben. Auch erfahrene Nutzer finden dort sicherlich noch manchen interessanten Hinweis.

Einen Überblick über alle Änderungen und Erweiterungen finden Sie wie immer unter `http://permail.uni-muenster.de/help-de-changes.html`. Aktuell gibt es neben einer Reihe geringfügiger Verbesserungen vor allem folgende wesentliche Erweiterungen:

- Wenn man mehrere E-Mails zusammen in einer E-Mail weiterleitet, entsteht eine Sammlungs-E-Mail. Auch Mailinglisten schicken bei entsprechender Einstellung alle Beiträge eines Tages als eine Sammlung (Digest). Schon bisher konnten mit perMail einzelne E-Mails aus so einer Sammlung herauskopiert und als normale E-Mail in einem Ordner abgelegt werden. Jetzt können Sie alle E-Mails der Sammlung mit einem einzigen Mausklick herauskopieren und ablegen.
- Die bisher fest vorgegebenen beiden Anordnungen „eng“ und „breit“ der Spalten auf der Index-Seite können jetzt beide auf der Einstellungen-Seite frei konfiguriert wer-

den. Dabei können jetzt auch etliche weitere Spalten aktiviert werden und wurden einige bisherige Sammelspalten in Einzelspalten aufgeteilt.

- Es gibt jetzt erheblich mehr Sortierkriterien für die Index-Seite. Durch Klick auf den Kopf einer Spalte kann nach dieser Spalte sortiert werden, weitere Sortierkriterien lassen sich an gewohnter Stelle mit einem Auswahlfeld aussuchen.
- Vorherige Sortierkriterien bleiben als sekundäre Sortierkriterien erhalten: Wer also nach Absender und bei gleichem Absender nach Datum sortieren möchte, der klickt erst auf den Kopf der Datum-Spalte und danach auf den Kopf der Absender-Spalte.
- Überlange Adressen und Betreffzeilen werden auf der Index-Seite abgekürzt. Die Maximallänge können Sie selbst einstellen. Die Voreinstellungen sind großzügig bemessen, so dass nur extrem lange Angaben gekürzt werden.

Auch allen perMail-Nutzern wird empfohlen, unter MeinZIV (ohne Neueingabe des Passworts erreichbar über die Einstellungen-Seite von perMail) die zentrale Spam-Filterung für das eigene Postfach zu aktivieren, so dass die allermeisten Spam-E-Mails gar nicht mehr im Postfach landen. Falls danach noch Bedarf besteht und Sie die Mühe des Trainings auf sich nehmen möchten, können Sie die in perMail eingebaute trainierbare Spam-Erkennung als zusätzlichen Filter einsetzen; den ausführlichen Artikel finden Sie unter oben angegebener Adresse.

Abschaltung des WLAN „Funk-Hoer1“ – Geänderter Zeitplan

D. Frieler

Aus „Funk-Hoer1“ wird „uni-ms“.

Das Netz Funk-Hoer1 wurde nicht wie angekündigt am 01.01.2007 abgeschaltet, sondern wird erst am 01.03.2007 heruntergefahren!

In infoWWW Nr. 03/2006 wurde berichtet:

`http://www.uni-muenster.de/ZIV/inforum/2006-3/a04.html`

„In den WLAN-Funkzellen der Universität und des UKM wird bisher im Allgemeinen ein ‚offener Zugang‘ angeboten. Das heißt, dass Verschlüsselungsmechanismen nicht zwangsweise eingesetzt werden, vielmehr ist es Sache des Nutzers sichere Protokolle zu verwenden. Diese Funkzellen mit dem Funknetznamen (SSID) ‚Funk-Hoer1‘ werden nun abgelöst durch Zellen nach aktuellem Standard (IEEE 802.11i) mit der SSID ‚uni-ms‘.“

Anbindung des MPI-Neubaus an das Wissenschaftsnetz Münster

M. Ketteler-Eising, M. Speer

Der Neubau des Max-Planck-Instituts für Molekulare Biomedizin in der Röntgenstr. 20 wurde im Oktober 2006 an das vom ZIV betriebene Wissenschaftsnetz Münster (WNM) angebunden.

Das WNM stellt ein leistungsfähiges Kommunikationssystem für eine Kooperation zwischen in Münster angesiedelten Einrichtungen dar. Insgesamt sind nun u. a. folgende Einrichtungen an das WNM angeschlossen:

- Westfälische Wilhelms-Universität Münster
- Universitätsklinikum Münster
- Fachhochschule Münster
- Max-Planck-Institut für molekulare Biomedizin
- eine Vielzahl von Studierendenwohnheimen verschiedenster Träger

Sophos-Virenschutzprogramme neu im Softwareangebot des ZIV

Chr. Schild

Sophos Anti-Virus erweitert die Virenschutz-Produktpalette

Während in der Universität Münster die Antiviren-Software von McAfee weit verbreitet ist und weiter genutzt werden soll, wurde im letzten Jahr auf Landesebene ein Rahmenvertrag mit der Firma Sophos geschlossen, der bis 2011 allen öffentlichen und privaten Einrichtung im Bereich Forschung und Lehre die Nutzung von Sophos-Anwendungen gestattet.

Das ZIV hat die Gelegenheit genutzt und folgende neuen Softwareprodukte mit in das Softwareangebot aufgenommen.

- Sophos Anti-Virus (SAV)
- Sophos Client Firewall (SFC)

Laut Beschluss der zuständigen Gremien und des Rektorats sollen Produkte, die die Sicherheit der Endgeräte und des Netzwerkes erhöhen, auf allen dienstlichen und auf privaten Rechnern der Mitarbeiter/innen und Studierenden installiert werden, wenn diese auch zum Zugang zur Universität genutzt werden. Nutzberechtigt sind also alle Angestellten und Studierende der Universität Münster. Die Nutzung der Sophos-Software ist kostenlos.

Im ZIV wurde die nötige Infrastruktur für den „Roll-Out“ der Sophos-Anti-Virus-Software aufgebaut, so zum Beispiel die Server zum Download der Software und der Anti-Viren-Updates.

Weitere Informationen zum Download und zur Konfiguration der Software finden Sie auf den Webseiten des ZIV: `http://www.uni-muenster.de/ZIV/Software/SoftwareVerteilungSophosAntivirus.html`.

Neue leistungsfähige Infrastruktur für die Teleport-DSL-Zugänge

M. Speer

Im Rahmen des „Teleport-Projektes“ wurde in Zusammenarbeit mit der T-Systems und der Fachhochschule Münster die Netzinfrastruktur für die DSL-Zugänge in den Wohnheimen des Studentenwerks innerhalb kürzester Zeit auf eine neue leistungsfähige Basis gestellt. Für die DSL-Nutzer stehen nun höhere Bandbreiten (bis 20 Mbps) zur Verfügung.

Das im infoWWU Nr. 3/2003 (Artikel „Über 500 Teleport-ADSL-Anschlüsse geschaltet“) dargestellte technische Konzept wurde grundsätzlich erneuert. Die Netzplattform des Teleport-Netzes wurde von der T-Systems von ATM-Technologie auf Gigabit-Ethernet-Technologie umgestellt. Ebenso wurde auf Seiten der Universität die ATM-Technologie für die Verbindung zum Teleport-Netz durch Gigabit-Ethernet-Technologie ersetzt.

Kundenseitig fand gleichzeitig eine Umstellung der ADSL-Technik auf ADSL2+ und eine Umstellung der Einwahltechnologie von PPTP auf PPPoE statt. Im Rahmen dieser Umstellung gelang es, von Anfang September bis Mitte Dezember 2006 sämtliche DSL-Bestandskunden (ca. 500 Kunden an ca. 10 Standorten) auf die neue Netztechnik umzustellen. Zusätzlich konnte die Zahl der DSL-Kunden in diesem Zeitraum auf insgesamt nun fast 1100 erhöht werden.

Das ZIV betreibt in diesem Zusammenhang die Netzzugangstechnologie für den authentifizierten Übergang der PPPoE-Verbindungen in das Universitätsnetz und das Internet. Außerdem ist die Weiterleitung von Verbindungen von Studierenden der Fachhochschule via L2TP zu einem System der Fachhochschule realisiert. Die technischen Details der Lösung werden in einem zukünftigen infoWWU-Artikel erläutert werden.

`www.teleport-online.de`

NOC Statistik 2006

M. Kamp, N. Gietz

Das Case-Management-System NOCase hat sich im Jahre 2006 für den NOC-Dienst bewährt.

Das in die Netz-Datenbank des ZIV integrierte Case-Management-System NOCase (Trouble-Ticket-System) hat sich zu einem unverzichtbaren Werkzeug für das Netz-Operations-Center (NOC) etabliert.

Im Jahre 2006 wurden 5037 Vorgänge (Cases) erfasst. Betrachtet man die jeweiligen Kundenbereiche, so entfallen 43,5 % der Fälle auf die Universität, 43,2 % auf das UKM, 7 % der Fälle betrafen ZIV-interne Vorgänge, der Rest betraf Zugangsnetze, Teleport und anderes.

In 9 % der Fälle handelte es sich um Beratungen aller Art, 42,3 % waren Änderungswünsche, also meist die Umstellung eines Netzanschlusses, und 43,5 % der Fälle waren Störungsmeldungen aller Art, also sowohl Störungen im Netz als auch Störungen, die vom Kunden selbst verursacht wurden.

Die Reaktionszeit seitens des NOC auf die einzelnen Vorgänge ist im Allgemeinen sehr gut. In über 80 % der Fälle wurde nach einer Stunde auf einen Vorgang reagiert, mehr als 50 % der Fälle waren sogar schon nach einer Stunde erledigt. Nach drei Stunden wurde auf über 90 % der Vorgänge reagiert und nach einem Tag waren über 85 % der Vorgänge abgeschlossen.

Die außerhalb der Dienstzeiten betriebene Rufbereitschaft des NOC wurde in 10 Fällen alarmiert.

Bei allen genannten Fällen hat sich das NOCase-System als unverzichtbare Hilfe erwiesen um die zeitnahe Bearbeitung zu gewährleisten und einzelne Vorgänge nicht aus dem Auge zu verlieren. Aus diesem Gründen sollten alle Kunden darauf achten, dass ihnen vom NOC eine NOCase-Nummer zugewiesen wird, um selbst Rückfragen zu den eigenen Vorgängen stellen zu können.

Neues von Multimedia

A. Scheffer

Für Nutzer an der WWU stehen im Servicepunkt Foto des ZIV seit kurzem ein A3-Scanner, Prozessorleistung aus 4 Kernen und neue Kurzanleitungen zu multimedialen Aufgaben bereit.

Im ZIV steht mit Erscheinen dieser infoWWU-Ausgabe auch ein A3-Scanner zur Verfügung. Eine Kurzanleitung für Einsteiger gibt es wie gewohnt im Netz. Des Weiteren sind nun Anleitungen zu häufigen Anfragen verfügbar wie z. B. „Doppelseitig scannen mit einseitigem Papiereinzug“ oder „Automatisches Scannen von mehreren Fotos ohne Fotoeinzug“. Die Nutzung insbesondere der geräteunabhängigen Anleitungen ist durch das Multimedia-Portal unter

`http://www.uni-muenster.de/ZIV/Multimedia/`

auch vom Heimarbeitsplatz aus möglich. Für die Bildbearbeitung detailintensiver Vorlagen steht dem Scanner ein leistungsstarker Rechner zur Seite, dessen Software-Stand in naher Zukunft weiter ausgebaut werden soll, um verschiedenartigen grafischen Ansprüchen gerecht zu werden. Für die Nutzung der beiden neuen Geräte sprechen Sie bitte direkt mich an (Tel. 31851, E-Mail `scheffa@uni-muenster.de`) – eine Buchbarkeit über das Online-System ist im Anschluss an das nun stattfindende Multimedia-Praktikum geplant.

ZIV-Präsentation

Digitale Übertragung aus Hörsälen

L. Elkemann

Eine große Anzahl von Hörsälen und Seminarräumen der Universität Münster sind mittlerweile mit audiovisueller Medientechnik ausgestattet. Eine Übersicht der von der Kommunikations- und Medientechnik der Universität, kurz KM genannt, ausgestatteten Räume ist auf der Webseite `http://www.uni-muenster.de/rektorat/km/hoersaele/index.html` dargestellt.

Die Übertragungen von Bild und Ton aus Hörsälen in andere weiter entfernte Räumlichkeiten war in der Vergangenheit zwar nicht die Regel, wurde aber doch schon mehrfach nachgefragt und wurde in einigen Fällen bereits ermöglicht und zwar über die standardisierten Methoden des Videoconferencing, insbesondere mit mehreren Videokonferenz-Endpunkten (aktiven Teilnehmern). Auch Mehrpunktkonferenzen und Konstellationen mit einem Sender und mehreren Empfängern sind im LAN mittels einer sogenannten MCU, Multipoint Control Unit, möglich. Alle Varianten unterstützen eine Vielzahl von standardisierten Kommunikationsverfahren (sog. Protokollen) wie H.323 und H.320. Somit können sowohl LAN- als auch ISDN-Verbindungen unterstützt werden.

Neben diesen Möglichkeiten, die bidirektionale Übertragungen darstellen, d. h. alle Standorte bekommen mehr oder weniger simultan alle Informationen, gibt es darüber hinaus Situationen, dass lediglich eine Quelle ihre Bild- und Toninformationen an mehrere Empfänger senden soll. Die Empfänger „schauen“ und „hören“ lediglich zu, ohne selbst Sender von Bild- und Tonsignalen zu sein. Dieses Verfahren wird als unidirektional bezeichnet. Das „Videostreaming“ ist eine typische Anwendung dieser Art der Übertragung.

Videostreaming über das LAN

Am 17.01.2007 wurde eine Senatsversammlung aus dem Senatssaal der WWU, Schlossplatz 2, in den Hörsaal 7 , Schlossplatz 7, erstmals live mittels Videostreaming übertragen. Die bereitgestellten Bild- und Tonsignale wurden mittels eines Proxy-Servers in das LAN der WWU als MPEG-2-Stream eingespielt.

An den Remote-Standorten, Hörsaal PC 7 und dem Kontrollcenter für die Bild- und Tonregie kamen der Windows Media Player und der kostenlose Media Player VLC als Softwarelösung zum Einsatz. Sowohl die Ton- als auch die Bildqualität war zufriedenstellend. Es kam während der Übertragung zu keinen Ausfällen oder Einfrierungseffekten der Übertragung. Solche Mängel waren in der Vergangenheit häufige Begleiterscheinungen dieser Übertragungsverfahren.

Ausgehend von diesem Live-Test wird der Ausbau dieser Anwendung dahingehend optimiert werden, dass zukünftige Übertragungen mit höheren Auflösungen (bisher ¼ Fersehnorm) und höheren Bildwiederholraten (bisher 25 Bilder pro Sekunde), stattfinden werden. Auch werden die Mitarbeiter, die für die Live-Übertragung von Veranstaltungen verantwortlich sind, zukünftig auf hardwarebasierte Videoserver- und Encoderlösungen zurückgreifen können, die eine gewisse Robustheit vorweisen können; im Vorfeld einer Übertragung ist die Zeit für Einrichtungsarbeiten oftmals nur bedingt vorhanden.

In Zukunft sind Übertragungen von Veranstaltungen aus der Universität überall, wo ein LAN- Anschluss vorhanden ist, über diesen Weg möglich. Parallel dazu stehen natürlich die anderen oben schon erwähnten Videokonferenzlösungen ebenfalls zur Verfügung, z. B. gerade dann, wenn eine Veranstaltung nach Übersee übertragen werden soll; hier sind nach wie vor die besten Ergebnisse über eine MCU mittels einer LAN-ISDN-Kopplung erreichbar. Ein Grund hierfür ist die fehlende Priorisierung von Echtzeitdaten innerhalb des globalen Internet, während bei ISDN-Nutzung Bandbreite exklusiv zur Verfügung steht. Die Performance des LANs der Universität ist jedoch bestens für Videostreaminglösungen geeignet, abgesehen von wenigen Ausnahmen. Genaue Informationen können im ZIV unter der Hotline-Nummer 31599 oder ✉ `NOC@uni-muenster.de` erfragt werden, am besten ist jedoch stets ein frühzeitiger Test.

Ausnahmslos gilt für alle Übertragungsmöglichkeiten die Notwendigkeit des Einsatzes von guten Kameras und Mikrofonen. Nur die Signale, die von hochwertigen Geräten bereitgestellt werden, können sinnvoll weiterverarbeitet und übertragen werden. Die von der Abteilung Kommunikations- und Medientechnik der WWU Münster eingesetzten Kameras und Mikrofone genügen diesen Anforderungen.

Bitte beachten Sie auch: Ein Großteil der durch den Bereich KM betreuten Veranstaltungen (und Übertragungen) werden generell oder auf Anfrage aufgezeichnet und können anschließend auf DVD oder VHS-Bändern den Veranstaltern zur Verfügung gestellt werden.

Unter ✉ km@uni-muenster.de stehen Ihnen der Bereich Kommunikation und Medien gerne für weitere Fragen zur Verfügung.

Aufgabenverteilung in der Informationsverarbeitung (IV)

Ein Bericht der IV-Kommission, Januar 2007

W. Held, W. Bosse, M. Goden, J. Lorenz, M. Möller, J.-A. Reepmeyer

1. Aufgabenteilung zwischen ZIV und IVVen

1.1 Allgemeine Situation

Vier Jahre nach dem letzten Bericht (Dezember 2002) soll auf Veranlassung der IV-Kommission das Münsteraner Modell der IV-Organisation und der Aufgabenverteilung zwischen IV-Versorgungseinheiten (IVVen) und dem Zentrum für Informationsverarbeitung (ZIV) erneut einer kritischen Würdigung durch die Beteiligten unterzogen werden. Zugleich soll aufgezeigt werden, wie sich geänderte Randbedingungen niederschlagen und Korrekturen an der Ausgestaltung des Modells erfordern.

Die Aufgabenteilung zwischen ZIV und IVVen ist unumstritten. Das ZIV erbringt vorrangig grundlegende Unterstützungs- und Infrastrukturleistungen für die IVVen und nimmt Koordinierungsaufgaben wahr. Die Betreuung der Endnutzer und Rechnersysteme in den einzelnen Fachbereichen und Einrichtungen soll durch die jeweiligen IVVen erfolgen, wobei im Bereich der Kommunikationssysteme sich viele Nutzer direkt an das ZIV wenden. Bei der Bewältigung dieser Aufgaben sollen die IVVen auch auf die Dienste des ZIV zurückgreifen können.

Diese Aufgabenteilung hat sich bewährt; konkrete Kritik hat weiter abgenommen. Das Münsteraner Modell ist durch zahlreiche Veranstaltungen, Vorträge und Berichte bundesweit bekannt. In Teilen der DFG-Empfehlung für die IV an Hochschulen für 2006 – 2010 findet man einige Passagen des hiesigen Konzepts fast wörtlich wieder. Mit dem Zuschlag des DFG-Projekts MIRO (Münster Information System for Research and Organization) im Rahmen der Förderung „Leistungszentren für Forschungsinformation“ ist diese IV-Organisation offensichtlich gewürdigt worden. Die IV-Organisation in Münster entspricht übrigens schon seit zehn Jahren den Notwendigkeiten eines universitätsinternen Shared-Service-Centers, eine Organisationsform, die zzt. in der Fachwelt diskutiert und empfohlen wird. Das gute Funktionieren des Gesamtsystems wurde vom Rektorat zum Anlass genommen zu prüfen, ob sich die Strukturen der IV modellhaft auf den Bereich Lehre- Studium-Prüfungen übertragen lassen.

Die Kommunikation zwischen den IVVen und dem ZIV ist ein wesentlicher Punkt des Gesamtsystems. Sie findet zwischen den Experten beider Seiten statt, aber auch zwischen den leitenden Mitarbeitern in regelmäßigen Arbeitstreffen. Wie in jedem größeren Unternehmen gab und gibt es einzelne Probleme in der Kommunikation; es wird aber von allen Seiten ständig daran gearbeitet, diese sachgerecht zu beseitigen. Ein wesentlicher Punkt dabei ist, dass bei allen Mitarbeitern das entsprechende Bewusstsein immer wieder geschärft wird und dass bei der Zusammenarbeit der Kommunikationspartner stets als kompetenter Kollege wahrgenommen wird. Ziel ist die rasche Problemlösung und nicht die Frage, wer Verursacher des Problems ist.

Die Aufgaben sind den IVVen von den Fachbereichen nicht immer gleichartig zugeordnet. Weil die IVVen „funktionieren“, werden sie oft auch als „Mädchen für alles“ betrachtet, also mit Aufgaben betraut, die nur entfernt mit ihren Kernaufgaben der Informationsverarbeitung zu tun haben. Dazu können z. B. gehören: Technische Hörsaalausstattung, Abwicklung der Evaluation, Bibliotheksunterstützung oder Unterstützung der Prüfungsämter und Dekanate. Diese unterschiedliche Auffassung über die Rollen der

IVV in den Fachbereichen war aber bei der Dezentralisierung ausdrücklich so gewollt. Da diese Zuordnungen gleichzeitig darauf hinweisen, dass in den Fachbereichen IV-nahe Aufgaben anstehen, die bisher noch nicht anders gelöst werden, wird später in Abschnitt 2 noch einmal darauf eingegangen.

Benutzern, denen das Münsteraner Modell und die Rolle der IVVen noch nicht vertraut sind, übergehen manchmal die IVVen oder treffen Entscheidungen, die die Arbeit der IVVen erschweren. Hier sollten die Dekanate neue Hochschullehrer und Mitarbeiter entsprechend informieren; ein von den IVVen zusammen mit dem ZIV zu entwickelndes Faltblatt über die IV-Organisation könnte dabei helfen.

Auch nach zehn Jahren haben einzelne Fachbereiche die Neustrukturierung der IV im Personalbereich nicht immer vollständig nachvollzogen. So sind technische Mitarbeiter zur IV-Betreuung immer noch einzelnen Lehrstühlen und Instituten und nicht den IVV en zugeordnet, was die Arbeit der IVVen erschwert.

Viele IVVen leiden unter dem Wegfall der WAP-Anträge. Zum einen fehlen die dafür erforderlichen HBFG-Mittel. Zum anderen führte die Aussicht auf eine Bezuschussung dazu, dass bei den Beschaffungen in den IVVen Standards durchgesetzt werden konnten, die das Management der Arbeitsplatzrechner erleichterten. Mit dem Wegfall des WAP fällt es den IVVen wieder schwerer, auf einheitlichen Regelungen zu bestehen. Hierauf wird später noch einzugehen sein (siehe dazu Abschnitt 3).

1.2 Darstellung der Aufgabenfelder

1.2.1 Koordinationsstelle

Die Koordinierung erfolgt weiterhin im Rahmen der regelmäßigen Treffen der IVV-Leiter mit dem ZIV und in Arbeitsgruppen, die zu einzelnen Themen gebildet werden. Dadurch gelingt eine weitgehende Absprache. Es wäre jedoch wünschenswert, diese Zusammenarbeit weiter zu intensivieren, damit eine noch bessere Arbeitsteilung zustande kommt und zusätzliche Projekte gemeinschaftlich durchgeführt werden können. Beispiele für Projekte, bei denen eine solche Zusammenarbeit sinnvoll wäre, sind u. a. die Verwaltung der Virenscanner, die automatisierte Softwareverteilung und bestimmte Teile des Identitätsmanagements. Eingerichtete Arbeitsgruppen, z. B. zu Windows, werden von einigen Beteiligten manchmal als nicht immer zielführend angesehen. In einigen Fällen mag das am ZIV liegen, in anderen Fällen kann man beobachten, dass einzelne IVVen ihre Vorstellungen in gemeinsamen Lösungen nicht hinreichend berücksichtigt sehen und ihnen daher eigene Lösungen sinnvoller erscheinen. Die IVVen sind jedoch grundsätzlich bereit, rechtzeitig eingeführte zentrale Lösungen einzusetzen, wenn diese ihrer Arbeit nützen. Sie haben ein ureigenes Interesse daran, dass Entwicklungen, die zusammen gehören, nicht auseinander laufen.

Die Informationsangebote von ZIV und IVVen sind noch nicht genügend vernetzt. Die Informationen sollten grundsätzlich von derjenigen Stelle bereitgestellt werden, die laut Aufgabenteilung für die Bearbeitung zuständig ist. Aus Benutzersicht ist es jedoch unbefriedigend, an verschiedenen Stellen suchen zu müssen. Gleiches gilt für die Informationsangebote der Universität. Hier muss doppelte Arbeit vermieden werden. Diese Themen sind deshalb von Anfang an als Arbeitspakete in das MIRO-Projekt aufgenommen worden. Zum einen wird ein gemeinsamer Dienstleistungskatalog für Information, Kommunikation und Medien (IKM) entstehen, der auch die Dienste der IVVen umfassen soll. Damit soll die an der WWU in einzelnen Bereichen vorhandene Spezialkompetenz besser zu erschließen sein und zur Lösung schwieriger Aufgaben, z. B. im Unix/Linux- oder im Windows-Bereich, herangezogen werden können. Zum anderen werden Portale und Suchmaschine, die zur Basisinfrastruktur von MIRO gehören, das Informationsmanagement in der Universität deutlich verbessern. Die IVVen werden in diese Entwicklung stärker eingebunden werden, damit Layout und Inhalte dem Bedarf der Universität entsprechend gut abgestimmt werden. Darüber hinaus wird die Unterstützung der IVVen zur Verbreitung der neuen Möglichkeiten dringend benötigt.

Das seit einiger Zeit im Aufbau befindliche Identitätsmanagementsystem wird im zweiten Quartal 2007 in Betrieb gehen. Komplexe Fragen des Datenschutzes haben viel Auf-

wand bei seiner Einführung verursacht. Die vom ZIV bisher schon aus der alten Nutzerverwaltung versorgten Active-Directory-Services (ADS) werden vom Identitätsmanagement weiterhin bedient werden. Neu hinzu kommende ADS können zukünftig vom Identitätsmanagement mit den darin enthaltenen Nutzerkennungen provisioniert werden.

Problematisch bleibt jedoch aus Sicht des ZIV der Umgang mit unterschiedlichen ADS einzelner IVVen, wenn diese weiterhin heterogen konfiguriert werden, um z. B. so genannte Schemaerweiterungen sehr schnell durchführen zu können. Schemaerweiterungen sind als heikel anzusehen, weil sie manchmal überhaupt nicht oder nur schwer rückgängig zu machen sind. Wegen dieser Konsequenzen gilt eine Verabredung mit fast allen IVVen, dass derartige Änderungen nur nach vorheriger Abstimmung innerhalb einer Woche durchgeführt werden. Solange man sich in der Hierarchie eines einzigen ADS bewegt, lassen sich z. B. Administrationsaufgaben und Zugänge zu Ressourcen anderer Domänen relativ einfach lösen. Wenn man jedoch, wie in Einzelfällen gewollt, ein zweites ADS aufgebaut hat, sind diese Vorteile kaum noch zu nutzen. Hier müssen IVV en und ZIV noch einmal einen Versuch zur Vereinheitlichung unternehmen; die Mithilfe der Gremien wäre sicher hilfreich. Wenn dazu die bereits in den IVVen gewachsenen Strukturen weitgehend berücksichtigt werden und den IVVen entsprechende Möglichkeiten zur Selbstverwaltung dauerhaft eingeräumt werden, würde dies die Chancen für einen mehr zentral orientierten Ansatz erhöhen.

1.2.2 Kommunikationssysteme

Die Zusammenarbeit mit dem Bereich Kommunikationssysteme funktioniert in der Regel beim alltäglichen Geschäft problemlos. Störungsmeldungen werden schnell und kompetent bearbeitet. Gelegentlich wird berichtet, dass die Problembehebung verzögert wird, weil sich die Ursache von Störungen nicht immer sofort zuordnen lässt. Eine Ausweitung der Instrumente des Systemmanagements sollte daher angestrebt werden (siehe auch Abschnitt 3).

Die Vernetzung von Daten für Kommunikations- und Rechnersysteme ist in Zukunft so zu organisieren, dass daraus folgende und heute noch bestehende Defizite beseitigt werden.

Die Umsetzung notwendiger Sicherheitsmaßnahmen ist in den letzten Jahren mit der Ausweitung der IV immer wichtiger geworden. Das ZIV ist deshalb mit zahlreichen Maßnahmen wie einem Sicherheits-Audit, VPN-Zugängen, virtuellen Firewalls oder dem Anti-Spam-Produkt BrightMail die Sicherheitsproblematik angegangen. Diese Maßnahmen haben etliche IVVen in ihre tägliche Arbeit aufgenommen.

Die sehr große Zahl der Netzkomponenten erfordert geeignete Instrumente und organisatorische Konzepte für deren Verwaltung. Hierzu wurde vom ZIV das Configuration-Management eingeführt. Die ersten Netzbereiche sind erfolgreich in Zonen mit unterschiedlichem Sicherheitsbedarf strukturiert worden. Wenn die Strukturierung der Netze beschleunigt werden könnte, so wäre dies ein zusätzlicher Sicherheitsgewinn. Allerdings ist der Aufwand auf Seiten des ZIV und der IVVen beachtlich; die Anstrengungen sowohl der IVVen als auch des ZIV müssen also verstärkt werden. So wurden bisher zwar Firewalls für den Zugang zu Subnetzen geschaffen. Die vom ZIV eingestellten Zugangsregelungen werden jedoch erst dann sinnvoll brauchbar, wenn sie zeitnah geändert werden können. Die vorgesehene Möglichkeit, dass die IVVen diese Regeln selbst verwalten können, konnte noch nicht abgeschlossen werden. Vermisst werden auch Vorgaben, Anregungen und Hilfestellungen für die Strukturierung, ohne die aufgrund der Arbeitsbelastung ein solches Projekt kaum umzusetzen sein wird. Durch Formalisierung und Standardisierung der Regeln sollen diese Verfahren erleichtert werden.

Von den IVVen wurde lange Zeit beklagt, dass es von der Beauftragung einer Netzwerkdose bis zu deren Inbetriebnahme zu lange dauert. Dies lag zum Teil an großen Maßnahmen wie den mit Vorrang einzurichtenden ca. 550 zusätzlichen Netzanschlüssen für Kopierer und Drucker verteilt auf alle Gebäude. Derartige Stoßgeschäfte kann das ZIV generell nicht ohne Engpässe an anderer Stelle bewältigen. Außerdem erwies sich die Handhabung für Kleinstaufträge durch Verkabelungsfirmen als ineffizient. Durch zusätzlich aus ZIV-Mitteln eingestellte Mitarbeiter werden 64 bzw. 87 % der Aufträge in-

zwischen nach 4 bzw. 8 Wochen erledigt. Einheitliche Regelungen und Sonderaktionen für die Einführung flächendeckender WLANs oder die Ablösung alter Netzinfrastrukturkomponenten werden ausdrücklich begrüßt.

1.2.3 Rechner- und Betriebssysteme sowie Gemeinschafts-Peripherie

Die auf diesen Bereich entfallenden Aufgaben verursachen in den IVVen sehr viel Arbeit. Hier können aber auch die größten Synergieeffekte erzielt werden. Ein beachtlicher Teil der oben geschilderten Probleme der Kommunikation findet seinen Ausdruck daher in diesem Bereich. Diese Probleme betreffen jedoch normalerweise nicht die bilaterale und persönliche Zusammenarbeit bei konkreten, eng begrenzten Projekten. So wurde bei einer IVV bei der schrittweisen Migration des E-Mail-Services auf die Systeme des ZIV jede Umkonfiguration eng mit dem ZIV abgestimmt, erforderliche Anpassungen an den ZIV-Servern wurden schnell umgesetzt. Eine andere IVV behielt zwar ihren eigenen E-Mail-Server, fand aber mit dem ZIV eine Lösung, die Viren- und Spamkontrolle des ZIV zu nutzen. Diese Lösung war so erfolgreich, dass sie auch von anderen übernommen wurde und von dort weitere Verbesserungen vorgeschlagen wurden. Verschiedene Ansichten der IVVen über die Notwendigkeit, einen eigenen E-Mail-Server zu betreiben, konnten trotz der Empfehlungen des Landesrechnungshofes, der den Betrieb von dezentralen E-Mail-Servern für inakzeptabel hält, nicht zusammengeführt werden. Parallelentwicklungen können in diesem Bereich schon einmal auftreten, wenn eine Entwicklung sowohl von mehreren IVVen als auch vom ZIV aufgegriffen und dann kein integriertes Projekt durchgeführt wird. Die beim Abschnitt „Koordination“ bereits angesprochenen Arbeitsgruppen haben manchmal nicht den gewünschten Erfolg. Eine weitere Verbesserung könnte mit den in Abschnitt 3 besprochenen Perspektiven erreicht werden.

Software, die vom ZIV zum Einsatz gebracht wird, sollte – wo immer das möglich ist – mandantenfähig (wie z. B. die NIC-Online-Datenbank) sein, damit IVVen individuelle Einstellungen vornehmen können, wenn dies unverzichtbar ist. So ist beispielsweise eine Verwaltung der Print&Pay-Druckerwarteschlange für Drucker in den Fachbereichen durch die IVV noch nicht möglich, was die Störungsbeseitigung unnötig verzögert. Nach Aussagen des ZIV ließe sich die dezentrale Administrierbarkeit dieser Drucker kurzfristig realisieren. Auch für die Verwaltung der Anti-Viren-Software würden einzelne IVVen ein zentrales mandantenfähiges System nutzen. Dies ist möglich und wird vereinzelt praktiziert.

Neue Themen sollten von den IVVen und dem ZIV gemeinschaftlich möglichst früh aufgegriffen werden. So ist es z. B. recht bald erforderlich, die zukünftige Bereitstellung von Plattenspeicherplatz (SAN) und damit verbunden die zukünftige Backupstrategie zu besprechen, wenn ein hochschulweites SAN-Konzept, das hohe Investitionen erfordert, eingeführt werden soll. Einige IVVen haben auch hier bereits eigene Lösungen begonnen.

Die vom ZIV organisierten Informationsveranstaltungen finden die ausdrückliche Zustimmung der IVVen.

1.2.4 Anwendungssysteme

Die Zusammenarbeit in diesem Bereich verläuft zwischen IVVen und ZIV problemlos. Die Verteilung der Lizenzen von SPSS, Mathematica etc. funktioniert gut. Eine zentrale Lösung spart erhebliche Lizenzkosten ein.

Neue Anwendungssysteme werden häufig zentral eingeführt; dadurch ergeben sich ganz andere Fragestellungen als bisher, die in den folgenden Kapiteln aufgegriffen werden.

Die ursprünglich in diesem Bereich subsumierten einzelnen Anwendungen, z. B. aus dem Office-Bereich, werden vorwiegend in den IVVen betreut und bereitgestellt. Die IVVen arbeiten aus eigenen Stücken hier intensiv zusammen und nutzen auch die Zusammenarbeit mit dem ZIV.

1.2.5 Mandantenfähigkeit, Transparenz, User Self Care und Leistungsmessung

Mandantenfähigkeit spielt an mehreren Stellen dieses Berichts eine Rolle. Das Thema wurde seit langem von den IVVen gewünscht und von der Abteilung Kommunikationssysteme des ZIV thematisiert. Es ist inzwischen in verschiedener Art und Weise umgesetzt, z. B. in NIC-Online. Die Mandantenfähigkeit ist inzwischen als wichtige Grundlage der Kooperation und Arbeitsteilung ständiges Entwicklungsziel des IV-Gesamtsystems. Ähnliches gilt auch für die Themen Transparenz der Dienste, User Self Care oder die Verabredung von Dienstqualitäten (Service Level). Diese müssen in Zukunft viel stärker als bisher zur Leistungsobjektivierung herangezogen werden. Zum Thema Dienstqualitäten und ihre Überwachung hat das ZIV gerade ein Produkt eingeführt, und auch die IVVen sammeln mit Ihren Systemen Erfahrungen auf diesen Gebieten.

2. Aufgabenteilung mit anderen zentralen Einrichtungen

In den letzten Jahren wurden vermehrt komplexe Anwendungssysteme zur Unterstützung der Geschäftsprozesse (z. B. Content-Management-System Imperia, Evaluationssoftware EvaSys, Verantaltungsverwaltung HISLSF, Prüfungssystem HISPOS oder das System BSCW) an verschiedenen Stellen der Universität implementiert. Für einen einwandfreien Betrieb dieser Systeme sind einerseits umfangreiche IV-Kenntnisse erforderlich, die eine Anbindung an die IV-Struktur im ZIV oder in den IVVen erfordern. Andererseits führt der Einsatz dieser Systeme nur zum Erfolg, wenn die Fachabteilung ihre Arbeiten auf diese Systeme abbilden kann, was für eine Anbindung an die Fachabteilung spricht. Diese Frage der (gemeinsamen) Zuständigkeiten wird von den IVVen unterschiedlich beantwortet. Das Thema sollte aber intensiver diskutiert und von den Gremien begleitet werden.

Bereits im Bericht aus dem Jahre 2002 wurde wegen der ständig weiter wachsenden Aufgaben im IV-Gesamtsystem die Einbeziehung weiterer zentraler Einrichtungen in die Aufgabenteilung gefordert. ULB, UniV und ZIV haben zur Verbesserung übergreifender Dienstleistungen einen gemeinsamen IKM-Service auf dem Gebiet Information, Kommunikation, Medien verabredet und im Jahre 2003 eingerichtet.

Nach Meinung einzelner IVVen wäre es bei Projekten mit IV-Beteiligung, insbesondere dann, wenn Geschäftsprozesse eine Rolle spielen, wünschenswert, wenn sie von den fachlich zuständigen Stellen wie Dekanaten oder Prüfungsämtern von Anfang an breiter als bisher einbezogen würden. Dies ist häufig ein Problem der zentralen oder dezentralen Verwaltung. Mit dem Projekt MOVE, in dem Verwaltungsprozesse gemeinsam mit Fachbereichen und Instituten identifiziert werden, hat die Verwaltung dazu schon einen wichtigen Schritt unternommen, der so mit Leben gefüllt werden könnte.

Die Zusammenarbeit mit dem zentralen Einkauf funktioniert gut. Rahmenverträge erleichtern die Beschaffungen. Das elektronische Vorlesungsverzeichnis ist funktionsfähig, vermag aber derzeit noch nicht alle angestrebten Funktionen zu erfüllen. Deutlich erschwert werden Betrieb und Ausbau des HISLSF-Systems durch das Fehlen einer generellen Regelung der organisatorischen Einbettung in die Arbeit in den Fachbereichen.

Leider hat sich die Arbeit der cHL-Anwendergruppe, die zwischen Fachbereichen und IKM-Service ein Sprachrohr zum eLearning werden sollte, als nicht sehr effizient erwiesen, da einige Vertreter der Fachbereiche kaum mitgearbeitet haben. Hier sollten die IVVen stärker aktiviert werden.

Die Konvergenz der Netze (Telefon- und Datennetz) ist beschlossen und wird derzeit im Detail vorbereitet. In Vorbereitung ist in Zusammenarbeit von Universitätsverwaltung und ZIV die Verbesserung der Infrastruktur für die hochschulweite Verbreitung relevanter Informationen in kritischen Situationen. Dazu gehört z. B. die Alarmierung in Katastrophenfällen.

3. Perspektiven zur Weiterentwicklung der IV-Versorgung

Die IV-Entwicklung bleibt bekanntlich nicht stehen, sie bleibt vielmehr sehr dynamisch. Man tut also gut daran, sich die notwendigen Freiräume für neue Aufgaben und Weiterentwicklungen der IV, von denen einige in den vorangehenden Abschnitten angespro-

chen wurden, zu schaffen, damit Münster in diesem Feld den Vorsprung gegenüber anderen Universitäten wahren kann. Andererseits schafft die Weiterentwicklung aber auch neue technische Möglichkeiten, sich von eingrenzenden Rahmenbedingungen zu lösen. Ein Beispiel hierfür ist die Virtualisierung, die es auf vielen Ebenen erlaubt, Vorgaben der Hardware mehr und mehr auf die Konfiguration eines virtuellen Systems abzuwälzen und die eigentliche Arbeit dadurch zu vereinfachen.

CIP- und WAP-Förderprogramme sind ausgelaufen. Mit HBFG-Mitteln können Server nur noch beschafft werden, wenn sie 200.000 € oder mehr kosten. Es ist daher zu befürchten, dass die notwendigen Koordinierungen bei Beschaffungen unterbleiben, die Heterogenität der Arbeitsplatzrechner wieder zunimmt und damit der Pflegeaufwand steigt. Fast alle Server werden nur noch allein aus Universitätsmitteln finanziert werden müssen, wenn nicht gegengesteuert wird.

Durch Standardisierung der Konfiguration der Arbeitsplatzrechner können Beschaffungskosten aufgrund größerer Stückzahlen verringert werden. Eine Vereinheitlichung würde auch die Folgekosten, u. a. durch eine automatisierte Software-Verteilung, und den bisher dafür notwendigen Personalaufwand reduzieren; dies könnte aber durch die o. a. Virtualisierung in gleicher Weise erreicht werden.

Eine solche Standardisierung ist allerdings nicht leicht zu erreichen, weil sie die Realisierbarkeit unterschiedlicher Ansprüche einschränken würde. So ist selbst der einfache Versuch des zentralen Einkaufs gescheitert, die Ausstattungsmerkmale von drei Standard-Monitoren zu definieren. Um wie viel schwerer dürfte dies bei Arbeitsplatzrechnern oder Notebooks werden. Dennoch muss man die Frage der Standardisierung in den IVVen und auch universitätsweit immer wieder auf die Tagesordnung setzen. Auf den verschiedenen Ebenen, dezentral in den Fachbereichen und IVVen sowie zentral in IV-Kommission, IV-Lenkungsausschuss und Rektorat, sind Anreize und Regelungen zu schaffen, die eine Standardisierung für den einzelnen akzeptabel und vorteilhaft erscheinen lassen.

Der Gemeinschaftsbetrieb von Servern sollte gefördert und zwischen IVVen und ZIV im Hinblick auf noch mehr Gemeinsamkeit ausgerichtet werden, damit eine Beantragung größerer Server-Cluster möglich wird. Universitätsverwaltung und ZIV haben Überlegungen eingeleitet, wie der Betrieb der Server der Verwaltung möglichst bald vom ZIV übernommen werden kann. Die Unterstützung und Forcierung eines gemeinsamen Server-Standortes am Schlossplatz durch die IVVen weist hier in die richtige Richtung. Auch hier bietet die Virtualisierung neue Möglichkeiten, die Geräte besser auszulasten und einen verlässlichen und sicheren Betrieb durch mehr Redundanz und den Einsatz von Instrumenten des Systemmanagements zu ermöglichen, ohne den IVV en die Möglichkeit der eigenen Verwaltung ihrer Systeme zu nehmen.

Diese Maßnahmen entsprechen ernst zu nehmenden Forderungen des Landesrechnungshofes. Sie tragen außerdem zur Weiterentwicklung der bekanntermaßen guten IV-Versorgungsstruktur bei, erleichtern die Einführung neuer IV-Prozesse und stärken Münster im Wettbewerb der Universitäten. Denn die IV-Prozesse, ihre Stabilität und Sicherheit werden immer mehr zu einem prägenden Element einer Universität.

Durch Rationalisierung und Automatisierung frei werdende Arbeitskraft wird dringend benötigt, um die vielfältigen neu anstehenden, oftmals komplexen IV-Prozesse angemessen und gut zu unterstützen. Die inhaltlichen und organisatorischen Voraussetzungen sind, wie in den Abschnitten 1 und 2 beschrieben wurde, nicht immer vorhanden, mit der Folge, dass manche IV-Lösungen und IV-gestützte Geschäftsprozesse zu langsam eingeführt werden.

Eine Möglichkeit zur Verbesserung der Situation besteht darin, dass die IVVen von den Fachbereichen für derartige Anwendungen stärker eingebunden werden, denn sie besitzen das notwendige Know-how. So hätten die Verwaltung und der IKM-Service bei der Einführung neuer Produkte kompetente Ansprechpartner, und die schon länger bewährte Kooperation zwischen dem ZIV und den IVVen könnte auf die Zusammenarbeit zwischen IVVen und UniV bzw. IVVen und IKM übertragen werden. Die Ausbreitung des für die Universität so bedeutsamen integrierten Informationsmanagements, gefördert im

MIRO-Projekt, wird mit tatkräftiger Unterstützung der IVVen sicher gelingen, weil sie ihr Wissen über die IV und über ihre Fachbereiche einsetzen können.

Mit der immer noch schnell wachsenden Ausweitung der IV-Prozesse wird allerdings auch dafür zu sorgen sein, dass genügend IV-Personal bereitsteht. Allein durch Rationalisierung und Automatisierung wird das nicht immer zu erreichen sein, denn die Ausstattung ist in Münster im Vergleich zu anderen Universitäten bereits knapp ausgelegt. Diese notwendig werdende Personalaufstockung entspricht einer Empfehlung des Landesrechnungshofes. Die Notwendigkeit ist jeweils im Detail zu begründen.

Das erste Sicherheits-Audit im ZIV

G. Richter, T. Rensing

Ende 2006 wurde ein erstes Sicherheits-Audit im ZIV abgeschlossen. Im folgenden Artikel sollen Ergebnisse, Erfahrungen und Konsequenzen hieraus dargelegt werden.

Seit etwa einem Jahr steht allen technisch Verantwortlichen für Geräte im LAN der Universität und des UKM ein IV-Sicherheits-Audit-Werkzeug[1] zur Verfügung, das in Anlehnung an die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine Risikoanalyse durch Erfassung und Bewertung des Ist-Zustands der IV-Sicherheit von IT-Endgeräten ermöglicht.

Hierzu wird in einem zweischrittigen Verfahren zunächst der Schutzbedarf eines Datenendgeräts selbst und anschließend die für dieses Datenendgerät getroffenen Sicherheitsvorkehrungen ermittelt und zur Bewertung gegenübergestellt. Die Datenerhebung erfolgt mit Hilfe des vom ZIV bereitgestellten, auf der Netzdatenbank (NIC_online) basierenden, Online-Sicherheits-Audit-Werkzeugs ISidoR in Form von Fragenkatalogen, die vom Auditor zu beantworten sind. Die Fragenkataloge zu getroffenen Sicherheitsvorkehrungen variieren in Art und Umfang in Abhängigkeit vom ermittelten Schutzbedarf. Sie reichen von reinen Fragen zum Datenendgerät selbst (Virenschutz, Aktualität des Betriebssystems, Betreuung, …) bis hin zu Fragenkatalogen zu Sicherheitsvorkehrungen am netz- und geräteseitigen Anschluss, Netzstrukturierung und Aufstellungsraum.

Eine umfangreiche Onlinedokumentation, ein Glossar und die Möglichkeiten, ganze Antwortkataloge vorzudefinieren bzw. auf andere Fragenkataloge zu übertragen, unterstützen den Auditor bei seiner Tätigkeit.

Die nachhaltige Erfassung und Bewertung des IV-Sicherheitsstatus durch das im Jahre 2005 vom ZIV bereitgestellte Werkzeug ISidoR wurde 2006 erstmals vollständig für alle Systeme des ZIV durchgeführt. Hierbei wurde ein Datenbestand von über 800 Systemen erfasst. Abbildung 1 zeigt die Verteilung der bei der Stichprobe ermittelten Schutzbedarfskategorien. Hierbei erfolgte bei der Ermittlung der Werte eine Unterscheidung hinsichtlich „Integrität und Vertraulichkeit“ und „Verfügbarkeit“ von Daten und Diensten. Ungefähr ein Drittel der Systeme weisen hierbei eine Schutzbedarfskategorie von mindestens „mittel“ auf.

Auf Basis dieser Werte wurden die getroffenen Sicherheitsmaßnahmen für ein jedes IT-System ermittelt und in Bezug auf ihre Wirksamkeit bewertet.

Die Erfahrungen aus diesem Prozess haben zu einer weiteren Verbesserung, insbesondere hinsichtlich der Handhabung des Verfahrens, der Visualisierung der Ergebnisse und Umfang der Begleitinformationen geführt. Des Weiteren wurde die Notwendigkeit für eine qualifizierte Begleitung und Unterweisung der Auditoren zur Verbesserung der Objektivität und Aufwandsabschätzung erkannt.

Für die IV-Sicherheit des ZIV selbst ergab sich eine Vielzahl von Erkenntnissen, die in größerem Umfang schon im zeitnahen Zusammenhang mit der Verfahrensdurchführung zur Abstellung von IV-Sicherheitsmängeln führten. Im Weiteren hatte das Verfahren eine wünschenswerte allgemeine Revisionierung hinsichtlich der Organisation, Aktualität und Dokumentation der IV-Strukturen und Datenbestände zur Folge.

Diese beiden Faktoren führten zu einem hohen, nicht generisch auf das Verfahren zurückzuführenden, Zeitaufwand. Diesem zuzuschreiben ist sicherlich die teilweise erst-

1 Vgl. infoforum 1/2005 http://www.uni-muenster.de/ZIV/inforum/2005-1/Welcome.html

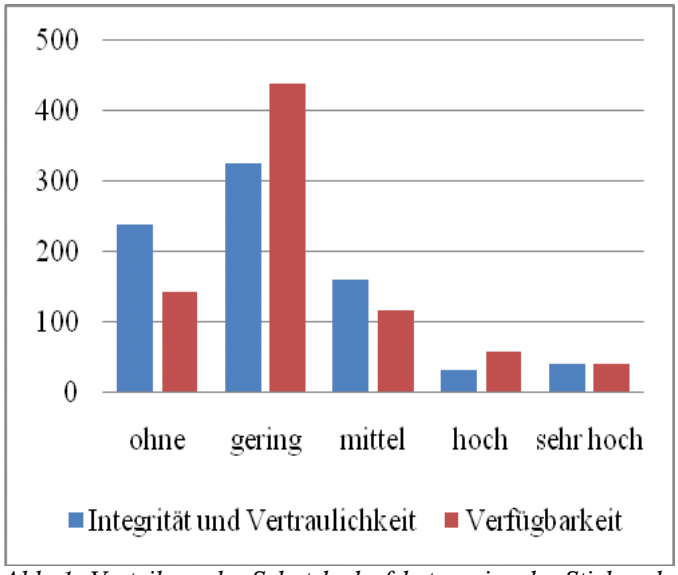


Abb. 1: Verteilung der Schutzbedarfskategorien der Stichprobe

malige und notwendige intensive Auseinandersetzung der durchführenden Systemadministratoren und technisch Verantwortlichen mit Fragestellungen hinsichtlich der IV-Sicherheit. Die damit verbundene stärkere Bewusstseinsbildung in Bezug auf Aspekte der IV-Sicherheit, ist ein weiterer wichtiger, durch die Durchführung des Verfahrens bedingter und erwünschter, Seiteneffekt.

Das ZIV wird weitere Maßnahmen durchführen, insbesondere soll die Netzstrukturierung im eigenen Bereich verstärkt werden. Im Anschluss hieran wird eine erneute Auditierung durchgeführt. Einige IV-Versorgungseinheiten haben bereits mit vorbereitenden Maßnahmen (Erstellung von Musterantwortkatalogen) begonnen, für 2007 wird deshalb ein umfangreicher Einsatz des Verfahrens erwartet, der durch die Abteilung 1 des ZIV begleitet werden kann. Anfragen hierzu richtet man am besten an Herrn Thomas Rensing (✉ `rensingt@uni-muenster.de`). Natürlich steht das ZIV auch mit Unterstützungsleistungen zur Seite, wenn eine Interpretation der Daten und die Umsetzung von Schlussfolgerungen notwendig sind. Hier erwarten wir, dass insbesondere der Prozess der Strukturierung des Netzes, soweit noch nicht geschehen, vorangetrieben wird, um die IV-Sicherheit zu erhöhen.

Intrusion-Prevention im Wissenschaftsnetz Münster

C. Ossendorf, G. Richter

In vorhergehenden Ausgaben des infoWWU wurde bereits mehrfach über das Netzssicherheitskonzept der Universität berichtet. Es beruht insbesondere auf einer Strukturierung des Netzes mit Hilfe von VLANs, virtuellen Routern und VPNs sowie der Einbettung von virtualisierten Sicherheitsfunktionen unmittelbar in dieses strukturierte Netz (*stateless und stateful packet screens*, Intrusion-Prevention-Instanzen, dedizierte VPN-Zugänge) und der Bereitstellung von anwendungskontrollierenden Gateways (z. B. Content-Filterung für E-Mail, Web und File Transfer oder Terminal-Server als personenbezogene Zugangssysteme).

Mit dem Einsatz der Intrusion-Prevention ab ca. März 2005 wurden erstmals Sicherheitsfunktionen verfügbar, die über reine Konnektivitätssteuerung hinausgingen. So weit wurden innerhalb des Netzes ausschließlich Kommunikationsbeziehungen auf der Basis von IP-Adressen und Anwendungsprotokolltypen („Ports“) kontrolliert (*packet screening*). Das eingesetzte Intrusion-Prevention-System (IPS) geht darüber hinaus, indem es Datenverkehr unterbinden kann, der aufgrund bestimmter eindeutiger Merkmale („Signaturen“) als gefährlich oder unerwünscht in verschiedenen Abstufungen erkannt werden kann; typische Vertreter für solche Angriffstypen sind z. B. benannt *mit-slammer*, *w32goabot* oder *w32/blaster-worm*. Darüber hinaus kann aufgrund des kommunikationstechnischen „Verhaltens“ eine ähnliche Qualifikation (z. B. weil als Scan-Angriff bewertet) erfolgen.

Von den verfügbaren Funktionalitäten sind bisher bei weitem nicht alle Möglichkeiten ausgeschöpft. Dies liegt zunächst einmal im Aufwand-Nutzen-Verhältnis begründet und dann in der Komplexität der rechtlichen Fragestellungen, da die Einschränkung von Datenverkehr in bestimmten Fällen als unrechtmäßige Einschränkung persönlicher Rechte betrachtet werden könnte. So sind heute nur Funktionen aktiv, wo diese Fragestellung eindeutig beantwortet werden kann, d. h. es werden ausschließlich Verkehrsströme blockiert, die eindeutig als Gefährdung zu betrachten sind[1], für die Abwendung von eindeutigen Gefahren besteht sogar eine gewisse Rechtsverpflichtung. „Unerwünschte Kommunikation“, die mancherorts z. B. bestimmten Peer-to-Peer-Protokollen zugeordnet wird, wird im Universitätsnetz derzeit nicht unterdrückt. Das ZIV richtet sich hier nach den Empfehlungen der Forschungsstelle Recht im DFN, die im Institut für Informations-, Telekommunikations- und Medienrecht, Zivilrechtliche Abteilung, an der Universität Münster beheimatet ist. Ausnahmen gibt es zurzeit nur für im Detail abgestimmte Netzbereiche außerhalb der Universität, wo eine Einschränkung von Rechten nicht gegeben ist.[2]

Noch nicht im breiten Einsatz, hauptsächlich aus Zeitgründen, sind verhaltensbasierte Funktionalitäten. Die besondere Problematik ist hier, dass die Verhaltenscharakteristika von Angriffen durchaus auch bei „normaler Nutzung“ angetroffen werden können. Ein Brute-Force-Password-Angriff per SSH kann durchaus so ähnlich aussehen wie das Verkehrsmuster eines mehrfach vergeblichen Einloggens eines vergesslichen Nutzers. Eine unbekümmerte Aktivierung von entsprechenden Funktionen könnte also auch zu Einschränkungen des ganz normalen Betriebes führen, was dann als Funktionsstörung des Netzes wahrgenommen würde und was zu schwierig zuzuordnenden Störungsmeldungen führen könnte. Hier ist zukünftig mit Erfahrungswerten zu arbeiten, die Schritt für Schritt gesammelt werden müssen. In einem ersten Anwendungsversuch werden auf Wunsch der IVV4 (NWZ) nun Brute-Force-Password-Angriffe (s. o.) über ftp, ssh, rsh, rlogin und telnet blockiert. Unerwünschte Nebeneffekte wurden soweit nicht festgestellt, die Aktivierung dieser Funktionalität wird deshalb bis auf Weiteres beibehalten.

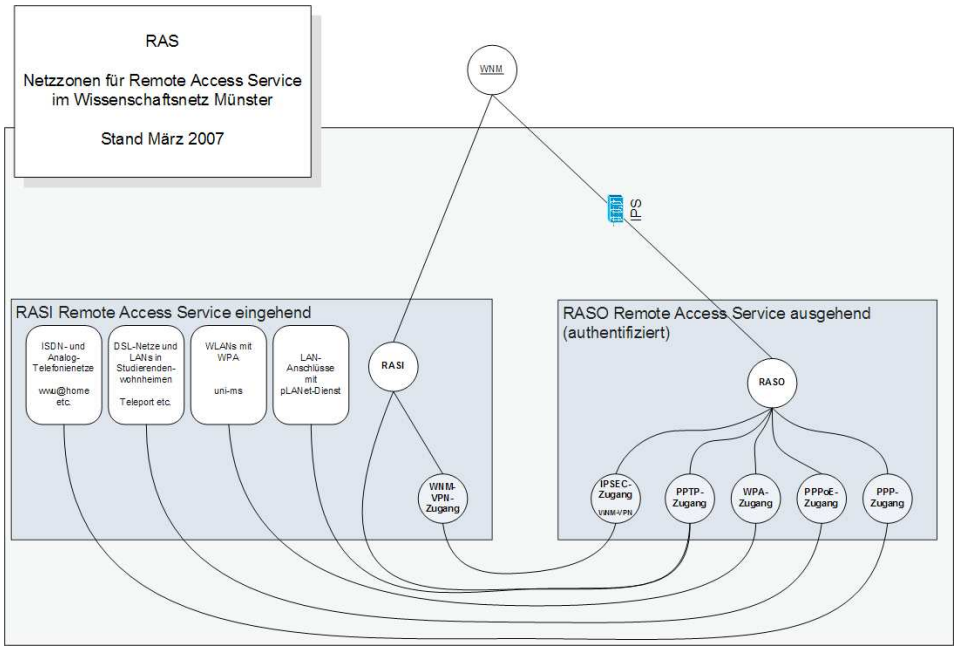
Für die weitergehende Ausschöpfung des Potenzials des IPS muss eine Basis geschaffen werden, die ein geordnetes abgestimmtes Verfahren auch zur kurzfristigen Aktivierung von IPS-Funktionen vorsieht, so dass die IPS-Systemadministratoren zum einen ein höheres Maß an Rechtssicherheit haben und dass zum anderen wichtige Schutzfunktionen (rechtzeitig) genutzt werden können. So könnte dann auch z. B. auch auf akute Denial-of-Service-Attacken reagiert werden. Die Abt. 1 des ZIV hat eine entsprechende Sicherheitsdetailregelung entworfen, die voraussichtlich in Kürze mit den IV-Gremien abgestimmt werden kann. Wir werden demnächst im infoWWU Genaueres darüber berichten.

Der bisherige Erfolg des IPS lässt sich am besten für den Bereich des Fernzugriffs (RAS, Remote Access Service) nachweisen. Der RAS-Bereich mit seinen Möglichkeiten

[1] Wir richten uns hier zunächst nach der Einschätzung des IPS-Herstellers (McAfee) für das Gefährdungspotential, zzt. werden alle (ca. 600) Exploits der höchsten Gefährdungsklasse blockiert. Darüber hinaus werden zusätzlich ca. 50 von McAfee zur Blockierung empfohlene Signaturen berücksichtigt, die nicht zur höchsten Gefährdungsklasse zählen.

[2] z. B. weil jegliche private Nutzung untersagt ist

IT-Systeme mit dem Netz der Universität zu verbinden – von zuhause oder unterwegs (Einwahl, VPN), auch im LAN der Universität mit mobilen Geräten über pLANet oder WLAN – und damit mit der Möglichkeit, zumeist private Geräte oder gar Systeme Dritter in das universitäre IT-System einzubringen, war zuvor stets ein Bereich unverhältnismäßig häufiger Sicherheitsvorfälle. Als Ursachen sind dort die auch sonst üblichen Hauptursachen auszumachen, nur mit erheblich größerer Wahrscheinlichkeit: Mangelnde Systempflege (insbesondere Betriebssystem- und Anwendungssicherheitsupdates und Einsatz aktueller Antivirus-Software). Mit dem Einsatz einer IPS-Instanz vor einer neu geschaffenen Netzzone RAS im Wissenschaftsnetz Münster hat sich die Zahl der durch das CERT-Team im ZIV zu bearbeitenden Sicherheitsvorfälle drastisch reduziert, insgesamt auf ca. 10 % früherer Werte! Eine Beeinträchtigung der RAS-Nutzer war durch den Einsatz des IPS in keiner Form gegeben. Der Nutzeffekt der IPS ist hier darin zu sehen, 1. dass die Nutzergeräte im RAS-Bereich selbst geschützt wurden, 2. dass andere vor malignen Systemen im RAS-Bereich geschützt wurden und 3. dass maligne Systeme im RAS-Bereich erkannt werden konnten, bevor Beschwerden durch Dritte bekannt wurden. Die Netzzone RAS musste zuvor erst geschaffen werden, heute fasst sie – mit begründeten Einschränkungen – alle als Externzugriff betrachteten Zugänge zum Wissenschaftsnetz Münster zusammen[3]: Einwahl (z. B. wwu@home), Verbindungen aus Studierendenwohnheimen (z. B. Teleport), VPN, pLANet, WLANs mit der Kennung (SSID) uni-ms. Die folgende Abbildung zeigt die Position der Intrusion-Prevention-Instanz im RAS-Bereich.



Auch in zurückliegenden Projekten zur Strukturierung des LAN (ZMK, vgl. infoWWW Nr. 1/2006) erwies sich das IPS als Erfolg. Neben dem eigentlichen Nutzen durch den Einsatz einer Intrusion-Prevention-Instanz für einen Unterbereich des LAN konnten, als positiver Seiteneffekt, mit Schadsoftware infizierte Systeme erkannt werden, und die für die Geräte zuständigen technisch Verantwortlichen konnten für eine entsprechende Bereinigung sorgen. Auch kann in solchen LAN-Unterbereichen eine spezielle Verfahrensweise hinsichtlich der Aktivierung von Intrusion-Prevention-Funktionen angewendet werden, da die lokale Sicherheitspolitik über eine „Mandantenschnittstelle“, also durch lokal Verantwortliche selbst angepasst werden kann.

[3] Netze Dritter selbst, auch das gesamte externe Internet, fallen nicht hierunter. Der Schutz hier wird durch IPS-Funktionen vor dem Universitätsnetz selbst gewährleistet.

Überwachung und Dokumentation von Geschäftsprozessen

M. Grote, M. Wagner

Seit Neuestem setzt das ZIV die Software @ctiveFRIEND zur Überwachung seiner Geschäftsprozesse ein.

Die gravierenden Veränderungen der Hochschullandschaft in den letzten Jahren und die dadurch gewandelten Anforderungen im IT-Bereich haben dazu geführt, dass sich das ZIV von einer rein universitären Einrichtung immer mehr zu einem kundenorientierten IT-Dienstleister entwickelt.

Damit die Sicherstellung des reibungslosen Betriebes wichtiger IT-Services gewährleistet werden kann, ist es notwendig, dass eine Überwachung und Dokumentation der hierfür verantwortlichen Prozesse ermöglicht wird. Die Firma Siemens bietet mit der Information-Management-Software @ctiveFRIEND eine Möglichkeit, diesen Ansprüchen genüge zu tragen. Konzeptionell handelt es sich hierbei um eine Applikation, die Unternehmen die Überwachung und Darstellung von Geschäftsprozessen gestattet. Bezogen auf die Tätigkeit des ZIV als IT-Dienstleister sind diese Geschäftsprozesse primär technischer Natur.

@ctiveFRIEND bietet die Möglichkeit, eingehende Daten aus unterschiedlichsten Quellen zu erfassen und den von ihnen beeinflussten Prozessen zuzuordnen. Kommt es zu einer Störung in einer Prozesskette, kann leicht die Ursache hierfür gefunden werden. Neben dieser Echtzeit-Überwachung sind mit @ctiveFRIEND eine einfache Kontrolle sowie der Nachweis von Verfügbarkeiten (Service-Level-Agreements) möglich. Diese werden in entsprechenden „Reports“ dargestellt und aufbereitet. Aufgrund der mit der Einführung der Software einhergehenden Analyse und Dokumentation der Prozesse ist es möglich, eine bisher nicht erreichte Transparenz des komplexen ZIV-Betriebes zu bieten. Das Produkt und seine Funktionsweise werden im Folgenden am Beispiel des E-Mail-Dienstes näher erläutert.

Im Hauptmenü der Weboberfläche unter „profiles“ (siehe Abb. 1, links) werden in unterschiedlicher Feinheit übersichtliche Darstellungen der mit dem Dienst verbundenen Prozesse angezeigt. Das Bild zeigt den aus einem Empfangs- und einem Versand-Teil bestehenden Mailprozess. Die Prozesskette ist in einer Grafik dargestellt. Den einzelnen Kästchen sind sogenannte Agenten zugeordnet, die ihren Zustand aufgrund von Ereignissen verändern können. Sind alle Agenten grün, so liegen keine Fehler vor. Der rote Agent zeigt eine Störung im Mail-Empfang in der Mail-Ablage.

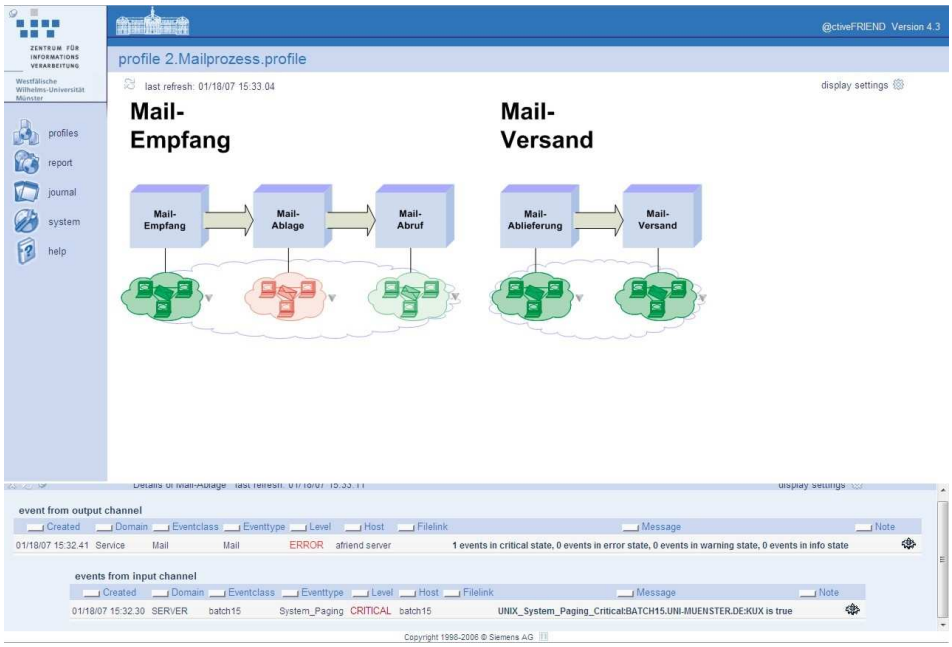


Abb. 1: Mailprozess mit einer Störung

Abb. 2 zeigt diese Mailablage im Detail. Dort ist die Ursache des in Abb. 1 gezeigten Fehlers zu erkennen: Der Server batch11 hat ein kritischen Ereignis gemeldet, batch14 und batch15 lösten jeweils eine Warnung aus.

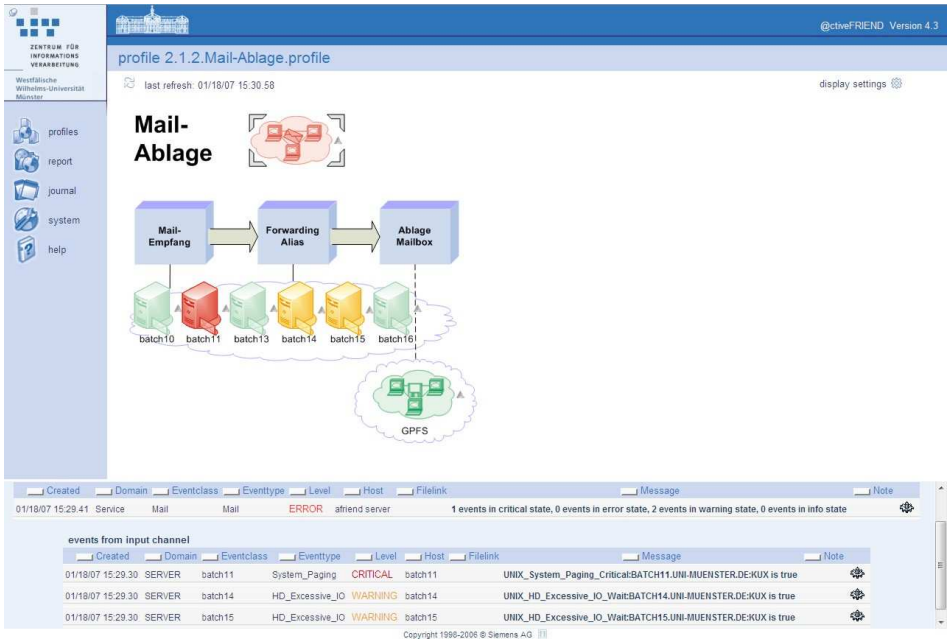


Abb. 2: Mail-Ablage im Detail mit zwei Warnungen und einem kritischen Ereignis

Zur Anbindung der externen Quellen an @ctiveFRIEND gibt es vorgefertigte Monitoring-Agents von Siemens, die z. B. die Verfügbarkeit eines Rechners per Ping überprüfen. Zusätzlich können auch eigene Skripte bzw. Programme erstellt werden, die Ereignisse an @ctiveFRIEND senden. So werden die Ausgaben des IBM Tivoli Monitoring 6.1 durch eine im ZIV erstellte Schnittstelle verarbeitet und in ein für @ctiveFRIEND verständliches Format überführt. Die Ausgaben der Ironport-Applikationen, die für den Mail-Empfang zuständig sind, können so ebenfalls ausgewertet werden.

Wenn Fehler oder kritische Ereignisse auftreten, können die zuständigen Mitarbeiter über E-Mail (oder demnächst auch über SMS und Telefonanruf) informiert werden. Sie können sich dann leicht durch einige Klicks die genaue Ursache eines Ereignisses anzeigen lassen und danach gezielt einwirken. Hierbei sind weitere Verarbeitungsmöglichkeiten denkbar, da @ctiveFRIEND diese Ereignisse in Form festgelegter Variablen ausgibt, die wiederum nur durch selbst erstellte Skripte oder Programme einer entsprechenden Weiterverarbeitung unterzogen werden müssen.

Single Sign-On im Web

S. Stoytchev

Was ist (Web-) Single Sign-On und welche Vorteile ergeben sich dadurch?

Single Sign-On (SSO) ist ein Authentifizierungsprozess, der es einem Benutzer ermöglicht, nach einmaliger Eingabe von Authentifizierungsdaten (in den meisten Fällen Benutzername und Passwort) mehrere separate geschützte Anwendungen zu nutzen. In diesem Prozess wird der Benutzer für sämtliche Anwendungen authentifiziert, für die er Zugangsberechtigung besitzt. Damit entfällt während einer Session (engl. für Sitzung) die wiederholte Eingabe von Authentifizierungsdaten.

Im Folgenden betrachten wir die Möglichkeiten für die Realisierung eines Web Single Sign-On – einer speziellen Form von SSO, in der sämtliche Anwendungen webbasiert und nur über einen WWW-Browser genutzt werden.

Bevor wir uns den technischen Details rund um SSO widmen, sollen die wichtigsten Vor- und Nachteile einer solchen Umgebung kurz skizziert werden. Zu den Vorteilen zählen:

- *Höhere Benutzerfreundlichkeit:* Die Arbeit wird nicht ständig durch Abfragen von Authentifizierungsdaten unterbrochen. Mit SSO ist die manuelle Eingabe von Authentifizierungsdaten im Idealfall nur einmal erforderlich.
- *Höhere Sicherheit:* Oft müssen sich Benutzer viele Passwörter merken – für jede Anwendung ein anderes. In einer SSO-Umgebung können Benutzer ein einziges, dafür aber komplexeres Passwort wählen, was die Sicherheit erhöht.
- *Effektivere Neuentwicklung*: SSO stellt ein einheitliches Sicherheitsframework zur Verfügung, so dass Entwickler sich nicht um Authentifizierung kümmern müssen. Sie können bei der Entwicklung neuer Anwendungen auf diese Funktionalität zurückgreifen und darauf vertrauen, dass die Authentizität der Anwender an anderer Stelle sicher und zuverlässig überprüft wird.

Zwei der meist genannten Schwächen von SSO sind:

- *Schwierige und zeitintensive Anpassung bestehender Anwendungen*: Die Einbindung von bereits existierenden Anwendungen in eine SSO-Infrastruktur ist in der Regel sehr aufwändig, da meistens eine Anpassung ihrer Sicherheitsmechanismen erforderlich ist. In den Fällen, in denen der Quellcode der Anwendung nicht verfügbar ist, könnte eine solche Anpassung sogar unmöglich sein.
- *Unbeaufsichtigter Arbeitsplatz:* Ein „Angreifer“ kann die vollständige Kontrolle über die Anwendungen eines anderen Benutzers übernehmen, wenn letzterer seinen Arbeitsplatz verlässt, ohne sich vorher abzumelden. Obwohl das ein allgemeines Risiko ist, wird dieses durch SSO zusätzlich verschärft, da die fremde Person Zugang zu sämtlichen Anwendungen des Opfers bekommen kann. Im Normalfall (ohne SSO) wäre nur eine Ressource gefährdet.

Fazit: SSO hat durchaus Nachteile, aus Sicht der Endanwender, Dienstanbieter und -entwickler scheinen jedoch die Vorteile zu überwiegen.

Wie kann man SSO realisieren?

Technisch gibt es verschiedene Möglichkeiten, ein Single Sign-On zu realisieren. Hier konzentrieren wir uns auf serverbasierte Lösungen und abstrahieren von solchen, die eine Anpassung der Clienten (z. B. Installation zusätzlicher Software wie Passwort-Safes) erfordern.

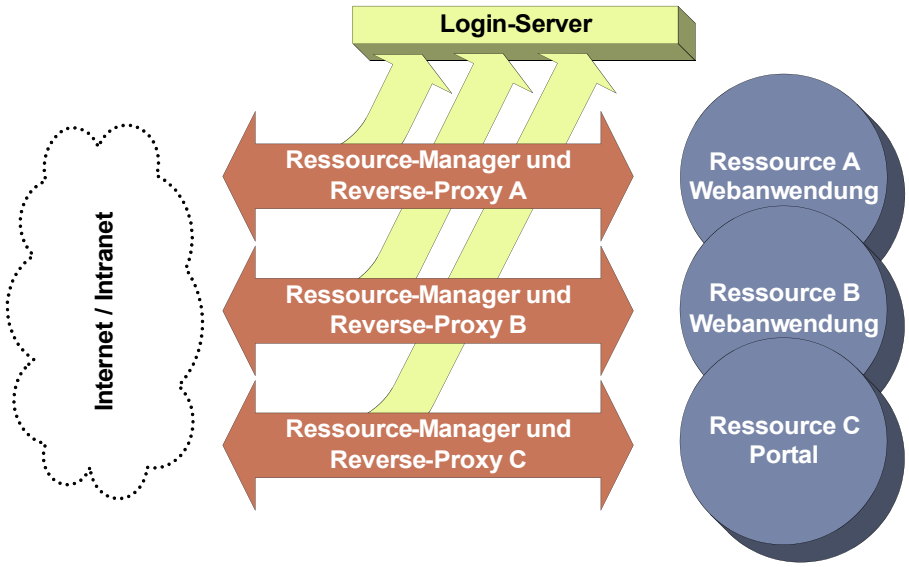
Ein wichtiger Begriff, der in diesem Kontext vorab geklärt werden muss, ist der Begriff des digitalen Tickets. Ein Ticket wird bei der Anmeldung erzeugt und dient im Folgenden der Authentifizierung des Benutzers. Technisch ist das Ticket eine Zeichenkette (Identifikationsnummer), mit deren Hilfe der Server die Gültigkeit einer Session automatisiert prüfen kann. Damit der SSO-Mechanismus funktioniert, muss bei jeder Anfrage an den Server dafür gesorgt werden, dass ein gültiges Ticket präsentiert wird. Beim Anwender sind keine lokalen Anpassungen bezüglich ihres Betriebssystems oder der verwendeten Software erforderlich. Tickets werden in Form von Browser-Cookies oder über die Request-URL gespeichert und stehen automatisch Verfügung. Tickets haben in der Regel eine begrenzte Gültigkeit, d. h. wenn ein Ticket abgelaufen ist, muss sich der Benutzer erneut anmelden, um ein neues zu bekommen.

Der sogenannte *Circle of Trust* ist ein relativ weit verbreiteter Lösungsansatz für ein SSO. Hierbei wird ein Netz aus vertrauenswürdigen Anwendungen aufgebaut. Meldet sich ein Benutzer bei einer der Anwendungen an, so ist er danach für alle anderen Anwendungen gleichermaßen angemeldet. Die ideale Lösung sieht dabei vor, dass der Benutzer bei der Anmeldung am ersten System ein Ticket bekommt, mit dem er sich bei allen anderen Anwendungen authentifizieren kann. Das Ticket muss hierzu bei jeder Anwendung aus dem *Circle of Trust* verifiziert werden können.

Diese Lösung zeichnet sich durch Einfachheit bei der Implementierung von neuen Anwendungen aus. Ein Nachteil zeigt sich allerdings bei der Anbindung bestehender Anwendungen, deren Sicherheitslogik angepasst werden müsste. Bei solchen Anwendungen, deren Quellcode nicht verfügbar ist, kann die nötige Anpassung nur über den Hersteller gewährleistet werden. Eine weitere Schwäche von Circle of Trust ergibt sich aus der Tatsache, dass potenziell jede Anwendung auf Authentifizierungsdaten des Benutzers zugreifen und diese verarbeiten kann. Daraus könnte ein erhöhter Koordinationsaufwand zwischen den Dienstanbietern resultieren. Darüber hinaus erhöht sich mit einer steigenden Anzahl von Anwendungen das Risiko, dass Fehler in einer Anwendung die Sicherheit des gesamten Circle of Trust gefährden könnten.

Der Einsatz eines zentralen Login-Servers könnte die zuletzt angesprochene Schwäche einer SSO-Umgebung entkräften. Bei dieser Lösung – mit einem dedizierten Login- bzw. Ticket-Server – wird eine eigene Anwendung implementiert, die zu Beginn jeder neuen Sitzung angesprochen werden muss. Nach erfolgreicher Anmeldung über diesen Server erhält der Client das Ticket, mit dem er sich gegenüber allen Anwendungen im Verbund authentifizieren kann. Das Ticket muss also vom Client bei jeder Anfrage an eine Anwendung des Verbunds mitgegeben werden, wo eine Überprüfung seiner Gültigkeit vorgenommen wird. Falls das Ticket erfolgreich verifiziert werden konnte, erhält der Benutzer Zugriff auf die Anwendung.

Dieser Ansatz impliziert, dass jede einzelne Anwendung eine spezielle Logik enthalten muss, die das Ticket verifiziert bzw. beim zentralen Ticket-Server verifizieren lässt. Bestehende Anwendungen müssen daher entsprechend dieser Logik angepasst werden, indem die alte Anmeldeprozedur durch einen neuen Ablauf ersetzt wird.



Offensichtlich erlaubt der Ansatz mit einem zentralen Login-Server die Authentifizierung von der Anwendung zu entkoppeln. Die Verifizierung des Tickets verbleibt jedoch in der Verantwortung der Anwendung. Wünschenswert wäre jedoch eine Lösung, bei der auch diese Funktionalität von der Anwendung abgelöst werden könnte, wodurch ein Anpassungsbedarf nahezu bzw. komplett entfallen würde. Idealerweise sollte eine Lösung so aussehen, dass sowohl die Authentifizierung als auch die Verwaltung (erstellen, verifizieren, löschen, ...) von Tickets außerhalb der Anwendung stattfinden. In einem generischen Modell (s. Abbildung) übernimmt ein Ressource-Manager diese Aufgabe.

Technisch handelt es sich hierbei um ein Reverse-Proxy oder auch Webserver-Modul, welches alle Anfragen an eine geschützte Ressource abfängt und die Gültigkeit des Tickets überprüft. Wenn ein Ticket ungültig ist oder fehlt, wird die Anfrage an den zentralen Login-Server weitergeleitet, wo die Authentifizierung des Benutzers und die Erstel-

lung eines gültigen Tickets erfolgen. Danach kann der Client mithilfe dieses Tickets alle Ressourcen nutzen, die im SSO-Verbund durch Ressource-Manager geschützt sind.

Im Rahmen vom Projekt MIRO [1] wurden zwei Produkte evaluiert, die den gerade beschriebenen Lösungsansatz zur Realisierung von SSO verfolgen: den *IBM Tivoli Access Manager for e-Business* [2] in Verbindung mit dem Reverse-Proxy *WebSeal* sowie die Open-Source Lösung *Shibboleth* [3]. Shibboleth weist aufgrund seiner offenen Schnittstellen, der gebotenen Flexibilität und einer großen Internet-Community viele Vorteile gegenüber der proprietären Lösung von IBM auf. Weiterhin bietet Shibboleth die Möglichkeit, Authentifizierungsdienste auch organisationsübergreifend zur Verfügung zu stellen und wird daher bereits von einigen anderen Universitäten und öffentlichen Einrichtungen getestet bzw. eingesetzt, um in Zukunft auch Dienste im Rahmen einer Föderation bzw. Kooperation anbieten zu können.

Die Rolle des zentralen Login-Servers übernimmt bei Shibboleth ein sogenannter Identity-Provider – eine Webanwendung die für die Authentifizierung und die Erstellung von Tickets verantwortlich ist. Der Identity-Provider kann flexibel in Kombination mit verschiedenen Benutzerdatenbanken (LDAP, ActiveDirectory, Kerberos, ...) eingesetzt werden. Als Ressource-Manager fungieren sogenannte Service-Provider, die technisch als Webserver-Module realisiert sind. Das Zusammenspiel von Identity-Provider und Service-Provider kann anhand der folgenden beispielhaften Sitzung beschrieben werden:

- Jeder nicht authentifizierte Aufruf eines Benutzer-Clients wird vom Service-Provider zuerst an den Identity-Provider umgelenkt.
- Nach erfolgreicher Anmeldung erhält der Client vom Identity-Provider ein Ticket und wird mittels einer vorher mitgegebenen Rücksprung-URL zurück zum Service-Provider geleitet. Technisch besteht das Ticket aus einem digital signierten Dokument, das verschiedene benutzerbezogene Informationen (z.B. Benutzername, Rollen, ...) enthält. Das Dokument benutzt die Syntax der Security Assertion Markup Language (SAML) [4].
- Der Service-Provider überprüft die Signatur des Tickets und liest die darin befindlichen Informationen aus. Der Aufruf des Clients wird erst dann zur geschützten Anwendung weitergeleitet.

Die Benutzerdaten können vom Service-Provider in Form von Umgebungsvariablen (z. B. REMOTE_USER) an die Anwendung zur Verfügung gestellt werden. Somit braucht die Anwendung lediglich diese Umgebungsvariablen auszulesen, um an die benötigten Benutzerdaten zu gelangen und kann sich gleichzeitig darauf verlassen, dass die Authentifizierung des Benutzers erfolgreich stattgefunden hat. Da die Verwendung von Umgebungsvariablen eine häufig eingesetzte Technik ist, machen viele vorhandene Anwendungen Gebrauch davon und müssen nicht aufwändig angepasst werden, um an einem auf Shibboleth basierenden SSO teilzunehmen. Im Fall des Portalservers wurde diese Anpassung bereits vorgenommen, was dank der Erweiterbarkeit von WebSphere problemlos möglich war.

Mit Shibboleth ergibt sich für ein universitätsweites Single Sign-On eine Architektur, die Ähnlichkeiten mit den oben vorgestellten Konzepten des Circle of Trust und des zentralen Login-Servers aufweist. Durch den Einsatz von Shibboleth versprechen wir uns eine höhere Produktivität durch benutzerfreundlichere Gestaltung der Anwendungslandschaft verbunden mit einem relativ geringen Aufwand der Realisierung.

Verweise:

[1] `http://www.uni-muenster.de/IKM/miro/`

[2] `http://www.ibm.com/software/tivoli/products/access-mgr-e-bus/`

[3] `http://shibboleth.internet2.edu/`

[4] `http://www.oasis-open.org/specs/index.php#samlv2.0`

Einführung des Identitätsmanagement-Systems in der WWU

R. Mersch

Die Einführung des Identitätsmanagements an der WWU ist weit fortgeschritten. Dieser Beitrag umreißt die Ziele des Systems und den Stand der Arbeiten. Weitere mehr ins Detail gehende Artikel werden folgen.

Ziele

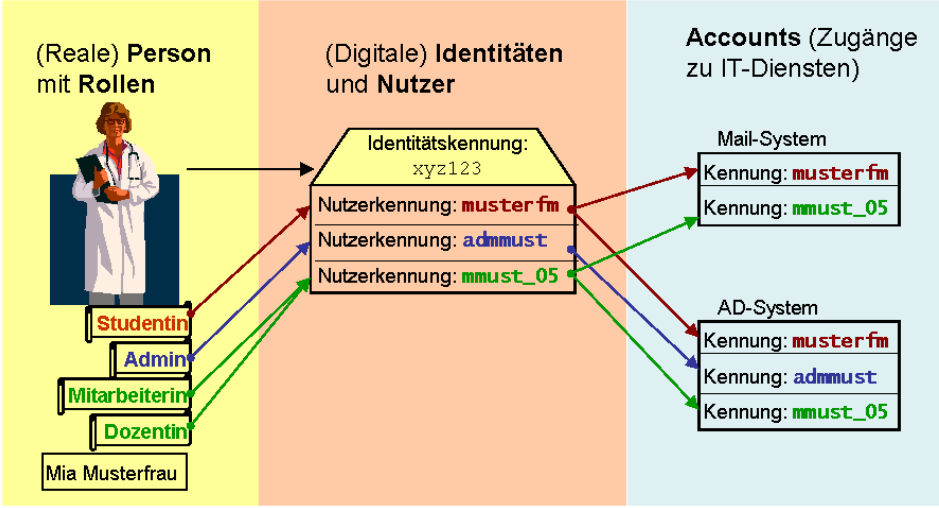
Das Identitätsmanagement hat die einheitliche Verwaltung von Personen, einschließlich Kontaktinformationen und Rollen, zum Ziel. Die zentrale Benutzerverwaltung WWU-BEN, die sich seit mehr als 10 Jahren im Einsatz befindet, soll in weiten Teilen durch das Identitätsmanagement abgelöst werden.

Zu den Zielen des Identitätsmanagements gehören:

- die Erhöhung der Effizienz der Administrationsprozesse durch
  - die Vermeidung von Parallelarbeiten,
  - die Automatisierung der Verwaltung von rollenbasierten Zugangsberechtigungen auf Endsystemen
  - und die Ablösung manueller und papierbehafteter Abläufe,
- die Verbesserung der Datenqualität durch
  - Synchronisation der Datenquellen
  - und Etablierung von zuverlässigen und dokumentierten Prozessen zur Datenpflege,
- die Verbesserung des Datenschutzes durch
  - informationelle Selbstbestimmung
  - und die Auditfähigkeit des Identitätsmanagements,
- die Erhöhung der Sicherheit des IT-Gesamtsystems durch
  - die einheitliche Verwaltung von Nutzerkennungen,
  - die Vermeidung von verwaisten Kennungen und Accounts (Lifecycle Management),
  - die zuverlässigere Zuordnung von Nutzerkennungen zu Personen bei administrativen Prozessen (wie z.B. Passwort-Rücksetzungen)
  - und insbesondere die Erkennung von nicht aus dem Identitätsmanagement stammenden Rechteänderungen,
- die Verbesserung des Services durch
  - Zusammenfassung aller Accounts und Rechte einer Person an einer Stelle,
  - Verkürzung von Reaktionszeiten aufgrund automatisierter Workflows
  - und Online Antrags- und Selbstverwaltungsverfahren für die Kunden.

Begriffe

Das folgende Bild veranschaulicht wesentliche Merkmale des angestrebten Systems:



Person
: Damit ist eine natürliche Person gemeint. Aus der Sicht eines IT-Dienstes stellt eine Person den Benutzer dar.

Identität
: Eine Sammlung von Attributen einer Person. Idealerweise besitzt eine Person nur eine Identität. Umgekehrt ist eine Identität immer nur einer Person zuzuordnen. Eine Identität wird durch ein eindeutiges Merkmal, die Identitätskennung, identifiziert. Dies tritt allerdings nach außen nicht in Erscheinung.

Account
: Der Zugang einer Identität zu einem IT-Dienst. Dem Account ist eine Kennung zugeordnet, mittels der sich die Person identifiziert. Eine Identität kann mehrere Accounts für denselben IT-Dienst mit dann unterschiedlichen Kennungen haben.

Nutzer
: Eine Menge von Accounts mit derselben Kennung. Diese Nutzerkennung ist eines der Attribute einer Identität. Einer Identität können mehrere Nutzerkennungen zugeordnet sein.

HR-Feed
: Einspeisung der Personendaten und Rolleninformationen aus den maßgeblichen Quellen (Human Resources), beispielsweise der Univerwaltung.

Provisionierung
: Die Versorgung eines IT-Dienstes mit Accounts.

Rolle
: Die Funktion der Person in der Universität. Für Mia Musterfrau sind die vier Rollen Studierende, Administratorin, Mitarbeiterin und Dozentin bekannt.

Die oben dargestellte Sichtweise hat sich nur langsam herauskristallisiert. Die verwendeten Produkte kennen nur die Trennung zwischen Identität und Account. Die in der WWU von vielen Seiten gestellte Forderung, dass eine Person mehrere Kennungen – auch auf demselben Zielsystem – haben können muss, hat uns schließlich zur Einfügung der Zwischenschicht „Nutzer“ gebracht. Die Realisierung erfordert allerdings erhebliche Anstrengungen.

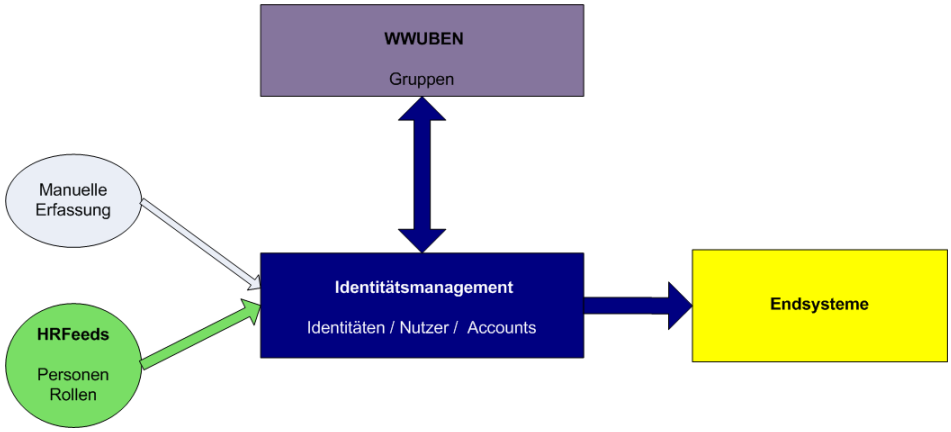
Die Bündelung aller Nutzerkennungen einer Person unter einer Identität ist ein wesentlicher Fortschritt gegenüber der WWUBEN. Dennoch sollte es der Regelfall bleiben, dass eine Person nur eine Nutzerkennung hat.

Rollen sollen nicht die aus der WWUBEN bekannten Gruppen (dort auch „Projekte“ genannt) ersetzen, beide werden künftig zu pflegen sein. Ob eine klare Trennung der beiden Konzepte zu erreichen ist, erscheint fraglich, die Grenzen sind wohl fließend. Als grober Anhalt mag dienen, dass eine Rolle eher globalen Charakter hat und die sich daraus resultierenden Rechte oft von weiteren Attributen abhängen. (Beispiel: Die Rolle „Dekan“ für sich alleine mag einige Rechte bedingen, viele aber nur in dem zugehörigen Fachbereich.)

Design

Das in der WWUBEN realisierte fein granulare Gruppenkonzept ist an der WWU so etabliert, dass es nicht aufgegeben werden kann. Andererseits lässt es sich aber auch nicht ohne Weiteres auf das im Identitätsmanagement enthaltene, eher grob granulare, Rollenkonzept abbilden. Wir haben uns daher entschieden, die Gruppenverwaltung in der WWUBEN bis auf Weiteres weiterzuführen.

Damit die vom Identitätsmanagement provisionierten Systeme mit Gruppeninformationen versorgt werden können, werden diese aus WWUBEN regelmäßig in das Identitätsmanagement eingespeist. Umgekehrt liefert das Identitätsmanagement Nutzerinformationen nach WWUBEN. Künftig werden in WWUBEN keine Nutzer mehr direkt erzeugt. Dies setzt voraus, dass das Identitätsmanagement einmal initial mit allen Nutzerdaten aus WWUBEN gefüttert wird.



Automatisierte HR-Feeds werden im ersten Schritt für Studierende sowie Mitarbeiterinnen und Mitarbeiter der Universität eingerichtet sein. Alle anderen, insbesondere die große Gruppe der Mitarbeiterinnen und Mitarbeiter des UKM, werden auf dem Wege des gewohnten Antragsverfahrens manuell eingetragen.

Personen und Identitäten

Die oben dargestellte Situation, dass Mia Musterfrau zwar drei Nutzerkennungen, aber nur eine Identität hat, stellt das Ziel dar. Die Ausgangssituation ist oftmals eine andere, weil Personen- bzw. Nutzerdaten aus mehreren Quellen stammen, ohne dass ersichtlich ist, dass sie dieselbe Person betreffen. Für Mia Musterfrau könnte dies bedeuten, dass sie drei Identitäten mit jeweils einer Nutzerkennung hat, weil ihre Daten aus WWUBEN, der Studierendendatenbank und der Mitarbeiterdatenbank stammen. Dies ist unbefriedigend und mit den o. g. Zielen nicht vereinbar. Daher sollen Mechanismen etabliert werden, die solche Identitäten zusammenführen.

Möglicherweise braucht Mia Musterfrau nicht wirklich drei Nutzerkennungen und empfindet das Arbeiten damit eher als lästig. Für das Zusammenführen von Nutzerkennungen (also die Übertragung der mit einer der Kennungen verbundenen Rechte auf die andere und Löschung der ersteren) derselben Identität soll ebenfalls ein Mechanismus geschaffen werden.

Die für die Aufgaben des Identitätsmanagement, insbesondere die Ermittlung der Identitäten und die Zuordnung von Rollen, erforderlichen Datenflüsse ins Identitätsmanagement müssen datenschutzrechtlich abgesichert sein. Dazu wurde eine Datenschutzvorabkontrolle durchgeführt und es wurde eine neue Benutzungs- und Identitätsmanagementordnung auf den Weg gebracht.

Weitere Schritte

Nach der Einführung des Identitätsmanagements stehen weitere Aufgaben an. Schwerpunkte werden sein:

1. Verwaltung der Nutzer der ULB unter Berücksichtigung der Externen („Bürger"),
2. HR-Feed der Mitarbeiter und Mitarbeiterinnen des UKM,
3. besondere Verfahren für Konferenz-Teilnehmer und Gäste,
4. Verfeinerung des Rollenkonzepts,
5. Dezentrale Administration und Delegation .

Netzstrukturierung im Naturwissenschaftlichen Zentrum (NWZ)

G. Wessendorf

Für den Bereich der IVV 4 werden zurzeit Strukturierungsmaßnahmen als Grundlage für eine verbesserte netzseitige IT-Sicherheit durchgeführt.

Wie bereits im infoRUM Nr.1/2005 und Nr. 1/2006 vorgestellt, wird vom ZIV die IT-Sicherheit durch netzseitige Maßnahmen wie hierarchische Netzzonenstrukturierung, Einbettung von Sicherheitsfunktionen wie *stateless* und *statefull packet screening* (Firewall-Technologien), Intrusion-Prevention-Systemen (IPS) sowie authentisierte Zugänge mittels Virtueller Privater Netze-Technologie (VPN) verbessert.

Zurzeit finden diese Strukturierungsmaßnahmen verstärkt im Bereich Naturwissenschaftliches Zentrum (NWZ) statt. Dem NWZ gehören die großen Fachbereiche Physik, Chemie/Pharmazie und Biologie an; insgesamt sind dies etwa 30 Institute. In Zusammenarbeit von ZIV mit der für das NWZ zuständigen IV-Versorgungseinheit 4 (IVV 4) und den IT-Verantwortlichen der jeweiligen Institute werden die Maßnahmen geplant und durchgeführt.

Im Wesentlichen liegt der Strukturierung jedes Institutes bzw. jeder (übergeordneten) Netzzone folgender Ablauf zugrunde:

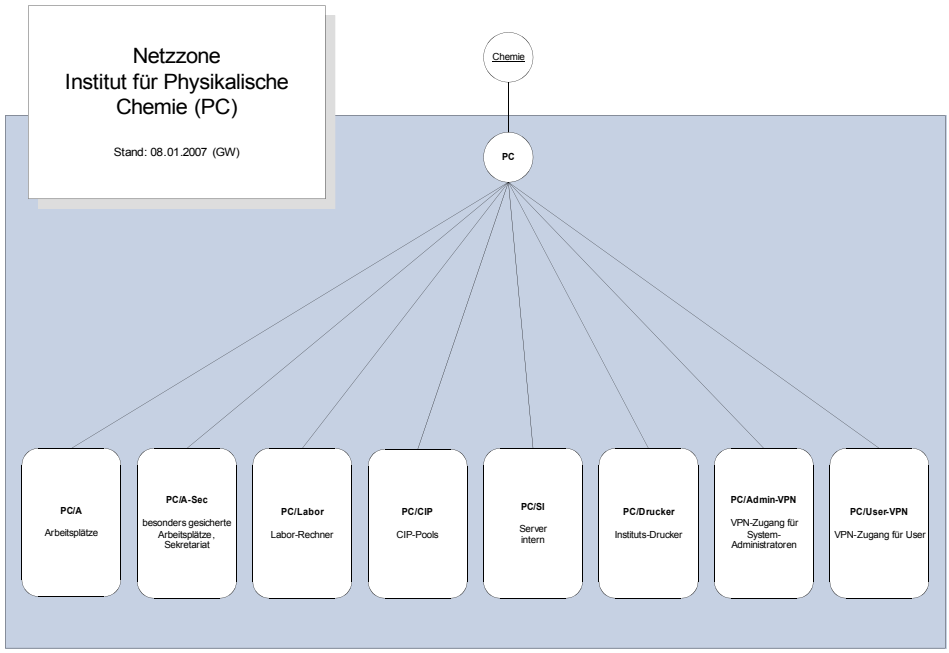
- Treffen von ZIV mit Instituts-IT-Verantwortlichen
  - Vorstellung und Planung eines Instituts-Konzeptes (Netzzonenmodell)
  - Feststellung der wesentlichen Verkehrsbeziehungen
  - Erste Planungen für Filterregeln
- ZIV: Umsetzung des Netzzonenmodells
  - Technische Änderungen/Erweiterungen der Netzinfrastruktur (Router, ACLs, VLANs, IP-Subnetze, VPN-Gateways, …)
- Institut: Revision der eigenen Netzzone
  - Detailliertere Informationen über Verkehrsbeziehungen (für Filterregeln)
  - Vorbereitung von ggf. nötigen Umzügen von Systemen in andere oder neue Netzzonen
- Gemeinsame Durchführung der Umstellung in angekündigten Zeitfenstern
- Kontrolle und ggf. Verfeinerung des Modells

Zur Verdeutlichung der Maßnahmen und der damit zu gewinnenden IT-Sicherheit soll die Strukturierung des Institutes für Physikalische Chemie (PC) dienen. Die dortige Strukturierung kann auch als Prototyp verstanden und andernorts angewendet werden.

ZIV-Präsentation

So sind in der Physikalischen Chemie inzwischen folgende Netzzonen eingerichtet (vgl. Abbildung):

- **A**: allgemeine „normale“ Arbeitsplätze, insbesondere für Instituts-Mitarbeiter(innen).
- **A-Sec**: besonders zu sichernde Arbeitsplätze, Endsysteme mit besonders vertraulichen Daten, wie z. B. Sekretariat, Prüfungsamt, etc.
- **Labor**: Rechner in Labor- und Werkstattumgebungen. Häufig Spezialsysteme zur Geräte- und Messsteuerung. Oft keine „Standard“-Endsysteme, oft nicht mit Sicherheits-Updates versorgbar oder grundsätzlich leicht angreifbar.
- **CIP**: Rechner in PC-Pools für Studierende.
- **SI** (Server-Intern): Ausschließlich für Instituts-internen Zugriff installierte Server, zumeist File-, Web- oder Terminal-Server.
  Die Variante „SE“ (Server-Extern) ist auch als Netzzone möglich, d. h. dann sinnvoll, wenn Instituts-Dienste Netzzonen übergeordnet angeboten werden sollen…
- **Drucker**: Netzwerkfähige Instituts-Drucker. Entweder direkt von Arbeitsplatz-Netzzonen oder über Print-Server (in SI-Netzzone) ansprechbar.
- **User-VPN**: VPN-Gateway für die sichere Einwahl von Institutsmitgliedern von „außerhalb“ (andere Uni-Netzzonen, Internet, Heimarbeitsplatz) in die eigenen Instituts-Netzzonen. Die Möglichkeit des autorisierten und verschlüsselten Zugriffs via VPN bietet auch den Vorteil, die Filterregeln für die einzelnen Netzzonen gegen „normalen“ Zugriff von „außerhalb“ viel restriktiver verfassen zu können. Die Berechtigung zur Nutzung der Instituts-VPN-Gateways kann von den IT-Verantwortlichen der Institute selbständig den eigenen Mitgliedern (Studenten, Mitarbeitern) erteilt werden.
- **Admin-VPN**: VPN-Gateway zur ausschließlichen Nutzung für IT-Administratoren zum Management der Systeme in eigenen Instituts-Netzzonen (z. B. der Server). Alternativ/ergänzend ist auch eine eigene Sysadmin-Netzzone mit fest installierten Rechnern möglich.



Die genannten Netzzonen sind inzwischen am Institut für Physikalische Chemie eingerichtet und die meisten Endgeräte-Umzüge in die neuen Bereiche vollzogen. Für jede Netzzone wurden Filterregeln abgesprochen und installiert. Im Wesentlichen wurden dabei folgende Kommunikationsregeln umgesetzt:

- Arbeitsplatzrechner dürfen (wie gewohnt) frei nach „draußen“ kommunizieren. Initiale Zugriffe von „außerhalb“ sind nicht erlaubt.
- Server dürfen nur bzgl. ihrer Dienste erreicht werden. Wenn es Server für rein Instituts-interne Dienste sind, so dürfen sie auch nur von den entsprechenden Netzzonen angesprochen werden.
- Für besonders zu sichernde Arbeitsplätze, Labor- und CIP-Pool-Rechner sind die Filterregeln sehr Instituts-spezifisch und müssen besprochen werden. Im Allgemeinen sind für diese Bereiche stärkere Einschränkungen sinnvoll.
- Die über User-VPN eingewählten Nutzer bekommen ähnliche Rechte wie lokale Arbeitsplätze bzw. besonders abgesicherte lokale Arbeitsplätze.

Häufig können für die Planungen der Filterregeln bereits gewonnene Erfahrungen und Regelsätze aus anderen Instituten als Vorlage genommen werden. Insbesondere sollte nicht versucht werden, gleich zu Anfang eine „vollkommene“ Lösung anzustreben. Einfache Grundstrukturen mit einfachen Grundregeln bringen schon sehr viel. Ein „Fein-Tuning“ kann später immer noch durchgeführt werden.

Zurzeit gehen wir davon aus, dass die Netz-Strukturierung des NWZ in den meisten Bereichen in diesem Sommer abgeschlossen werden kann. Die gewonnenen Erfahrungen und die in Arbeit befindliche Implementierung des Netzzonenmodells sowie die Unterstützung der Filterregelverwaltung in NIC_online werden das Verfahren weiter beschleunigen und vereinfachen können. Gerne beraten wir weitere Interessenten über die Möglichkeiten der Strukturierung und Absicherung ihrer Netzbereiche.

Der neue Webserverpark

R. Perske

Der bevorstehende Abschied von der AIX-DCE/DFS-Infrastruktur war Anlass für die Entwicklung einer grundlegend neu konzipierten Infrastruktur für die zentralen WWW-Server. Das neue Konzept auf Basis von Linux-Servern, GPFS-Dateisystem und SAN-Datenspeicherung berücksichtigt die gestiegenen Anforderungen an Sicherheit, Verfügbarkeit und Skalierbarkeit ebenso wie die Belange und geänderten, vielfältigen Bedürfnisse der Informationsanbieter.

Aus verschiedenen Gründen müssen die vorhandenen Webserver innerhalb der nächsten Monate bis auf wenige Ausnahmen komplett ersetzt werden. Natürlich nutzen wir diese Gelegenheit, um ein grundlegend verbessertes Konzept zu realisieren und das Angebot für unsere Infoanbieter weitestmöglich zu verbessern.

Wesentliche Neuerungen für die Infoanbieter werden sein:

- **Dynamische generierte Inhalte**: PHP-Skripte und beliebige CGI-Programme für jeden Infoanbieter überall im Webspace
- **Konfigurierbarkeit**: Die Eigenschaften des Webservers können auf Verzeichnisebene über .htaccess-Dateien weitestgehend frei konfiguriert werden.

Der Umstieg erfolgt schrittweise im Laufe dieses Jahres. WWW-Angebote, die auf das Betriebssystem AIX oder auf sonstige spezifische Eigenschaften der bisherigen Systeme angewiesen sind, können für eine Übergangszeit weiterhin auf den bisherigen Servern laufen, die als spezielle Backend-Server in den neuen Webserverpark integriert werden. (DCE/DFS wird aber bald nicht mehr verfügbar sein.)

Beim Entwurf des Webserverparks wurden neben den verbesserten Möglichkeiten für die Informationsanbieter insbesondere die folgenden Aspekte berücksichtigt:

- **Skalierbarkeit und Performanz**: Eventuell auftretende Kapazitätsengpässe im neuen Webserverpark sollten durch Hinzufügen weiterer Komponenten beseitigt werden können, egal ob die Engpässe CPU-Leistung, I/O-Performance, Netzwerkbandbreite, Plattenplatz oder sonstige Komponenten betreffen.
- **Ausfallsicherheit und Stabilität**: Falls eine Komponente des Webserverparks ausfällt, müssen andere Komponenten dessen Aufgaben automatisch übernehmen. Möglichst nur erprobte Komponenten sollen beim Aufbau des Webserverparks Verwendung finden.

- **Einfaches Management**: Der Webserverpark soll ohne ständige Beaufsichtigung oder gar Eingriffe durch Systemadministratoren laufen können. Notwendige Sicherheitsupdates sollen möglichst automatisch vorgenommen werden. Soweit wie möglich sollen nur standardisierte Komponenten verwendet werden.
- **Erweiterbarkeit und Anpassungsfähigkeit**: Der Webserverpark soll auch zukünftigen Anforderungen nach Möglichkeit gewachsen sein. Notwendige Erweiterungen sollen ohne Schwierigkeiten eingebaut werden können.
- **Sicherheit**: Neben umfangreichen Maßnahmen zur Systemsicherheit sollen natürlich auch Datensicherheit und Datenschutz gewährleistet sein.

Das jetzt realisierte Konzept verwendet für fast alle Server ein langlebiges und stabiles Linux (RedHat Advanced Server über Landeslizenz) als Betriebssystem und Softwarebasis auf leistungsfäiger Standard-Intel-Serverhardware. Nur in notwendigen Fällen wird zusätzliche Software installiert, damit soweit wie möglich der automatische Update-Service von RedHat genutzt werden kann. Als gemeinsames Dateisystem für alle WWW-Daten wird das GPFS-Dateisystem verwendet, welches bereits im ZIV-Cluster seine Stabilität und Performanz bewiesen hat. Zur Datenspeicherung werden gespiegelte RAID5-Plattensysteme in einem in allen Teilen redundant aufgebauten Storage Area Network (SAN) verwendet. Die tägliche Datensicherung erfolgt mit dem bewährten Tivoli-Storage-Manager TSM.

Die Server werden in mehrere funktionelle Gruppen aufgeteilt, wobei einzelne Rechner durchaus auch mehreren Gruppen angehören können:

- Anfänglich zwei **Frontend-Server** nehmen sämtliche WWW-Kontakte zur zentralen WWW-Adresse www.uni-muenster.de und einigen anderen WWW-Adressen aus dem Internet entgegen. Ein vorgeschaltetes Lastverteilungssystem verteilt ankommende Anfragen auf die Frontend-Server und sorgt dafür, dass nur laufende Frontend-Server bei der Verteilung berücksichtigt werden. Sofern Anfragen von den Frontend-Servern nicht unmittelbar mit einem Verweis (Redirect) auf ein anderes WWW-Angebot beantwortet werden können, arbeiten diese als Reverse-Proxy-Server und verteilen sie (mittels eingebautem Balancer) auf mehrere Backend-Server.
- Mehrere **normale Backend-Server** leisten die Hauptarbeit und greifen auf ein gemeinsames GPFS-Dateisystem zu. Nach Bedarf können weitere Server hinzugefügt werden.
- Drei **File-Server** sorgen ausfallsicher für den Zugriff auf das **GPFS-Dateisystem**.
- Ein **Upload-Server** erlaubt Infoanbietern die manuelle Pflege ihres WWW-Angebots. (Da Ausfälle dieses Servers keine so gravierenden Folgen haben, wird auf den Aufbau einer Hochverfügbarkeitslösung verzichtet.) Auf den Upload-Server kann per **SSH / SCP / SFTP** (Dienstname upload.uni-muenster.de) zugegriffen werden, außerdem wird mittels Samba für Nutzer aus der Windows-Domain UNI-MUENSTER das **Netzwerklaufwerk** \\upload.uni-muenster.de\www angeboten.
- Einige **spezielle Backend-Server** erledigen besondere Aufgaben, z. B. die zentrale Suchmaschine oder das Content-Management-System Imperia, und liegen teilweise innerhalb, teilweise außerhalb des Webserverparks. Jeder WWW-Server kann auf diese Weise eingebunden werden, insbesondere ist dies bei allen noch unter AIX laufenden WWW-Servern der Fall.

Jeder Informationsanbieter erhält seinen eigenen, unter einer speziell dafür eingerichteten Nutzerkennung laufenden virtuellen Server auf den Backend-Servern. Die Frontend-Server sorgen für die korrekte Abbildung der WWW-Adressen auf die virtuellen Server.

Alternativ kann ein WWW-Angebot auch ganz oder teilweise mit dem Content-Management-System Imperia gepflegt werden. Dieses wird auf einer Gruppe von speziellen Backend-Servern in den Webserverpark eingebunden.

Als wesentlicher Beitrag zum Thema Sicherheit werden alle Zugriffe von außen auf den Webserverpark werden durch restriktiv konfigurierte Paketfilter auf den verschiedenen

Servern blockiert. Ausgenommen sind nur HTTP- und HTTPS-Zugriffe auf die Frontend-Server und SSH- und SMB-Zugriffe auf den Upload-Server sowie SSH-Zugriffe nur von wenigen Administrator-Systemen auf alle Server. Auch zwischen den Servern des Webserverparks werden durch die Paketfilter nur die benötigten Zugriffe gestattet, so dass die Frontend-Server gleichzeitig die Funktion einer Application Firewall ausüben.

Erstmals im ZIV wird zur Anmeldung per SSH / SCP / SFTP auf dem Upload-Server zwingend die Public-Key-Authentifizierung verlangt, eine Anmeldung nur mit Nutzerkennung und Passwort ist nicht mehr möglich. Ein eigener Artikel beschreibt, wie man sich einen Public Key erzeugt und diesen mittels MeinZIV auf dem Upload-Server hinterlegt. Nach dieser einmaligen Einrichtung ist der Zugang sowohl sicherer als auch in der Bedienung noch einfacher.

Alle Konfigurationsdateien der verschiedenen WWW-Server werden aus einer einzigen Konfigurationsquelle erzeugt. Für jedes WWW-Angebot (zu dem u. U. je zwei virtuelle Hosts auf Frontend-Server und auf Backend-Server gehören) ist nur eine einzige Zeile in diese Konfigurationsquelle einzutragen. Dies vermindert die Gefahr von Konfigurationsfehlern. (Bei Angeboten unter Host- oder Domainnamen muss zusätzlich dafür gesorgt werden, dass die DNS-Server für diesen Namen die IP-Adresse des Frontend-Servers herausgeben.)

Der Webserverpark ist jetzt nahezu vollständig wie beschrieben aufgebaut und befindet sich jetzt im Testbetrieb. Es fehlen noch der Mechanismus zur Verteilung der Anfragen auf die Frontend-Server (derzeit trägt ein Server die Last alleine und müsste im Falle eines Ausfalls manuell durch den anderen ersetzt werden) und die Installation des Content-Management-Systems Imperia sowie einige Kleinigkeiten.

Die zentrale Suchmaschine läuft bereits als spezieller Backend-Server im Webserverpark, und eine Reihe von Informationsanbietern nehmen mit ihren Webspaces am Testbetrieb teil. Neue Entwicklungen sollten ab sofort nicht mehr auf den alten Webservern, sondern bereits im Webserverpark durchgeführt werden.

Sobald der Verteilmechanismus realisiert und ausgetestet ist, soll als erstes der Name „www.uni-muenster.de“ auf den Webserverpark umgelegt werden. Der bisherige zentrale Webserver wird dabei als spezieller Backend-Server im Webserverpark eingebunden, so dass die Informationsangebote anschließend nach und nach auf die normalen Backend-Server verschoben werden können. Der Umzug aller Infoanbieter soll im Laufe dieses Jahres abgeschlossen werden.

Für die Abrufer der Informationen sollte diese Umstellung völlig unsichtbar erfolgen; die Anbieter werden individuell informiert und müssen sich zum Zeitpunkt des Umzugs ihres jeweiligen Webspaces umstellen. Der nächste Artikel gibt die dafür notwendigen Informationen.

Webspaces im neuen Webserverpark

R. Perske

Dieser Artikel beschreibt technische Einzelheiten der verschiedenen Arten von WWW-Angeboten, die im neuen Webserverpark realisiert werden können.

Der neue Webserverpark unterstützt verschiedene Formen von WWW-Angeboten, sowohl in Bezug auf die WWW-Adresse als auch in Bezug auf die Realisierung. Im Normalfall werden nicht nur die Adressen, sondern auch die Inhalte vom Webserverpark vorgehalten. Dieser Artikel gibt unseren Informationsanbietern die für die Pflege ihrer Angebote notwendigen Hinweise.

URLs und Webspaces

Die WWW-Adressen (URLs) der über den Webserverpark angebotenen Informationen können drei verschiedene Formen annehmen (die Angabe *NNN* steht für einen vereinbarten eindeutigen Namen):

- Angebote unter einem **Verzeichnisnamen** *NNN*

  Startadressen sind:

  – http://www.uni-muenster.de/*NNN*/ (unverschlüsselt) und

  – https://www.uni-muenster.de/*NNN*/ (SSL-verschlüsselt!)

  Dies ist der Normalfall für einen Webspace. Anders als auf den bisherigen Webservern bestehen keine funktionalen Einschränkungen gegenüber anderen Angeboten; im Gegenteil stehen HTTPS-Zugang und das Content-Management-System Imperia sogar nur für diese Angebote zur Verfügung.

- Angebote unter einem **Hostnamen** *NNN*

  Startadressen sind:

  – http://*NNN*.uni-muenster.de (unverschlüsselt) und

  – http://www.*NNN*.uni-muenster.de (unverschlüsselt)

  Dies ermöglicht „visitenkartenfreundliche“ WWW-Adressen, bietet jedoch keine SSL-Verschlüsselung.

  Nur Rechnernamen, die nicht anderweitig belegt sind, können verwendet werden.

- Angebote unter einem **Domainnamen** *NNN*.de; Startadresse ist:

  – http://www.*NNN*.de. (unverschlüsselt)

  Dies ermöglicht „visitenkartenfreundliche“ WWW-Adressen, bietet jedoch keine SSL-Verschlüsselung.

  Die Domain muss nach vorheriger Absprache mit dem ZIV kostenpflichtig bestellt werden. Auch andere Toplevel-Domains als „de“ sind möglich.

  Dieses Angebot gilt nur sehr eingeschränkt für WWW-Angebote von Universitätseinrichtungen, da diese verpflichtet sind, im WWW unter der Domain uni-muenster.de aufzutreten.

Angebote unter Hostnamen oder Domainnamen können in besonderen Ausnahmefällen auch SSL-geschützt abrufbar eingerichtet werden. Meist ist jedoch eine Kombination mit einem Angebot unter einem Verzeichnisnamen die bessere Wahl, weil dann keine zusätzliche IP-Adresse und kein zusätzliches SSL-Zertifikat benötigt werden und außerdem das Content-Management-System Imperia benutzt werden kann.

Hinter jeder dieser drei Adressformen kann einer der folgenden Angebotsformen realisiert werden:

- Ein **Webspace** (Virtual Host) im Webserverpark und ein Durchreichen (Reverse Proxy) der WWW-Zugriffe an diesen Webspace (dies ist der Normalfall)
- Ein **Reverse Proxy** (Durchreichen) zu einem anderen WWW-Angebot
- Ein **Redirect** (Umleitung) auf eine andere WWW-Adresse

Webspaces unter einem Verzeichnisnamen können teilweise oder ganz mit dem zentralen Content-Management-System Imperia gepflegt werden. Nicht mit Imperia gepflegte (Teile von) Webspaces können als Netzwerklaufwerk eingebunden und/oder mit SSH / SCP / SFTP gepflegt werden.

Die Redirects funktionieren für Verzeichnisbäume: Wenn http://*NNN*.uni-muenster.de auf http://www.uni-muenster.de/*aaa* umgeleitet wird, dann wird automatisch auch ein Abruf von http://*NNN*.uni-muenster.de/*bbb*/*ccc* auf http://www.uni-muenster.de/*aaa*/*bbb*/*ccc* umgeleitet.

Häufig werden ein Webspace unter einem Verzeichnisnamen *NNN* und eine Umleitung unter einem Hostnamen *NNN* wegen der jeweiligen Vorteile (Content-Management-System und SSL-Verschlüsselung beim Webspace, kurze Adresse bei der Umleitung) mit-

einander **kombiniert**. Nur in diesem Fall kann der gleiche Name *NNN* für verschiedene Angebotsformen verwendet werden.

Eine sinnvolle Anwendung für einen Reverse Proxy wäre ein für die Öffentlichkeit bestimmtes WWW-Angebot auf einem Institutsserver, der aus Sicherheitsgründen mit einer „privaten" Internet-Adresse versehen wurde und/oder durch eine Firewall besonders geschützt wird.

Verzeichnisbäume im Webserverpark

Das Wurzelverzeichnis für sämtliche Daten des Webserverparks findet man beim Zugriff per SSH / SCP / SFTP auf **upload.uni-muenster.de** unter **/www/data/**, beim Zugriff über ein Netzwerklaufwerk unter **\\upload.uni-muenster.de\www**. Die nachfolgende Beschreibung verwendet als Kurzform /www/data/.

Sie sehen in diesem Verzeichnis /www/data/ für jedes WWW-Angebot *NNN* sowohl ein Datenverzeichnis *NNN* als auch ein Logdateiverzeichnis *NNN*.logs. Als Infoanbieter können Sie die Inhalte des Datenverzeichnisses verändern und die Inhalte des Logdateiverzeichnisses lesen. Auf die Verzeichnisse anderer Infoanbieter haben Sie keinen Zugriff. (Die für Sie lesbaren Dateien groups.dir und groups.pag benötigen Sie ausschließlich bei der Einschränkung von WWW-Zugriffsrechten auf zentral eingerichtete Nutzergruppen, siehe unten.)

Im Logdateiverzeichnis **/www/data/*NNN*.logs/** finden Sie Protokolle über Fehler, die bei Zugriffen auf Ihren Webspace auftreten. Diese Protokolle können hilfreich sein, wenn selbst geschriebene PHP- und CGI-Programme nicht so funktionieren wie sie sollen.

Im Datenverzeichnis **/www/data/*NNN*/** befinden sich das Unterverzeichnis htdocs, dieses ist das Wurzelverzeichnis Ihres WWW-Angebots, und die Unterverzeichnisse home, cgi-bin und eventuell imperialive. Sie können hier weitere Unterverzeichnisse anlegen. Auf die in /www/data/*NNN*/home, /www/data/*NNN*/imperialive oder den weiteren Unterverzeichnissen enthaltenen Dateien kann nicht über das WWW direkt zugegriffen werden. (Aber Ihre PHP- und CGI-Programme können diese Verzeichnisse nutzen.)

Im Verzeichnis **/www/data/*NNN*/htdocs/** und evtl. in **/www/data/*NNN*/cgi-bin/** befinden sich Ihre WWW-Dateien. Dabei gelten die folgenden Zuordnungen von WWW-Adressen zu Dateinamen:

- WWW-Angebote unter Verzeichnisnamen:

  http://www.uni-muenster.de/*NNN*/*bbb*/*ccc*
  https://www.uni-muenster.de/*NNN*/*bbb*/*ccc*

  → /www/data/*NNN*/htdocs/*NNN*/*bbb*/*ccc*

- WWW-Angebote unter Host- oder Domainnamen:

  http://*NNN*.uni-muenster.de/*aaa*/*bbb*/*ccc*
  http://www.*NNN*.uni-muenster.de/*aaa*/*bbb*/*ccc*
  http://www.*NNN*.de/*aaa*/*bbb*/*ccc*

  → /www/data/*NNN*/htdocs/*aaa*/*bbb*/*ccc*

- http://*NNN*.uni-muenster.de/cgi-bin/*bbb*/*ccc*
  http://www.*NNN*.uni-muenster.de/cgi-bin/*bbb*/*ccc*
  http://www.*NNN*.de/cgi-bin/*bbb*/*ccc*

  → /www/data/*NNN*/cgi-bin/*bbb*/*ccc*

Bei WWW-Angeboten unter einem Verzeichnisnamen befinden sich im schreibgeschützten Verzeichnis **/www/data/*NNN*/imperialive/** die über das Content-Management-System Imperia erzeugte WWW-Dateien. Diese können mittels symbolischer Links

/www/data/*NNN*/htdocs/*NNN*/*bbb* → /www/data/*NNN*/imperialive/*NNN*/*bbb*

in das htdocs-Unterverzeichnis eingebunden werden. (Bei komplett mit Imperia gepflegten Webspaces werden entsprechende symbolische Links bereits beim Einrichten des Webspaces vom ZIV angelegt.)

Eine Einbindung von mit Imperia gepflegten Verzeichnisbäumen in Webspaces unter Host- oder Domainnamen ist schwierig, weil die Standard-Imperia-Templates der Universität Links erzeugen, die auf den Hostnamen www.uni-muenster.de verweisen. Als Umgehung des Problems bietet sich oben genannte Kombination von Webspace und Umleitung an.

Im Verzeichnis **/www/data/*NNN*/home/** befinden sich einige zum SSH-Login benötigte Daten, insbesondere Ihr hinterlegter Public Key.

Regelmäßige Unix-Nutzer werden sich eine Datei /www/data/*NNN*/home/*Nutzerkennung*/.bashrc anlegen wollen, um die Arbeitsumgebung an eigene Gewohnheiten anzupassen. Nutzer mit Zugriff auf mehrere Webspaces haben aber nur in einem Webspace ein home-Verzeichnis.

Für den gesamten Verzeichnisbaum unter /www/data/*NNN*/ (also ohne Logdateien) gibt es eine gemeinsame Plattenplatzquote, welche bei Bedarf erhöht werden kann. (home und die weiteren Verzeichnisse neben htdocs sind nur für Daten gedacht, die im Zusammenhang mit dem WWW-Angebot anfallen, nicht für persönliche oder sonstige Daten. Dafür nutzen Sie bitte die anderen Angebote des ZIV.)

Dateisystem-Zugriffsrechte

Die Dateisystem-Zugriffsrechte regeln, wer welche Dateien über SSH / SCP / SFTP oder über ein Netzwerklaufwerk bearbeiten darf. (Davon völlig getrennte, in einem weiteren inforum-Artikel beschriebene WWW-Zugriffsrechte regeln, wer über das WWW auf welche Angebote zugreifen darf.)

Die unveränderlichen Zugriffsrechte auf Ihr Datenverzeichnis *NNN* sorgen dafür, dass ausschließlich der WWW-Server und die Mitglieder Ihrer Infoanbieter-Nutzergruppe auf das Datenverzeichnis zugreifen können. Es ist also überhaupt kein Problem und daher eine sinnvolle Vereinfachung, alle Dateien in Ihrem Webspace für jedermann les-, schreib- und ausführbar zu machen.

Beim Zugriff über das Netzwerklaufwerk sorgt unser Samba-Server dafür, dass automatisch die richtigen Dateisystem-Zugriffsrechte auf neu angelegte Dateien und Unterverzeichnisse eingestellt werden und dass (von einer kleinen Ausnahme abgesehen) keine Änderungen möglich sind.

Beim Zugang per SSH / SCP / SFTP müssen Sie leider selbst darauf achten, immer die richtigen Zugriffsrechte zu setzen. Im Zweifel können Sie über SSH mit dem folgenden Befehl alle von Ihnen angelegten Dateien wieder mit geeigneten Zugriffsrechten versehen, ohne die Sicherheit zu gefährden:

chmod -R 777 /www/data/*NNN*/htdocs

Weitere Einzelheiten finden Sie im WWW unter `http://www.uni-muenster.de/ZIV/Server/WWW/`.

Hinweise für eigene Programme (in PHP usw.)

Aus der Konzeption des Webserverparks ergeben sich einige Besonderheiten, die beim Programmieren und Installieren eigener Programme zu beachten sind.

Auf die Steuerung von WWW-Zugriffsrechten und auf die umfangreichen Möglichkeiten für eigene Einstellungen gehen eigene Artikel in diesem inforum ein.

Sitzungen / Sessions

Da verschiedene WWW-Zugriffe von verschiedenen Backend-Servern verarbeitet werden, muss bei der Verwaltung von Sitzungen darauf geachtet werden, dass die Sitzungsdaten an einer Stelle abgelegt werden, auf die alle Backend-Server zugreifen können.

PHP-Programme, die die Session-Funktionen benutzen, sollten daher als eine der ersten Anweisungen im Programm die Lage der Sitzungsdaten angeben:

ini_set('session.save_path','/www/data/*NNN*/sessions');

Natürlich sollte das Verzeichnis /www/data/*NNN*/sessions/ vorher angelegt werden.

In gleicher Weise sollten auch Sitzungsdaten bei Verwendung anderer Programmiersprachen und überhaupt alle anderen Daten, die von einem Zugriff zum nächsten überdauern sollen, in Unterverzeichnissen von /www/data/*NNN*/ abgelegt werden.

Programmiersprachen / Skriptsprachen

Zur Verfügung stehen unter anderem:

- PHP 4.x in der von RedHat gepflegten Version (bereits eingebunden als Apache-Handler)
- PHP 5.x in einer selbst kompilierten Version (bereits eingebunden als Apache-Handler)
- Alle weiteren zum Lieferumfang von RedHat Advanced Server gehörenden Sprachen (entsprechende Programme müssen aber als CGI-Programme aufgerufenen werden)

Aus Sicherheitsgründen nicht zur Verfügung stehen jedoch die Apache-Module mod_php und mod_perl. Daher stehen vereinzelte PHP-Features nicht zur Verfügung (insbesondere keine persistenten Datenbankverbindungen).

Auf Wunsch können Perl-Module und in gewissem Rahmen andere Software nachinstalliert werden. Bitte nehmen Sie bei Bedarf frühzeitig Kontakt mit uns auf, damit wir gemeinsam die beste Lösung für Ihre Problemstellung finden können.

Beantragung

Bei diesem Thema gibt es keine organisatorischen Änderungen:

Sinnvolle **Reverse Proxys** und **Redirects** werden ohne förmliches Antragsverfahren durch das ZIV eingerichtet: Verantwortliche Betreiber von Webservern und Webspaces in der Universität können sich bei konkretem Bedarf an das ZIV wenden.

Wenn ein **Webspace** ganz oder teilweise **manuell** (nicht mit Imperia) gepflegt werden soll, muss förmlich eine Nutzergruppe beantragt und eingerichtet werden. Die einzeln zu benennenden Mitglieder dieser Nutzergruppe haben das Recht, das Netzwerklaufwerk einzubinden oder sich mit SSH / SCP / SFTP auf dem Upload-Server anzumelden und dort die Dateien des Webspaces zu pflegen.

Um einen **Webspace** ganz oder teilweise mit **Imperia** zu pflegen, müssen entsprechende Rubriken und Rollen unter Imperia eingerichtet werden. Auch hier sind in der Regel förmliche Anträge erforderlich, Einzelheiten sprechen Sie bitte mit der Online-Redaktion der Universität ab.

Umzug der bisherigen WWW-Angebote

Wer seine WWW-Angebote ausschließlich mit dem Content-Management-System Imperia pflegt, braucht sich nicht umzustellen. Der Umzug des „Live-Systems“ wird vom ZIV durchgeführt.

Informationsanbieter, die ihre Angebote auf den bisherigen WWW-Servern ganz oder teilweise manuell pflegen, werden beim Umzug jeweils einen neuen Server und einen neuen Pfad in ihre Upload-Software einstellen müssen. Dabei gelten die folgenden Entsprechungen:

Pflege über ein Netzwerklaufwerk (SMB):

alt: \\samba.uni-muenster.de\www\dat*NNN*
neu: \\upload.uni-muenster.de\www*NNN*\htdocs*NNN*

Pflege mit SSH / SCP / SFTP:

alt: /dfs/p/www/dat/*NNN* auf zivunix.uni-muenster.de
neu: /www/data/*NNN*/htdocs/*NNN* auf upload.uni-muenster.de

Symbolische Links in Imperia-gepflegte Bereiche:

alt: /dfs/p/www/dat/*NNN*/*bbb* → /dfs/p/www/cms/imperia/htdocs/*NNN*/*bbb*
neu: /www/data/*NNN*/htdocs/*NNN*/*bbb* → /www/data/*NNN*/imperialive/*NNN*/*bbb*

Wer den Zugang zu einem Teil seiner WWW-Seiten mittels Nutzerkennung und Passwort schützt und sich dabei der zentralen Nutzerverwaltung bedient, wird seine „.htaccess"-Dateien anpassen müssen. Weiter hinten in diesem infoWWW erhalten Sie genaue Informationen.

Wer seinen Webspace mit SSH / SCP / SFTP pflegt, wird sich einen Public Key erzeugen und im Webserverpark hinterlegen müssen. Ein weiterer Artikel in diesem infoWWW gibt dafür eine Schritt-für-Schritt-Anleitung.

Der Umzug von CGI-Servern und Dynamic-Content-Servern gestaltet sich etwas aufwändiger, da die Programme an die neue Systemumgebung angepasst werden müssen. Dabei wird das ZIV intensive Hilfestellung leisten.

Steuerung der WWW-Zugriffsrechte im neuen Webserverpark

R. Perske

Der neue Webserverpark bietet verschiedene Methoden, um die Zugriffe auf WWW-Seiten einzuschränken.

Die WWW-Zugriffsrechte werden wie andere eigene Einstellungen mit den Dateien **.htaccess** und **.htsslaccess** (jeweils mit Punkt am Anfang) im obersten Verzeichnis des jeweiligen Verzeichnisbaumes gesteuert. Beim unverschlüsselten Zugriff über HTTP wird nur die Datei .htaccess beachtet. Beim verschlüsselten Zugriff über HTTPS wird, falls vorhanden, die Datei .htsslaccess beachtet und nur, falls diese nicht vorhanden ist, ebenfalls die Datei .htaccess beachtet.

Zugriffskontrolle anhand von IP-Adressen

Von der Verwendung dieses Mechanismus, um den Zugriff auf bestimmte Personenkreise einzuschränken, wird abgeraten. Denn jeder Einwohner Westfalens hat rechtmäßig Zugang zu einigen Rechnern, die am lokalen Netz der Universität angeschlossen sind (Landesbibliothek, Kliniken usw.).

Der früher angebotene Mechanismus, Verzeichnisse namens wwuonly auf diese Weise nur für am lokalen Netz angeschlossene Rechner zugreifbar zu machen, wird daher im Webserverpark nicht mehr verwendet.

Falls Sie trotzdem Unterverzeichnisse nur für einzelne IP-Adressen freigeben möchten, müssen Sie beachten, dass alle Zugriffe über die als Reverse-Proxy-Server fungierenden Frontend-Server des Webserverparks laufen und die IP-Adressen daher der HTTP-Kopfzeile X-Forwarded-For entnommen werden müssen. Um beispielsweise nur den IP-Adressen 128.176.123.45 und 128.176.67.89 den Zugriff zu erlauben, schreiben Sie in die Datei .htaccess:

```
SetEnvIf X-Forwarded-For "^128\.176\.123\.45$" DarfZugreifen
SetEnvIf X-Forwarded-For "^128\.176\.67\.89$" DarfZugreifen
Order Deny,Allow
Deny from all
Allow from env=DarfZugreifen
```

Für weitere Einzelheiten beachten Sie bitte die Apache-Dokumentation unter `http://httpd.apache.org/docs/2.2/`.

Zugriffskontrolle anhand von Nutzerkennung und Passwort

Um den Zugriff über das WWW auf einen bestimmten (möglicherweise auch sehr großen) Personenkreis einzuschränken, können Sie vom Leser die Angabe von Nutzerkennung und Passwort verlangen.

Damit niemand Passwörter im Klartext über das Netz schickt, verwenden Sie natürlich eine HTTPS-Adresse und verbieten den Zugriff über HTTP. Für Letzteres schreiben Sie in die Datei .htaccess:

```
Order Allow,Deny
Deny from all
Satisfy All
```

Zentrale Nutzerkennungen und Standardpasswörter

Am einfachsten für Infoanbieter und Nutzer ist es, wenn die zentralen Nutzerkennungen und zentralen Standardpasswörter verwendet werden. Dazu schreiben Sie in die Datei .htsslaccess die folgenden Zeilen:

```
AuthName "Restricted Area"
AuthType Basic
AuthBasicProvider pam
AuthDBMGroupFile /www/data/groups
Require group u0mitarb u0dawin
```

Die ersten beiden Zeilen aktivieren die Zugangskontrolle und legen fest, welcher Text (ohne Umlaute!) bei der Passwortabfrage angezeigt wird. (Das Beispiel verwendet *Restricted Area*, wählen Sie bitte eine eigene sinnvolle und eindeutige kurze Beschreibung.) Die dritte Zeile verbindet die Zugangskontrolle mit den zentralen Standardpasswörtern. Die vierte Zeile versorgt sie mit den zentralen Nutzergruppen. Die letzte Zeile beschränkt den Zugriff auf Mitarbeiter und Studierende der Universität Münster (denn genau die sind Mitglieder der Nutzergruppen *u0mitarb* bzw. *u0dawin*.)

Um nur die Personen mit den Nutzerkennungen *held* und *bosse* zuzulassen, schreiben Sie:

```
Require user held bosse
```

Sie können mehrere Require-Zeilen angeben. Bei dieser Methode ist es erforderlich, dass sämtliche Nutzer, denen Sie Zugang gewähren möchten, eine zentrale Nutzerkennung besitzen. Dies ist bei allen Mitarbeitern und Studierenden der Universität Münster und bei Angehörigen etlicher weiterer Personenkreise der Fall.

Nicht in allen Fällen wird es geeignete Nutzergruppen geben, so dass Sie in solchen Fällen die Liste aller Nutzer in die Konfigurationsdatei eintragen müssen.

Eigene Nutzerkennungen und Passwörter

Mit etwas mehr Aufwand können Sie auch eigene Nutzerkennungen und Passwörter einrichten. Die Datei .htaccess sieht dabei genauso aus wie oben, in die Datei .htsslaccess schreiben Sie die folgenden Zeilen:

```
AuthName "Restricted Area"
AuthType Basic
AuthBasicProvider file
AuthUserFile /www/data/NNN/restricted-area-users
Require valid-user
```

Außerdem legen Sie (geeignete Namen suchen Sie sich bitte selbst aus) die in der Zeile AuthUserFile genannte Datei /www/data/*NNN*/*restricted-area-users* an. Dazu benutzen Sie bitte in einer SSH-Dialogsitzung für die erste Nutzerkennung das Kommando:

```
/www/data/sys/htpasswd -c /www/data/NNN/restricted-area-users username
```

und für jede weitere Nutzerkennung das Kommando:

/www/data/sys/htpasswd /www/data/*NNN*/*restricted-area-users username*

Für *username* setzen Sie jeweils eine Nutzerkennung Ihrer Wahl ein; anschließend werden Sie nach einem Passwort Ihrer Wahl gefragt. Diese Nutzerkennungen und Passwörter geben Sie dann bitte an die jeweiligen Personen weiter.

Sowohl eigene als auch zentrale Nutzerkennungen und Passwörter

Sie können beide Verfahren auch mischen. Schreiben Sie dazu in die Datei .htsslaccess die folgenden Zeilen:

AuthName "*Restricted Area*"
AuthType Basic
AuthBasicProvider file pam
AuthUserFile /www/data/*NNN*/*restricted-area-users*
AuthDBMGroupFile /www/data/groups
Require *user held bosse lars-mueller thomas-schulze*

In diesem Fall werden eingegebene Nutzerkennungen zuerst anhand der Datei /www/data/*NNN*/*restricted-area-users* überprüft. Nur wenn die eingegebene Nutzerkennung in dieser Datei gar nicht vorkommt, wird sie anhand der zentralen Nutzerverwaltung überprüft.

Wenn Sie diese Methode wählen, empfiehlt es sich, für die eigenen Nutzerkennungen solche mit Bindestrich zu wählen. Dadurch vermeiden Sie, dass Sie eine eigene Nutzerkennung wählen, die es auch als zentrale Nutzerkennung geben kann.

Anonymer Passwortschutz

Ein einfacher Fall für eigene Passwörter liegt vor, wenn Sie keinen wirklichen Schutz, sondern nur eine Hürde aufbauen möchten. Beispielsweise möchten Sie die Unterlagen einer Vorlesung schützen, aber jeder, der ein von Ihnen in der Vorlesung genanntes Passwort kennt, soll zugreifen dürfen, ohne dass Sie die Nutzerkennungen aller Teilnehmer erfassen möchten.

Dann verwenden Sie genau die oben unter „Eigene Nutzerkennungen und Passwörter“ beschriebene Methode, richten aber nur eine einzige Nutzerkennung mit Passwort ein und geben diese in Ihrer Vorlesung bekannt.

Für weitere Einzelheiten beachten Sie bitte die Apache-Dokumentation unter `http://httpd.apache.org/docs/2.2/`.

Windows-Nutzer beachten bitte, dass alle Zeilen in den Dateien .htaccess und .htsslaccess nicht mit den Windows-Zeilenende-Zeichen CRLF, sondern nur mit dem Unix-Zeilenende-Zeichen LF abgeschlossen werden dürfen, andernfalls erscheint bei jedem WWW-Zugriff auf den Verzeichnisbaum ein „Internal Server Error“.

Eigene Einstellungen im neuen Webserverpark

R. Perske

Der neue Webserverpark erlaubt den Informationsanbietern weit gehende Kontrolle über Eigenschaften des WWW-Servers.

Um eigene Einstellungen für einen kompletten Webspace oder für einzelne Verzeichnisbäume innerhalb des Webspaces vorzunehmen, kann man im obersten Verzeichnis des Webspaces *NNN*/htdocs bzw. im obersten Verzeichnis des jeweiligen Verzeichnisbaumes zwei Dateien **.htaccess** und **.htsslaccess** (jeweils mit Punkt am Anfang) ablegen. Beim unverschlüsselten Zugriff über HTTP wird nur die Datei .htaccess beachtet. Beim verschlüsselten Zugriff über HTTPS wird, falls vorhanden, die Datei .htsslaccess beachtet und nur, falls diese nicht vorhanden ist, ebenfalls die Datei .htaccess beachtet.

In diesen Dateien können zahlreiche Einstellungen vorgenommen werden. Ausführliche Informationen enthält die Online-Dokumentation des Apache-Webservers unter `http://httpd.apache/org/docs/2.2/`. Nachfolgend wird nur auf die wichtigsten Anwendungen und auf lokale Besonderheiten eingegangen.

WWW-Zugriffsrechte

Sie können für Ihren Webspace oder Teile davon den Zugriff auf bestimmte Personen oder Gruppen beschränken, dies wird in einem weiteren Artikel beschrieben.

Dateinamen der Titelseiten

Falls beim Abruf einer WWW-Seite die Adresse eines Verzeichnisses angegeben wird, beispielsweise http://www.uni-muenster.de/*NNN*/*bbb*/, dann wird im entsprechenden Verzeichnis /www/data/*NNN*/htdocs/*NNN*/*bbb*/ nach folgenden Dateien gesucht, Groß-kleinschreibung ist wichtig:

1. Welcome.shtml
2. Welcome.html
3. welcome.html
4. welcome.htm
5. index.cgi
6. index.php
7. index.shtml
8. index.html
9. index.htm
10. index.html.var
11. /ErrNotFound.asis

Die Liste können Sie abändern, indem Sie in .htaccess bzw. in .htsslaccess eine Zeile mit dem Wort „DirectoryIndex“, gefolgt von den gewünschten Dateinamen, eintragen. (Die Verwendung der Welcome-Namen in der voreingestellten Liste hat historische Gründe, diese Namen sollten nicht mehr verwendet werden.)

Die erste gefundene Datei aus dieser Liste wird als Titelseite des Unterverzeichnisses angezeigt. Die letztgenannte Datei /ErrNotFound.asis sorgt dafür, dass eine Fehlermeldung erzeugt wird, falls keine der anderen Dateien gefunden wird. Wenn Sie statt der Fehlermeldung ein Inhaltsverzeichnis des Verzeichnisses anzeigen lassen möchten, lassen Sie in der Zeile DirectoryIndex einfach diese Datei weg.

Die Datei /ErrNotFound.asis liegt im Wurzelverzeichnis des WWW-Servers und ist nur bei WWW-Angeboten unter einem Verzeichnisnamen immer vorhanden. Bei WWW-Angeboten unter Host- oder Domainnamen sind Sie selbst dafür verantwortlich, eine solche Datei anzulegen. Die ersten beiden Zeilen dieser Datei müssen lauten „Status: 404 Not Found“ und „Content-Type: text/html“, danach muss eine Leerzeile folgen und danach eine ganz normale HTML-Seite.

Eigene Fehlermeldungsseiten

Fehlermeldungen beim Versuch, auf nicht vorhandene oder zugangsbeschränkte Seiten zuzugreifen, erscheinen normalerweise im Layout der Universität Münster. Wenn Sie eigene Fehlerseiten gestalten möchten, können Sie diese mit folgenden Zeilen in .htaccess bzw. .htsslaccess angeben:

ErrorDocument 404 /*NNN*/FehlerNichtGefunden.html
ErrorDocument 403 /*NNN*/FehlerZugriffVerweigert.html
ErrorDocument 401 /*NNN*/FehlerFalschesPasswort.html

Die angegebenen WWW-Seiten müssen Sie natürlich dann selbst in Ihrem Verzeichnis /www/data/*NNN*/htdocs/ erstellen. (Der erste Schrägstrich in den ErrorDocument-Zeilen entspricht dem Schrägstrich hinter htdocs.)

Eigene Umleitungen

Wenn Sie den WWW-Browser eines Nutzers beim Zugriff auf ein (ehemaliges) Unterverzeichnis Ihres Webspaces auffordern möchten, doch bei einer anderen Adresse nachzuschauen, können Sie folgende Anweisung in .htaccess bzw. .htsslaccess verwenden:

RedirectPermanent /*NNN*/*bbb*/*ccc*/ http://irgend.wo/anders/

Server Side Includes

Häufig ist es sinnvoll, gemeinsame Teile von HTML-Dateien (Seitenkopf, Seitenfuß, Navigationselemente usw.) nur an einer Stelle abzuspeichern und in der einzelnen HTML-Datei nur einen Verweis (eine Include-Anweisung) einzutragen. Die zentralen WWW-Server durchsuchen die WWW-Seiten nach solchen Include-Anweisungen und fügen die Inhalte der jeweils angegebenen Teil-Dateien an der Stelle der jeweiligen Include-Anweisungen ein. Es ist sogar möglich, Teile der WWW-Seiten nur dann einzufügen, wenn gewisse Bedingungen erfüllt sind.

Das gilt jedoch nur für solche WWW-Seiten, für die das Durchsuchen eingeschaltet ist; das ist der Fall, falls eine der folgenden Bedingungen erfüllt ist:

- Der Name der Datei endet auf .shtml (statt .html oder .htm).
- Die Einstellung *XBitHack* ist auf *on* oder *full* gestellt und die Dateisystem-Zugriffsrechte erlauben das „Ausführen“ durch den Eigentümer (das ist bei Verwendung der von uns empfohlenen Einstellungen der Fall).
- In einer für das aktuelle Verzeichnis wirksamen Datei .htaccess bzw. .htsslaccess steht die folgende Anweisung:

```
AddOutputFilter INCLUDES.html
```

Aufgrund der von uns empfohlenen Einstellung, das „Ausführen“ von Dateien auch durch die Gruppe zu erlauben, gilt bei der standardmäßig bei uns gültigen Einstellung *XBitHack full*, dass die Dateien wie normale HTML-Dateien mit einem Datum der letzten Änderung ausgeliefert werden. Wenn Sie nicht nur Navigationselemente, sondern wesentliche Inhalte aus Include-Dateien einbinden, kann das dazu führen, dass WWW-Browser alte Versionen der Seite anzeigen. Dann sollten Sie entweder das Ausführen-Recht von der Gruppe wegnehmen oder die Einstellung auf „XBitHack on“ umsetzen.

Verknüpfung von Dateiendungen mit Apache-Handlern

Voreingestellt sind folgende Verknüpfungen:

- AddHandler send-as-is asis
- AddHandler imap-file map
- AddHandler type-map var
- AddHandler php4-script php4
- AddHandler php5-script php5
- AddHandler php4-script php
- AddHandler cgi-script cgi

Das heißt unter anderem, dass Dateien mit der Endung .php vom PHP-4-Interpreter und Dateien mit der Endung .cgi als CGI-Programme ausgeführt werden. Da kein Perl-Handler zur Verfügung steht, müssen Perl-Skripte mit dem CGI-Handler ausgeführt werden.

Um auch Perl-Dateien mit der Endung .pl als CGI-Programme auszuführen, muss einerseits die Endung .pl mit dem CGI-Handler verknüpft werden, dazu ist die folgende Zeile in .htaccess bzw. .htsslaccess einzutragen:

AddHandler cgi-script pl

Andererseits ist in der ersten Zeile der Datei der Interpreter zu benennen:

#!/usr/bin/perl

Windows-Nutzer beachten bitte, dass diese Interpreter-Angabe und alle Zeilen in den Dateien .htaccess und .htsslaccess nicht mit den Windows-Zeilenende-Zeichen CRLF, sondern nur mit dem Unix-Zeilenende-Zeichen LF abgeschlossen werden dürfen, andernfalls erscheint bei jedem WWW-Zugriff auf die Datei bzw. auf den Verzeichnisbaum ein „Internal Server Error“.

SSH-Zugang zum neuen Webserverpark

R. Perske

Der SSH-Zugang zum neuen Webserverpark erfordert eine sichere, nach einmaliger Einrichtung aber auch bequeme Public-Key-Authentifizierung. Diese Anleitung beschreibt für verschiedene SSH-Software genau, was zu tun ist.

Auch bei anderen SSH-Zugängen kann diese Vorgehensweise zur Verbesserung der Sicherheit beitragen, daher sei diese Anleitung auch allen anderen SSH-Nutzern, insbesondere natürlich Systemverwaltern, ans Herz gelegt.

Auf praktisch allen **Linux**- und sonstigen **Unix**-Systemen finden Sie die Software SSH (Secure SHell). Diese ermöglicht durch Verschlüsselung abhörsichere Dialogverbindungen zu fremden Rechnern, auf denen ein SSHD (Secure SHell Daemon) entgegen nimmt. Meist enthält diese Software auch ein Programm SCP (Secure CoPy) und/oder ein Programm SFTP (Secure File Transfer Program) zur Übertragung von Dateien zwischen dem eigenen und dem fremden Rechner.

Für Windows-Systeme gibt es verschiedene freie SSH-Software. Die Software PuTTY enthält sowohl ein SSH-Programm mit typischer Windows-Oberfläche als auch ein SCP- und ein SFTP-Programm, die jedoch über die Eingabeaufforderung bedient werden: `http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html`. Der wesentliche Vorteil von PuTTY besteht darin, dass man die Programme aufrufen kann, ohne sie vorher installieren zu müssen, man kann sie also auch auf Rechnern nutzen, auf denen man keine Administrator-Rechte hat. Trotzdem ist es natürlich am einfachsten, sich den *Windows-style installer putty-0.58-installer.exe* zu besorgen und zu installieren.

Eine Windows-typische Fensteroberfläche bietet die Software FileZilla, welche Datenübertragungen nicht nur per unsicherem FTP, sondern auch per SFTP erlaubt und dabei auf PuTTY basiert: `http://www.filezilla.de/`. Wir empfehlen, beide Programme zu installieren.

Als Alternative zu PuTTY und FileZilla gibt es, ebenfalls mit **Windows**-Oberfläche, die Windows-Version von OpenSSH, welches nach der Installation über ein SSH- und SFTP-Icon auf dem Desktop leicht aufgerufen werden kann: `ftp://ftp.cert.dfn.de/pub/tools/net/ssh/`, dort nur die selbstentpackende Installationsdatei SSHSecureShellClient.....exe (die Pünktchen stehen für die Versionsnummer).

Aber auch für viele **andere** Systeme gibt es SSH-Software, siehe `http://www.openssh.org`.

Verbindung aufbauen – ohne Passwörter

Aus Sicherheitsgründen akzeptiert keiner der Rechner im Webserverpark noch irgendwelche Passwörter bei der Anmeldung. SSH-Verbindungen können ausschließlich mit Public-Key-Authentifizierung durchgeführt werden.

Um Dateien in Ihrem Webspace ablegen zu können, müssen Sie sich daher zuerst ein Schlüsselpaar erzeugen und den öffentlichen Schlüssel auf dem Upload-Server hinterlegen. Der geheime Schlüssel verbleibt bei Ihnen und wird mit einem Schlüssel-Passwort geschützt. Nur wer den geheimen Schlüssel besitzt und das Schlüssel-Passwort kennt, kann sich anmelden.

Wenn Sie die folgenden Anleitungen beachten, werden Sie sehen, dass das Verfahren zwar kompliziert klingt, nach einmaliger Einrichtung aber noch bequemer ist als die gewohnte Passworteingabe. Eine Bebilderung der Anleitungen würde den Rahmen des

infoWWW bei weitem sprengen, die Anleitungen sind aber sicherlich auch in dieser Form leicht verständlich.

Das Verfahren lässt sich natürlich auf fast alle weiteren SSH-Zugänge übertragen (leider nicht bei Servern, bei denen das Homeverzeichnis im DCE/DFS liegt); Sie müssen nur den Public Key an der richtigen Stelle auf dem per SSH erreichbaren Server ablegen. (Meist handelt es sich um die Datei authorized_keys im Verzeichnis .ssh im Homeverzeichnis des Nutzers.)

SSH-Zugang zum Webserverpark mit PuTTY und FileZilla unter Windows

Einmalige Vorbereitung

Um den Zugang zum Webserverpark einzurichten, müssen Sie einmalig die folgenden Schritte durchführen:

1. Starten Sie PuTTYgen: *Start* | *Alle Programme* | *PuTTY* | *PuTTYgen*
2. Es erscheint ein Fenster *PuTTY Key Generator*
3. Klicken Sie im Bereich *Actions* auf den Knopf *Generate*
4. Sie werden aufgefordert, Ihre Maus über die leere Fläche zu bewegen, um Zufälligkeiten zu sammeln
5. Ein Schlüsselpaar wird erzeugt
6. Oben im Fenster erscheint danach im Bereich *Key* über mehrere Zeilen der öffentliche Schlüssel als Zeichensalat, der etwa so aussieht: s*sh-rsa aaaAB3NzaC1yc2EaaaABJQ.....tm3J6O0YpQTS74j6i8= rsa-key-20060915*
7. Markieren Sie diesen Zeichensalat mit der Maus und kopieren Sie ihn mit Strg-C in die Zwischenablage
8. Etwas tiefer tippen Sie in die Eingabefelder *Key passphrase* und *Confirm* passphrase ein neues Passwort ein (nicht Ihr Login-Passwort), welches Sie später benötigen werden, um diesen Schlüssel zu benutzen
9. Klicken Sie noch tiefer auf *Save private key* und speichern Sie Ihr Schlüsselpaar damit auf Ihrer Festplatte ab (oder besser einem USB-Stick oder anderen Speichermedium, welches Sie ggf. auch zu anderen Rechnern mitnehmen können)
10. Jetzt können Sie das Fenster *PuTTY Key Generator* schließen.

In der Zwischenablage befindet sich jetzt der öffentliche Schlüssel, der im Webserverpark hinterlegt werden muss. Dabei hilft Ihnen MeinZIV:

1. Starten Sie ein WWW-Programm und gehen Sie zu *MeinZIV* unter der Adresse `https://www.uni-muenster.de/ZIV/MeinZIV/`
2. Melden Sie sich mit Ihrer Nutzerkennung und Ihrem Passwort an
3. Klicken Sie auf der dann erscheinenden Seite in der linken Navigationsspalte auf *Webspacezugang*
4. Markieren Sie auf der dann erscheinenden Seite mit der Maus das zweite Eingabefeld (das erste hinter *SSH-Schlüssel*) und kopieren mit *Rechte Maustaste* | *Einfügen* den Inhalt der Zwischenablage in dieses Eingabefeld
5. Falls Sie mehrere Webspaces verwalten dürfen oder von verschiedenen Rechnern aus Ihren Webspace verwalten möchten, achten Sie bitte darauf, ob die Einstellungen der anderen Eingabefelder richtig sind
6. Klicken Sie auf den Knopf *SSH-Schlüssel hinterlegen*
7. Wenn kein Fehler auftritt, können Sie das WWW-Programm wieder schließen

Falls Sie diesen Zugang auch von anderen Rechnern aus benutzen möchten, müssen Sie entweder den oben abgespeicherten privaten Schlüssel zu den anderen Rechnern mitnehmen oder die ganze Prozedur vom anderen Rechner aus wiederholen. Achten Sie im letztgenannten Fall dann in MeinZIV darauf, dass Sie die vorhandenen Schlüssel ergänzen, nicht ersetzen.

Verbindungsaufbau zum Upload-Server

Die folgenden Schritte müssen Sie während einer Windows-Sitzung nur einmal durchführen und erst nach einer Neuanmeldung wiederholen:

1. Starten Sie den PuTTY-Schlüssel-Agenten *Pageant*: *Start* | *Alle Programme* | *PuTTY* | *Pageant*
2. Es erscheint in der Taskleiste links neben der Uhr ein Computer mit Hut
3. Klicken Sie mit der rechten Maustaste auf dieses Symbol und dann auf *Add Key*
4. Wählen Sie die (bei der Schlüsselerzeugung angelegte) Datei mit Ihrem Schlüsselpaar und klicken Sie auf Öffnen
5. Sie werden nach dem Schlüssel-Passwort gefragt

Bei jedem Verbindungsaufbau sind dann die folgenden Schritte fällig:

1. Starten Sie FileZilla
2. Tippen Sie im Feld *Adresse* bitte ein: *sftp://upload.uni-muenster.de*
3. Tippen Sie im Feld *Benutzer* bitte Ihre Nutzerkennung ein
4. Sie brauchen kein Passwort einzutippen, sondern klicken direkt auf *Verbinden*

Nur beim ersten Verbindungsaufbau erhalten Sie eine Warnung, dass der Host Key des Servers noch unbekannt sei; klicken Sie auf *Ja*, um den Host Key zu speichern und die Verbindung aufzubauen.

Wie Sie sehen, werden Sie jetzt von FileZilla (und genauso von PuTTY) nicht nach einem Passwort gefragt, da FileZilla Sie mit Hilfe des von Pageant vorgehaltenen Schlüsselpaares passwortlos anmelden kann.

Weitere Vereinfachungsmöglichkeiten

Es bietet sich an, das Pageant-Programm in Ihren Autostart-Ordner schieben.

Natürlich können Sie in PuTTY und FileZilla vorbereitete Einstellungen abspeichern, um nicht jedesmal die oben genannte Adresse und Ihre Nutzerkennung neu eintippen zu müssen, beachten Sie bitte dazu die Hilfe-Seiten dieser Programme.

SSH-Zugang zum Webserverpark mit SSH Secure Shell unter Windows

Einmalige Vorbereitung

Um den Zugang zum Webserverpark einzurichten, müssen Sie einmalig die folgenden Schritte durchführen:

1. Starten Sie SSH Secure Shell: *Start* | *Alle Programme* | *SSH Secure Shell* | *Secure Shell Client*
2. Im neuen Fenster - *default* - *SSH Secure Shell* öffnen Sie die Einstellungen: *Edit* | *Settings*
3. Im neuen Fenster *Settings* klicken Sie in der linken Spalte unter *Global Settings* | *User Authentication* auf *Keys*
4. Auf der dargestellten Unterseite *Keys* klicken Sie auf *Generate New...*
5. Im neuen Fenster *Key Generation - Start* klicken Sie auf *Weiter* >

6. Im Fenster *Key Generation - Key Properties* behalten Sie die Voreinstellungen bei und klicken Sie auf *Weiter >*
7. Im Fenster *Key Generation - Generation* warten Sie die Schlüsselgenerierung ab und klicken Sie danach auf *Weiter >*
8. Im Fenster *Key Generation - Enter Passphrase* tippen Sie in das Eingabefeld *File Name* bitte einen sinnvollen Dateinamen an, z. B. *MeinKey*
9. Das Eingabefeld *Comment* können Sie ausfüllen oder auch nicht
10. Tippen Sie in beide Eingabefelder *Passphrase* ein neues Passwort ein (nicht Ihr Login-Passwort), welches Sie später benötigen werden, um diesen Schlüssel zu benutzen
11. Auf der Seite *Key Generation - Finish* benutzen Sie nicht den Knopf *Upload Public key*, sondern klicken Sie direkt auf *Fertig stellen*
12. Zurück auf der Unterseite *Keys* des *Fensters Settings* klicken Sie in der Liste der Schlüssel unter *Private Key file name* auf den oben angegebenen Dateinamen *MeinKey* und dann auf *Export...*
13. Im neuen Fenster *Select Folder* wählen Sie im oberen kleinen Eingabefeld den Ordner *Eigene Dateien* und klicken dann auf *Speichern*
14. Ignorieren Sie eventuell erscheinende Fehlermeldungen, indem Sie jeweils auf *OK* klicken
15. Schließen Sie das Fenster *Settings*, indem Sie auf *OK* klicken
16. Schließen Sie das Fenster - *default* - SSH Secure Shell*
17. Bestätigen Sie im Rückfragefenster *Confirm File Save* mit Klick auf *Yes*

Unter Eigene Dateien sollte jetzt eine Datei mit dem oben angegebenen Namen *MeinKey.pub* von etwa 2 KB Größe liegen. Diese enthält den öffentlichen Schlüssel, der im Webserverpark hinterlegt werden muss. Dabei hilft Ihnen MeinZIV:

1. Starten Sie ein WWW-Programm und gehen Sie zu *MeinZIV* unter der Adresse `https://www.uni-muenster.de/ZIV/MeinZIV/`
2. Melden Sie sich mit Ihrer Nutzerkennung und Ihrem Passwort an
3. Klicken Sie auf der dann erscheinenden Seite in der linken Navigationsspalte auf *Webspacezugang*
4. Wählen Sie mit dem dritten Eingabefeld (dem zweiten hinter *SSH-Schlüssel*) die oben unter *Eigene Dateien* abgelegte Datei *MeinKey.pub* aus
5. Falls Sie mehrere Webspaces verwalten dürfen oder von verschiedenen Rechnern aus Ihren Webspace verwalten möchten, achten Sie bitte darauf, ob die Einstellungen der anderen Eingabefelder richtig sind
6. Klicken Sie auf den Knopf *SSH-Schlüssel hinterlegen*
7. Wenn kein Fehler auftritt, können Sie das WWW-Programm wieder schließen

Falls Sie diesen Zugang auch von anderen Rechnern aus benutzen möchten, müssen Sie entweder den oben erzeugten privaten Schlüssel exportieren, zu den anderen Rechnern mitnehmen und dort wieder importieren oder die ganze Prozedur vom anderen Rechner aus wiederholen. Achten Sie im letztgenannten Fall dann in MeinZIV darauf, dass Sie die vorhandenen Schlüssel ergänzen, nicht ersetzen.

Verbindungsaufbau zum Upload-Server

SSH-Secure-Shell-Nutzern steht kein Agent zur Verfügung, der einem das wiederholte Eintippen des Schlüssel-Passworts erspart. Bei jedem Verbindungsaufbau sind die folgenden Schritte fällig:

1. Starten Sie *Secure Shell Client* oder *Secure File Transfer Client*
2. Klicken Sie bitte auf *Quick Connect*
3. Es erscheint ein Fenster *Connect to Remote Host*
4. Tippen Sie im Feld *Host Name* bitte ein: *upload.uni-muenster.de*
5. Tippen Sie im Feld *User Name* bitte Ihre Nutzerkennung ein
6. Belassen Sie das Feld *Port Number* bitte auf 22
7. Wählen Sie im Feld *Authentication Method* bitte Public Key aus
8. Klicken Sie bitte auf *Connect*
9. Im Fenster *Enter Passphrase for Private Key* tippen Sie bitte im Feld *Passphrase* Ihr Schlüssel-Passwort (nicht das Login-Passwort) ein und drücken die Eingabe-Taste oder klicken auf *OK*.

Nur beim ersten Verbindungsaufbau erhalten Sie ein Warnfenster *Host Identification*, weil der *host public key* noch unbekannt ist; klicken Sie auf *Yes*, um den Host Key zu speichern und die Verbindung aufzubauen.

Weitere Vereinfachungsmöglichkeiten

Natürlich können Sie mit SSH Secure Shell vorbereitete Einstellungen (Profile) abspeichern, um nicht jedesmal Rechnername, Nutzerkennung und Authentifizierungsmethode neu angeben zu müssen (das wird Ihnen sogar nach jedem *Quick Connect* direkt angeboten), beachten Sie bitte dazu die Hilfe-Seiten dieser Programme.

SSH-Zugang zum Webserverpark mit SSH und SCP unter Linux

Einmalige Vorbereitung

Um den Zugang zum Webserverpark einzurichten, müssen Sie einmalig die folgenden Schritte durchführen (statt eines *rsa*-Schlüssels wie nachfolgend beschrieben können Sie gerne auch einen *dsa*-Schlüssel erzeugen):

1. Rufen Sie auf: *ssh-keygen -t rsa*
2. Bei der Frage *Enter file in which to save the key (...)* drücken Sie nur die Eingabetaste, um den in Klammern vorgeschlagenen Dateinamen zu übernehmen (meist *.ssh/id_rsa.pub* im eigenen Homeverzeichnis; dann brauchen Sie später beim *ssh-add* den Dateinamen auch nicht anzugeben)
3. Bei der Frage *Enter passphrase* tippen Sie ein neues Passwort ein (nicht Ihr Login-Passwort), welches Sie später benötigen werden, um diesen Schlüssel zu benutzen
4. Bei der Frage *Enter same passphrase again* tippen Sie das gleiche Passwort noch einmal ein

Die Datei *.ssh/id_rsa.pub* im eigenen Homeverzeichnis sollte jetzt etwas über 200 Byte groß sein und enthält den öffentlichen Schlüssel, der im Webserverpark hinterlegt werden muss. Dabei hilft Ihnen MeinZIV:

1. Starten Sie ein WWW-Programm und gehen Sie zu *MeinZIV* unter der Adresse `https://www.uni-muenster.de/ZIV/MeinZIV/`
2. Melden Sie sich mit Ihrer Nutzerkennung und Ihrem Passwort an
3. Klicken Sie auf der dann erscheinenden Seite in der linken Navigationsspalte auf *Webspacezugang*
4. Wählen mit dem dritten Eingabefeld (dem zweiten hinter *SSH-Schlüssel*) die oben angelegte Datei *.ssh/id_rsa.pub* aus

5. Falls Sie mehrere Webspaces verwalten dürfen oder von verschiedenen Rechnern aus Ihren Webspace verwalten möchten, achten Sie bitte darauf, ob die Einstellungen der anderen Eingabefelder richtig sind
6. Klicken Sie auf den Knopf *SSH-Schlüssel hinterlegen*
7. Wenn kein Fehler auftritt, können Sie das WWW-Programm wieder schließen

Falls Sie diesen Zugang auch von anderen Rechnern aus benutzen möchten, müssen Sie entweder die Dateien *.ssh/id_rsa* und *.ssh/id_rsa.pub* zu den anderen Rechnern mitnehmen oder die ganze Prozedur vom anderen Rechner aus wiederholen. Achten Sie im letztgenannten Fall dann in MeinZIV darauf, dass Sie die vorhandenen Schlüssel ergänzen, nicht ersetzen.

Verbindungsaufbau zum Upload-Server

Von vielen Linux-Installationen werden beim Login eines Nutzers bereits automatisch das Programm *ssh-agent* gestartet und notwendigen Umgebungsvariablen gesetzt.

(Falls nicht, kann der Befehl *ssh-agent* auch in einem Terminal-Fenster eingetippt werden. Dabei werden zwei Zeilen *SSH_AUTH_SOCK=...* und *SSH_AGENT_PID=...* ausgegeben. Diese sind in jedem Terminalfenster auszuführen, in dem später *ssh-add*, *ssh* oder *scp* aufgerufen werden sollen, um die nötigen Umgebungsvariablen zu setzen. Oder man startet den Agenten mit *eval $(ssh-agent)*, wenn man nur im gleichen Fenster *ssh-add*, *ssh* und *scp* benutzen möchte.)

Nur einmal pro Sitzung ist dann der Befehl *ssh-add* aufzurufen, dieser fragt nach dem Schlüssel-Passwort.

Anschließend kann dann beliebig oft *scp* oder *ssh Nutzerkennung@upload.uni-muenster.de* aufgerufen werden, ohne dass nach einem Passwort gefragt wird.

Nur beim ersten Verbindungsaufbau erhalten Sie eine Warnung, dass der Host Key des Servers noch unbekannt sei; tippen Sie das komplette Wort *yes* ein, um den *Host Key* zu speichern und die Verbindung aufzubauen.

Zahlenrätsel – Schlittenfahrt durch die Zeit

Olaf Teschke

Dieses „infoforum-Quiz“ drucken wir mit freundlicher Genehmigung des Matheon Berlin nach.

Es war das Rätsel vom 24. Türchen des Mathekalenders, der viele in der letzten Adventszeit erfreut hat.

Vielleicht kennen Sie die Mathematik, vielleicht bemühen Sie eine Suchmaschine. Die Auflösung finden Sie im nächsten infoforum oder bei `http://www.mathekalender.de`.

Der Weihnachtsmann – dessen Schlitten sich bekanntlich auch in der Zeit bewegen kann, damit er überall pünktlich ist – soll sechs verschiedenen Mathematiker(inne)n in unterschiedlichen Jahren Weihnachtsgeschenke bringen. Leider ist der Weihnachtsmann etwas zerstreut und hat die genauen Auslieferungsjahre vergessen. Auf seinem Notizblock steht nur noch eine Prüfsumme, die aus der Summe der Quadrate der Jahreszahlen besteht, deren letzte Ziffer aber durch eine dicke Schneeflocke verwischt ist.

Zum Glück erinnert sich der Weihnachtsmann noch an einige Details. So sind fünf der Jahreszahlen Primzahlen; außerdem weiß er noch einiges aus dem Leben der Beschenkten:

Der erste Mathematiker passte im Laufe von (manchmal erzwungenen) Wohnsitzwechseln mehrfach seinen Namen dem Aufenthaltsort an. Er war auf einer Reihe von Gebieten der Mathematik tätig, von den Grundlagen bis hin zu weitreichenden Anwendungen. Leider zeitigten diese einige Nebenwirkungen – ein von ihm entworfenes Computermodell macht Viren ihre Tätigkeit besonders leicht, und er erkrankte später schwer an den Folgen von Experimenten mit seiner durchschlagendsten Anwendung. Das machte ihn freilich posthum zum Star – er war das Vorbild für den Titelhelden eines bekannten Films. Der Weihnachtsmann bringt ihm ein Geschenk in dem Jahr, in dem seine Arbeiten zu logischen Grundlagen der Mathematik und zur Mathematisierung der Quantenmechanik veröffentlicht werden.

Die Zweite lernte Mathematik neben vielen anderen Dingen von ihrem Vater, den sie bald übertraf – vielen galt sie als die umfassendste Wissenschaftlerin ihrer Zeit, die auch

in der Philosophie, Literatur und Astronomie glänzte. In ihrer Heimatstadt wurde ihr ein Lehrstuhl für Philosophie an einer der berühmtesten Universitäten der Epoche eingeräumt. Ob sie auch an der anderen Elite-Uni jener Zeit gelehrt hat, ist nicht ausreichend belegt; doch ist sie wahrscheinlich in einem späteren berühmten Renaissancegemälde dieser Bildungsstätte als einzige Frau verewigt worden. Leider nahm sie ein tragisches Ende – Anhänger eines radikalen Erzbischofs nahmen Anstoß an ihr und ermordeten sie auf grausame Weise. Der Erzbischof wurde später von der katholischen Kirche heiliggesprochen. Der Weihnachtsmann bringt ihr ein Geschenk sechs Jahre vor ihrem Tod.

Der Dritte konstruierte in seiner Jugend ein wunderschönes (leider sehr ungenaues) Modell des Planetensystems, indem er die Umlaufbahnen der damals bekannten fünf Planeten zu den fünf platonischen Körpern in Beziehung setzte. Noch bevor die Entdeckung eines weiteren Planeten dieses harmonische Bild zerstören konnte, fand er allerdings eine wesentlich bessere Beschreibung. Eine vom ihm gestellte Frage wurde erst Jahrhunderte später beantwortet und löste unter Mathematikern einen tiefen Zwist darüber aus, was man unter einem Beweis versteht. Sein Werk über die Entstehung der Schneeflocke wird dagegen einhellig von allen Weihnachtselfen gelobt. Obwohl er riesige astronomische Berechnungen vollbrachte und äußerst genaue Planetentafeln für die Schifffahrt aufstellte, verdankte er den größten Teil seines Lebensunterhalts der angewandten Astronomie (im Sinne jener Zeit), nämlich der Erstellung von Horoskopen. Durch diese Tätigkeit erlangte er die Protektion der Mächtigen, konnte aber nicht verhindern, dass seine Mutter als Hexe angeklagt und gefoltert wurde. Der Weihnachtsmann bringt ihm ein Geschenk in seinem Geburtsjahr – mit drei Tagen Verspätung.

Der Vierte war sehr vielseitig – neben seiner mathematischen Tätigkeit war er u. a. auch Philosoph, Redakteur, Profisportler und Landwirt. Mit seinem Bruder zusammen verfasste er auch ein Theaterstück, das allerdings nicht sehr erfolgreich war – die eigentliche literarische Berühmtheit der Familie war die erste Frau seines Bruders, die auch heute noch als herausragende Lyrikerin verehrt wird. In der Mathematik bewies er fundamentale Sätze in der Algebra – einer davon wurde zumindest teilweise nach ihm benannt, andere tragen fremde Namen. Als Außenseiter in der Wissenschaft blieb ihm trotz seiner Leistungen eine Professur verwehrt. So musste er sein Geld vor allem als (Denk-) Sportler verdienen, wobei er es bis zum Weltmeister brachte. Der Weihnachtsmann bringt ihm ein Geschenk in dem Jahr, in dem er an der Universität Erlangen in Mathematik promovierte.

Der Fünfte hatte dieselbe Nationalität wie der erste und übertraf ihn sogar in seiner Reiselust, hatte allerdings eine deutliche Abneigung gegen dessen explosive Experimente. Berühmt ist er für die Vielzahl und Bandbreite seiner Veröffentlichungen, die oft mit Koautoren entstanden. Dies führte auch zur Definition einer berühmten nach ihm benannten Zahl. Bekannt ist auch seine Exzentrizität und Drogensucht – aufgrund einer Wette setzte er zwar einmal seinen Konsum aus, beklagte aber den dadurch entstandenen Schaden an der Mathematik. Seine Vorstellung eines göttlichen Buches der Beweise führte später zu einem mathematischen Bestseller – was ihn angesichts seiner völligen materiellen Bedürfnislosigkeit kaum gerührt hätte. Auch den Cole- Preis der American Mathematical Society, den ihm Weihnachtsmann brachte, stiftete er anderen.

Nummer sechs zeigte schon früh seine mathematische Begabung, ebenso wie seine Liebe zur Musik und für ausgedehnte Wanderungen. Nachdem er einige Jahre in gutbezahlten Positionen im Ausland tätig war, meinte er genügend Geld zu haben, um für den Rest seines Lebens in Ruhe unabhängig Mathematik treiben zu können. Er kehrte nach Hause zurück, wo er sehr zurückgezogen über eine Theorie nachdachte, mit der unter anderem ein berühmtes Jahrhundertproblem bewiesen werden konnte. Seinen Beweis dazu publizierte er im Internet, lehnte es aber ab, einen Preis für seine Leistung entgegenzunehmen – er wolle nicht Galionsfigur einer mathematischen Gemeinschaft werden, der er sich nicht mehr zugehörig fühle. Der Weihnachtsmann bringt ihm sein Geschenk in dem Jahr, in dem er die Publikation seines Beweises im Internet abschloss.

Mögliche Antworten:

Die Zahl auf dem Notizblock lautet:

1. 17792490
2. 17792491
3. 17792492
4. 17792493
5. 17792494
6. 17792495
7. 17792496
8. 17792497
9. 17792498
10. 17792499

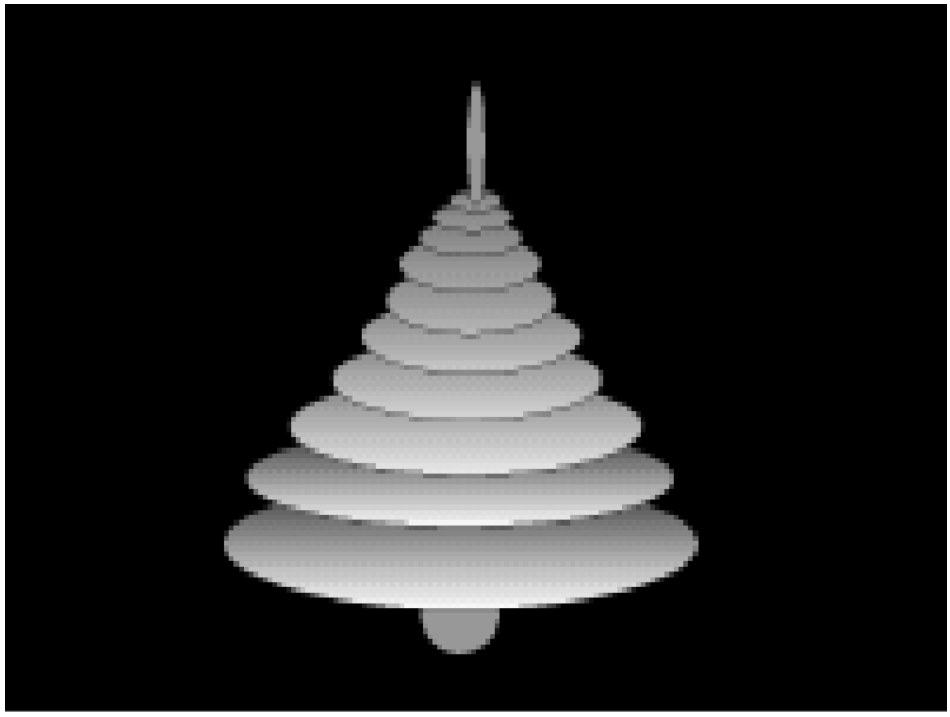
Hinweise der inforum-Redaktion: Diese Aufgabe lässt sich auf bemerkenswert viele Weisen lösen:

- Sie können nach Mathematikern suchen, müssen die gefundenen Jahreszahlen aber noch hinterfragen.
- Sie können, wenn Sie manche Jahreszahlen ausschließen, das Problem rein mathematisch lösen.
- Sie können ein „Brute Force"-Programm schreiben, müssen aber auch hier noch Jahreszahlen ausschließen. (Wenn Ihres kurz und übersichtlich ist, könnte man es auch im inforum veröffentlichen.)
- Wenn Sie besonders wenig Zeit haben, genügt es, nur die Jahreszahl des vierten Mathematikers zu kennen, dann reichen eine Multiplikation, eine Subtraktion und eine Division mit Rest zur Ermittlung der Lösung. Aber auch hier müssen Sie eine Jahreszahl ausschließen.

Lösung inforum-Quiz Nr. 3/2006

E. Sturm

Bei Stereogrammen wird immer ein Musterbild gemäß einem Grauwertbild so modifiziert, dass das Auge, besser: die Augen ein räumliches Gebilde zu erkennen glauben. Vom letzten inforum-Quiz brauche ich das Musterbild, glaube ich, nicht abzudrucken, es besteht ja nur aus zufällig angeordneten Punkten. Das Grauwertbild war das folgende:



Die Umrechnung erfolgt nun so, dass die Punkte dort mehr verschoben werden, wo das Grauwertbild heller ist. Bei Schwarz wird nicht verschoben. Mit etwas gutem Willen erkennt man das Tänn-schen, das der Sachse in New York kaufen wollte, als er „Attention, please!“ sagte.

ZIV-Lehre

Veranstaltungen in der Vorlesungszeit (Sommersemester 2007)
für Hörer aller Fachbereiche

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11–12,
✆ 83-3 15 61

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse `http://www.uni-muenster.de/ZIV/Zivlehre.html` erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind möglich ab 1. März 2007. Weitere Informationen unter `http://www.uni-muenster.de/ZIV/Lehre/`.

260011 **Programmieren in Perl** — Küfer, Th.
Dienstag 14-16 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60,
Beginn: 17.04.2007

260026 **Einführung in MySQL** — Leweling, M.
Donnerstag 9-11 Uhr
Hörsaal: ZIV-Pool 3, Einsteinstr. 60,
Beginn: 05.04.2007

260030 **Dynamische Webseiten mit PHP für Fortgeschrittene** — Sturm, E.
Mittwoch 10-12 Uhr
Hörsaal: M4, Einsteinstr. 64,
Beginn: 11.04.2007

260045 **Kommunikationssysteme:** — Richter, G.
IT-Sicherheit und Überwachung von IT-Infrastruktur — Forsmann, A.
Donnerstag 14-16 Uhr — Kamp, M.
Hörsaal: Raum 206, Röntgenstr. 9-13 — Speer, M.
Beginn: 12.04.2007 — Wessendorf, G.

260050 **Kolloquium des Zentrums für Informationsverarbeitung** — Held, W.
Freitag 14-16 Uhr
Hörsaal: Raum 206, Röntgenstr. 9-13

Kommentare zu den Veranstaltungen

260011 **Programmieren in Perl**

Perl, die Practical Extraction and Report Language, ist eine Skript-Sprache, die sich besonders gut zur Lösung der tagtäglichen Probleme eignet, mit denen sich System-Administratoren und Anwendungsentwickler auseinandersetzen müssen.

Perl ist ursprünglich eine Sprache zur komfortablen Bearbeitung von Texten und Dateien und verfügt daher über einen besonders mächtigen Satz von regulären Ausdrücken zum Auffinden und Modifizieren von Textstellen. Darüber hinaus sind CGI-Skripte für Web-Server häufig in Perl implementiert.

Perl gibt es für die verschiedenen Unix-Derivate, für Windows, für Macintosh, für OS/2 und sogar für VMS. Über das Internet organisiert, gibt es eine Bibliothek von frei verfügbaren Perl-Modulen, die Lösungen für Standardprobleme anbietet (CPAN, Comprehensive Perl Archive Network).

Diese Vorlesung führt in das Programmieren mit Perl ein und beschäftigt sich demnach mit den grundlegenden Eigenschaften der Sprache: Syntax, Datentypen, Anweisungen und Funktionen. Weitere Schwerpunkte sind die Behandlung der regulären Ausdrücke, die Benutzung der Perl-Module (z. B. CGI und DBI) und die objektorientierte Programmierung mit Perl. Zum Abschluss wird auch die Programmierung von grafischen Oberflächen mit Perl erklärt.

An Voraussetzungen sollten Sie die Dateistruktur Ihres Unix- oder Windows-Systems kennen, einen Editor bedienen und einen Web-Browser benutzen können. Programmierkenntnisse, vorzugsweise in C oder einer anderen Skriptsprache, werden nicht vorausgesetzt, schaden aber keinesfalls.

Gedacht ist die Vorlesung für diejenigen, die bestimmte Vorgänge automatisieren möchten und erfahren haben, dass man nicht jedes Problem idealerweise durch „Anklicken“ löst.

260026 Einführung in MySQL

MySQL ist das am weitesten verbreitete Datenbanksystem in der Open-Source-Szene. Die Kombination aus Linux als Betriebssystem, Apache als Webserver, MySQL als Datenbanksystem und Perl/PHP/Python als Skriptsprachen hat sich mittlerweile unter dem Akronym „LAMP“ als kostengünstige Gesamtlösung bei der Erstellung dynamischer Websites etabliert.

Der Schwerpunkt der Vorlesung besteht aus einer Einführung in die Datenbanksprache SQL. Mit SQL-Anweisungen werden etwa Datenbankobjekte verwaltet, Daten und Tabellen gespeichert und abgefragt, sowie Zugriffsrechte vergeben. Einfache Abfragen in Perl sowie die Vorstellung der Administrationsoberfläche phpMyAdmin sind ebenfalls Bestandteil der Vorlesung.

260030 Dynamische Webseiten mit PHP für Fortgeschrittene

Diese Veranstaltung ist die Fortsetzung der Lehrveranstaltung „Erstellen von dynamischen Webseiten mit PHP“. Kenntnisse von HTML und CSS sowie Grundkenntnisse von PHP werden vorausgesetzt.

Großen Raum wird die Vorstellung der Datenbank MySQL einnehmen. Weitere Themen sind Sitzungsverwaltung, Rollenmanagement, Up- und Download, E-Mail sowie die Nutzung von XML. Besprochen werden sollen auch JavaScript und Ajax.

260045 Kommunikationssysteme: IT-Sicherheit und Überwachung von IT-Infrastruktur

In der Veranstaltung sollen zwei ausgewählte Themen aus dem Bereich „Informationstechnologie“ vertieft behandelt werden.

IT-Sicherheit

Es sollen hierbei zum einen die in ein Netzwerk integrierten Sicherheitsfunktionen erläutert werden. Aber auch die auf den Endsystemen (Server, Arbeitsplatzrechner) realisier-

baren Sicherheitsfunktionen sollen im Zusammenhang vorgestellt werden. Stichwortliste:

- Firewalls
- Packet Screening
- Intrusion Detection / Prevention
- Strukturierung von Netzen
- Virtualisierung von Netzen
- IPsec – Internet Protocol Security
- VPN – Virtuelle Private Netze
- Authentifizierter Netzzugang
- Endsystemsicherheit
- Security-Auditing

Überwachung von IT-Infrastruktur

Gemeint ist hier die Überwachung (engl. „Monitoring“) von Netzwerken mit dem Ziel, einen möglichst störungsfreien Betrieb für die Nutzer der Netzwerkinfrastruktur zu gewährleisten. Es sollen hierbei die technologischen Grundlagen, die angewandten Methoden und ausgewählte Tools vorgestellt werden. Stichwortliste:

- Netzwerkmanagement
- SNMP – Simple Network Management Protocol
- MIB – Management Information Base
- Überwachung verschiedener Netzfunktionen: Erreichbarkeit von Systemen, Leitungszustände, Überwachung von Netzdiensten wie z. B. DNS
- Event-Verarbeitung
- Visualisierung von Netzwerken

260050 Kolloquium des Zentrums für Informationsverarbeitung

Im Rahmen des Kolloquiums werden Vorträge über aktuelle Themen der Informationsverarbeitung gehalten. Vortragstermine werden im WWW und durch Aushang bekanntgegeben.

ZIV-Regularia

Fingerprints

R. Perske

Diese regelmäßig hier veröffentlichten kryptographischen Prüfsummen benötigen Sie, um die Echtheit der Schlüssel und Zertifikate der Zertifizierungsstelle der Universität Münster (WWUCA) und der obersten Zertifizierungsinstanz im Deutschen Forschungsnetz (DFN-PCA) zu kontrollieren. Weitere Infos unter `http://www.uni-muenster.de/WWUCA/`.

```
X.509-Wurzelzertifikate der DFN-PKI bzw. DFN-PCA:

* C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Classic - G01
  MD5-Fingerprint:  EF:08:E6:9F:6A:C7:25:2C:58:8C:55:FD:45:13:31:0A
  SHA1-Fingerprint: 12:63:41:60:D0:8C:FE:6A:87:6D:F7:86:D3:AD:C2:F7:74:FF:21:9F

* C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Basic - G01
  MD5-Fingerprint:  76:95:48:F0:40:72:3C:2B:A6:A1:A1:FD:CC:AF:7F:F4
  SHA1-Fingerprint: 35:5E:69:67:8E:B5:D7:2B:5D:C8:82:27:68:47:F2:7C:0D:3C:41:56

* C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Grid - G01
  MD5-Fingerprint:  41:39:4A:58:2E:F0:45:B2:29:28:F1:72:AB:F7:05:08
  SHA1-Fingerprint: 1C:BB:D4:BA:97:7B:3A:B9:FF:CD:4A:97:77:50:87:9C:6A:2E:8E:38

* C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
    CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
  MD5-Fingerprint:  3e:1f:9e:e6:4c:6e:f0:22:08:25:da:91:23:08:05:03
  SHA1-Fingerprint: 8e:24:22:c6:7e:6c:86:c8:90:dd:f6:9d:f5:a1:dd:11:c4:c5:ea:81

* C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA,
    CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
  MD5-Fingerprint:  45:bb:9b:c8:8a:a4:84:8b:2d:a0:08:8f:9e:b6:b8:10
  SHA1-Fingerprint: df:a5:6f:b5:fc:41:e3:a8:92:1f:77:ad:16:22:ee:fd:91:52:a5:ad


X.509-Zertifikate der WWUCA:

* C=DE, O=Universitaet Muenster, CN=Zertifizierungsstelle Universitaet Muenster
    (Classic) 2006-2007/emailAddress=ca@uni-muenster.de
  MD5-Fingerprint:  23:AD:54:AE:57:68:30:76:33:74:06:49:08:29:89:37
  SHA1-Fingerprint: 14:3E:72:75:1A:E1:68:9C:73:18:3A:0A:EE:71:F8:CB:A1:BE:3D:A6

* C=DE, O=Universitaet Muenster, CN=Zertifizierungsstelle 2004-2005/Email=ca@uni-muenster.de
  MD5-Fingerprint:  26:19:6b:ef:66:b2:70:44:52:cc:be:11:4c:5f:3c:b8
  SHA1-Fingerprint: 17:65:ae:6d:57:c7:79:14:d2:af:ba:f3:43:9c:e1:39:66:e1:a0:ae

* C=DE, O=Universitaet Muenster, CN=Zertifizierungsstelle 2002-2003/Email=ca@uni-muenster.de
  MD5-Fingerprint:  a4:31:ad:41:d8:f2:18:56:4e:31:cc:69:71:e6:17:4f
  SHA1-Fingerprint: 69:45:20:ca:1a:fe:5c:fa:6c:37:52:eb:b7:72:b0:54:90:ec:d9:79

* C=DE, O=Universitaet Muenster, CN=Zertifizierungsstelle 2000-2001/Email=ca@uni-muenster.de
  MD5-Fingerprint:  da:e3:e2:5d:bc:93:ef:03:37:96:4e:25:c1:ab:2b:d1
  SHA1-Fingerprint: a7:64:55:75:e0:ad:9a:2c:0c:b4:c8:ed:be:e0:bf:d4:72:6c:5c:b2


PGP-Wurzelzertifizierungsschlüssel der DFN-PCA:

* DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2006-2007) <http://www.pca.dfn.de/>
  D24D8B7F/2048 2005-12-15 Fingerprint: 4E8D 42A8 25C4 66F7 02E8 11EB D259 3AEF

* DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005) <http://www.dfn-pca.de/>
  FDCB1C33/2048 2003-10-26 Fingerprint: 96B0 AD7F B8DC 0018 DCA0 7053 1C3B 4DA5

* DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003) <http://www.dfn-pca.de/>
  F2D58DB1/2048 2001-11-20 Fingerprint: DE31 690D BC6A E779 4DCD A1B5 8180 FE7B

* DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001) <not-for-mail>
  63EB5391/2048 2000-12-28 Fingerprint: CFAF 6C29 4E57 4E0E E81C BDB4 54FD 2AAB

* DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1999-2000) <not-for-mail>
  F7E87B9D/2048 1998-12-29 Fingerprint: 6570 7274 B5E0 3FF0 EA7C ABE4 465F B8B2

* DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1997-1998) <not-for-mail>
  35DBF565/2048 1997-04-16 Fingerprint: 097C 0919 D3C3 86DC 7A30 1511 1295 8DE3


PGP-Zertifizierungsschlüssel der WWUCA:

* Zertifizierungsstelle Universitaet Muenster 2006-2007
  31027DB5/2048 2005-10-11 Fingerprint: A57B 0407 1F91 9CB9 3771 3736 E195 6C62

* Zertifizierungsstelle Universitaet Muenster 2004-2005
  38B7A481/2048 2003-11-03 Fingerprint: 973E 0725 040B 1745 F272 180D 08C2 C15A

* Zertifizierungsstelle Universitaet Muenster 2002-2003
  BC811EB1/2048 2001-11-14 Fingerprint: 2864 01BC F0EF D5BA D9A0 866C 4379 4C1D

* Zertifizierungsstelle Universitaet Muenster 2000-2001
  313C02F5/2048 2000-03-24 Fingerprint: 3762 F5E0 C278 7697 530F 2DF2 F3B3 27F5

* Rainer Perske +49(251)83-31582 Certification Key
  EF750F1D/2048 1997-10-14 Fingerprint: 2F38 6EF8 DC2E D85E 5B35 DB49 8AE4 52AF


PGP-Kommunikationsschlüssel für verschlüsselte E-Mails an die DFN-PCA:

* DFN-PCA (2006), ENCRYPTION Key <dfnpca@dfn-pca.de>
  E0F94D51/2048 2005-12-14 Fingerprint: 2B33 4369 1D38 036D 7FFA 659E 2524 DBB2


PGP-Kommunikationsschlüssel für verschlüsselte E-Mails an die WWUCA:

* Zertifizierungsstelle Universitaet Muenster (E-Mail) <ca@uni-muenster.de>
  4CB7658D/2048 2000-07-06 Fingerprint: 383D 0F16 CEFC 1F9E B7C3 04B1 2020 FCE6
```

infoforum Februar 2007

Liebe Leserin, lieber Leser,

wenn Sie **infoforum** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **infoforum** nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.

Bitte haben Sie Verständnis dafür, dass ein Versand außerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.

Vielen Dank!

Redaktion **infoforum**

☐ Ich bitte um Aufnahme in den Verteiler.

☐ Bitte streichen Sie mich/den nachfolgenden Bezieher aus dem Verteiler.

☐ Mir reicht ein Hinweis per E-Mail nach dem Erscheinen einer neuen WWW-Ausgabe.
Meine E-Mail-Adresse:

_____

An die
Redaktion **infoforum**
Zentrum für Informationsverarbeitung
Röntgenstr. 9–13
48149 Münster

☐ Meine Anschrift hat sich geändert.
Alte Anschrift:

_____

_____

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

Uni-Nutzerkennung: _____

E-Mail: _____

Außerhalb der Universität:

_____

(Bitte deutlich lesbar in Druckschrift ausfüllen!)

Ich bin damit einverstanden, dass diese Angaben in der **infoforum**-Leserdatei gespeichert werden (§ 4 DSG NW).

_____ _____

Ort, Datum Unterschrift