

# inforum

---

Zentrum für Informationsverarbeitung der Universität Münster  
Jahrgang 30, Nr. 1 – April 2006 ISSN 0931-4008

---

## Inhalt

Editorial.....	2
<b>ZIV-Aktuell</b> .....	<b>3</b>
It's TIME again .....	3
„mein ZIV“ – Ihr Portal für ZIV-Dienste .....	7
„wwu@home“-Einwahl: Verfügbarkeit in den Region-50-Bereichen erweitert.....	8
Netzseitige IT-Sicherheitsmaßnahmen des ZIV 2006.....	9
VPN-Service des ZIV.....	12
Stateful-Firewall-Service des ZIV.....	13
Erheblich verbesserte SPAM-Erkennung in der Erprobung.....	15
Tabellenloses Layout unter Imperia.....	15
Neues von der Zertifizierungsstelle.....	16
<b>ZIV-Präsentation</b> .....	<b>18</b>
Energiesparen leicht gemacht .....	18
Professionelles Systemmanagement mit SMS an der WWU .....	21
HIPEC II .....	24
Zahlenrätsel.....	27
Ostereier.....	28
<b>ZIV-Lehre</b> .....	<b>30</b>
Veranstaltungen in der Vorlesungszeit (Sommersemester 2006).....	30
Veranstaltungen in der vorlesungsfreien Zeit (August–Oktober 2006).....	31
Kommentare zu den Veranstaltungen.....	32
<b>ZIV-Regularia</b> .....	<b>38</b>
Fingerprints.....	38



## Impressum

**inforum**  
ISSN 0931-4008

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

E-Mail: [ziv@uni-muenster.de](mailto:ziv@uni-muenster.de)  
WWW: <http://www.uni-muenster.de/ZIV/>  
Redaktion: E. Sturm ☎ 83-31679, ✉ [sturm@uni-muenster.de](mailto:sturm@uni-muenster.de)  
Satz: B. Schultze  
Satzsystem: StarOffice 8  
Druck: UniPrint

Auflage dieser Ausgabe: 1400

## Editorial

*E. Sturm*



Auch in diesem **inforum** finden Sie wieder mehrere Artikel, die nicht aus der Feder eines ZIV-Mitarbeiters stammen. Zum einen haben wir Artikel aus Zeitschriften anderer Universitätsrechenzentren abdrucken dürfen und zum anderen ist wieder ein Erfahrungsbericht aus dem Institut für Rechtswissenschaft dabei.

Dies sind keine Einzelfälle, und so möchte ich Sie ermutigen, ebenfalls einen Artikel im **inforum** zu veröffentlichen. Bedenken Sie, dass Sie mit dem **inforum** sowohl zahlreiche interessierte Studierende als auch über 800 Abonnenten erreichen, die an der Informationsverarbeitung besonders interessiert, wenn nicht sogar Fachleute sind, davon etwa 100 außerhalb Münsters. Mein Lieblingswunsch wäre ein Artikel etwa eines Koreaners über die Benutzung von perMail mit einer nicht-lateinischen Schrift. (Mich faszinieren einfach diese Schriften.)

Auch Leserbriefe sind natürlich jederzeit willkommen.

Wenn Sie sich fragen, wo denn diesmal das allgegenwärtige Thema „Sicherheit der Informationsverarbeitung“ bleibt, auch da bieten wir wieder mehrere Artikel. Die allerneuesten Entwicklungen konnten wir aber noch nicht berücksichtigen: „root kits“ als Basis für Viren sind nämlich bald schon „out“. Diese benutzen ja Funktionen des Betriebssystems, um sich etwa vor das dir-Kommando zu hängen, sodass die Virus-Dateien gar nicht mehr aufgelistet werden.

Es geht aber noch tiefer: Wenn ein Virus (oder Wurm oder was auch immer) eine virtuelle Maschine installiert, sodass beim nächsten Neustart alles, was Windows macht, von der virtuellen Virus-Maschine kontrolliert wird, hat man wohl keine Chance mehr. Man merkt es allenfalls noch daran, dass manche Programme etwas langsamer laufen.

Es bleibt weiterhin nur, das Einnisten von Viren zu verhindern. Als neue Möglichkeit fällt mir da ein: Am besten nimmt man mit dem Internet nur noch Kontakt auf, indem man eine spezielle virtuelle Maschine benutzt, die man bei Virenbefall einfach durch eine frische Version ersetzt.

## ZIV-Aktuell

### It's TIME again

*Die informations- und kommunikationstechnische Infrastruktur und ihre mittelfristige Entwicklung an den Hochschulen des Landes NRW*

*Christian Bischof (Aachen), Waldemar Brett (Düsseldorf), Wilhelm Held (Münster), Ulrich Lang (Köln), Bruno Lix (Essen), Gudrun Oevel (Paderborn), Harald Ziegler (Dortmund)*

**Der Arbeitskreis der Leiter wissenschaftlicher Rechenzentren in Nordrhein-Westfalen (ARNW) hat die Stellungnahme TIME zu aktuellen Entwicklungsfragen der Kommunikations-, Informations- und Medientechnik (KIM) verabschiedet. Hier wird nur ein Extrakt mit den wichtigsten Empfehlungen nachgedruckt. Die vollständige Ausarbeitung finden Sie unter [www.arnw.de/docs/TIME\\_II/index.html](http://www.arnw.de/docs/TIME_II/index.html).**

Oberstes Ziel der Hochschulen ist die Aufrechterhaltung der Qualität von Lehre und Forschung auf hohem internationalem Niveau. Hierbei spielt die IuK-Infrastruktur, unter der die Gesamtheit aller technischen Einrichtungen zur Erfassung, Speicherung, Verarbeitung, Übertragung und Wiedergabe von Informationen mit den darauf aufbauenden Anwendungen verstanden werden soll, eine entscheidende Rolle.

IuK und ihre Organisation muss – soweit nicht schon geschehen – als Gesamtaufgabe der Hochschule gesehen werden. Ihre Betrachtung allein in den Rechenzentren oder in einzelnen Fachbereichen führt nicht zu global effektiven Lösungen. Alle im Gesamtsystem anstehenden Aufgaben können entweder zentral vom HRZ, von IuK-Expertengruppen der Fachbereiche oder vom Nutzer selbst gelöst werden. Diese Aufgabenzuordnung ist so zu regeln, dass Doppelarbeiten oder gar gegenläufige Lösungen vermieden werden. Wirtschaftlichkeit und Effizienz müssen Vorrang haben vor Partikularinteressen einzelner Personen, Gruppen oder Einrichtungen.

Die dynamische Fortentwicklung der IuK folgt grundsätzlich weiterhin den Entwicklungslinien, die im ersten Bericht aufgezeigt wurden. Um die Perspektiven deutlicher herauszuarbeiten, die für die IuK-Infrastruktur insgesamt und ihre Verzahnung mit der Entwicklung der Hochschule als Ganze und hier insbesondere ihres Informationsmanagements von Bedeutung sind, werden einige übergeordnete Sichtweisen vorangestellt, deren Tragweite sich erst in den letzten Jahren als so weit reichend herausgestellt hat, wie wir sie heute verstehen.

### *Generelle Entwicklungsperspektiven*

#### **Informationsmanagement, Prozessorientierung und Identity Management**

Es ist immer deutlicher geworden, dass die Hochschulen ihre gesamten Prozesse zur Informationsgewinnung, -verarbeitung und -vermittlung unter einheitlichen Gesichtspunkten und unter strategischer Führung der Hochschulleitung neu und effizienter gestalten müssen, damit Forschung, Lehre, Studium, Verwaltung und Öffentlichkeitsarbeit den vollen Nutzen aus der modernen Informations- und Kommunikationstechnik ziehen können. Dafür haben sich – gefördert durch die einschlägigen Ausschreibungen der DFG – Begriffe wie Informationsmanagement und integriertes Servicemanagement eingebürgert.

Neugestaltung und bessere Unterstützung der Prozesse führen zwangsläufig zu neuen Organisationsformen für die Zusammenarbeit der IuK-Infrastruktureinrichtungen untereinander und mit den Fachbereichen und Fakultäten. Aus Nutzersicht konkretisieren sich solche neu gestalteten Prozesse in verbesserten und neuartigen Dienstleistungen wie den vielerorts angestrebten Hochschulportalen, die personalisierten und integrierten Zugang zu Informations-, Lehr- und Wissensangeboten eröffnen, und – verzahnt mit e-Learning- und Verwaltungssystemen – Lehr-, Lern- und Verwaltungsprozesse aktiv und dezentral so unterstützen, dass sie an einer Stelle (vorzugsweise dem eigenen Computer) unter einer einheitlichen Oberfläche erledigt werden können. Es ist deutlich geworden, dass ein einheitliches Identitätsmanagement unverzichtbarer Kernbestandteil einer dergestalt neu zu strukturierenden IuK ist.

## Sicherheit und Verlässlichkeit

Die sichere Gestaltung der IuK-Infrastruktur und der darauf angebotenen Dienste ist zu einem zentralen Thema geworden. Dafür sind vor allem drei Gründe verantwortlich:

- Hochschulweites Informationsmanagement verlangt die zunehmende Verzahnung der bisher auch aus Sicherheitsgründen getrennten Prozesse für Verwaltung und Wissenschaft (integrierte Service-Infrastruktur).
- Die jetzt schon sehr ausgeprägte Abhängigkeit der täglichen Arbeit in Wissenschaft und Verwaltung von einer funktionierenden IuK-Infrastruktur nimmt immer noch zu.
- Mit zunehmender Komplexität und Leistungsfähigkeit ist die in weltweite Netze eingebundene IuK-Infrastruktur immer größeren Gefährdungen durch Nachlässigkeit, aber auch durch böswillige oder mutwillige Angriffe von innen und außen ausgesetzt.

Deshalb rückt die Bedeutung von Sicherheitskonzepten und verlässlichem Sicherheitsmanagement immer deutlicher ins allgemeine Bewusstsein und muss als wichtige Führungsaufgabe begriffen werden.

## Kooperationen, Konvergenz und Mobilität

Eine immer bessere Kooperation zwischen den Dienstleistern (vor allem HRZ, MZ, UB, Verwaltung) und mit den Fachbereichen und Fakultäten ist unerlässlich zur Bewältigung der erforderlichen Vernetzung, der Komplexität und des integrierten Servicemanagements. Ihre zweckmäßige Organisation wird von einer ganzen Reihe wichtiger Faktoren beeinflusst.

## Überwindung von Hochschulgrenzen

Die ständig weiter steigenden Anforderungen an die IuK-Infrastruktur und die darauf aufsetzenden Dienste können mit den vorhandenen Ressourcen nur gemeistert werden, wenn Dienste verstärkt hochschulübergreifend erbracht werden. Mit den Grid-Technologien, die immer deutlichere Konturen gewinnen, zeichnet sich dafür eine sehr leistungsfähige technische Basis ab. Gleichwohl sind die eigentlichen Herausforderungen organisatorischer Art.

Die Hochschulen in NRW haben mit erfolgreichen landesweiten Projekten (z. B. Ressourcenverbund NRW, diverse Landeslizenzen) gezeigt, dass sie gemeinsame Projekte zum Nutzen sehr vieler Hochschulen auf den Weg bringen und erfolgreich betreiben können. Sie haben sich in Zusammenarbeit mit dem zuständigen Ministerium Organisationsformen geschaffen, die ein gemeinsames Handeln organisieren helfen und Projekte begleiten, steuern und kontrollieren können: DV-ISA (DV-Infrastrukturausschuss des Landes NRW), Netzagentur, Ressourcenverbund NRW (RV-NRW) sowie Lenkungsausschüsse für Konsortial- und Landeslizenzen. Schon jetzt ist der Zugriff zu Hoch- und Höchstleistungsrechnern und zu sehr großen Datenspeichern nur noch kooperativ möglich, weil die meisten Hochschulen solche Systeme nicht mehr selbst betreiben. Diese Ressourcen stehen Wissenschaftlern und Studierenden im Rahmen des RV-NRW zur Verfügung.

Dieser Vorsprung, den NRW bei der Organisation kooperativen Handelns in der IuK gegenüber anderen Bundesländern erarbeitet hat, sollte unbedingt weiter ausgebaut werden.

## Konvergenz

Netze (Sprache, Daten, Gebäudeüberwachung, Festnetze, Funknetze), Dienste (Internet, Telefon, Fax, E-Mail, Video) und Endgeräte (Handy, Notebook, Organizer, PDA, Telefonapparat, Fernseher, Videorekorder, Mobiler Datenspeicher, Musikabspielgerät) wachsen zusammen und überlappen einander immer stärker. Dadurch entstehen neue Dienste und Anwendungen, die aus Gründen einer verbesserten Effizienz neue Organisationsformen und weit gehende neue Kooperationen verlangen. So ist heute z. B. die

Erneuerung oder Erweiterung einer Telefonanlage ohne enge Integration in das Daten-netz nicht mehr verantwortlich zu planen.

### **Mobilität**

Immer mehr Dienste, die früher an stationäre Geräte und Festnetzanschlüsse gebunden waren, können heute von mobilen Geräten aus in Anspruch genommen werden. Damit entstehen neue Kooperationsformen und neue Dienste wie z. B. im DFN-Roaming, mit dem es Hochschulangehörigen als Gast in einer fremden Universität möglich wird, von dort aus alle IuK-Dienste in seiner eigenen Universität in Anspruch zu nehmen.

### *Innovative IT-Felder*

Es werden folgende Empfehlungen ausgesprochen:

### **Entwicklungslinien**

- Die Hochschulleitung sollte sich dem Thema IuK verstärkt zuwenden und die notwendigen Schritte zur Verbesserung der Produktivität und zur Unterstützung des geänderten Nutzerverhaltens einleiten und dabei die weiter unten folgenden Empfehlungen berücksichtigen.

### **Organisationsfragen**

- Für die gemeinsam von Fakultäten, HRZ, Verwaltung, Bibliothek und anderen Einrichtungen wahrzunehmenden Aufgaben in der IuK-Versorgung sind im Detail die Aufgaben, der Support und die damit verbundenen Verantwortlichkeiten zu spezifizieren. Eine vertikale Organisationsstruktur (vom HRZ bis zu den konzentriert zusammen geführten IuK-Experten in den Fakultäten) und eine horizontale Organisation für die überlappenden Aufgabengebiete der zentralen Dienstleister sind einzuführen. Noch anzutreffende Einzelbetreuer sind in die Gruppe der IuK-Experten der Fakultäten zu integrieren, oftmals können deren Aufgaben auch direkt übernommen werden.
- Das Rektorat sollte prüfen, ob der IuK-Bedeutung entsprechend ein Lenkungsgremium (CIO) eingerichtet wird; dabei sind auch die Aufgaben der Senatskommission für die IuK in Verbindung mit der Senatskommission für die Bibliothek neu zu überdenken.
- Die bisherigen hochschulübergreifenden Dienstleistungen des RV-NRW müssen stärker in die Hochschulen hineingetragen werden. Eine hochschulübergreifende Zusammenarbeit des IuK-Personals ist zu fördern. Die bewährten kooperativen Strukturen zwischen den Hochschulen und dem MIWFT NRW sollten intensiv genutzt und weiter entwickelt werden.

### **Identitätsmanagement, Informationsmanagement und Portale**

- Die Einführung eines Identitätsmanagements zur einheitlichen und verbesserten Nutzerverwaltung muss weiter mit Nachdruck verfolgt werden. Die Hochschulleitung muss die Arbeit nach wie vor fordern und fördern.
- Die Einführung eines leistungsfähigen Informationsmanagements muss in den nächsten Jahren in Angriff genommen werden. Hierzu muss die Hochschulleitung Start-hilfe leisten.
- Die Einrichtung von Portalen erfordert die Mitwirkung aller Fachbereiche und zentralen Einrichtungen. Deshalb sollte auch hierzu der Anstoß vom Rektorat kommen.

### **E-Learning: Nachhaltige Integration in den Lehrbetrieb**

- Hochschulen sollten ein Konzept zum e-Learning vorlegen, in dem didaktische, organisatorische, technische und insbesondere verwaltungstechnische Aspekte aufeinander abgestimmt sind. Neue Kommunikationsformen sowie der Anspruch der

Unterstützung von Mobilität haben auch in Zukunft weit reichende Konsequenzen auf den Betrieb und den Ausbau der IuK-Infrastruktur und sollten in Konzepten zum e-Learning berücksichtigt werden.

- Neue Kommunikationsformen sowie der Anspruch der Unterstützung von Mobilität haben auch in Zukunft weit reichende Konsequenzen auf den Betrieb und den Ausbau der IuK-Infrastruktur und sollten in Konzepten zum e-Learning berücksichtigt werden.

### **Grid-Computing**

- Kompetenznetzwerke für Schulungs-, Beratungs-, und Unterstützungsaktivitäten zur Grid-Technologie sollten in den HRZ aufgebaut werden, lokal fokussiert durch thematische Schwerpunktbildungen der Hochschulen, vernetzt über hochschulübergreifende Kooperationsmechanismen und gestützt auf eine verbindliche Zusage der jeweiligen Hochschulen zur hochschulübergreifenden Dienstleistung.

### **Rechnerinfrastruktur und Vernetzung**

- Fest installierte CIP-Geräte müssen weiterhin regelmäßig modernisiert, aber in ihrer Anzahl nicht mehr weiter ausgebaut werden. Stattdessen sollten mit Laptops, die sich auch ausleihen lassen, innovative Szenarien unterstützt werden.
- Manche wissenschaftliche Rechenvorhaben verlangen Hochleistungsrechner, die in ihrer Leistungsfähigkeit um mindestens eine Größenordnung über den Workstations liegen, einige verlangen sogar die leistungsfähigsten Rechner, die es überhaupt gibt. Diese Anwendungen auf Hoch- und Höchstleistungsrechnern sind für die Forschung oftmals von herausragender Bedeutung. Die Hochschulen müssen deshalb den Zugang zum HPC und zum Höchstleistungsrechnen unbedingt erhalten, wollen sie nicht riskieren, aus wichtigen Gebieten an der Front der Forschung in kaum mehr aufzuholender Weise auszuscheiden. Der DV-Infrastrukturausschuss in Zusammenarbeit mit dem MIWFT des Landes NRW sollte basierend auf fachlicher Begutachtung Beschaffungen so steuern, dass das Nutzungspotential für die Wissenschaft in NRW maximiert sowie eine effektive Nutzung der Beschaffungen gewährleistet werden.
- Der Bedarf an Massenspeicher wird weiter schnell steigen, kleinteilige Lösungen sind dabei unwirtschaftlich. Für den Betrieb ist Professionalität ökonomisch sinnvoll und notwendig.
- Eine zeitnahe Modernisierung der Netzkomponenten ist notwendig. Die Konvergenz der Netzdienste (LAN und Telefon) muss auch organisatorisch realisiert werden.
- Die Verteilung von Software muss soweit wie möglich automatisiert werden. Die Beschaffung der Software sollte innerhalb und möglichst sogar hochschulübergreifend koordiniert werden.
- HRZ sollten ihre Kompetenz für den Einsatz von anspruchsvollen Standardanwendungen weiter ausbauen und neuartige Anwendungen unterstützen. Zukünftig sollten die HRZ den fachübergreifenden Anwendungen wieder mehr Aufmerksamkeit widmen, ohne die Kommunikations- und Systemdienste zu vernachlässigen. Die HRZ sollten darauf hinarbeiten, ihre Kompetenz als Projektpartner in der Forschung einzubringen und zu schärfen.
- Die IuK-Angebote einer Hochschule zur Aus- und Weiterbildung der Studierenden und Bediensteten sind unter allen Anbietern abzustimmen und durch Nutzung neuester multimedialer Techniken möglichst noch auszuweiten. Der fortlaufenden Qualifizierung der Dienstleister ist größere Aufmerksamkeit zu widmen.

### **Dienste: Qualität, Management und Sicherheit**

- Qualitätsstandards, die nicht unterschritten werden dürfen, sind zu überprüfen, festzulegen und einzuführen.

- Netzmanagement- und Systemmanagement-Instrumente sind bedeutende Instrumentarien für einen verlässlichen Service. Ihre Ausweitung auf alle wichtigen Systeme – insbesondere auf alle Server in der Hochschule – ist dringend geboten. Ihre Zusammenführung mit anderen Management-Instrumenten erschließt weitere Synergien.
- Sicherheit und Katastrophenschutz sollten von der Hochschulleitung als strategische Aufgabe gesehen werden.
- Das notwendige Know-how für die einzelnen Schutzmaßnahmen ist in den Hochschulen vorhanden; personelle und finanzielle Ressourcen für die Umsetzung müssen ergänzend bereitgestellt werden.

### **Beschaffungspolitik und Finanzen**

- Verwaltungen und HRZ sollten verstärkt auch hochschulübergreifend kooperieren, um das Beschaffungswesen für IuK zu vereinfachen.
- Eine Kosten- und Leistungsrechnung sollte eingeführt werden; wobei der Leistungsrechnung eine besondere Bedeutung zukommt. Die Kostenträgerrechnung muss ohne großen Verwaltungsaufwand durchzuführen sein. Seinen vollen Nutzen entfaltet dieses Instrument allerdings erst, wenn es die gesamte Hochschule erfasst.

## **„mein ZIV“ – Ihr Portal für ZIV-Dienste**

*R. Perske*

**Nutzerverwaltung, E-Mail, wwu@home, Print&Pay u. v. a. m. Sind auf den ZIV-Webseiten über die Hauptnavigation erreichbar.**

Die bisherigen Seiten „Zentrale Nutzerverwaltung Online“ wurden zu einem Portal ausgebaut und umfassen jetzt auch „wwu@home“, „Print&Pay“ und viele weitere Einstellungs- und Anmelde-möglichkeiten.

Schon lange konnten Sie mit Ihrer Nutzerkennung und Ihrem Passwort zahlreiche Einstellungen auf verschiedenen WWW-Seiten des ZIV vornehmen: Vorläufige Nutzerkennungen freischalten, Passwörter ändern, E-Mail-Aliasnamen und -Weiterleitungen einrichten, Änderungen persönlicher Daten mitteilen, sich für Lehrveranstaltungen des ZIV anmelden u. v. a. m.

Bislang waren diese Einstellungsmöglichkeiten weit über verschiedene WWW-Seiten verstreut und demzufolge häufig schwierig zu finden. Seit einiger Zeit bemühen wir uns, diese Einstellungsmöglichkeiten in einem Portal an zentraler Stelle zusammenzufassen. Unter dem Namen „mein ZIV“ finden Sie dieses Portal auf jeder ZIV-Seite oben in der Hauptnavigation.

Hatte sich dieses Portal bisher auf Einstellungen zur Nutzerkennung und zum E-Mail-Postfach beschränkt, so finden Sie jetzt dort auch alle Anmelde- und Einstellungsmöglichkeiten zu unserem Druckangebot „Print&Pay“ und zu unserem Einwahlangebot „wwu@home“ (früher „uni@home plus“). Auch einen (fast) kompletten Auszug aller Daten, die das ZIV über Sie gespeichert hat, können Sie jetzt abrufen.

Wie es sich für ein vernünftiges Portal gehört, können Sie aus „mein ZIV“ heraus per „Single Sign-On“, also ohne erneute Anmeldung, Ihre E-Mails mit unserem Webmail-Angebot „perMail“ bearbeiten, sich für ZIV-Lehrveranstaltungen unter „ZIVlehre“ anmelden, mit „ZIVintro“ eine Schlüsselkarte für den Rund-um-die-Uhr-Zugang zu den Rechnerpools im ZIV bestellen, als „Print&Pay“-Nutzer oder Mitarbeiter mit „ZIVprint“ Druckaufträge an die zentralen Drucker senden und weitere Dienste nutzen. Selbst wenn wie bei den Online-Rechnungen für „Print&Pay“ und für „wwu@home“ aus technischen Gründen auf eine erneute Passwortabfrage noch nicht verzichtet werden kann, werden Sie in „mein ZIV“ zumindest Verweise auf diese Dienste finden, beispielsweise auf das universitätsweite „HIS-LSF“-System für Anmeldungen zu Lehrveranstaltungen und Prüfungen.

Natürlich präsentiert sich „mein ZIV“ jetzt im neuen Universitäts-Design des Zentrums für Informationsverarbeitung. Die nach der Anmeldung erscheinende Übersichtsseite fasst alle aktuell für Sie zur Verfügung stehenden Einstellungsmöglichkeiten kompakt zusammen. Auch die Navigationsleiste wird selbstverständlich auf Ihre persönliche Situation zugeschnitten dargestellt. Zu jeder Schaltfläche gibt es in der rechten Spalte ausführliche Erläuterungen über Sinn und Zweck.

„mein ZIV“ wird Schritt für Schritt ausgebaut. Auf vielfachen Wunsch unserer Nutzer wird auch eine englischsprachige Version vorbereitet.

## „wwu@home“-Einwahl: Verfügbarkeit in den Region-50-Bereichen erweitert

M. Speer

**Die Zahl der Region-50-Bereiche, in denen der Internet-Einwahldienst „wwu@home“ verfügbar ist, wurde noch einmal erweitert.**

Zum Januar 2006 wurde die Zahl der Ortsnetzbereiche (ONB) der Deutschen Telekom, in denen der Internet-Einwahldienst „wwu@home“ genutzt werden kann, noch einmal erweitert. Es wurden 7 zusätzliche Region-50-Bereiche freigeschaltet. Insgesamt ist „wwu@home“ nun im gesamten Tarifbereich Münster City für 0,77 Cent/Min. und in 40 Region-50-Bereichen für 1,29 Cent/Min. rund um die Uhr verfügbar. Die folgende Tabelle listet die nun abgedeckten Region-50-Bereiche auf, dabei wurden die neu hinzugekommenen Bereiche hervorgehoben:

Vorwahl	ONB	Vorwahl	ONB	Vorwahl	ONB
2303	Unna	2553	Ochtrup	<b>5401</b>	<b>Georgsmarienhütte</b>
2306	Lünen	2554	Laer	<b>5405</b>	<b>Hasbergen</b>
2361	Recklinghausen	2555	Schöppingen	541	Osnabrück
2364	Haltern	2556	Metelen	5451	Ibbenbüren
2381	Hamm	2558	Horstmar	5459	Hörstel
<b>2382</b>	<b>Ahlen</b>	2562	Gronau	5481	Lengerich
2389	Werne	2572	Emsdetten	5482	Tecklenburg
2521	Beckum	2581	Warendorf	<b>5485</b>	<b>Ladbergen</b>
<b>2542</b>	<b>Gescher</b>	2584	Warendorf-Milte	5923	Schüttorf
2543	Billerbeck Westf.	2591	Lüdinghausen	5971	Rheine
2546	Coesfeld-Lette	2592	Selm	5973	Neuenkirchen
2551	Steinfurt-Burgsteinfurt	2594	Dülmen	5975	Rheine-Mesum
2552	Steinfurt-Borghorst	<b>5242</b>	<b>Rheda-Wiedenbrück</b>	5976	Salzbergen
				<b>5978</b>	<b>Hörstel-Dreierwalde</b>

Tabelle 1: Von „wwu@home“ abgedeckte Region 50-Bereiche

Der Vollständigkeit halber sind in der folgenden Tabelle noch einmal sämtliche Ortsnetzbereiche des von „wwu@home“ komplett abgedeckten Tarifbereichs Münster City aufgelistet:

Vorwahl	ONB	Vorwahl	ONB	Vorwahl	ONB
251	Münster	2509	Nottuln Appelhülsen	2571	Greven Westf.
2501	Mstr Hilstrup	2526	Sendenhorst	2573	Nordwalde
2502	Nottuln	2532	Ostbevern	2575	Greven Reckenfeld
2504	Telgte	2533	Mstr Nienberge	2582	Everswinkel
2505	Altenberge Westf.	2534	Mstr Roxel	2593.	Ascheberg Westf.
2506	Mstr Wolbeck	2535	Sendenhorst Albersloh	2597.	Senden Westf.
2507	Havixbeck	2536	Mstr Albachten	2598	Senden Ottmarsbocholt
2508	Drensteinfurt	2538	Drensteinfurt Rinkerode		

Tabelle 2: Von „wwu@home“ komplett abgedeckt: Tarifbereich Münster City

Weitere ausführliche Informationen findet man auf der „wwu@home“-Homepage: [www.uni-muenster.de/ZIV/wwuhome](http://www.uni-muenster.de/ZIV/wwuhome).

## Netzseitige IT-Sicherheitsmaßnahmen des ZIV 2006

G. Richter

**Netzseitige Maßnahmen zur IT-Sicherheit ermöglichen an lokalen Bedarf angepasste Schutzfunktionen und zeigen nachweisbare Erfolge.**

Das ZIV hatte im [info:wwu](#) Nr.1/2005 „netzseitige IT-Sicherheitsmaßnahmen“ vorgestellt, die auf einer hierarchischen Strukturierung des Netzes unter unmittelbarer Einbettung von wichtigen Sicherheitsfunktionen beruhen: *stateless* und *stateful packet screening*, Intrusion-Prevention sowie differenzierter VPN-Zugang.

Der vorliegende Artikel ist nur eine erste Fortschreibung dieses Beitrags. Dazu beitragen sollen auch die hier folgenden Artikel zum Stateful-Packet-Screening-Service und zum VPN-Service. In einer nächsten [info:wwu](#)-Ausgabe soll dann detaillierter auf den netzbaasierten Intrusion-Prevention-Service, den Stateless-Packet-Screening-Service und weitere Maßnahmen zur Strukturierung eingegangen werden.

Notwendige Schlüsseltechnologie ist die Virtualisierung für LAN-, Routing- und Sicherheitsfunktionen (vgl. [1]). Als unabdingbar wird die Selbstverwaltungsmöglichkeit für die Sicherheitsbelange vor Ort (Mandantenfähigkeit) angesehen. Netzstrukturierung und ihre Implementierung sind ohnehin als langfristige Prozesse anzusehen, die laufend an die sich verändernde Bedarfssituation angepasst werden müssen. Dennoch sind in vielen Bereichen der Universität und des Universitätsklinikums kontinuierlich Strukturierungsmaßnahmen durchgeführt worden, die das Sicherheitsniveau verbessert haben.

Musterhaft konnte in einem Pilotprojekt für das Zentrum für Zahn-, Mund- und Kieferheilkunde (ZMK) im Universitätsklinikum (UKM) vorgegangen werden. Unter Zusammenarbeit der lokalen IT-Verantwortlichen, dem IT-Zentrum des UKM und dem ZIV wurde eine Netzzone „ZMK“ innerhalb der Netzzone „UKM“ konzipiert; die Netzzone „ZMK“ selbst ist unterstrukturiert in derzeit 18 ebenfalls neu geschaffene Netzzone, die unterschiedlichsten Zwecken bei unterschiedlichen personellen Zuständigkeiten dienen und die unterschiedlichen Sicherheitsbedürfnissen unterliegen (vgl. Abb. 1):

- 7 Netzzone für Arbeitsplatzrechner entsprechend der Vielzahl der Arbeitsbereiche bzw. Kliniken,
- 1 Systemadministratorenzone,

- 5 Server-Netzzonen für einzelne Kliniken oder gemeinsame interne Nutzung sowie für externe Nutzung (z. B. Web-Server),
- 3 Sonderzonen (Veranstaltungsräume, TV-Studio, zentrale Drucker),
- 2 Zonen für den VPN-Zugang unterschiedlicher Personenkreise (mit unterschiedlichen Rollen und entsprechenden Rechten beim Zugang zu anderen Netzzonen)

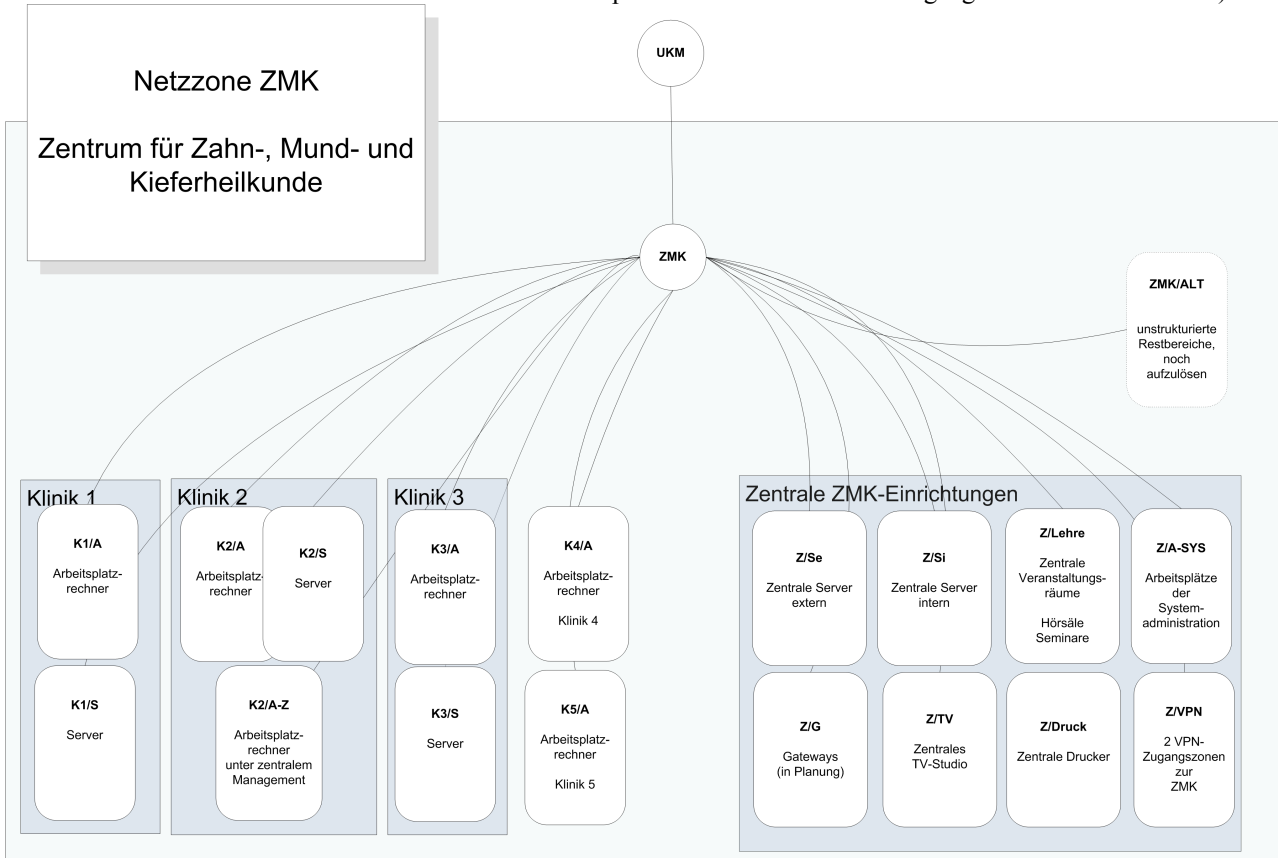


Abb. 1: Struktur der Netzzone ZMK (weitgehend anonymisiert)

Alle Netzzonen innerhalb der Zone „ZMK“ unterliegen wechselseitig einer Einschränkung der Zugangsmöglichkeiten, ebenso gegenüber dem externen Netz (übergeordnete Netzzonen bis hin zum Internet), indem *stateless packet screening* angewendet wird. Hier kommt die neueste Switch-Technologie zum Einsatz (Cisco Catalyst 6509), die es erlaubt, über einen eigenen „virtuellen Router“ für die Netzzone „ZMK“ Interfaces mit so genannten ACLs (Access-Control-Listen) für die einzelnen Netzzonen einzurichten. Die Vorgehensweise ist hier in der Regel eine restriktiv, um ein möglichst hohes Schutzniveau zu erreichen: Kommunikation, die nicht ausdrücklich erlaubt ist, wird durch ACLs strikt unterbunden.

Während Switch-basierte ACLs eine Zugangskontrolle ohne Leistungseinbußen und ohne besonderen Investitionsaufwand ermöglichen und deshalb im großen Umfang einsetzbar sind, können Stateful-Packet-Screening- und Intrusion-Prevention-Funktionen nur an strategisch ausgezeichneten Punkten in der Netztopologie eingebettet werden. Im ZMK-Projekt wurden diese Funktionen deshalb nur einmal, für die gesamte Netzzone „ZMK“ eingerichtet. Entsprechende Schutzfunktionen wirken nur auf den Datenverkehr von und nach „außen“, nicht aber zwischen den untergeordneten Netzzonen.

*Stateful packet screening* (Cisco Firewall Service Module) soll zunächst beispielsweise dazu verwendet werden, Rechnern in Arbeitsplatznetzzonen zu ermöglichen, Verbindungen nach außen zu initiieren, während das Öffnen von Verbindungen von außen (Internet, allgemein Systeme außerhalb der Netzzone „ZMK“) in der Regel unterbunden wird. Intrusion-Prevention-Funktionen erhöhen für alle Systeme in der Netzzone ZMK

die Sicherheit in Bezug auf solche Angriffe, die hier ebenfalls von außen erfolgen und für deren Typus die verwendete Intrusion-Prevention-Appliance (McAfee Intrushield 4000) aktiviert wurde. Gerade diese Sicherheitsfunktion erwies sich sehr schnell als sehr wertvoll, nicht nur weil die Gerätestatistik eine Vielzahl geblockter Angriffe regelmäßig nachweisen konnte, sondern auch weil anfangs unerwünschter Datenverkehr „von innen nach außen“ registriert werden musste, der Hinweise auf problembehaftete Endgeräte in der Netzzone und zu einer Bereinigung Anlass gab. Auch der gezielte Zugang über VPN (authentifiziert, 3DES-verschlüsselt) unmittelbar in verschiedene Netzzone innerhalb der Netzzone „ZMK“, je nach Autorisierung, wurde realisiert.

Den Erfolg dieses Projektes „ZMK“ mag man auch daran ablesen, dass das Universitätsklinikum sich entschlossen hat, diese Sicherheitstechnologie und -strategie in Zusammenarbeit mit dem ZIV weiter auszubauen. Ein unmittelbar nächster Schritt wird beispielsweise der Einsatz einer Intrusion-Prevention-Instanz über der Netzzone „UKM“ sein.

Eine weitere Anwendung für die beschriebenen Sicherheitsmaßnahmen hier sind Zugänge aus externen Bereichen (Remote Access System, „RAS-Bereich“). Gemeint sind die Einwahlzugänge über ISDN- und Analogverbindungen, der authentifizierte Zugang über frei zugängliche LAN-Anschlüsse (pLANet) und Funk-LAN-Zellen der Universität sowie Zugänge aus Studierendenwohnheimen. Seit langem ist dieser Bereich, über den ja zumeist private Rechner an das Universitätsnetz gekoppelt werden, problematisch, weil uns darüber eine Vielzahl von Beschwerden erreicht, die mühsam im ZIV-CERT bearbeitet werden müssen. Ursache ist häufig ein infizierter Rechner in diesem Zugangsbereich. Als eine besonders wichtige Sicherheitsmaßnahme wurde deshalb das Netz so umstrukturiert, dass der gesamte RAS-Bereich auf oberster Hierarchieebene vom übrigen Netz getrennt wurde (vgl. Abb. 2, Netzzone Wissenschaftsnetz Münster, Netzzone RAS-I und RAS-O). Gleichzeitig wurde eine Intrusion-Prevention-Instanz an der Stelle eingebettet, an der der RAS-Datenverkehr in das lokale Netz endgültig und in Gesamtheit eintritt (RAS-O). Der Erfolg dieser Maßnahme war ganz erheblich, in der Größenordnung wurde mindestens eine Drittelung der CERT-Vorfälle erzielt.

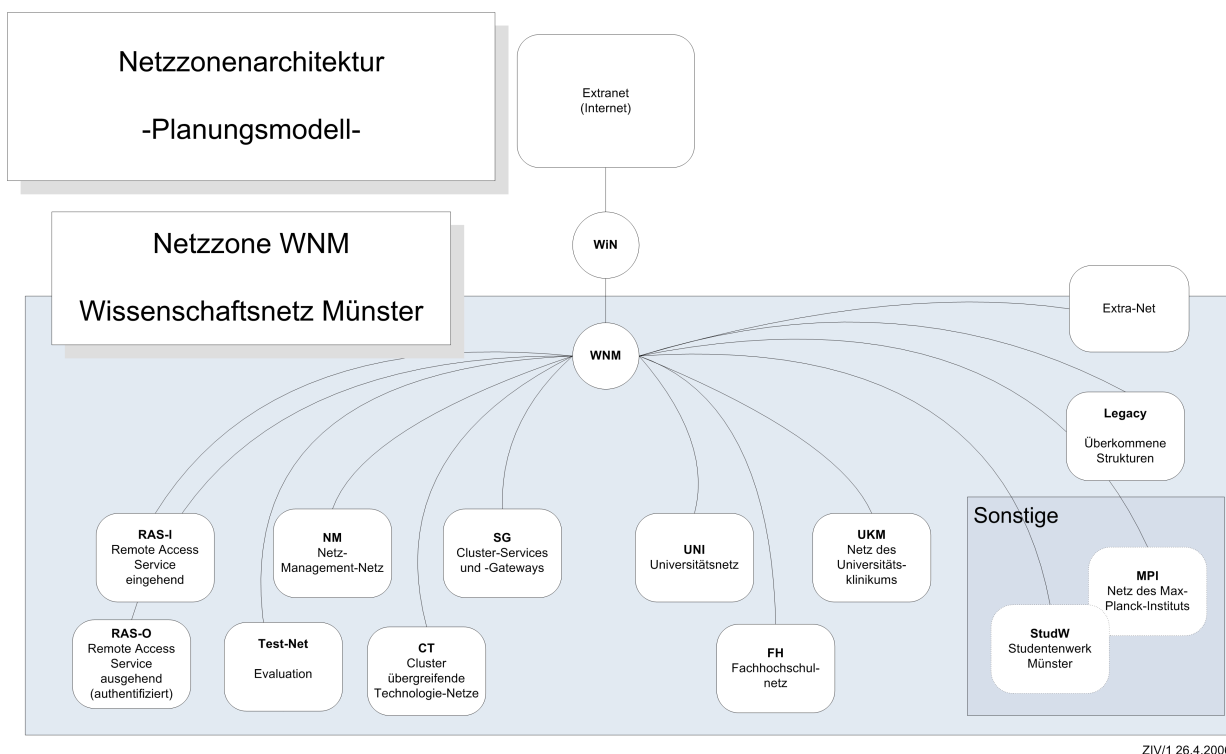


Abb. 2: Struktur der hierarchisch obersten Netzzone (WNM)

Für die Universität ist bereits vorbereitet auch eine Intrusion-Prevention-Instanz oberhalb der Netzzone der Universität (vgl. Abb. 2, Netzzone UNI) einzubetten, eine Aktivierung kann in wenigen Wochen erfolgen.

[1] G. Richter et al., 2006: „Schutz großer Netze“, in: 13. DFN-CERT Workshop „Sicherheit in vernetzten Systemen“, Hrsg.: Chr. Paulsen

## VPN-Service des ZIV

A. Forsmann

**Die Resonanz auf den neuen VPN-Service ist erfreulich positiv. Eine „Policy Enforcement“-Lösung soll bald für ausgewählte Verbindungen überprüfen, ob VPN-Clients konform zu Sicherheitsanforderungen sind.**

Im Artikel „Neue VPN-Technologie an der Universität“ im letzten **inforum** (Nr. 3/2005) wurde der neue IPSec-basierende VPN-Service des ZIV bereits vorgestellt und dessen Benutzung erklärt.

Folgende Vorzüge des neuen VPN-Service seien hier noch einmal kurz aufgezählt:

- einfache Installation und Handhabung der VPN-Clients für alle gängigen Betriebssysteme (Windows, Linux, MacOS),
- verschlüsselter 3DES-Verkehr mit einem Durchsatz bis zu 1,9 GBit/s und bis zu 8000 gleichzeitigen Tunnel-Verbindungen pro VPN-Service-Modul,
- systeminherente Virtualisierungsmöglichkeiten erlauben die Konfiguration (nahezu beliebig) vieler paralleler VPN-Gateways,
- mandantenfähige Nutzerverwaltung für die VPN-Gateways,
- zurzeit werden zwei VPN-Service-Module in Catalyst-Router-Switches an getrennten Standorten eingesetzt. Grundsätzlich ist jedes VPN-Gateway auch auf dem jeweils anderen Service-Modul konfiguriert, so dass Redundanz erreicht wird.

Aufgrund dieser Eigenschaften kann das ZIV den IV-Versorgungseinheiten, Instituten, Kliniken, Fachbereichen usw. „virtuell“ eigene VPN-Gateways für deren Netzzonen auf Anfrage bereitstellen. Die Resonanz auf den neuen VPN-Service ist sehr positiv, so dass im Augenblick schon mehr als 25 VPN-Gateways für unterschiedliche Verwendungszwecke eingerichtet sind. U. a. dienen sie als

- zentraler Allgemeinzugang zum Netz der Universität und des Universitätsklinikums (UKM) für alle IV-System-Nutzungsberechtigten, über das Internet von zu Hause und unterwegs,
- Wartungszugang für Systemadministratoren zu diversen Server-Netzzonen,
- Wartungszugang für Mitarbeiter externer Firmen für spezielle Netzzonen mit fremdgewarteten IV-Systemen,
- Zugang für „Teleworker“ zu geschützten Netzzonen von Organisationseinheiten in Universität und UKM,
- Kopplung von externen Rechnernetzen über so genannte „Site-to-Site“-VPN-Verbindungen, d. h. ein externes Rechnernetz wird über das Internet mittels eines verschlüsselten VPN-Tunnels sicher an Netzzonen im Rechnernetz der Universität oder des UKM gekoppelt; diese Variante wird z. B. für externe Netze von Firmen für Wartungszwecke oder für externe Netze der Universität (z. B. Haus Rothenfelde) genutzt.

Am Ausgang eines jeden VPN-Gateways ist zumeist ein „stateless“ Paketfilter definiert, der den Datenverkehr durch den VPN-Tunnel nach Bedarf auf das Notwendige oder Erlaubte einschränkt. Bei besonderem Sicherheitsbedarf kann zusätzlich eine Intrusion-Prevention-(IPS)- oder eine Stateful-Firewall-Instanz am Ausgang des VPN-Gateways installiert werden.

Die Sicherheit der Verbindungen über VPN-Tunnel bezieht sich zunächst nur auf die Abhörsicherheit der Übertragung und die Authentifizierung des Clients gegenüber dem VPN-Gateway. Nicht jedoch ausgeschlossen sind damit Sicherheitsprobleme, die durch die Clients selbst hervorgerufen und über die Tunnel in die Netzzonen eingebracht werden können. Die Thematik der Durchsetzung von Sicherheitsregeln (Security Policy Enforcement) auf Clients bei deren Netzzugang beschäftigt inzwischen die Netzindustrie unter den Stichworten NAC – Network Admission Control (Cisco), NAP – Network Access Protection (Microsoft) und TNC – Trusted Network Connect (Open Standard Non Profit Organization). Trotz aller überschäumenden Marketing-Aktivitäten hier ist eine allgemein einsetzbare Lösung noch nicht verfügbar, für den VPN-Service aber ist der Bedarf für ein Security-Policy-Enforcement sehr ausgeprägt, da gerade über VPN-Tunnel der Zugang auch zu hochgradig zu schützenden Netzzonen ermöglicht werden soll. Das ZIV testet deshalb zurzeit eine „NAC-Lösung“, die viel versprechend erscheint. Dabei wird die VPN-Verbindung erst freigeschaltet, wenn das Endgerät gewünschte Sicherheitsanforderungen erfüllt. Es kann z. B. überprüft werden, ob eine Anti-Virus-Software mit den zugehörigen aktuellen Viren-Updates aktiviert ist oder ob das Betriebssystem durch wichtige Sicherheitsupdates aktualisiert wurde. Auch andere Parameter des Endgerätes können dabei kontrolliert werden, z. B. ob bestimmte Applikationen laufen oder nicht. Endsysteme, die gegen die Sicherheitsanforderungen verstoßen, werden zunächst in eine „Quarantäne-Zone“ verwiesen, in der lediglich die notwendigen Maßnahmen für die Herstellung der Security Policy Compliance stattfinden können; so könnten z. B. von dort die neuesten Sicherheitsupdates für das Betriebssystem und die der Anti-Virus-Software bezogen werden. Erst wenn das Endsystem allen Sicherheitsanforderungen genügt, kann der VPN-Tunnel verwendet werden.

Interessenten, die einen sicheren Zugang zu ihren Netzzonen benötigen, können sich im ZIV gerne über die Möglichkeiten der Einrichtung eines eigenen VPN-Gateways und weiteren Sicherheitsfunktionen beraten lassen.

## Stateful-Firewall-Service des ZIV

G. Wessendorf

### Das ZIV betreibt neue leistungsfähige Firewall-Technik.

In [infoforum](#) Nr. 1/2005 wurden „netzseitige IT-Sicherheitsmaßnahmen des ZIV“ vorgestellt. In diesem Beitrag wollen wir einen genaueren Abriss über den Stand und die Technik der inzwischen eingesetzten und in Pilotprojekten in Betrieb befindlichen stateful-Firewall-Technologie des ZIV geben.

Im Kernnetz der Universität werden Switch-Router vom Typ Catalyst 6509 der Firma Cisco Systems eingesetzt. Diese Systeme haben einen Gesamtdurchsatz von bis zu 400 Mio. IP-Datenpaketen/s bzw. 720 GBit/s. Die Catalyst-Switche sind modular aufgebaut und erlauben neben dem Einschub von z. B. Ethernet-Interface-Modulen (z. B. Module mit 4x10 GBit/s-Ports) auch den Einschub von so genannten Servicemodulen. Neben dem VPN-Servicemodul (siehe Beitrag „VPN-Service des ZIV“ in diesem [infoforum](#)) wird auch das Firewall-Servicemodul vom ZIV eingesetzt.

Für an technischen Details interessierte Leser hier einige wesentliche Betriebsparameter des Firewall-Servicemoduls:

- hardware-basierte stateful Firewall,
- bis zu 5,5 GBit/s bzw. 1 Mio. Pakete/s Durchsatz ohne Verluste,
- bis zu 1 Mio. gleichzeitige Kommunikationsverbindungen (sog. Sessions bzw. Sitzungen),
- bis zu 100.000 Sitzungsneuaufbauten pro Sekunde,
- bis zu 100 Firewall-Instanzen (virtuelle Firewalls).

Somit steht dem ZIV ein vergleichsweise sehr leistungsfähiges Stateful-Firewall-System zur Verfügung. Zur Realisierung der im Netz verteilt einzubettenden Sicherheitsfunktionen sind insbesondere die Virtualisierungs-Möglichkeiten hervorzuheben: Bis zu 100 virtuelle Firewalls können pro Modul definiert werden. Jede virtuelle Firewall kann unabhängig von den anderen virtuellen Firewalls des gleichen Moduls konfiguriert und betrieben werden. Somit können viele verschiedene Netzzonen mit unterschiedlichsten Sicherheitsbedürfnissen gleichzeitig über Firewall-Sicherheitsfunktionen durch ein einziges Modul geschützt werden. Damit die Wahrscheinlichkeit einer Durchsatz-Überbuchung gering gehalten wird, hat sich das ZIV entschlossen, zunächst maximal 25 virtuelle Firewalls pro Modul zu konfigurieren. Auch ist jeweils eine genaue Analyse der Kommunikationsbeziehungen und des zu erwartenden Verkehrsflusses notwendig, bevor eine Firewall-Instanz in Übertragungswege des Kernnetzes eingeschleift wird und damit ein Firewall-Service für eine Netzzone bereitgestellt wird. Oft genügt zur Grundabsicherung von z. B. Server-Subnetzen, welche auf eine höchst-performante Netzanbindung angewiesen sind, der Einsatz von Router-Interface-basierten *stateless* Filterfunktionen (Access-Listen bzw. ACLs). ACLs können auf den oben erwähnten Router-Switches Catalyst 6509 nämlich ohne Leistungseinbußen bzw. Datenverluste mit voller Interfacegeschwindigkeit abgearbeitet werden. Der Einsatz einer *stateful* Firewall ist aber dagegen z. B. dann einer *stateless* ACL-Filterung vorzuziehen oder notwendig, wenn

- die benötigten Verbindungen nur „stateful“ behandelt werden können, weil z. B. die benutzten Kommunikationsprotokolle TCP/UDP-Port-Nummern dynamisch aushandeln (z. B. H.323 und SIP (relevant für Voice over IP) oder FTP),
- oder wenn aus Netzbereichen heraus relativ komplexe vielfältige Verbindungen nach „außen“ aufgebaut werden dürfen, aber umgekehrt eine weitestgehende Abschottung gegen Zugriff von „außen“ gegeben sein soll. Die „stateful“-Eigenschaft der Firewall vereinfacht solche Regelwerke ganz erheblich. Typische Einsatzszenarien sind z. B. CIP-Pool- oder Mitarbeiter-Netze, in welchen keine von außen zu erreichende Dienste angeboten werden,
- und wenn gleichzeitig das zu erwartene Durchsatzvolumen dies erlaubt.

Ein weiterer erwähnenswerter Vorteil der eingesetzten Firewall-Servicemodule ist die Mandantenfähigkeit der zugehörigen Management-Software. Es kann den jeweiligen Netzzonenverantwortlichen die Möglichkeit eingerichtet werden, die Konfiguration der zugehörigen virtuellen Firewall(s) einzusehen oder auch selbstständig zu ändern. Auch ist es inzwischen nach einiger Eigenentwicklung im ZIV möglich, das Monitoring der anfallenden Sicherheitsmeldungen der Firewalls mandantenfähig anzubieten, d. h. die Netzzonenverantwortlichen haben Einsicht auf die für ihren jeweiligen Bereich anfallenden Logging-Daten.

Zurzeit werden zwei Firewall-Servicemodule eingesetzt. Wird nämlich eine Netzzone durch den Stateful-Firewall-Service abgesichert, wird sie grundsätzlich von zwei virtuellen Firewalls, verteilt auf die beiden Servicemodule (in verschiedenen Gebäuden), abgesichert. Nur jeweils genau eine virtuelle Firewall ist für eine Netzzone zu einer bestimmten Zeit aktiv. Die jeweils andere (sekundäre) virtuelle Firewall ist zwar zu jeder Zeit gleich konfiguriert und betriebsbereit, wird aber nur (automatisch) aktiv, wenn der primäre Weg ausfallen sollte. Durch gleichmäßige Verteilung von primären und sekundären virtuellen Firewalls auf die Servicemodule kann eine Lastverteilung erreicht werden.

Zurzeit findet bereits ein umfangreicher Betrieb des Firewall-Services im Universitätsklinikum (UKM), Bereich Zentrums für Zahn-, Mund- und Kieferheilkunde (ZMK) als Pilotprojekt statt. Weitere Bereiche sollen in Kürze folgen, u. a. für die Videokonferenzsysteme vom Dez. 4.43, Kommunikations- und Medientechnik, insbesondere weil hier die o. g. Protokolle H.323 bzw. SIP dies notwendig machen. Gerne beraten wir weitere Interessenten über die Möglichkeiten der Absicherung ihrer Netzbereiche.

## Erheblich verbesserte SPAM-Erkennung in der Erprobung

D. Bucher

Im Rahmen einer Teststellung erprobt das ZIV momentan eine E-Mail-Lösung der Firma Symantec. Hiermit wird die Erkennungsrate von unerwünschter Werbe-E-Mail (sog. SPAM) auf über 90% bei extrem geringer Fehlerrate (1:1 Million) gesteigert. Das System wird erkannte SPAM markieren, sodass der Nutzer über entsprechende Filterregeln reagieren kann. Weitere Informationen hierzu werden nach Einbindung in das zentrale E-Mailsystem in Kürze auf der ZIV-Homepage (<http://www.uni-muenster.de/ZIV>) veröffentlicht.

## Tabellenloses Layout unter Imperia

W. Kaspar, A. Scheffer, Wichmann

**Hinter den Kulissen des Webauftritts der Universität Münster vollzieht sich derzeit ein grundlegender Wandel, bei welchem dem Contentmanagementsystem Imperia eine besondere Bedeutung zukommt: Die Seiten werden barrierefrei im Sinne des Behindertengleichstellungsgesetzes.**

Eine auf dem Gleichstellungsgesetz basierende Umsetzungsverordnung, die BITV-NRW (Barrierefreie Informationstechnologie-Verordnung), schreibt es Landeseinrichtungen vor, bestehende Webangebote bis zum 31.12.2008 BITV-konform umzubauen. Neue Auftritte müssen bereits heute die Vorgaben der Verordnung erfüllen.

Um dies zu erreichen, haben Online-Redaktion und ZIV in den letzten Monaten gemeinsam mit einer Agentur den möglichst reibungslosen Wechsel von der alten, tabellenbasierten Layout-Struktur der Universitätsseiten im WWW hin zu einer auf dem sogenannten *Box-Modell* beruhenden Kodierung vorbereitet. Tabellen werden auf ihren eigentlichen Ursprung zurückgeführt und nur noch für die Darstellung von Daten verwendet. Für die Positionierung grafischer Elemente kommen Blockelemente, vor allem die *Divisions* oder *DIV-Tags*, zum Einsatz.

Positioniert werden sie über entsprechende Definitionen in den verknüpften Stylesheet-Dateien, externen Formatvorlagen also. Dies führt zu einer sehr strikten Trennung von HTML-Struktur, Inhalt und Layout – und damit auch zu einer problemlosen Modifizierung des Layouts für verschiedene Ausgabemedien. Dies kommt dem Gedanken der Barrierefreiheit entgegen, weil Menschen mit Seh- oder anderen Behinderungen die Darstellung der Seiten stärker beeinflussen und leichter in den Seiten navigieren können. Darüber hinaus ergeben sich eine Reihe von weiteren Vorteilen:

- Durch die Verschlanung und übersichtlichere Strukturierung des Quellcodes lassen sich die Seiten schneller und einfacher produzieren.
- Die Dateien werden kleiner, die Ladezeiten und die benötigte Bandbreite entsprechend geringer.
- Die Verwendung von XHTML macht uns „vorwärtskompatibel“. Wir sind für kommende Browsergenerationen gerüstet.
- Alternative Darstellungsgeräte wie Handy, PDA oder Sprachbrowser werden von uns über entsprechende Stylesheets direkt mitbedient.
- Layoutwechsel sind einfacher möglich, da sie im Wesentlichen über die externen CSS-Dateien erfolgen.
- Suchmaschinen können unsere Seiten besser erfassen. Die Listings verbessern sich.

Der Wechsel auf den neuen Standard kann durch den Einsatz eines Contentmanagementsystems (CMS) wie Imperia „hinter“ den Seiten vollzogen werden, da hier Layout und Inhalt der Webseiten getrennt verwaltet werden und deshalb bei einem Layoutwechsel nur die Layoutinformationen ausgetauscht werden müssen. Das CMS verbindet dann die bisherigen Inhalte mit dem neuen Layout und erzeugt auf diese Weise die neuen tabellenlosen Seiten.

Da sich beim Wechsel vom tabellengesteuerten zu einem tabellenlosen Box-Modell-Layout nur die „innere Programmierung“ der Webseiten, nicht aber ihr äußeres Erscheinungsbild ändert, sind die neuen Seiten von „außen“ kaum von den bisherigen zu unterscheiden. Erst ein Blick in den Quelltext offenbart die Unterschiede.

*Wer heute noch kein Contentmanagementsystem (CMS) verwendet, wird für einen solchen Wechsel in der Regel jede Webseite neu schreiben müssen. Alle Nutzer von Imperia im Bereich der Universität Münster kann dies relativ unberührt lassen. Das ZIV und die zentrale Online-Redaktion übernehmen die notwendigen Arbeiten für sie fast unbemerkt und im laufenden Betrieb, ohne dass sich im Workflow irgendetwas ändert.*

Die Umschaltung auf das tabellenlose Layout wird unter Imperia über den neuen Rubrikparameter „barrierefrei“ gesteuert. Durch diese Parametersteuerung müssen nicht alle Webseiten auf einen Schlag umgestellt werden, sondern können schrittweise und für jede Einrichtung getrennt in das neue Layout überführt werden.

Jeder Anwender kann seine Webseiten umstellen, indem er in einer Rubrik, in der er das Administrationsrecht besitzt, den Parameter „barrierefrei“ auf den Wert „1“ setzt und dann alle Dokumente dieser Rubrik und der darin enthaltenen Unterrubriken auffrischt. Sicherheitshalber sollten die neuen Webseiten beim Auffrischen zunächst nur auf dem Entwicklungssystem erzeugt und noch nicht freigeschaltet werden (d. h. als Aktion nach dem Auffrischen „Dokument der Freischaltliste hinzufügen“ auswählen). Vorsichtige Anwender können dies auch erst in einer Unterrubrik an einzelnen Dokumenten testen und dann schrittweise ihren gesamten Rubrikenbaum einbeziehen.

Danach sollte der größte Teil der Webseiten im neuen Layout erzeugt sein. Da die Umstellung seitens des ZIV noch nicht in allen Details abgeschlossen ist, werden einzelne Seiten, für die die erforderliche neue Strukturinformation noch fehlt, weiterhin im bisherigen Layout erzeugt. Dies betrifft zur Zeit vor allem die Webseiten, für deren Erzeugung selbstkreierte HTML-Bausteine der Form „bereich\_XX\_baustein“ eingesetzt werden. Für diese nur vereinzelt verwendeten Bausteine müssen dann Ersatzbausteine geschrieben werden.

Sollten nach dem Auffrischen aus einem von uns noch nicht berücksichtigten Grund die Webseiten verunstaltet sein, reicht es den Parameter „barrierefrei“ auf den Wert „0“ zu setzen und die Webseiten erneut aufzufrischen.

In allen Fällen, in denen die Umstellung nicht reibungslos vonstatten geht, kann sich jeder Imperia-Nutzer natürlich an seine gewohnten Ansprechpartner wenden.

## Neues von der Zertifizierungsstelle

R. Perske

**Neuer Mitarbeiter, neue Schlüssel, neue Wege zum X.509-Zertifikat, neue WWW-Seiten.**

Zum Jahreswechsel gab es erhebliche Umstellungen bei der Zertifizierungsstelle der Universität Münster (WWUCA).

Auch mein ZIV-Kollege Oliver Winkelmann ist jetzt bei der übergeordneten DFN-PCA als Mitarbeiter der WWUCA akkreditiert, so dass sich jetzt zwei ZIV-Mitarbeiter um die Aufgaben der WWUCA kümmern. Sie können bei allen Fragen rund um die Zertifizierung ihn ebenso ansprechen wie mich.

Der Verwendungszeitraum für den zuletzt verwendeten PGP-Zertifizierungsschlüssel endete mit Ablauf des Jahres 2005. Der Schlüssel selbst und die damit ausgestellten Zertifikate bleiben natürlich gültig. Für die Jahre 2006 bis 2007 wurde ein neuer Zertifizierungsschlüssel generiert, die technischen Daten finden Sie im Abschnitt Fingerprints in diesem [inforum](#). Ansonsten gibt es im PGP-Bereich keine Änderungen: PGP- und GnuPG-Schlüssel können gleichermaßen zertifiziert werden.

Ebenfalls mit Ablauf des Jahres 2005 endete auch der Verwendungszeitraum des X.509-Zertifizierungsschlüssels der WWUCA, auch hier bleiben natürlich die ausgestellten Zertifikate für die im jeweiligen Zertifikat angegebene Dauer gültig.

X.509-Zertifikate können sowohl für SSL/TLS-geschützte Zugänge zu WWW-, E-Mail- und sonstigen Servern ausgestellt werden als auch für Personen, welche mit S/MIME signierte und verschlüsselte E-Mails senden und empfangen oder Programmobjekte signieren möchten. (S/MIME ist in vielen gängigen E-Mail-Programmen wie Mozilla Thunderbird oder Microsoft Outlook standardmäßig eingebaut.)

Leider war das Verfahren zur Erzeugung eines Schlüsselpaares und eines X.509-Zertifizierungsantrages sehr kompliziert, so dass X.509-Zertifikate in der Universität bislang praktisch ausschließlich für WWW-, E-Mail- und NetNews-Server verwendet wurden. Zum Jahreswechsel wurde daher die bisherige Methode zum Ausstellen von X.509-Zertifikaten aufgegeben und auf den vom DFN neu angebotenen Dienst DFN-PKI-2 umgestellt. Der vom DFN in unserem Auftrag betriebene Zertifizierungsserver ist unter der Adresse <https://pki.pca.dfn.de/wwuca/pub> zu erreichen.

Dramatisch vereinfacht wird dadurch allen unseren Nutzern der Weg zu einem persönlichen X.509-Zertifikat: Es bedarf jetzt nur noch einiger Mausklicks, um sich ein persönliches Schlüsselpaar zu generieren und dessen Zertifizierung zu beantragen. Sobald eine dabei ausgedruckte WWW-Seite persönlich (wegen Ausweiskontrolle) bei einem WWUCA-Mitarbeiter abgegeben wurde, erhalten Sie das Zertifikat.

Beim Ausstellen von Server-Zertifikaten betreffen die Verbesserungen im Wesentlichen nur das organisatorische Umfeld (die vorbereiteten Zertifizierungsanfragen werden jetzt über eine sichere WWW-Verbindung übermittelt, nur noch das Antragsformular muss persönlich übergeben werden) und die interne Arbeit der Zertifizierungsstelle.

Die neuen Zertifizierungsrichtlinien im Rahmen der *Public Key Infrastructure* des DFN im von uns verwendeten Sicherheitsniveau "Classic" legen die gleichen Qualitäts- und Sicherheitsstandards fest wie die bisher verwendeten Richtlinien; d. h. Zertifikate werden nur ausgestellt, wenn die Identität des Zertifikatnehmers durch Kontrolle des Personalausweises oder ein gleichwertiges Verfahren verifiziert wurde.

Die WWW-Seiten der WWUCA unter <http://www.uni-muenster.de/WWUCA/> oder (zertifiziert) <https://www.uni-muenster.de/WWUCA/> wurden zu Jahresbeginn komplett überarbeitet und im Universitätsdesign neu gestaltet. Gleich auf der Titelseite finden Sie die Zertifikate der DFN-PCA und der WWUCA zum Import in Ihren WWW-Browser und in Ihr E-Mail-Programm. Wenn Sie diese Zertifikate importiert haben, dann werden diese Programme bei Zugriffen auf die abhörsicheren WWW-Server („mein ZIV“, „perMail“ u. v. a. m.) und SSL-/TLS-geschützten E-Mail- und NetNews-Server keine irritierenden Warnmeldungen über unbekannte Zertifizierungsstellen mehr ausgeben.

Ausführlich bebilderte Anleitungen helfen Ihnen nicht nur beim Import der Zertifikate, sondern zeigen insbesondere auch, wie Sie mit verschiedenen WWW-Browsern und E-Mail-Programmen X.509- und PGP-Zertifikate beantragen und nutzen können.

Bei Fragen und Anregungen können Sie uns gerne unter ☎ 83-31590 (zu üblichen Dienstzeiten – Gleitzeitregelung) oder ✉ [ca@uni-muenster.de](mailto:ca@uni-muenster.de) ansprechen.

# ZIV-Präsentation

## Energiesparen leicht gemacht

Maximilian Goth, Dieter Oberle

**Dieser Artikel wurde uns freundlicherweise von den Autoren, Mitarbeitern des Rechenzentrums Universität Karlsruhe, zur Verfügung gestellt. Die angegebenen Zahlen sind natürlich nur Anhaltspunkte, wenn man sie auf unsere Universität übertragen möchte.**

### Tipps für PC-Nutzer

Die geschätzte Anzahl der Arbeitsplatz-PCs im Büro- und Ausbildungsbereich an der Universität Karlsruhe liegt nach dem Überblick des Rechenzentrums bei ca. 12.000 Geräten. Jedes davon verbraucht im Betriebszustand einschließlich Bildschirm im Durchschnitt ungefähr 200W. Die Gesamtleistung beträgt damit ca. 2.400 KW. Um eine solche Leistung bereitzustellen, sind beispielsweise zwei moderne Windräder mit je 1,2 MW Leistung erforderlich.

Werden diese Geräte alle rund um die Uhr betrieben, wie das häufig aus verschiedenen Gründen der Fall ist, sei es, um Zeit fürs neue Hochfahren zu sparen oder die Datensicherung außerhalb der Bürozeiten erledigen zu lassen oder aber um laufende Programme nicht zu unterbrechen, kommen schnell 57.000 KWh pro Tag zusammen. Bei einem Preis von 0,1 €/KWh sind das sage und schreibe rund 5.700 Euro Stromkosten pro Tag. Werden die Wochenenden noch mitgezählt, fallen rund 2,1 Mio. Euro Stromkosten pro Jahr an. Geht man davon aus, dass nur etwa die Hälfte der Geräte tatsächlich genutzt wird, dann handelt es sich immer noch um einen Betrag von gut 1 Mio. Euro im Jahr. Legt man die gesamten Stromverbrauchskosten der Universität, die 3,6 Mio. Euro im Jahr 2003 betragen, zugrunde, so dürfte es sich dabei um eine realistische Schätzung handeln.

Würde also jeder PC-Arbeitsplatz nur zwölf Stunden am Tag genutzt und dann abgeschaltet, könnte die Universität ca. 500.000 Euro im Jahr sparen!

Doch wie kann das erreicht werden?

Zunächst sollte bei der Beschaffung neuer Hardware auch der Stromverbrauch nicht außer Betracht gelassen werden. Wer achtet denn heute schon bei der Auswahl seiner Produkte auf diesen Aspekt? Was zählt, ist das Verhältnis von Leistung und Preis, und auch die Beschaffungsrichtlinien der Universität orientieren sich an diesen Größen.

Mehr Rechenleistung bedeutet in den meisten Fällen aber auch einen höheren Stromverbrauch. Bedenkt man, dass sich die meisten Computeranwendungen im Büroalltag auf Internet- und Office-Applikationen beschränken, so ist dafür sicher nicht die neueste Highend Hardware mit superschneller Grafik und möglichst hoher CPU-Taktfrequenz notwendig. Notebooks sind im Übrigen die sparsamsten Systeme, denn die sind auf Batteriebetrieb und lange Laufzeiten getrimmt. Da kann dann lässig auch noch ein externer TFT-Bildschirm dazugerechnet werden.

Verschiedene Analysen haben ergeben, dass gerade moderne High-Performance-Grafikkarten sich als regelrechte Stromfresser entpuppt haben. Hierbei hat sich gezeigt, dass eine Standard-Grafikkarte bis zu 60W weniger Leistung verbraucht wie eine leistungsfähige 3D-Variante. So eine passiv gekühlte Karte mit beispielsweise 64MByte Speicher hat keinerlei Schwierigkeiten, mit entsprechenden Standardaufgaben klar zu kommen. Für 3D-Spiele, Animationen und CAD-Anwendungen ist sie dann allerdings nicht geeignet. Ein herkömmlicher Röhrenmonitor hat bei einem PC-System sehr viel Anteil am

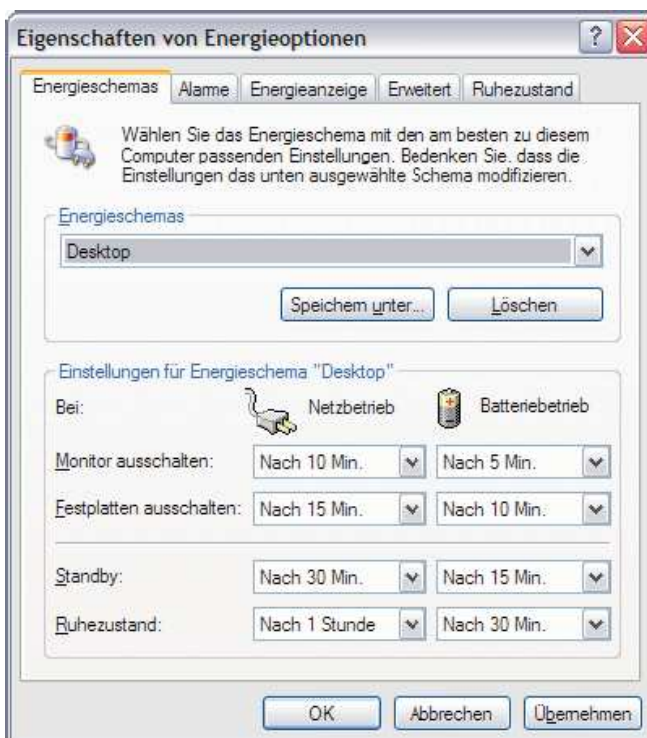


Abb. 1: So könnte eine sinnvolle Einstellung für einen Desktopbetrieb aussehen. Die Option Batteriebetrieb kann in diesem Fall einfach ignoriert werden.



Abb. 2: Stromfressende Bildschirmschonereinstellung, besser „Schwarzer Bildschirm“ auswählen.

Gesamtverbrauch. Moderne TFT-Bildschirme können den Systemverbrauch leicht um mehr als 70W senken. Das ist immerhin etwa ein Drittel des gesamten durchschnittlichen Stromverbrauchs. Auch das häufige Ein- und Ausschalten eines TFT-Bildschirmes stellt kein Problem für die Technik mehr dar und geht nicht zu Lasten der Lebensdauer. Noch eine Anmerkung zu den wunderschönen Bildschirmschonern. Wenn Sie unter dem Menü „Systemsteuerung“ -> „Anzeige“ unter „Bildschirmschoner“ eine aktive Variante auswählen und einsetzen bzw. einen externen aktiven Bildschirmschoner verwenden, hat Ihr Rechner etwas zu tun, das heißt das Bild muss ständig berechnet und ergänzt werden. Dies führt automatisch zu einem höheren Stromverbrauch des Prozessors und des Prozessors auf der Grafikkarte. Bestimmte komplexe Bildschirmschoner erhöhen sogar den Stromverbrauch Ihres Rechners nicht unerheblich. Daher wird empfohlen, einfach den schwarzen Bildschirm zu nutzen, das schont das Display und den Geldbeutel der Uni!

Alle aktuellen Mainboards (Hauptplatine des Computers) verfügen heute über die Grundvoraussetzung zur Steuerung des Power-(Energie)management-Systems. Es gibt derzeit zwei Standards:

- Advanced Power Management (APM) als das ältere und
- das aktuelle Advanced Configuration and Power Interface (ACPI).

Neben der geeigneten Hardwareauswahl steht außerdem eine weitere, sehr simple Variante des Stromsparens zur Verfügung: Die softwaregesteuerten Energie- Optionen, welche schon seit längerer Zeit in die Windows-Betriebssystem-Versionen integriert sind.

Als Beispiel seien hier die Einstellungsmöglichkeiten bei WindowsXP aufgeführt. Diese erreicht man im Menü „Systemsteuerung“ -> „Energieoptionen“. Hier können verschiedene Energieschemen definiert und eingestellt werden. Das Verhalten der Festplatte(n), des Monitors und des gesamten Systems unter bestimmten vorgegebenen Voraussetzungen kann festgelegt und entsprechend dem persönlichen Bedarf optimiert werden. Es kann eingestellt werden, nach welcher Zeit der Inaktivität der Rechner in den Standby-Modus wechselt oder in den „Ruhezustand“ (Hibernation) geht. Letzterer muss allerdings bei den meisten Desktop-PCs noch aktiviert werden. Dies geschieht durch ein einfaches Setzen des Häkchens unter „Ruhezustand“.

Im Standby-Modus werden einige Peripheriegeräte abgeschaltet, wobei sämtliche Speicherinformationen noch im flüchtigen RAM vorhanden bleiben. Würde es nun zu einer plötzlichen Stromunterbrechung kommen, wären die Daten, die vorher noch nicht gesichert wurden, verloren.

Dieser Modus eignet sich für kürzere Arbeitsunterbrechungen wie Mittagspausen oder Meetings. Die Reaktivierung kann durch einen Druck auf die Tastatur bzw. durch Mausbewegung erfolgen. Der Rechner ist sofort wieder betriebsbereit. Im Ruhezustand wird

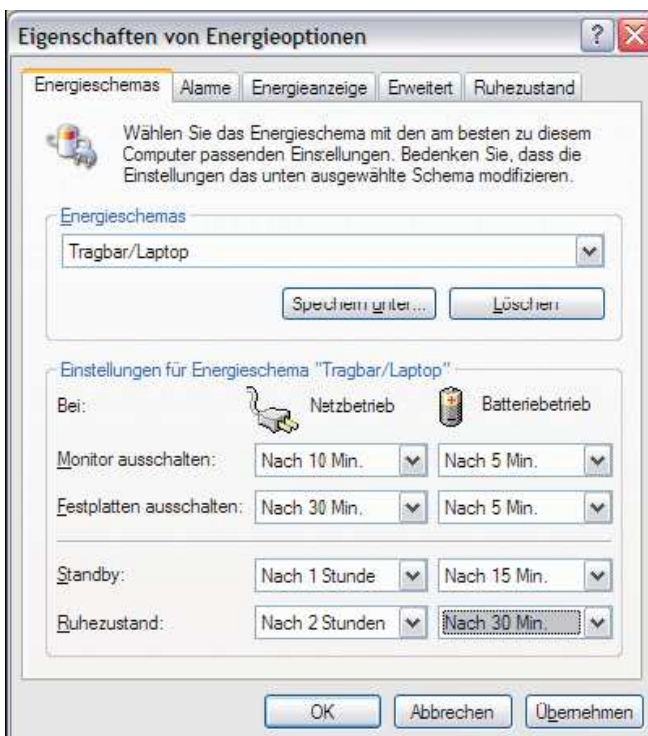


Abb. 3: So könnten sinnvolle Einstellungen für ein Notebook aussehen.

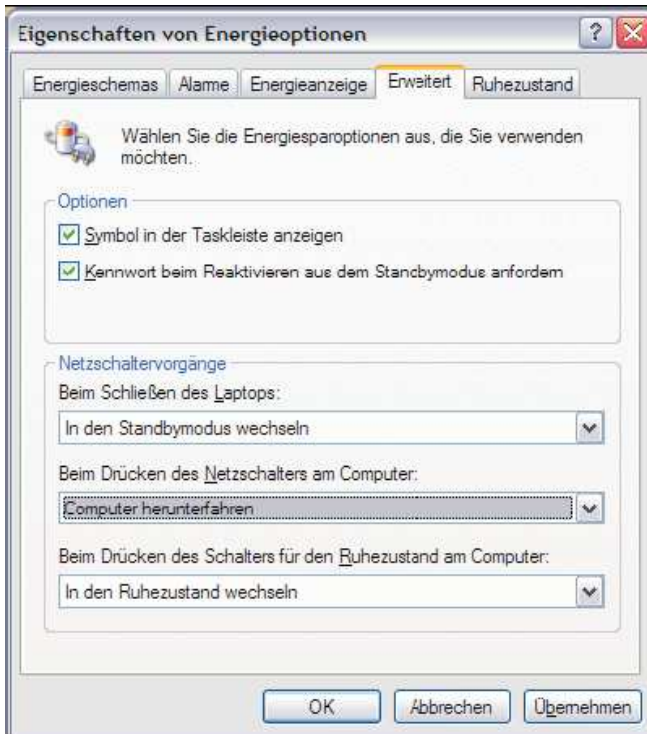


Abb. 4: Die Aktionen beim Ausschalten des Computers können auch unter „Erweitert“ eingestellt werden. Ebenso die Option für die Reaktivierung mit Kennwortschutz. Das ist nebenbei auch ein wichtiger Beitrag zur IT-Sicherheit. Wenn jemand in Ihr leer stehendes Büro kommt, ist Ihr Computer damit vor einem Zugriff Fremder geschützt. Natürlich kann diese Option auch ohne das Energiemanagement genutzt werden.

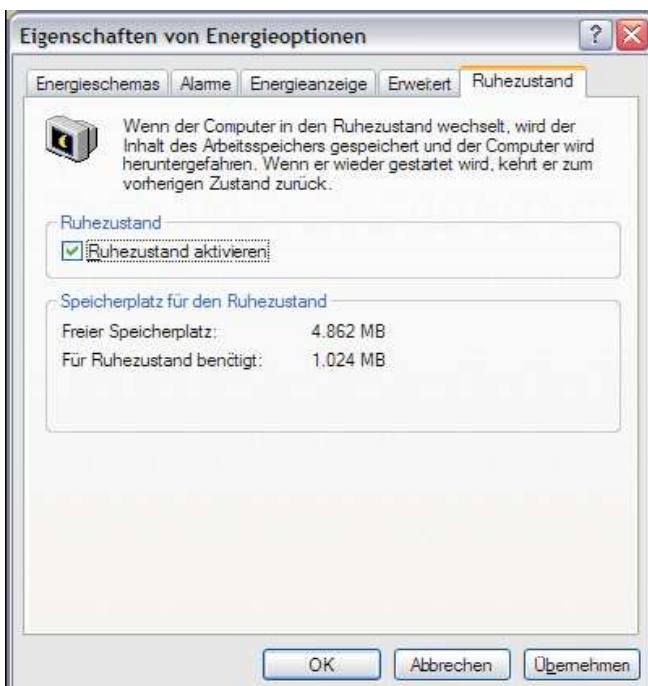


Abb. 5: Das „Häkchen“ für die Aktivierung des Ruhezustandes muss vom Administrator gesetzt werden, ein normaler Nutzer kann das leider nicht. Sprechen Sie Ihren Administrator daraufhin an!

ein komplettes Speicherabbild auf die Festplatte geschrieben. Das hat den Vorteil, dass der PC komplett heruntergefahren werden kann. Bei Wiedereinschalten des Gerätes kann der ursprüngliche Zustand wieder hergestellt werden. Das Hochfahren dauert dabei etwas länger als die Reaktivierung aus dem Standby-Modus und ähnelt dann einem normalen Bootvorgang. Man kann also verlustfrei dort weitermachen, wo man mit dem Arbeiten aufgehört hat. Dieser Modus empfiehlt sich zum Beispiel für längere Pausen oder nach Feierabend.

Diese ganzen Modi können natürlich auch direkt „von Hand“ ausgewählt und sofort aktiviert werden. Wenn man auf das Menü „Start“ -> „Herunterfahren“ verzweigt, wird neben den Optionen wie „Herunterfahren“, „Neu Starten“ noch die Auswahl „Standby-Modus“ angezeigt.

Hat man zuvor den „Ruhezustand“ unter den Energieoptionen aktiviert, so kann durch Drücken bzw. Halten der Shift-Taste noch zusätzlich die Option „Ruhezustand“ selektiert werden.

Grundsätzlich müssen alle Komponenten in einem PC den APM/ACPI-Standard erfüllen, sonst ist eine reibungslose und fehlerfreie Verwendung der Energiesparoptionen nicht möglich.

Es kann deshalb sein, dass auch dann, wenn man ein aktuelles modernes System verwendet und beispielsweise eine alte Steckkarte oder andere alte interne Komponenten verwendet, die den Standard nicht erfüllen, dass die Nutzung der Optionen „Ruhezustand“ bzw. „Standby“ nicht möglich sind.

Ein ausgeschalteter PC verbraucht nach wie vor noch ca. 5W Strom, da das Stromversorgungsteil des PC im Standby-Modus verharrt. Der Einsatz einer ausschaltbaren Steckdosenleiste, an die der komplette Computer samt Monitor und Peripherie angeschlossen wird, bietet eine einfache aber sehr effektive Möglichkeit bei längerer Nichtbenutzung des PCs auch diesen Verbrauch zu unterbinden. Gleiches gilt auch für alle sogenannten Steckernetzteile in Verbindung mit Peripheriegeräten, für Drucker und Scanner oder dergleichen.

Grundsätzlich gilt: Nur wirklich vom Stromnetz getrennte Verbraucher konsumieren keinen Strom! Das gilt auch für moderne PCs und andere intelligente elektronische Systeme. Wie bereits erwähnt, können ältere Komponenten, die nicht standardkonform sind, zur Unterbindung der beschriebenen Optionen beitragen. Dies kann dann auch zu folgenden Fehlfunktionen führen:

- Der Rechner lässt sich aus dem Standby bzw. Ruhezustand nicht mehr reaktivieren.
- Der Rechner hängt sich bei Aktivierung einer der Modi auf.

- Das Bild ist nach der Reaktivierung aus einem der Modi verändert.
- Die Netzwerkverbindung ist unterbrochen.
- Die WLAN-Verbindung lässt sich nicht mehr herstellen.

Sicher kann diese Liste noch beliebig erweitert werden, entsprechend den zahlreichen, möglichen Kombinationen von Hardwarekomponenten eines PCs.

Am zuverlässigsten funktioniert die Nutzung der verschiedenen Einstellmöglichkeiten bei Notebooks und PCs von Markenherstellern, da hier alle Komponenten auch im Sinne der Energiesparoptionen aufeinander abgestimmt sind. Es lohnt sich also, auch einmal andere Schwerpunkte bei der Auswahl zu setzen.

Weitere Informationen unter:

<http://www.zdnet.de/enterprise/client/0,39023248,391198216,00.htm>,  
<http://www.physnet.uni-hamburg.de/energie/aktuell/02042002.html>,  
<http://www.energyoffice.org/>,  
<http://www.triga.de/power2/powermanagement-Standards.htm>.

Dieter Oberle, ☎. -2067, ✉: [oberle@rz.uni-karlsruhe.de](mailto:oberle@rz.uni-karlsruhe.de).

## Professionelles Systemmanagement mit SMS an der WWU

*Dr. Weber-Steinhaus*

**Professionelles Systemmanagement ist für eine effiziente IT-Struktur unerlässlich. Mit dem SMS-Server 2003 kann dies universitätsweit umgesetzt werden.**

Die Notwendigkeit eines professionellen Systemmanagements für die Betreuung von Arbeitsplatzrechnern an der Universität ist heute unbestritten. Nahezu jeder an der Universität arbeitet rechnergestützt und ist damit auf eine stabile und sichere Systemumgebung angewiesen.

Auch wenn viele Nutzer ein hohes Maß an EDV-Kompetenz besitzen, ist es nicht deren vornehmliche Aufgabe, Rechner einzurichten und Programme aufzuspielen. Dies gilt auch dann, wenn manchem die Auseinandersetzung mit seinem PC mehr Freude bereitet als die eigentliche Arbeit. Der Arbeitsplatzrechner ist damit nicht Gegenstand der Forschung, sondern Hilfsmittel für Forschung, Lehre und Verwaltung. Auch Sicherheitsaspekte gebieten es, dass Nutzer nicht als Administratoren ihrer eigenen Arbeitsplatzrechner fungieren.<sup>1</sup> Da die Nutzer nun nicht mehr selbst Hand anlegen sollen, ist die Installation und Pflege der Arbeitsplatzrechner eigens den dafür zuständigen Administratoren übertragen worden.

### Die technischen Hürden in der Vergangenheit

Da die IVVen bei der Masse der zu betreuenden Rechner nicht bei jedem Gerät einzeln Hand anlegen wollten, gab es bereits etliche Versuche, Installation und Softwareverteilung zu automatisieren. So gab es in der IVV 3 schon zu Zeiten von OS/2 Ansätze, mit „Wininstall“ Software zu paketieren und zu verteilen, was mehr schlecht als recht funktionierte. Auch der Ansatz mancher IVVen, Arbeitsplatzrechner zu klonen, war nicht von durchschlagendem Erfolg gekrönt. Selbst bei einem koordinierten Hardwareerwerb sind die Rechnerkomponenten in den meisten Fällen nicht hinreichend homogen, um mit einem Image auszukommen. Das Clonerverfahren war im Ergebnis damit schwer verwaltbar. Auch die ersten Versionen des Systems Management Servers (SMS) der Firma Microsoft waren nicht praxistauglich.

Insgesamt musste man also enttäuscht feststellen, dass der PC als „persönlicher Computer“ und „stand-alone-Gerät“ nicht gut aus der Ferne aufgesetzt und administriert werden konnte.

<sup>1</sup> Vgl. nur *Ost*, Erfahrungsbericht: XP als Hauptbenutzer, in [info<sup>rum</sup>](#) Nr. 3/2005.

## Bessere Zeiten

Nachdem Microsoft das Thema „Systemmanagement“ zunächst mit den ersten Versionen von SMS nur zögerlich angegangen war, verbesserte sich mit der Verfügbarkeit des Active Directory und dem Erscheinen der Betaversion von SMS 2003 die Situation nachhaltig. In einem vom ZIV organisierten Workshop stellte ein Microsoft-Schulungspartner die neue Version ausführlich vor. Obwohl noch im Betastadium befindlich, war damals bereits zu erkennen, dass mit diesem Produkt professionelles Systemmanagement realisiert werden kann.

Dies veranlasste die damals eingerichtete SMS-AG den Beschluss zu fassen, dieses Produkt universitätsweit einzusetzen. Zudem wurde betont, dass angesichts der Komplexität der Thematik der Einsatz divergierender Systeme unbedingt zu vermeiden sei.

Auch das Aufsetzen neuer Rechner über das Netz ist gelöst. Mit dem „Remote-Install-System“ (RIS) kann man die Grundinstallation nunmehr weitgehend automatisieren, wobei unterschiedliche Hardware individuell konfigurierbar ist.

Dem Beschluss entsprechend nahm die IVV 3 die Arbeit auf. Nach der Grundinstallation über RIS wird hier Software mittels SMS auf die Arbeitsplatzrechner der Fakultät überspielt. Zudem leistet SMS wertvolle Hilfe u. a. bei der Fernwartung und der Inventarisierung. Gleiches gilt für das ZIV, die IVV 5 und das UKM, die SMS ebenfalls erfolgreich einsetzen.

Im vergangenen Jahr wurde die Thematik durch den Landesrechnungshof erneut aufgegriffen, nachdem dieser die Qualität der IT-Dienstleistungen an der Universität näher unter die Lupe genommen hatte. Der Landesrechnungshof stellte fest, dass die Universität kaum Gebrauch von heutzutage üblichen Managementsystemen macht und dies insbesondere im Bereich der Softwareverteilung nicht hinnehmbar sei. In dem Bericht des Landesrechnungshofes heißt es: *„Eine vollautomatisierte Betriebssystem- und Softwareinstallation gibt es bis auf eine Ausnahme grundsätzlich nicht“*<sup>2</sup>

Um dieser Kritik des Landesrechnungshofes den Wind aus den Segeln zu nehmen, trat die SMS-AG wieder zusammen, um zu klären wie man möglichst umgehend und universitätsweit Systemmanagement einführt. Neben dem Microsoft-Produkt SMS wurde der Einsatz von Tivoli erwogen, im Ergebnis aber verworfen und dafür erneut die Präferenz für SMS ausgesprochen. Vielfältige Funktionen wie die systemnahe Integration in die Windows- und Active-Directory-Umgebung, Mandantenfähigkeit und Skalierbarkeit sowie hoher Verbreitungsgrad und geringe Lizenzkosten waren hierbei entscheidende Gesichtspunkte.

## Universitätsweite SMS-Koordination

Um auch den Bereichen, die sich bislang noch nicht tiefgehend mit SMS auseinandergesetzt haben, einen Einstieg – in das zugegebenermaßen komplexe Produkt SMS – zu bieten, hat die IVV 3 Anfang dieses Jahres einen zweiten SMS-Workshop veranstaltet, an dem Administratoren der Universität und des Oberverwaltungsgerichtes Nordrhein-Westfalen teilgenommen haben.

Mit dem SMS-Workshop der IVV 3 wurde die Arbeit der universitätsweiten SMS-AG konsequent fortgesetzt. Einerseits konnten die IVVn, die bereits einen SMS-Server betreiben, sich über ihre Erfahrungen und konkreten Problemlösungen austauschen. Andererseits konnten Abteilungen, die einen SMS-Server planen, praktische Erfahrungen sammeln. So schnürten die Teilnehmer eigene Softwarepakete und verteilten diese auf die Computer des Workshop-Netzes. Weiterhin wurde eine noch engere Zusammenarbeit beschlossen, da sich zahlreiche Synergieeffekte im Rahmen der Softwarepaketstellung erzielen lassen.

---

<sup>2</sup> Prüfung der IT-Services und IT-Schulungen an den Hochschulen, Bericht des Landesrechnungshofes, Az II A-2004-8-1 vom 28. April 2005, S. 24.

Die Paketierung kann je nach Software mit erheblicher Arbeit verbunden sein. Ist das Paket aber erst einmal erstellt und getestet, kann es allen Einrichtungen der Universität für eine problemlose Verteilung zur Verfügung gestellt werden.

Die IVV 3 bietet hierfür eigens die folgende Website an:

<http://www.jura.uni-muenster.de/go/organisation/ivv/projekte/sms.html>

Diese Seite bietet für alle SMS-Administratoren der WWU und solche, die es werden wollen, erste Hinweise und Kontaktmöglichkeiten. Es heißt dort:

- Unter der Rubrik: „Kontakte“ finden Sie Ansprechpartner an der WWU, die bereits erfolgreich einen SMS-Server betreiben.
- Unter der Rubrik: „geschnürte Pakete“ können Sie nachschauen, welche IVV bereits die Arbeit für Sie erledigt hat und Ihnen zusätzliche Informationen bieten kann.
- Unter der Rubrik: „Diskussionsforum“ finden Sie Hinweise zur Nutzung des BSCW-Servers, der ein Forum zu SMS bereithält.
- Unter der Rubrik: „SMS-Share“ können Sie lauffähige Installationspakete für SMS herunterladen.
- Unter der Rubrik: „Links“ finden Sie Hinweise auf weiterführende Links zum Thema „Software-Verteilung mit SMS“.
- Unter der Rubrik: „Literatur“ finden Sie Hinweise auf weiterführende Literatur zum Thema SMS.

### Die Insellösung

Nicht unerwähnt bleiben soll, dass in der IVV 7 ein eigener Weg eingeschlagen wurde und ein Produkt namens openSAM eingesetzt wird.<sup>3</sup> Zur Begründung wird die Einsparung von Lizenzgebühren genannt. Wenn man bedenkt, dass auch der Einsatz von Personal Kosten verursacht, Programme gepflegt und weiterentwickelt werden müssen, kann man bei eigenen Lösungen bald an Grenzen stoßen. Zudem wird das Rad hier überflüssigerweise noch einmal erfunden. Weiterhin dürfte es auch zweifelhaft sein, ob dieses Rad rund läuft, wenn man bedenkt, dass selbst Microsoft mehrere Jahre gebraucht hat, die vielfältigen Funktionalitäten von SMS zu entwickeln, die eine weltweite Systembetreuung ermöglichen.

So ist SMS derart tiefgehend mit dem Active Directory verwoben, dass sogar ein universitätsumfassender Einsatz praktikierbar ist. Das hierfür notwendige Rechtemanagement ist in SMS vorhanden, das beispielsweise die Delegation der Administration auf Untergruppen ermöglicht. Von daher braucht nicht jeder, der lediglich Software über SMS verteilen möchte, einen eigenen SMS-Server. Hardware- und Systembetreuungskosten können somit minimiert werden. Neben der campusweiten Softwareverteilung bietet SMS über das Inventarisierungsmodul die Option, Investitionsplanungen auf eine sichere Datenbasis zu stellen. Auch hier beschränkt sich die Erfassung nicht lediglich auf den Bereich einer IVV, sondern kann universitätsweit betrieben werden.

Bei dem Einsatz verschiedener Systeme können diese weitergehenden Funktionalitäten keine Wirkung entfalten, obwohl ihnen im Rahmen der „total costs of ownership“ (TCO) ein hoher Stellenwert beizumessen ist.

Eine effiziente IT-Infrastruktur darf sich demnach nicht an einer vermeintlich billigen Insellösung orientieren, sondern sollte das gesamte IT- und Organisationsumfeld der Universität berücksichtigen und alle eingesetzten Mittel ins Verhältnis zum erzielten Ergebnis setzen. Ein gemeinsames Systemmanagement eröffnet daher ein enormes Potential, IT-Know-How an der Universität auszutauschen und weit reichende Synergieeffekte zu erzielen. Der Beschluss, gemeinsam SMS einzusetzen, ist damit zugleich Meilenstein in der praktischen Umsetzung des IT-Konzeptes der Universität.

<sup>3</sup> Vgl. Software-Verteilung leicht gemacht, Münster Universitätszeitung, 1. Februar 2006, S. 4.

## Das Angebot steht

Die Universität braucht für ihre IT eine professionelle Managementumgebung. SMS bietet die notwendige Funktionalität, ist hinreichend ausgereift und getestet. Der organisatorische Rahmen ist ebenfalls vorhanden. Das Angebot braucht lediglich aufgegriffen zu werden. Auf Alleingänge sollte hingegen verzichtet werden.

## HIPEC II

### *High Performance Computing Nordrhein-Westfalen*

*Arbeitskreis der Leiter von Rechenzentren an wissenschaftlichen Hochschulen des Landes Nordrhein-Westfalen (ARNW)*

**Ein kooperatives Versorgungskonzept für das Hochleistungsrechnen in den Hochschulen des Landes**

**Eine Stellungnahme des Arbeitskreises der Leiter von Rechenzentren an wissenschaftlichen Hochschulen des Landes Nordrhein-Westfalen (ARNW)**

### **Ein Konzept zur mittel- und langfristigen Entwicklung des High Performance Computing in NRW**

Für Hochschulen in Nordrhein-Westfalen ist neben einer generell leistungsfähigen Informations- und Kommunikationsinfrastruktur (IuK-Infrastruktur) insbesondere die Verfügbarkeit von Rechnern für das High Performance Computing (HPC) ein entscheidender Differenzierungsfaktor im nationalen und internationalen Wettbewerb.

Das hier vorgelegte „Kooperative Versorgungskonzept für das Hoch- und Höchstleistungsrechnen in den Hochschulen des Landes“ ermöglicht den Hochschulen, die Investitionsplanung in diesem Segment der IuK-Infrastruktur auf eine gesicherte Planungsbasis zu stellen. Damit ist keine feste Mittelzusage verbunden, da einerseits das entsprechende Antrags- und Begutachtungsverfahren des Hochschulbauförderungsgesetzes (HBFUG) abgeschlossen sein muss und andererseits das Ministerium an die Vorgaben des Haushaltsgesetzgebers gebunden ist. Allerdings führt der skizzierte Abstimmungsprozess dazu, dass ein fachlich positiv begutachteter und empfohlener Beschaffungsantrag mit hoher Wahrscheinlichkeit realisiert werden kann. Weiterhin versetzt es Hochschulen in die Lage, durch das Partizipieren an einem Verbund Ressourcen zu nutzen, die eine Hochschule für sich alleine nicht oder nur unter großen Anstrengungen hätte beschaffen können.

Die vorgelegte Konzeption bietet Instrumentarien und Wege, die vorhandenen Ressourcen ökonomisch zu nutzen. Dies gelingt vor allem durch die starke Präferenzierung des Verbund- bzw. Kooperationsgedankens.

### *Rechnerausstattung*

Die Heterogenität der Rechnersysteme in den Hochschulen des Landes hat sich bewährt. In den letzten Jahren hatte sich eine Konvergenz hin zu Linux- oder Open Source Unix (z. B. Solaris) basierten SMP-Clustern ergeben; aber in letzter Zeit werden von den großen Rechnerherstellern auch wieder stark auf bestimmte Anwendungsklassen zugeschnittene Architekturen auf den Markt gebracht. Beispiele sind das Niagara-Design von Sun mit massivem Multithreading, „field programmable gate arrays“-Erweiterungen von Intel Chips durch Cray, massiv-parallele Gitterrechner wie Blue Gene von IBM oder Vektorrechner auf einem Chip wie der Cell-Prozessor von IBM/Sony. Deshalb ist es im HPC-Bereich auch in Zukunft weiterhin wichtig, Anwendungsanforderungen mit Hardware-Möglichkeiten sinnvoll abstimmen zu können.

Vor diesem Hintergrund ist es Ziel des kooperativen Versorgungskonzeptes, zukünftig sowohl eine ausgewogene Rechnervielfalt auf aktuellem technischen Niveau zu erhalten, wie auch sicherzustellen, dass durch eine entsprechende Größe der Ressourcen der wissenschaftliche Mehrwert maximiert und der Betriebsaufwand minimiert wird. Dabei soll die Beschaffung im Rahmen der skizzierten verstetigten Investitionsplanung erfolgen.

Für die Nutzung der Hoch- und Höchstleistungsrechner ist eine adäquate Ausstattung mit geeigneter Software auf allen Ebenen der sog. Rechnerpyramide notwendig. Für die kommerzielle Software wird die Beschaffung im Rahmen des HFBG-Verfahrens angestrebt, wenn dies durch die Bündelung der Nachfrage sinnvoll möglich ist. Dies bedeutet aus Landessicht den Erwerb von entsprechenden Landeslizenzen für alle Hochschulen des Landes. Verschiedene in den letzten Jahren durchgeführte koordinierte Software-Beschaffungen zeigen, dass unabhängig von der Art der Software diese Bündelung zu äußerst vorteilhaften Konditionen führt, die selbst großen Hochschulen auf sich allein gestellt nicht eingeräumt worden wären.

Auch muss sichergestellt werden, dass durch geeignete Mechanismen die für die Nutzung paralleler Rechner notwendige Anwendungs- und Programmierkompetenz vorhanden ist, um Anwender in der Nutzung von HPC-Ressourcen zu unterrichten und vorausschauend den Markt zu sondieren. Hierdurch wird die Eigenentwicklung von Software im Bereich des Hoch- und Höchstleistungsrechnens unterstützt und der Einsatz von personellen und finanziellen Ressourcen im HPC-Umfeld optimiert.

### *Investitionsmodell*

#### • **Ist-Analyse**

Der Menge und Vielfalt der Hochschulen des Landes steht eine Knappheit der Ressourcen beim Land und den Hochschulen gegenüber. Unter Ressourcen sind hierbei Investitions- und Personalmittel, sowie konsumtive Mittel zu verstehen. Die Bereitstellung von investiven Mitteln wird häufig mit der Darstellung eines entsprechenden Bedarfes oder einer strategischen Bedeutung verbunden. Da es sich in der Regel um einmalige Ausgaben handelt, lassen sich in diesem Bereich jedoch verhältnismäßig gut Mittel zur Verfügung stellen – auch wenn es dabei mitunter zu einer zeitlichen Verzögerung oder einer Streckung kommt. Weitaus größere Problemfelder sind die konsumtiven und die Personalmittel. Beide werden aus den Globalhaushalten der Hochschulen bestritten, die durch den Qualitätspakt von Kürzungen ausgenommen sind. Allerdings ist auch nicht mit einer Erhöhung der Mittelansätze in den Hochschulhaushalten zu rechnen. Im Rahmen der Finanzautonomie unterliegen diese Haushalte der Bewirtschaftung durch die Hochschulen.

Das wesentliche Element des kooperativen Versorgungskonzeptes für das Hochleistungsrechnen ist eine verstetigte Investitionsplanung zwischen den Hochschulen des Landes. Hierzu werden zunächst die geplanten Investitionen bzw. Reinvestitionen für einen Planungszeitraum, der in der Größenordnung von ein bis zwei Jahren liegen sollte, gesammelt und mit Prioritäten versehen. Die von den Hochschulen daraufhin eingereichten Beschaffungsanträge werden vom Ministerium unter Bezugnahme auf die Prioritätensetzung in das Begutachtungsverfahren gegeben. Nach einer entsprechenden positiven Begutachtung durch die Deutsche Forschungsgemeinschaft (DFG) und der Empfehlung des Wissenschaftsrates werden die Anträge im Rahmen der haushaltsmäßigen Mittelverfügbarkeit entsprechend ihrer Prioritätenreihenfolge bedient. Zum Ende des jeweiligen Planungs- bzw. Realisierungszeitraumes werden den Hochschulen entsprechende Ergebnisberichte bekannt gegeben.

Grundsätzlich gibt es aber für die Hochschulen keinen Zwang zur Antragstellung und auch keinen Automatismus der Mittelbereitstellung. Allerdings erhalten die Hochschulen so die Möglichkeit, die Versorgung mit einer Komponente der Rechnerpyramide, nämlich dem Hochleistungsrechner, auf der Basis einer gesicherten Planung zu realisieren. Im Gegenzug erklären sich die Hochschulen bereit, Kapazitäten dieses Rechners planbar und mit definierter Dienstgüte auch anderen Hochschulen des Landes zur Nutzung freizugeben. NRW hat dazu mit dem Ressourcenverbund NRW (RV-NRW) einen geeigneten organisatorischen und technischen Rahmen. In diesem Verbund werden Dienste der Hochschulrechenzentren landesweit verfügbar gemacht. Damit erhalten auch Hochschulen mit geringerer personeller, maschineller und/oder finanzieller Ausstattung insbesondere auch die Möglichkeit, ihren Wissenschaftlern und Forschern entsprechende Rechenkapazität anbieten zu können. Diese dynamische Planung ermöglicht es, den Erfordernissen der Hochschulen und des Landes gerecht zu werden.

## • Umsetzung

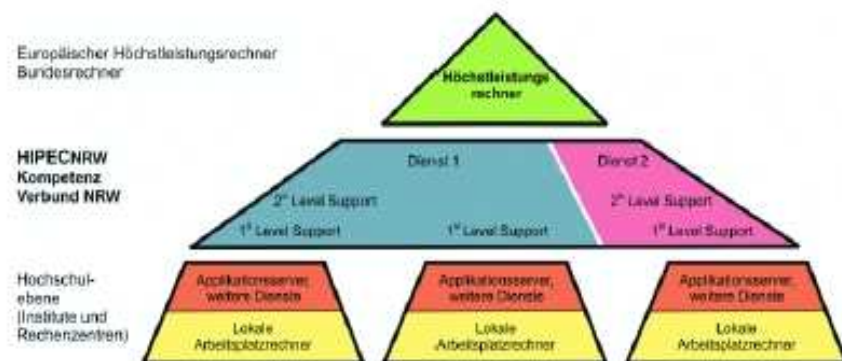
Zur Umsetzung dieses Investitionsmodells bedarf es entsprechender Absprachen zwischen den Hochschulen und dem Ministerium. Dabei müssen die Terminvorgaben des HBFVG-Verfahrens berücksichtigt werden. Das Modell der verstetigten Investitions- und Beschaffungsplanung stellt sich in einer chronologischen Abfolge prinzipiell wie folgt dar:

1. Der DV-Infrastrukturausschuss erarbeitet alle zwei Jahre eine strategische Konzeption, die u. a. die geplanten Investitionen/ Reinvestitionen für die nächsten zwei Jahre enthält.
2. Nach Abstimmung mit dem Ministerium wird den Hochschulen dieser Entwurf mitgeteilt.
3. Danach reichen die Hochschulen für die Investitionsplanung des Folgejahres ihre entsprechenden Anträge ein. Im Regelfall soll dies bis zum 31.03. des laufenden Jahres erfolgen.
4. Die Anträge werden vom Ministerium gesammelt, geprüft und mit Prioritätenfolge an die DFG weitergeleitet.
5. Sofern eine ausreichende Anzahl an Anträgen vorliegt, wird eine Prüfung im Rahmen von nur einer Gutachtersitzung angestrebt. Wünschenswert wäre der Abschluss der Begutachtung bis zum 30.10. des laufenden Jahres.
6. Sofern das Begutachtungsverfahren positiv abgeschlossen wird, kann dann die Beschaffung des Hochleistungsrechners im Rahmen der gesetzlichen Vorgaben eingeleitet werden.
7. Der DV-Infrastrukturausschuss wird über den Ausgang der Begutachtungsverfahren und der abgeschlossenen Beschaffungen einmal jährlich informiert.

## Rahmenbedingungen

Zur fachlichen Ausgestaltung gehört die Beschreibung der folgenden Rahmenbedingungen:

- Netzinfrastruktur,
- Organisation des Betriebs und der Nutzungsarten,
- Zugangsvoraussetzungen,
- Zugangsregelungen,
- Verlässlichkeit der Dienstleistung,
- Bildung von Nutzergruppen.



Rechnerversorgungspyramide in einem Kompetenzverbund

## Zahlenrätsel

Günter M. Ziegler

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 Textstellen, vielleicht bemühen Sie eine Suchmaschine. Die Auflösung finden Sie im nächsten

**infoforum** oder bei [www.mathekalender.de](http://www.mathekalender.de).

Was Zahlen so alles zählen können, sieht man an der folgenden Sammlung: Lauter Zitate aus bekannten und unbekannteren Büchern, Gedichten, Texten, Liedern:

### Tunnel

Um den Berg herum schlängelten sich verschiedene Wege mit kleinen Brücken und Durchfahrten. Außerdem gab es auch noch ein kurvenreiches Eisenbahngleis. Es lief durch  $x/1$  Tunnel, die kreuz und quer durch den Berg und seine beiden Gipfel führen.

### Jahre

Am darauffolgenden Freitag ging er wieder zu den Barkassen. Und wie alle Freitage kehrte er ohne den erwarteten Brief nach Hause zurück. «Wir haben genug gewartet», sagte an jenem Abend seine Frau zu ihm. «Man muss deine Viechsgeduld haben, um  $x/2$  Jahre lang auf einen Brief zu warten»

### Sinne

O du, Geliebte meiner  $x/3$  Sinne, ich liebe dir! – Du deiner dich dir, ich dir, du mir. – Wir?

Das gehört [beiläufig] nicht hierher.

Wer bist Du, ungezähltes Frauenzimmer?

### Saucen

Sie erklärte, dass sie  $x/4$  verschiedene Fischsaucen zu bereiten verstehe, – sie habe den Mut, dafür einzustehen, obgleich ihr eigener Mann sie gewarnt habe, davon zu sprechen. „Sprich nicht davon!“ habe er gesagt. „Niemand wird es dir glauben, und wenn man es glaubt, so wird man es lächerlich finden!“ Und doch wolle sie es heute einmal sagen und offen bekennen, dass es  $x/4$  Fischsaucen seien, die sie machen könne.

### Männer

Ich hab schon  $x/5$  Männer  
 Ins kühle Grab gebracht,  
 Erst hab ich mir mit Henna  
 Die Haare rot gemacht.  
 Dann wollt' ich auch mal blonde  
 Dann warn sie wieder grün;  
 Ich bin die hysterischste Ziege von ganz Berlin.

### Köpfe

Zu H\*\*\* K\*\*\*, dem Denkenden, kam ein falscher Schüler und erzählte ihm: «In Amerika gibt es ein Kalb mit  $x/6$  Köpfen. Was sagst Du darüber?» H\*\*\* K\*\*\* sagte: «Ich sage nichts.» Da freute sich der falsche Schüler und sagte: «Je weiser du wärest, desto mehr könntest du darüber sagen.»

Der Dumme erwartet viel. Der Denkende sagt wenig.

### Töchter

Es war einmal ein König, der hatte  $x/7$  Töchter, eine immer schöner als die andere. Sie schliefen zusammen in einem Saal, wo ihre Betten nebeneinander standen, und abends, wenn sie darinlagen, schloss der König die Türe zu und verriegelte sie. Wenn er aber am Morgen die Türe aufschloss, so sah er, dass ihre Schuhe zertanzt waren, und niemand konnte herausbringen, wie das zugegangen war.

**Jahre**

Der König ist  $x8$  Jahre alt.  
 $x8$  Jahre und schon der Staat.  
 Er schaut, wie aus einem Hinterhalt,  
 vorbei an den Greisen vom Rat

**Meter**

Ein Mathematiker hat behauptet,  
 dass es allmählich an der Zeit sei,  
 eine stabile Kiste zu bauen,  
 die  $x9$  Meter lang, hoch und breit sei.

**Brote**

Und J\*\*\* sprach zu ihnen: Wie viele Brote habt ihr? Sie antworteten:  $x10$  und ein paar Fische.

Gefragt ist die Summe  $x1 + x2 + x3 + x4 + \dots + x10$

**Antwortmöglichkeiten:**

1. 42
2. 68
3. 792
4. 809
5. 1117
6. 1118
7. 1122
8. 1132
9. 1978
10. 2005

Günter M. Ziegler, 1963 in München geboren, ist Professor für Mathematik an der TU Berlin. Seine Arbeitsgruppe beschäftigt sich mit „Diskreter Geometrie“, besonders mit der Geometrie von Flächen, Kachelungen und Polyedern. Gemeinsam mit Martin Aigner von der FU Berlin hat er Das BUCH der Beweise geschrieben. Im Matheon ist er für die Bereiche „Diskrete Mathematik und Optimierung“ und „Visualisierung“ mitverantwortlich.

**Ostereier**

*E. Sturm*

Nachdem für ein Computerspiel neulich einige Tricks bekannt geworden waren, die zu „erweitertem Spielspaß“ verhelfen, sind jetzt auch bei seriöser Software Nebenwirkungen herausgekommen, nämlich bei der bekannten Web-Programmiersprache PHP.

Unter der Webadresse

<http://www.netzeitung.de/internet/376669.html>

konnte man nachlesen, wie's geht.

Also, man nehme irgendeine Webadresse, die sich auf ein PHP-Programm bezieht, und hänge etwas kryptische Parameter dahinter, etwa

`https://cgi.uni-muenster.de/exec/ZIV/zivintro.php?=PHPE9568F36-D428-11d2-A769-00AA001ACF42`



Dann erscheint doch tatsächlich der nebenstehende Hund! Ich habe nicht lange nachgedacht, aber aus mir unerfindlichen Gründen erhält man bei der Adresse

`http://web20spot.de/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42`

mit demselben Code einen anderen Hund!

Wer will, kann mal im PHP-Quellcode nachschauen, PHP ist ja Open-Source-Software. Bekannt sind auch noch zwei Logos (keine Hunde!), die man erhält, wenn man jeweils folgenden Code hinter eine PHP-Adresse schreibt:



`?=PHPE9568F34-D428-11d2-A769-00AA001ACF42`

`?=PHPE9568F35-D428-11d2-A769-00AA001ACF42`

Es verwundert nicht, dass die Autoren auch ihre eigenen Namen preisgeben bei folgendem Parameter:

`?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000`

Solche geheimen „credits“ gab's auch schon beim seligen OS/2, dort in Verbindung mit Flamingos.

Übrigens, am 1.4. haben die angegebenen Adressen noch funktioniert!

Nein wirklich, es ist kein Aprilscherz!

## ZIV-Lehre

### Veranstaltungen in der Vorlesungszeit (Sommersemester 2006) 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. Weitere Informationen unter <http://www.uni-muenster.de/ZIV/Lehre/>.

- |               |  |  |
|---------------|--|--|
| <b>260081</b> | <b>Programmieren in Perl</b><br>Dienstag 13-15 Uhr<br>Hörsaal: ZIV-Pool 3, Einsteinstr. 60,  | Küfer, T.  |
| <b>260096</b> | <b>Einführung in MySQL</b><br>Donnerstag 9-11 Uhr<br>Hörsaal: ZIV-Pool 3, Einsteinstr. 60,   | Leweling, M.   |
| <b>260100</b> | <b>Dynamische Webseiten mit PHP, XML und MySQL für Fortgeschrittene</b><br>Mittwoch 9-11 Uhr<br>Hörsaal: M4, Einsteinstr. 64,                    | Sturm, E.  |
| <b>260115</b> | <b>Kommunikationssysteme: IT-Sicherheit und Überwachung von IT-Infrastruktur</b><br>Donnerstag 14-16 Uhr<br>Hörsaal: Raum 206, Röntgenstr. 9-13, | Richter, G.<br>Forsmann, A.<br>Kamp, M.<br>Speer, M.<br>Wessendorf, G. |
| <b>260120</b> | <b>Internet-Protokoll Version 6 (IPv6): Grundlagen und Praxis</b><br>Montag 14-16 Uhr<br>Hörsaal: Raum 206, Röntgenstr. 9-13                     | Schild, C.   |
| <b>260134</b> | <b>Kolloquium des Zentrums für Informationsverarbeitung</b><br>Freitag 14-16 Uhr<br>Hörsaal: Raum 206, Röntgenstr. 9-13                          | Held, W.   |

## Veranstaltungen in der vorlesungsfreien Zeit (August–Oktober 2006) 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 ab 1. Juli 2006 möglich.

- |               |   |               |
|---------------|---|---------------|
| <b>260149</b> | <b>Sicher ins Internet</b><br>vom 18.09. bis 22.09.2006,<br>Mo-Fr 10-17 Uhr<br>Hörsaal: ZIV-Pool 3, Einsteinstr. 60                                   | Perske, R.    |
| <b>260153</b> | <b>Publizieren mit LaTeX</b><br>vom 04.09. bis 15.09.2006,<br>Mo-Fr 9-16 Uhr<br>Hörsaal: ZIV-Pool 3, Einsteinstr. 60                                  | Bucher, D.    |
| <b>260168</b> | <b>Präsentieren mit LaTeX</b><br>vom 09.10. bis 13.10.2006,<br>Mo-Fr 9-16 Uhr<br>Hörsaal: M4, Einsteinstr. 64   | Kaspar, W.    |
| <b>260172</b> | <b>Programmieren in Java</b><br>vom 18.09. bis 29.09.2006,<br>Mo-Fr 9-11 Uhr<br>Hörsaal: M4, Einsteinstr. 64  | Süselbeck, B. |
| <b>260187</b> | <b>Multimedia-Praktikum</b><br>vom 02.10. bis 13.10.2006,<br>Mo-Fr 9-16 Uhr<br>Hörsaal: MM-Räume, Einsteinstr. 60                                     | Scheffer, A.  |
| <b>260191</b> | <b>Paralleles Rechnen und Grid Computing</b><br>vom 18.09. bis 22.09.2006,<br>Mo-Fr 10-13 Uhr<br>Hörsaal: Raum 206, Röntgenstr. 9-13                  | Leweling, M.  |
| <b>260206</b> | <b>Betriebssystem Linux/Unix: Einführung und Grundlagen</b><br>vom 02.10. bis 13.10.2006,<br>Mo-Fr 10-16 Uhr<br>Hörsaal: ZIV-Pool 3, Einsteinstr. 60. | Grote, M      |
| <b>260210</b> | <b>Systemadministration für Linux-Systeme</b><br>vom 25.09. bis 29.09.2006,<br>Mo-Fr 9-16 Uhr<br>Hörsaal: ZIV-Pool 2, Einsteinstr. 60                 | Hölters, J.   |

- 260225 Administration eines Windows-Systems** Kämmerer, M.  
vom 28.08. bis 01.09.2006,  
Mo-Fr 9-16 Uhr  
Hörsaal: ZIV-Pool 3, Einsteinstr. 60
- 260230 Systemadministration für Windows-Server in einer Active Directory Umgebung** Lange, W.  
vom 25.09. bis 29.09.2006, Winkelmann, O.  
Mo-Fr 10-16 Uhr  
Hörsaal: ZIV-Pool 3, Einsteinstr. 60

## Kommentare zu den Veranstaltungen

### 260081 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 und grafische Oberflächen 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 Prozeduren. Weitere Schwerpunkte sind die Behandlung der regulären Ausdrücke, die Benutzung der Perl-Module (z. B. CGI und DBI) und die objektorientierte Programmierung mit Perl.

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

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

### 260096 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.

**260100 Dynamische Webseiten mit PHP, XML und MySQL 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 sowie die Nutzung von XML.

**260115 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) realisierbaren 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
- 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, Leistungszustände, Überwachung von Netzdiensten wie z. B. DNS
- Event-Verarbeitung
- Visualisierung von Netzwerken

**260120 Internet-Protokoll Version 6 (IPv6): Grundlagen und Praxis**

Das neue Internet-Protokoll in der Version 6 (IPv6) ist dazu gedacht, das mittlerweile in die Jahre gekommene alte IP-Protokoll (in der Version 4) abzulösen. Nachdem IPv6 ursprünglich lediglich den leidigen Adressmangel von IPv4 lösen sollte, sind in der Protokollentwicklung viele neue Features hinzugekommen, die dieses grundlegende Protokoll bereichern.

Da IPv6 das alte IPv4 nicht schlagartig ablösen, sondern schrittweise ersetzen soll, existieren neben dem Protokoll selbst zahlreiche Mechanismen, die den sanften Übergang ermöglichen. Sie garantieren die Kommunikation zwischen den beiden Adressierungsarten und erleichtern die Migration zu IPv6.

Das neue Protokoll hat sich langsam aber sicher seinen Weg in viele aktuelle Betriebssysteme und Anwendungen erschlichen. Wie für ein tief in den Protokollschichten vergrabenes Protokoll zu erwarten, ist dies fast unbemerkt vom Anwender geschehen. An vielen praktischen Beispielen läßt sich zeigen, wo IPv6 schon überall Fuß gefasst hat.

Die Vorlesung behandelt demnach im Allgemeinen:

- Aufbau und Funktionsweise des neuen Protokolls
- Neue Verfahrensweisen mit IPv6
- Migrations- und Integrations-Mechanismen
- Aktueller Status und Verbreitung von IPv6
- Fortgeschrittene Weiterentwicklungen an und um IPv6

Da IPv6 in vielen Schichten des Internets wichtig ist, werden im Verlauf des Kurses viele allgemeine Themen zum Internet und dessen Funktionsweise angesprochen. So werden während der Vorlesung ganz nebenbei auch allgemeine Verfahren im und am Internet erklärt.

Teilnahmevoraussetzungen: Folgendes Grundwissen ist für den Kurs hilfreich, aber nicht zwingend notwendig. Fehlendes Wissen läßt sich leicht während der Vorlesung zusammen erarbeiten:

- TCP/IP
- OSI-(Schicht-)Modell

Die Vorlesung kann je nach Bedarf der Kursteilnehmer auf einen anderen Termin verschoben werden, daher bitte unbedingt den Termin für die Vorbesprechung beachten. Wer zur Vorbesprechung nicht erscheinen kann, sollte sich gerne per E-Mail beim Dozenten informieren.

#### **260134 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.

#### **260149 Sicher ins Internet**

Das Internet birgt neben seinen unendlichen Möglichkeiten auch zahlreiche Gefahren und Fallstricke, welche häufig selbst für Fortgeschrittene nur schwer zu erkennen sind. Diese Veranstaltung richtet sich in Form eines Praktikums an PC-Nutzer, die schon mal eine E-Mail verschickt haben. Die Teilnehmer lernen an bereit gestellten „virtuellen“ Rechnern konkret, wie man mit dem eigenen Rechner das Internet sinnvoll, sicher und geschützt nutzen kann. Kernpunkte sind die Absicherung des eigenen Rechners, sicheres Surfen im WWW (inkl. Homebanking) und vertrauenswürdige E-Mail.

#### **260153 Publizieren mit LaTeX**

LaTeX ist ein mächtiges und flexibles Satzsystem, das sich besonders für wissenschaftliche und technische Publikationen eignet. Autoren können aus einer Vielzahl von fertigen Layouts auswählen und diese eigenen Vorstellungen anpassen. Mit speziellen Komponenten, z. B. zur Erzeugung von PDF-Dateien, können LaTeX-Publikationen für die Veröffentlichung auf CD-ROM oder im Internet vorbereitet werden. Das komplette Satzsystem ist frei erhältlich und steht praktisch auf allen verbreiteten Betriebssystemen zur Verfügung.

In dieser Veranstaltung werden die Grundkonzepte und wichtigsten Erweiterungen von LaTeX vorgestellt, u. a.

- die Komponenten des Satzsystems,
- allgemeine Dokument- und Textstrukturen,
- Formeln, Tabellen, Grafiken und
- die Erzeugung von PDF-Dokumenten,

und wie hiermit ordentlich strukturierte und typografisch ansprechende Dokumente erstellt werden können. Voraussetzung für diese Veranstaltung sind Grundkenntnisse im Umgang mit Pcs.

#### **260168 Präsentieren mit LaTeX**

LaTeX ist vor allem als ein TeX-Makropaket zur Herstellung hervorragend gesetzter Bücher bekannt. Dass aber schon die erste LaTeX-Version aus dem Jahre 1985 eine Dokumentklasse für die Herstellung von Overheadprojektorfolien enthielt, dürfte weniger bekannt sein. Dabei ist es für Arbeiten, die mit LaTeX gesetzt wurden, recht naheliegend, auch für die Präsentation LaTeX zu verwenden, um z. B. Text oder Formeln direkt übernehmen zu können. Inzwischen sind weitere LaTeX-Klassen entwickelt worden, mit denen anspruchsvolle Präsentationen erstellt und als pdf-Dateien mit dem Adobe Reader überall gezeigt werden können.

In dieser Veranstaltung wird die LaTeX-Klasse „beamer“ vorgestellt, die unter anderem eine schrittweise Anzeige des Seiteninhalts, wie z. B. Formelteile, und die Herstellung eines Handouts aus den Präsentationstexten unterstützt.

#### **260172 Programmieren in Java**

Java ist eine objektorientierte Programmiersprache, die inzwischen weltweit große Verbreitung gefunden hat und sich weiterhin dynamisch entwickelt. Sie basiert auf dem Konzept einer virtuellen Maschine, die es ermöglicht, Anwendungen für unterschiedliche Plattformen ohne Neuübersetzung zu entwickeln, und verfügt über eine sehr umfangreiche Klassenbibliothek, die ständig erweitert wird. Grundkenntnisse in Java sind für die Softwareentwicklung in vielen Bereichen unbedingt erforderlich.

Die Vorlesung bietet eine Einführung in die objektorientierte Programmierung anhand von Java. Sie ist auch für Hörer/innen ohne Vorkenntnisse im Programmieren geeignet.

#### **260187 Multimedia-Praktikum**

Das Praktikum führt in die elementaren Techniken der Bildgewinnung und deren Präsentation ein. Es besteht aus einem vorbereitenden theoretischen Teil, der vorab im Internet veröffentlicht wird, und einem Praktikumsteil. Im theoretischen Teil werden unter andere folgende Themen behandelt:

- Die Grundlagen der Gewinnung eines digitalen Fotos (Bayer-Muster) o Algorithmen zur Umwandlung von Bayer-Mustern in Fotos
- Die Qualität digitaler Bilder (Modular Transfer Function)
- Grundlagen der Farbenlehre o Bildbearbeitungsalgorithmen (Farbumfang, Schärfung usw.)
- Bildformate (Jpeg, Tiff, Gif usw.)
- Kurzeinführungen in die verwendeten Standardprogramme (Photoshop, Acrobat usw.)
- Schrittweise Arbeitsanleitungen für die Experimente des praktischen Teils

Im praktischen Teil werden die Hörer/innen Erfahrung im Umgang mit Flachbett-Scannern, Dia-Scannern, digitalen Kameras, Videokameras und Webcams gewinnen. Gleichzeitig wird auch die Präsentation des gewonnen Bildmaterials als Druckausgabe, Photo-CD, Video-CD und DVD trainiert. In Experimenten wird behandelt:

- Die Gewinnung von gerasterten Bildern (von Druckvorlagen); Gerät: Flachbettscanner; Präsentation: Druck
- Die Gewinnung von Bildern mit kontinuierlicher Farbverteilung (von Photos); Gerät: Dia-Scanner; Präsentation: Druck
- Die Bildgewinnung mit einer digitalen Kamera; Präsentation: Still-Video-CD
- Die Bildgewinnung mit einer digitalen Video-Kamera (d. h. Filmerstellung); Präsentation: Video-CD
- Die Durchführung einer Video-Konferenz; Gerät: Webcam; Präsentation: Bildschirm

Die Teilnehmer des Praktikums arbeiten bei diesen Experimenten in den Multimedia-Räumen des ZIV und in Gruppen von maximal drei Personen. Die Experimente werden von den Mitarbeitern des ZIV betreut. Dem praktischen Teil angegliedert sind Einführungen zu den Themen:

- Filmsprache und -gestaltung (findet im Servicepunkt Film statt)
- Digitaler Videoschnitt an professionellen Schnittplätzen (findet im Servicepunkt Film statt)
- Digitale Spiegelreflex-Fotografie

Die Teilnehmer des Praktikums legen ein Praktikumsbuch an. Das Praktikum erfordert eine Voranmeldung. Auf Grund der eingeschränkten Räumlichkeiten ist die Teilnehmerzahl beschränkt. Entscheidend für die Teilnahme am Praktikum ist neben der Online-Anmeldung die Anwesenheit am ersten Praktikumstag, an dem die Gruppen eingeteilt werden.

#### **260191 Paralleles Rechnen und Grid-Computing**

Die Veranstaltung kombiniert eine Einführung in die Benutzung des Linux-Parallelrechners ZIVcluster mit einer Einführung in Grid-Computing mit dem ZIVGrid. Der ZIVcluster eignet sich insbesondere für die Ausführung parallelisierter Programme. Zu den Grundlagen der Benutzung gehören Linux, das Batch System PBS, sowie die Verwendung der installierten Compiler und Programmbibliotheken (z. B. MPI, MKL). Anhand von Beispielen wird die parallele Programmierung in Fortran erläutert. Auf der anderen Seite stellt das ZIVGrid Rechenkapazität auf ZIV-Pool-Rechnern zur Verfügung. Das ZIVGrid eignet sich für Benutzer, die serielle Programme laufen lassen wollen, und ergänzt somit das Angebot des ZIVclusters. Dabei kommt die Grid-Software Condor zum Einsatz.

#### **260206 Betriebssystem Linux/Unix: Einführung und Grundlagen**

Linux ist ein leistungsstarkes Unix-System für viele Hardware-Architekturen, das sich als preiswerte Windows-Alternative etabliert hat.

Die Vorlesung will in die Linux-Benutzung einführen. Neben einer an üblichen Unix-Einführungen orientierten Beschreibung des Unix-Datei-Systems und der wesentlichen Unix-Befehle wird die grafische Oberfläche KDE behandelt, die für viele ein Linux-System erst attraktiv macht.

**260210 Systemadministration für Linux-Systeme**

Die Vorlesung richtet sich an fortgeschrittene Linux-Anwender/innen, die Unterstützung bei der Installation und System-Integration von Linux-Systemen benötigen. Voraussetzung sind die grundlegende Kenntnisse der Unix-Kommandos.

Die Teilnehmer/innen werden in der Veranstaltung ein Linux-System selbst installieren und in die Netzwerk- und Systeminfrastruktur der Universität einbinden, dazu gehört die Nutzung eines Verzeichnisdienstes für die Account- und Nutzerinformation, sowie die Nutzung eines Kerberosdienstes zu Authentisierung. Ferner wird auch die automatisierte Installation und Parametrierung einer größeren Anzahl von Linux-Systemen behandelt.

**260225 Administration eines Windows-Systems**

Für Hörer/innen mit Windows-Vorkenntnissen werden Aufbau und Betrieb von Windows XP und Windows Server 2003 vorgestellt und gemeinsam erprobt.

Die folgenden Themen werden u. a. behandelt:

- Installation des Betriebssystems und Absicherung gegen Angriffe von außen
- Zugriffsrechte und Netz-Freigaben o Benutzer- und Gruppenverwaltung, lokale Administration
- Druck-, Datei-, Logon- und allgemeine Programm-Services
- Diagnose- und Überwachungsfunktionen
- Internet, LAN, Netz-Protokolle

Die speziellen Dienste E-Mail-, Datenbank-, Web- und Media-Server können im Rahmen dieser Veranstaltung nicht bearbeitet werden. Die Einbindung in eine Windows Active Directory Domäne wird nur am Rande erwähnt. Wir verweisen auf die weitere Veranstaltung „Systemadministration für Windows-Server in einer Active Directory Umgebung“.

**260230 Systemadministration für Windows-Server in einer Active Directory Umgebung**

Die Veranstaltung richtet sich an fortgeschrittene Windows-Benutzer, die ihre Kenntnisse mit Blick auf die Anforderungen in einem großen Rechnernetz erweitern möchten. Als Schwerpunkte sind u. a. der Aufbau und Betrieb von Servern in einer Active Directory Umgebung (Windows-Netzwerk) vorgesehen.

Themenauswahl:

- Installation und Konfiguration
- Benutzerverwaltung
- Sicherheit u. a.: Dateisystem, Registry, Netzwerk, Sicherheitsrichtlinien
- Server im Active Directory: Gesamtstrukturen, Domänenstrukturen, Domänen, Organisationseinheiten (OU), Vertrauensstellungen, Standorte, Replikation, Gruppenrichtlinien
- Softwareverteilung und Systemüberwachung

Im Rahmen der Veranstaltung wird auch Gelegenheit zu praktischen Übungen gegeben.

## ZIV-Regularia

### Fingerprints

*R. Perske*

**Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptographischen Prüfsummen der Zertifizierungsstelle der Universität Münster (WWUCA) und der obersten Zertifizierungsstelle im Deutschen Forschungsnetz (DFN-PCA)**

Im letzten **inform** haben sich beim Satz leider einige Fehler in den Fingerprints-Artikel eingeschlichen, dafür bitten wir um Entschuldigung. Um diese Fehlerquelle auszuschließen, drucken wir die Fingerprints ab dieser Ausgabe in Form einer von der WWUCA erstellten Abbildung ab.

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:89: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:rel: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/>  
F2D580B1/2048 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 B0B4 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

Liebe Leserin, lieber Leser,

wenn Sie **inforum** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **inforum** 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 **inforum**



- .....
- 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 **inforum**  
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 **inforum**-Leserdatei gespeichert werden (§ 4 DSGVO).

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift