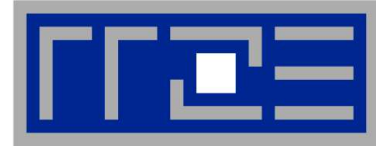


Management virtueller Hosts von Lehrstühlen und Einrichtungen

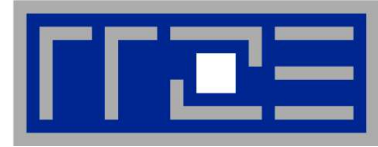
Dipl. Inf. Wolfgang Wiese

**ZKI & AMH Web-Admin-
Workshop**

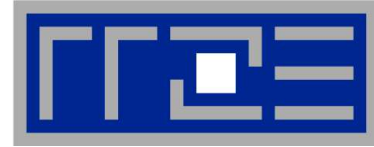
24. Juni 2003



- **Problemstellung**
 - **Kundenerwartung**
 - **Sicherheitsprobleme**
- **Lösung**
 - **Organisatorisch**
 - **Technisch**
- **Erfahrungen & Ausblick**



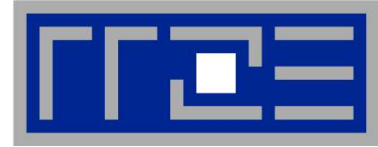
- **Hintergrund der Universität Erlangen-Nürnberg**
 - **Stark gewachsene Strukturen (insbesondere auch in Bezug auf Verantwortung und Leitung)**
 - **Dezentrales Konzept der DV-Betreuung**
 - **Im Rechnerbereich sehr heterogen:**
 - **Windows,**
 - **Linux,**
 - **MacOS,**
 - **Solaris,**
 - **HP-UX**
 - **Ca. 10.000 Angestellte (inkl.Klinikum) und ca. 35.000 Studierende**
 - **Sehr unterschiedliche Ansprüche in Bezug auf Sicherheit und Datenschutz**



- **Kundenerwartung**

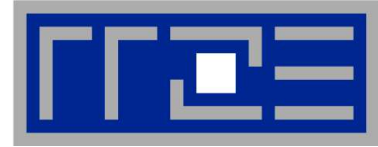
- Übliche Formen des Kundenkontakts:

- *„Wir wollen alles! Eine eigene SecondLevel-Domain unter .de, CGI, PHP, SSL, ASP, Servlets, SSI, Zugriffsstatistik und ein CMS wären das mindeste!“*
 - *„Unser Auftraggeber möchte das wir das CMS XYZ installieren, welches das Perlmodul Very::Exotic::Parser benötigt und außerdem brauchen wir aktiviertes PHP-FileUpload“*
 - *„Hilfe! Meine aus dem Netz aus irgendeiner Quelle geladenen PHP/CGI-Skripts gehen nicht!“*

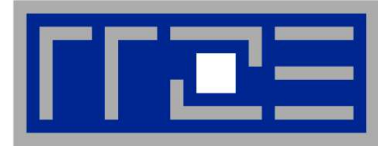


- **Es besteht Bedarf an:**
 - **Nutzung von üblichen Webtechniken (CGI, PHP, SSI)**
 - **Nutzung von Datenbanken (MySQL, Oracle, Firebird, ...)**
 - **Zugriff auf das Filesystem**
 - **Tagesaktuelle Zugriffstatistiken**
 - **Ausreichend Speicherplatz auch für große Dateien**
 - **Hohe Verfügbarkeit aller Server**
 - **Sichere Server**

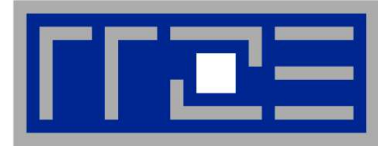
(... und dies alles am Besten als kostenloses Angebot des RZ)



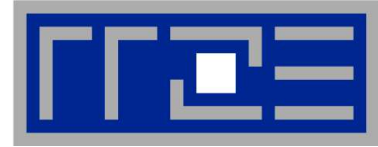
- **Aber:**
 - **Sehr unterschiedliche Wissensstände über Web-Techniken**
 - **Meist keine ausreichende Sensibilisierung gegenüber Sicherheitsprobleme**
 - **Durch Zeitverträge oft wechselnde Ansprechpartner, die meist schlecht vom Vorgänger informiert wurden**
 - **Mangelndes Wissen über einzuhaltende Standards (z.B. WAI) und Regeln (z.B. Impressumspflicht)**



- **Sicherheitsprobleme 1**
 - **CGI- und PHP- Skripts können bei schlechter Programmierung unerwünschte Aktionen auf dem Webserver auslösen:**
 - ***Remote Access Exploids*** (Zugriff aufs Dateisystem als User)
 - ***Code and Data Injection*** (Einspeisung von fremden Code oder Text auf die Website)
 - ***Cross Site Scripting*** (Übermittlung von Code, der bei anderen Besuchern der Site ausgeführt wird.)
 - **Inhaltliche Gefahren**
 - **Unkenntnis von relevanten Gesetzen fördern die Gefahr von Rechtsproblemen.**
Bsp: Impressumspflicht, Urheberrecht und Datenschutzrecht

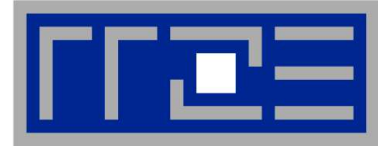


- **Sicherheitsprobleme 2**
 - **Gefährliches Halbwissen in Bezug auf Security mit PHP**
2 besonders häufige Probleme:
 - **PHP-Skripts mit MySQL, die ihre Zugangsdaten in „config.inc.php“ ablegen und nur mittels „.htaccess“ schützen, aber Zugang übers Filesystem vergessen**
 - **„SafeMode“-Irrtum. (Irrtum, das PHP-Skripten wie CGIs vom User ausgeführt werden)**
 - **„Security by obscurity“:**
Viele Kunden glauben, dass ungelinkte Dateien und Verzeichnisse sicher seien...
Bsp.: Das Verzeichnis
<http://domain/PhpMyAdmin-2.01/>



■ Organisatorisch 1

- **Mind. zwei Personen je Webauftritt müssen benannt sein: Webmaster und ViSdP. (in der Regel der Lehrstuhlinhaber)**
- **Der Webmaster muss per Mail erreichbar sein**
- **Einführung spezieller Webmaster-Accounts**
- **Regeln btrf. Einhaltung von Standards und rechtl. Rahmenbedingungen werden von der Hochschulleitung aufgestellt**
(Siehe z.B.: <http://www.uni-erlangen.de/regeln.shtml>)
 - **Darin auch enthalten: Regeln zur Nutzung von Logos und Emblemen der FAU**
 - **Rahmenbedingungen für die Gestaltung von Websites**
 - **Bei Nichtbefolgen der Regeln kann der Zugriff auf die Sites durch das RRZE gesperrt werden.**



■ Organisatorisch 2

- Klare Namensstruktur bei der Vergabe von Domainnamen:

Für Fakultätswebsites:

www.fakultaet.uni-erlangen.de

Für Lehrstühle:

www.lehrstuhl.fakultaet.uni-erlangen.de

Lehrstuhlprojekten:

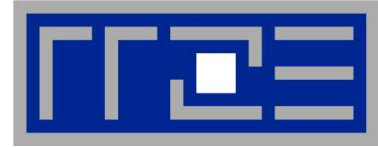
www.projekt.lehrstuhl.fakultaet.uni-erlangen.de

Oder bei überfakultäre Projekten oder bei Einrichtungen:

www.projekt.uni-erlangen.de

- Alle Domains an Lehrstühlen müssen die Endung „.uni-erlangen.de“
- Ausnahmen (alte Domains vor der Regelung) werden durch Userdruck auf neue Domainnamen

„empfohlen“

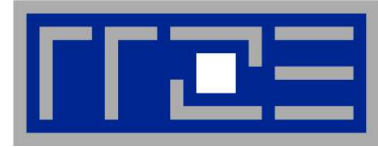


■ Technisch 1

- Konzept der virtuellen Hosts im Webserver Apache
- Standardeintrag:

```
<VirtualHost 131.188.3.67>
  ServerName www.iwr.uni-erlangen.de
  User jfdp00wm
  Group jfdpwm
  HostNameLookups off
  DocumentRoot /webbaum/www.iwr.uni-erlangen.de
  ScriptAlias /cgi-bin /cgibaum/www.iwr.uni-erlangen.de
  TransferLog /logs/apache/www.iwr.uni-erlangen.de
</VirtualHost>
```

„webbaum“ ist Platzhalter für einen über NFS gemounteten Webbereich. Hier: **/proj/websource/docs/FAU/sonst/**

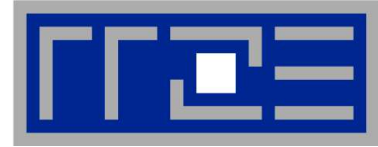


■ Technisch 2

- DocumentRoot- und CGI-Verzeichnisse werden speziell geschützt:

- Zugriff auf den Webbaum **/proj/websource** erlaubt nur für Webmaster-Accounts mit Hilfe von „NIS maps“ (net.groupID), obwohl dieser Bereich dann auf allen Server vorhanden ist.
- Zugriff auf das spezielle DocumentRoot-Verzeichnis geschützt über ACLs. Beispielsweise obige Site:

```
> getfacl /proj/websource/.../www.iwr.uni-erlangen.de
# owner: jfdp00wm
# group: jfdpwm
user::rwx
user:www:r-x          #effective:r-x
group::r-x           #effective:r-x
mask:rwx
other:---
```



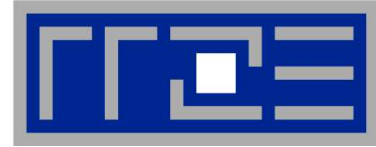
■ Technisch 3

■ Datenbankserver:

- MySQL wird wegen Probleme im Hochlastbereich und wegen schlechterer Datensicherheit nur „unsupported“ angeboten.
- Benutzern wird die Nutzung von Firebird nahegelegt wegen höherer Redundanz gegenüber MySQL.
- Datenbankserver (Software) läuft auf eigener Hardware.
- Datenbanken mit schützenswerten Daten liegen auf einem Server, der nur über den Webserver auszugreifbar ist.

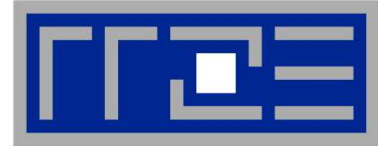
■ Kosten und Dienste:

- Campuslizenz für SSH (Zugriff mittels FTP seit Anfang 2000 deaktiviert).
- Campuslizenz für IBEExpert für Datenbank-Administration.
- Kosten je Webmaster-Account pro Jahr bei 30 Euro, zzgl. Kosten für Speicherplatzbedarf über 500 MB und Kosten für etwaige eigene SecondLevelDomains.



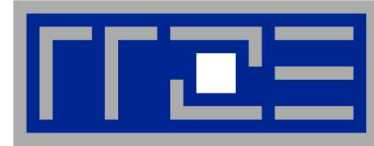
■ **Technisch 4**

- **Zugriff auf die eigentlichen Webserver ist nur Administratoren erlaubt; Benutzer können nur über die auf einem Dialogserver gemountete Bereiche zugreifen**
- **Hardware:**
 - **3 Sun Enterprise-Server für Webserver**
 - **Sun E3000 (Fallback)**
 - **Sun E450 (für Standard-Domains)**
 - **(in Kürze:) Sun Fire 280 für Domains mit besonderer Last**
 - **2 Sun Server für Datenbanken**
 - **Sun E450 für Firebird und MySQL, X500**
 - **Sun Ultra Workstation für Firebird, MySQL**
 - **Sun Ultra Workstation für Oracle**
 - **Diverse Dialog- und Homeserver**



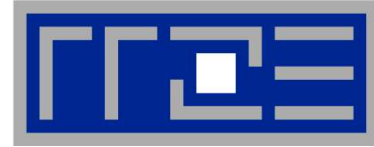
■ **Erfahrungen 1**

- **Probleme mit unsauberer Programmierung im Griff. Fehler treffen nicht mehr die gesamte Hochschule, sondern nur den einzelnen Auftritt.**
- **Aufgrund der klar erkennbaren Verantwortlichen nur noch wenig Anfragen oder Beschwerden an das RRZE**
- **RRZE tritt in Bezug auf Webauftritte nur beratend und als Providing-Dienstleister auf**
- **Providing Angebot wird stark und gern genutzt. Seit 1999 Anstieg der Websites von 16 auf über 300 . Gleichzeitige starke Abnahme von selbst gepflegten Lehrstuhl-Webservern.**
- **Weiterhin jedoch: Ständiger Schulungsbedarf**

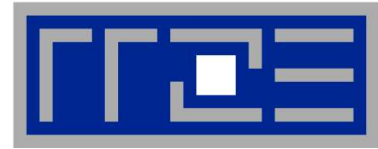


■ Erfahrungen 2

- **Einheitliches Design für die Hochschule nur teilweise realisierbar aufgrund gewachsener Strukturen.**
- **Einheitliches WCMS für alle Webauftritte politisch nicht durchsetzbar und nicht gewollt.**
Aber: Dank obiges Konzept ist jeder Lehrstuhl und jede Einrichtung in der Lage eigene CMS-Systeme zu nutzen, die mit einem Unix-basierten Webserver arbeiten.
- **Derzeit viele unterschiedliche Systeme parallel im Einsatz, die individuell auf die Lehrstühle angepasst werden konnten:**
 - **E-Learning Systeme (z.B. ILKA, VHB)**
 - **Kursverwaltungssysteme (z.B. OKTIS)**
 - **WCMS (SchemaText, Altjira, Typo3, ZOPE, OpenCMS, ...)**
 - **Spezielle Redaktionssysteme (UnivIS, Newsticker, ...)**
 - **Beliebige Skripten und beliebige Editoren**
 - **Bewährt für die zentrale Homepage: Dreamweaver MX**
- **Nutzung von Webmaster-Mailverteiler (Hieraus Anregung zu höherstufigen Verteiler: Bsp.: „AK-By-Web“)**



- **Ausblick**
 - **Starker Anstieg der Anfragen nach Webdienstleistungen und Schulungen erfordern Verstärkung des Webmaster-Teams.**
 - **Schaffung eigener Webmaster-Stellen (bzw. Stellen für „Online-Management“).**
 - **Verstärkung der Web- und Datenbankserver.**
 - **Zukünftige Web- und Internetdienste müssen berücksichtigt werden.**
 - **Standards werden immer wichtiger.
(Bsp.: **WAI**, CSS, Web-Services, RSS)**



**Vielen Dank
für Ihre
Aufmerksamkeit !**

...noch Fragen?