

# 12:3=4

mit diesem Memo können Sie 4 mal im Jahr rechnen.

## II – 2010

### Umstellung des Backup-Dienstes

Am 30. Juni wurde der alte Backup-Dienst für die RUB eingestellt. In den Wochen zuvor sind alle Kundenrechner auf den neuen UAMR-Backup-Dienst umgestellt worden. Als Backup-Software kommt jetzt Tivoli Storage Manager (TSM) von IBM zum Einsatz. Das Backup erfolgt auf leistungsfähiger Hardware ebenfalls aus dem Hause IBM. Dadurch konnten insgesamt die Backup-Kosten gesenkt werden. Außerdem ist mit TSM die Wiederherstellung von Backup-Daten jederzeit online durch den Systembetreuer möglich. Ansprechpartner bei Backup-Problemen ist weiterhin Ihr Rechenzentrum.

<http://www.rub.de/rz-backup>

### Erfolgreiche IT-Azubis

Im Juni hat unser Auszubildender zum Fachinformatiker, Alexander Klink, seine Abschlussprüfung bestanden. Bereits im Januar legte Hendrik Redder die vorgezogene Prüfung zum Fachinformatiker der Fachrichtung Systemintegration erfolgreich ab. Dazu gratulieren wir beiden herzlich! Im September werden drei neue Auszubildende die Ausbildung im Rechenzentrum beginnen. Ab sofort läuft das Bewerbungsverfahren für Herbst 2011. Voraussichtlich werden in der RUB wieder 15 Ausbildungsplätze im IT-Bereich zu besetzen sein.

<http://www.rub.de/it-ausbildung>

### [www.it.uamr.de](http://www.it.uamr.de)

Die gemeinsamen Aktivitäten der drei zentralen IT-Versorger in der UAMR sind nun auf eigenen Webseiten dokumentiert. Dort finden Sie auch eine Übersicht über die aktuell UAMR-weit verfügbaren IT-Dienste.

<http://www.uamr.de>

### Fileserverzugang außerhalb der RUB-Domäne

Der Zugang zu den Fileservern des RZ (fs-stud für Studierende und Fileservice-Dienst für Institute) ist jetzt auch außerhalb der RUB-Domäne sowie im RUB-WLAN über verbundene Netzlaufwerke möglich. Hierzu muss die Datenverbindung über einen VPN-Tunnel aufgebaut werden, siehe

<http://www.rz.rub.de/dienste/netze/vpn.html>

### Corel® PaintShop Photo™ Pro X3

Corel® PaintShop Photo™ Pro X3, das Bildbearbeitungsprogramm für passionierte Fotografen, ist eingetroffen und im Rahmen unseres Campusvertrages verfügbar. Neben einem brandneuen RAW-Editor und praktischen Stapelverarbeitungsfunktionen enthält diese umfassende Bildbearbeitungslösung Funktionen für die Fotoverwaltung, die Gestaltung kreativer Projekte, das Foto-Sharing und neu auch die Gestaltung von Diashows mit HD-Videos. Es enthält alles, was Sie benötigen, um schnell professionelle Resultate zu erzielen. Die ideale Lösung für digitale Spiegelreflexkameras!

<http://www.rz.ruhr-uni-bochum.de/dienste/software/beschaffung/firmen/corel.html>

# 12:3=4

mit diesem Memo können Sie 4 mal im Jahr rechnen.

## Terminabfragen mit UAMR-Doodle

Seit mittlerweile einem Jahr verfügt die UAMR über ein Doodle-Abo, das insbesondere werbefreie Terminabfragen ermöglicht. Die Initiatoren von Terminabfragen müssen über eine zentrale Emailadresse einer der drei UAMR-Partnerhochschulen verfügen. Die Teilnehmer an der Abfrage unterliegen dagegen keiner Einschränkung.

<http://www.it.uamr.de/uamr-doodle.html>

## Bladeserver

Seit dem Jahr 2003 bietet das Rechenzentrum Serverhosting-Dienste auf Basis von HP-Bladeservern an. Die erste Generation dieser Server wird nun außer Betrieb genommen. Die betroffenen Kunden erhalten von uns in den nächsten Wochen ein Umstellungsangebot.

<http://www.rz.rub.de/dienste/ressourcen/zs/betrieb/s-host.htm>

## Webserver-Zertifikate

Das Rechenzentrum vermittelt Webserver-Zertifikate (siehe rechts) für eine gesicherte Datenübertragung zu Ihren eigenen Webservern in der Domäne ruhr-uni-bochum.de. Wahlweise sind Zertifikate des DFN-Vereins oder der Firma Thawte erhältlich. Für letztere entstehen jährliche Kosten in Höhe von zurzeit 101 EUR. Beide Zertifikatstellen sind in die aktuellen Versionen der Standardbrowser als „vertrauenswürdige Dritte“ integriert, so dass die Zertifikate automatisch verifiziert werden.

<http://www.ruhr-uni-bochum.de/pki/>

## Haben Sie's gewusst?

### Was steckt hinter https?

Der Datenaustausch zwischen einem Webserver und einem Webbrowser per HTTP erfolgt unverschlüsselt. So werden Formulareingaben wie Bankverbindungen oder Passworte im Klartext über die Datenverbindung geschickt und können von jedem Lauscher mitgelesen werden. Zur Sicherung von Transaktionen wurde bereits für die ersten Versionen des Netscape (1994) das Verfahren SSL (Secure Socket Layer) definiert, das eine durch Verschlüsselung gesicherte Übertragung ermöglicht. Nach mehrfacher Überarbeitung wurde es im Jahre 1999 von der IETF als Standard festgelegt und in TLS (Transport Layer Security) umbenannt. Eine durch SSL/TLS gesicherte Verbindung kommt durch Voranstellen der Protokollbezeichnung https:// vor die Internetadresse zustande. Browser und Server einigen sich im sogenannten SSL-Handshake auf eine Reihe von Verschlüsselungsverfahren, die den späteren vertraulichen Datenaustausch ermöglichen. Zur Verschlüsselung kommen symmetrische und asymmetrische Verfahren zum Einsatz. Bei einer symmetrischen Verschlüsselung sind beide Partner im Besitz desselben Schlüssels. Symmetrische Verfahren, z.B. RC4, DES oder AES arbeiten sehr schnell. Das Problem besteht im vertraulichen Austausch des einen Schlüssels.

Asymmetrische Verfahren arbeiten mit zwei Schlüsseln: einem öffentlichen (public key) und einem geheimen (private key). Der öffentliche Schlüssel kann allgemein bekannt gemacht werden, denn Daten, die mit ihm kodiert worden sind, können ausschließlich mit dem privaten Schlüssel dekodiert werden. Asymmetrische Verfahren, z.B. RSA, sind langsamer als symmetrische. Die Authentizität des öffentlichen Schlüssels wird über digitale Zertifikate gewährleistet, die von vertrauenswürdigen Dritten ausgestellt werden.

Beim SSL-Handshake übermittelt der Server ein Zertifikat mit seinem öffentlichen Schlüssel an den Klienten. Der Klient überprüft das Zertifikat auf Gültigkeit und errechnet seinerseits einen symmetrischen Schlüssel, den er mit dem öffentlichen Schlüssel des Servers kodiert und an diesen überträgt. Der anschließende Datenaustausch erfolgt unter Nutzung dieses Schlüssels nach einem symmetrischen Verfahren. Der erfolgreiche Aufbau einer gesicherten Verbindung wird im Browser durch ein geschlossenes Vorhängeschloss angezeigt. Probleme beim Aufbau, z.B. ungültige Serverzertifikate, werden direkt als Warnung angezeigt. Informationen zur aktuellen Verschlüsselung erhält man im Internet Explorer durch Klick mit der rechten Maustaste in das Browserfenster und Anwahl von „Eigenschaften“, im Firefox durch Doppelklick auf das Vorhängeschloss.

## IMPRESSUM

Rechenzentrum der Ruhr-Universität Bochum  
Universitätsstrasse 150, Gebäude NAF  
D-44 780 Bochum

Telefon: +49 234 32-24001, Servicecenter: -24025

Telefax: +49 234 32-14214

E-Mail: [rz@ruhr-uni-bochum.de](mailto:rz@ruhr-uni-bochum.de)

ViSdP: Rainer Wojcieszynski

Homepage: <http://www.rz.ruhr-uni-bochum.de/>

12:3=4 erscheint vierteljährlich in einer Auflage von 1000 Exemplaren. Juni 2010