Ausgabe Dezember 2002
ISSN 1435-1684

Con nect

Zeitschrift
des Rechenzentrums
der Universität
Augsburg

Die Titelseite zeigt die Rückansicht
des Parallelrechners IBM RS/6000 SP
der Universität Augsburg.

Impressum

connect – Zeitschrift des Rechenzentrums der Universität Augsburg ◆ ISSN 1435-1684 ◆ Herausgegeben im Auftrag des Rechenzentrums der Universität Augsburg ◆ Erscheinungsdatum Dezember 2002 ◆ Auflage 1000 ◆ **Redaktion:** Dr. Leopold Eichner (verantwortlich), Dr. Annja Zahn, Dr. Markus Zahn ◆ **Layout und Satz:** Dr. Annja Zahn ◆ Herstellung Joh. Walch GmbH & Co, Augsburg ◆ **Redaktionsanschrift:** Rechenzentrum der Universität Augsburg, Universitätsstrasse 8, 86159 Augsburg, Tel. 0821/598-2000, Fax 0821/598-2028, E-Mail: *redaktion.connect@rz.uni.augsburg.de,* WWW: http://www.rz.uni-augsburg.de/connect/

Liebe connect-Leserinnen, liebe connect-Leser,

wieder ist ein Jahr für das Rechenzentrum viel zu schnell vergangen. Viele wichtige Vorhaben konnten umgesetzt werden und eine Reihe anderer Vorhaben sind auf den Weg gebracht. Und wenn wir auf unsere interne Liste mit wichtigen Projekten blicken, dann sollte sie ja eigentlich im Umfang abgenommen haben – aber das Gegenteil ist der Fall! Arbeiten wir also zu langsam oder wächst der Bedarf an zentraler Dienstleistung so stark? Schauen wir doch einmal an, was sich im zurückliegenden Jahr alles getan hat.

Erster großer Schwerpunkt – das Datennetz. Hier gab es große und kleine Sanierungsmaßnahmen, einige „Sondereinsätze“ und Planungen: Gebäude der Wirtschaftswissenschaftlichen Fakultät und der Zentralbibliothek, Informatik und Studentenwerk Eichleitnerstraße, ehemaliger Kindergarten im Mensagebäude, Poolraum in der Teilbibliothek Geisteswissenschaften, Kernkompetenzzentrum für IT & Finanzdienstleistungen, Unterstützung von Tagungen, Sportzentrum, Musikwissenschaften Schillstraße, usw. Gelohnt hat sich die Ausarbeitung eines Konzepts für die Versorgung einiger Bereiche mit einer Funknetz-Infrastruktur (Wireless LAN), denn für die Umsetzung hat das Ministerium nun am Jahresende Sondermittel bereitgestellt. Neues gibt es auch von unserem Anschluß an das Wissenschaftsnetz (G-WiN) zu berichten: die Kapazität unseres Zugangs zum G-WiN wird im Dezember von 34 MBit/s auf 155 MBit/s erhöht und ein gemeinsamer, gleichzeitig leistungsfähiger und kostensparender Clusteranschluß mit der Fachhochschule Augsburg wird eingerichtet. Für den Zugang über das normale Telefonnetz gibt es nun zusätzlich zum schon länger bestehenden Dienst „Uni@Home“ auch Verträge zu „DFN@Home“ und „DFN@Home DSL“.

Aufbauend auf der Datennetz-Infrastruktur bietet unser Rechenzentrum eine weitere wichtige, aber keinesfalls selbstverständliche, Dienstleistung. „Ein Schlüssel für alles“ ist, etwas verkürzt ausgedrückt, das Konzept, mit dem das Rechenzentrum den Zugang zu nahezu allen Basisdiensten ermöglicht. Ob Mailkennung, Einwählservice, Rechner-Logins und File- und Backupservice – jeder Dienst wird für den Nutzer über seine persönliche RZ-Benutzerkennung erschlossen. Die Zahl der eingetragenen Benutzer für diese Services ist im Jahr 2002 auf rund 15.000 gestiegen – ein überzeugender Beweis für die Akzeptanz und die Wichtigkeit dieser zentralen Dienstleistung. Ein Grundstein für eine effiziente Fortentwicklung der IT-Infrastruktur an der Universität Augsburg ist damit gelegt.

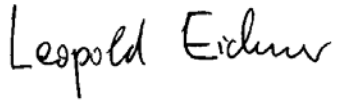
Verstärkt bemüht sich das Rechenzentrum auch um einen – im Vergleich zu anderen Universitäten wettbewerbsfähigen – Service für Studenten. Selbstverständlich sind E-Mail-Adresse und Plattenplatz, zentraler Backupservice, Internetzugang und Einwählservice. Mit einem Angebot von 86 PC-Arbeitsplätzen für Studierende ist das Rechenzentrum inzwischen der zweitgrößte Betreiber von CIP-Pools in der Universität. Die Mühe lohnt sich, denn selbst in der vorlesungsfreien Zeit ist eine hohe Auslastung der Pools zu beobachten. Ergänzt wird dieser Service für Studenten durch ein für unsere personellen Gegebenheiten großes Angebot an praktischen Kursen.

Auch ein paar Schritte in Richtung Multimedia-Unterstützung mußten wir gehen, um dem schnell wachsenden Bedarf Rechnung zu tragen. Unter der Koordination des Rechenzentrums gab es unter Ausnutzung von Fördermitteln eine deutliche Verbesserung der Hörsaalausstattung. Ein zusätzlich eingerichteter Verleihdienst für Videoprojektoren und Notebooks erfreut sich ausgesprochen reger Nachfrage. Gerne wurden großformatige Grafiken in hochwertiger Qualität auf unserem Hochleistungsplotter ausgedruckt. Nicht unerheblich war der Zeitaufwand für die Unterstützung von Videokonferenzen – hier wird es aber im kommenden Jahr Abstriche in der Dienstleistung geben müssen. Hauptsächlich zur Unterstützung des Lehrbetriebs in den neuen Studiengängen Medien und Kommunikation wird vom Rechenzentrum - zunächst probeweise im Wintersemester – ein BSCW-Server (Basic Support for Cooperative Work) in Zusammenarbeit mit der Professur für Medienpädagogik betrieben.

Ist das nun viel oder wenig? Habe ich schon von Internetdiensten, Netzüberwachung und Sicherheit gesprochen, von Hochleistungsrechnen und Visualisierung? Und von den vielen „Kleinigkeiten“ wie Softwarelizenzen, Skripte, Kleingeräte, Kabel und vieles mehr?

Wissen Sie eigentlich, daß Ihr Rechenzentrum dies alles mit einer „halben Mannschaft“ bewältigt? Wissen Sie, daß die DFG Rechnerkommission schon 1990 unsere Personalausstattung als unzureichend bezeichnet hat und eine Verdopplung für notwendig hielt? Haben Sie sich eigentlich schon einmal für die Verbesserung der Personalausstattung des Rechenzentrums eingesetzt?

Ich weiß – das Hemd ist näher als die Jacke und Sie sind genügend mit ihren Problemen vor Ort beschäftigt. Aber ohne ein dickes Fell sind Sie nicht gegen die Virenstürme dieses Winters gerüstet!



(Dr. Leopold Eichner)

Alles in bester Ordnung?

Über die Neugestaltung des Web-Auftritts der Universität Augsburg

Die Internetpräsenz der Universität Augsburg wurde gründlich überarbeitet und auch neu gestaltet. Sie ist schöner, freundlicher und moderner geworden. In diesem Beitrag stelle ich Ihnen die grundlegenden Fragen vor, die sich in diesem Zusammenhang gestellt haben – und wie diese gelöst wurden.

Bis zu 50.000 verschiedene Besucher surfen pro Monat auf die Eingangsseiten der Universität. Tendenz steigend. Informationsquelle Nummer eins über die Universität ist und bleibt das Internet. Umso wichtiger ist ein geschlossener, campusweiter Web-Auftritt. Im Arbeitskreis „Corporate Design" wurde ein einheitliches Erscheinungsbild für den Web-Auftritt konzipiert. Seit August verwandelt sich nun Schritt für Schritt bzw. Seite für Seite das Internetangebot der Universität Augsburg in ein gemeinschaftliches Ganzes.

Grundlegendes

Der Anstoss, das Web-Angebot der Universität gerade jetzt zu überarbeiten, kam aus der Gemeinsinn-Werkstatt. Die Gemeinsinn-Werkstatt fand dieses Jahr im Mai als Pilotprojekt an unserer Universität statt. Der dort geäußerte Wunsch, die Universität geschlossen im Internet zu präsentieren, kam meinem Anliegen nach einem uniweiten Web-Auftritt entgegen. Der bisherige Arbeitskreis „Webmaster" machte sich mit einer Handvoll neuer Mitglieder umgehend an die Arbeit. Besonders hervorzuheben ist, dass nicht nur alle Fakultäten sondern auch zentrale Einrichtungen sowie Studierende in diesem Arbeitskreis mitwirken. So können sich alle Interessensgruppen der Universität einbringen. Das gesteckte Arbeitsziel war es, ein „Corporate Design" zu entwickeln und dieses in Web-Richtlinien festzuschreiben.

Dr. Annja Zahn, Rechenzentrum

Corporate Design umfasst weit mehr, als nur die Gestaltung von Web-Seiten. An erster Stelle stehen die Informationen, um deretwillen der Besucher eine Website aufruft. Diese sollen sowohl optisch ansprechend gestaltet aber vor allen Dingen leicht zu finden sein. Daher zählt die Informations-Struktur und der Aufbau jeder einzelnen Web-Seite zu den wesentlichen Merkmalen eines Corporate Designs. Des weiteren sind rechtliche Bestimmungen zu berücksichtigen sowie die Verantwortung für den Web-Auftritt genau zu definieren.

Die Gestaltung einer Web-Seite bzw. deren Aufbau ist noch relativ einfach zu bewerkstelligen:

1. Die Anordnung der Informationen sollte einheitlich auf allen Web-Seiten gestaltet sein. Das heisst, dass z. B. immer an gleicher Stelle das Unisiegel, das Menü und die Informationen platziert werden.
2. Die Farbe soll gleichzeitig als Muster dienen, das heisst, dass z. B. Überschriften immer in der Farbe des Rahmens gesetzt werden sollen.
3. Die Auswahl einer Schrift bzw. einer Schriftenfamilie rundet das Bild ab.

Daneben müssen auch die Informationen „in Form" gebracht werden. Eine einheitliche Gliederung sowie gleiche Bezeichnungen für gleiche Inhalte sorgen dann für den nötigen Durchblick.

Neben der Gliederung und der Gestaltung des Inhalts gibt es einen weiteren wichtigen Punkt: Die Technik. Insbesondere Einrichtungen des öffentlichen Dienstes werden dazu angehalten, das Behindertengleichstellungsgesetz *(http://www.behindertenbeauftragter.de/download/gleichstellungsgesetz.htm)* umzusetzen. Kurz gefasst steht darin, dass Web-Seiten so gestaltet und programmiert sein sollen, dass Menschen mit Behinderungen darauf zugreifen können. Dies nennt man „barrierefreie Gestaltung" des Internets. Wenn nämlich in Bildern transportierte Informationen nicht gleichzeitig textlich vermittelt werden, bleiben Sehbehinderte ausgeschlossen. Für die Konzeption einer Website bedeutet dies, dass multimediale Inhalte den Web-Auftritt *ergänzen* aber nicht ersetzen sollen. Unabhängig von diesem Gesetz sollten Web-Seiten lesbar und navigierbar sein, auch ohne dass modernere Techniken eingesetzt werden. Web-Seiten müssen daher mit allen gängigen Browsern ohne Probleme zu betrachten sein.

Das Ergebnis

Nach etlichen mehrstündigen Treffen mit Kaffee und Keksen und kontroversen Diskussionen wurden wir uns schließlich

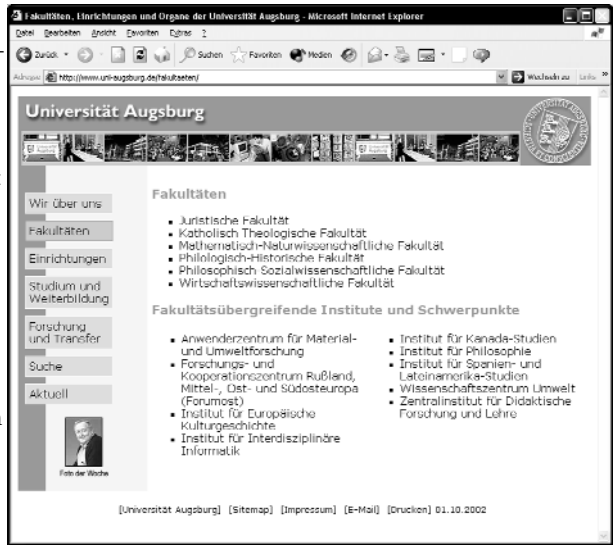


Abbildung 1: Der neue Web-Auftritt der Universität.

einig. Auf der neuen „Aktuell"-Seite der Universität erkennt man die wesentlichen Gestaltungselemente:

- Das Siegel der Universität in der Kopfzeile am rechten Rand
- Der Schriftzug des jeweiligen Bereiches der Universität in der Schriftart Gill am linken oberen Rand
- Eine Farbe zur Kennzeichnung der Organisationseinheit
- Eine kleine Fotoleiste mit anklickbaren Fotos
- Das Menü am linken Rand
- Die Fußzeile mit Link zum Impressum und Aktualisierungsdatum.

Neben der Gestaltung der Web-Seiten gehört auch die Bezeichnung der Menüpunkte zum „Corporate Design". Eine vor eineinhalb Jahren durchgeführte Umfrage – wie unsere Nutzer die Web-Seiten beurteilen und wo sie Verbesserungspotenzial sehen – ergab, dass eine einheitliche Menübezeichnung gewünscht wurde. Verschiedene Bezeichnungen für gleiche Informationen verwirren die Besucher unnötig und erschweren die Informationssuche. Dieser sinnvoller Vorschlag wurde bei der Neugestaltung berücksichtigt und umgesetzt. Die gefundenen Bezeichnungen helfen Ihnen schon jetzt, sich besser auf unseren Seiten zurecht zu finden.

Umsetzung

Seit August 2002 sind die ersten zentralen Einrichtungen und Fakultäten im neuen Design online. Neben den zentralen Eingangsseiten gehören dazu:

- Akademisches Auslandsamt
- Rechenzentrum
- Studentenkanzlei
- Universitätsarchiv
- Zentralverwaltung
- Juristische Fakultät
- Katholisch-Theologische Fakultät
- Mathematisch-Naturwissenschaftliche Fakultät
- Philologisch-Historische Fakultät
- Philosophisch-Sozialwissenschaftliche Fakultät.

Die Umsetzung bis auf die tieferliegenden Web-Seiten erfolgt Schritt für Schritt. Als nächste zentrale Einheit wird sich die Universitätsbibliothek dem neuen Design anschliessen.

Die neu gestalteten Web-Seiten wurden bzw. werden auf zwei Arten implementiert: Zum Einen kommt die Server Side Include Technik des Apache-Web-Servers zum Einsatz, zum Anderen werden die Web-Seiten mit PHP realisiert. Die Idee und das Ergebnis beider Techniken entsprechen sich: Es gibt an einer Stelle Rahmendateien (auch unter dem Begriff Templates bekannt), die in alle Web-Seiten eingebunden werden. Dadurch erhält man das gewünschte einheitliche Layout. Den letzten Schliff erhalten die Web-Seiten durch Verwendung von Cascading Style Sheets (CSS). Damit erfüllen wir nicht nur die eingangs erwähnten Richtlinien zur barrierefreien Gestaltung des Internets, CSS sind ein einfaches aber wirkungsvolles Mittel, Schriften, Farben, Links und einiges mehr festzulegen. Alle Web-Seiten, die das Style Sheet einbinden, haben damit automatisch schon ein grundlegendes Corporate Design.

Abbildung 2: Die neue Startseite des Rechenzentrums.

Ausblick

Um auf die Frage in der Überschrift dieses Beitrages zurückzukommen: Alles in bester Ordnung? Ich würde sagen, dass wir noch nicht so weit sind. Der Universität liegen die in diesem Artikel vorgestellten Konzepte in Form von Web-Richtlinien zur Verabschiedung vor. Erst wenn diese Richtlinien von allen Mitarbeitern der Universität anerkannt und umgesetzt werden, erst dann ist alles in bester Ordnung. Aber ich freue mich dennoch über die zahlreichen Einrichtungen und Fakultäten, die sich bereits freiwillig an die Web-Richtlinien halten. Es zeigt den Bedarf nach richtungsgebenden Leitlinien, und auch den Willen, sich mit der Universität zu identifizieren. Die Universität Augsburg ist auf einem guten Weg, einen campusweiten Web-Auftritt zu verwirklichen.

Die nächste Aufgabe des Arbeitskreises besteht darin, einen Interessensgruppen-orientierten Web-Auftritt zu konzeptionieren. Schüler, angehende Studierende, Studierende, Wissenschaftler sowie Besucher sollen ein eigenes Eingangsportal zur Universität erhalten.

Neue Veranstaltungsreihe des Rechenzentrums:

Das RZ-Kolloquium

Ab dem 19. November 2002 bietet das Rechenzentrum der Universität Augsburg ein Kolloquium an, zu dem alle Interessierten herzlich eingeladen sind.

Die Idee: Wir möchten diese Kolloquiumsreihe nutzen, um über Themen aus dem Umfeld unserer Arbeit am Rechenzentrum zu informieren.
Die Dozenten: Mitarbeiter von Firmen und Gastdozenten anderer Universitäten werden einmal im Monat aktuelle Themen aus ihrem Arbeitsbereich vorstellen.
Die Zielgruppe: Alle Mitarbeiter, Studierende und Interessierten der Universität Augsburg.
Die Termine: Die Vortragsreihe findet einmal im Monat statt, immer dienstags um 15.00 Uhr im Raum 1005 NW1/RZ.

Ausführliche Informationen über die aktuellen Themen finden Sie bei uns im Internet unter *http://www.rz.uni-augsburg.de/kolloquium*. Wir freuen uns auf Ihr Kommen!

Anschluss gesucht

Anschluss der WiWi und der Bibliothek über ein Hochgeschwindigkeitsnetz an das Rechenzentrum

Ein weiterer Zwischenschritt in der Datennetzsanierung steht vor der Fertigstellung. Entsprechend den Konzepten in der Eichleitnerstrasse und im NW1/RZ-Gebäude wird gegenwärtig eine sogenannte „strukturierte Verkabelung“ im Gebäude der Wirtschaftswissenschaft sowie der Zentralbibliothek und der Teilbibliothek WiWi durchgeführt.

Die gravierendsten Änderungen in der Verkabelung werden im WIWI-Gebäude durchgeführt. Bei der bestehenden 10Mbps-Ethernet-Verkabelung mit Koax-Kabel werden alle Kabel eines Gebäudeflügels in einem Unterverteilerraum zusammengeführt. Die Koax-Kabel werden in den Unterverteilerräumen auf aktive Netzkomponenten (sog. Hubs) geführt. Die Hubs haben die Aufgabe die Signale aus den Koax-Kabeln zu verstärken und via Lichtwellenleiter (LWL) auf einen Switch im zentralen Verteilerraum zu leiten. Der Nachteil dieser Verkabelung ist, dass alle Endgeräte (PC's, Drucker, usw.) auf einem Koax-Kabel sich die Bandbreite von 10Mbps teilen. Durch den Hub wird die Teilnehmerzahl im Segment noch erhöht. Er verstärkt zwar das Signal nimmt aber keine Segmentierung vor, so dass mit jedem angeschlossenen Koax-Kabel weitere Datenendgeräte auf die 10Mbps Bandbreite zugreifen. Eine Segmentierung findet erst durch den zentralen Switch statt. Gemäß diesem Konzept sind im WIWI-Gebäude gegenwärtig 4 Räume mit Hubs ausgestattet ausgestattet. Das gesamte Gebäude wird also mit lediglich 40 Mbps versorgt. Die Weiterleitung der Daten von der WIWI an die zentralen Server des Rechenzentrums bzw. ins Internet erfolgt via ATM.

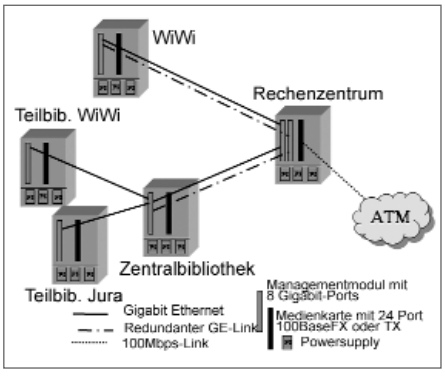


Abbildung: Verkabelungsschema

Strukturierte Verkabelung

Die neue strukturierte Verkabelung in der WIWI sieht hingegen vor, dass jedes Zimmer direkt an den zentralen Verteilerraum der WIWI angeschlossen wird. Die Unterverteiler in den Gebäudeflügeln werden nicht mehr für aktive Netzkomponenten benötigt. Jedes Büro wird mit einem 4 faserigen Lichtwellenleiterkabel angefahren. Im zentralen Verteilerraum wird dann nur noch ein großes modulares Switchingsystem installiert. Auf diesen Switch wird jedes Büro mit 100 Mbps (Fast Ethernet) angeschlossen. Damit die PC's und Drucker in den einzelnen Räumen nicht mit 100 Mbps-LWL-Karten ausgestattet werden müssen versorgen wir jeden Raum mit einem unmanaged 4 Port-Switch. Dieser Switch bietet 4 x 10/100 Mbps Kupfer – Ports an, ein 100 Mbps-LWL-Port wird zum Anschluß an das zentrale Switchingsystem genutzt. Das Verkabelungsschema ist in der Abbildung dargestellt. Die Verkabelung in der Zentralbibliothek und der Teilbibliothek WISO erfolgt analog.

Parallel zur Kabelinstallation findet die Evaluierung der aktiven Netzkomponenten für die beschriebenen Gebäude statt. Aus der Vielzahl von Anbietern haben sich für die Universität zwei Hersteller als geeignet heraus kristallisiert. Das Konzept sieht vor, daß jeder neu verkabelte Gebäudekomplex mit zwei Gigabit-Ethernet-Verbindungen auf einen zentralen Gigabit-Switch im Rechenzentrum angeschlossen wird. Bei Ausfall einer der beiden Gigabit-Links läuft der Datenverkehr über die verbleibende Verbindung weiter. Die beiden Gigabit-Links werden als sog. Trunk aufgebaut, jeder Link innerhalb des Trunks wird auf unterschiedliche Module gelegt. Der Switch behandelt alle, innerhalb eines Trunks zusammengebunden Links, als eine logische Verbindung. Zwischen den Links wird die Netzlast verteilt, so dass höhere Geschwindigkeiten gefahren werden können.

Bei dem neuen Gigabit-Switch handelt es sich um ein modular aufgebautes Switchingsystem. Dies hat den Vorteil das der Switch, durch Einsatz von sog. Linecards, bis zu seinem Maximalausbau bedarfsgerecht ausgebaut werden kann. Die Chassisgröße wurde immer so gewählt das, nach heutigem Bedarf, mindestens 2 Reserveeinschübe für Erweiterungen zur Verfügung stehen. Dies entspricht weiteren 48 Ports mit jeweils 100Mbps Bandbreite. Der zentrale Gigabit-Switch wird durch zwei Managementmodule und drei Powersupplies ausfallsicher ausgelegt. Die Anbindung des neuen Gigabit-Ethernet-Netzwerkes an das bestehende ATM-Netzwerk erfolgt ebenfalls über einen Trunk (4 x 100MBPS-Verbindungen) auf den bestehenden ATM-Switch im Rechenzentrum.

Ausblick

Wir hoffen, dass wir das neue Netz bis Ende dieses Jahres installiert haben, so dass in der nächsten Connect ein erster Erfahrungsbericht über die neuen Netzkomponenten erfolgen kann.

**Dieter Machui,
Rechenzentrum**

Der Kopierschutz nach Änderung des Urheberrechts

Noch ist die letzte Reform nicht erkaltet und das neue Urhebervertragsrecht gerade erst wirksam, da steht bereits die nächste Neuerung an. Zum 01.01.2003 soll eine weitere Urheberrechtsnovelle in Kraft treten. Das im Entstehen befindliche Gesetz dient der Umsetzung der Richtlinie des Europäischen Parlaments und des Rates vom 22.05.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. Es ist dies die jüngste von mittlerweile sieben EU-Richtlinien auf dem Gebiet des Urheberrechts. Gleichzeitig ist es eine von vielen Richtlinien, die sich mit den rechtlichen Aspekten der Informationsgesellschaft und damit auch des elektronischen Geschäftsverkehrs befassen. Nach dem ersten Referenten-Entwurf vom 18.03.2002 liegt inzwischen aus dem Bundesjustizministerium ein Regierungsentwurf mit dem Stand vom 31.07.2002 vor, der Gegenstand des folgenden Beitrags ist. Zu beachten bleibt allein, dass die vorliegende Gesetzesfassung im Gesetzgebungsverfahren noch verändert werden kann.

I. Vorbemerkung

1. Allgemeines

Das Urheberrecht ist – ungeachtet seiner ältesten Wurzeln – immer noch ein Kind der Technik. Erst die Erfindung des Buchdrucks ließ die Notwendigkeit eines Schutzes des Schöpfers kultureller Werke offenbar werden. Aus ihr ergab sich die Erforderlichkeit staatlicher Regulierung, deren Novellierungen ebenfalls fast stets mit technischen Entwicklungen einhergingen. Dabei waren die Gerichte naturgemäß dem Gesetzgeber ein wenig voraus. Dem europäischen Gesetzgeber obliegt freilich in erster Linie die Harmonisierung des nationalen Rechts, doch gibt auch die nunmehr umzusetzende Richtlinie ungeachtet dessen eine Vielzahl von technisch bedingten Normen vor, für die es bislang kein nationales Vorbild gibt.

Rechtsanwalt Dr. Stefan Ernst, Freiburg im Breisgau

2. Urheberinteressen und Kopierschutz

Angesichts der unbeschränkten Kopiermöglichkeiten in Originalqualität hat das Interesse der Industrie an „digitalem Selbstschutz“ erheblich zugenommen. Dieser kann im Wesentlichen nur aus Zugangskontrollen und Kopiersperren bestehen. Dass damit Kollisionen zu den Nutzerinteressen auftreten müssen, ist offenbar, denn der Kopierschutz wirkt nicht nur gegen illegale Piraterie, sondern auch gegen berechtigte Nutzung. Dies gilt auch und gerade für das Recht zur privaten Vervielfältigung. So sehr auch die Zulassung von Privatkopien – gegen Vergütung durch die Geräte- und Leerkassettenabgabe – für analoge Werke die einzig sinnvolle Lösung gewesen ist, so problematisch bleibt die Lage auf dem digitalen Markt. Durch das Internet sind Kopien in bisher nicht da gewesener Zahl möglich geworden, so dass die Rechteinhaber verständlicherweise zu Maßnahmen greifen, die von vornherein jede Vervielfältigung verhindern. Dass diese Kopierschutzsysteme dabei keinen Unterschied zwischen zulässiger und unzulässiger Nutzung machen können, liegt auf der Hand. Allein sie können verhindern, dass massenhaft neue Vervielfältigungsstücke in Originalqualität entstehen. So ist denn die Regelung des Schutzes solcher technischen Maßnahmen der bemerkenswerteste Part der vorgesehenen Novelle. Die in den einschlägigen Normen umgesetzten Vorschriften der Richtlinie beruhen dabei ihrerseits bereits auf (allgemein gehaltenen) Verpflichtungen aus den internationalen Abkommen.

3. Abgrenzung zu Zugangskontrolldiensten

Das Urheberrecht kann nur die Frage der Kopiersperren regeln. Der parallele Schutz durch Zugangskotrollen wird im ebenfalls recht jungen Zugangskontrolldiensteschutzgesetz behandelt. Zugangskontrolldienste sind technische Verfahren oder Vorrichtungen, die die erlaubte Nutzung eines zugangskontrollierten Dienstes ermöglichen. Solche Dienste können entgeltliche Rundfunk-, Tele- oder auch Mediendienste sein. Das Gesetz verbietet strafbewehrt die Herstellung, Einfuhr und Verbreitung von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken, bußgeldbewehrt Besitz, Einrichtung, Wartung und Austausch dieser Vorrichtungen zu gewerbsmäßigen Zwecken und (unbewehrt) die Absatzförderung.

Hier geht es also um die Überwindung etwa von Pay-TV oder kostenpflichtigen Online-Zugängen im Wege des Hacking, was für den Täter selbst schon im Strafgesetzbuch unter Strafe steht. Das neue Gesetz weet die Verantwortlichkeit auf die Verbreiter der entsprechenden Vorrichtungen aus.

II. Der Schutz technischer Maßnahmen

Im Folgenden wird die im Regierungsentwurf beschriebene neue Rechtslage im Einzelnen vorgestellt. Der Gesetzestext selbst ist recht unübersichtlich und sprachlich für den Laien kaum zugänglich, da den Entwurfsverfassern die möglichst wörtliche Umsetzung der Richtlinie geboten schien.

1. Schutz technischer Maßnahmen

a) Definition

Der Gesetzentwurf definiert den Schutzgegenstand der Norm – wirksame (nicht: unumgehbare) technische Maßnahmen –

als Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, bestimmte Verwertungshandlungen – insbesondere das Kopieren – durch das Urheberrechtsgesetz geschützter Werke oder Schutzgegenstände zu verhindern. Gemeint sind insbesondere Zugangskontrollen, Verschlüsselung und Kopierschutzvorrichtungen. Technische Schutzmaßnahmen werden unabhängig von der verwendeten Technologie vor Umgehung geschützt. Die Norm gilt also sowohl für Hardware (z. B. Dongles) als auch für Software-implementierte Schutzmaßnahmen.

b) Umgehungsverbot

Technische Schutzmaßnahmen der genannten Art dürfen ohne Zustimmung des Rechteinhabers nicht umgangen werden, um Zugang zum geschützten Werk zu erhalten. Das Kopieren eines urheberrechtlich geschützten Werkes oder eines anderen durch das Urheberrechtsgesetz geschützten Schutzgegenstandes unter Umgehung eines Kopierschutzes ist demnach verboten. Dies gilt ungeachtet der urheberrechtlichen Schrankenbestimmungen, die in bestimmten Fällen auch ungefragtes Kopieren – zum Teil gegen Entgelt – gestatten. Zur Durchsetzung dieser Schrankenbestimmungen hat der Gesetzgeber eine eigene Norm vorgesehen, die unten vorgestellt (2.) wird. Allein Umgehungshandlungen zu wissenschaftlichen Zwecken (z. B. Kryptografie) werden nicht erfasst.

c) Vertrieb von Hacking-Werkzeugen

Der nächste Absatz regelt das Verbot von Hacking-Werkzeugen, greift also bereits im Vorfeld der oben genannten Handlungen ein. Gemeint sind

- Vorrichtungen, Erzeugnisse oder Bestandteile, die die Umgehung technischer Schutzmaßnahmen beabsichtigen (Nr. 1),
- solche Vorrichtungen, die von der Umgehung abgesehen nur einen begrenzten wirtschaftlichen Nutzen haben (Nr. 2) oder
- hauptsächlich dazu dienen, diese Umgehung zu ermöglichen oder zu erleichtern (Nr. 3).

Dabei ist zu erwarten, dass es hinsichtlich der Varianten 2 sowie 3 und der Abgrenzung zu erlaubten Geräten und Software, die das Kopieren ebenfalls erleichtern können, in der Zukunft vielfältigen Streit geben wird.

Verboten sind die Herstellung, Einfuhr, Verbreitung (insbesondere Verkauf und Vermietung, aber auch Verleih und kostenlose Weitergabe) sowie die Werbung für diese Werkzeuge. Ausdrücklich verboten ist aber auch schon der – zu gewerblichen Zwecken dienende – Besitz von Hacking-Werkzeugen oder die Erbringung entsprechender Dienstleistungen.

d) Strafverfolgung und polizeiliche Gefahrenabwehr

Allein Polizei und Strafverfolgungsbehörden dürfen die beschriebenen Verbote in Erfüllung ihrer Pflichten ausdrücklich umgehen.

2. Durchsetzung von Schrankenbestimmungen

In den Normen des Gesetzes sind diverse Schranken des Urheberrechts normiert. Diese dienen dazu, im Interesse der Kulturwirtschaft und der Allgemeinheit u. a. die Nutzung und auch das Kopieren urheberrechtlich geschützter Werke zwar zum Teil gegen Entgelt, aber in jedem Fall auch gegen den Willen des Rechteinhabers zu gestatten. Damit diese Schranken durch den Einsatz von Kopiersperren nicht leer laufen, wurden Verpflichtungen zu Lasten des Rechteinhabers formuliert. Soweit diese technischen Maßnahmen eine ansonsten berechtigte Nutzung verhindern, hat den Begünstigten bestimmter Schranken die Umgehung des entsprechenden Schutzes ermöglichen. Es handelt sich dabei um die Schranken zu Rechtspflege und öffentlicher Sicherheit, für Behinderte, Schul- und Unterrichtsgebrauch, Schulfunksendungen, öffentliche Zugänglichmachung für Unterricht und Forschung, Archiv, eigene Unterrichtung und sonstiger eigener Gebrauch, jeweils in Papierform oder nichtwirtschaftlich und für Sendeunternehmen. Das Recht zur privaten Vervielfältigung ist nur betroffen, soweit es um die Vervielfältigung in Papierform oder ähnliche Träger geht, nicht aber auf Bild-, Ton- oder Datenträger.

Wie die Berechtigten ihrer Verpflichtung nachkommen, ist diesen freigestellt. So mögen etwa Schlüsselinformationen an die durch die Schranken privilegierten Personen und Institutionen weitergegeben werden. Dies kann aber auch auf Verbände beschränkt werden, wenn die Erfüllung der Pflichten damit gesichert ist. Nicht zuletzt mag auch die Möglichkeit zum Online-Abruf weiterer Vervielfältigungsstücke hinreichend sein.

Dies bedeutet aber nicht, dass in diesen Fällen der Einsatz von Kopierschutzknackern gestattet würde. Der Entwurf gewährt dem Berechtigten der genannten Schrankennormen lediglich einen Anspruch gegen den Hersteller darauf, ihm die zur Wahrnehmung der Rechte benötigten Mittel zur Verfügung zu stellen. Es gibt keine Möglichkeit zur Selbsthilfe, kein „right to hack“. Dass diese Regelung freilich die Anspruchsdurchsetzung verzögern und zuweilen ganz verhindern kann (insbesondere bei Fällen mit Auslandsbezug) ist eine andere Frage. Neben dem allgemeinen Prozessrisiko ist dies stets zumindest mit zeitlichem Aufwand und Verzögerung verbunden. Aus diesem Grunde wird mit der Rechtsänderung zugleich eine Ergänzung des Unterlassungsklagengesetzes, das eine Prozessführung etwa durch Verbraucherverbände und Kammern ermöglicht.

3. Schutz der zur Rechtewahrnehmung erforderlichen Informationen

Der Entwurf verbietet grundsätzlich die Veränderung von werkintegrierten Informationen, die der Berechtigte zur Erleichterung der Rechtewahrnehmung angebracht hat. Das Gesetz definiert dies als elektronische Informationen, die das Werk selbst oder den Rechteinhaber identifizieren oder auch Informationen über Nutzungsmodalitäten enthalten.

Hierunter fallen also zum einen spezielle dem Schutz dienende Instrumente wie zum Beispiel digitale Wasserzeichen. Unter die Norm fällt aber auch die Veränderung von einfachen Informationen etwa die automatische Nennung des Autors einer Textdatei unter „Eigenschaften“. Wurde die Information verändert oder entfernt, darf das Werk nicht mehr weiter gegeben oder öffentlich wiedergegeben werden.

4. Kennzeichnungspflichten

Damit der Käufer über technische Schutzmaßnahmen bei einem Werk sofort informiert ist, ist geboten, dass auf diese deutlich sichtbar und mit Angaben

zu den Eigenschaften des Schutzes hingewiesen wird. Das Kennzeichnungsgebot dient also dem Verbraucherschutz. Fehlt ein solcher Hinweis und ist das erworbene Werkstück aus diesem Grunde für den Käufer nicht nutzbar, kann er Gewährleistungsrechte (Neulieferung, ggf. Umtausch) geltend machen.

5. Keine Geltung für Software

Die Normen zum technischen Schutz sollen auf Computerprogramme keine Anwendung finden. Dies ist dadurch bedingt, dass die hier umgesetzte Richtlinie auf Computerprogramme keine Anwendung findet und Abgrenzungsprobleme zum Recht zur Erstellung einer Sicherungskopie und zu den Regelungen zur Dekompilierung vermieden werden sollen. Die meisten Schranken, insbesondere eine freie Kopie zum Privatgebrauch, sind bei Software ohnehin vom Gesetz nicht vorgesehen.

III. Straf- und Bußgeldnormen

1. Strafbarkeit unerlaubter Eingriffe

Ein zahnloser Tiger verbreitet relativ wenig Schrecken. Der vorgesehene Schutz wird aus diesem Grunde mit kräftigen Mitteln untermauert. Dies entspricht der erforderlichen Umsetzung der Richtlinie, die angemessene Sanktionen für alle Pflichten verlangt. Wer gegen die oben beschriebenen Verbote verstößt, kann sich strafbar machen, auch wenn eine Strafverfolgung nur bei Vorliegen eines Strafantrags erfolgt. Das Strafmaß wird bei gewerbsmäßigem Handeln erhöht.

Strafbar sind demnach im Einzelnen

- die Umgehung eines Kopierschutzes in der Absicht, sich oder einem anderen Zugang zu einem geschützten Werk zu verschaffen;
- die Entfernung einer Information für die Rechtewahrnehmung, also z. B. eines digitalen Wasserzeichens;
- die Einfuhr, Verwertung oder öffentliche Wiedergabe eines Schutzgegenstandes, bei dem etwa z. B. ein Wasserzeichen entfernt wurde;
- die Herstellung, Einfuhr, Verbreitung, Verkauf, Vermietung eines Kopierschutzknackers zu gewerblichen Zwecken.

2. Straflosigkeit bei privatem Gebrauch

Straflos bleibt allerdings die Tat, die ausschließlich zum eigenen privaten Gebrauch des Täters oder mit dem Täter verbundener Personen erfolgt oder sich auf einen derartigen Gebrauch bezieht. Die persönliche Verbindung im Sinne der Norm ist aber eng allein im Sinne des Familien- und Freundeskreises auszulegen.

3. Ordnungswidrigkeiten

Aufgrund des geringeren Unrechtsgehalts lediglich ordnungswidrig, aber immer noch bußgeldbewehrt, handelt, wer

- Kopierschutzknacker nicht gewerbsmäßig verkauft, vermietet oder an Personen weitergibt, die nicht mit ihm persönlich verbunden sind;
- Kopierschutzknacker zu gewerblichen Zwecken besitzt
- für den Verkauf oder die Vermietung von Kopierschutzknackern wirbt
- entsprechende Dienstleistungen erbringt

Auf der anderen Seite wird aber auch der Rechteinhaber mit Bußgeld bedroht, wenn er die geforderten Mittel zur Nutzung der Urheberrechtsschranken nicht zur Verfügung stellt oder seinen Kennzeichnungspflichten nicht oder nicht vollständig nachkommt.

Leistungsstarker Web-Server mit umfangreichem Dienstleistungsangebot

von Dr. Markus Zahn, Rechenzentrum

Im August 2002 hat das Rechenzentrum seine Serviceleistung im Bereich „Web-Hosting“ erweitert. Schon seit mehreren Jahren bietet das Rechenzentrum den Fakultäten, Instituten und sonstigen Einrichtungen der Universität die Möglichkeit, einen Web-Server des Rechenzentrums als sogenannten „virtuellen Web-Server“ oder „virtual Host“ zu verwenden. Für die Nutzer liegen die Vorteile klar auf der Hand: Die technische Betreuung eines eigenen Web-Servers entfällt und sie können sich auf die eigentliche Aufgabe, nämlich die Bereitstellung der Inhalte, konzentrieren. Selbstverständlich bleibt die ursprüngliche Adresse des Servers, also z.B. www.kthf.uni-augsburg.de, dabei erhalten. Die Bezeichnung „virtueller Server“ rührt daher, dass alle vom Rechenzentrum betriebenen Web-Server auf nur einem einzigen Rechnersystem bereitgestellt werden. Dieser Ansatz hat sich in der Vergangenheit als platzsparende und wartungsfreundliche Variante erwiesen.

Dynamischer Web-Auftritt

Das bisherige Leistungsspektrum beschränkte sich bislang allerdings auf statische HTML-Seiten und sogenannte „Server Side Includes“. Dynamische Inhalte wie PHP, Java Server Pages, Java Servlets oder CGI-Skripte wurden durch die bisherige Installation nicht unterstützt. Genau an dieser Stelle setzen nun die neuen Serviceleistungen an. Das Rechenzentrum hat zu diesem Zweck im Frühjahr ein neues, leistungsfähiges Rechnersystem beschafft, das nun – Zug um Zug – die Aufgaben des bisherigen Systems übernimmt. Zusätzlich besteht pro (virtuellem) Server die Möglichkeit, dynamische Inhalte über die genannten Techniken (PHP, Java Server Pages, Java Servlets oder CGI-Skripte) bereitzustellen. Auch Web-Angebote, die intern auf eine Datenbank zurückgreifen müssen, werden unterstützt. Der Einsatz von MySQL macht es möglich.

Vertrauen ist gut, Kontrolle ist besser

Um die Nutzer dieser Dienstleistung vor unnötigen Datenverlusten zu schützen, werden die gesamten Daten auf täglicher Basis gesichert. Als besonderer Service steht für jeden (virtuellen) Server unter der URL http://<servername>/webstats/, also z.B. http://www.kthf.uni-augsburg.de/webstats/, eine tägliche Auswertung der Zugriffsstatistiken bereit. Unter der Adresse http://<servername>/checkbot/ gibt es zudem eine Analyse über ungültige oder veraltete Links. Auf diese Weise bleiben Anbieter immer im Bilde, wie frequentiert ihre Web-Seiten genutzt werden und ob sich Fehler bei der „Verlinkung“ eingeschlichen haben.

Träume in hellblau

Individuelle Präsentationen mit Microsoft PowerPoint erstellen – Eine Anleitung

Die Präsentationssoftware PowerPoint von Microsoft kennt – wenigstens dem Namen nach – jeder. Dieser Artikel beschreibt, wie Sie Ihre individuelle Vorlage mit PowerPoint erstellen können und gibt darüber hinaus einige Tipps, die Ihnen die Arbeit bei der Erstellung Ihrer Präsentation erleichtert.

Da das Rechenzentrum regelmäßig mit Weiterbildungskursen in Erscheinung tritt, bestand eine meiner ersten Aufgaben darin, eine Vorlage für unsere Lehrveranstaltungen mit PowerPoint zu entwickeln. Diese Aufgabe diente auch dazu, mich mit den Werkzeugen und Möglichkeiten von PowerPoint vertraut zu machen. Ich arbeite schon seit längerem mit diesem Programm, das Erstellen einer eigenen Folienvorlage unter dem Folienmaster war aber ein neues Abenteuer für mich. Die nun im Folgenden beschriebenen Arbeitsschritte, die zu der fertigen Folie führten, sollen auch die Arbeit mit PowerPoint etwas näher bringen.

Die Qual der Wahl

Bevor ich mit den Grenzen von PowerPoint konfrontiert werden sollte, habe ich mir erst einmal Gedanken über das Layout gemacht. Welche Farben waren für das Auge am Angenehmsten, wie sollte der Hintergrund gestaltet sein, welche Elemente kann man einbringen, die für das Rechenzentrum spezifisch waren?

Nach endlosen Seiten im Internet über die Farbenlehre fiel die Entscheidung auf einen blauen Hintergrund. Vor einiger Zeit lernte ich einen Mitarbeiter der Firma Carl Zeiss Optik kennen, der in der Forschung tätig ist. Er untersucht unter anderem die Reaktion des menschlichen Auges auf verschiedene Farb- und Lichteffekte. Er erklärte mir, dass unser Auge die Farbkombination blau/weiß als besonders beruhigend und angenehm empfindet. Das sei auch der Grund, warum er für seine Vorträge PowerPoint-Folien verwendet, die einen blauen Hintergrund mit weißer Schrift haben. Letztendlich hat mich auch ein Satz aus Goethes Farbenlehre überzeugt:

Blau

Diese Farbe macht für das Auge eine sonderbare und fast unaussprechliche Wirkung. Sie ist als Farbe eine Energie; allein sie steht auf der negativen Seite und ist in ihrer höchsten Reinheit gleichsam ein reizendes Nichts. Es ist etwas Widersprechendes von Reiz und Ruhe im Anblick. (779)

Die ersten Enscheidungen sind also gefallen: Der Hintergrund wird blau, die Schrift weiß und die Überschrift gelb. Diese Farbkombination finden Sie auch auf der neuen Homepage des Rechenzentrums, da Blau, Gelb und Weiß sehr gut miteinander harmonieren

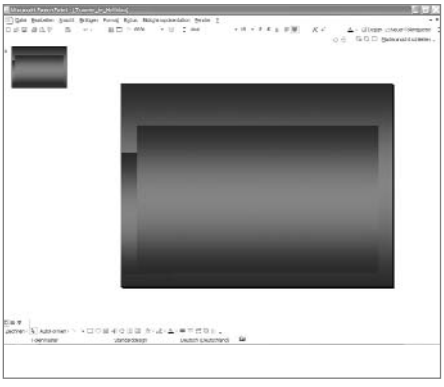
Die im folgenden beschriebenen Schritte zeigen, wie man unter dem Folienmaster *(Ansicht/Master/Folienmaster)* eine Präsentationsvorlage erstellen kann, die automatisch für jede neue Folie, die Sie einfügen, verwendet wird.

Der Hintergrund

Ein blauer Hintergrund ohne Verlauf erschien sehr eintönig. Zum Glück kann man dank einiger Werkzeuge unter PowerPoint seiner Fantasie freien Lauf lassen.

Leider gibt es bei PowerPoint keine Funktion, die speziell den Hintergrund bestimmen oder bearbeiten lässt. Daher muss man zu einem kleinen Trick greifen: In der untersten Symbolleiste, die den Bereich *Zeichnen* markiert, klickt man auf das Rechteck und zeichnet mit dem Pfeil eine dem Hintergrund entsprechend große Fläche. Ebenfalls in dieser Leiste finden sich die Funktionen *Füllfarbe, Linienfarbe* etc. Um den störenden Rand um das Rechteck wegzuzaubern, klickt man unter *Linienfarbe* auf *keine Linie*. Unter *Füllfarbe* wird nun bei *Fülleffekte* Farbe und Verlaufseffekt gewählt. Diese Vorgehensweise kann man übrigens bei den meisten Microsoft Programmen verwenden, die Funktionen sind überall fast die gleichen.

Dies sei noch am Rande erwähnt: Um den Hintergrund aufzulockern habe ich als „Muster" weitere Rechtecke eingefügt. Diese Rechtecke überlappen sich, das heißt das eine Rechteck verschwindet zum Teil hinter dem anderen. Dies kann man ebenfalls in der untersten Symbolleiste unter dem Menüpunkt *Zeichnen* einstellen. Hier bestimmt man dann die *Reihenfolge* des angeklickten Objektes, ob es im *Hintergrund, Vordergrund, eine Ebene hinten, eine Ebene vorne* etc. stehen soll.



Der erste Schritt: der Hintergrund

Exkurs: Photoshop

Für mich gehörte zu dem Folienlayout auch ein Foto des Rechenzentrums, welches mit möglichst weichen Übergängen in den Hintergrund übergehen sollte.

Eva Kökeny,
Rechenzentrum

Das Rechenzentrum ...

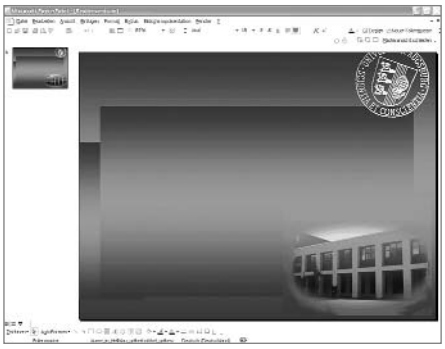
... mit reduzierten Rot- und Grüntönen ...

... und mit weichen Kanten.

Vielleicht ist der „Trick", den ich hier angewendet habe, für den Einen oder Anderen hilfreich.

Da der Folien-Hintergrund blau ist, habe ich die Bildvorlage vom Rechenzentrum unter Photoshop nachbearbeitet. Unter *Bild/Einstellen/Farbbalance* wurden die Rot- und Grünwerte reduziert, bis das Bild überwiegend in Blautönen erschien. Man kann jetzt, damit der Bildrand weicher in den Hintergrund übergeht, unter Photoshop mit der *Auswahllellipse* (z. B. mit *Weiche Kant 20 px*) das Bild eingrenzen, *kopieren* und unter eine neue Arbeitsfläche *einfügen*. Dadurch werden die Kanten weicher, verschwommener und heben sich nicht so deutlich vom Hintergrund ab. Das Bild wird dann, um es ohne Probleme in PowerPoint einfügen zu können, z. B. im GIF-Format gespeichert und unter *Einfügen/Grafik/Aus Datei* aufgerufen.

Um das Bild noch harmonischer in den Hintergrund der PowerPoint-Folie einzufügen, empfiehlt sich ein zweiter Kniff: Ziehen Sie ein weiteres Rechteck in der Größe der Grafik, passen Sie die Farbe den RGB-Werten des verwendeten Blautones an und erhöhen Sie mit einem Doppelklick auf das Rechteck im Menü *Autoform Formatieren* den Transparenzwert. Sie haben jetzt ein „durchsichtiges" blaues Rechteck das Sie auf das Bild legen können. So verschwand das Foto noch mehr in den Hintergrund.



Folienhintergrund mit Bild

Anschließend wählte ich alle Elemente, die den Hintergrund bilden, mit gedrükkter Shift-Taste und Mauszeiger aus und gruppierte sie mit *Zeichnen/Gruppierung*. Dies hat den Vorteil, dass man die einzelnen Elemente nicht aus Versehen wieder verschieben kann. Natürlich lässt sich dies unter *Zeichnen/Gruppierung aufheben* wieder rückgängig machen.

Handzettel

In PowerPoint können Folien sehr bequem als Handzettel gedruckt werden. Man kann dabei wählen, wieviele Folien auf einer Seite gedruckt werden sollen – die Anzahl liegt dabei zwischen eins und neun. Handzettel bieten sich daher für die Verteilung von Kursunterlagen unserer Lehrveranstaltungen an.

Druckte man nun die Folien aber als Handzettel S/W aus, erschienen auch die von mir eingefügten Rechtecke auf dem Ausdruck – und das sollte natürlich nicht der Fall sein. Wenn man also auf dem Handzettel nur den Text haben will, muss man ein weiteres Mal in die „Trickkiste" greifen. Speichern Sie den Hintergrund als neue Grafik ab – es empfiehlt sich das JPG-Format – und fügen Sie sie dann erneut unter einem leeren Folienmaster als Grafik ein: *Einfügen/Grafik/Aus Datei*. Meiner Erfahrung nach lässt sich die Grafik im JPG-Format am Besten in den Hintergrund einer PowerPoint-Folie einfügen. Geht man jetzt unter *Drucken* auf *Handzettel* und *Vorschau,* erscheint der Folientext wie gewünscht ohne den Hintergrund und ohne die störenden Rechtecke.

Handzettel-Text mit Hintergrund

Aufzählungszeichen

Die Anfänge im Folienmaster waren nun geleistet und die Arbeit schien schnell voranzugehen … bis ich mir in den Kopf gesetzt habe, individuelle Aufzählungszeichen zu gestalten. Ich wollte hier keine vorgegebenen Zeichen aus der PowerPoint-Liste nehmen, denn auch dieses Detail sollte ein nur für das Rechenzentrum typisches Merkmal darstellen.

Ich entschied mich, das Experiment mit Photoshop zu wagen, da man hier be-

Handzettel-Text ohne Hintergrund

sonders mit den Effekten gut arbeiten kann. Die Idee für die Aufzählungspunkte fand ich auf einer von mir häufig besuchten Website – *http://www.drweb.de* – die gute Tipps im Umgang mit Photoshop bietet.

Nach einigen Versuchen hatte ich eine leicht abgeänderte Form des dort dargestellten „Knopfes" und war an sich recht zufrieden. Die Probleme tauchten erst auf, als ich versuchte, den Knopf in PowerPoint einzufügen. Das Aufzählungszeichen war im Verhältnis zur Schrift zu groß. Legte man die Pixelgröße unter Photoshop fest, wurde das von PowerPoint trotzdem in der falschen Größe gesetzt. Zudem war zwischen Zeichen und Text ein zu geringer Abstand.

Die schon in der PowerPoint-Liste vorgegebenen Aufzählungszeichen haben alle eine Größe von 12x12 Pixel. Im ersten Versuch wurde die Größe reduziert, jedoch skaliert PowerPoint die Grafik wieder hoch. Dadurch sah der Knopf in der Folie pixelig und fransig aus. Verwendete ich eine höhere Auflösung, wurde der Knopf zu groß und war so ebenfalls nicht verwendbar. Letztendlich ließ sich dieses Problem beheben, indem der transparente Hof um den Knopf vergrößert wurde. Dadurch wird das Aufzählungszeichen, sobald es in PowerPoint eingefügt wird, kleiner und auch der Abstand zum Text größer. Nun war auch dieses Hindernis überwunden und das passable Endergebnis wurde einstimmig angenommen.

Die fertige Vorlage speichert man nun als *Entwurfsvorlage* (.dot) und fügt sie unter *Design* (oberste Symbolleiste) *Entwurfsvorlage* mit der *Durchsuchen*-Funktion in die Liste der vorgegebenen Vorlagen ein, so dass man bequem darauf zugreifen kann.

Fazit

Auch wenn man schon tiefer gehende Kenntnisse mit PowerPoint hat, so ist das Erstellen einer eigenen Masterfolie dennoch eine Herausforderung. Abgesehen

Das Endergebnis

von der Schwierigkeit, ein für das Auge angenehmes Design zu finden, die für alle oder zumindest für die meisten Mitarbeiter akzeptabel ist, die diese Folie verwenden wollen, darf man auch die Wege und Mittel zur Verwirklichung nicht unterschätzen.

Zwar muss man zur Problemlösung öfters in die Trickkiste greifen, letztendlich lernt man doch noch dazu und ich kann jedem, der sich etwas näher mit PowerPoint beschäftigen möchte, nur raten, das Abenteuer zu wagen.

Personalia

Seit dem 3. Juni 2002 verstärkt *Herr Dr. Michael Westerburg* das Rechenzentrum durch seine Mitarbeit in der Arbeitsgruppe „Betriebssysteme und zentrale Server." Der Schwerpunkt seiner Arbeit liegt im Entwurf und in der Umsetzung eines Sicherheitskonzeptes für die IT-Infrastruktur an der Universität Augsburg. Mit der leider auf drei Jahre befristeten Stelle kann endlich auf die rapide zunehmenden Gefahren durch den Missbrauch des Internets reagiert werden.

Bereits die Ergebnisse der ersten Wochen und Monate seiner Tätigkeit haben unsere schlimmsten Vermutungen bestätigt – oder sogar noch übertroffen. Bei manchen Bedrohungen, z. B. durch Computer-Viren, dauert es für einen beliebigen Rechner auf dem Campus im Mittel gerade mal vier Minuten(!), bis er von „Angreifern" auf die entsprechende Schwachstelle getestet wird. Fehlen die notwendigen Wartungsstände (Betriebssystem, Virenschutz), ist der Rechner bereits „verseucht".

Dr. Westerburg hat in Marburg und Freiburg Physik und Mathematik studiert. In der Folgezeit war er als Doktorand am Lehrstuhl von Prof. Dr. Friedrich Busse in Bayreuth und dort als Systembetreuer des Unix-Clusters der theoretischen Physik tätig. Er verfügt über Programmierkenntnisse (u.a. C, Fortran) und einschlägige Erfahrungen mit verschiedenen Betriebssystemen (u.a. IRIX, OSF1, Linux).

Seit dem 22. Juli 2002 ist *Frau Eva Kökeny* in der Arbeitsgruppe „Öffentlichkeitsarbeit und Internet" tätig. Sie wird im Rahmen Ihrer Tätigkeit die Grundlagen für einen koordinierten Einsatz von modernen Multimediatechniken im Rechenzentrum schaffen. Hierzu gehört zunächst die Evaluation von Spezialsoftware, die Auswahl und Definition von Standardwerkzeugen, die beispielhafte Erstellung multimedialer Inhalte für das Web, die Bereitstellung von Standardvorlagen, die Erarbeitung und Dokumentation adäquater Arbeitstechniken und die Schulung und Unterstützung der Mitarbeiter beim Einsatz der evaluierten Werkzeuge und Techniken. Frau Kökenys halbe Stelle ist vorerst auf ein Jahr befristet.

Frau Kökeny studierte an der Ludwig-Maximilians-Universität in München die Fächer Ägyptologie, Geschichte der Medizin und Philologie des Christlichen Orients. Bereits als Studentin war sie zwei Jahre als Hilfskraft am Rechenzentrum tätig. Nach ihrem Studium arbeitete sie als wissenschaftliche Hilfskraft im Zentrum für Weiterbildung und Wissenstransfer (ZWW) an der Universität Augsburg. Neben organisatiorischen Tätigkeiten vertiefte sie ihre Kenntnisse in diversen Programmpaketen (z.B. Microsoft PowerPoint, Adobe Photoshop, Illustrator und PageMaker). Frau Kökeny zeichnet sich für diese Stelle insbesondere durch ihren sicheren Umgang mit EDV-Werkzeugen sowie ihrer Kreativität aus.

Wir heissen Frau Eva Kökeny und Herrn Dr. Michael Westerburg herzlich im Rechenzentrum willkommen und wünschen ihnen bei ihrer Arbeit viel Freude und anhaltenden Erfolg.

0190-Dialer

Was sind die Gefahren und wie Sie sich davor schützen können

Der ursprüngliche und seriöse Nutzen von sogenannten 0190-Dialern liegt darin, bestimmte Dienste kostenpflichtig per Internet anzubieten. Das können z. B. Downloads kostenpflichtiger Software (Spiele, Programme, SMS-Logos), Support und andere Hilfeleistungen im Internet, Abruf kostenpflichtiger Nachrichtendienste und Informationen, oder Erotikangebote sein. Bei seriösen Anbietern wird der Nutzer auf entstehende Kosten im Voraus hingewiesen und der Dialer kann jederzeit wieder deinstalliert werden. Leider gibt es immer mehr schwarze Schafe unter den Anbietern, deren Dialer sich unbemerkt installieren und die Telefonrechnung des Nutzers in astronomische Höhen treibt. Dabei handelt es sich oft ganz schlicht um Betrug. Im Folgenden werde ich auf die Gefahren und die Methoden der 0190-Dialer eingehen und Möglichkeiten zum Schutz vorstellen.

Die Gefahren von 0190-Dialern

Wer einen DSL-Anschluss zu Hause hat, kann an dieser Stelle des Textes bereits aufatmen. Aufgrund der speziellen Technik von DSL Anschlüssen ist es nicht möglich eine spezielle Nummer anzuwählen, man meldet sich vielmehr an einem Netzwerk an. Somit stellen für DSL Nutzer Dialer keine Gefahr da.

Ganz anders bei Nutzern herkömmlicher Internetzugänge: 0190-Dialer wählen sich teils in Nummern ein, deren Einwahl schon einige Euros kostet und dann noch pro Minute hinzu. Die 0190-Nummern werden von diversen Netzbetreibern angeboten und kosten auch unterschiedlich viel.

Besonders tückisch sind Nummern mit der Vorwahl 0193. Wählt sich der Dialer in eine solche Nummer ein, so kann die Anwahl mehrere hundert Euro kosten. Der Besitzer der Nummer kann ganz flexibel festlegen wie tief er den ahnungslosen Opfern in die Tasche greift.

Alexander Heiß, Rechenzentrum

Wie schütze ich meinen PC vor Dialersoftware?

Dialer der neusten Generation nutzen Sicherheitslücken im System, wie z. B. Active X. Diese Technologie erlaubt es einen Dialer unbemerkt auf ein fremdes System zu laden, diesen unbemerkt zu installieren und zu starten. Das kann man verhindern indem man Active X im Browser oder E-Mail-Programm deaktiviert. Generell sollte man weder auf E-Mail-Angebote noch auf Installationsaufforderungen beim Surfen reagieren. Sicherheitszertifikate sagen gar nichts aus, jeder kann sie erstellen. Es werden teilweise auch gecrackte Dialer angeboten, die angeblich kostenlos sind. Das ist auch nur ein neuer Trick. 0190-Nummern sind immer kostenpflichtig, es ist nicht möglich diese Kosten zu umgehen.

Im Internet gibt es nunmehr einige Programme (z. B. 0190-Warner, YAW), die die Aktivitäten des DfÜ-Netzwerks überwachen und verhindern sollen, dass eine 0190, 0193, oder eine andere dieser teueren Vorwahlen gewählt wird. Leider finden die Betreiber der 0190-Dialer immer neue Wege diese Programme zu umgehen. So ist es auch möglich eine Einwahl über CAPI, Create Sockets, öffnen von Ports, TAPI zu erreichen. Manche Dialer entfernen gezielt die gängigsten Anti-Dialer aus dem Speicher, wodurch diese wirkungslos werden. Nichts desto trotz bieten aktuelle Anti-0190-Dialer Programme guten Schutz, vorausgesetzt man hält die Software aktuell, indem man sie regelmässig updatet. Auch eine Firewall, bzw. Software Firewall wie „Zone Alarm“ oder „Tiny Personal Firewall“ und eine aktuelle Antiviren Software sollte eigentlich auf keinem Internet-PC fehlen, da manche Dialer sich über Wurmviren verbreiten oder als Trojanerviren in ihr System gelangen. Der sicherste Weg ist allerdings die Sperrung der 0190 und 0193 Nummern beim Netzbetreiber. Hierdurch muss man natürlich auch auf seriöse und teilweise sinnvolle 0190-Dienste verzichten wie z.B. die Support-Hotlines vieler Hersteller. Zudem werden die 0190-Nummern bis 2004 nach und nach durch 0900-Nummern ersetzt werden. Ob man diese Nummern ebenfalls schon jetzt sperren kann sollte man direkt bei seinem Netzbetreiber erfragen.

Was tun wenn man Opfer geworden ist?

Einen hundertprozentigen Schutz kann man nicht erreichen. Bedenken Sie bitte, dass Dialer nur illegal sind, wenn Sie zu keiner Zeit auf die Kosten hingewiesen wurden. Wenn Sie eine überhöhte Telefonrechnung bekommen, reklamieren Sie diese sofort. Man kann bei der Telefongesellschaft den Betreiber der gewählten Nummer herausfinden und weitere Schritte einleiten. Sie sollten auf jeden Fall Beweise sammeln: Den Namen der Betreiberfirma, die Webseite von der der Dialer stammt, die Uhrzeit, u.s.w. Je lükkenloser die Beweise, desto höher liegen die Chancen die Rechnung nicht bezahlen zu müssen. Wenden Sie sich sofort an die Polizei und regionale Verbraucherschutzverbände die ihnen auch spezialisierte Anwälte nennen können. Zusätzlich sollten Sie schriftlich Beschwerde einreichen bei der „Freiwilligen Selbstkontrolle Telefonmehrwertdienste e.V., Liesegangstr. 10, 40211 Düsseldorf“ . Leider sind diese Fälle gesetzlich noch nicht eindeutig geregelt, aber die Chancen stehen gut, wenn man sich professionelle Hilfe sucht. Informieren Sie sich auch im Internet zu dem Thema, dort finden Sie sowohl Software zum Download als auch rechtliche Hinweise.
Links zum Thema im Internet

- *www.dialerschutz.de*
- *www.trojaner-info.de/dialer/dialer.shtml*
- *www.dialerundrecht.de*

Vertrauen ist gut, verschlüsseln ist besser

Eine Einführung in die Secure Shell

Für den Datentransfer über das Internet existiert ein Werkzeug, welches alle Wünsche erfüllt: die Secure Shell. Sie ist einfach zu benutzen, weit verbreitet und bietet ein hohes Maß an Sicherheit. Ihre Zuverlässigkeit basiert aber nicht zuletzt auf der richtigen Anwendung. Der folgende Artikel möchte dem unerfahrenen Einsteiger die grundlegenden Ideen der Secure Shell und ihren Befehlsumfang vorstellen.

Sicherheit bei der PC-Arbeit bedeutet nicht nur, Sicherungskopien wichtiger Dateien zu erstellen. Spätestens, wenn auf dem eigenen PC ein Virus sein Unwesen treibt und die persönlichen Daten oder gar der ganze Rechner befallen sind, ist es mit der Vorbeugung zu spät. Um sich unnötige Arbeit und vor allem viel ärger zu ersparen, bietet das Rechenzentrum den Studierenden und Mitarbeitern der Universität Augsburg bereits die Anti-Virensoftware Sophos an.

Die Zunahme des Datentransfers im Internet rückt noch einen weiteren Aspekt der Sicherheit immer mehr in den Vordergrund. Egal, ob beim Recherchieren im Internet oder beim Versenden und Empfangen von E-Mails, der eigene PC tauscht – für den Benutzer unsichtbar – permanent Daten mit fremden Rechnern aus. Übertragen werden u. a. nicht nur die persönlichen Daten, sondern gelegentlich auch das eigene Paßwort. Die Verbindung erfolgt zudem über viele Zwischenstationen, an denen neugierige Ohren mit geringem Aufwand alles mithören könnten.

Vorsicht geboten

Ein Ausweg wäre es, auf die Vorteile und Annehmlichkeiten des Internets zu verzichten. Eine attraktivere Alternative dazu bietet hingegen die Verschlüsselung der gesamten Kommunikation. Nur verschlüsselte Daten garantieren ihrem Besitzer, daß während ihrer Übertragung kein Unbefugter deren Inhalt liest oder gar verändert. Dies zu verhindern, ist die eigentliche Aufgabe der Secure Shell. Sie umfasst eine Reihe von Tools zum Datenaustausch mit entfernten Rechnern, die die herkömmlichen Programme, wie z. B. `telnet`, `rsh` oder `ftp`, vollständig ersetzen. Neben der Integrität der Daten bietet die Secure Shell mit der Authentifizierung den entscheidenden Vorteil. Im weltweiten Netz ist es nämlich überhaupt nicht selbstverständlich, daß der Rechner, mit dem man gerade Daten austauscht, auch der Web- oder Mailserver ist, für den man ihn eigentlich hält. Nur wer sich eindeutig ausweisen kann, darf mitreden.

Schlüsselbegriffe

Hierfür muß jeder Rechner zwei spezifische Schlüssel besitzen, einen *public* und einen *private key*. Nimmt ein Rechner (im weiteren *client* genannt) zu einem zweiten (dem *server*) Verbindung auf, so verschickt der *server* an den *client* seinen *public key*. Der *client* vergleicht diesen mit seiner Datenbank, die aus ihm bekannten Paaren „öffentlicher Schlüssel, Rechnername“ besteht. Ist dem *client* das Paar bekannt, chiffriert er mit dem *public key* des *servers* eine Zufallszahl und schickt diese zurück. Die Dechiffrierung ist nur dem *server* mit seinem *private key* möglich. Die gewählte Zufallszahl, mit der der weitere Datenaustausch verschlüsselt wird, kennen dann lediglich der *client* und der *server*. Eine exklusive Verbindung zwischen den beiden Rechnern ist zustande gekommen.

Einziger Knackpunkt bei dem vereinfacht dargestellten Authentifizierungsverfahren ist die zuverlässige Kenntnis des *public keys* des *servers*. Der Benutzer muß sich diesen vor dem ersten Aufruf der Secure Shell auf einem sicheren Weg beschaffen. Unabhängig von den Rechner *keys* kann jeder zusätzlich eigene User *keys* in das Verschlüsselungs- und Authentifizierungsverfahren einbringen. Falls doch einmal jemand unzulässig Zugriff auf den *private key* des *servers* bekommen sollte, verhindert dies das Entschlüsseln der eigenen Daten.

Zusätzlicher Schutz

Zur Erzeugung persönlicher Schlüsselpaare dient das Programm `ssh-keygen`. Ein spezielles Paßwort – die *passphrase* – verschlüsselt den eigenen *private key* und schützt ihn vor unauthorisiertem Zugriff. Die *passphrase* ersetzt beim Verbindungsaufbau das Userpaßwort. Der `ssh-agent` erspart die Eingabe der *passphrase* beim wiederholten Einloggen. Die *passphrases* der einzelnen Verbindungen werden im Speicher des Agenten gehalten und mit dem Programm `ssh-add` verwaltet.

Das klingt alles komplizierter als es tatsächlich ist. Die Akzeptanz der Secure Shell erklärt sich nämlich nicht nur mit dem verbesserten Schutz der eigenen Privatsphäre, sondern auch mit ihrer einfachen Anwendbarkeit und guten Dokumentation. Schwierig werden die Dinge einmal mehr aufgrund der unterschiedlichen Implementierung der Dienste unter den einzelnen Betriebssystemen. Der Befehlsumfang und die Möglichkeiten der Secure Shell lassen sich unter Unix übersichtlich darstellen. Im Anschluss wird auf die Besonderheiten unter Windows eingegangen.

Dr. Michael Westerburg, Rechenzentrum

SSH unter Unix

Auf den AIX-Rechnern des Rechenzentrums ist das Programmpaket *OpenSSH* des *OpenBSD* Projekts installiert. Zum Befehlsumfang der Secure Shell gehören im wesentlichen der *SSH*-Client `ssh` zum Einloggen auf entfernten Rechnern und die Programme `scp` und `sftp` zur Datenübertragung.

Um die Vorgehensweise anhand von Beispielen zu veranschaulichen, sei ein User angenommen, der auf dem lokalen Rechner `everest` den Loginnamen `hillary` und auf einem entfernten Rechner `eiger` einen Account namens `harrer` habe. Beim Aufrufen der Secure Shell fragt das Programm ggf. nach der Authentizität des *servers*. (Siehe Box 1)

Der *RSA key fingerprint* ist eindeutige Darstellung des *public keys* des Rechners `eiger`. Kennt man diesen zuverlässig und beantwortet die Frage positiv, wird das Paar „öffentlicher Schlüssel, Rechnername" in der Datei `known_hosts` gespeichert und die Abfrage des Paßworts des Users `hillary@eiger` erfolgt. Läuft der Account auf dem entfernten Rechner unter einem anderen Loginnamen, muß die Option `-l` gesetzt sein. (Siehe Box 2)

Der eigene Schlüssel

Ein wichtiges Werkzeug beim Arbeiten mit der Secure Shell ist das Programm `ssh-keygen`, u.a. zur Erzeugung des eigenen Schlüssels. Die *passphrase* sollte den üblichen Empfehlungen eines guten Paßworts genügen. Es dürfen keine einfachen Wörter sein, auch nicht, wenn sie um ein oder zwei Zahlen ergänzt werden. Sicherheit verspricht nur eine zufällige Folge von Buchstaben, Ziffern und Sonderzeichen. (Siehe Box 3)

`ssh-keygen` dient aber auch zur Ausgabe des *key fingerprints*. Hier existieren verschiedene Formate eines Schlüssels. Sie können jeweils mit der zugehörigen Option aufgerufen werden. (Siehe Box 4)

Mit dem eigenen Schlüssel läßt sich das Ausweisen beim Einloggen vereinfachen. Hierzu muß der User `hillary@everest` lediglich den öffentliche Schlüssel `~/.ssh/id_rsa.pub` aus seinem Homeverzeichnis in die Datei `~/.ssh/authorized_keys` seines Accounts `harrer@eiger` kopieren. Das Anmelden erfolgt dann einfach über die Eingabe der *passphrase*. (Siehe Box 5)

Falls jetzt noch dem `ssh-agent` die *passphrases* aller Schlüssel übergeben werden, erspart man sich ihre erneute Eingabe beim wiederholten Einloggen. Sämtliche Benutzerdaten legt *OpenSSH* im Verzeichnis `~/.ssh` ab. Wichtig sind hierbei die Zugriffsrechte. Private Schlüssel dürfen keinesfalls für andere lesbar oder schreibbar sein. (Siehe Box 6)

SSH und DCE

Das zur Verwaltung der Benutzerdaten an der Universität Augsburg verwendete *DCE* erlaubt keine Authentifizierung durch eigene Schlüssel und die Eingabe der *passphrase*. *DCE* nutzt eigene Authentifizierungsmechanismen, die die Eingabe des Userpaßworts erfordern. Die Benutzung der Secure Shell unterliegt keinen weiteren Einschränkungen.

Außer der Möglichkeit, sich auf entfernten Rechner einzuloggen, können mit dem Befehl `scp` Dateien übertragen und mit `ssh` auch Kommandos abgesetzt werden. Vergleichbar dem lokalen Kopieren mit `cp`, vererbt die Option `-p` die Zugriffsrechte. Überhaupt besteht bei den Optionen weitgehend übereinstimmung zwischen der Secure Shell und den herkömmlichen Befehlen `rsh` oder `rcp`. (Siehe Box 7)

Weiterleitung von TCP-Ports

Die Secure Shell kann aber mehr: Zur Verbesserung der Transferrate können der Verschlüsselungsalgorithmus ausgewählt und Daten während der übertragung komprimiert werden. Die Secure Shell erleichtert außerdem die Umleitung der graphischen Ausgabe. Das Setzen der Umgebungsvariablen *DISPLAY* erfolgt genauso automatisch, wie die Authentifi-

```
hillary@everest>ssh eiger
The authenticity of host 'eiger (111.222.33.4)' can't be established.
RSA key fingerprint is 5e:f6:1a:d0:95:2d:be:82:aa:be:a8:b9:f4:a0:b8:05.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'eiger,111.222.33.4' (RSA) to the list of known
  hosts.
hillary@eiger's password:
hillary@eiger>
```

Box 1: Authentifizierung beim Einloggen

```
hillary@everest>ssh -l harrer eiger
harrer@eiger's password:
harrer@eiger>
```

Box 2: Einloggen unter anderem Login-Namen

```
hillary@everest>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/hillary/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in   /home/hillary/.ssh/id_rsa.
Your public key has been saved in /home/hillary/.ssh/id_rsa.pub.
The key fingerprint is:
86:9a:ab:0f:05:ae:e0:f8:cb:8a:e1:dd:4d:f2:f6:2e  hillary@everest
hillary@everest>
```

Box 3: Erzeugung eines Schlüssels

```
harrer@eiger>cd /usr/local/etc
harrer@eiger>ssh-keygen -l -f ssh_host_rsa_key.pub
1024 5e:f6:1a:d0:95:2d:be:82:aa:be:a8:b9:f4:a0:b8:05 ssh_host_rsa_key.pub
```

Box 4: Ausgabe des *key fingerprints*

```
hillary@everest>ssh -l harrer eiger
Enter passphrase for key '/home/hillary/.ssh/id_rsa':
harrer@eiger
```

Box 5: Einloggen mit der *passphrase*

```
hillary@everest>ls -o /home/hillary/.ssh
-rw-----   1 hillary        951 Sep 01 17:55  id_rsa
-rw-r-r-   1 hillary        244 Sep 01 17:28  id_rsa.pub
-rw-r-r-   1 hillary        561 Sep 01 17:54  known_hosts
-rw-----   1 hillary        024 Sep 01 17:55  prng_seed
```

Box 6: Listing der Benutzerdaten

zierung für den Zugriff auf den *(lokalen) X*-Server. Auf diese Weise läßt sich, ohne weitere Befehle, der *X*-Client eines entfernten Rechners auf dem *(lokalen)* Bildschirm ausgeben. (Siehe Box 8)

Sehr nützlich ist die Umleitung von *TCP* Ports durch einen sicheren Secure Shell Tunnel. Hierdurch eröffnet sich beispielsweise die Möglichkeit, den Steuerkanal von ftp zu verschlüsseln. Diese Absicherung ist natürlich auch auf andere *TCP* Dienste anwendbar. Im folgenden soll der Port 2345 des Rechners `everest` zum ftp Port des Rechners `eiger` (typischer Weise der Port 21) umgeleitet werden. (Siehe Box 9)

Anschließend leitet die Secure Shell eine ftp Anfrage am Port 2345 des Rechners `everest` wie gewünscht um. (Siehe Box 10)

SSH und Windows

Auf den Windows Rechnern in den *CIP*-Pools des Rechenzentrums steht die *SSH* Secure Shell der Firma *SSH* Communications Security zur Verfügung. Zum Befehlsumfang gehört ein Programm zum Einloggen auf entfernten Rechnern, das mit einem Doppelklick auf das dazugehörige Icon *SSH-Telnet* gestartet werden kann. Im Startmenü unter *Programme – Telnet (SSH Secure Shell)* findet sich zusätzlich der *Secure File Transfer Client* zur Datenübertragung.

Unter Windows öffnet sich für jede Anwendung jeweils ein eigenes Fenster. Mit den für Windows üblichen Buttons und Pulldownmenüs bekommt der User Zugriff auf den gesamten Befehlsumfang der Secure Shell. Die erforderlichen Eingaben sind selbsterklärend, sowohl beim Verbindungsaufbau zu einem entfernten Rechner via *SSH Secure Shell* als auch beim Datentransfer mit dem *Secure File Transfer Client.*

Ist ein Fenster aktiv, genügt die Betätigung der Eingabetaste, um eine Verbindung zu einem entfernten Rechner aufzubauen. Zur Authentifizierung ist wieder die Bestätigung des *key fingerprints* des *servers,* jetzt aber im sog. Bubblebabble Format, gefordert.

Noch einmal zur Wiederholung: Die Kenntnis des *public keys* des *servers* ist ein wesentlicher Bestandteil des Authentifizierungsverfahrens. Nur bei zuverlässiger Kenntnis des Schlüssels, kann die Verbindung als sicher gelten. Das Programm `ssh-keygen` liefert den *key fingerprint* im Bubblebabble Format, wenn die Option `-B` gesetzt wird. (Siehe Box 11)

Die Erzeugung eigener User *keys* erfolgt unter dem Menüpunkt *Edit – Settings* und weiter im Dialogfenster unter *Global Settings – Appearance – User Keys.* Die Einschränkung des Authentifizierungsverfahrens beim Verbindungsaufbau mit einem *DCE* Account gilt auch hier. Der Benutzer muß sich mit seinem Userpaßwort anmelden. Seine Daten werden lokal unter *C:\\WINNT\Profiles\hillary\Application Data\SSH* abgelegt. Die *public keys* der als bekannt anerkannten Rechner liegen im Unterverzeichnis *HostKeys.* Da sie in den CIP-Poo.ls beim Beenden einer Sitzung komplett gelöscht werden, erfolgt die Frage nach dem *public key* jeden Tag auf's Neue.

```
hillary@everest>scp -p ~/file1.txt harrer@eiger:/tmp
hillary@everest>scp harrer@eiger:/tmp/file1.txt ~/file2.txt
hillary@everest>ssh -l harrer eiger rm /tmp/file1.txt
hillary@everest>ls -o file?.txt
 -rw-r--   1 hillary        2 Sep 01 19:52  file1.txt
 -rw-r--   1 hillary        2 Sep 01 19:53  file2.txt
```

Box 7: OpenSSH Befehlsumfang `ssh` und `scp`

```
hillary@everest>ssh -f -X eiger xterm
hillary@eiger's password:
hillary@everest
```

Box 8: Umleiten der graphischen Ausgabe

```
hillary@everest>ssh -l harrer -g -L 2345:eiger:21 eiger
harrer@eiger's password:
harrer@eiger>
```

Box 9: Weiterleitung von TCP-Ports

```
hillary@everest>ftp hillary 2345
Connected to hillary.
220 eiger FTP server (Digital UNIX Version 5.60) ready.
Name (hillary:everest): harrer
331 Password required for harrer.
Password:
230 User harrer logged in.
ftp>
```

Box 10: Verschlüsselter Datentransfer

```
harrer@eiger>cd /usr/local/etc
harrer@eiger>ssh-keygen -B -f ssh_host_rsa_key.pub
1024 xumer-suvif-novim-sucyf-dilyv-vasop-paveb-vekuf-dodum-fozop-lexox
  ssh_host_rsa_key.pub
```

Box 11: Ausgabe des *key fingerprints*

Sicherheit zuhause

Sehr nüzlich ist der *Secure File Transfer Client,* der eine sichere Datenübertragung gewährleistet, beispielsweise zwischen dem *RZ*-Account und dem eigenen PC daheim. Seine Installation empfiehlt sich auch, weil sämtliche Dienste des Rechenzentrums, die heute noch eine unverschlüsselte übertragung der Paßwörter zulassen, mittelfristig durch sichere Programme ersetzt werden.

Die *SSH* Software wird auf dem ftp-Server der Universität Augsburg unter *pub – packages – ssh* bereitgestellt, wobei an dieser Stelle auf die Lizenzvereinbarungen hingewiesen wird. Ist die Software auf dem eigenen PC installiert, kann sich jeder, der über einen Account an der Universität Augsburg verfügt, mit seinem Loginnamen und Userpaßwort z.B. an einem der *AIX* Rechner im *CIP* Pool anmelden. Dies sind die Rechner
`uxpool01.student.uni-augsburg.de,`
`...,`
`uxpool18.student.uni-augsburg.de.`

Für alle weiterführenden Fragen sei abschließend auf die Quellen in der Literaturliste verwiesen.

- Homepage des OpenSSH Projekts *www.openssh.org*
- Homepage der SSH Communications Security Corp *www.ssh.com*
- SSH The Secure Shell, D.J. Barrett, R.E. Silverman, O'Reilly Verlag *(www.snailbook.com)*
- OpenSSH aus der Sicht des Admins, Karl-Heinz Haag, Linux Magazin, 5/2002 und 7/2002

Modernisierung der Hausdruckerei

Die Hausdruckerei auf dem Weg zum innovativen Servicezentrum

Moderne Hausdruckereien sind integraler Bestandteil serviceorientierter Hochschulen. Kostentransparenz und -verantwortung sollen die Effizienz der Verwaltung sicherstellen, um den verantwortungsvollen Umgang mit öffentlichen Mitteln gewährleisten zu können. Wer eine innovative Universität betreiben will, braucht dazu die Effizienz-Potenziale einer modernen Infrastruktur.

Die Qualität der Druckerzeugnisse ist Spiegelbild einer modernen Hausdruckerei, da diese als Bestandteil einer hervorragend organisierten Universitätsverwaltung sowohl gegenüber den Fakultäten als auch nach Außen in Erscheinung tritt.

Zustand vorher

Der Kern der Hausdruckerei der Universität Augsburg bestand aus einer Grosskopiermaschine und diversen veralteten Geräten zur Endbearbeitung. Damit wurden im Durchschnitt monatlich circa 250 Druckaufträge mit einem Gesamtvolumen von etwa 300.000 Blatt Papier durchgeführt. Die Druckerzeugnisse werden je nach Bedarf geschnitten, gefalzt und geheftet. Leider musste bereits bei Fotodruck oder für farbige Prospekte und Broschüren auf andere Druckereibetriebe zurückgegriffen werden. Da jedoch gerade diese Ansprüche wachsen musste die Hausdruckerei der Universität Augsburg modernisiert werden.

Planungen zur Modernisierung

Durch Einführung netzwerkfähiger Digitaldruckmaschinen, die mit Printing-on-Demand-Funktion ausgestattet sind, ist binnen kürzester Zeit ein kostendeckender Betrieb sichergestellt.

Christian Schmidt,
Referat V/3, Verwaltung

Printing-on-Demand bedeutet Drucken nach Bedarf und bringt Vorteile, wie beispielsweise Kostenreduzierung, Einsparung von Lagerkapazität, Transport-Optimierung oder eine bislang nicht vorstellbare Aktualität zu erstellender Dokumente. Wer eine innovative Universität betreiben will, braucht eine moderne Infrastruktur. Dies zeigt sich auch in Tendenzen hin zu modernen Kompetenzzentren. Um den heutigen Ansprüchen der Kunden gerecht zu werden, war die Modernisierung der Hausdruckerei zwingend erforderlich.

Konkret wirkt sich dies für den Kunden so aus: Anstatt eine Druckvorlage in der Druckerei abgeben zu müssen genügt es, per E-Mail oder auch per Diskette/CD eine Datei im druckfähigen Format an die Hausdruckerei zu übermitteln. Dazu muss auf dem Rechner des Kunden nur der Treiber der Digitaldruckmaschine installiert werden. Beim Erzeugen der druckfähigen Datei wird dann – anstatt eines angeschlossenen Druckers – dieser Druckertreiber ausgewählt. Einfacher und schneller geht es fast nicht mehr.

Diese Modernisierungsmaßnahme wurde nicht nur seitens der Verwaltung der Universität Augsburg, sondern auch von den verschiedenen Lehrstühlen angeregt. Zur Durchführung dieser Maßnahme waren finanzielle und personelle Mittel zwingend notwendig.

Die Möglichkeit zukunftsorientiert zu agieren, um bei dem fortschreitenden Wettlauf mit anderen Universitäten sowie bei dem Einsatz neuer Technologien konkurrenzfähig zu bleiben, durfte nicht verpasst werden.

Aktueller Stand

- Verträge wurden bereits mit der Firma Canon unterzeichnet
- es stehen momentan zwei s/w- und eine Farb-Digitaldruckmaschine zur Verfügung
- weitere neue Endbearbeitungsgeräte wurden beschafft (Laminieren, Planax, Spiralbinder, komplettes Endverarbeitungsangebot z. B. Block und Satzverleimung, Broschüren in DIN A5 und DIN A4)
- ein in den Ruhestand getretener Mitarbeiter wurde seit September durch Herrn Geirhos ersetzt, d. h. die Annahme von Druckaufträgen erfolgt über Frau Zankl und Herrn Geirhos. Es wird auch gerne jederzeit fachgerechte Beratung angeboten.
- die Hausdruckerei ist nun auch per E-Mail *(hausdruckerei@verwaltung.uni-augsburg.de)* erreichbar
- zukünftig Drucken über das interne Uni-Netzwerk in die Hausdruckerei möglich
- neues Druckauftragsformular mit sämtlichen Neuerungen der Angebote in der Hausdruckerei. Auch über das Uni-Netz abrufbar.

Fazit

In diesem Servicezentrum sind zwei Themenfelder von besonderer Bedeutung:

Vernetztes Printing-on-Demand für:

- höhere Qualität,
- schnellere Verfügbarkeit,
- geringere Seiten- und Systemkosten,
- Vermeidung von Lagerhaltung wie in bisherigem Umfang.

Transparenz für

- wirtschaftliche Betriebsführung in der Verwaltung,
- das Berichtswesen,
- das Management by Objectives.

Diese Modernisierungsmaßnahme mit den neuen Möglichkeiten des Digitaldrucks und der Einbettung in die vorhandene Netzwerkstruktur wird viele Geschäftsprozesse grundlegend verbessern. Entscheidend dabei bleibt, dass die neue Vielfalt zum Vorteil des Kunden genutzt wird.

Kleiner Zwerg ganz groß

Die Datenbank MySQL und der Einsatz von InnoDB-Tabellen-Typen mit Transaktionskonzept

Thomas Birke, Rechenzentrum

Durch Installation des kostenlosen Zusatzpaketes InnoDB, kann MySQL mit geringem Aufwand um Transaktionen, ein Transaktions-Management, `FOREIGN KEYS` und eine ausgeklügelte Crash Recovery erweitert werden. Aus dem Zwerg MySQL wird so ein kleiner Riese in einer weiten und rauhen Datenbanklandschaft.

Eines der grundlegenden Konzepte in modernen kommerziellen und nichtkommerziellen Datenbank-Systemen ist der gleichzeitige Zugriff mehrerer Benutzer auf ein Datenbank-System (Multiprogramming) mit bestimmten Garantien durch das System. Betrachten wir dazu ein vereinfachtes Bank-Szenario, reduziert auf einige Konten und Transaktionen, die Konten manipulieren und entsprechend die Kontostände aktualisieren. Manipulationen im täglichen Bankgeschäft sind z. B. die Gutschrift von Geldbeträgen oder die Abbuchung von Geldbeträgen auf andere Konten. Damit mehrere Kunden gleichzeitig durch die Bank bedient werden können, sollen diese Vorgänge parallel ablaufen. Plötzlich geht bei der einer Buchung ein Betrag von mehreren 1.000 Euro – nicht mehr nachvollziehbar – verloren, ein Softwaredefekt der Bank ändert die Kontostände der Kunden, oder mehrfach, parallele Buchungen liefern jeweils unterschiedlich, falsche Kontostände. Weitere Horrorszenarien sind denkbar. Welcher Kunde würde es nun seiner Bank gestatten, bei der Kontoführung – eine typische Datenbank Anwendung – bei gleichzeitiger multipler Buchung zu schlampen?

Zur Umsetzung dieses „Garantie"-Konzeptes werden als Basisstruktur Transaktionen eingesetzt. Transaktionen sind gekapselte Programmeinheiten, die auf Daten zugreifen und/oder diese auch manipulieren dürfen. Transaktionen erfüllen und garantieren bestimmte Grundprinzipien, welche das „Gütesiegel" einer einzelnen Transaktion wiederspiegelt. Damit die Verlässlichkeit der Datenbank bei vielen, gleichzeitig auftretenden Transaktionen nicht in Frage gestellt werden kann, muss das System die Interaktion zwischen konkurrierenden Transaktionen mittels sinnvoller Lese- und Schreibsperren (Locking) kontrollieren und koordinieren. Ein solches Modell, basierend auf Sperrmechanismen, bezeichnet man als Concurrency Control.

In MySQL ist der Mechanismus zur Concurrency Control, wie in der letzten Ausgabe von connect beschrieben, nicht sonderlich ausgeprägt implementiert. Traditionell führt MySQL den MyISAM-Tabellen-Typus ein. Dieser unterstützt Locking ausschließlich auf Tabellenebene und nicht auf Datenebene. Es wird daher als nicht feingranular bezeichnet, d. h. Locks können nicht auf einer Teilmenge der Daten angewandt werden. Ein Datenbank-Szenario mit ausgeklügeltem Transaktionskonzept, z. B. ein Bibliothekssystem mit einem komplexen Buchungssystem, kann nur mit großen Klimmzügen oder gar nicht umgesetzt werden. Abhilfe schafft hier zusätzliche Software, um die MySQL erweitert werden kann. Optional gibt es drei Transaktions-unterstützende Tabellen-Typen in Form von Zusatzpaketen: BerkleyDB (BDB), InnoDB und Gemini. Transaktions-unterstützende InnoDB-Tabellen-Typen implementieren feingranulare Lock Mechanismen.

In diesem Artikel soll ausschießlich auf den InnoDB Tabellen Typ eingegangen werden. InnoDB unterstützt:

- `COMMIT` – erfolgreicher Abschluss einer Transaktion.
- `ROLLBACK` – das Zurücksetzen von Transaktionen.
- Recovery – zur Herstellung eines gesunden Datenbankzustandes im Fehlerfall.

Der InnoDB-Tabellen-Typ kann auf sämtlichen Unix/Linux Derivaten, MacOSx und Windows in Verbindung mit MySQL installiert und eingesetzt werden. InnoDB unterstützt Locking in der Art, wie es auch bei den meisten kommerziellen Systemen eingesetzt wird: auf dem Row-Level, d. h. auf der Zeilenebene einer Tabelle. InnoDB ist somit entsprechend feingranularer als der MyISAM-Tabellen-Typ, der diese Sperreigenschaft nur auf Tabellenebene gestattet. Man bezeichnet diese Art von Locking bei InnnoDB auch als „Index-Record Locks", da mittels eines entsprechend entwickelten Algorithmus

- Shared Locking (vgl. MyISAM read lock, ähnlich dem Oracle Consistent Non-Locking Read bei `SELECT`-Statements): nach dem Sperren ist eine Manipulation der Daten durch `UPDATE` oder `DELETE` nicht möglich; die Suche mittels `SELECT` ist gestattet,
- bzw. exclusives Locking: nach dem Sperren ist eine Manipulation der Daten durch `UPDATE, DELETE` und `SELECT` nicht gestattet,

auf den Index Records durchgeführt werden. Dies führt zur Steigerung der Anzahl gleichzeitiger Benutzer und steigert die Performance des Systems. Performancetests (Benchmarks) finden Sie auf der Homepage von InnoDB *(http://www.innodb.com)*.

Darüber hinaus erweitert InnoDB MySQL um `FOREIGN KEY` Constraints, inklusive der ergänzenden Möglichkeit zum `DELETE ON CASCADE`. Bei `DELETE ON CASCADE` wird, falls ein Ein-

```
[mysqld]
# You can write your other MySQL server options here
# ...
#                           Data file(s) must be able to
#                           hold your data and indexes.
#                           Make sure you have enough
#                           free disk space.
innodb_data_file_path = ibdata1:10M:autoextend
#                           Set buffer pool size to
#                           50 - 80 % of your computer's
#                           memory
set-variable = innodb_buffer_pool_size=70M
set-variable = innodb_additional_mem_pool_size=10M
#                           Set the log file size to about
#                           25 % of the buffer pool size
set-variable = innodb_log_file_size=20M
set-variable = innodb_log_buffer_size=8M
#                           Set ..flush_log_at_trx_commit
#                           to 0 if you can afford losing
#                           some last transactions
innodb_flush_log_at_trx_commit=1
```

Abbildung 1: Beispiel eines MySQL-Konfigurationsfiles.

trag, auf den eine Fremdschlüsselbeziehung verweist, gelöscht wird, auch der Eintrag in der entsprechenden Tabelle gelöscht in der der Fremdschlüssel steht. Tabellen vom Typ InnoDB können ohne Probleme mit dem traditionellen MyISAM Tabellen-Typ von MySQL kombiniert werden.

Das Produkt InnoDB wird unter der GNU GPL License Version 2 vom Juni 1991 vertrieben.

Installation

Technisch ist das Produkt InnoDB ein eigens entwickeltes Datenbank-Backend für MySQL mit eigenem Bufferpool, Caching der Daten und Indices im Hauptspeicher. Tabellen des Typus InnoDB können von jeder beliebigen Größe(!) sein und werden in einen eigens für InnoDB konfigurierten Bereich abgelegt. Selbst Restriktionen wie die 2 Gigabyte Grenze unter Windows können aufgeweicht werden (Kleiner Tipp am Rande: Vorsicht, damit nicht in die Bereiche des Betriebssystems geschrieben wird!). Ab MySQL 3.23.34a und MySQL-max ist das Produkt InnoDB im MySQL-Quellcode enthalten.

Damit unter Unix/Linux der InnoDB-Tabellen-Typ verwendet werden kann, muss das Binary mit der Option

```
./configure ... -with-InnoDB
```

kompiliert werden. Für Windows ist das Paket in MySQL-max bereits enthalten. Damit der Datenbank-Administrator InnoDB-Tabellen erzeugen kann, müssen einige Optionen im MySQL-Konfigurationsfile `my.cnf` für Unix/Linux bzw. `my.ini` für Windows – diese werden am besten als globale Server Variablen gesetzt – eingetragen werden (Abbildung 1).

Als Minimaleinstellung genügt der Eintrag `innodb_data_file_path`. Dabei können die in `innodb_data_file_path` angegebenen InnoDB-Files auch ins Raw-Device gelegt werden. Achtung: neue Directories müssen von Hand erstellt werden. Mit `default-table-type=innodb` erfolgt die permante Verwendung des InnoDB-Tabellen-Typs. Bei Systemtabellen sollte man davon absehen eine händische Umwandlung von MyISAM Tabellen durch `ALTER TABLE … TYPE=INNODB` (Ab Version > 3.23.50) durchzuführen. Weitere Einstellungen und Optimierungen der InnoDB Tabellen entnehmen Sie bitte dem Handbuch.

Abschließend muss der MySQL Sever neu gestartet werden, und Sie können mit den Tabellen vom Typ InnoDB loslegen.

Anlegen einer Datenbank

Das Erstellen von InnoDB-Tabellen geschieht wie folgt. Dargestellt wird eine Datenbank `Test`, die eine einfache eins zu eins Beziehung zwischen den Tabellen `MyTestA` und `MyTestB` darstellt, wobei `MyTestB` den Schlüssel inta, als Fremdschlüssel, von `MyTestA` erhält (Abbildung 2). Ab Version 3.23.50 liefert folgender Befehl die definierten `FOREIGN KEY` Beziehungen:

```
SHOW CREATE TABLE MyTestA
SHOW TABLE STATUS FROM DB
  LIKE 'T'
```

(Anmerkung: `PRIMARY KEYS` werden in den InnoDB-Tabellen mit Hilfe von Cluster Indices angelegt.)

Ganz interessant kann folgender Befehl sein. Mit `SHOW TABLE STATUS FROM Test LIKE 'MyTestB'` kann die Größe der InnoDB Tabelle bestimmt werden.

Transaktions-Management

Dem Datenbank-Administrator stehen folgende Befehle zum selbständigen Taransaktions-Management zur Verfügung:

```
CREATE DATABASE Test;

USE Test;

CREATE TABLE MyTestA(
     inta INT NOT NULL PRIMARY KEY,
     intb INT NOT NULL,
     intc INT NOT NULL
) TYPE=INNODB;

# Tabelle mit Fremdschlüsselbeziehung. Achtung: Index nicht
# vergessen! sonst klappt's nicht.
CREATE TABLE MyTestB(
     inta INT NOT NULL,
     INDEX inta_index (inta),
     intb INT NOT NULL,
     FOREIGN KEY (inta) REFERENCES MyTestA(inta)
                  ON DELETE CASCADE
) TYPE=INNODB;
```

Abbildung 2: Anlegen der Datenbank `Test`.

- BEGIN,
- COMMIT,
- ROLLBACK,
- SET AUTOCOMMIT=0, welches bei einem erneutem Verbindungsaufbau standardmäßig auf 1 (ein) gesetzt ist.

Es folgt ein Beispiel für ein benutzerdefiniertes Transaktions-Management, welches über ein Perl-DBI realisiert ist (Abbildung 3):

Das Programm liefert folgende Ausgabe:

```
1. Die Datenbank enthaelt das Tuppel(,,)
2. Die Datenbank enthaelt das Tuppel(,,)
3. Die Datenbank enthaelt das Tuppel(1,1,1)
4. Die Datenbank enthaelt das Tuppel(1,1,1)
```

An dieser Stelle ist anzumerken, dass je nach Schwere eines Fehlers ein COMMIT bzw. ein ROLLBACK eingeleitet wird. Folgende SQL-Statements erzeugen explizit ein COMMIT der aktuellen Transaktion: ALTER TABLE, BEGIN, CREATE INDEX, DROP DATABASE, DROP TABLE, RENAME TABLE, TRUNCATE, LOCK TABLES, UNLOCK TABLES. Das CREATE Statement wird als Sonderfall behandelt und ist losgelöst von der Concurrency Control, d. h. ein ROLLBACK funktioniert nicht. LOCK TABLES in MySQL entspricht BEGIN TRANSACTION. In diesem Falle wird AUTOCOMMIT MODE auf 0 gesetzt, d. h. es muss vom Datenbank-Administrator ein COMMIT gesetzt werden, sonst wird die Transaktion nicht geschrieben.

Das Transaktion Isolation Level ist ab Version 3.23.50 automatisch auf REPEATABLE READ gesetzt. Das Transaktion Isolation Level dient zur Zusicherung bestimmter Restriktionen bei konkurrierenden Transaktionen, d. h. es werden gewisse Concurrency Control Mechanismen festgelegt. Mit REPEATABLE READ geht man den Kompromiss ein, dass „Phantom Reads“ auftreten – d. h. Eingaben, die vorher noch nicht sichtbar waren, können bei wiederholten Anfragen auftauchen, da in der Zwischenzeit die Tabelle durch eine weitere Transaktion manipuliert wurde. Das Beispiel (Abbildung 3) mit SELECT Statements ohne „LOCK IN SHARE MODE SERIALIZABLE“ Zusicherung, liefert dann folgendes Ergebnis:

```
#!/usr/bin/perl

use DBI;

#Initialisierung der Datenbankhandles dbh1, dbh2
$dbh1 = DBI->connect("DBI:mysql:database=Test;
               host=xyz.RZ.Uni-Augsburg.DE","user","password",
               {AutoCommit => 0, # Ausschalten Autocommit
               RaiseError => 1, })
      or die "DB-Fehler: $DBI::errstr\n";
$dbh2 = DBI->connect("DBI:mysql:database=Test;
               host=xyz.RZ.Uni-Augsburg.DE","test","*poole*",
               {AutoCommit => 0, , # Ausschalten Autocommit
               RaiseError => 1,})
      or die "DB-Fehler: $DBI::errstr\n";

#Begin des Transaktions-Managements.
my @failed; # Nur zur Fehlerausgabe

#Jetzt geht's los!
eval{
   $sth = $dbh1->prepare("SELECT * FROM Test.MyTestA")
      or die "Fehler: $DBI::errstr\n";
   $sth->execute
      or die "Fehler: $DBI::errstr\n";
   #Ausgabe des SELECT-Statements
   while (($inta,$intb,$intc)= $sth->fetchrow_array){
      print "1. Die Datenbank enthaelt das Tuppel($inta,$intb,$intc)\n"
   }
   #Einlesen eines neuen Wertes in die Datenbank
   $sth = $dbh2->prepare("INSERT INTO Test.MyTestA VALUES (1,1,1)")
      or die "Fehler: $DBI::errstr\n";
   $sth->execute
      or die "Fehler: $DBI::errstr\n";
   $sth = $dbh1->prepare("SELECT * FROM Test.MyTestA")
      or die "Fehler: $DBI::errstr\n";
   $sth->execute
      or die "Fehler: $DBI::errstr\n";
   #Ausgabe des SELECT-Statements
   while (($inta,$intb,$intc)= $sth->fetchrow_array){
      print "2. Die Datenbank enthaelt das Tuppel($inta,$intb,$intc)\n";
   }
   #Einlesen eines neuen Wertes in die Datenbank wird commited
   $dbh2->commit();
   $sth = $dbh1->prepare("SELECT * FROM Test.MyTestA LOCK IN SHARE MODE")
      or die "Fehler: $DBI::errstr\n";
   $sth->execute
      or die "Fehler: $DBI::errstr\n";
   #Ausgabe des SELECT-Statements
   while (($inta,$intb,$intc)= $sth->fetchrow_array){
      print "3. Die Datenbank enthaelt das Tuppel($inta,$intb,$intc)\n";
   }
   #SELECT-Statements werden commited.
   $dbh1->commit();
   $sth = $dbh1->prepare("SELECT * FROM Test.MyTestA LOCK IN SHARE MODE")
      or die "Fehler: $DBI::errstr\n";
   $sth->execute
      or die "Fehler: $DBI::errstr\n";
   #Ausgabe des SELECT-Statements
   while (($inta,$intb,$intc)= $sth->fetchrow_array){
      print "4. Die Datenbank enthaelt das Tuppel($inta,$intb,$intc)\n";
   }
};

# Tritt ein Fehler auf ... heul
if ($@){
   #Fehlermeldung ausgeben
   warn "Fehler beim Verarbeiten: $@\n";
   #Etwaige Aenderungen werden Rueckgaengig gemacht
   $dbh1->rollback();
   $dbh2->rollback()
};

#habe fertig
$dbh1->disconnect()
      or warn "DISCONNECT  Fehler: $DBI::errstr\n";
$dbh2->disconnect()
      or warn "DISCONNECT  Fehler: $DBI::errstr\n";
```

Abbildung 3: Beispiel für ein benutzerdefiniertes Transaktions-Management.

```
1. Die Datenbank enthaelt
   das Tuppel(,,)
2. Die Datenbank enthaelt
   das Tuppel(,,)
3. Die Datenbank enthaelt
   das Tuppel(,,)
4. Die Datenbank enthaelt
   das Tuppel(1,1,1).
```

Die strengste Zusicherung an Transaktionen ist die Forderung nach vollständiger Serialisierbarkeit konkurrierender Transaktionen (Transaktion Isolation Level: `SERIALIZABLE`). Das Transaktion Isolation Level kann wie folgt gesetzt werden:

```
Set [SESSION | GLOBAL ]
  TRANSACTION ISOLATION
  LEVEL [SERIALIZABLE |
  REPEATABLE READ]
```

Die im SQL-99-Standard vorgesehenen Transaktion Isolation Level `READ UNCOMMITED` und `READ COMMITED` werden nicht unterstützt und wie `REPEATABLE READ` behandelt.

Standardmäßig garantiert `REPEATABLE READ` konsistente Lesezugriffe. Realisiert ist das ganze durch ein *Shared Locking*. Dies bedeutet, eine Query erhält zu einem Zeitpunkt eine Datenbanksicht, d. h. einen bestimmten Ausschnitt der Datenbank. Für alle Transaktionen bedeutet das: Änderungen, welche vor diesem Zeitpunkt durchgeführt wurden, gelten als committed, alle übrigen als uncommited. Alle konsistenten Lesezugriffe verwenden denselben Snapshot innerhalb einer Transaktion. Werden Änderungen an einer Tabelle durchgeführt tauchen diese erst im nächsten neu generierten Snapshot auf. Den gesamten Vorgang bezeichnet man auch als Multi-Versioning Concurrency Modell.

Tabelle 1 verdeutlicht, welche Auflösung der Locks bei den entsprechenden SQL-Statements im Transacation Isolation Level `REPEATABLE READ` erfolgt

Es gibt aber auch die Möglichkeit zum Sperren konkurrierender Lesezugriffe, z. B. bei Manipulation der Tabellen oder wenn ein „Phantom Read“ ausgeschlossen werden soll. Dies geschieht mit Hilfe des „exclusiven Locks“. SQL-Anfragen müssen hierzu wie folgt formuliert werden:

```
SELECT * FROM MyTestB LOCK
  IN SHARE MODE SERIALIZABLE.
```

Alle Tabellen werden während einer Transaktion für alle konkurrierenden Zugriffe gesperrt; explizit ist auch der Lesezugriffe mittels `SELECT` nicht gestattet. Auf diese Art kann referentielle Integrität garantiert werden.

SQL-Statement	Isolation Level – `REPEATABLE READ`
`SELECT ... FROM ...` [1.]	Shared Locks
`SELECT ... FROM ... LOCK IN SHARE MODE` [2.]	Exclusive Locks auf Indexebene
`INSERT INTO ... VALUES`	Exclusive lock auf die eingelesene Zeile
`INSERT INTO T SELECT … FROM S WHERE …`	Exclusive Locks
`CREATE TABLE ... SELECT ...`	Siehe `SELECT` [1.), 2.]
`REPLACE`	Exclusive `Lock` auf die eingelesene Zeile
`UPDATE … SET … WHERE`	Exclusive `Locks` auf Indexebene
`DELETE FROM ... WHERE ...`	Exclusive `Locks` auf Indexebene
`FOREIGN KEY`	Shared `Lock` auf Datenrecord-Basis
`LOCK TABLES ...`	Locks auf Tabellenebene
`SHOW TABLE STATUS`	Exclusive `Lock` auf Zeilenbasis.

Tabelle 1: Auflösung SQL-Statement/Locking im Repeatable Read Isolation Level.

Probleme im Umgang mit exklusiven Locks sind Verklemmungen, sogenannte Deadlocks. Formuliert man im Beispiel (Abbildung 3) alle `SELECT` Statements mit `SELECT * FROM MyTestB LOCK IN SHARE MODE SERIALIZABLE`, erhält man nur folgende Ausgabe:

```
1. Die Datenbank enthaelt
   das Tuppel(,,),
```

danach kommt der Fehler Timeout.

Ein Deadlock wird durch einen Timeout aufgelöst. Dies bedeutet alle `INSERT`-Statements werden durch ein `ROLLBACK` rückgängig gemacht. Generell können Deadlocks durch Eintrag des Parameters innodb_lock_wait_timeout in `my.cnf` bzw. `my.ini` im angegebenen Zeitintervall aufgelöst werden.

Recovery

Nach Ausfall des Datenbank-Servers werden bei Verwendung des InnoDB Tabellen-Typs automatisch die Datenbank-Logs untersucht, die jeder Transaktion automatisch angelegt werden. Zusätzlich wird versucht aus diesen Daten einen funktionsfähigen Datenbank-Server zu rekonstruieren. Realisiert wird dies durch einen Roll-Forward aller commited Transaktionen und einem Roll-Back aller nicht committed Transaktionen – es wird also versucht einen möglichst aktuellen Datenbankzustand zu rekonstruieren. Checkpoint Labels können gesetzt werden. Ein Checkpoint Label ist ein fest eingetragener Zeitpunkt in der Log-Folge des Datenbank-Logs zu dem alle Daten entsprechend dieser abgeschlossenen Transaktion erfolgreich manipuliert worden sind. Alle Informationen aus dieser Datenbank-Logdatei können auf Grund von Ceckpoint-Labels zur performanteren Wiederherstellung des Systems (Recovery) verwendet werden.

Monitoring

Ein Monitoring und das Auslesen von Statistiken der InnoDB ist ab Version 3.23.52 mit Hilfe des Befehls `SHOW INNODB STATUS` möglich. Analoges kann in älteren Versionen aus dem File *yourhostname.err* gelesen werden.

Zusammenfassung

InnoDB-Tabellen verstärken den Einsatz von MySQL durch Crash Recovery und ein ausgeklügeltes Transaktions-Management enorm. Erst hierdurch wird MySQL zur echten Datenbank und zu einer wirklichen Alternative kommerzieller Datenbank-Produkte. Alle Komponenten für die Verwendung von InnoDB-Tabellen sind leicht zu installieren und wurden auf AIX 4.3.3 unter MySQL 3.23.51 erfolgreich konfiguriert und getestet. Selbst das Einspoolen von 10.000 Datensätzen funktioniert schnell und reibungslos. Das komfortable Zusatzfeature für Monitoring kann durch ein kommerzielles Zusatzprodukt verstärkt werden, welches bei *www.innodb.com* zu beziehen ist. Im Großen und Ganzen ist InnoDB ein hervorragendes Paket, das MySQL zur kostengünstigen Alternative gegenüber teuren, kommerziellen Produkten wachsen lässt.