Universität Karlsruhe (TH)
Rechenzentrum

juni / juli 2003

RZ news

Internet-Gefahren

Viren, Würmer, Trojaner, Hoaxes

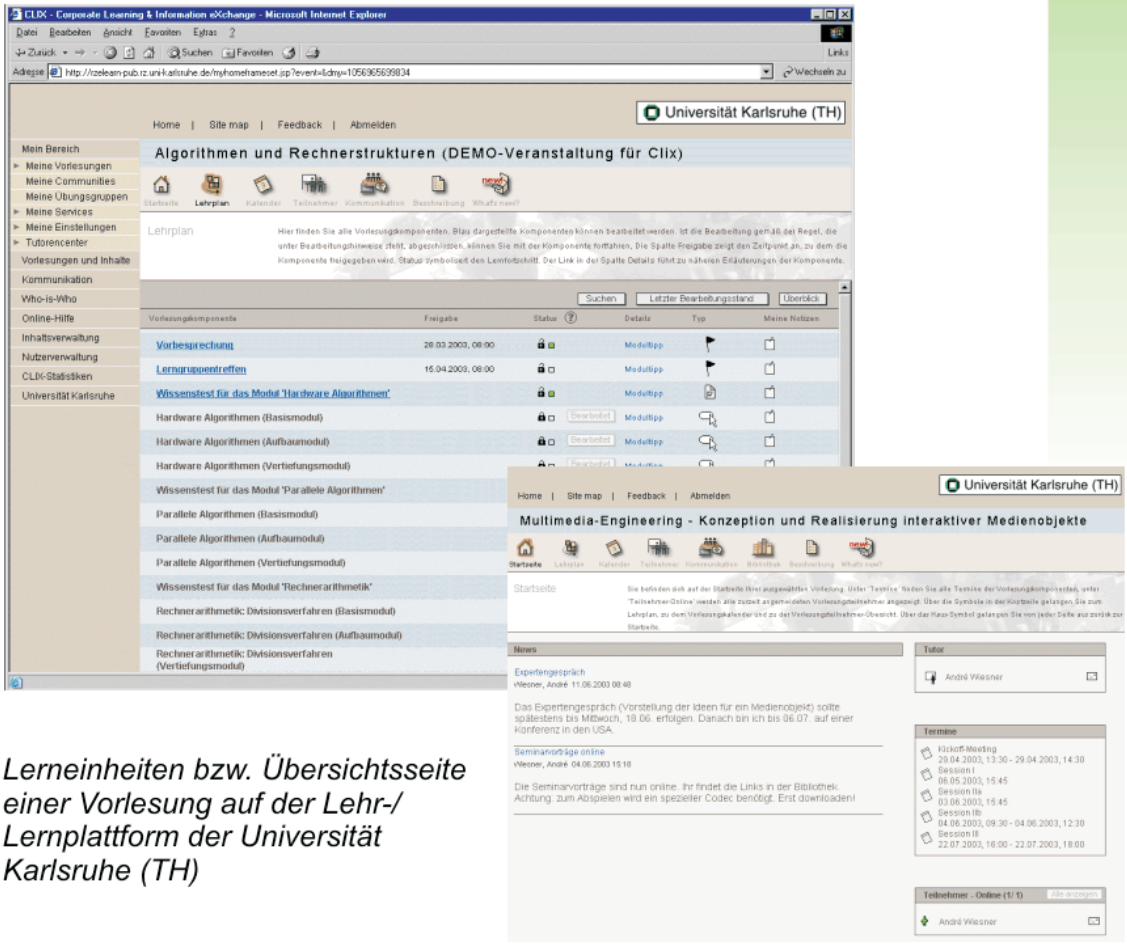
Multimedia Transfer

Neue Ausschreibung seit Juni 2003

virusscan

apple-systeme

RZ betreibt Lehr-/Lernplattform für gesamte Uni



Lerneinheiten bzw. Übersichtsseite einer Vorlesung auf der Lehr-/ Lernplattform der Universität Karlsruhe (TH)

ISSN 1432-7015

INHALT

IMPRESSUM

Herausgeber:
Prof. Dr. Wilfried Juling
Redaktion: Ursula Scheller, Klaus Hardardt
Tel.: 0721/608-4865 oder -7391

Universität Karlsruhe (TH)
Rechenzentrum
D-76128 Karlsruhe
http://www.rz.uni-karlsruhe.de/~RZ-News/
Nummer 2003/6, 7
ISSN 1432-7015

Internet-Gefahren

Viren, Würmer, Trojaner, Hoaxes

Harald Bauer

Hinter dem umgangssprachlichen Begriff „Computer-Virus“ verbergen sich über 65.000 Programme, von denen etwa fünf Prozent im Umlauf sind. Sie werden nach ihren Eigenschaften in Viren, Würmer und Trojaner unterteilt und können zum einen als rein technisch-funktionale, zum anderen als methodische Konzepte gekennzeichnet werden. Daneben existiert ein rein psychologischer Ansatz, der als solcher zwar keinen aktiven Code repräsentiert, diesen aber als Dateianhang per E-Mail verbreiten kann und daher – hier dem methodischen Konzept zugeordnet – auch beschrieben werden soll.

Zum technischen Konzept werden Viren und Würmer gezählt, zu letzterem Trojaner und (hier) Hoaxes. Im Gegensatz zu Viren und Würmern besitzen Trojaner keinen eigenen Vervielfältigungsmechanismus. Für die Verbreitung von Hoaxes sorgt der „wohlmeinende“ Benutzer höchstpersönlich und absichtlich.

Viren

Viren werden in der Regel als kleiner Progammcode realisiert, der in Leerbereiche oder an das Ende existierender Programmdateien (.com, .exe, .scr, .vbs, etc.) eingefügt wird. Bedingt durch den kleinen Code haben sie keinen großen Funktionsumfang, was ihr Gefährdungspotenzial jedoch nicht schmälert. In Abhängigkeit von Wirkungsfeld, Schadfunktion und technischer Realisierung wird eine Vielzahl spezieller Viren unterschieden. Der heute verbreitetste Typ ist der Makro-Virus (z.B. *Alcarys-Fam., Melissa, Killboot*), der sich beispielsweise im Makro-Code von MS-Office Dokumenten (Word-, Excel-, Power Point-Dateien) einnistet und beim Öffnen des Dokuments oder einer Dateivorlage (beispielsweise *normal.dot*) aktiv wird. Makro-Viren funktionieren jedoch häufig aufgrund von Sprachkonflikten nicht mit deutschen Office-Installationen.

Durch Deaktivieren bzw. Erzwingen einer Abfrage, ob der in einem Dokument enthaltene Makro-Code ausgeführt werden soll, ist man vor unmittelbarem Schaden relativ geschützt, es verhindert jedoch nicht die weitere Verbreitung über den Austausch infizierter Dokumente! Das automatische Aktivieren von Makros läßt sich in MS-Office-Anwendungen über *Extras → Optionen → Allgemein → Makrovirus-Schutz* deaktivieren.

Zusätzlich kann die Systemsicherheit durch Verschieben oder Umbennen kritischer Programme wie *format.com* erhöht werden, da Makros zum Programmaufruf eine absolute Pfadangabe benötigen.

Weiterhin nicht ganz unbedeutend sind die Bootsektor-Viren (z. B. *Parity Boot*), die zu „Diskettenzeiten“ den häufigsten Typ darstellten. Sie nutzen den Umstand, dass bei entfernbaren Medien (Disketten, CD-ROMs, etc.) bei jedem Zugriff der sogenannte Bootsektor gelesen wird, wodurch der Virus aktiviert wird. Formatbedingt beträgt die Länge des infizierten Codes 512 Bytes. Schutz bietet nur entsprechend konfigurierte Anti-Viren (AV)-Software.

Neben diesen beiden Formen gibt es BIOS-, wie zum Beispiel *Chernobyl* (*CIH*), Dateisystem- und Hybrid-Viren, Logische Bomben (z. B. *Honnecker*-Virus), Polymorphe Viren (*Nimda*-Varianten), Programm-, Datei-, Retro-, Script-, Stealth-Viren und andere (siehe unten aufgeführte Links).

Würmer

Würmer infizieren im Gegensatz zu Viren keine anderen Programme, sondern sind eigenständige Programme. Sie können daher beliebig groß sein und entsprechend viele Funktionskomponenten beinhalten, die auch als eigenständige Programmdateien abgelegt werden können. Typische Funktionalitäten sind Verbreitungs-/Reproduktions- und Schadmechanismen sowie das Einrichten von Hintertüren (backdoor) mit sogenannten Trojanern, durch die der Hacker Zugriff auf den befallenen Rechner erhält (siehe unten). Sie sind heute der gängigste Typ und verbreiten sich über:

- E-Mail (Dateianhang und HTML-formatierte E-Mails, vor allem über MS-Outlook in der unsicheren Standardkonfiguration. Die Dateianhänge sind häufig als Screensaver, Multimediadateien

oder Schutz-/Sicherheitsprogramme getarnt. Derlei nicht angeforderte E-Mails sollten sofort gelöscht werden).
- Windows-Netzwerkfreigaben (hier empfiehlt es sich, Freigaben nur temporär zuzulassen und soweit möglich, Win-NT, -2000, -XP mit einem sicheren Kennwort zu versehen).
- Chat (mIRC, ICQ, etc.).
- Web (auch hier bevorzugt über den I-Explorer in Standardkonfiguration. Das Deaktivieren von aktiven Elementen, insbesondere ActiveX, ist sehr empfehlenswert).
- Peer-to-Peer (P2P, File-Sharing), Netze (Napster, KaZaA, Grokster, e-donkey, etc.) sowie
- untergeordnet jede andere Form von Netzwerkkommunikation.

Bekannte ältere Wurmvertreter sind der *Navidad*- und *I Love You*-"Virus", die *Hybris*- und *Code-Red*-Varianten sowie die meisten der heute für Schlagzeilen sorgenden „Viren", z. B. die *Bugbear*-, *Klez*-, *Lovgate*-, *Oror*-, *Yaha-,* und aktuell, *Sobig*-Varianten.

Zu den methodischen Typen zählen Trojaner und Hoaxes, wobei noch einmal betont werden soll, dass es sich bei letzteren nicht um aktive Komponenten im Sinne eines "Virus" handelt (siehe unten).

Trojaner

Trojaner sind Programme, die einen unbemerkten, externen Zugriff auf einen Rechner ermöglichen und im Hintergrund laufen (ursprünglich zur Fernwartung von Rechnern entwickelt). Meist werden sie als Teilkomponente eines Wurms auf dem Rechner installiert. Zur Tarnung bedienen sie sich verschiedener Methoden. Zu den gängigsten gehört die Einbindung der Funktionen in normale Anwendungen oder die Vortäuschung eines defekten Programmes nach der Erstinstallation oder zu einem späteren Zeitpunkt durch fingierte Fehlermeldungen. Das Deinstallieren/Löschen eines solchen "defekten" Programmes belässt die bösartigen Komponenten unbeschadet! Der Start des Trojaners kann durch verschiedenste Umstände gesteuert werden. Ist der Trojaner an ein infiziertes Programm gekoppelt, wird er mit diesem gestartet. Handelt es sich um ein eigenständiges Programm, sorgen passende Einträge in der Registry, autoexec.bat, win.ini, system.ini, winini.bat oder im Autostart-Verzeichnis für eine Aktivierung bei jedem Neustart des Rechners. Andere Mechanismen koppeln den Start an bestimmte Systemzustände (z. B. Datum/Uhrzeit) oder den Start eines anderen Programmes. Dazu gehören vor allem Internet-Anwendungen wie Einwahl-Programme, Netzwerk-Klienten (Browser, Mail-Programme, Home-Banking, Terminal-Emulatoren) u.ä., die Authentisierungsmechanismen nutzen.

Die Funktionsvielfalt eines Trojaners ist beliebig und nur von den Absichten des Hackers abhängig. Gängige Funktionen umfassen unter anderem:
- Sammeln von Benutzerdaten mit sogenannten Keylog-Programmen (eine Trojaner-Variante, die Tastatureingaben protokolliert, z. B. auch Benutzernamen, Kennwörter, PINs, etc. In diesem Zusammenhang ist zu beachten, dass das Deaktivieren der Funktion *Formulardaten/Kennwort speichern* keine Auswirkung auf die Sicherheit/Privatsphäre des Benutzers hat!). Eine separate (Wurm-) Komponente kann die gesammelten Daten an den Hacker senden.
- Ausspionieren von Dateien (Kennwort-, Formular- und anderen Dateien) und Dateisystemen (Verzeichnisstrukturen)
- Datenträgermanipulation (Löschen/Verschieben/Kopieren/Umbenennen von Dateien und Verzeichnissen, Formatieren von Festplatten, auch über Netzwerkfreigaben).

Neben eigenständig operierenden Trojanern gibt es auch interaktive Client/Server-„Lösungen", die dem Hacker den direkten, operativen Zugriff auf den Fremdrechner erlauben. Infizierte Rechner (Server-Seite) können dem Hacker über Rückmeldungen bekannt sein oder werden durch clientseitiges Scannen (Hacker) des Netzes gefunden. Diese Form wird besonders für den Missbrauch fremder Systemresourcen (Remote-Computing) genutzt, z. B. für getarnte und/oder massenhafte Angriffe auf weitere Rechner (DDoS: „Distributed Denial of Service"-Attacken.

Beispiele für bekannte Trojaner sind *Backdoor, Back Orifice, NetBus, SubSeven (Sub7).*

Hoaxes

Hoaxes (engl.: Falschmeldung, „Ente") sind keine „Viren" im eigentlichen Sinn, können aber solche im Dateianhang enthalten. Primär dienen sie dazu, E-Mails möglichst rasch zu verbreiten, was durch entsprechend spektakuläre Angebote und Aussagen wie „Bitte an alle Bekannten weiterleiten" noch forciert werden soll. Kennzeichen vieler Hoaxes sind „meter-

lange“ To:-Felder. Unter den Begriff fallen unter anderem alle Arten von Kettenbriefen (z. B. Petitionen), Geschäftsbriefe mit betrügerischem Hintergrund (auch solche der sogenannten Nigeria-Connection) und E-Mails mit gefälschten Absendern (support@microsoft.com, support@symantec.com, etc.), irreführenden Betreffs und bewusster Fehlinformation im Nachrichtenteil.

Letztere sind der eigentliche Grund der Aufnahme von Hoaxes in diesen Artikel. Hier wird versucht, den Empfänger dazu zu bewegen, die im Dateianhang befindlichen und in vielerlei Form getarnten „Viren“ oder 0190-Dialer-Programme („neustes Update“, „Sicherheitssoftware“, Multimediadateien, Screensaver) auf seinem Rechner zu installieren. Es wird daher auf vielfache Stellungnahmen bekannter Softwarehersteller hingewiesen, dass diese keine unaufgeforderten Warnungen oder Hinweise per E-Mail versenden! Bezüglich der „Dialer“-Software sei darauf aufmerksam gemacht, daß zum Teil horrende Summen (300,-) allein für einen Verbindungsaufbau abgerechnet wurden! Hoaxes eignen sich daher besonders gut zum Löschen.

Die Vielzahl der Methoden ermöglicht Hackern jede denkbare Kombination, also z. B. einen Wurm, der als Hoax auftritt und dessen Einzelkomponenten wiederum aus einem Virus, Trojaner oder weiteren Funktionskomponenten bestehen.

Virenschutz

Schutz vor „Viren“ bietet bereits der vernünftige Umgang mit dem Medium. Dazu gehört die richtige Konfiguration der sicherheitsrelevanten Einstellungen des Programms (Outlook: Automatisches Öffnen von Dateianhängen deaktivieren, siehe unten Link zur Konfiguration von Internetanwendungen) und der Verzicht auf HTML-formatierte E-Mails, auch wenn dadurch der Komfort etwas eingeschränkt wird (alle Mailprogramme bieten die Möglichkeit, HTML-formatierte E-Mails in Klartext (plain) umzuwandeln. Als positiver Nebeneffekt werden die Mails dadurch deutlich kleiner). Auch sollten unerwartete E-Mails mit Dateianhang nicht ohne vorherige Rückversicherung beim Absender geöffnet werden. Das gilt im Grunde aber auch für E-Mails von Bekannten, die sich der Infektion ihres Rechners nicht bewusst sein müssen oder deren Adresse in einem infizierten Dritt-System gefunden und als Absender eingesetzt wurde!

Mailprogramme sollten daher so konfiguriert sein, dass sie HTML-formatierte E-Mails in Klartext umwandeln und das automatische Öffnen von Dateianhängen deaktiviert ist (siehe unten den Link zur Konfiguration von Internetanwendungen).

Um dennoch effektiv und sicher mit dem Medium arbeiten zu können, ist der Einsatz einer Antiviren Software mit regelmäßig aktualisierter Datenbank nötig, die sowohl eingehende E-Mails, als auch auswechselbare Datenträger (Disketten-, CD-ROM-, ZIP-Laufwerke, etc.) und speziell eingerichtete Download-Verzeichnisse im laufenden Betrieb überwacht. Damit wird das System nicht nur auf der technische Seite sondern auch vor der Fahrlässigkeit des Anwenders geschützt. Einen absoluten Schutz kann jedoch auch eine Antiviren-Software nicht leisten. So kann sie, bedingt durch der dem Chatten zugrunde liegenden Technik, hier keinen Schutz bieten. Aus demselben technischen Grund können auch Firewalls an dieser Stelle nur unzureichenden Schutz bieten, weshalb man für diese Anwendung verallgemeinert sagen kann, dass sich Anspruch an Funktionalität und Sicherheit grundsätzlich widersprechen! Ähnliches gilt leider auch für Peer-to-Peer Netze.

Es sei an dieser Stelle auch an die Wahl des Mailprogramms erinnert, bei denen es auch Unterschiede hinsichtlich der Sicherheit gibt. Auch oder gerade weil MS-Outlook das verbreitetste Mailprogramm ist, haben sich „Viren“-Autoren und Hacker auf die reichlich vorhandenen Programm- und Konfigurationsschwächen konzentriert und nutzen die Sicherheitslücken zusammen mit dem unsicheren Windows- oder Outlook-Adressbuch zu Verbreitung ihrer „Viren“. Als Alternativen seien an dieser Stelle Netscape Messenger, Opera, Eudora oder Pegasus genannt, die als Free- oder Shareware im Internet und teilweise auf der aktuellen BelUp-CD (siehe http://www.rz.uni-karlsruhe.de/~ISDN/#Belup%20CD) zu finden sind.

Abschließend sei auf den nicht unbedeutenden Umstand hingewiesen, daß ein infiziertes System in der Regel nicht nur für den Besitzer, sondern auch für viele andere Anwender eine Menge Arbeit und Ärger bedeuten kann. Konsequente Schutzmaßnahmen dienen somit nicht nur dem Anwender selbst sondern auch der Allgemeinheit.

Ergänzende Informationen zur Typologie:
http://www.rz.uni-karlsruhe.de/Uni/RZ/Netze/Sicherheit/V-TypI.html
Informationen zur Konfiguration von Internetanwen-

dungen, Windows-VBS:
http://www.rz.uni-karlsruhe.de/Uni/RZ/Netze/Sicherheit/
Informationen zu aktuellen Viren:
http://www.rz.uni-karlsruhe.de/Uni/RZ/Netze/Sicherheit/index_Vir.html

Liste zur Warnung vor aktuellen Internet-Gefahren (virus-alert-l@UNI-KARLSRUHE.DE):
http://www.rz.uni-karlsruhe.de/Uni/RZ/Netze/Sicherheit/Akt_List.html.
Harald Bauer, Tel. -7703
E-Mail: Harald.Bauer@rz.uni-karlsruhe.de.

Virenschutz

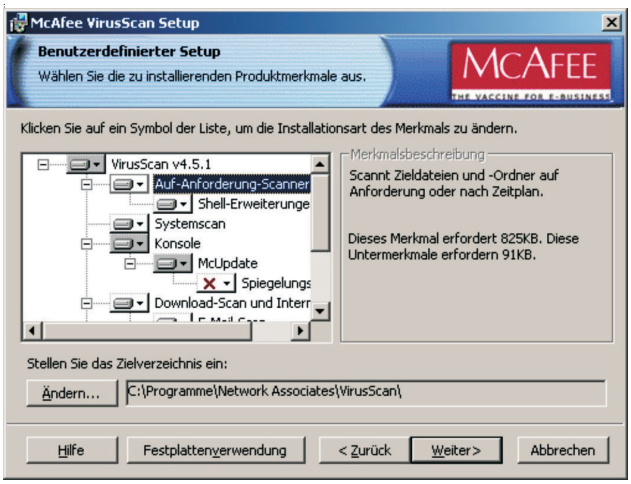
Installation von McAfee VirusScan 4.5

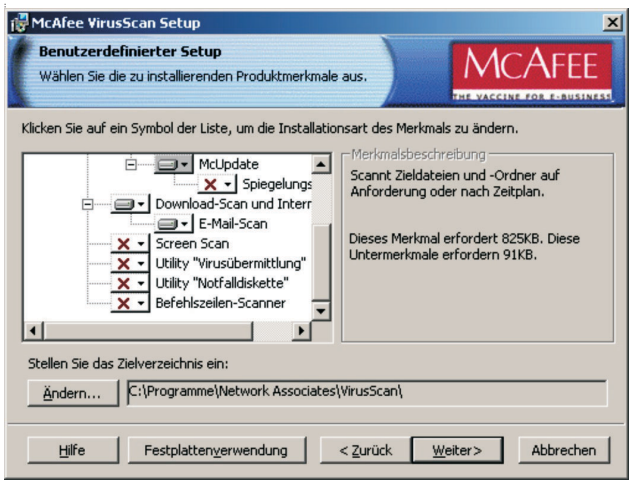
Wolfgang Preuß

Falls Sie bereits einen anderen Virenscanner installiert haben und diesen durch VirusScan ersetzen wollen, dann sollten Sie das bisherige Produkt zuerst deinstallieren. Da ihr PC dann „ungeschützt“ ist, sollten Sie bis zum Abschluss dieser Installation die Netzverbindung unterbrechen.

Installation von CD (im Beispiel: Laufwerk O:)

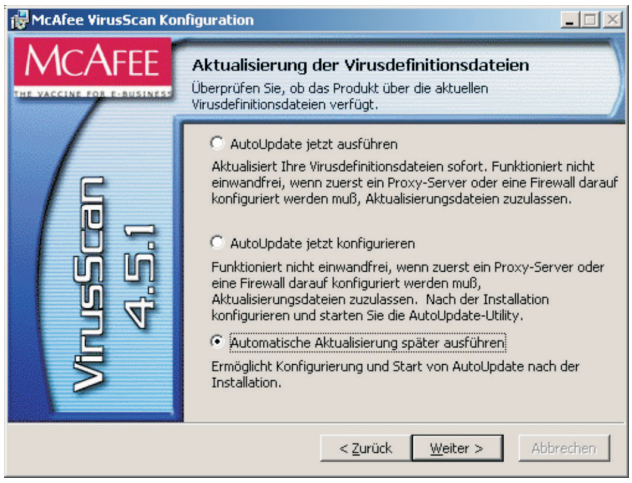
- O:\Autorun\AUTORUN.EXE aufrufen (wenn nicht automatisch gestartet), VirusScan 9x/NT72000 4.5 im Anfangsfenster anklicken
- Lizenzvertrag akzeptieren
- Standard-Sicherheit auswählen
- Benutzerdefinierte Installation auswählen
- Weitere Einstellungen:





- Meldung: “Bereit zum Installieren des Programms”: [Installieren] anklicken. Die Installation beginnt.

[Weiter] *anklicken*



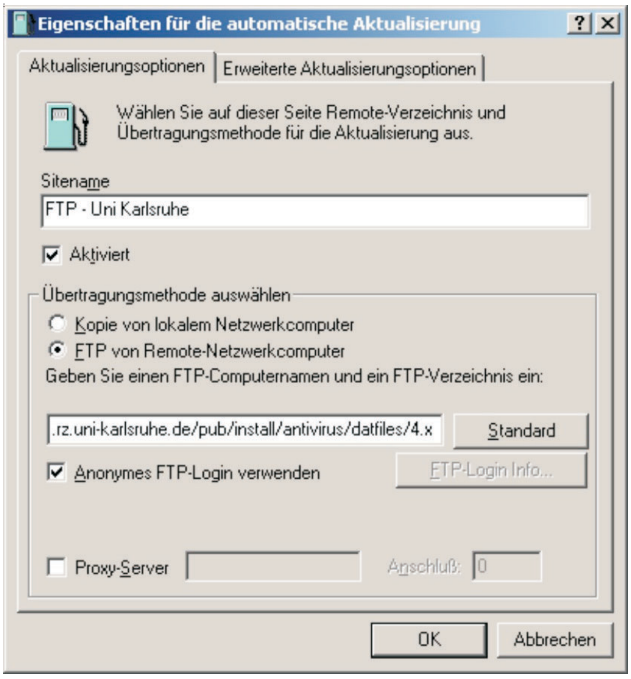
Weiter *anklicken*

Fertigstellen *anklicken*

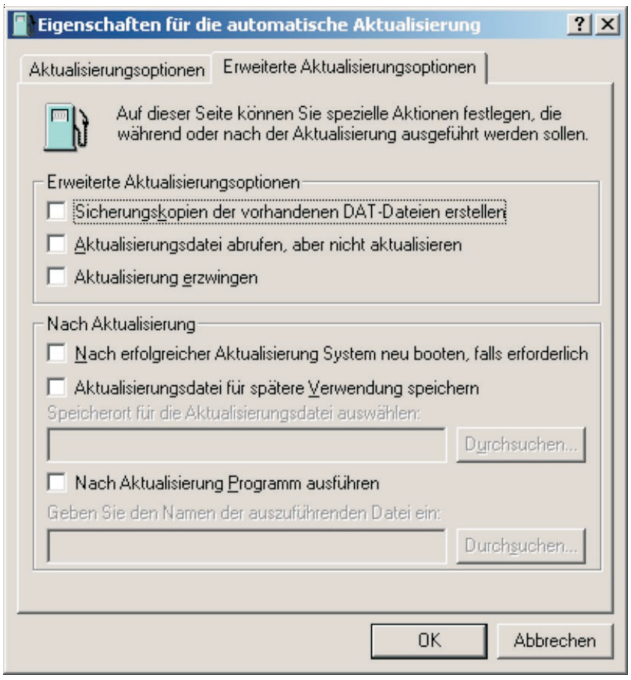
- Meldungen wegen alter Virus-Datenbank bzw. alter Scan-Engine können an dieser Stelle ignoriert werden.
- Falls VirusScan gestartet wird, abbrechen.
- VirusScan-Konsole aktivieren und aufrufen:
  Start – Programme – Network Associates – VirusScan-Konsole
  Bei Meldung: "Initialisierungsfehler" AvSync-Manager aktivieren lassen durch Anklicken von Ja und nochmals Start – Programme – Network Associates – VirusScan-Konsole.

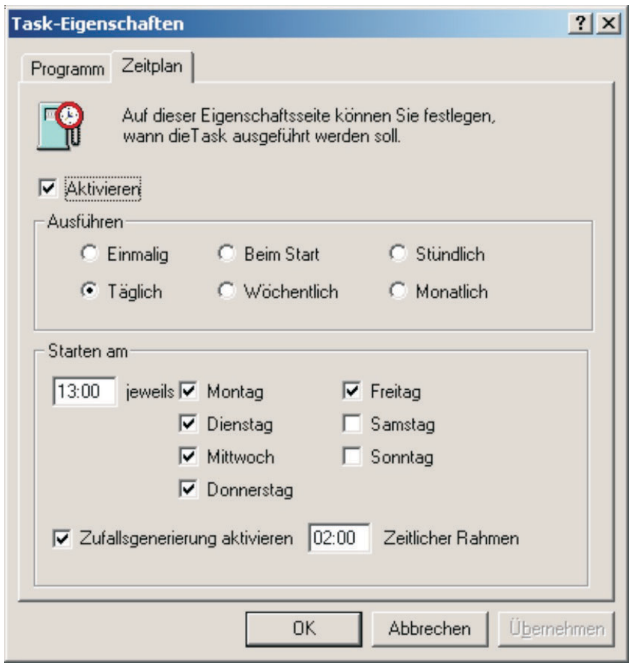
Auto Update einrichten

Das Auto Update sorgt dafür, dass automatisch die Virus-Datenbank immer auf den neuesten Stand gebracht wird. Hierzu im geöffneten Fenster der Virus Scan-Konsole Doppelklick auf „Auto Update" und dann im aufgehenden Fenster Konfigurieren... anklicken, im nächsten aufgehenden Fenster Bearbeiten... anklicken, dann die Einstellungen im Fenster beispielsweise wie folgt vornehmen:



Bei „Geben Sie einen FTP-Computernamen und ein FTP-Verzeichnis ein:" war ursprünglich eingetragen: ftp.nai.com/pub/antivirus/datfiles/4.x. Hier sollte der lokale Mirror eingetragen werden: ftp.rz.uni-karlsruhe.De/pub/install/antivirus/datfiles/4.x. Nach Abschluss der Installation sollte (über die VirusScan Konsole) als zweite Wahl auch der ursprüngliche Standardwert zusätzlich eingetragen werden. Durch diese Reihenfolge wird bewirkt, dass der benötigte Datentransfer optimiert wird, bei Ausfall des lokalen Mirrors aber trotzdem ein Update stattfinden kann.





OK *eingeben, und nochmals im verbleibenden Fenster* OK *eingeben.*

Im verbleibenden Fenster "Task-Eigenschaften" die Registrierkarte "Zeitplan" anklicken.

Sie können natürlich die Einstellung Ihren Wünschen entsprechend modifizieren. Das Fenster noch nicht schließen.

In Sonderfällen (Bekanntwerden eines gefährlichen Virus) kann über die verfügbare VirusScan-Konsole auch eine umgehende Aktualisierung manuell gestartet werden.

Virus-Datenbank (DAT-Files) auf neuesten Stand bringen

- Im oben rechts geöffneten Fenster die Registrierkarte „Programm" anklicken bzw. bei einem Neustart Start – Programme – Network Associates – Virus Scan-Konsole
- Doppelklick auf „Auto Update", Registrierkarte „Programm",
- und dann im aufgehenden Fenster Jetzt ausführen Wenn fertig, OK eingeben, und VirusScan-Konsole schließen.

Bei weiteren Fragen wenden Sie sich bitte an Harald Bauer, Tel. -7703, E-Mail: Harald.Bauer@rz.uni-karlsruhe.de.

Alexander von Humboldt-Stiftung beruft Prof. Juling in Auswahlausschuss

Ursula Scheller

Prof. Dr. Wilfried Juling, Informatikprofessor an der Universität Karlsruhe (TH) und Leiter des Universitätsrechenzentrums, wurde im Mai diesen Jahres in den Auswahlausschuss der Alexander von Humboldt-Stiftung berufen. Er tritt damit die Nachfolge des ehemaligen Universitätsrektors und derzeitigen Vorstandsvorsitzenden des Deutschen Zentrums für Luft- und Raumfahrt, Prof. Dr. Sigmar Wittig, an.

Die Alexander von Humboldt-Stiftung ist eine gemeinnützige Stiftung zur Förderung der internationalen Forschungskooperation, errichtet von der Bundesrepublik Deutschland. Sie vergibt Humboldt- und

Friedrich Wilhelm Bessel-Forschungspreise als Ehrung an hoch qualifizierte ausländische Wissenschaftlerinnen und Wissenschaftler und ermöglicht ihnen langfristige Forschungsaufenthalte in Deutschland.

Die Vergabe dieser Forschungspreise erfolgt durch einen Auswahlausschuss der Alexander von Humboldt-Stiftung, dem international ausgewiesene Wissenschaftlerinnen und Wissenschaftler angehören.

Multimedia Transfer

Neue Ausschreibung seit Juni 2003

Vera Keplinger / Anne Habbel

Frauensonderpreis beim Multimedia Transfer 2004 sucht Female IT-Talents

„Auch in diesem Jahr möchten wir den *Women´s Special* – wie im vergangenen Jahr - beibehalten", so der Direktor University Relations von IBM Deutschland, Dr. Johannes Windeln, anlässlich des Sponsorentreffens am Rechenzentrum der Universität Karlsruhe.

Einmal jährlich kommen die Unternehmen, die den Wettbewerb unterstützen, in Karlsruhe zu einem Strategiegespräch zusammen. Unter Leitung von Prof. Dr. Wilfried Juling, dem Direktor des Rechenzentrums, wird gemeinsam die Ausrichtung des neuen Jahrgangs festgelegt. Mit dabei war ebenfalls die Geschäftsführerin der Akademie der Energie Baden-Württemberg, Dagmar Woyde-Köhler, die die Vor-Ort-Kooperation zwischen der Universität und der Karlsruher EnBW für maßgeblich hält.

Nach der erfolgreichen Einführung des speziellen Frauenpreises für den MMT 2002 möchten das Hochschulrechenzentrum und die Firmen an diesem erfolgreichen Konzept festhalten: "Mehr Frauen in die IT!", so lautet die Devise.

Der Erfolg des Preises zeigt sich vor allem an den steigenden Zahlen der Einreicherinnen. Vergleicht man zwischen dem Jahr 2000 und 2003, so hat sich der Anteil von 27 auf 51 fast verdoppelt. Der *Women´s Special* fungiert somit als Türöffner in einem Bereich, in dem die Frauen erst noch im Kommen sind.

„Der Preis hat mir gezeigt, dass ich meinen Platz in der Multimedia-Welt habe", so die Gewinnerin des diesjährigen *Women´s Special* Preises, Isabel Zorn von der Universität Bremen. Sie bringt damit die Zielsetzung des Preises auf den Punkt. Der *Women´s Special* will Frauen Mut machen, sich zu den eigenen technischen und multimedialen Fähigkeiten zu bekennen. Isabel Zorn berichtet, dass sie erst nach mehreren E-Mails von verschiedenen vifu (Virtuelle Internationale Frauenuniversität)-Nutzerinnen an eine Teilnahme am Multimedia Transfer gedacht hat: „Bei den ersten Mails habe ich den Gedanken noch verworfen, aber ab der dritten E-Mail dachte ich, wenn diese Leute alle Vertrauen in die Gewinnchancen der vifu haben, dann werde ich es eben versuchen."

Der Einsatz hat sich für sie gelohnt: Isabel Zorn war im Februar für ihr Projekt vifu, die „Virtuelle Internationale Frauenuniversität" mit einem Preisgeld in Höhe von 2.500 Euro ausgezeichnet worden. Der Server vifu vernetzt 700 Wissenschaftlerinnen aus über 100 Ländern und stellt zusätzlich verschiedene Kommunikationsdienste und eine internationale Expertinnendatenbank bereit.

Die diesjährige Ausschreibung wird im Juni beginnen und am 15. Oktober 2003 enden. Aufgerufen sind neben den frauenspezifischen Themen alle Projekt- und Abschlussarbeiten in den Kategorien Creative Design, E-Learning, Tools, Web-Engineering und Hot Trends. Die Arbeiten werden nach den Kriterien Innovationsgehalt, Medieneinsatz, Benutzerfreundlichkeit und Design bewertet.

Die 20 besten Teilnehmer/innen präsentieren ihren Beitrag auf der Learntec, der Messe für Bildungs- und Informationstechnologie in Karlsruhe (10. bis 14. Februar 2004). Dort können sie ihre Ideen, Projekte und Produkte als Aussteller am Gemeinschaftsstand "Forum Multimedia Transfer" hochrangigen Entscheidern aus der Wirtschaft vorstellen und so wertvolle Kontakte für den Berufsstart knüpfen.

Aktuelle Informationen demnächst unter: www.rz.uni-karlsruhe.de/mmt.

Kontakt:
Rechenzentrum der Universität Karlsruhe (TH)
Vera Keplinger, Anne Habbel
Zirkel 2, D-76128 Karlsruhe
Tel. 0721 / 608-4873 oder -6113
Fax: 0721 / 69 56 39
E-Mail: mmt@rz.uni-karlsruhe.de.

RZ betreibt Lehr-/Lernplattform für gesamte Uni

Peter Henning

Netzgestützte Vorlesungen und Kurse

An der Universität Karlsruhe gibt es mit zunehmender Tendenz eine Vielzahl von Projekten im Bereich netzgestützter und multimedialer Lehre. Als prominente Vertreter seien hier die Projekte Vikar und VIROR genannt.

Auch am Rechenzentrum der Universität Karlsruhe wurde seit längerem an der Auswahl einer Lernumgebung für die gesamte Universität gearbeitet.

Um Synergien zu nutzen, vorhandenes Know How zu bündeln, Projekte zu entlasten und zukünftigen Inhaltsanbietern den Einstieg zu erleichtern, sollte diese Lernumgebung zentral vom Rechenzentrum betrieben werden. Um andere Institute der Universität einzubeziehen und die Auswahl einer Lernplattform auf eine breitere Grundlage zu stellen, wurde eine Arbeitsgruppe zur Auswahl einer Lernplattform ins Leben gerufen. Diese Arbeitsgruppe hat sich für die Lernplattform CLIX Campus der Firma IMC entschieden, deren Betrieb zum Wintersemester 2002/2003 startete. Allen Interessierten der Universität Karlsruhe steht nun die Möglichkeit offen, Vorlesungen und Kurse mit Hilfe dieser Plattform über das Internet anzubieten.

Was ist eine Lernplattform?

Eine Lernplattform gibt Dozenten die Möglichkeit, Vorlesungen und Kurse multimedial und netzgestützt über das Internet zu verbreiten. Denkbar sind hier sowohl komplett über das Internet abgehaltene Vorlesungen oder Kurse als auch ergänzende Zusatzdienste zur traditionellen Lehre wie die Ablage von Studienmaterial, z. B. multimedialen Animationen. Zusätzlich stellt eine Lernplattform integrierte Werkzeuge zur Kommunikation und Kollaboration zwischen den Teilnehmern (Student-Dozent/Tutor, Student-Student) zur Verfügung. Der Student kann per E-Mail Rückfragen an seinen Dozent/Tutor stellen oder in einem gemeinsamen Arbeitsbereich Aufgaben in einer Gruppe bearbeiten. Außerdem stellt die Plattform Diskussionsforen, Chat, Dokumentenarchive und Werkzeuge zur Durchführung von Tests, die als Bedingung des weiteren Lernpfades dienen können, zur Verfügung. Dem Studenten

Personalisierte Einstiegsseite der Lehr-/ Lernplattform

kann so Studienmaterial orts- und zeitunabhängig angeboten werden, durch die integrierten Kommunikationstools kann der Austausch zwischen den Teilnehmern eines Kurses unabhängig von eventuellen Präsenzterminen, Sprechstunden, Lokalitäten usw. erheblich verbessert werden und somit zu einer wesentlich flexibleren Lehr-/ Lernsituation führen.

Was muss ich tun, um Kurse mit Hilfe der Lernplattform anzubieten?

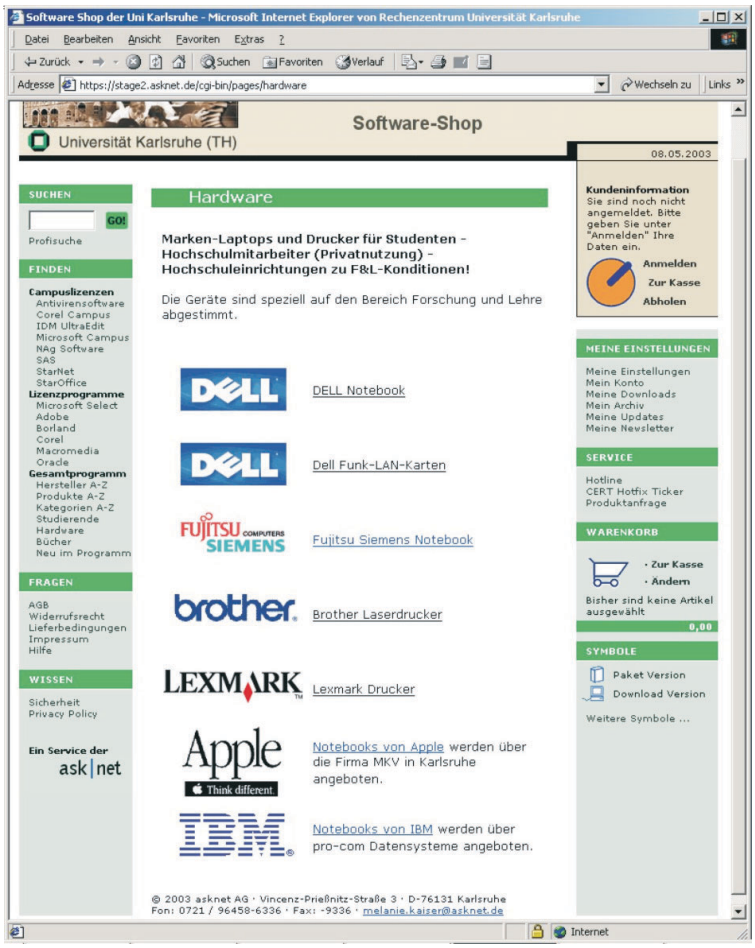
Der Dozent/Autor muss das gesamte Kursmaterial wie HTML-Seiten, Videodateien, Animationen usw. außerhalb der Lernplattform erstellen. Das Material wird über einen Dateiupload ins System gebracht und dort zum Kurs strukturiert. Zusätzliche Dienste wie Foren, E-Mail, gemeinsame Arbeitsbereiche usw. werden vom System zur Verfügung gestellt und können in den Kurs integriert werden.

Um den Autoren den Einstieg in die Lernplattform zu erleichtern, werden in regelmäßigen Abständen Schulungen im Rechenzentrum durchgeführt. Interessenten wenden sich bitte an:

Peter Henning, Tel. -8041
E-Mail: henning@rz.uni-karlsruhe.de.

Apple-Systeme zu Hochschul-Sonderkonditionen

Dieter Oberle



Software-Shop der Universität Karlsruhe (TH)

In Zusammenarbeit mit dem Rechenzentrum hat die Firma Apple und der für die Universität zuständige ortsansässige „Apple Education Vertriebspartner", die Firma MKV, nun auch Apple-Geräte zu Hochschul-Sonderkonditionen im Angebot. Wie üblich sind die aktuellen Angebote über die Homepage des Rechenzentrums im Online-Shop abrufbar und bestellbar.

Der Shop hat seit dem 20.5.2003 ein neues Erscheinungsbild. Für alle bisher registrierten Shopnutzer werden die Berechtigungen automatisch in den neuen Shop übernommen.

Dieter Oberle, Tel.: -2067,
E-Mail: oberle@rz.uni-karlsruhe.de.

Aktuelle PDAs

Dieter Oberle

Die Nachfrage nach kleinen mobilen im DUKATH verwendbaren Geräten steigt rapide. Verschiedene Markenhersteller bieten ihre aktuellen Geräte zu Sonderkonditionen für Mitglieder unserer Hochschule an. Diese Angebote sind im RZ-Shop unter https://rzunika.Asknet.de/cgi-bin/pages/hardware zu finden.

Damit die Entscheidung etwas leichter fällt, habe ich eine Übersicht über die nach meinem Ermessen und meiner Erfahrung geeigneten Geräte zusammengestellt. Diese Tabelle erhebt keinen Anspruch auf Vollständigkeit, beschreibt aber einige der zurzeit verfügbaren brauchbaren Geräte, die auch im Rechenzentrum genutzt werden. Zu beachten ist, dass die angegebenen Preise immer inclusive der bei einigen Modellen notwendigen Erweiterung für die Mobilität über Bluetooth und WLAN kalkuliert sind.

Neue Geräte werden ab Mitte Juli 2003 mit dem neuen Betriebssystem „Windows Mobile ™“ auf den Markt kommen. Alle in der Tabelle aufgeführten Hersteller sind dabei. Auch wird es für die in der Tabelle aufgeführten Modelle Upgrademöglichkeiten geben. Näheres dazu jedoch zu einem späteren Zeitpunkt.

Dieter Oberle, Tel. -2067,
E-Mail: oberle@rz.uni-karlsruhe.de.

PDA Vergleich Farbe für Nachteile Farbe für Zubehör Stand: Mai 2003	**Fujitsu Siemens** **POCKET LOOX 600**	**HP-Compaq** **iPAQ H5450 WLAN 802.11 B**	**Toshiba** **Pocket PC E750 WLAN**	**DELL** **AXIM X5 Pocket PC**
				
CPU	Intel XSCALE PXA250	Intel XSCALE PXA250	Intel XSCALE PXA250	Intel XSCALE
Taktfrequenz	400 MHz	400 MHz	400 MHz	400 MHz
Hauptspeicher	64 MB	64 MB	64 MB	64 MB
Flash-ROM Speicher	32 MB	48 MB	32 MB	48 MB
Farbtiefe	16 Bit	16 Bit	16 Bit	16 Bit
Display / Auflösung	TFT Reflektiv / 240x320	TFT Transreflektiv /240x320	TFT Transreflektiv /240x320	TFT/3,5" QVGA/240x320
Bildgröße	56*74 mm; Diagonal 90 mm	57,6*76,8 mm; Diagonal 96 mm	57,6*76,8 mm; Diagonal 96 mm	
WLAN intern	nein	ja	ja	nein
WLAN extern (FlashCard)	ja			ja
Bluetooth intern	ja	ja	nein	nein
Bluetooth extern			ja	ja
Eingabe	Stift, Fingerspitze	Stift, Fingerspitze	Stift, Fingerspitze	Stift, Fingerspitze
Fingerprint Bootlock	nein	ja	nein	nein
Startkennwort	ja	ja	ja	ja
Compact Flash Einschub	Typ II	nein	Typ II	Typ II
SD-Card Slot	ja	ja	ja	ja
PC Card Slot Jacket extern	optional	optional	optional	nein
Docking Station	USB	USB+Seriell	USB	USB o. Seriell
IrDA	ja	ja	ja	ja
seriell	nein	ja	nein	nein
Audio in Micro	ja	ja	ja	ja
Audio out Kopfhörer	ja	ja	ja	ja
Lautsprecher	ja	ja	ja	ja
Netzteil	ja	ja	ja	ja
Gewicht	175 g	206 g	190 g	196 g
Maße	132x82x17 mm	133x84-77x15,9 mm	125x80x16 mm	128x81,5x18 mm
Betriebszeit:				
1 Akku ohne Licht ohne Funk	10 h	12,3 h	7,1 h	10,4 h
1 Akku mit Licht ohne Funk	3,5 h	4,5 h	2,2 h	4,9 h
PDA Etui	ja	ja	keine Angaben	ja

Microsoft Pocket PC 2002 Anwendungssoftware	ja MM/Office/WAP/Internet/E-Mail	ja MM/Office/WAP/Internet/E-Mail	ja MM/Office/WAP/Internet/E-Mail	ja MM/Office/WAP/Internet /E-Mail
Bring-In Collect&Return Service Garantie	2 Jahre	2 Jahre	2 Jahre	1 Jahr NBD Exchange
Preis incl. MWSt 16%	480,79	622,92	805,39	661,55
Stand: 20.5.03 Vertrieb	asknet AG	Baien	Bechtle	Dell direkt
Kommentar D. Oberle:	Bestes Preis/Leistungsverhältnis, leicht! Läßt sich nicht über USB Kabel laden! Hat CF u. SD Slot! Sehr gut brauchbar in der Praxis. Kein WaveLAN, nur über FlashCard! Bildschirmqualität kommt nicht an die des IPAQ 5450 ran! Mein Favorit nach Erfahrung im Einsatz von IPAQ 5450 und LOOX!	Sehr guter Bildschirm! Komplette Ausstattung für Kommunikation. Kein CF Slot!	Schlechte Akkulaufzeit! Bluetooth nur über FlashCard!	Gutes robustes Gerät! Bluetooth und WLAN nur über CF-Cards möglich.

Vorlesungsbeginn

RZ druckte 1,1 Millionen Seiten

Harald Meyer

Druck-Tipps für Skript-Autoren

Zu Beginn der Vorlesungszeit im Sommersemester 2003 kam es wieder zu dem üblichen großen Semesteranfangs-Andrang an den Schwarzweißdruckern des Rechenzentrums: Statt des durchschnittlichen Druckvolumens von ca. 600.000 Seiten pro Monat wurden im Mai 2003 mehr als 1,1 Millionen Seiten gedruckt, dies entspricht einer Steigerung um mehr als 30 Prozent im Vergleich zum ersten Vorlesungsmonat des Sommersemesters 2002.

Der Löwenanteil der Ausgabe (ca. 1 Million Seiten) entfiel dabei auf die beiden zentralen "bw600dpi"-Massendrucksysteme in der Medienausgabe des RZ, die restlichen 130.000 Seiten wurden an den Pooldruckern des RZ ausgegeben.

Wegen des hohen Druckaufkommens kam es anfangs zu Staus bei der Druckausgabe, die erst an den jeweiligen Wochenenden abgearbeitet werden konnten. Inzwischen hat sich die Situation jedoch wieder normalisiert.

In diesem Zusammenhang seien noch ein paar Tipps zur Verminderung dieser Lastspitzen genannt, die meisten davon richten sich an die Autoren der Skripten:

- Verteilen Sie Ihre Ausgabe über einen größeren Zeitraum: Es müssen ja nicht alle Kapitel eines vorlesungsbegleitenden Skriptums schon in der ersten Woche ausgedruckt werden. Durch die Unterteilung in kleinere Einheiten rutschen Sie außerdem in der Warteschlange nach vorne. Am einfachsten wäre es hier, wenn die Skripten schon selbst in mehreren Teilen vorlägen.
- Beim Drucken von Powerpoint- und anderen Folien kann man häufig wegen des geringen Textumfangs und der hohen Schriftgöße mehrere Folien auf einer Seite zusammenfassen. Dieses Zusammenfassen kann man auf einfache Weise erreichen, in dem man zunächst einmal unter Windows in eine eigene Datei druckt und dabei in den Treibereinstellungen die Layout-Einstellung "Seiten pro Blatt: 2" oder "Seiten pro Blatt: 4" auswählt. Überprüfen Sie danach mit einem Preview-Programm wie Ghostscript, ob die Zusammenfassung das gewünschte Resultat erbracht hat und senden Sie die Datei danach zum Drucker.
- Hintergrundfarben oder -farbverläufe, die sich über die gesamte Seite erstrecken, mögen ja bei der Projektion während der Vorlesung ganz schön aussehen. Wenn sie jedoch beim Drucken in Grautöne umgewandelt werden, verschlechtern sie häufig die Lesbarkeit. Außerdem führen diese Hintergrundfarben nach der Umwandlung des Dokuments in das druckerspezifische Ausgabeformat zu großen Bitmapdateien bzw. zu Übertragungsengpässen beim Transfer der entsprechenden Rasterdaten. Wenn die erstellende Anwendung die Möglichkeit bietet, Hintergrundfarben beim Drucken wegzulassen, sollten Sie diese Einstellung wählen.

Harald Meyer, Tel. -4036,
E-Mail: Harald.Meyer@rz.uni-karlsruhe.de.

Erste Ansprechpartner
auf einen Blick

So erreichen Sie uns

Telefonvorwahl: +49 721/608-
Fax: +49 721/32550
E-Mail: Vorname.Nachname@rz.uni-karlsruhe.de

BIT8000 (Help Desk)	Tel. -8000, E-Mail: BIT8000@rz.uni-karlsruhe.de
Sekretariat	Tel. -3754, E-Mail: rz@uni-karlsruhe.de
Information	Tel. -4865, E-Mail: info@rz.uni-karlsruhe.de
MicroBIT-Hotline	Tel. -2997, E-Mail: microbit@rz.uni-karlsruhe.de
Scientific Supercomputing Center (SSC) Karlsruhe	Tel. -8011, E-Mail: contact@ssc.uni-karlsruhe.de
Anwendungen	Tel. -4031/4035, E-Mail: anwendung@rz.uni-karlsruhe.de
Netze	Tel. -2068/4030, E-Mail: netze@rz.uni-karlsruhe.de
UNIX	Tel. -4038/4039, E-Mail: unix@rz.uni-karlsruhe.de
Virus-Zentrum	Tel. 0721/9620122, E-Mail: virus@rz.uni-karlsruhe.de
Mailing-Liste für Internetmissbrauch	abuse@uni-karlsruhe.de
asknet AG (SW-Lizenzen)	Tel. 0721/964580, E-Mail: info@asknet.de
Zertifizierungsstelle (CA)	Tel. -7705, E-Mail: ca@uni-karlsruhe.de
PGP-Fingerprint	pub 1024/A70087D1 1999/01/21 CA Universität Karlsruhe 7A 27 96 52 D9 A8 C4 D4 36 B7 32 32 46 59 F5 BE
Multimedia Transfer	Tel. -4873/-6113, E-Mail: kontakt@mmt.uni-karlsruhe.de

Öffentliche Rechnerzugänge

World Wide Web:
http://www.rz.uni-karlsruhe.de/ (Informationssystem des Rechenzentrums der Universität Karlsruhe)
http://www.uni-karlsruhe.de/Uni/CA/ (Zertifizierungsstelle am Rechenzentrum der Universität Karlsruhe)

Ftp:
ftp.rz.uni-karlsruhe.de; Benutzernummer: ftp (anonymer Ftp-Server des Rechenzentrums)