KATHOLISCHE UNIVERSITÄT EICHSTÄTT INGOLSTADT

IN KUERZE

IN formationen Katholische Universität Eichstätt-Ingolstadt RechenZEntrum

Jahrgang 14 Nummer 2 ISSN 0939 – 3277 November 2003

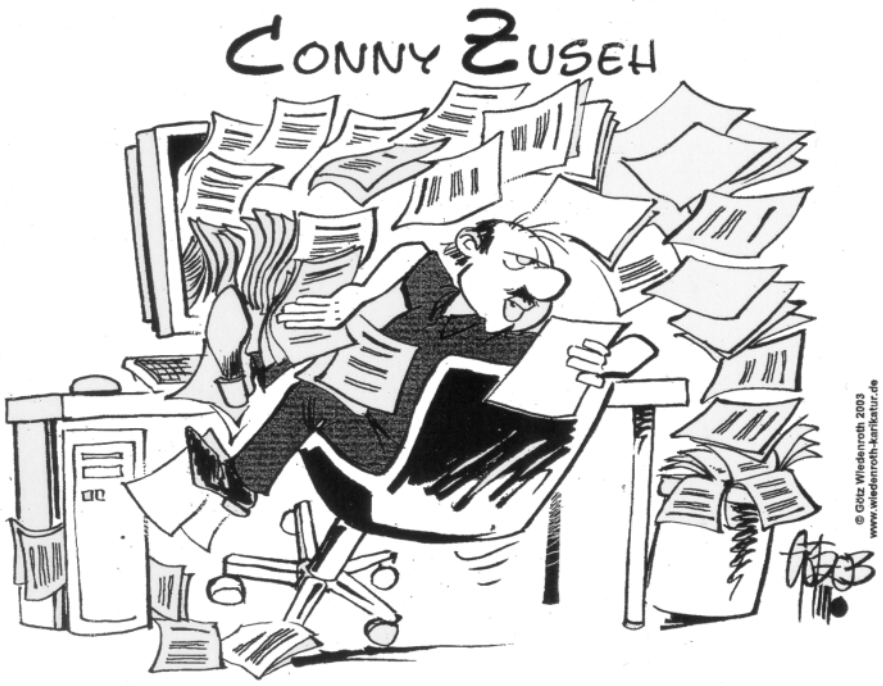
Editorial

P. Ihrler

„A virus is a virus“ konnte der französische Virologe André Lwoff nach langer Forschung sagen. Was er sich wohl dabei gedacht hat? Computernutzer, ob erfahren oder nicht, können allenfalls ein Lied über Viren singen. Besonders lästig sind in letzter Zeit die vielen E-Mails geworden, die es sich in den Mail-Boxen unserer Universität bequem machen und zu einem großen Teil Viren im Anhang mitliefern. Damit Ihr Arbeitsplatzrechner wirksam gegen Viren und unerwünschte E-Mails geschützt werden kann, ist auch Ihr Engagement gefordert. Nehmen Sie sich bitte die Zeit, um in zwei Artikeln dieser Ausgabe der INKUERZE zu erfahren, was dabei Ihr Part ist und wie das Rechenzentrum Sie dabei unterstützen kann.

Mit einem weitaus erfreulicheren Thema beschäftigt sich ein zweiter Schwerpunkt: Es geht um Möglichkeiten der Nutzung moderner audiovisueller Medien in der Lehre. Zum einen wird der mit modernster – so modern, dass alles sogar noch einfach bedienbar ist – Multimediatechnik ausgestattete neue Hörsaal der Informatik vorgestellt, zum anderen ein Werkzeug, das gleichzeitig die Präsentation von Inhalten an der Leinwand und im Web ermöglicht und trotzdem fast keine Wünsche offen lässt.

Mit dem vor zwei Jahren eingeführten kooperativen DV-Betreuungskonzept beschäftigt sich der erste Artikel. Was sich aufgrund dieses Konzeptes in dieser Zeit geändert hat, welche Lehren für die Zukunft zu ziehen sind und wo Sie davon betroffen sind, erfahren Sie in diesem Resümee. Natürlich finden Sie wie immer Informationen über neue Software-Versionen, Neuanschaffungen und zusätzliche Dienstleistungsangebote, die darauf warten, dass sie von Ihnen genutzt werden. Nur was man weiß, macht einen heiß!



„Nun versenden die sogar schon die Werbung für Anti-Spam-Filter per Massen-E-Mail!“

Inhaltsverzeichnis

Impressum

Herausgeber:	Katholische Universität Eichstätt-Ingolstadt, Rechenzentrum 85071 Eichstätt
Redaktion:	Bernhard Brandel, Peter Ihrler, Peter Kahoun, Dr. Wolfgang A. Slaby, Dr. Bernward Tewes, Peter Zimmermann
V. i. S. d. P.:	Dr. Wolfgang A. Slaby
Satz:	Theresia Stalker
Ausgabe:	z. Zt. halbjährlich
Auflage:	800 Exemplare
E-Mail:	`inkuerze@ku-eichstaett.de`
URL:	`http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/schriften/inkuerze`

Kooperatives DV-Betreuungskonzept der KU – eine erste Bilanz

Dr. W. A. Slaby

Im Sommersemester 2001 hat der Senat der Kath. Universität Eichstätt-Ingolstadt (KU) das von einer Senats-Arbeitsgruppe entwickelte Modell für eine kooperative, die Fakultäten und übrigen Einrichtungen der Universität aktiv einbeziehende Betreuung der IT-Infrastruktur verabschiedet und zum 1. Oktober 2001 zunächst für eine Erprobungsphase in Kraft gesetzt. Nachdem seither gut zwei Jahre vergangen sind, erscheint eine erste Analyse der tatsächlichen Umsetzung dieses Modells sowie der festzustellenden Auswirkungen sinnvoll und angemessen.

Wie bereits in der *INKUERZE* 1/2001 ausführlich dargestellt wurde, besteht der zentrale Punkt des kooperativen DV-Betreuungskonzepts der KU darin, dass sich das Universitätsrechenzentrum wieder stärker auf seine Kernaufgaben, den Betrieb der zentralen Server, die Bereitstellung der zentralen DV-Dienste, die Netz-Infrastruktur, die Schulung von Mitarbeitern und Studierenden sowie die Beschaffung von Rechnersystemen und sonstiger DV-Ausstattung konzentrieren soll und dass andererseits die Zuständigkeit für den Betrieb des eigenen Arbeitsplatzrechners einschließlich der Installation und Konfiguration des Betriebssystems sowie von Standard-Software bei dem jeweiligen Anwender liegt. Anhand der sechs Kernpunkte des Modells, mit denen diese Ziele weiter konkretisiert werden, möchte ich die tatsächliche Umsetzung des Betreuungskonzepts zunächst näher beleuchten:

1. Jeder Anwender ist für den Betrieb seines Arbeitsplatzrechners zuständig. Das Rechenzentrum hat die gesamte Verantwortung für zentrale DV-Dienste und die Vernetzung der Universität. [Eine genauere Klassifizierung ist in einer detaillierten Zuständigkeitsliste festgelegt.]

Dass sich das Universitätsrechenzentrum seiner Gesamtverantwortung für die zentralen DV-Dienste und die Vernetzung der Universität bewusst ist und dieser Verantwortung nach besten Kräften gerecht zu werden versucht, steht sicherlich außer Frage. Dagegen stößt die Forderung des Versorgungskonzepts, dass jeder Anwender für den Betrieb seines eigenen Arbeitsplatzrechners zuständig ist, in einigen Bereichen durchaus noch auf erhebliche Vorbehalte, insbesondere natürlich dort, wo eine Fakultät, ein Fachgebiet, ein Lehrstuhl oder eine zentrale Einrichtung diese Zuständigkeit und die damit verbundenen Aufgaben nicht organisiert hat und damit der einzelne Anwender auf sich gestellt sowie auf weitere umfassende Unterstützung durch das Universitätsrechenzentrum angewiesen ist (siehe auch Punkt 3).

2. Die Qualität der verbleibenden Dienstleistungen des Rechenzentrums wird sichergestellt. Insbesondere muss das Rechenzentrum so reorganisiert werden, dass die zum Teil jetzt entstehenden hohen Wartezeiten auf ein akzeptables Minimum reduziert werden.

Ob die verbleibenden Dienstleistungen des Universitätsrechenzentrums in angemessener Qualität erbracht werden und ob eine möglichst hohe Qualität auch weiterhin gewährleistet ist, müssen Andere, insbesondere die Empfänger dieser Dienstleistungen beurteilen. Für die eigentlich notwendige Konzeption und Umsetzung eines umfassenden Qualitätsmanagements mit Service Level Agreements ist die Personaldecke des Universitätsrechenzentrums leider auch weiterhin zu dünn.

Durch die Bereitstellung zumindest einer der beiden im Evaluationsgutachten für das Universitätsrechenzentrum empfohlenen Personalstellen in der DV-Systemtechnik konnten die teilweise aufgetretenen längeren Wartezeiten bei der Beschaffung und Installation von neuen PC-Konfigurationen weitgehend reduziert werden. Allerdings treten im Bereich der Netzdienste bereits neue Engpässe auf, die ihre Ursache in zusätzlichen in diesem Bereich wahrzunehmenden Aufgaben haben, wie Installation und Betrieb eines (demnächst) hochschulweiten Funknetzes, umfangreiche Netzsanierungsmaßnahmen der Gebäudenetze, Aufbau eines eigenen virtuellen Netzes für freie Notebook-Anschlüsse und das FunkLAN, etc.

3. Die Verteilung der Kompetenzen und Aufgaben innerhalb der Fakultäten, Fachbereiche oder Lehrstühle sowie innerhalb der Abteilungen der Bibliothek und der Verwaltung bleibt diesen Instanzen überlassen.

Die Organisation der Zuständigkeit und die Verteilung der Aufgaben für die Betreuung der Arbeitsplatzrechner des eigenen Bereichs wird von den verschiedenen Fakultäten und zentralen Einrichtungen durchaus sehr unterschiedlich gehandhabt. Das Spektrum reicht dabei von eigenen DV-Referaten in der Bibliothek und der Verwaltung über offiziell benannte DV-Beauftragte wie z.B. in der Geschichts- und Gesellschaftswissenschaftlichen Fakultät oder in einzelnen Fachgebieten wie der Geographie, der Informatik, der Journalistik und der Psychologie bis hin zu Zuständigkeitsregelungen auf Lehrstuhlebene wie beispielsweise in der Wirtschaftswissenschaftlichen Fakultät oder der Delegation der Verantwortung an jeden einzelnen Anwender. Gerade die zuletzt genannte Variante, die in etwa der Hälfte der Fakultäten praktiziert wird, führt im Universitätsrechenzentrum weiterhin zu einem erhöhten Betreuungs- und Unterstützungsaufwand, wie er nach dem Modell für ein **kooperatives** DV-Betreuungskonzept eigentlich nicht vorgesehen ist.

4. Die Anwender werden in die Lage versetzt, die ihnen zugedachten Aufgaben zu beherrschen. Das Rechenzentrum bietet dazu Kurse und Informationsmaterial an. Es können nur solche Aufgaben von dem Rechenzentrum an die Anwender übergehen, die vom Rechenzentrum entsprechend beschrieben und dokumentiert sind. Wenn jemand die Schulung des Rechenzentrums in Anspruch genommen hat und dennoch Probleme bei der Durchführung der Arbeiten hat, ist das Rechenzentrum nach besten Kräften behilflich.

Für den vom Anwender selbstständig zu übernehmenden Aufgabenkomplex der Installation und Konfiguration von Standard-Software hat das Universitätsrechenzentrum umfangreiche Anleitungen erarbeitet, die auf seinen Web-Seiten unter `http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/` bereitgestellt sind und je nach Verfügbarkeit von neuen Programmversionen laufend aktualisiert werden; mehr als 25 verschiedene Anleitungen stehen dort inzwischen zur Verfügung. Darüber hinaus hat das Universitätsrechenzentrum über mehrere Semester für wichtige Softwareprodukte Installationskurse mit praktischen Übungen angeboten; diese Installationskurse stießen allerdings auf eine derart geringe Resonanz, dass sie zum Sommersemester 2003 wieder eingestellt wurden.

5. Das Rechenzentrum richtet eine telefonische Hotline ein, unter der täglich wenigstens sechs Stunden ein allgemein kompetenter Mitarbeiter erreichbar ist. Außerdem wird eine zentrale E-Mail-Adresse „urz-hotline“ eingerichtet.

Die telefonische URZ-Hotline ist montags bis donnerstags 8.00–12.00 Uhr und 13.00–16.00 Uhr sowie freitags 8.00–12.00 Uhr unter der Telefonnummer -1010 zu erreichen. Neben der E-Mail-Adresse `urz-hotline@ku-eichstaett.de`, an die Anfragen, Fehlermeldungen und Problembeschreibungen gesandt werden können, hat das Universitätsrechenzentrum unter der Adresse http://urz-helpdesk.ku-eichstaett.de/ ein **Helpdesk-System** eingerichtet, mit dem die Meldung und Verfolgung von Problemen besonders unterstützt wird.

6. Die Reparatur beschädigter Software-Installationen wird zukünftig – wo möglich – ersetzt durch das Rücksetzen in eine funktionsfähige Anfangsinstallation. Das Rechenzentrum stellt dafür CDs für die einfache Installation zur Verfügung. Dies setzt allerdings die Einhaltung gewisser Standards bei der Hard- und Software-Beschaffung voraus.

Durch die große Vielfalt unterschiedlicher Hardware-Konfigurationen ist die Bereitstellung funktionsfähiger Anfangskonfigurationen über entsprechende Clone-CDs nur eingeschränkt möglich. Das Universitätsrechenzentrum arbeitet jedoch daran, diese Situation durch Einbeziehung geeigneter Backup-Verfahren weiter zu verbessern.

Fazit:

Nach der zweijährigen Erprobungsphase kann zumindest aus Sicht des Universitätsrechenzentrums festgehalten werden, dass das Modell für ein kooperatives DV-Betreuungskonzept an der KU weitgehend erfolgreich eingeführt werden konnte. Dadurch dass das Modell nicht strikt und mit voller Konsequenz für den Anwender durchgesetzt sondern mit großer Un-

terstützungsbereitschaft und flexibler Reaktion seitens des Universitätsrechenzentrums gehandhabt wurde, konnten Härten und Frustrationen weitgehend vermieden werden. Dies war allerdings nur möglich, weil eine der beiden im Evaluationsgutachten empfohlenen Personalstellen zeitnah zur Modelleinführung bereitgestellt werden konnte und der am Standort Ingolstadt an der dortigen Abteilung des Universitätsrechenzentrums vorhandene personelle Engpass durch die Bereitstellung einer allerdings befristeten halben Personalstelle zumindest zeitweise abgemildert wurde. (Mit dem Wegfall dieser halben Personalstelle zum 1. August 2003 hat sich die Betreuungssituation dort wieder entsprechend verschärft.)
Für die weitere Umsetzung des Modells für ein kooperatives DV-Betreuungskonzept wäre es sehr wünschenswert, wenn auch die bisher eher abwartend reagierenden Fakultäten oder Fachgebiete durch Benennung von Ansprechpartnern oder DV-Beauftragten ihre Kooperation in der DV-Betreuung intensivieren könnten. Hier wird über die verschiedenen universitären Gremien noch weitere Überzeugungsarbeit zu leisten sein. Das bisher für derartige Diskussionen und Beratungen prädestinierte Gremium der **DV-Kommission** wurde leider zu Gunsten einer umfassenderen Kommission für Zentrale Einrichtungen abgeschafft, die sich angesichts des erweiterten Zuständigkeitsbereichs und der damit verbundenen größeren Vielfalt an Beratungsthemen nur um die besonders wichtigen Punkte kümmern konnte.

Ansprechpartner im URZ:	*Zimmer:*	*Telefon:*	*PMail:*
Dr. Wolfgang A. Slaby	EI: eO-109a	-1214/-1462/-1670	`wolfgang.slaby`

Neue Virenbedrohungen

B. Brandel/H. Zimmermann

Der diesjährige Sommer brach nicht nur sämtliche Hitzerekorde – auch in puncto Windows-Computerviren sprengte er alles bisher da Gewesene. Dazu trugen insbesondere W32.Blaster und Sobig.F bei, die auf besonders neuartige und aggressive Weise trotz vorhandener Internetfirewalls in Windeseile ganze Firmennetze lahm legten und auch Windows-Rechner in unserem Universitätsnetz befielen. Dieser Artikel hat das Ziel, die Funktionsmechanismen dieser beiden Viren exemplarisch zu beschreiben und dadurch auf die Gefahren aufmerksam zu machen, die uns allen von neuartigen Computerviren drohen. Gleichzeitig werden Gegenmaßnahmen aufgezeigt, mit denen man diese Bedrohungen abwehren kann. Besonders wichtig sind regelmäßige, möglichst automatisierte Windows- und Virenscanner-Updates.

Danksagung
Besonderer Dank gebührt den Autoren der Gesellschaft für Wissenschaftliche Datenverarbeitung Göttingen (GWDG) und der Universität Kiel, die die Probleme mit W32.Blaster, Sobig.F sowie das WindowsUpdate hervorragend beschrieben haben und die wir in unserem Artikel mehrfach ausführlich zitieren ([1], [2] und [10]).

W32.Blaster – kein typischer Virus ...
Am 12. August begann der Wurm W32.Blaster sein Unwesen. Da in seinem Programmcode folgende Kommentarzeilen versteckt waren, wurde er auch LovSan genannt:

```
I just want to say LOVE YOU SAN!!
billy gates why do you make this
possible? Stop making money and
fix your software!!
```

Der Virusautor wollte damit eine schallende Ohrfeige an Microsoft austeilen: Die Existenz von W32.Blaster zeigt auf, dass Microsofts Betriebssysteme Windows2000, XP und 2003 entgegen allen vollmundigen Versprechungen eklatante Sicherheitsmängel aufweisen.
Das besonders heimtückische an W32.Blaster ist, dass er kein typischer Wurm ist und sich

eben nicht per E-Mail verbreitet. Dadurch wurden von ihm auch sicherheitsbewusste Nutzer betroffen, die weder Mail-Attachments leichtsinnig öffnen noch Outlook benutzen.

... sondern ein automatisierter Hackerangriff ...

Man muss W32.Blaster eher mit einem automatisierten Hackerangriff vergleichen, bei dem vom befallenen PC aus möglichst viele Rechner in seiner unmittelbaren Netzumgebung, also im lokalen Universitäts- bzw. Firmennetz, das ja Teil des Internet ist, angegriffen und mit W32.Blaster infiziert werden. Schneeballartig sollte so W32.Blaster im gesamten Internet verteilt werden.

... zum Lahmlegen des Microsoft Windows Update-Servers

In einer zweiten Phase ab dem 16. August 2003 sollte dann von allen befallenen PCs aus ununterbrochen der zentrale Microsoft Windows Update-Server `windowsupdate.com`, der Updates und Service-Packs für Microsoft Windows 2000 und XP bereitstellt, mit Datenpaketen überflutet und somit lahm gelegt werden. Damit wäre das Update-Konzept von Microsoft unbrauchbar geworden – ein immenser Schaden für Microsoft wäre entstanden.

W32.Blaster im Detail: Infektion und Weiterverbreitung

Grund für die Existenz von W32.Blaster war eine sehr gefährliche Sicherheitslücke in den Netzdiensten von Windows. Genauer gesagt nutzte der Wurm die DCOM-Schwachstelle im Remote-Procedure-Call(RPC)-Dienst aus. Dieses Problem war zwar seit Mitte Juli 2003 samt Patches von Microsoft für seine Betriebssysteme WindowsNT, 2000, XP und Server 2003 gemeldet [4], bei vielen Firmen und auch in unserem Campusnetz waren aber noch nicht alle Rechner gepatcht.

In obigen Betriebssystemen konnte man nämlich im RPC-Dienst (Port 135) einen so genannten Pufferüberlauf erzeugen: Bei Eingabe eines Befehls mit überlangen Parametern wird dieser normalerweise als inkorrekt erkannt und nicht ausgeführt. Bei einem Pufferüberlauf vergisst der Rechner, diese Maximallänge abzuprüfen. Der überzählige Befehlscode überschreibt den angrenzenden Speicherbereich des Hauptspeichers und gelangt ebenfalls zur Ausführung. Durch geschickte Gestaltung dieses überlangen Befehls kann nun ein Hacker erreichen, dass Befehle seiner Wahl auf dem Rechner ausgeführt werden und dieser damit beliebig manipulierbar wird.

Genau diesen Weg beschritt der Autor von W32.Blaster. Da der zum Angriff benötigte Pufferüberlauf genau auf das jeweilige Betriebssystem zugeschnitten sein musste, war es nötig, das Betriebssystem des Zielrechners zu erraten und dann den zum Zielsystem passenden Exploit (Befehlsfolge zur Ausnützung der Schwachstelle) anzuwenden. Dazu ging Blaster folgendermaßen vor:

Er „riet“ mit einer 20-prozentigen Chance Windows2000 und mit einer 80-prozentigen Chance WindowsXP als Zielbetriebssystem. Anschließend griff er den Zielrechner mit dem Windows2000- bzw. WindowsXP-Pufferüberlauf an. Das erklärt, warum ungepatchte WindowsNT-Systeme von W32.Blaster zwar angegriffen und destabilisiert, aber nicht befallen wurden: Der Autor des Wurms war einfach an WindowsNT-Rechnern nicht interessiert. Trotzdem sollten WindowsNT-Systeme ebenfalls gepatcht werden, falls ein neuer Virus auch die NT-Schwachstelle ausnützt.

Ein kleiner Trost für Nutzer von konzeptionell unsicheren Windows95/98/ME-Computern: Da auf ihren Rechnern kein RPC-Dienst läuft, sind sie von W32.Blaster nicht gefährdet.

Nach erfolgreichem Eindringen ins Zielsystem wurde dieses dazu gebracht, sich per TFTP (Trivial File Transfer Protocol, Port 69) vom angreifenden Rechner eine Kopie des Virus zu laden, diese unter dem Namen `msblast.exe` bzw. `penis32.exe` abzuspeichern und auszuführen. Mittels eines entsprechenden Registrierschlüssels wurde zudem sichergestellt, dass der Virus auch nach jedem Rechnerneustart aktiviert wird.

W32.Blaster im Detail: Lokale Schäden

Zum Glück war der Schaden, den der Wurm auf den befallenen PCs anrichtete, vergleichsweise niedrig. Die Hauptschäden waren nicht näher spezifizierbare Fehlfunktionen, Probleme beim Netzzugang (`svchost.exe`) und gelegentliche Neustarts (nur unter WindowsXP). Dauerhafte Schäden verursachte der Wurm kaum. Nach der Desinfektion konnten die Anwender

mit ihren Systemen wieder problemlos arbeiten. Allerdings soll es auch Varianten des Wurms geben, die zusätzliche Hintertür-Software installieren. Eine Desinfektion mittels Antivirussoftware wäre dann nur scheinbar erfolgreich, da die Hintertür und damit ein potenzieller Remote-Zugang für ungebetene Gäste vom Antivirusprogramm nicht erkannt und somit weiterhin aktiv gewesen wäre.

W32.Blaster im Detail:
Angriff gegen Microsoft ...

Den Hauptschaden wollte der Wurmautor jedoch Microsoft zufügen. In einer zweiten Phase ab dem 16. August 2003 startete der Wurm eine Distributed-Denial-of-Service(DDoS)-Attacke auf den WWW-Server `windowsupdate.com`, auf dem Microsoft Updates und Service-Packs für Microsoft Windows2000, XP und 2003 bereitstellt. Mit dieser DDoS-Attacke sollte versucht werden, den Windows Update-Server ununterbrochen von jedem befallenen PC aus mit jeweils 50 SYN-Paketen pro Sekunde zu überfluten, so dass dieser sofort seinen Dienst eingestellt hätte.

... aber Glück im Unglück

Zum Glück für Microsoft und seine Nutzer hatte der Wurmautor aber nicht bedacht, dass der voreingestellte Servername, von dem jeder neuere Windows-PC seine Updates bezieht, `windowsupdate.microsoft.com` lautet und dass `windowsupdate.com` lediglich ein Alternativname dieses Rechners ist.

Somit gab es ein ganz triviales Mittel, um den Angriff ins Leere laufen zu lassen: Microsoft brauchte lediglich den Rechnernamen `windowsupdate.com` ungültig zu machen. Schon war unter `windowsupdate.com` kein Rechner mehr erreichbar, während der eigentliche Update-Rechner weiterhin unter `windowsupdate.microsoft.com` unbehelligt seine Arbeit verrichten konnte.

Somit war der Spuk zum Glück zwar mit nicht unerheblichen Schäden, wenigstens aber ohne Supergau zu Ende gegangen.

Stadtmauern verhindern nicht die Pest

Auch wenn die KU zum Schutz der Netzfreigaben unter Windows zumindest die Netbios-Ports auf dem Übergang vom Internet (G-WiN) zum Intranet der KU schon länger blockiert hatte, half das leider nur wenig gegen die recht ausgeklügelte Verbreitungslogik des Wurms, der immer zuerst die Rechner in seiner Nachbarschaft infizierte. Damit war nur ein Schutz vor Angriffen aus dem Internet gegeben. Der Schutz fürs lokale Netz war in dem Moment ausgehebelt, wo ein befallener Rechner (z.B. ein Notebook) im Intranet ans Netz ging und damit so zu sagen als Ratte die Pest in die Stadt brachte. So lange es immer noch Rechner gab, bei denen die erforderliche Korrektur noch nicht eingefahren war, konnte sich der Virus im Hochschulnetz weiterverbreiten.

Vorboten von W32.Blaster

Dass ein Wurm wie der W32.Blaster erscheinen würde, war in der Tat vorhersehbar und auch von der Internet-Gemeinde erwartet worden. Allein aufgrund der Tragweite der DCOM-Schwachstelle war nämlich abzusehen, in welchem Ausmaß eine Attacke ablaufen würde und in den Tagen und Wochen nach dem 16. Juli kursierten bereits so genannte Exploits, also Programme, welche diese Schwachstelle auszunutzen verstanden. Diese erreichten eine beängstigende Perfektion und demonstrierten eindrucksvoll, wie von außen problemlos die Windows-Systeme korrumpiert, in sie beliebige Programme eingeschleust und sie dann nach eigenem Belieben ferngesteuert werden konnten. Dieses gelang bei den Windows-Versionen vom 10 Jahre alten WindowsNT bis hin zum modernen Windows2003. Lediglich Windows95, 98 und ME blieben von diesen Attacken verschont, da sie diese RPC-Dienste nicht implementiert haben.

Wie kann man
ähnliche Angriffe vermeiden?

Nun könnte man sich auf den Standpunkt stellen, der Hersteller – hier Microsoft – hatte ja rechtzeitig gewarnt und die erforderlichen Korrekturen bereitgestellt. Es hätte also einzig an den Anwendern gelegen, dass diese Epidemie so große Ausmaße annahm, denn hätten sie nur rechtzeitig ihre Systeme aktualisiert, dann wäre der W32.Blaster nicht so erfolgreich gewesen. Diese Weitergabe des Schwarzen Peters von Microsoft übers Rechenzentrum an Sie als unsere Nutzer wäre aber höchst unfair – es ist schließlich die Aufgabe des Rechenzentrums, Ihnen bei diesen Problemen weiter zu helfen und Ihnen Lösungsmöglichkeiten anzubieten.

Zeitnahes Schließen von Windows-Sicherheitslücken

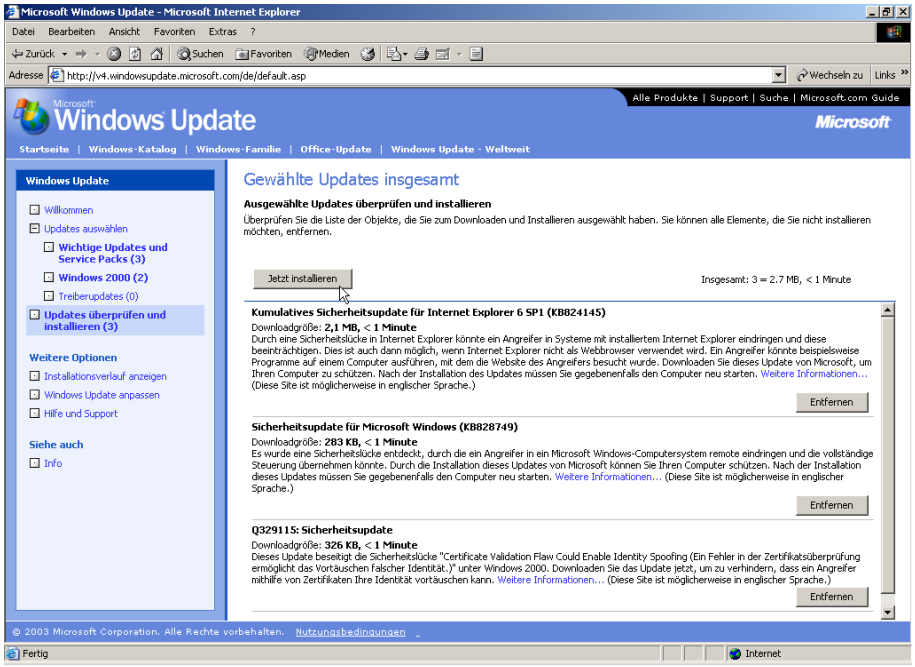
Ziel muss es deshalb sein, die Sicherheitslücken auf allen Rechnern der KU möglichst umgehend nach ihrem Bekanntwerden zu schließen. Dazu gibt es folgende Möglichkeiten, die Herr Bert Schinkel von der Universität Kiel [10] zusammengestellt hat und die wir, leicht für unseren Campus modifiziert, ebenfalls propagieren. Grundvoraussetzung ist, dass Sie auf Ihrem PC mit Administrator-Rechten angemeldet sind. Alle Möglichkeiten können Sie mit den vom Rechenzentrum unterstützten Betriebssystemen Windows2000/XP Professional nützen, während beim Auslaufmodell WindowsNT leider keine Update-Unterstützung existiert. Für Windows98/ME gibt es wenigstens teilweise Lösungen.
An der KU können Sie folgende Update-Dienste nutzen:

- „Windows Update“ via Webseite
- Update via „Automatischer Update-Service“
- „Microsoft Baseline Security Analyzer“ als umfassendes Analysetool

Einen Update-Service über einen KU-eigenen Windows-Server bietet das Rechenzentrum momentan nicht an.

- „Windows Update“ via Webseite:

  Manuell können Sie den Microsoft Windows Update-Service über eine spezielle Update-Seite im Internet benutzen. Zu dieser Internetseite gelangen Sie über den Aufruf *Windows Update* im Startmenü oder innerhalb des Internet Explorers im Menü *Extras* bzw. durch Aufruf der Internetseite: `http://windowsupdate.microsoft.com`. Wenn Sie auf Ihrem PC mit Administratorrechten angemeldet sind, können Sie sicherheitskritische Updates („Wichtige Updates und Service Packs“) sowie sonstige Verbesserungen an Ihrem Betriebssystem („Windows2000/XP-Updates sowie Treiber-Updates“) auswählen, herunterladen und installieren.



- Update via „Automatischer Update-Service“:

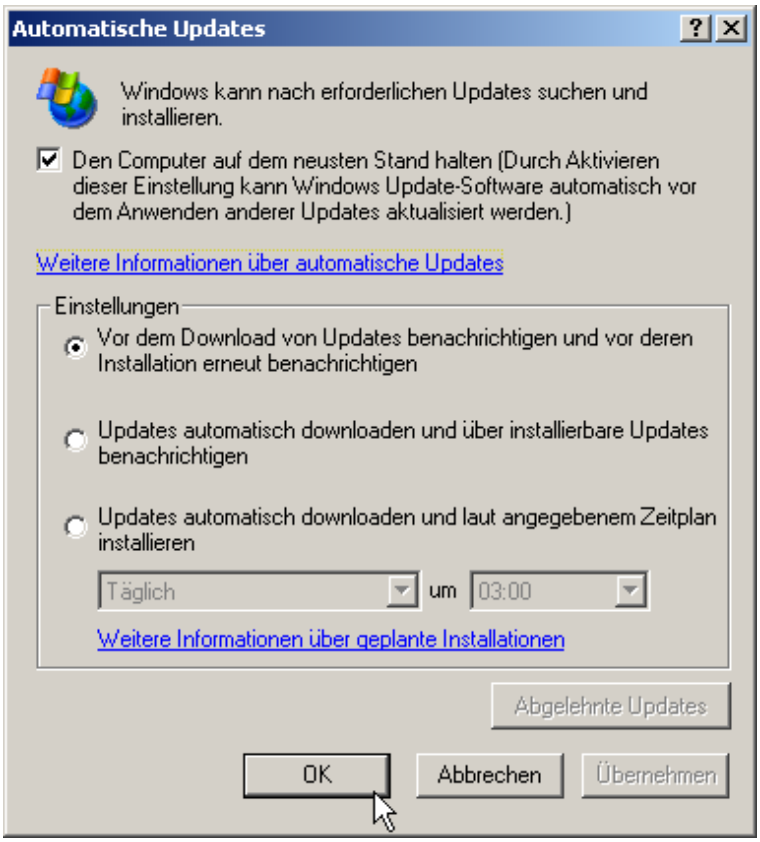
  Neben der manuellen Update-Installation existiert eine weitere Möglichkeit, die sicherheitskritischen Updates (und nur diese) automatisch herunterzuladen und zu installieren. Der Nutzer muss dann lediglich im Akutfall der Installation der Updates zuzustimmen. Sonstige Verbesserungen

am Betriebssystem müssen weiterhin gemäß dem Webseiten-Update durchgeführt werden.

Der „Automatische Update-Service“ steht Ihnen in Windows-Betriebssystemen zur Verfügung, wenn folgende Voraussetzungen bei Ihrem Betriebssystem erfüllt sind:

- Windows2000: Service Pack 3 oder höher ist notwendig (`I:\Archiv\win2000\w2ksp3.exe`)
- WindowsXP: Service Pack 1 oder höher ist notwendig (`I:\Archiv\WinXP\Patches\xpsp1_de_x86.exe`)
- Windows98 und ME: Es muss eine Erweiterung „Benachrichtigung über Updates“ via Windows-Update installiert werden.

Entspricht Ihr System diesen Voraussetzungen, so existiert in der Systemsteuerung ein weiteres Icon. Öffnen Sie (mit Administratorrechten!) das Icon, können Sie den automatischen Update-Service konfigurieren.

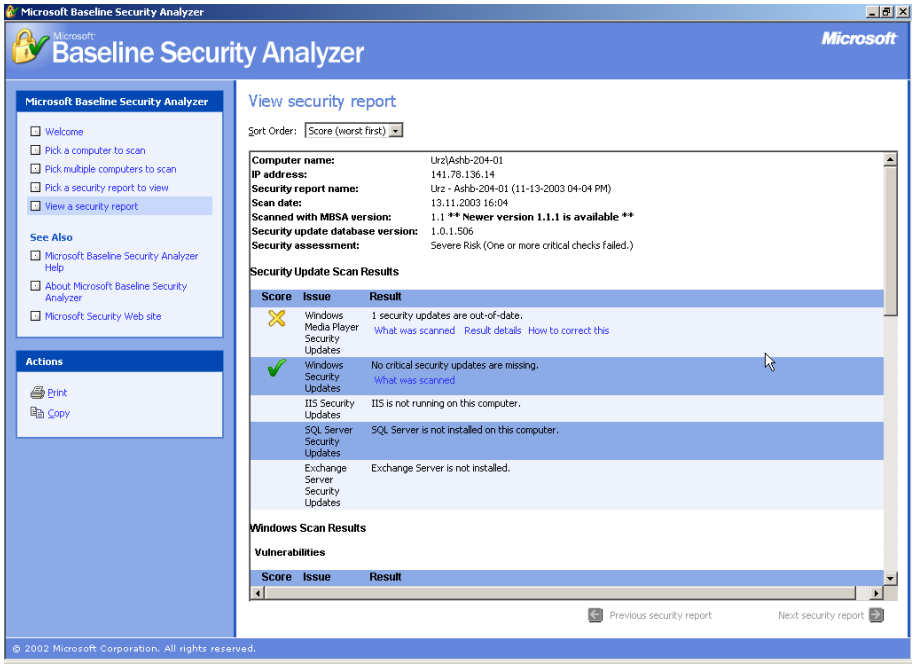


▷ „Microsoft Baseline Security Analyzer“ als umfassendes Analysetool:

Microsoft hat ein Tool veröffentlicht, mit dem der eigene PC (unter Windows2000 und WindowsXP) und entfernte PCs (sofern man darauf über Administratorrechte verfügt) auf mehrere sicherheitsrelevante Dinge untersucht wird – u.a. auf Verfügbarkeit neuer Updates und Patches oder sicherheitsrelevante Einstellungen.

Den „Microsoft Baseline Security Analyzer“ (MBSA) finden Sie direkt bei Microsoft unter [11]. Der MBSA ist nur in englischer Sprache verfügbar.

Nachdem Sie den MBSA heruntergeladen und installiert haben, können Sie das Programm starten, Ihr System auf Sicherheitslücken prüfen und diese beseitigen.



Bewertung der Update-Mechanismen
Keiner der vorgestellten Update-Mechanismen ist für sich allein genommen als die ideale Lösung zu sehen. Wie so oft ist der Mittelweg aus den drei Methoden empfehlenswert:

- ▷ Automatisches Software-Update um sicher zu gehen, dass die wichtigsten Updates installiert sind;
- ▷ MBSA zur Überprüfung von Sicherheitsaspekten;
- ▷ Update via Webseite zur Aktualisierung von weniger kritischen Komponenten.

Nochmals der Appell an Sie als Benutzer eines PCs mit Microsoft Windows Betriebssystem: Nutzen Sie die Update-Funktionen, um Ihren Rechner z.B. vor ungebetenen Gästen zu schützen und Schwachstellen zu schließen!
Nähere Hinweise zu diesen Methoden/Tools finden Sie unter [11]. Für Rückfragen stehen Ihnen die Autoren dieses Artikels gern zur Verfügung.

Ergänzende Maßnahmen
Außer dem regelmäßigen Einspielen von Updates gibt es noch folgende Maßnahmen zur Erhöhung der Sicherheit auf Ihrem PC:

- ▷ Einsatz einer Personal Firewall

  Sofern Sie WindowsXP einsetzen, können Sie über die eingebaute Internet Connection Firewall (ICF) Angriffe auf bestimmte Ports ebenfalls schnell und einfach blockieren. Dazu muss nur unter *Start → Einstellungen → Systemsteuerung → Netzwerkverbindungen* die entsprechende aktive Verbindung ausgewählt werden – meistens handelt es sich hierbei ja um die *LAN-Verbindung*, *DFÜ-Verbindungen* sollten Sie jedoch ebenfalls nicht vergessen. Das Registermenü *Eigenschaften → Erweitert* führt Sie direkt zur Internetverbindungsfirewall. Mit der Aktivierung des Eintrags *Diesen Computer und das Netzwerk schützen ...* wird die Firewall sofort in Betrieb gesetzt. Siehe hierzu auch [2].

  Unter Windows2000 sollten Sie die Beschaffung einer Personal Firewall zur Sperrung der gefährlichen Ports vornehmen [15].

- ▷ Auch wenn Ihr Virenscanner nicht das von W32.Blaster ausgenutzte Sicherheitsloch gestopft hätte, hätte sein Hintergrundwächter doch die Wurminfektion beim Abspeichern der Wurmdatei auf der Festplat-

te erkannt, da Sophos über die automatische Update-Funktion bei jedem in das Hochschulnetz integrierten PC immer tagesaktuell gehalten wird.

- ▷ Als letzten Rat empfehle ich Ihnen: Steigen Sie einfach auf Linux um! Es tut nicht weh – auch dieser Artikel wurde mit Kile/LaTeX unter Linux geschrieben!

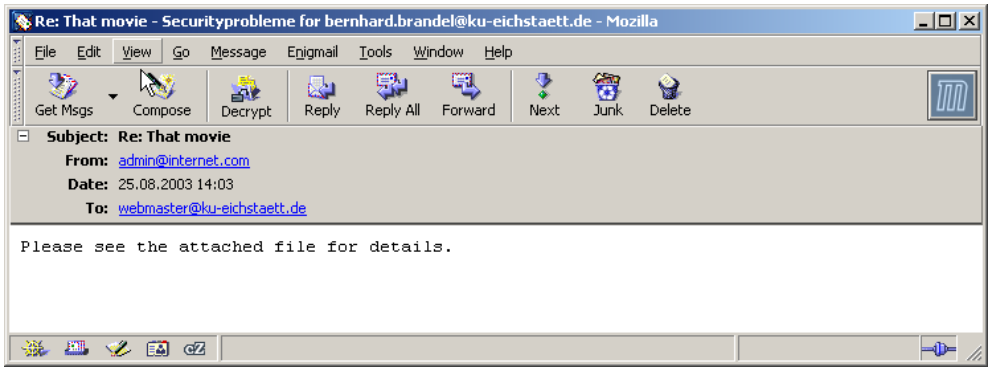
Sobig.F:
Prototyp eines Supervirus? (siehe [1])
Kaum waren die schlimmsten Folgen von W32.Blaster abgeklungen, betrat in der Nacht zum 19. August bereits ein zweiter Schädling die Bühne, dieses Mal ein alter Bekannter in neuem Gewand: Sobig.F. Diese Viren-Familie beschäftigt die Welt ja seit Beginn dieses Jahres und wird deshalb auch alphabetisch durchnummeriert, von Sobig.A bis jetzt aktuell Sobig.F. Es wird inzwischen sogar vermutet, dass es sich hier um ein größeres Projekt handelt, bei dem die verschiedensten Techniken ausprobiert werden und dessen Endergebnis uns dann sicherlich irgendwann als der „Supervirus“ heimsuchen wird.

Sobig.F: Blitzartige Verbreitung ...
Bei dieser F-Variante wurde offenbar erstmals eine neuartige Verbreitungstechnik eingesetzt, derer sich sonst nur Spammer bedienen: Zeitgleich wurde Sobig.F in zahllosen Kopien ins Internet gepumpt, so dass die Infektionsrate um etwa siebenmal höher lag als beim bisherigen Rekordhalter Klez.H zu seinen besten Zeiten. Bei einer derartig hohen Ausbreitungsgeschwindigkeit blieb den Herstellern der Antiviren-Software kaum Zeit, rechtzeitig die dafür erforderlichen Signaturen fertig zu stellen, geschweige denn, diese Signaturen den Endkunden rechtzeitig zur Verfügung zu stellen. Somit waren selbst die Anwender, die regelmäßig zeitnah ihre Virenscanner aktualisieren, für einige Stunden ungeschützt.
Glücklicherweise war die Angriffstechnik nicht besonders neu und den meisten Anwendern seit „VBS.Loveletter.A“ durchaus bekannt: der virale Dateianhang musste erst geöffnet werden, um den Virus zu aktivieren. Danach versendete er sich wie seine Vorgänger über seinen eigenen SMTP-Server, d.h. er braucht dafür kein E-Mail-Programm, und dieser eingebaute Mailverteiler unterstützte zudem noch Multi-Threading, was es dem Virus ermöglichte, mehrere Verbindungen parallel zu öffnen. Für seine schnelle Verbreitung war also bestens gesorgt. Auch die für Sobig-Viren typische begrenzte Lebensdauer war bei ihm zu beobachten; am 10. September war seine Aktivität beendet.

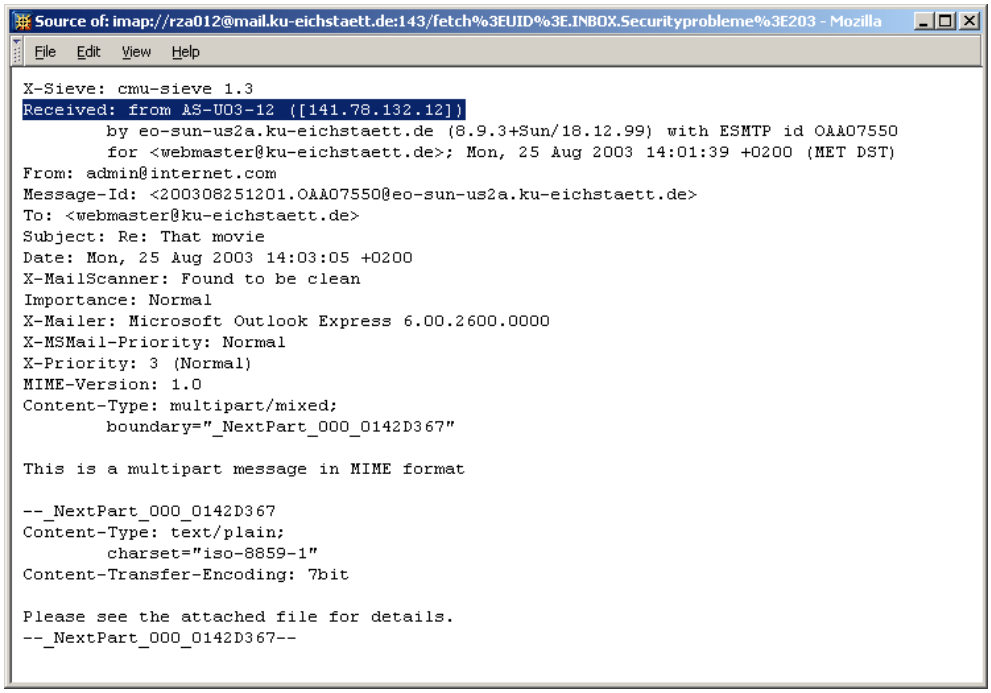
Sobig.F: Tohuwabohu
durch gefälschte Absenderadressen
Diesem Datum werden schon allein deswegen viele entgegen gefiebert haben, weil er durch eine besondere Eigenschaft für extrem viel Unruhe und Irritationen sorgte: er wirkte rufschädigend, indem er wie seine Vorgänger in der Lage war, Absenderadressen zu fälschen. Hierfür musste sich die betreffende E-Mail-Adresse nur irgendwo auf dem infizierten Rechner befunden haben – z. B. über eine ehemals aufgerufene Webseite im Browser-Cache –, und schon war die Wahrscheinlichkeit gegeben, dass diese Adresse von Sobig.F als Absender missbraucht wurde. Auch wenn dieses Verhalten nicht neu war und bereits von Klez und Bugbear wirkungsvoll eingesetzt wurde, so geschah dies doch allerdings nie in diesem Ausmaß wie bei Sobig.F.
Da inzwischen viele Mailserver mit Virenschutzprogrammen versehen sind, die virale Mails generell abweisen mit einer entsprechenden Meldung an den vermeintlichen Absender, so wurde diese Mitteilung, man hätte angeblich Viren versendet, natürlich genau an die Adresse geschickt, die Sobig vorgetäuscht hatte. Diese Internet-Nutzer waren sich aber keiner Schuld bewusst, da sie ja auch nicht die Absender dieser Mail gewesen waren. Zahllose Anwender und Institute, deren Rechner gar nicht infiziert waren, wurden somit trotzdem von dem Wurm in Mitleidenschaft gezogen: das Mail-Aufkommen explodierte gewissermaßen durch die massenhaften Viren-Mails, durch die dann ebenfalls massenhaft eintreffenden falsch adressierten Viren-Warnungen der E-Mail-Wächter und schließlich auch noch durch die sogenannten „Delivery failure“-Antworten, weil die von Sobig.F gefälschten Adressen inkorrekt waren und niemanden erreicht hatten.

Wie erkennt man
den wahren Absender einer E-Mail?
Das folgende Beispiel macht deutlich, wie ei-

ne (z.B. von Sobig.F) mit gefälschtem Absender versehene E-Mail aussieht und wie man den wahren Absender (zumindest den absendenden Rechner) ermitteln kann:
Folgende Mail, gerichtet an `webmaster@ku-eichstaett.de` stammte scheinbar von dem ominösen Absender `admin@internet.com`, den es natürlich überhaupt nicht gibt, da das Internet leider Gottes oder besser gesagt zum Glück nicht zentral administriert wird:



Ihr Mailclient bietet nun die Möglichkeit, bei geöffneter Mail die vollständigen Mailheader anzuzeigen, Unter Netscape/Mozilla geht das über den Menüpunkt *View* → *Message Source*, unter PegasusMail mittels der Tastenkombination STRG+H. Jeder unmanipulierte Mailheader enthält eine oder meist mehrere `Received:`-Zeilen, die den Weg beschreiben, den die Mail vom Absender zum Empfänger nimmt. In der **letzten** `Received:`-Zeile steht unter `From:` der wahre Absenderrechner der Mail:



In unserem Beispiel haben wir nur eine `Received:`-Zeile mit dem vom Absenderrechner vorgegebenen Rechnernamen AS-U03-12 samt verifizierter IP-Adresse 141.78.132.12. In unserem Fall stimmen sowohl Rechnername als auch IP-Adresse, da der Sobig.F-Wurm nicht so intelligent war, um auch diese Header zu fälschen. Somit wissen wir, dass der PC, von dem die Mail verschickt wurde, ein Poolrechner aus Ingolstadt war.

Da wir wissen, dass es einen Administrator des gesamten Internet erstens nicht gibt und zweitens, wenn es ihn gäbe, er ganz gewiss nicht in Ingolstadt säße, ziehen wir den Schluss: Die Absenderadresse war gefälscht und obiger PC ist wahrscheinlich virenverseucht. Letzteres bestätigt uns der (aktuelle!) Virenwächter von Sophos beim Abspeichern (nicht Doppelklicken!) des Attachments. Daher löschen wir umgehend diese Mail und wenden uns wieder unserer eigentlichen Arbeit zu.

Wenn Sie ähnliche Vorfälle bemerken, informieren Sie bitte unbedingt das Rechenzentrum, damit wir weniger wachsame Nutzer ebenfalls schnell warnen können!

Eine genaue Beschreibung der Header von E-Mails finden Sie unter [12].

Sobig.F:
Beginnt jetzt das CyberWar-Zeitalter?

Neben der neuartigen Verbreitungstechnik wurde in Sobig.F allerdings noch eine weitere Eigenschaft implementiert. Erstmalig enthielt er einen Trojaner, über den er zu einem festgelegten Zeitpunkt Dateien von speziellen Servern auf die infizierten Computer nachladen sollte, um einerseits sich selbst aktualisieren zu können und zusätzlich weitere im Internet Schaden bringende Software auf den Wirtsrechnern zu installieren.

In einem dramatischen Wettlauf mit der Zeit konnten jedoch zum Glück die in dem Virus in verschlüsselter Form abgelegten 20 Serveradressen bis zum fraglichen Zeitpunkt ausfindig gemacht und selbige vom Netz genommen werden, so dass Schäden von vielleicht nie gekannter Höhe ausblieben. Es gab sogar Befürchtungen, dass Personen oder Staaten mit besonders hoher krimineller Energie das CyberWar-Zeitalter einläuten wollten ([5],[6]).

Vorsorge ist der beste Schutz

Nachdem Sie in der letzten Ausgabe der *INKUERZE* einen überwiegend theoretischen Überblick über die verschiedenen Virentypen und ihre Eigenschaften [13] bekommen haben und nachdem wir in diesem Artikel zwei besonders agressive Viren genauer unter die Lupe genommen haben, wollen wir Ihnen noch einige **praktische Ratschläge** dazu geben, was Sie selber zu einer weitgehenden Verringerung eines Virenbefalls tun können. Denn auch hier gilt: Vorsorge ist der beste Schutz.

- Wie am Ende des Artikels in der letzten Ausgabe bereits erwähnt, ist die wichtigste Vorsorgemaßnahme immer noch die Installation und dann regelmäßige Aktualisierung eines Antiviren-Programms. Deshalb hier noch einmal unser Hinweis:
  Das Universitätsrechenzentrum hat auf allen Rechnern der öffentlichen PC-Pools das Antivirenprogramm Sophos AntiVirus installiert. Die für Antivirenprogramme unablässige regelmäßige Aktualisierung findet dort automatisch statt. Den an der Universität angestellten Mitarbeitern wird, soweit noch nicht geschehen, dringend empfohlen, auf Ihren Büro-PCs ebenfalls die Installation dieses in campus-weiter Lizenz verfügbaren Sophos AntiVirus mit automatischem Update vorzunehmen. Eine detaillierte Installationsanleitung für die Betriebssysteme WindowsNT/2000/XP finden Sie auf den Internet-Seiten des Universitätsrechenzentrums unter `http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/install` [9].

- Bekanntlich nutzen viele Viren die modernen und schnellen Kommunikationsmöglichkeiten mittels E-Mail und Internet. Damit das Antivirenprogramm erst gar nicht einen Virenbefall melden muss, sollten Sie im Umgang mit diesen Kommunikationsformen gewisse Grundregeln befolgen. Eines der größten Risiken für einen Virenbefall sind **E-Mail-Attachments**, also Anhänge, die Ihnen in Verbindung mit einer E-Mail übersandt werden. Alle derartigen Anhänge, ob ausführbare Programme, Textdokumente, Listen oder Tabellen, sind mögliche Überträger von Viren.

- Leider sind der Dreistigkeit hier inzwischen keine Grenzen mehr gesetzt: In jüngster Zeit werden E-Mail-Nutzer massiv mit einer Mail bombardiert, deren (vermeintlich seriöser) Absender `security@microsoft.com` den Empfänger mit einem Betreff „Use this patch immediately!“ unter Hinweis auf die Gefährlichkeit bestimmter Viren im Internet dazu auffordert, sofort einen in der Anlage befindlichen Sicherheitspatch zu installieren. Die Datei, die den angeblichen Si-

cherheitspatch enthält, ist unter verschiedenen Namen im Umlauf; beispielsweise erscheint sie unter dem Namen `patch.exe`. Wird das Attachment durch Doppelklick auf diese Datei geöffnet und damit auch als Programm ausgeführt, so wird dadurch ein Virus (Dumaru-Virus) aktiviert, der nun seine schädigende Wirkung entfalten kann. **Öffnen Sie deshalb keine E-Mail-Attachments durch Doppelklick**!

- Speichern Sie E-Mail-Attachments zunächst als Datei auf einem Datenträger (Festplatte oder Diskette) ab. Bei den am URZ verwendeten Mailsystemen Pegasus-Mail, Mozilla und Netscape Messenger geschieht dies durch **einfaches(!)** Anklicken des Attachments und anschließendes Auswählen der Option *Save* bzw. Rechtsklick → *Save as ...* Wenn Sie, wie auf den Rechnern unserer Universität, ein Antivirenprogramm mit On-Access-Scanmodus (d.h. Virenüberprüfung sofort bei Zugriff auf eine Datei) installiert haben, kann das Antivirenprogramm beim Ablegen der verseuchten Datei, in diesem Fall des verseuchten E-Mail-Attachments, unverzüglich eingreifen.

- Da sich Viren und Würmer mittlerweile schneller verbreiten als aktuelle Virensignaturen vom Antiviren-Software-Hersteller verfügbar sind, ist ein gesundes Misstrauen gegenüber den Mails und ganz besonders gegenüber ihren Dateianhängen dringend geboten, auch dann, wenn sie von Bekannten kommen und wenn auch der Virenscanner keinen Virus erkennt. Seit Klez, Bugbear und Sobig wissen wir, die Absenderadresse könnte jederzeit gefälscht sein. Außerdem tauschen viele Menschen auch im Freundes- und Bekanntenkreis per E-Mail Bildschirmschoner, Grußkarten, Animationsprogramme oder ähnliches aus, die sie aus dem Internet heruntergeladen haben. Auch diese aus dem Internet geholten Programme oder Dokumente sind des öfteren bereits virenverseucht. Prüfen Sie in Zweifelsfällen wie oben beschrieben die Header und fragen Sie beim Rechenzentrum um Rat.

- Schalten Sie Ihren gesunden Menschenverstand ein: Fragen Sie sich, wie wahrscheinlich es ist, dass ein deutscher Kollege Ihnen auf englisch E-Mails mit englischem Betreff wie z.B. „See this attachment“ schickt. Dass die deutsche Sprache international so unbedeutend ist, ist in diesem Fall ausnahmsweise von Vorteil: Ein Virenautor schreibt meist seine E-Mail-Viren in der Sprache, die überall verstanden wird, also auf Englisch. Auf Deutsch würde der Virus sich längst nicht so gut verbreiten.

- E-Mail-Programme wie Outlook und Outlook Express sollten Sie meiden wie der Teufel das Weihwasser. Der nächste Virus ist Ihnen sonst schon garantiert (siehe [14]).

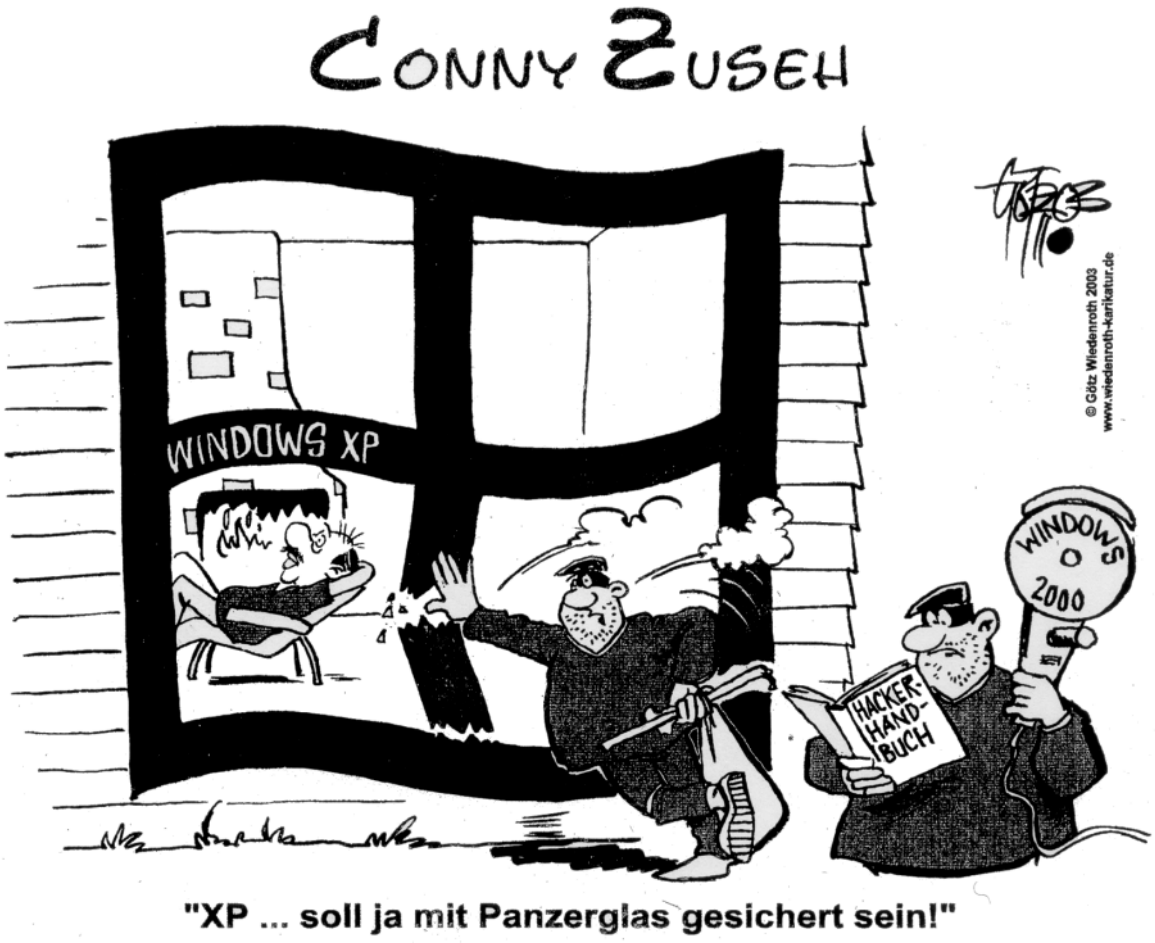
- Wenn das Kind schon in den Brunnen gefallen ist und sie einen Virus auf Ihrem PC vermuten, wenden Sie sich bitte unverzüglich ans Rechenzentrum. Ein einfaches Update Ihres Virenscanners bei kompromittiertem System nützt nicht immer, da intelligente Viren das System in ihrer Hand haben und „gegnerische“ Software erkennen und deaktivieren können. Wir versuchen Ihnen dann mittels Tools wie „Stinger (Mcafee)“ [8] oder „SAV32CLI (Sophos)“ [7] weiterzuhelfen, mit denen man auch solche Viren im laufenden kompromittierten Betrieb entfernen kann.

- Ob ein Virus eine Hintertür für „wissende“ Internet-Nutzer eingebaut hat, die damit auch nach Entfernen des Virus auf Ihren PC Zugang haben, kann auch die beste Antivirussoftware nicht bemerken. Nehmen Sie daher bitte **immer** im Schadensfall Kontakt zum Rechenzentrum auf, um dieses Risiko abschätzen zu können!

Fazit und Konsequenzen

Es hat sich gezeigt, dass Würmer wie W32.Blaster und Viren wie Sobig.F eine neue Herausforderung an das bestehende Sicherheitskonzept darstellen. Für die Anwender bedeutet dies, dass sie sich vielleicht auf bekannte und in der Vergangenheit bewährte Sicherheitsmaßnahmen nicht mehr werden hundertprozentig verlassen können. Das uneingeschränkte Vertrauen auf nur ein Produkt, wie z.B. den Virenscanner, mag alleine auf Dauer nicht genügen. Doch viel

wichtiger noch als das wahllose Hochrüsten mit Sicherheitsprodukten, die dann womöglich sich gegenseitig oder gar die tägliche Arbeit behindern, ist die genauere Kenntnis der Gefahren. Wenn man weiß, welche Gefahr droht, kann man sich viel besser dagegen schützen.
Das Rechenzentrum ist stets bemüht, Sie rechtzeitig vor den Gefahren zu warnen, Lösungsmöglichkeiten zu eröffnen und durch flankierende Maßnahmen das Schadenspotenzial möglichst gering zu halten. Als ein nicht unwichtiger Teil eines Sicherheitskonzepts darf aber nicht vernachlässigt werden, dass man auch als Anwender stets davon ausgehen sollte, selber irgendwann einmal das Opfer eines Wurms oder Virus' zu werden. Je öfter man dann dieses Szenario durchspielt und die erforderlichen Gegenmaßnahmen erprobt, desto weniger wird man in Panik verfallen, falls diese Situation dann wirklich eintritt.
Das Universitätsrechenzentrum bietet regelmäßig Kurse zum Thema Security an, bei denen genau diese Probleme angesprochen werden. Die Resonanz zu diesen Kursen könnte deutlich besser sein. Viele Nutzer interessiert das Thema Security erst dann, wenn ihr PC virenverseucht oder gehackt worden ist. Vielleicht kann dieser Artikel dazu beitragen, auch diesbezüglich eine Bewusstseinsänderung herbei zu führen. Sie sind herzlich zu unseren Kursen eingeladen!



"XP ... soll ja mit Panzerglas gesichert sein!"

Literatur (Links)

zu W32.Blaster, Sobig.F und Personal Firewall:
[1] GWDG:
`http://www.gwdg.de/forschung/publikationen/gwdg-nr/GN0309/gn0309_03.html`

[2] Firewall unter XP:
`http://www.gwdg.de/service/sicherheit/aktuell/msblast.html`

[3] Personal Firewall Reviews:
`http://www.firewallguide.com/software.htm`

[4] Microsoft Security Bulletin MS03-026:
`http://www.microsoft.com/technet/security/bulletin/MS03-026.asp`

[5] F-Prot:
`http://www.f-secure.com/v-descs/sobig_f.shtml`

[6] F-Prot:
`http://www.f-secure.com/news/items/news_2003082200.shtml`

zur Entfernung im Akutfall:
[7] Stinger(McAfee):
`http://download.nai.com/products/mcafee-avert/stinger.exe`

[8] Sav32.cli (Sophos):
bei installiertem Sophos AntiVirus als `sav32cli.exe` im Verzeichnis
`c:\programme\Sophos SWEEP for NT`

zu URZ-Services:
[9] Sophos-Anleitung (mit AutoUpdate):
`http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/install`

zu Update-Sicherheit:
[10] Uni Kiel:
`http://www.uni-kiel.de/rz/pc/windows-update/`

[11] Microsoft Baseline Security Analyzer (MBSA) 1.1.1:
`http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp`

Beschreibung der Header von E-Mails:
[12] `http://sites.inka.de/ancalagon/faq/headerfaq.php3`

URZ-Artikel zum Thema E-Mail-Sicherheit:
[13] Wegen Infektionsgefahr geschlossen ...:
`http://www1.ku-eichstaett.de/urz/inkuerze/1_03/viren.html`

[14] Finger weg von Internet Explorer und Outlook!:
`http://www1.ku-eichstaett.de/urz/inkuerze/2_02/ieoutlook.html`

Ansprechpartner im URZ:	*Zimmer:*	*Telefon:*	*PMail:*
Bernhard Brandel	IN: HB-204	-1888	`bernhard.brandel`
Heribert Zimmermann	EI: eO-003	-1662	`heribert.zimmermann`

Wider die SPAM-Mail-Flut

Dr. W. A. Slaby

Wachsende Klagen unserer Nutzer gegen die zunehmende Flut unerwünschter Werbe-Mails veranlassen uns, schon vor der Fertigstellung und Inbetriebnahme universitätsweiter Abwehrmechanismen auf dem zentralen Mail-Server diese konkreten Pläne und Entwicklungen vorzustellen. Außerdem soll beschrieben werden, wie jeder Nutzer auch jetzt schon bei Verwendung eines der Mail-Clients* NetscapeMail *des* Netscape Communicators *7.1 bzw.* Pegasus Mail *4.12a auf einfache Weise unerwünschte Werbe-Mails aus seinem Posteingangsfach herausfiltern kann. Die Darstellung zu* NetscapeMail *stützt sich dabei weitgehend auf einen Artikel von Dr. Markus Zahn in der Benutzerzeitschrift connect 1/2003 des Rechenzentrums der Universität Augsburg, den wir mit freundlicher Genehmigung nachstehend zitieren.

„Der massenhafte Versand von Werbe-Mails an wahllose Adressaten, kurz „SPAM“ oder „Junk-Mail“ genannt, hat in der jüngsten Vergangenheit leider eine rasante Entwicklung genommen. Dies wird durch nationale wie internationale Statistiken belegt und lässt sich von vielen Nutzern auch mit einem Blick auf das eigene elektronische Postfach schnell bestätigen. Doch bei der gezielten Unterdrückung solcher unerwünschter Botschaften ist guter Rat teuer. Bevor wir uns in die Praxis stürzen, werfen wir zum besseren Verständnis des Verfahrens zunächst noch einen kurzen Blick auf die zugrunde liegende Theorie.

Die Theorie

In der Vergangenheit wurde versucht, die „bösen“ Mailserver, also Mailserver, die entweder explizit SPAM-Mails verschicken oder zumindest deren Versand nicht unterbinden, kategorisch auszugrenzen. Leider bietet dieser Ansatz nur unzureichend Schutz. Zum einen können mit diesem Verfahren ohnehin nicht alle Bösewichte erwischt werden, zum anderen kommt es auch vor, dass hin und wieder gewollte E-Mails irrtümlich unterdrückt werden, nur weil sie auf dem Weg über einen dieser „bösen“ Mailserver gewandert sind. Der Verlust einer wichtigen Nachricht wiegt dabei meist wesentlich schwerer als der Frust mit den SPAM-Nachrichten.

Im August 2002 fand Paul Graham mit seinem Artikel „A Plan for SPAM“ große Aufmerksamkeit. Anstatt schwerfälliger, nicht auf die Anwender zugeschnittener Abwehrmaßnahmen rückt der Autor einen statistischen Ansatz („Bayesian Filtering“) in den Mittelpunkt. Kurz gesprochen entscheidet bei diesem Verfahren jeder Anwender für sich selbst, welche E-Mails bei ihm den Status „unerwünscht“ erhalten. Ein passender Mail-Filter lernt aus diesen Aktionen des Nutzers und erkennt mit der Zeit automatisch, ob neu eintreffende Mail für diesen Anwender als erwünscht oder unerwünscht gilt. Was zunächst abenteuerlich klingt, erweist sich bei näherer Betrachtung als raffinierte und gleichzeitig äußerst zuverlässige Idee.

Ausgangspunkt für das von Paul Graham beschriebene Verfahren (`http://www.paulgraham.com/spam.html`) ist eine Grundmenge an erwünschter und unerwünschter Mail. Jede dieser Mails wird in ihre einzelnen Worte („Tokens“) aufgeteilt und für jedes dieser Tokens wird bestimmt, wie oft es in erwünschter Mail auftritt und wie oft es in der Menge unerwünschter Mail zu finden ist. Aus diesen Trefferlisten wird dann für alle erkannten Tokens die Wahrscheinlichkeit bestimmt, mit der eine Mail, die dieses Token enthält, SPAM ist.

Jede neu eintreffende Post wird ebenfalls in ihre Bestandteile zerlegt. Ausgehend von der zuvor aufgestellten Wahrscheinlichkeitstabelle werden die 15 auffälligsten Worte der Mail ermittelt. Das sind die Tokens, deren Wahrscheinlichkeit den größten Abstand zu einem neutralen Wert besitzt. Diese Tokens sind daher besonders gute Indizien für die Beantwortung der Frage „SPAM oder nicht SPAM?“ Aus den Werten dieser 15 aussagekräftigen Tokens wird abschließend eine „kombinierte Wahrscheinlichkeit“ errechnet und die neue Post wird dieser Berechnung entsprechend als „gut“ oder „schlecht“ eingestuft.

Die Praxis

Zu unserem Glück müssen wir als Nutzer diese Berechnugen nicht selbst vornehmen. Mehr und mehr E-Mail-Programme unterstützen heute derartige statistische Verfahren. Ein gutes Beispiel ist NetscapeMail, das Mailprogramm des Netscape Communicators 7.1, das ich hier vorstelle, [Netscape Communicator 7.1 steht mit Beginn des Wintersemesters 2003/2004 in allen Pools zur Verfügung; die Installationsdatei für die anderen Nutzer findet sich unter `I:\ARCHIV\Netscape\v7.1`.]

Zunächst gilt es, wie oben beschrieben, eine Menge von SPAM-Mails zu horten. Sammeln Sie dazu am besten einige Tage lang die unerwünschten Mails. Markieren Sie diese Mails in NetscapeMail durch ein Klick auf den „Junk"-Knopf als unerwünscht.

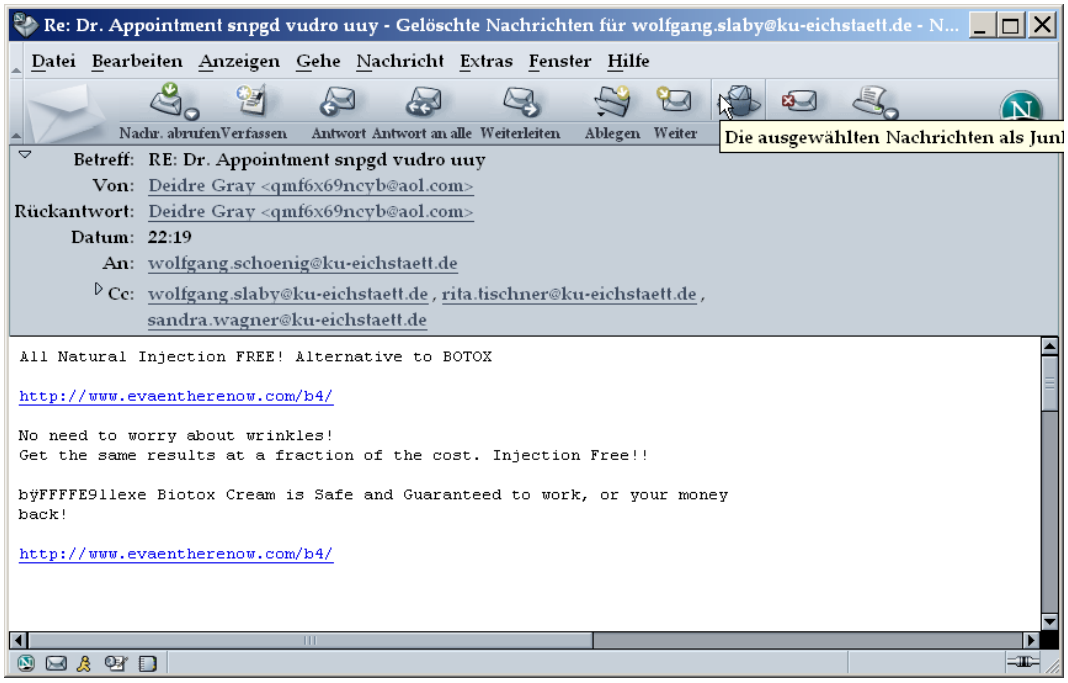


Abb. 1: So markieren Sie Mails als SPAM ...

Die Mail wird dadurch als SPAM deklariert und das Mail-Programm lernt wieder ein paar „Vokabeln" für spätere Aufgaben dazu. Je mehr Mails Sie auf diese Weise klassifiziert haben, desto besser passt sich der Algorithmus an Ihre persönlichen Bedürfnisse an. Anschließend können Sie die Mails entweder löschen oder in den Ordner „Junk" verschieben.

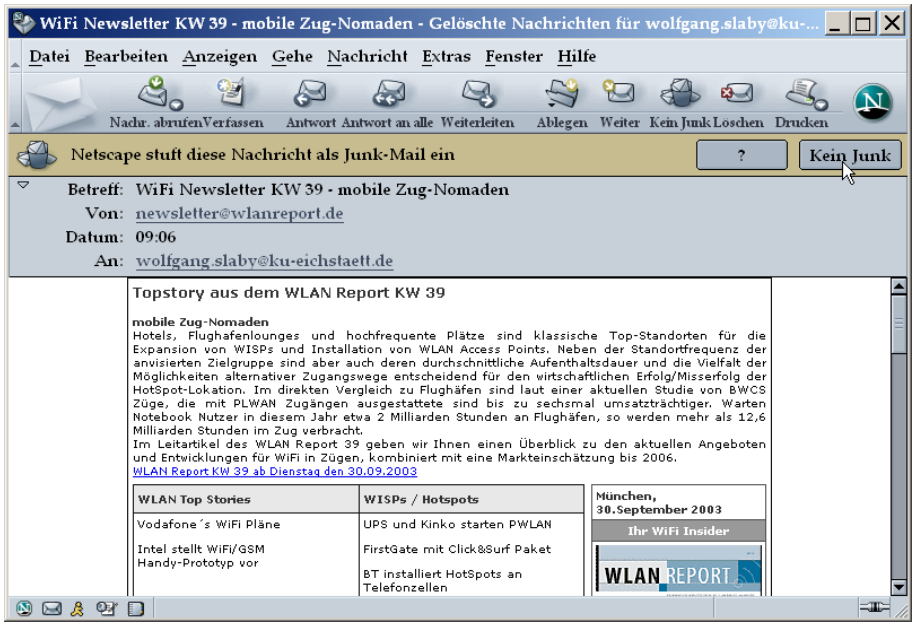
Sobald Sie Ihr Mail-Programm ausreichend trainiert haben, können Sie die automatische SPAM-Erkennung zuschalten. Wählen Sie dazu aus dem Menü *Extras* den Punkt *Junk-Mail-Filter ...* aus und aktivieren Sie die Option *Junk-Mail-Filter aktivieren*. [Zusätzlich sollten Sie ankreuzen, dass eingehende Nachrichten, die als Junk-Mail eingestuft wurden, automatisch in den „Junk"-Ordner verschoben werden, und dass manuell als Junk markierte Nachrichten gelöscht werden. Abschließend klicken Sie auf *OK*.] Ab jetzt werden alle eingehenden E-Mails ohne Ihr Eingreifen getestet. Sollte das Programm sich einmal irren, dann vergessen Sie bitte nicht, den Status der Mail durch einen Klick auf den „Junk"-Knopf zu korrigieren – nur so können Sie das Verhalten des Programm sukzessive an Ihre Bedürfnisse anpassen.

Abb. 2: ... und passen die persönlichen SPAM-Einstellungen an.

Persönliches Fazit

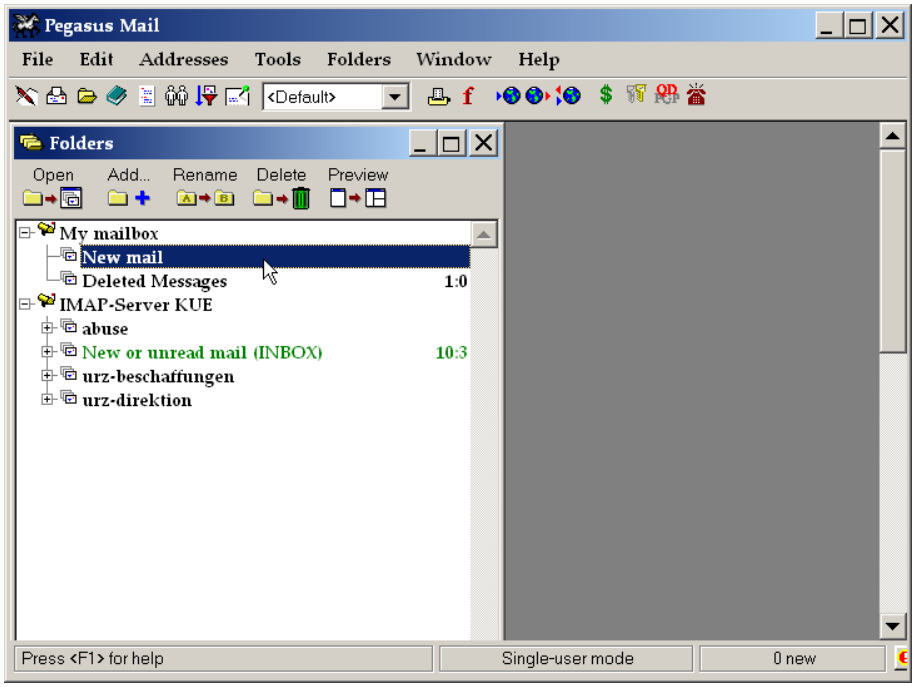
Ich selbst habe vor gut einem Monat angefangen, dieses Feature von NescapeMail zu nutzen. In den vergangenen Wochen habe ich über 2000 unerwünschte Mails erhalten, im Schnitt also etwas mehr als 60 Junk-Mails pro Tag. Ein Blick auf mein normales Mailaufkommen verrät mir, dass ich damit deutlich mehr unerwünschte als erwünschte Mails erhalte. Bereits nach einem Monat Training erkennt mein Mail-Programm aber über 95% der eingehenden SPAM-Mails als unerwünscht und verschiebt sie wie gewünscht und ohne weitere Zuarbeit automatisch in den Junk-Ordner. Die wenigen nicht erkannten Werbe-Mails markiere und verschiebe ich von Hand. Damit kann ich das Verhalten meines Mail-Programms Schritt für Schritt verbessern.

Von Zeit zu Zeit gehe ich dann zur Sicherheit mit einem schnellen Blick quer über die neu hinzu gekommenen SPAM-Mails im Junk-Ordner. Falls eine wichtige Mail vom Programm fälschlicherweise als SPAM deklariert wurde, kann ich dies auf diesem Wege entdecken und durch Klicken auf den Schaltknopf *Kein Junk* korrigieren. Dies ist bislang allerdings nur höchst selten passiert! Insgesamt bin ich mit der neuen Möglichkeit der SPAM-Erkennung sehr zufrieden und kann das Verfahren allen SPAM-Geplagten wärmstens weiter empfehlen.“



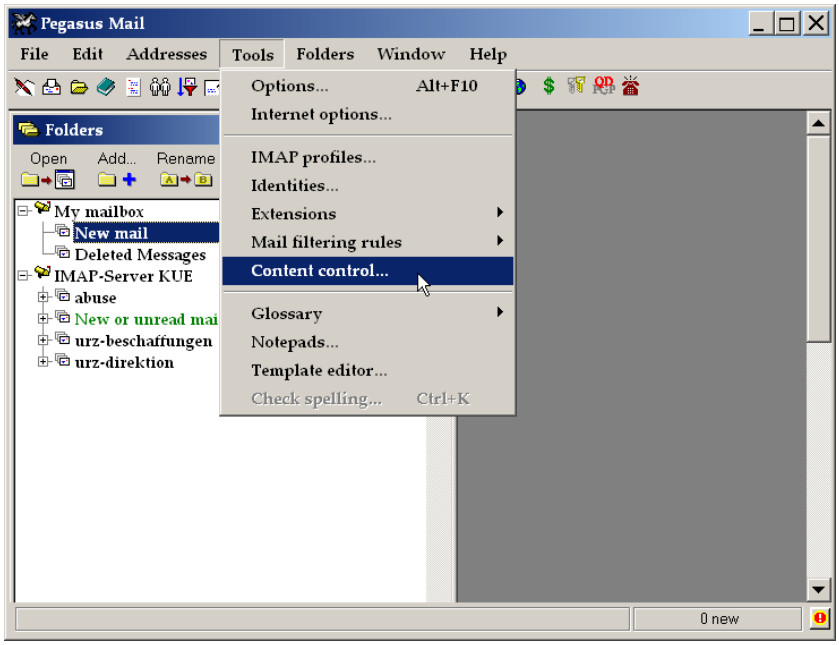
Aussieben mit PegasusMail

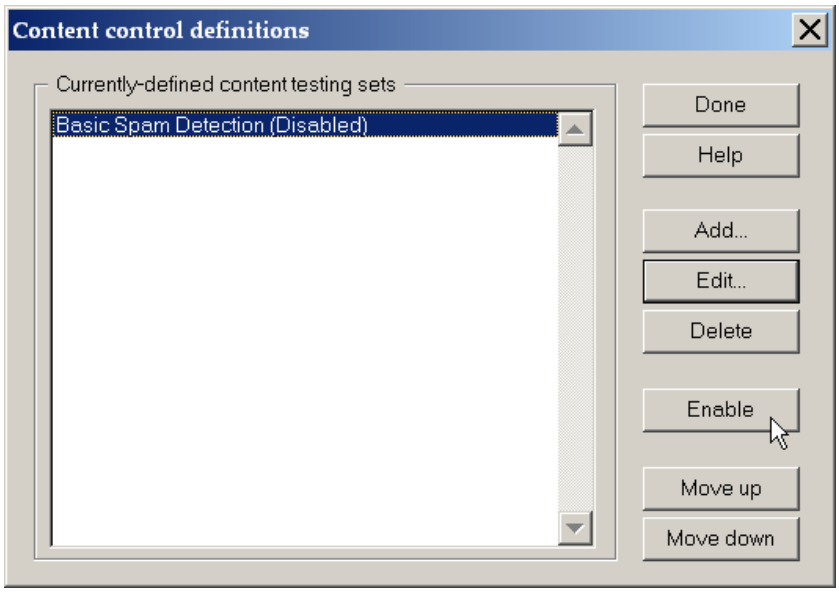
Leider funktioniert die oben beschriebene Methode des Herausfilterns unerwünschter Werbe-Mails mit NetscapeMail nur dann, wenn entweder Ihr Eingangspostfach auf dem IMAP-Mailserver des Universitätsrechenzentrums liegt oder Sie Ihre eingegangenen Mails über das POP3-Protokoll zur weiteren Bearbeitung mit NetscapeMail auf Ihren lokalen Arbeitsplatzrechner herunterladen. Andernfalls, wenn also Ihr Eingangspostfach auf einem unserer NetWare-Server liegt und von Ihnen auch dort verwaltet wird, bietet Ihnen jedoch PegasusMail eine ähnliche Möglichkeit, SPAM-Mails auszusieben. Dieses bei PegasusMail so genannte *Content Control* lässt sich allerdings nur auf Ihr Posteingangsfach auf dem NetWare-Server, den *New mail* Ordner, anwenden.



Anders als NetscapeMail arbeitet PegasusMail dabei nicht mit einem statistischen Verfahren zur Bewertung von SPAM, sondern mit einer Datei `spambust.dat` von Filterregeln, die anhand von Absenderangaben bzw. von typischen Begriffen im Mail-Header oder im Nachrichtentext unerwünschte Werbe-Mails aussortieren. Ein ausgefeiltes System von Filterregeln wird von PegasusMail bereits mitgeliefert; es kann von jedem Nutzer im Bedarfsfall ergänzt werden.

Über die Option *Tools* ⟶ *Content control ...* starten Sie ein Fenster, in dem Sie die Filterung aktivieren oder das System der Filterregeln weiter bearbeiten und ergänzen können.



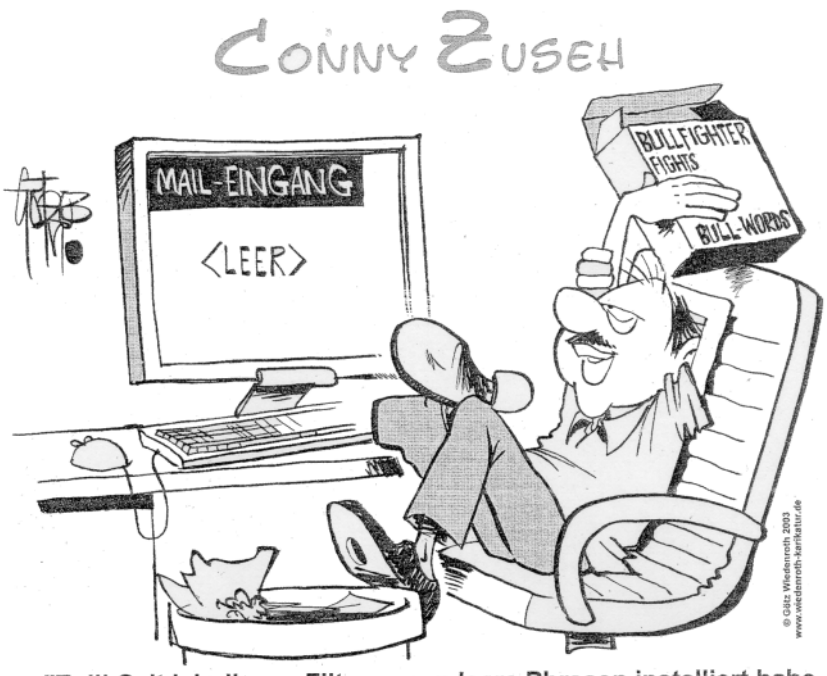


Ein Betätigen des Schaltknopfes *Enable* aktiviert das in `spambust.dat` hinterlegte System von Filterregeln, mit denen anschließend jede eingehende Mail überprüft und gegebenenfalls ausgesondert wird; ein Klicken auf *Done* schließt diesen Aktivierungsvorgang ab.

Das Ziel

Wesentlich sinnvoller und ökonomischer, als jeden Nutzer einzeln die notwendigen Vorkehrungen zum Aussondern unerwünschter Werbe-Mails treffen zu lassen, ist es selbstverständlich, entsprechende Filter-Verfahren am zentralen Mail-Server der Universität einzusetzen. Da dies auf der bisherigen Hardware unseres Mail-Servers nicht möglich ist, haben wir vor kurzem einen neuen Mail-Server beschafft, auf dem unter dem Betriebssystem LINUX mit Hilfe verschiedener Programme folgendes Verfahren eingerichtet wird: Jede auf dem Mail-Server eingehende E-Mail, die vom Mail-Server-Prozess **postfix** entgegengenommen wird, wird zunächst an das SPAM-Filterprogramm **SpamAssassin** zur Überprüfung weitergeleitet, welches ebenso wie das Filterprogramm in NETSCAPEMAIL auf der Grundlage einer statistischen Analyse des Mail-Inhalts eine Bewertung vornimmt, in welchem Grade es sich dabei um SPAM handelt oder nicht. Da das Universitätsrechenzentrum (ähnlich wie Ihr Briefträger bei der Postzustellung zuhause) nicht berechtigt ist, selbst mit hoher Wahrscheinlichkeit als SPAM eingestufte Mails eigenmächtig zu vernichten, werden an dieser Stelle derartige Mails nur durch einen Zusatz der Form `{Spam ...}` im Betreff-/Subject-Feld gekennzeichnet, der Ihnen und Ihrem Mail-Client ein leichtes Aussondern ermöglicht.
Anschließend wird jede Mail mit dem SOPHOS Virencheck-Programm daraufhin untersucht, ob die Mail oder einer ihrer Anhänge mit einem Virus infiziert ist. Auch in diesem Fall wird im Betreff-/Subject-Feld eine entsprechende zusätzliche Kennzeichnung der Form `{Virus!}` angebracht. Erst nach diesen beiden Überprüfungen wird die Mail in Ihrem Eingangsfach bereitgestellt.
Wir hoffen, den neuen Mail-Server mit diesem Verfahren der SPAM- und Virenüberprüfung bis zum Jahresende einsatzfähig zu haben und dann die E-Mail-Postfächer unserer Benutzer Zug um Zug auf diesen neuen Mail-Server umstellen zu können.

Ansprechpartner im URZ:	*Zimmer:*	*Telefon:*	*PMail:*
Alexander Kaltenbacher	IN: HB-203	-1885	`alexander.kaltenbacher`
Tomasz Partyka	EI: eO-107	-1668	`tomasz.partyka`
Dr. Wolfgang A. Slaby	EI: eO-109a	-1214/-1462/-1670	`wolfgang.slaby`



"Toll! Seit ich diesen Filter gegen leere Phrasen installiert habe, kommen auch keine Mails von meinem Chef mehr an!"

Informatik Osten-14: Wenn die Projektionsleinwand Tafel und Kreide ersetzt

Prof. Dr. J. Desel/ P. Ihrler

Im vergangenen Sommersemester ist der Lehrstuhl für Angewandte Informatik (Prof. Jörg Desel) in das Gebäude in der Ostenstraße 14 gezogen. Mittlerweile sind dort auch die Dienstzimmer der Informatik-Professur bezogen, denn Prof. Stephan Diehl hat den Ruf auf diese Stelle zum 1. Oktober angenommen. Während im Altbau Büros und Server der Informatiker untergebracht sind, wurden im neu errichteten Anbau im Garten ein Hörsaal und ein Seminarraum mit zukunftsweisender Multimedia-Ausrüstung eingerichtet, die ein Lehren und Lernen mit state-of-the-art Technologie ermöglichen.

Zunächst einmal fällt auf, dass in beiden Räumen Rechner, Bildschirme und weitere Technik auf den ersten Blick nicht auffallen. Tischreihen im Hörsaal und Tische in U-Form im Seminarraum erlauben klassische Lehr- und Lernformen ohne Beeinträchtigung durch Bildschirme auf den Tischen und verwirrende Kabelstränge. Auch ist die Technik nicht zu hören, denn auf Geräte mit Lüfter wurde fast vollständig verzichtet. Trotzdem stehen in diesen Räumen vielfältige technische Möglichkeiten zur Ergänzung der Lehre zur Verfügung. Grundprinzip bei der Konzeption des Technikeinsatzes war aber, dass Informatik nicht nur Programmieren ist, sondern sich mit dem Einsatz von Rechnertechnologie für den Menschen beschäftigt und entsprechend auch in der Informatik-Lehre Rechner sich den Bedürfnissen und Gewohnheiten der Dozenten und Studierenden unterordnen, und nicht umgekehrt.

Abb.1: Dozentenpult/Medientisch

In beiden Räumen können Studenten an Tischen arbeiten, in denen jeweils zwei Glasscheiben den Blick auf darunter montierte Flachbildschirme erlauben. Die zugehörigen lautlosen Rechner (thin clients) sind am Tischgestell fest montiert. Die Rechnerleistung wird von zwei Windows-Servern übernommen, die bald durch zwei Unix-Server ergänzt werden. Im Hörsaal stehen dem Dozenten zusätzlich zwei leistungsfähige Windows-Rechner zur Verfügung, die in einem riesigen Dozentenpult untergebracht sind. Im Seminarraum ist ein zusätzlicher Multimedia-Rechner mit dem dort fest installierten Smartboard verbunden. Über Smartboards wurde in der INKUERZE-Ausgabe 1/2002 (`http://www1.ku-eichstaett.de/urz/inkuerze/1_02/hoersaele.html`) bereits berichtet, der vorliegende Beitrag konzentriert sich deshalb auf die Ausstattung des größeren Hörsaals im Gebäude Ostenstraße 14.
Mit ein paar Fingertips auf einen Touch-Bildschirm schalten sich die Projektoren und weitere Medien an, die verschiedenartige Formen einer Lehrveranstaltung unterstützen. Und falls es interessierte und reisemüde Zuhörer/-schauer z.B. in Ingolstadt gibt, so können diese über eine Videokonferenz teilnehmen.

Der Hörsaal ist mit einer Vielzahl von Geräten ausgestattet, die teilweise in dem Dozentenpult untergebracht sind und teilweise dem Studenten an seinem Arbeitsplatz zur Verfügung stehen. Manche Geräte können auch gemeinsam genutzt werden. Grundidee ist, dass alle Geräte über eine zentrale Steuereinrichtung, den Crestron-Touch-Bildschirm mit einer intuitiv aufgebauten Menüstruktur, gesteuert werden. So kann man beispielsweise über die Menüs des Bildschirms, die einer PC-Bedieneroberfläche ähnlich sind, auswählen, dass der Dozenten-PC-1 auf dem Projektor-2 angezeigt wird und der Bildschirm von Student xy auf dem Projektor-1.

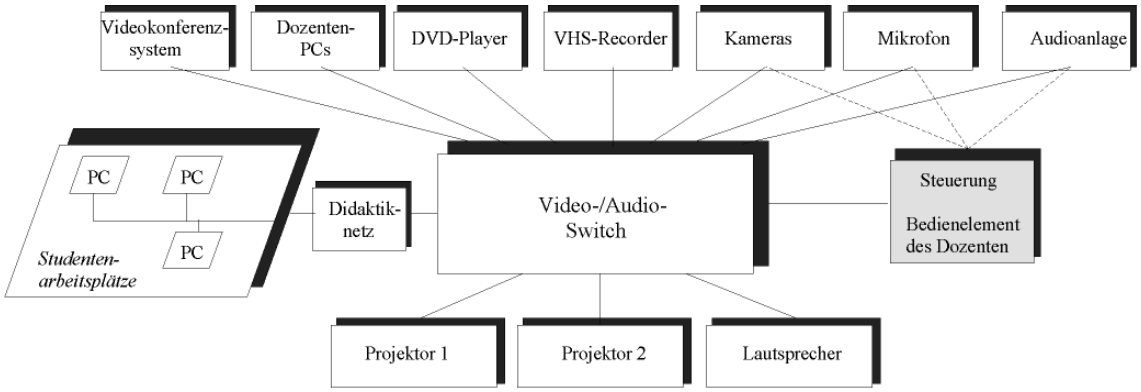


Abb.2: Konfiguration der Steuerung und des Switches

Im Folgenden werden die einzelnen Geräte aufgelistet und beschrieben:

1. Präsentationsgeräte:

- ▷ Zwei Videoprojektoren (Beamer);
- ▷ Audio-Anlage mit Verstärker, Mischer, Lautsprecher;
- ▷ Videovorschau-Monitore: Die Bildschirme der beiden Dozenten-PCs können als Kontrollbildschirme benutzt werden, um z. B. einen Video-Film an die gewünschte Stelle zu spulen, bevor er auf die Leinwand projiziert wird.

2. Computer:

- ▷ 2 Dozenten-PCs: Die PCs sind in den Dozententisch eingebaut, die Bildschirme unterhalb der Arbeitsplatte aus Glas ange-

bracht, so dass sie den Sichtkontakt zwischen Studenten und Dozent nicht stören;

- ▷ Laptop-Anschluss: über ein in den Dozententischen eingelassenes Steckerfeld (Anschlüsse für Strom, Netzwerk, Projektor, Audio);
- ▷ 24 Studenten-PCs: Die PCs und ihre Bildschirme sind in ähnlicher Weise wie die Dozenten-PCs in die Tische eingebaut.

3. „Quellen"-Geräte:

Sie werden in der Regel mit einem Projektor auf eine der beiden Leinwände projiziert und/oder über die Audioanlage ausgegeben.

- ▷ VHS-Videoplayer:
  spielt Video-Kassetten ab;
- ▷ DVD-Player:
  spielt (Film, Musik)-DVDs und -CDs ab;
- ▷ Kameras:
  Sie nehmen zum einen den Dozenten und zum anderen die Studenten ins „Visier". Die Kameras werden in erster Linie für Videokonferenzen eingesetzt, ihre Bilder können jedoch auch auf die Leinwände projiziert werden.
- ▷ Mikrofon:
  Sowohl der Dozententisch als auch alle Studentenarbeitsplätze sind mit Mikrophonen ausgestattet, letztere als Headsets. Sie dienen ebenfalls hauptsächlich als Audioquelle für Videokonferenzen.
- ▷ Graphiktablett:
  Das Graphiktablett ist ein Touch-Bildschirm, auf den außerdem mit einem Stift geschrieben werden kann. Es ist damit eine interaktives Whiteboard wie das Smartboard, von denen mehrere an der Universität schon im Einsatz sind (`http://www1.ku-eichstaett.de/urz/inkuerze/1_02/hoersaele.html`). Das Graphiktablett befindet sich auf der Arbeitsfläche des Dozententisches und kann an die Leinwand projiziert werden. Im Gegensatz dazu ist das Smartboard zugleich die Leinwand und der Touchscreen.
- ▷ Dokumentenkamera:
  Eine Dokumentenkamera ist vergleichbar mit einem Tageslichtprojektor, jedoch mit den Vorteilen, dass man Papier oder auch dreidimensionale Objekte auflegen kann und somit keine Folien benötigt, dass eine Zoom-Funktion zur Verfügung steht und dass das Bild sowohl über einen der Beamer auf die Leinwand projiziert als auch in eine Videokonferenz geschickt werden kann.

4. Videokonferenzsystem:

- ▷ PC-basierte Videokonferenz:
  Die Dozenten-PCs sind mit einer Videokarte ausgestattet, auf die die beiden Kameras geschaltet werden können;
- ▷ MPEG-2-Codecs:
  Sie liefern hohe Video- und Audioqualität über das Internet. Die gleichen Geräte stehen in den Hörsälen KGI-A-201 in Eichstätt und ASNB-301 in Ingolstadt zur Verfügung und sollen in Zukunft die Übertragung von Vorlesungen über das Internet in hoher Qualität ermöglichen.

5. Didaktik-Netz:

Alle Studenten-Bildschirme sind über ein Didaktiknetz hardware-verschaltet. Damit ist es u. a. möglich, dass der Dozent einen beliebigen Studenten-Bildschirm auf die Leinwand projiziert. So kann ein individuelles Problem vor dem gesamten Auditorium diskutiert werden. Neben Bildschirm, Tastatur und Maus kann sich der Dozent auch des Tons und Mikrofons eines Studentenplatzes bemächtigen und diese z.B. in eine Videokonferenz einspielen.

6. Video-/Audio-Switch:

Alle genannten Geräte sind mit ihren Ein-/Ausgabe-Anschlüssen (Video, Datensignale, Audio) an einen Umschalter (softwaregesteuerte Schaltmatrix) angeschlossen. Dieser macht das manuelle Umstecken von Kabeln überflüssig und

schaltet z.B. eine Kamera auf einen Projektor.

7. Steuerungssystem:

Damit niemand direkt die Schaltmatrix bedienen oder den Ton eines Films direkt am DVD-Player oder Verstärker lauter machen muss, steht ein Touch-Panel (Berührungsbildschirm) zur Verfügung, das auch die Steuerung der Geräte unterstützt. Das Steuergerät der Firma Crestron hat die entsprechenden Schnittstellen (RS232, Infrarot ...) zu den Geräten und steuert so das Umschalten der Schaltmatrix, die Lautstärke des DVD-Players etc. Eine Ebene höher sind über die Steuerung Szenarien definiert, die entsprechende Lehrformen optimal unterstützen.

Zum Beispiel können über einen einzigen Fingerdruck auf „Videokonferenz“

1. sich beide Projektoren einschalten,
2. sich beide Kameras einschalten,
3. das Mikrofon, Lautsprecher, Kamera und Projektor auf den MPEG-Codec umgeleitet werden,
4. die Lautstärke auf eine gewisse Voreinstellung gebracht werden usw.

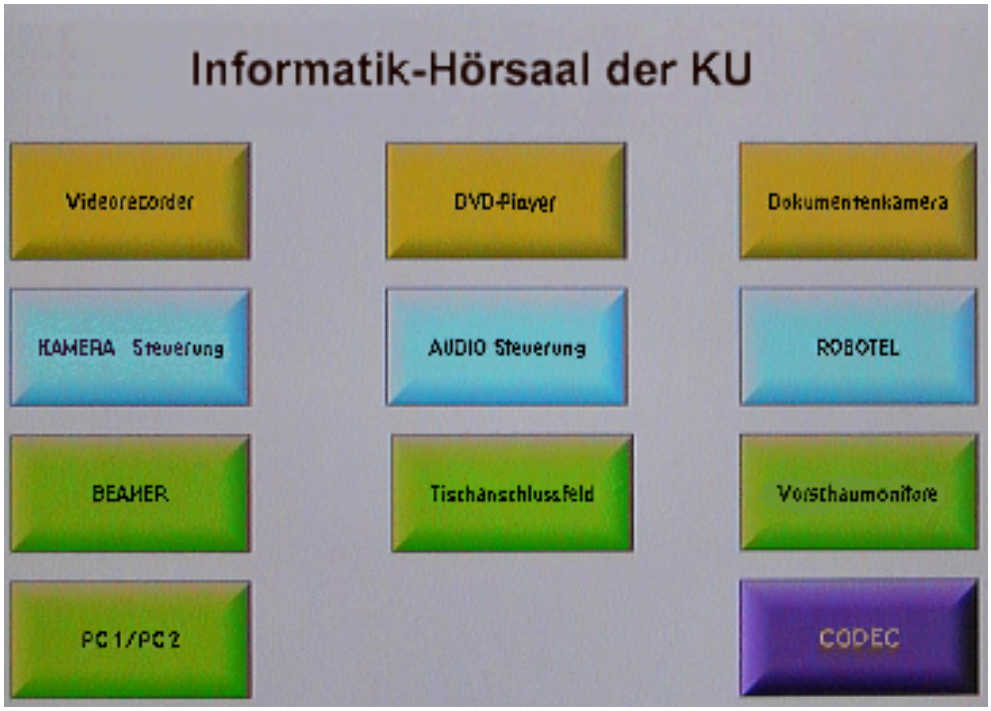


Abb. 3: Steuerungssystem

Ansprechpartner im URZ:	*Zimmer:*	*Telefon:*	*PMail:*
Peter Ihrler	Ei: eO-004	-1585	`peter.ihrler`

Computeralgebra in Neuauflage: Maple 9

Dr. B. Tewes

Wieder einmal ist eine neue Version des Computeralgebra-Systems Maple herausgekommen und bei uns im Netz verfügbar. Und wie es bei Maple üblich ist, gibt man sich nicht lange mit kleinen Versionsnummeränderungen ab, sondern macht gleich ein neues Major Release, d.h. auf die Version 8 folgt nicht vielleicht 8.1, sondern die Version 9.

Was bringt denn diese Version Neues, das diese Veränderung der Versionsnummer rechtfertigt? Nun, wer nach erfolgreicher Installation die Verknüpfung *Maple 9* anklickt, wartet zunächst einmal länger als vorher, bis das Programm geladen ist. Dann erkennt man, dass die Oberfläche „renoviert“ wurde. Das allein wäre etwas wenig und nicht unbedingt ein Fortschritt. Also werfen wir einen Blick darauf, was der Hersteller als Neuerungen anpreist. Hier werden vier Schwerpunkte genannt:

- ▷ **Verbesserte Benutzeroberfläche**
  Diese schon angesprochene Veränderung soll insbesondere Vereinfachungen bei der Formatierung in den Worksheets bringen. Ferner sollen ein verbessertes Hilfesystem und ein grafisch orientierter Debugger die Arbeit mit Maple 9 erleichtern.

- ▷ **Pakete für den Mathematik-Unterricht**
  Schon in Maple 8 gab es mit dem Paket Student[Calculus1] erste Gehversuche, über interaktive Tutoren verschiedene Themengebiete der Analysis zu erläutern. Neben einer Erweiterung dieses Pakets sind hier zwei weitere Pakete dazugekommen, nämlich Student[Precalculus] und Student[LinearAlgebra].

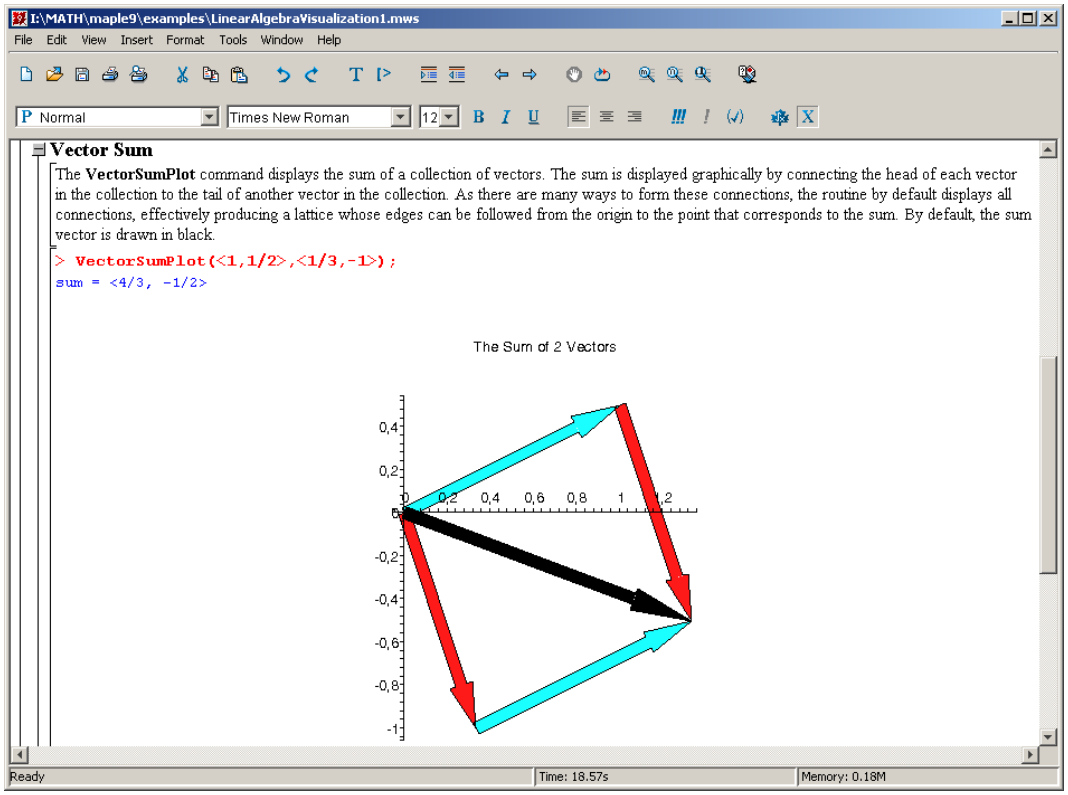


Abb. 1: Neue Benutzeroberfläche mit Visualisierung der Vektoraddition aus dem Paket Student[LinearAlgebra]

- **Zusammenarbeit mit anderen Produkten**
  So kann nun aus Maple-Code neben Java-, Fortran- und C- auch MATLAB- und VisualBasic-Code generiert werden. Durch das OpenMaple API können aus C oder VisualBasic direkt Maple-Routinen gestartet werden und durch eine Zusammenarbeit mit NAG (Numerical Algorithms Group) sind nun einige leistungsfähige numerische Routinen bei Maple 9 dazugekommen.

- **Verbesserungen im Bereich der mathematischen Algorithmen**
  Nicht zuletzt durch die schon angesprochene Zusammenarbeit mit NAG sind neue Routinen dazugekommen oder bereits vorhandene verbessert worden.

Wem die neue (javabasierte) Oberfläche nicht gefällt, wem sie beim Laden zu langsam ist oder eventuell auch zu instabil, der hat über den Link *Classic Worksheet Maple 9* auch weiterhin die Möglichkeit, eine Oberfläche zu starten, die der altbekannten der Vorgängerversion entspricht.

Wie man die neue Maple-Version auf dem eigenen PC bei uns im Netz nutzen kann, ist der aktuellen Installationsanleitung auf den Web-Seiten des Universitätsrechenzentrums zu entnehmen.

Ansprechpartner im URZ:	*Zimmer:*	*Telefon:*	*PMail:*
Dr. Bernward Tewes	Ei: eO-106	-1667	`bernward.tewes`

Der WWW-Browser als Präsentationswerkzeug

P. Ihrler

Vielleicht haben Sie sich auch schon einmal Gedanken darüber gemacht, warum Forschungsergebnisse, Vorlesungsunterlagen oder andere wissenschaftliche Dokumente einmal mit PowerPoint, einmal als PDF-Dateien mit dem Adrobat Reader und ein andermal über HTML mit WWW-Browsern präsentiert werden. In einem anderen Vortrag werden Dias gezeigt oder ein Film mit einem VHS-Recorder oder DVD-Player auf die Projektionswand geworfen. Braucht man all diese Medien wirklich oder nur um auch im Multimedia-Trend mitzuschwimmen? Mit dem WWW-Browser Opera soll anhand von Beispielen gezeigt werden, dass man sehr wohl sein Wissen in einem einzigen Dokument so aufbereiten kann, dass es gleichzeitig WWW-, präsentations-, druck-, datenbankabfrage- und audiovisuell-tauglich ist.

Die heutigen Web-Technologien (HTML, CSS, XML, JavaScript, CGI, PERL, PHP) bieten ziemlich alles, um Texte, Animationen, Video, Audio, Datenbankzugang usw. zu integrieren. Was spricht also dagegen, diese Technologien auch zur Präsentation im Hörsaal zu verwenden?

Außerdem basieren diese Technologien auf Standards und freier Software, so dass man herstellerunabhängig und kostengünstig operieren kann. Also, warum denn in die Ferne schweifen ... Sie werden sich jetzt fragen, warum dann hier auf Opera und nicht auf Browser wie Internet Explorer, Mozilla oder Netscape gesetzt wird. Der Grund liegt darin, dass sich Opera am besten des CSS-Standards (Cascading Style Sheets) annimmt. CSS ist eine Erweiterung von HTML. Es definiert Formateigenschaften einzelner HTML-Elemente und erleichtert somit eine einheitliche und angepasste Gestaltung für die Präsentation am Bildschirm, an der Leinwand, auf dem Papier, der behindertengerechten Computerperipherie, dem Handheld-Computer oder dem WAP-Handy – und das ohne das Dokument, das die Wisseninhalte enthält, anpassen zu müssen.

HTML und CSS als Präsentationswerkzeug

Anhand einer einfachen Kurzpräsentation mit drei Folien soll nun gezeigt werden, wie das gehen kann. In Abbildung 1 sieht man eine einfache HTML-Seite, die im „Web-Stil“ die Vor- und Nachteile einer – nicht ganz zufällig unserer – Thematik beschreibt. Diese Seite sieht immer gleich aus, egal ob Sie Opera, den Internet Explorer oder irgend einen anderen Browser verwenden.

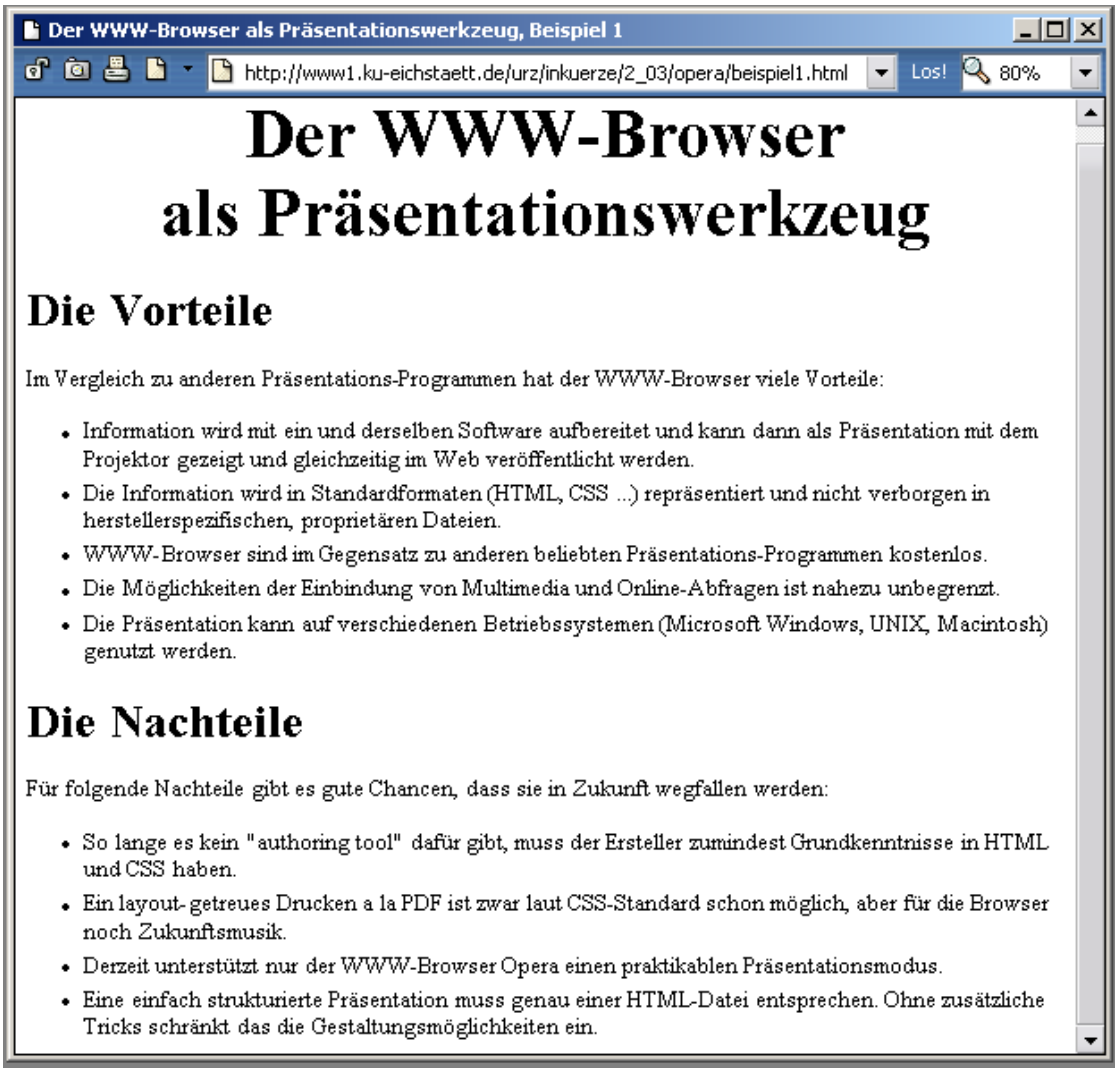


Abb.1: Eine normale Web-Seite

Wenn Sie jedoch bei Opera auf den Vollbildmodus (z. B. mit der Funktionstaste „F11“) umschalten, sehen Sie auf einer Bildschirmseite zunächst die Überschrift, dann die Vorteile (vgl. Abb. 2) und schließlich die Nachteile. Um von „Folie“ zu „Folie“ zu kommen, drücken Sie einfach die Leertaste oder die Bild-nach-unten-Taste, den Rückwärtsgang legen Sie mit der Bild-nach-oben-Taste ein. Die Buchstaben im Vollbildmodus, auch Projektionsmodus genannt, sind meist bunter und größer gestaltet, so auch in unserem Beispiel. Mit der Esc-Taste beendet man die Präsentation. Wenn Sie Opera schon installiert haben, können Sie sich dieses Beispiel live ansehen unter `http://www1.ku-eichstaett.de/urz/inkuerze/2_03/opera/beispiel1.html`. Opera gibt es kostenlos unter `http://www.opera.com` oder auf unserem Novell-Server im Verzeichnis `I:\archiv\opera`.

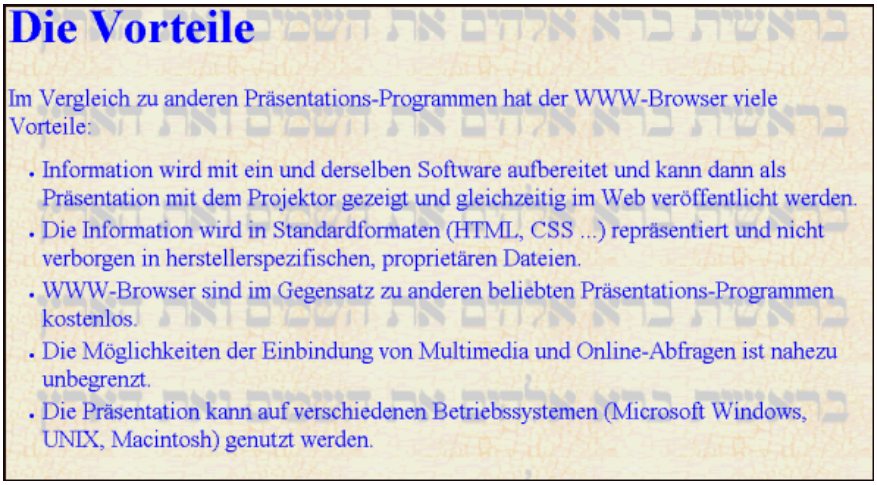


Abb. 2: „Folie 2“ im Vollbildmodus

Die CSS-Definition in Abb. 3 beschreibt die Formatierung des Textes für die normale Anzeige. Hier heißt es nur, dass der Text schwarz sein soll. Abb. 4 beschreibt die Formatierung für den Projektionsmodus: hier ist die Farbe des Textes blau, es gibt ein Hintergrundbild und die Buchstaben sind um 180% größer als normal. Der Trick ist aber das CSS-Statement `page-break-before:`, das heißt, dass bei jedem `<h1>`-Tag (Formatierungsbefehl für große Überschriften) auf die nächste Seite geblättert wird, also die nächste Folie gezeigt wird. Den Auslöser dazu gibt der Tastendruck auf die Leertaste oder die Bild-nach-unten-Taste.

```
/* Datei bildschirm1.css */

body {
 color: black;       /* Farbe des Textes */
}
```

Abb. 3: Formatangabe für normale Web-Darstellung

```
/* Datei projektion1.css  */

body {
 background: url("heb.gif");    /* Hintergrundbild */
 color: blue;                   /* Farbe des Textes */
 font-size: 180%;               /* Die Buchstaben sollen um x Prozent
                                   größer sein */
}

h1 {
page-break-before: always;      /* immer wenn der Tag <h1> (d. h. große
                                   Überschrift) kommt, wird nach dem Drücken
                                   der Leertaste oder der "Bild nach unten"-
                                   Taste die nächste "Folie" angezeigt */
}
```

Abb. 4: Formatangabe für den Präsentationsmodus

Im HTML-Code (Abb. 5) wird dann auf die beiden CSS-Dateien verwiesen. Im „normalen“ Modus gilt also `media="screen"` mit der CSS-Definition von `bildschirm1.css` während im Vollbildmodus oder Projektionsmodus `media="projection"` mit `projektion1.css` gilt.

```
<html>
  <head>
    <title>Der WWW-Browser als Präsentationswerkzeug, Beispiel 1</title>
    <link rel="stylesheet" type="text/css"
       href="bildschirm1.css"
       media="screen" />
    <link rel="stylesheet" type="text/css"
       href="projektion1.css"
       media="projection" />
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  </head>
<body>


<center style="font-size:xx-large; font-weight:bold;">
Der WWW-Browser <br> als Präsentationswerkzeug</center>

<h1>Die Vorteile</h1>
Im Vergleich zu anderen Präsentations-Programmen hat der WWW-Browser viele
Vorteile:<ul><li>
Information wird mit ein und derselben Software aufbereitet und kann dann als
Präsentation mit dem Projektor gezeigt und gleichzeitig im Web veröffentlicht
werden.</li><li>
Die Information wird in Standardformaten (HTML, CSS ...) repräsentiert und
nicht verborgen in herstellerspezifischen, proprietären Dateien.</li><li>
WWW-Browser sind im Gegensatz zu anderen beliebten Präsentations-Programmen
kostenlos.</li><li>
Die Möglichkeiten der Einbindung von Multimedia und Online-Abfragen ist nahezu
unbegrenzt.</li><li>
Die Präsentation kann auf verschiedenen Betriebssystemen (Microsoft Windows,
UNIX, Macintosh) genutzt werden.
</li></ul>

<h1>Die Nachteile</h1>
Für folgende Nachteile gibt es gute Chancen, dass sie in Zukunft wegfallen
werden:<ul><li>
So lange es kein "authoring tool" dafür gibt, muss der Ersteller zumindest
Grundkenntnisse in HTML und CSS haben.</li><li>
Ein layout-getreues Drucken a la PDF ist zwar laut CSS-Standard schon möglich,
aber für die Browser noch Zukunftsmusik.</li><li>
Derzeit unterstützt nur der WWW-Browser Opera einen praktikablen
Präsentationsmodus. </li><li>
Eine einfach strukturierte Präsentation muss genau einer HTML-Datei entsprechen.
Ohne zusätzliche Tricks schränkt das die Gestaltungsmöglichkeiten ein.</li></ul>

</body>
</html>
```

Abb. 5: HTML-Code mit dem Aufruf von zwei medien-spezifischen CSS-Dateien

Die Einbindung von Multimedia-Elementen

In der INKUERZE 1/2000 (`http://www1.ku-eichstaett.de/urz/inkuerze/1_00/video.htm`) wurde bereits beschrieben, wie man Filme und Ton in HTML-Seiten einbetten kann. Interessant für Präsentationen ist vor allem, dass der Film innerhalb einer HTML-Seite abgepielt werden kann, ohne dass ein eigenes, häufig störend wirkendes Fenster für den Player erscheint. So läuft im nachstehenden Beispiel durch einen Mausklick auf das Foto mit dem Jungen am Bildschirm ein Film ab und zwar genau an der Stelle, an der jetzt das Foto ist.

Abb. 6: Bei Klick auf das Foto läuft genau an der Stelle ein Film ab

Abb. 7 zeigt den relativ einfachen Code. `Starter.mov` ist das Foto und `TastaturFilm.mp4` ein Film im MPEG-4-Format. Leider wird das Abspielen von Filmen innerhalb des Browserfensters nicht von allen Browserherstellern in einheitlicher Form unterstützt. Für Präsentationen ist das kein Problem, weil man da ja ohnehin Opera benützt. Problematisch kann es werden, wenn die Seiten über das Internet beliebigen Browserbenutzern zugänglich gemacht werden sollen.

```
<embed width="380" src="Starter.mov" height="280" href="TastaturFilm.mp4"
border="0" target="myself"></embed>
```

Abb. 7: Code zur Film-Einbindung

Das leidige Ausdrucken von HTML-Seiten

HTML-Seiten kommen häufig nicht so aus dem Drucker wie man es erwartet. Mal enden Zeilen am Papierrand oder es sind Seiten halb leer, weil als nächstes ein Foto kommt, das nicht mehr auf die Seite passte etc. PDF-Dateien sind nicht unbedingt die Alternative, da sie wieder eigens erstellt werden müssen.

Mit CSS können Seitenränder, Papierformat, Seitenvorschub etc. in einer `MeinDruckformat.css`-Datei ähnlich wie in Abb. 1 und Abb. 2 gezeigt definiert werden.

Die Verknüpfung erfolgt dann in der HTML-Datei mit `media="print"`.

Leider werden einige dieser Druckbefehle noch nicht von allen Browsern unterstützt. Die Befehle finden Sie unter `http://www1.ku-eichstaett.de/urz/selfhtml/css/eigenschaften/printlayouts.htm`.

Dynamisches Programmieren, Interaktion und die Präsentation von aktuellsten Daten durch Datenbankabfragen

Beim Web-basierten Präsentieren erübrigt sich das Umschalten zwischen einem Präsentationsgrafik-Programm und dem Browser, um aktuelle Daten aus einer Webseite anzeigen zu können. Aktuelle Informationen können durch eine online-Datenbankabfrage zum Zeitpunkt der Präsentation automatisch am Bildschirm angezeigt werden. Es können auch interaktive Elemente in die Präsentation eingebaut werden wie z. B. das Ausfüllen eines Fragebogens und dessen unmittelbare Auswertung, das Errechnen von Werten aufgrund der Eingabe von Parametern etc. Solche Anwendungen können z. B. mit PHP, Perl oder Java programmiert werden.

Das Authoring-Tool

Jetzt fehlt eigentlich nur noch, die Software vorzustellen, die mit einer einfachen, „plug&work"-Technologie, a la PowerPoint oder Dreamweaver diese Dokumente erstellt. Ideal wäre ein Werkzeug, das das Wissen gleich in XML repräsentiert und von dort eine Präsentation generiert. Die Entwicklung einer solchen Software ist denkbar einfach, zumindest um die Grundfunktionen abzudecken. Leider steht aber ein solches Werkzeug noch aus – eine Marktlücke. Ansonsten bleibt nur – der aufmerksame Leser hat es bereits bemerkt – sich mit HTML und CSS zu beschäftigen.

Beispiele zum Experimentieren und Lernen

Oben beschriebenes Beispiel:
`http://www1.ku-eichstaett.de/urz/inkuerze/2_03/opera/beispiel1.html`

Das obige Beispiel etwas verschönert:
`http://www1.ku-eichstaett.de/urz/inkuerze/2_03/opera/beispiel2.html`

Beispiel aus der Zeitschrift iX 5/2003, S. 136:
`http://www1.ku-eichstaett.de/urz/inkuerze/2_03/opera/ix-beispiel.html`

Quellen und weiterführende Literatur

Opera als Präsentationstool:
`http://www.opera.com/support/tutorials/operashow/`

Zeitschrift iX 5/2003, S. 136: Webdesign:
`http://www.heise.de/ix/artikel/2003/05/136`

selfhtml gutes Nachschlagewerk für HTML und CSS:
`http://selfhtml.teamone.de`

Ansprechpartner im URZ:	*Zimmer:*	*Telefon:*	*PMail:*
Dr. Bernward Tewes	EI: eO-106	-1667	`bernward.tewes`
Peter Ihrler	EI: eO-004	-1585	`peter.ihrler`

TEX-Info

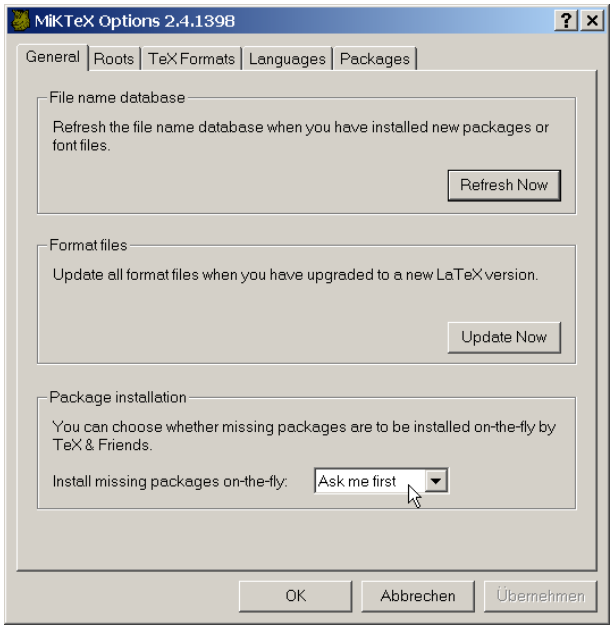
P. Zimmermann

Wer wünscht sich nicht eine an seine Bedürfnisse optimal angepasste Software auf seinem Rechner? MiKTeX kommt diesem Wunsch in der neuen Version 2.4 schon ziemlich nahe: ausgehend von einer «kleinen» TEX-Basis installiert das MiKTeX-System bei Bedarf fehlende Komponenten nach.

Die Hinweise unter «Tipps und Tricks» beziehen sich auf ein rasches Hin- und Herwechseln zwischen Quelltext und dvi-Dokument. Sie sollen helfen, die tägliche Arbeit zu erleichtern.

MiKTeX Version 2.4 mit automatischer Paketinstallation

Die neue MiKTeX Version 2.4 verfügt über einen eingebauten Automatismus zur Nachinstallation von in einer Arbeit angeforderten Paketen. Stellt MiKTeX fest, dass ein zu ladendes Paket noch nicht vorhanden ist, so wird dieses automatisch von einem lokalen Speicherplatz oder aus dem Internet geholt und ins System eingefügt. Damit steht einem sehr schlanken TEX-System, das nur die tatsächlich verwendeten Komponenten enthält, nichts mehr im Wege: man startet mit einem minimalen MiKTeX-System, das nach und nach die gewünschten Pakete nachschiebt. Wählen Sie dazu über MiKTeX Options (*Start* → *Programme* → *MiKTeX* → *MiKTeX Options*) im Feld «Package Installation» ein `Yes` oder `Ask me first` hinter der Frage «Install missing packages on-the-fly:».

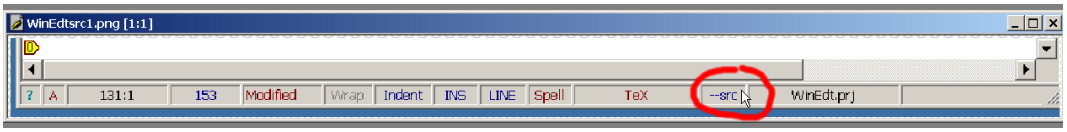


Falls Sie noch kein MiKTeX-System auf Ihrem Rechner haben, rufen Sie das Einrichteprogramm mit `i:\Archiv\TeX\MiKTeX\setup.exe` auf und folgen der Installationsanleitung (WWW-Seiten der KU oder Laufwerk I:). Bei einem vorhandenen MiKTeX-System stoßen Sie die Installation über *Start* → *Programme* → *MiKTeX* → *MiKTeX Update Wizard* an. Das Update erfolgt in zwei Schritten: zuerst werden zentrale MiKTeX-Programme ersetzt (in der Update List ist nur das Paket `miktex-bin` ausgewählt); nach einem erneuten Update-Aufruf folgen die restlichen Komponenten nach. Sie finden die jeweils aktuelle MiKTeX-Version auf dem Netz der KU im Verzeichnis `i:\Archiv\TeX\MiKTeX`.

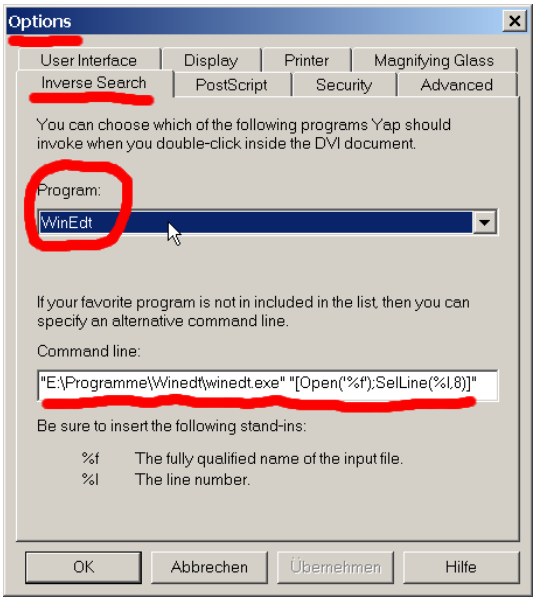
Mit der Version 2.4 liegt dem TeX-System das erweiterte e-TEX zugrunde. Damit entspricht CHRISTIAN SCHENK, der MiKTeX-Schöpfer und Betreuer, den Wünschen des LATEX-Entwicklerteams, das insbesondere die zusätzlichen Möglichkeiten von e-TEX für LATEX3 nutzen möchte.

Tipps und Tricks zum praktischen Arbeiten

Wird eine `dvi`-Datei mit speziellen Informationen über die Quelldateien versorgt, so kann durch Doppelklick von der Bildschirmausgabe (YAP) zur entsprechenden Stelle in der Quelldatei gesprungen werden. Das Einbringen von Hinweisen auf die Quelldatei in die `dvi`-Datei geschieht während der TEX-Bearbeitung mittels der TEX-Programmoption `-src`, die im WinEdt durch Klick im dritten Feld der Statuszeile von rechts an- und abgeschaltet werden kann.



Die Informationen über die Quelldatei vergrößern die `dvi`-Datei um bis zu 20 Prozent, was in der Erarbeitungsphase unproblematisch sein sollte. Im YAP ist unter *View* → *Options* → *Inverse Search* als *Program:* `WinEdt` einzutragen. Die *Command line:* sollte automatisch den korrekten Text `"C:\Programme\Winedt\winedt.exe" "[Open('%f');SelLine(%l,8)]"` enthalten.



Sprung von der Quelle in die `dvi`*-Datei:*

Von einer bestimmten Position in der Quelldatei zur entsprechenden Stelle in der `dvi`-Datei gelangt man über einen Klick auf das `DVI Search`-Symbol bzw. mittels der Tastenkombination `Shift-Strg-S`.

Ansprechpartner im URZ:	*Zimmer:*	*Telefon:*	*PMail:*
Peter Zimmermann	EI: eO-106	-13 51	`peter.zimmermann`

IN aller KUERZE

Multimedia-Labor in neuen Räumen
Das Multimedia-Labor des Universitätsrechenzentrums ist seit Sommer im Raum KGI-A-301 untergebracht. Ansprechpartner ist Peter Ihrler. Weitere Informationen insbesondere auch zur Ausstattung finden Sie unter `http://www.ku-eichstaett.de/Rechenzentrum/ausstattung/mm_labor/`

Multimedia-Hörsaal KGI-A-302
Durch den Umzug des Lehrstuhls für Angewandte Informatik in das neue Gebäude in der Ostenstraße 14 ist der Multimedia-Hörsaal KGI-A-302 in den Verantwortungsbereich des Universitätsrechenzentrums übergegangen. Der Hörsaal stellt 2 Projektoren mit vielen Anschlussmöglichkeiten, 2 Dozenten-PCs und 12 ThinClients für Studenten zur Verfügung. Weitere Informationen zur Bedienung finden Sie unter `http://www.ku-eichstaett.de/Rechenzentrum/ausstattung/mm_ausstattung/`.

Dokumentenkamera
Ab sofort kann eine Dokumentenkamera VZ-5F in der Medienzentrale (Herr Pfaller, Herr Koderer, Raum KGI-A-010) ausgeliehen werden. Eine Dokumentenkamera funktioniert ähnlich wie ein Tageslichtprojektor, jedoch braucht man keine Folien, sondern man kann direkt Papier und auch dreidimensionale Gegenstände auflegen. Um das Bild an die Wand zu bringen, benötigt man zusätzlich einen Datenprojektor, wie er inzwischen in zahlreichen Hörsälen und Seminarräumen zur Verfügung steht. Weitere Informationen zur Bedienung finden Sie unter `http://www.ku-eichstaett.de/Rechenzentrum/ausstattung/mm_ausstattung/`.

Neuer Datenbank-Server für die Verwaltung
Seit August ist der neue Datenbank-Server für die Universitätsverwaltung, eine Sun Fire 280R, in Produktion. Der Server ist an das Storage Area Network (SAN) des Universitätsrechenzentrums mit einem redundant ausgelegten Festplatten-Speicherbereich angeschlossen. Die Inbetriebnahme verzögerte sich wegen Fehlern in der Informix-Datenbanksoftware der Firma IBM erheblich. Der alte Datenbank-Server dient in Zukunft als Test- und Backup-Server.

Kopieren von VHS-Kasetten auf DVDs
Mit dem DVD-Recorder Panasonic DMR-E 100 HEGS können VHS-Filme auf DVD gebrannt und damit „digitalisiert“ werden. Es werden 1:1 Kopien gemacht, das heißt eine VHS-Kasette wird auf eine DVD (Format DVD-R) gebrannt. Hilfreich ist es, wenn Sie die Dauer des Films mit angeben. Die DVDs können dann auf den meisten PCs mit DVD-Laufwerk und einer DVD-Player-Software (Cyberlink PowerDVD, Intervideo WinDVD) oder DVD-Playern abgespielt werden. Setzen Sie sich bei Bedarf bitte mit Herrn Koderer oder Herrn Pfaller in der Medienzentrale in Verbindung. Für das Digitalisieren von Videosequenzen zum Einbinden in Webseiten oder anderen Bildschirmpräsentationen nehmen Sie bitte mit Herrn Ihrler vom Universitätsrechenzentrum Kontakt auf.

Pool-Auslastung im Web
Seit dem vergangenen Sommersemester bietet das Universitätsrechenzentrum auf seinen Web-Seiten `http://www.ku-eichstaett.de/Rechenzentrum/allgemein/poolauslastung` aktuelle Informationen über die Auslastung seiner PC-Pools an. Dabei wird jeweils für die PC-Pools in Eichstätt oder in Ingolstadt bei jedem Aufruf der entsprechenden Seite und anschließend im Minutentakt die derzeitige Auslastung der PC-Pools neu ermittelt und aktualisiert dargestellt. Auf diese Weise können Sie sich einen Überblick darüber verschaffen (lassen), in welchem der PC-Pools Sie derzeit noch einen freien Arbeitsplatz vorfinden.

Neuer DFN-Dienst DFNNetNews
Mit dem neuen DFN-Dienst DFNNetNews bietet das Universitätsrechenzentrum seinen Nutzern die Möglichkeit, über einen zentralen, professionell betreuten News-Server auf Tausende so genannter Newsgruppen zuzugreifen, in denen das Expertenwissen eines internationalen Teilnehmerkreises durch Lesen der entsprechenden Beiträge abgerufen bzw. durch Schreiben eigener Postings angefragt werden kann.

Um diesen Dienst nutzen zu können, muss Ihr Rechner entweder in das Festnetz oder Funk-LAN unserer Universität integriert sein oder über einen der Zugangsdienste `DFN@home` oder `uni@home` in das Hochschulnetz eingewählt sein. Da die üblichen Web-Browser wie NETSCAPE 7.x mit der Komponente *eMail & Diskussionsforen* oder INTERNET EXPLORER unter der Rubrik *Extras → Mail und News* bereits über entsprechende News-Reader verfügen, ist keine weitere spezielle Software erforderlich; lediglich der Name des News-Servers `news.cis.dfn.de` ist dazu bei der Konfigurierung einzutragen.

Neue E-MailAdresse „urz-beschaffungen“

Damit Anfragen und Anträge an das Universitätsrechenzentrum zu DV-Beschaffungen auch bei Urlaub oder sonstiger Abwesenheit eines der Sachbearbeiter zeitnah bearbeitet werden können, richten Sie bitte derartige E-Mails an die neue Adresse `urz-beschaffungen@ku-eichstaett.de`.

PC-Pools eO-112 und ASHB-111 erneuert

Rechtzeitig zum laufenden Wintersemester konnte die veraltete Ausstattung in den PC-Pools eO-112 in Eichstätt und ASHB-111 in Ingolstadt erneuert werden: 10 PCs (Pentium IV, 2.4 GHz) bzw. 15 PCs (Pentium IV, 2.6 GHz) mit modernen TFT-Monitoren, die wahlweise unter Windows2000 und künftig auch unter Linux betrieben werden können, bieten nun wieder die erforderliche Rechenpower und Leistungsfähigkeit zur Nutzung des breiten Software-Spektrums, welches das Universitätsrechenzentrum in seinen PC-Pools auf insgesamt 150 PCs bereitstellt. Die ebenfalls noch für 2003 geplante Ersatzbeschaffung für die 18 PCs (Pentium II, 350 MHz) des Pools ASHB-U03 wurde leider durch die inzwischen verfügte Haushaltssperre vereitelt; wir hoffen nun, dass eine Realisierung zum Sommersemester 2004 möglich ist.

Neue Programmversion von Corel Office

Beim Versionswechsel von 9 auf 10 der Bürokommunikationssoftware Corel Office ging ein Aufschrei durch die deutsche Landschaft, wurden doch ab sofort die Programmoberfläche, die Menüs etc. nur noch in englisch angeboten. Die daraufhin einsetzenden massiven Proteste haben den Konzern überraschenderweise recht schnell zu einer Revidierung dieser Entscheidung bewogen und die Version 11 auch wieder mit deutscher Oberfläche versehen. Insbesondere WordPerfect-Anwender können aufatmen und das campusweit zur Verfügung stehende Programm in gewohnter Weise benutzen.

Dies gilt auch für die jüngsten Versionen der Corel Graphics Suite (11) mit Corel Draw, Photo-Paint und RAVE und des publishing programs Ventura (10).

Die Installationsdateien (setup) finden Sie auf `i:\corel\wpoffice11` bzw. `i:\graphik\coreldraw11`, die Anleitungen dazu auf der Web-Seite des Universitätsrechenzentrums unter *Dienstleistungen → Installationsanleitungen*. Zu dienstlichen Zwecken können die Programme auch auf dem privaten PC/Laptop/Notebook installiert werden. Leihen Sie sich dafür die entsprechenden Installations-CDs im Universitätsrechenzentrum aus.

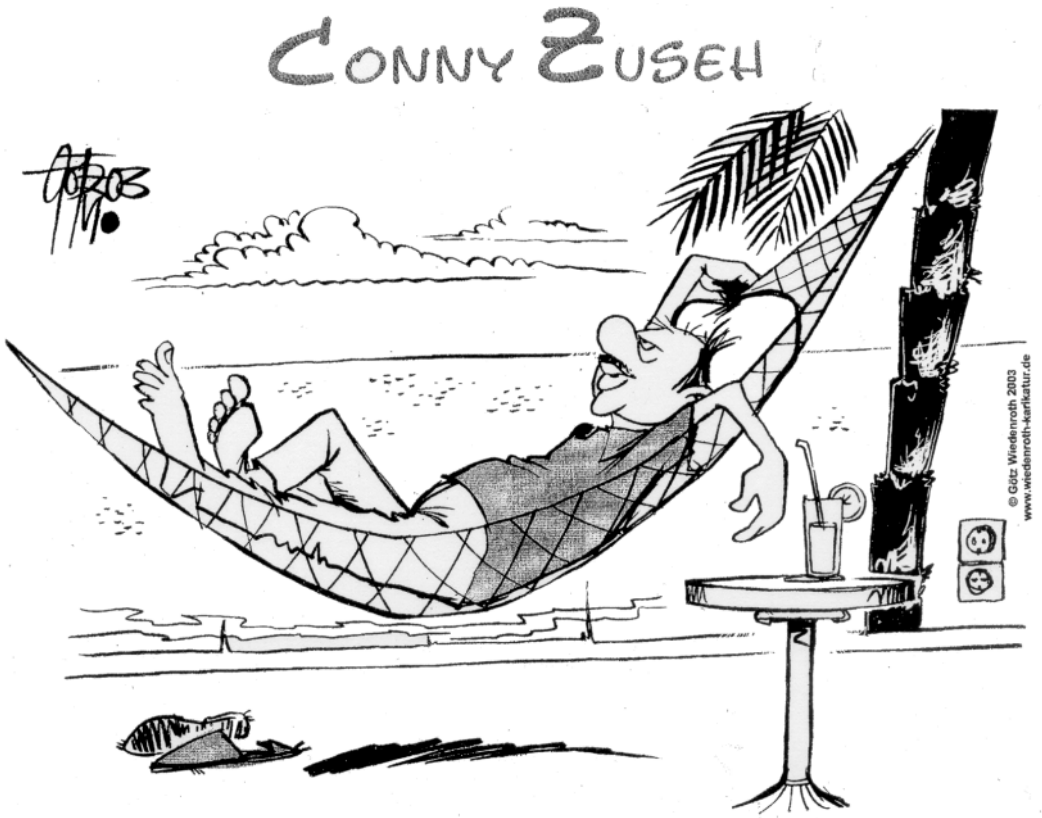
Hausdruckerei online

Künftig ist auch die Hausdruckerei in der Zentralverwaltung unserer Universität online erreichbar: Zum einen können über das auf den Web-Seiten der KU unter `http://www.ku-eichstaett.de/Ueberblick/Verwaltung/ZUV/formulare_zuv/` angebotene Formular Druckaufträge online ausgefüllt und an die Hausdruckerei abgesandt werden, zum anderen müssen die Druckvorlagen nicht mehr unbedingt in Papierform eingereicht werden, sondern können alternativ auch als PDF-Datei auf dem NetWare-Server `eo-nw-1` in Eichstätt in dem zur jeweiligen Fakultät oder Einrichtung gehörenden Unterverzeichnis von `J:\ORG\Druckerei\` bereitgestellt oder auf CD an die Druckerei geliefert werden.

Weiterer Ausbau des FunkLANs

Zum 10. November 2003 hat das Universitätsrechenzentrum das FunkLAN der Universität, das bisher auf den Lesesaal der Zentralbibliothek und das Foyer des Gebäudes „Universitätsallee“ beschränkt war, um zwei Bereiche erweitert: Sowohl im Aufenthaltsbereich des Gebäudes „Ehemaliges Waisenhaus“ als auch bei den Magazin-Arbeitsplätzen in der Teilbibliothek II „Aula/Ehemalige Reitschule“ wurden insgesamt vier FunkLAN-Zugangsstationen installiert, über die sich mit einer FunkLAN-Karte entsprechend ausgestattete Notebooks in

das FunkLAN der Kath. Universität Eichstätt-Ingolstadt (KU) einwählen können.
Diese neuen FunkLAN-Zugangsstationen arbeiten dabei sowohl nach dem bisherigen Standard IEEE 802.11b mit einer Übertragungsrate von nominell 11 Mbit/s als auch nach dem neuen Standard IEEE 802.11a mit einer Übertragungsrate von nominell 54 Mbit/s. Damit lassen sich die bisher schon in der Zentralbibliothek ausleihbaren ebenso wie die im Universitätsrechenzentrum zu kaufenden FunkLAN-Karten in allen Funknetz-Bereichen der KU weiterverwenden. Zusätzlich werden in der Teilbibliothek II und künftig in der Wirtschaftswissenschaftlichen Zweigbibliothek in Ingolstadt FunkLAN-Karten neuen Typs zur Ausleihe angeboten, die mit beiden Übertragungsnormen arbeiten können.
Wenn Ihr Notebook bereits über einen eingebauten FunkLAN-Adapter verfügt, können Sie diesen gegebenenfalls nutzen, wenn er die festgelegten Sicherheitsoptionen für die Datenübertragung im Funknetz erfüllt und mit seiner Netzadresse zuvor im Sekretariat des Universitätsrechenzentrums registriert wird. Dort erhalten Sie auch ein Merkblatt „Kommunikationsparameter für das FunkLAN der KU“, welches die für die Konfiguration des FunkLAN-Adapters notwendigen Parameter enthält.
Auch der weitere Ausbau des Funknetzes der KU steht unmittelbar bevor: In den nächsten Wochen werden an der Wirtschaftswissenschaftlichen Fakultät in Ingolstadt insgesamt zehn FunkLAN-Zugangsstationen installiert und in Betrieb genommen, mit denen der Aufenthaltsbereich im Untergeschoss des Altbaus, der Lesesaal der Wirtschaftswissenschaftlichen Zweigbibliothek sowie die Foyers in beiden Fakultätsgebäuden abgedeckt werden.



"Das ist das einzige Netzwerk, das mich im Moment interessiert!"

Beratungsthemen und ihre Ansprechpartner

Zu vielen Themenbereichen bietet das Universitätsrechenzentrum Beratungsleistungen an. Nachfolgender alphabetischer Auflistung können Sie die jeweiligen Ansprechpartner entnehmen. Informationen zur Kontaktaufnahme sind auf der Mitarbeiter-Seite im Web-Angebot des Universitätsrechenzentrums zu finden; bei akuten Problemen wenden sich Eichstätter Nutzer jedoch zweckmäßigerweise zunächst an die URZ-Hotline, die montags – freitags, 8.00–12.00 Uhr, und montags – donnerstags, 13.00–16.00 Uhr, unter der Nummer -1010 zu erreichen ist.

Access
EI:/IN: B. Woitas

Antiviren-Programme
EI: H. Zimmermann, Ch. Schneider
IN: A. Kaltenbacher, B. Brandel

Benutzerkennungen – Beantragung
EI: J. Reile, H. Schermer
IN: Th. Stalker

Benutzerkennungen – Problembearbeitung Novell NetWare
EI: H. Zimmermann, P. Zimmermann, L. Hüttinger
IN: H. Sendlbeck, A. Kaltenbacher

Bibliotheks-DV
EI:/IN: P. Kahoun, W. König

C/C++
EI: P. Zimmermann, B. Woitas
IN: B. Brandel, A. Kaltenbacher

CD-Brenner
EI: L. Hüttinger, Ch. Schneider
IN: A. Kaltenbacher, H. Sendlbeck

CD-ROM-Server
EI:/IN: W. König

Corel Draw
EI: K. Keil, N. Kropf
IN: A. Kaltenbacher

Corel WP Office
EI: K. Keil, N. Kropf
IN: A. Kaltenbacher

Datenbanksysteme
EI: B. Woitas, P. Zimmermann
IN: A. Kaltenbacher

Disketten/ CD-Rohlinge/ DV-Verbrauchsmaterial
EI: J. Reile, H. Schermer
IN: Th. Stalker

Dokumentationen
EI: J. Reile, H. Schermer
IN: Th. Stalker

Druck-Kontingente
EI: J. Reile, H. Schermer
IN: Th. Stalker

DV-Ausbildung, Kurse
EI: Dr. W. A. Slaby, P. Zimmermann, Dr. B. Tewes
IN: B. Brandel

Einwähl-Service des URZ
EI:/IN: P. Kahoun, T. Partyka

Electronic Mail
EI: T. Partyka, P. Kahoun
IN: A. Kaltenbacher, B. Brandel

Excel
EI: B. Woitas
IN: A. Kaltenbacher

Externe Datenbanken
EI: Dr. W. A. Slaby, P. Zimmermann
IN: B. Brandel, A. Kaltenbacher

Fax-Server
EI: K. Keil, N. Kropf, P. Zimmermann
IN: A. Kaltenbacher

FTP
EI: T. Partyka, P. Kahoun, Dr. W. A. Slaby
IN: A. Kaltenbacher, B. Brandel

FunkLAN
Ei: P. Kahoun, T. Partyka
In: H. Sendlbeck, A. Kaltenbacher

Graphik-Systeme
Ei: K. Keil, Dr. B. Tewes
In: A. Kaltenbacher

Hardware-Installation
Ei: L. Hüttinger, Ch. Schneider
In: H. Sendlbeck

Hardware-Probleme
Ei: L. Hüttinger, Ch. Schneider
In: H. Sendlbeck

Hardware-/Software-Beschaffung
Ei: Dr. W. A. Slaby, H. Zimmermann, Ch. Schneider
In: Dr. W. A. Slaby, B. Brandel

HTML
Ei: Dr. B. Tewes
In: B. Brandel

IMAP4-Mailserver
Ei:/In: T. Partyka

Informix
Ei:/In: P. Ihrler, B. Woitas

Internet-Dienste
Ei: T. Partyka, P. Kahoun
In: B. Brandel, A. Kaltenbacher

Internet Explorer (WWW-Client)
Ei: Dr. B. Tewes
In: B. Brandel

IT-Sicherheit
Ei:/In: B. Brandel, Dr. W. A. Slaby

Java
Ei: P. Zimmermann
In: A. Kaltenbacher

Kermit
Ei:/In: T. Partyka, Dr. W. A. Slaby

LDAP (Directory-Dienst)
Ei: P. Zimmermann
In: A. Kaltenbacher

Maple/Mathematica
Ei: Dr. B. Tewes
In: B. Brandel

Mercator
Ei:/In: Dr. B. Tewes

Micrografx
Ei: K. Keil, N. Kropf
In: A. Kaltenbacher

MS Office
Ei: B. Woitas
In: A. Kaltenbacher, H. Sendlbeck

Multimedia
Ei: P. Ihrler
In: B. Brandel

Netscape (WWW-Client)
Ei: Dr. B. Tewes
In: B. Brandel

Netz
Ei: L. Hüttinger (HW), P. Kahoun (SW)
In: H. Sendlbeck (HW), A. Kaltenbacher (SW)

Novell NetWare
Ei: P. Zimmermann, H. Zimmermann, P. Kahoun
In: H. Sendlbeck, A. Kaltenbacher

OPAC
Ei:/In: P. Kahoun, W. König, Dr. W. A. Slaby

Open Office
Ei: K. Keil, Dr. B. Tewes
In: A. Kaltenbacher, H. Sendlbeck

Opera (WWW-Client)
Ei: Dr. B. Tewes
In: B. Brandel

Oracle
Ei: B. Woitas, P. Zimmermann, Dr. W. A. Slaby
In: A. Kaltenbacher

Pascal
Ei: P. Zimmermann, K. Keil, Dr. B. Tewes
In: A. Kaltenbacher

Pegasus Mail
EI: T. Partyka
IN: A. Kaltenbacher

PGP (Pretty Good Privacy)
EI: T. Partyka, Dr. W. A. Slaby
IN: B. Brandel, A. Kaltenbacher

Poolreservierung für DV-Veranstaltungen
EI: H. Schermer, J. Reile
IN: Th. Stalker

PostScript
EI: K. Keil
IN: A. Kaltenbacher

PowerPoint
EI: B. Woitas
IN: A. Kaltenbacher

Probleme beim Arbeiten im Pool
EI:/IN: studentische Aufsichtskräfte

Programmierung, allgemeine Fragen
EI: P. Zimmermann, K. Keil, B. Woitas
IN: B. Brandel, A. Kaltenbacher

SAS
EI: Dr. B. Tewes
IN: B. Brandel

Scanner
EI:/IN: Ch. Schneider, L. Hüttinger

Secure Telnet/FTP
EI: T. Partyka, Dr. B. Tewes
IN: B. Brandel, A. Kaltenbacher

Software-Installation
EI: L. Hüttinger, K. Keil
IN: A. Kaltenbacher, H. Sendlbeck

SPSS
EI: Dr. B. Tewes
IN: B. Brandel

SSH
EI: T. Partyka, Dr. B. Tewes
IN: B. Brandel, A. Kaltenbacher

StarOffice
EI: K. Keil, Dr. B. Tewes
IN: A. Kaltenbacher, H. Sendlbeck

Statistik-Software
EI: Dr. B. Tewes
IN: B. Brandel

Telematik-Server
EI: K. Keil, N. Kropf, P. Zimmermann
IN: A. Kaltenbacher

Telnet
EI: T. Partyka, Dr. W. A. Slaby
IN: A. Kaltenbacher, B. Brandel

Terminal-Emulation
EI: T. Partyka, Dr. W. A. Slaby
IN: A. Kaltenbacher

TEX
EI: P. Zimmermann, B. Woitas
IN: B. Brandel, A. Kaltenbacher

Textverarbeitung
EI: P. Zimmermann, K. Keil, Dr. B. Tewes, B. Woitas, H. Zimmermann
IN: A. Kaltenbacher, B. Brandel

Tobit InfoCenter
EI: K. Keil, N. Kropf
IN: A. Kaltenbacher

Unix
EI: P. Zimmermann, T. Partyka, B. Woitas
IN: B. Brandel, A. Kaltenbacher

UseNet News
EI: Dr. B. Tewes
IN: B. Brandel

Verwaltungs-DV
EI:/IN: P. Ihrler, B. Woitas

Virenbehandlung
EI: H. Zimmermann, L. Hüttinger, Ch. Schneider
IN: B. Brandel, A. Kaltenbacher

VoiceMail-Server
EI: K. Keil, N. Kropf, P. Zimmermann
IN: A. Kaltenbacher

WindowsNT/Windows2000
EI: K. Keil, N. Kropf, Dr. B. Tewes
IN: A. Kaltenbacher

Word für Windows
EI: B. Woitas
IN: A. Kaltenbacher

WordPerfect Textsystem
EI: K. Keil, N. Kropf, Dr. B. Tewes
IN: A. Kaltenbacher

WorldWideWeb (WWW)
EI: Dr. B. Tewes
IN: B. Brandel

X/Windows
EI: Dr. B. Tewes
IN: B. Brandel

Zope-Server
EI: Dr. B. Tewes
IN: B. Brandel

Veranstaltungen des Universitätsrechenzentrums Sommersemester 2004

Im Sommersemester 2004 werden seitens des Universitätsrechenzentrums die folgenden Veranstaltungen angeboten:

IN EICHSTÄTT:

Für jeden Kurs ist eine Anmeldung im Sekretariat des Universitätsrechenzentrums (Raum: eO-109 mo–do von 9.00–11.30 und 14.00–15.30 Uhr bzw. Tel.: 08421/93-1462) bzw. über WorldWideWeb (`http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/kurse/`) erforderlich.

1. **Datenanalyse mit SPSS für Windows (Blockveranstaltung)** — Dr. Tewes

Ort: eO-001
Zeit: 29.03.–02.04.2004 jeweils 8.15–11.45 und 13.15–16.00 Uhr
Maximale Teilnehmerzahl: 40

SPSS ist ein weitverbreitetes Statistik-Analysesystem, welches an der Kath. Universität in der Version SPSS für Windows zur Verfügung steht. In dieser Veranstaltung werden grundlegende Techniken zur Handhabung von SPSS für Windows vorgestellt. Neben der Dateneingabe und -bearbeitung stehen ausgewählte elementare statistische Prozeduren und Graphiken im Mittelpunkt.

2. **Einführung in das Arbeiten mit dem PC** — P. Zimmermann

Ort: eO-112
Zeit: 15.04.2004 8.15–12.00 Uhr
Maximale Teilnehmerzahl: 15

In dieser Blockveranstaltung werden grundlegende Kenntnisse und Fertigkeiten zum Arbeiten mit den PCs des Universitätsrechenzentrums vermittelt. Neben einer Einführung in die Arbeitsweise und die wichtigsten Kommandos des Betriebssystems Windows2000 wird der Zugang zum und das Arbeiten im Netz vorgestellt. Alle behandelten Themen werden durch umfangreiche praktische Übungen während der Veranstaltung vertieft. Allen an einer der übrigen DV-Lehrveranstaltungen Interessierten, die bisher nicht über irgendwelche DV-Kenntnisse verfügen, wird die Teilnahme an dieser Blockveranstaltung dringend empfohlen.

3. **Einführung in die Multimedia-Ausstattung der Hörsäle (nur für Dozenten)** Ihrler

Ort: KGA-305/KGA-201
Zeit: 16.04.2004 10.15–11.45 Uhr

Die Veranstaltung wendet sich an Dozenten. Im Sommersemester 2002 wurde ein Teil der Hörsäle und PC-Pools mit Videoprojektoren und Audioanlagen ausgestattet. Die Veranstaltung soll in den Gebrauch der Geräte einführen und Fragen und Anregungen behandeln. Außerdem werden Dokumentenkamera und Videokonferenzsystem vorgeführt.

4. **Einführung in Corel Draw/Photopaint** Keil

Ort: eO-112
Zeit: di 14.15–15.45 Uhr
Beginn: 20.04.2004
Maximale Teilnehmerzahl: 15

Die Veranstaltung versteht sich als grundlegende Einführung in die Grafikbearbeitung am Beispiel einer führenden einschlägigen Software. Corel Draw (jetzt in der Version 11) ist Bestandteil der Corel Learning License, steht campusweit zur Verfügung und kann von Bediensteten auch zu Hause benutzt werden.

5. **Einführung in das Programmieren mit C++** P. Zimmermann

Ort: eO-112
Zeit: do 8.15–10.00 und 16.15–18.00 Uhr
Beginn: 22.04.2004
Maximale Teilnehmerzahl: 15

Die Programmiersprache C, die von Kernighan und Ritchie in Zusammenhang mit der Entwicklung des Betriebssystems Unix entworfen wurde, verfügt sowohl über assembler-ähnliche Sprachelemente, die ein hardwarenahes Programmieren ermöglichen, als auch über Kontrollstrukturen der modernen blockstrukturierten Sprachen, die ein systematisches, strukturiertes Programmieren unterstützen. Durch ein hohes Maß an Portabilität stehen Compiler für C/C++ auf nahezu allen Rechnertypen mit den unterschiedlichsten Betriebssystemen zur Verfügung; C und vor allem die Weiterentwicklung C++, eine objektorientierte Programmiersprache, sind heute unentbehrliche Werkzeuge der Softwareentwickler.

In dieser Veranstaltung werden vornehmlich mit dem Borland C++ System (CBuilder 5) auf den WindowsNT/2000-Workstations die Sprachelemente von C und C++ anhand von konkreten Beispielen vermittelt.

6. **MS-Office-Anwendungen (PowerPoint, Word, Access, Excel)** Woitas

03.05.2004 PowerPoint
17.05.2004 Word Einführung
24.05.2004 Word für Fortgeschrittene
07.06.2004 Access
14.06.2004 Excel I
21.06.2004 Excel II

Ort: eO-001
Zeit: jeweils 8.15–11.45 Uhr
Maximale Teilnehmerzahl: 30

Microsoft PowerPoint ist ein komplettes Präsentationsgrafikpaket, mit dem Sie in Minutenschnelle ansprechend formatierte Präsentationen und Folien erstellen können.
Anhand von MS-Word erstellen Sie Textdokumente.
Mit dem relationalen Datenbanksystem Microsoft Access können eigene Datenbanken entwickelt, Daten erfasst, bearbeitet und nach verschiedensten Kriterien selektiert werden.
Das Tabellenkalkulationsprogramm Microsoft Excel 2000 ist ein Arbeitsmittel zur Planung von Berechnungen und Analyse von Daten. In Tabellen werden Texte, Zahlen und Formeln gespeichert, manipuliert und berechnet. Diese Daten können in Diagrammen schnell und anschaulich dargestellt werden.

7. Erstellung von Web-Dokumenten mit Kontentor/Zope — Dr. Tewes

Ort: eO-112
Zeit: 07.05.2004 8.15–11.45 Uhr
Maximale Teilnehmerzahl: 15

Der Web-Auftritt der Kath. Universität basiert im Wesentlichen auf einem Content Management System. Die technische Basis hierfür stellen Kontentor und Zope dar. Hiermit wird es u.a. ermöglicht, die Seiten direkt im Browser zu bearbeiten oder zu erstellen. Im Rahmen dieser Einführungsveranstaltung soll das Konzept erläutert werden und exemplarisch der Umgang mit dem System geübt werden.

8. SPSS für Fortgeschrittene — Dr. Tewes

Ort: eO-112
Zeit: 14.05./28.05./18.06.2004 jeweils 8.15–11.45 Uhr
Maximale Teilnehmerzahl: 15

Aufbauend auf der Einführungsveranstaltung sollen hier Kenntnisse vermittelt werden, die häufig bei der Verwendung von SPSS für Windows im Rahmen einer wissenschaftlichen Arbeit benötigt werden. Schwerpunkt sollen die multivariaten Verfahren Faktorenanalyse, Diskriminanzanalyse und Clusteranalyse sein. Ferner werden Konfigurationsmöglichkeiten besprochen. Anregungen vor und in der Veranstaltung sind willkommen.

9. TEX im täglichen Einsatz – das neue LATEX 2003 — P. Zimmermann

Ort: eO-112
Zeit: 25.06.2004 15.15–18.00 Uhr
Maximale Teilnehmerzahl: 15

Der Kurs bietet einen Überblick über die Neuerungen der im Dezember 2003 neu herausgegebenen aktuellen LATEX-Version.

10. Einführung in die Internetdienste (Mail, WWW, SSH, SecureFTP) — Dr. Slaby

Ort: eO-112
Zeit: 28.06./05.07.2004 jeweils 08.15–11.45 Uhr
Maximale Teilnehmerzahl: 15

Neben Electronic Mail als „klassischem“ Instrument personenbezogener Datenkommunikation spielen die Informations- und Kommunikationsangebote im weltweiten Internet eine immer größere Rolle. Diese Veranstaltung soll Ihnen einen Überblick über die aktuell verfügbaren Kommunikationsinstrumente vermitteln. Eine Auswahl dieser Dienste wird näher untersucht, wobei typische Anwendungsfälle unter WindowsNT/2000 exemplarisch betrachtet werden.

11. X-Windows und Internetdienste unter Linux Partyka

Ort: eO-112
Zeit: 29.06./06.07./13.07.2004 jeweils 08.15–11.45 Uhr
Maximale Teilnehmerzahl: 15

Diese Veranstaltung richtet sich an Personen, die Interesse an Linux und der Benutzung von Internetdiensten unter diesem Betriebssystem haben. Neben dem klassischen E-Mail werden auch andere Dienste wie telnet, ftp, www, chat ... vorgeführt, die unter Linux zum Teil andere Möglichkeiten bieten als Windows.

12. Textverarbeitung und Publikation wissenschaftlicher Texte mit TEX (Blockveranstaltung) P. Zimmermann

Ort: eO-112
Zeit: 27.–29.07.2004 jeweils 08.15–12.00 und 14.15–18.00 Uhr
Maximale Teilnehmerzahl: 15

Das Publikationssystem TEX gehört zu den Textverarbeitungssystemen, bei denen der Gesamtprozess der Dokumentenanfertigung in die beiden Schritte Texterfassung und Satz/Umbruch aufgespalten ist. Zur Steuerung des Umbruchs werden bei der Texterfassung bestimmte Kommandos in den Text eingefügt. TEX verfügt über nahezu unbegrenzte Möglichkeiten der Satzgestaltung und bietet eine flexible automatische Handhabung von Fußnoten, Verweisen, Referenzen, Inhaltsverzeichnis u.Ä. Insbesondere der professionelle Satz von Formeln oder spezieller Textzeichen (Diakritika u.Ä.) und fremder Alphabete (Arabisch, Griechisch, u.v.m.) sind herausragende Merkmale von TEX. Neben einer reinen Druckversion kann auch leicht ein PDF- oder HTML-Format generiert werden. Damit eignet sich TEX vorzüglich für die Anfertigung wissenschaftlicher Texte, die in professioneller Satzqualität vorliegen sollen.

IN INGOLSTADT:

Für jeden Kurs ist eine Anmeldung im Sekretariat der Abteilung Ingolstadt des Universitätsrechenzentrums (Raum: HB-202 mo–fr von 8.30–11.00 Uhr bzw. Tel.: 0841/937-1887) bzw. über WorldWideWeb (`http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/kurse/`) erforderlich.

1. Statistische Datenanalyse mit SPSS und R Brandel

Ort: HB-U03
Zeit: mo 16.00–18.00 Uhr
Beginn: 19.04.2004
Maximale Teilnehmerzahl: 20

SPSS ist ein weitverbreitetes Statistik-Analysesystem, welches an der Kath. Universität Eichstätt-Ingolstadt in der Version SPSS für Windows zur Verfügung steht. R ist ein sehr flexibles Statistik-Programm mit einer großen Anzahl von Funktionen und in Statistikkreisen weit verbreitet. Im Gegensatz zur nahe verwandten Software S-PLUS ist R eine GNU-Software, also gratis. In dieser Veranstaltung werden grundlegende Techniken zur Handhabung von SPSS für Windows und R vorgestellt. Neben der Datenverwaltung stehen ausgewählte statistische Prozeduren und Graphiken im Mittelpunkt. Voraussetzung zur Teilnahme an diesem Kurs sind Kenntnisse in Statistik, Erfahrungen im Umgang mit MS-WindowsNT/2000 sind vorteilhaft.

2. **Vertiefungskurs Word und Excel** Kaltenbacher

Ort: HB-113
Zeit: di 10.15–12.00 Uhr
Beginn: 20.04.2004
Maximale Teilnehmerzahl: 20

Die Grundkenntnisse in den beiden Office-Produkten werden durch weiterführende Themen vertieft, dabei gehe ich vor allem bei WinWord auf die Gestaltung von Briefen und Dokumenten ein (DIN 5008, Verzeichnisse und Indizes, Fuß- und Endnoten, Zentraldokument, Formeln, Makros usw.), bei Excel lege ich den Schwerpunkt auf die Verbreiterung des Wissens bei der Gliederung von Tabellen, Pivot-Tabellen, dem Arbeiten mit Matrizen, Methoden der Datenanalyse, Makros und dem (grundlegenden) Programmieren mit VBA.

3. **Einführung in HTML** Brandel

Ort: HB-U03
Zeit: 22.04.2004 8.30–12.00 und 13.00–15.30 Uhr
Maximale Teilnehmerzahl: 30

HTML (Hypertext Markup Language) ist eine Textmarkierungssprache für die Dokumente des WorldWideWeb. Wer im WWW Informationen veröffentlichen will (oder muss), dem schadet es nicht, sich zumindest Grundkenntnisse anzueignen, auch wenn diese speziell für die Pflege des Web-Auftritts der Kath. Universität dank der neuen technischen Basis (Zope) nicht mehr zwingend erforderlich sind. Dieser Kurs will nicht nur die wichtigsten Sprachelemente vermitteln, sondern auch in geeignete Software zur Erstellung von Dokumenten einführen und allgemeine Hilfen zur Gestaltung von Hypertext-Dokumenten geben.

4. **Erstellung von Web-Dokumenten an der Kath. Universität** Brandel

Ort: HB-U03
Zeit: 23.04.2004 8.15–12.15 Uhr
Maximale Teilnehmerzahl: 20

Der Web-Auftritt der Kath. Universität ist auf eine neue technische Basis gestellt worden, die es u.a. ermöglicht, die Seiten auch ohne HTML-Kenntnisse direkt im Browser zu bearbeiten oder zu erstellen. Für Lehrstühle wird ein einheitliches Minimalkonzept bereitgestellt, das individuell erweitert werden kann.

Lieber Leser,

wenn Sie *INKUERZE* regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts.
Hat sich Ihre Anschrift geändert oder sind Sie am weiteren Bezug von *INKUERZE* nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.
Bitte haben Sie Verständnis dafür, dass ein Versand auáerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.

Vielen Dank!

Redaktion *INKUERZE*

An die
Redaktion
INKUERZE
Rechenzentrum der
Kath. Universität
Eichstätt-Ingolstadt

85071 Eichstätt

Absender:

Name:_____

Fakultät:_____

Straße:_____

Außerhalb der Universität:_____

_____

Bitte deutlich lesbar in Druckschrift ausfüllen!

☐ Ich bitte um Aufnahme in den Verteiler.
☐ Bitte streichen Sie mich aus dem Verteiler.
☐ Meine Anschrift hat sich geändert.

Alte Anschrift:_____

_____

Ich bin damit einverstanden, dass diese Angaben in der *INKUERZE*-Leserdatei gespeichert werden (Art. 4 Abs. 1 Nr. 2 BayDSG).

_____ _____

(Datum) (Unterschrift)