GWDG Nachrichten

2 / 2003

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Inhaltsverzeichnis

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

26. Jahrgang, Ausgabe 2 / 2003

http://www.gwdg.de/GWDG-Nachrichten

Herausgeber: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg, 37077 Göttingen-Nikolausberg

Redaktion: Dr. Th. Otto Tel. 0551/201-1828, E-Mail: Thomas.Otto@gwdg.de
Herstellung: S. Greber Tel. 0551/201-1518, E-Mail: Sigrun.Greber@gwdg.de

1. Betriebsstatistik Januar 2003

1.1 Nutzung der Rechenanlagen

Rechner	Zahl der Prozessoren	CPU-Stunden
DECalpha	13	2.849,74
IBM RS/6000 SP	224	93.166,71
IBM Regatta	96	45.772,38

1.2 Betriebsunterbrechungen

Rechner/PC-Netz	Störungen		System-pflege	
	Anzahl	Stunden	Anzahl	Stunden
UNIX-Cluster	1	3,00	0	
IBM SP/Regatta	1	7,30	0	
PC-Netz	1	3,00	0	
Nameserver	0		0	
Mailer	2	10,50	0	

2. UNIX-Cluster

2.1 Meilenstein auf dem Weg zur Langzeit-Archivierung: Inbetriebnahme eines verteilten Bandroboter-Systems am 28.1.2003

Sicherung (Backup) und (Langzeit-)Archivierung sind unerlässliche Bestandteile eines effektiven und zuverlässigen Datenmanagements in der heutigen Zeit der Informationsgesellschaft. Sowohl im wirtschaftlichen Bereich als auch insbesondere im Bereich der Wissenschaft gewinnt dieses Thema zunehmend an Bedeutung, was u. a. auch in den strengen gesetzlichen Vorschriften sowie den von wissenschaftlichen Institutionen selbst erlassenen Richtlinien zur Datenaufbewahrung zum Ausdruck kommt.

Die GWDG unterstützt schon seit vielen Jahren die von ihr betreuten Institute der Max-Planck-Gesellschaft und der Universität Göttingen sowie weitere wissenschaftliche Einrichtungen mit einem umfangreichen Leistungsangebot zum Backup und zur Archivierung. Der Archiv-Server der GWDG dient der längerfristigen Speicherung umfangreicher Datenbestände, auf die relativ selten und i. d. R. nur noch lesend zugegriffen wird. Aus Sicherheitsgründen liegen die Dateien in zweifacher Ausfertigung auf Magnetbandkassetten einer angeschlossenen automatischen Bandbibliothek vor, deren Datenvolumen z. Z. ca. 30 TeraByte (d. h. ca. 30.000 GigaByte) beträgt. Der zentrale Backup-Service dient der regelmäßigen (täglichen) automatischen Sicherung aller Nutzerdatenbestände und wichtiger Systemverzeichnisse nicht nur des Workstation-Clusters der GWDG, sondern vorwiegend „externer“, d. h. in den Benutzerinstituten vor Ort betriebener Rechner und wird momentan von über 900 externen Rechnern in Anspruch genommen - Tendenz steigend. Dieser Service greift ebenfalls auf die auch vom Archiv-Server genutzte automatische Bandbibliothek zu.

Abb. 1: Das bisherige Bandroboter-System bei der GWDG

Um den gestiegenen und zukünftigen Anforderungen der Benutzerinstitute an einen verlässlichen, zentralen Archiv- und Backup-Service zu entsprechen, wurden am 28. Januar 2003 im Rahmen einer Informationsveranstaltung zur Langzeit-Archivierung eine weitere automatische Bandbibliothek sowie zwei leistungsstärkere Backup-Server offiziell in Betrieb genommen, die die Speicherkapazität des bestehenden Backup- und Archivierungssystems mehr als verdoppeln.

Die neue Bandbibliothek kann in ihrer derzeitigen Ausbaustufe ein Datenvolumen von maximal ca. 270 TeraByte aufnehmen. Damit lässt sich zusammen mit der alten, bei der GWDG befindlichen Bandbibliothek, die z. Z. eine Speicherkapazität von ca. 200 TeraByte besitzt, ein Datenvolumen von ca. 470 TeraByte für Backup und Archivierung nutzen. Dies entspricht, unter der Annahme einer mit 5 KByte beschriebenen DIN-A4-Seite, umgerechnet einem Papierstapel von ca. 9.400 km Höhe. Mit der Beschaffung weiterer Module für die beiden Bandbibliotheken lässt sich bei zukünftigem Bedarf die Kapazität ohne größere Probleme nochmals verdoppeln.

Aus Sicherheitsgründen stehen die neue Bandbibliothek sowie einer der beiden Backup-Server nicht, wie bisher üblich, im Maschinenraum der GWDG, sondern an einem zweiten, entfernten Standort, dem Medizinischen Rechenzentrum (MRZ) der Universität Göttingen.

Abb. 2: Das neue Bandroboter-System der GWDG, aufgestellt im MRZ

Abb. 3: Blick in das neue Bandroboter-System

Beide Bandroboter sind über eine schnelle Glasfaser-Strecke des GÖNET miteinander verbunden. Mit diesem zukunftsweisenden Konzept der verteilten redundanten Datensicherung betritt die GWDG Neuland und kann sicherstellen, dass auch im Katastrophenfall, also bei Wegfall eines der beiden Standorte, ein zentraler Backup-Service sowie Kopien aller archivierten Daten weiterhin zur Verfügung stehen - eine Anforderung, die von immer

mehr Benutzerinstituten gestellt wird und nun endlich erfüllt werden kann.

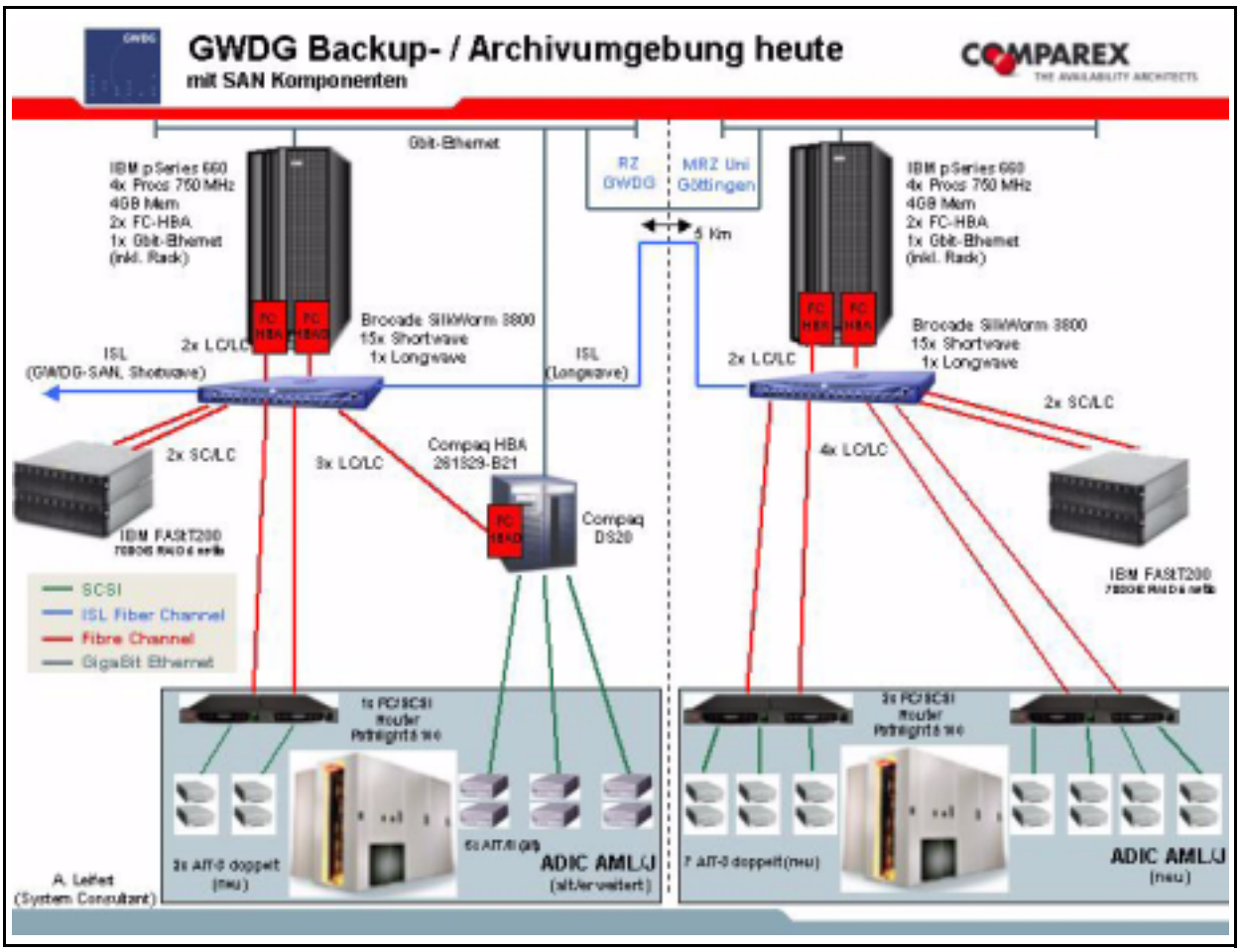


Abb. 4: Übersicht über das neue Backup-/Archivierungssystem der GWDG

Diese Kooperation zwischen GWDG und MRZ ist ein erster bedeutender Schritt, wichtige Dienste und Datenarchivierungen durch das Betreiben von redundanten Geräten am jeweils anderen Standort zu sichern. Langfristiges Ziel ist der Aufbau eines räumlich abgesetzten gemeinsam betriebenen Redundanz-Rechenzentrums, das gewährleisten soll, dass bei Ausfall von Geräten in einem der z. Z. noch bestehenden dezentralen Rechenzentren wichtige Dienste, wie z. B. Mailing und Internetzugang, weiterhin verfügbar und archivierte Daten durch Spiegelung gesichert sind. Für Betriebsunterbrechungen können u. a. der Ausfall der Stromversorgung, ein Brand oder ein Wasserschaden verantwortlich sein. In Zukunft soll in Zusammenarbeit der beiden großen Rechenzentren am Standort Göttingen, GWDG und MRZ, unter Einbeziehung der Universitätsbibliothek und verschiedener weiterer Rechen- und Medienzentren ein örtlicher IT-Verbund realisiert werden, der Forschung, Lehre sowie Dienstleistungen für die beteiligten Nutzergruppierungen mit höchster Effizienz unterstützt. Hierfür wurde vor kurzem ein gemeinsamer Antrag auf Förderung im Rahmen der Förderinitiative der Deutschen Forschungsgemeinschaft (DFG) zur Stärkung der Informationsstrukturen an deutschen Hochschulen und Forschungseinrichtungen gestellt (siehe GWDG-Nachrichten 11/2002).

Während der Informationsveranstaltung am 28. Januar 2003 beschäftigten sich mehrere Vortragende in kurzen Beiträgen mit verschiedenen Aspekten der Langzeit-Archivierung. Zunächst ging Prof. Dr. Hartmut Koke, Geschäftsführer der GWDG, auf das Thema „Langzeit-Archivierung als strategische Aufgabe“ ein. Langzeit-Archivierung wird zunehmend ein zentraler Dienst im Leistungsangebot der GWDG, der in Zukunft ein noch engeres Zusammenarbeiten der beteiligten Wissenschaftseinrichtungen in Göttingen und im gesamten Max-Planck-Bereich erforderlich macht. Anschließend erläuterte Prof. Dr. Elmar Mittler, Leiter der Niedersächsischen Staats- und Universitätsbibliothek Göttingen, vor dem Hintergrund der sich in den letzten Jahren durch das Internet enorm veränderten Anforderungen an die Bibliotheken die große Bedeutung eines zuverlässigen und leistungsfähi-

gen Archivierungssystems für diesen Bereich. Die Niederländische National-Bibliothek in Den Haag hat hierfür eine interessante Lösung gefunden, von der viele Komponenten bereits bei der GWDG im Einsatz sind. Dagmar Ullrich, Mitarbeiterin der GWDG, stellt diese Lösung kurz vor und zeigte dann auf, wie die vorhandene Infrastruktur in Göttingen in Richtung dieses Ansatzes weiterentwickelt werden könnte. Zum Schluss erläuterte Andreas Leifert, zuständiger Mitarbeiter der Firma COMPAREX Informationssysteme GmbH, die als IT-System-Dienstleister das neue Backup- und Archivierungskonzept zusammen mit der GWDG entwickelt und die erforderlichen Komponenten geliefert hat, die technische Seite und die Besonderheiten der verteilten Redundanzlösung in Göttingen.

Nach den vier Kurzvorträgen erfolgte dann die offizielle Inbetriebnahme des neuen Bandroboter-Systems, indem per Live-Bild aus dem MRZ dieses System bei seiner Arbeit, d. h. dem Suchen, Einlegen und Zurückstellen von angeforderten Magnetbandkassetten gezeigt wurde.

Abb. 5: Live-Bild vom neuen Bandroboter-System im MRZ

Im Anschluss an einen kleinen Empfang nutzten viele Teilnehmer der Veranstaltung die Gelegenheit, sich bei der GWDG das dort befindliche zweite Bandroboter-System zeigen und erläutern zu lassen.

Abb. 6: Präsentation des Bandroboter-Systems bei der GWDG

Wer einmal selbst dieses System live bei der Arbeit beobachten möchte, kann dies per Real-Video im WWW unter dem URL

```
http://www.gwdg.de/service/backup/
                                roboter.html
```

tun. Auf der Greifvorrichtung für die Magnetbandkassetten ist nämlich eine Mini-Web-Kamera installiert, die sämtliche Bewegungen mitmacht und ein lebhaftes Bild von den stattfindenden Aktionen vermittelt, wobei es natürlich auch mal Pausen gibt.

Otto

---

3. Kommunikation und Netze

3.1 Video-Server der GWDG

3.1.1 Einführung

Die GWDG betreibt einen Video-Server, den Helix Universal Real-Server von RealNetworks, dessen Dienste allen Benutzern der GWDG zur Verfügung stehen.

Der Real-Server ist eine Server-Software, die in Echtzeit oder vorher aufgenommene Medien über das Netzwerk (Internet oder Intranet) zu Computer-Clients überträgt.

Er ermöglicht also das Übermitteln von Audio- und Videosequenzen, Images, Animationen, Texten und anderen Datentypen zu Computer-Clients über das Internet.

Drei Methoden der Medienbereitstellung werden dabei von ihm angeboten:

1. „Video on Demand“

   Multimediales Datenmaterial, zum Beispiel Präsentationen, Vorlesungsmaterialien, Vorträge oder Informationen zu Forschungsprojekten,

welches für die Übertragung aufbereitet wurde, wird vom Real-Server verwaltet und dem Publikum auf Abruf schnell zur Verfügung gestellt. Die Clients können dabei die Medien mit Befehlen wie Start, Stopp, Pause oder Vor- und Rückspulen steuern.

2. Übertragungen in Echtzeit

   Der Real-Server erlaubt die Übertragung beliebiger Datenströme nahezu in Echtzeit. Damit ist es zum Beispiel möglich, ein entferntes Publikum an Veranstaltungen, Schulungen oder Präsentationen teilnehmen zu lassen. Hierbei kann nicht nur der Videostrom, der den Vortragenden zeigt, sondern auch parallel dazu beispielsweise eine mit MS-PowerPoint erstellte Präsentation übertragen werden. Eine weitere denkbare Anwendung ist die Fernüberwachung zum Beispiel von Experimenten oder Anlagen.

3. Simulierte Echtzeitübertragung

   Die Datenströme einer Veranstaltung können auch zu einem späteren Zeitpunkt vom Real-Server wiedergegeben werden. Wie beim Rundfunk und Fernsehen werden Ereignisse aufgenommen und dann später zu einem vorher geplanten Zeitpunkt gesendet.

3.1.2 Wie arbeitet der Real-Server?

Der Real-Server überträgt die Medienströme über ein Netzwerk bzw. über das Internet zu den Empfängern. Er arbeitet gewöhnlich in Verbindung mit einem Web-Server und erzeugt, wie bereits beschrieben, drei Produkte mit speziellen Funktionen. Dabei nutzt er im Wesentlichen zwei Hauptprotokolle, um mit den Clients zu kommunizieren. Diese sind das Real Time Streaming Protokoll (RTSP) und das Progressive Networks Audio (PNA).

Vom Server wird eine dynamische Anpassung an die jeweils zur Verfügung stehende Bandbreite sichergestellt. Dabei bedient er jeden Client mit der für ihn besten Bandbreite. So kann sichergestellt werden, dass Betrachter mit niedriger Bandbreite die Datenströme unterbrechungsfrei, aber mit entsprechend geringer Qualität empfangen können, während Betrachter mit hohen Bandbreiten in den Genuss der optimalen Videoqualität kommen. Bereits mit einem ISDN-Anschluss (64 Kbit/s) ist eine einigermaßen gute Qualität gewährleistet.

Die Audio-/Videoübertragung im Internet besteht aus drei Komponenten: der Produktion, der Übertragung und dem Empfang der Datenströme.

Produktions-Tools

Der Medieninhalt kann mit Hilfe von Softwareprodukten verschiedener Hersteller erzeugt werden. Diese wandeln die Audio-, Video-Daten oder Animationen in Datenformate, die der Real-Server übertragen kann. Dabei erzeugen sie so genannte Synchronisierte Multimedia Integrations Language (SMIL) Files, die verschiedene Datenströme mit eventuellen Präsentationen synchronisieren.

Die Datenströme werden entsprechend der zur Verfügung stehenden Bandbreite komprimiert. Mit den Produktionswerkzeugen können vorgefertigte Inhalte für die Übertragung aufbereitet werden, aber auch Echtzeitereignisse zur direkten Übertragung kodiert werden.

Real-Server

Wie ein Web-Server dem Web-Browser Seiten über das Internet liefert, liefert der Real-Server unterschiedliche Medienclips zu den Clients. Ein großer Vorteil gegenüber der „statischen“ Einbindung über einen normalen Web-Server besteht darin, dass der Betrachter nicht warten muss, bis die Daten vollständig in den PC geladen sind.

Client-Software

Clients wie beispielsweise der RealPlayer geben die Medienströme wieder. Zusätzlich zur RealSystem-Software können auch andere geeignete Wiedergabe-Softwareprodukte verwendet werden oder die Medien werden in Web-Seiten eingebettet über einen Web-Browser wiedergegeben. Auf diese Weise können beispielsweise Web-Seiten mit Multimedia-Inhalten ergänzt bzw. vom Informationsgehalt aufgewertet werden.

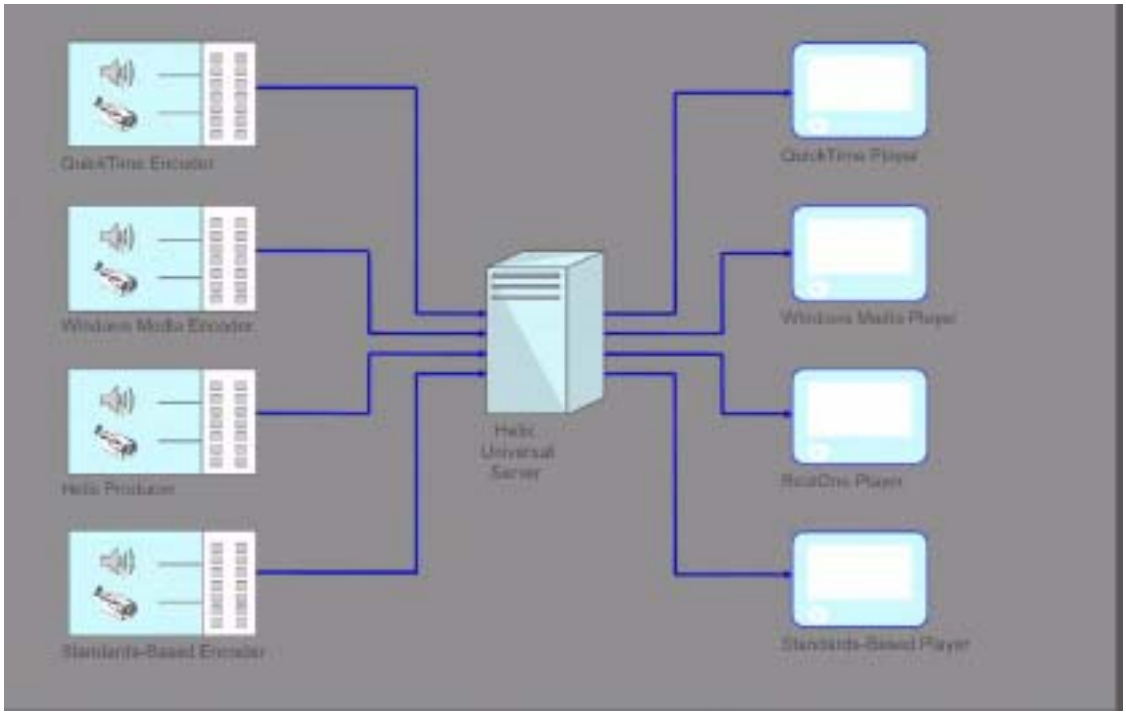


Abb. 1: Prinzip der Multimedia-Übertragung im Internet

3.1.3 Der Helix Universal Real-Server der GWDG

Mit dem Helix Universal Real-Server der GWDG, welcher an das G-WiN mit einer Bandbreite von 155 Mbit/s angeschlossen ist, können gleichzeitig bis zu 60 Multimedia-Ströme (bei Bedarf erweiterbar) zur Verfügung gestellt werden.

Es wird dabei neben den verschiedenen Arten von Medien eine große Auswahl von Media-Playern unterstützt. Dazu gehören der RealOne Player, der Windows Media Player und der Apple QuickTime Player. Folgende gängigen Medien-Formate sind einsetzbar.

Einsetzbare Medien-Formate	
RealNetworks	RealAudio (.rm), RealVideo (.rm, .rmvb), RealPix (.rp), RealText (.rt)
Macromedia	Windows Media (.asf, .wma, .wmv)
Apple	QuickTime (.mov)
Standard-Based	MPEG-1, MPEG-2, MPEG-4, MP3
Image Format	GIF (.gif), JPEG (.jpg, jpeg), PNG (.png)
Andere	AU (.au), AIFF (.aif, .ief), WAV (.wav)

3.1.4 Vorgehensweise für die Real-Server-Nutzung

Video-Konserven für Video on Demand können beispielsweise mit dem RealProducer erzeugt und auf File-Server der GWDG abgelegt werden.

Dieser kann in der einfachsten Version kostenlos unter

```
http://www.realnetworks.com/
```

bezogen werden. Der Real-Server wird nach Abruf des Datenmaterials durch den Empfänger dieses in das Internet übertragen und es dem Betrachter über einen Media-Player oder in Web-Seiten eingebettet zur Verfügung stellen.

Video-Übertragungen in Echtzeit können ebenfalls mit dem RealProducer aus der RealSystem-Familie realisiert werden. Dabei wird mit dem Producer die Video-Aufnahme von einer Kamera über eine Videokarte im PC in Echtzeit in das benötigte

Datenformat gewandelt und über das Netz zum Real-Server transferiert. Dieser überträgt dann die Daten in Echtzeit über das Internet zu den Empfängern.

Zur Erstellung digitaler Videosequenzen für Video on demand bzw. für deren Bearbeitung steht der Videoarbeitsplatz der GWDG zur Verfügung.

3.1.5 Beispiele und Ansprechpartner

Unter

`http://www.gwdg.de/service/multimedia/realserver`

befinden sich zwei Anwendungsbeispiele, die vom Real-Server der GWDG gesendet werden.

Beratung und Unterstützung zum Real-Server sowie zur Erstellung und Wiedergabe von Inhalten erhalten Sie von Herrn Thomas Körmer (Tel.: 0551/201-1555, E-Mail: tkoerme@gwdg.de).

Körmer

3.2 Neue Nameserver im GÖNET

Die GWDG betreibt für das GÖNET Nameserver sowohl für die Auflösung von Internet-Name zu IP-Adressen (Domain Name System **DNS**) als auch für die Auflösung von NetBIOS-Name zu IP-Adressen (Windows Internet Name Service **WINS**). In beiden Fällen betreibt die GWDG mehrere Server, so dass beim Ausfall eines Servers der Dienst über einen zweiten Server weiterhin genutzt werden kann. (In allen gängigen Betriebssystemen kann man jeweils mehrere Server angeben.) Lange Zeit wurden diese Server nur in den Räumen der GWDG betrieben. Um die Redundanz und Ausfallsicherheit im Netz zu erhöhen, hat die GWDG entsprechende Server in der Fernmeldezentrale der Universität aufgestellt bzw. wird sie dort aufstellen.

Nun müssen aber leider die Server in den Betriebssystemen durch Angabe von IP-Adressen konfiguriert werden und IP-Adressen sind leider ortsgebunden. Um diese verbesserte Ausfallsicherheit nutzen zu können, müssen also auf jedem Rechner die entsprechenden Einträge geändert werden.

Als DNS-Server stehen innerhalb des GÖNET jetzt die Rechner

134.76.10.46 (wie bisher) und
134.76.33.21 (neu)

zur Verfügung. Als WINS-Server sollten die Rechner

134.76.26.21 (neu) und
134.76.11.71 (wie bisher)

eingetragen werden.

Die bisherigen, jeweils an zweiter Stelle empfohlenen Server (134.76.98.2 als DNS-Server) und 134.76.11.72 (als WINS-Server) werden noch bis mindestens Ende 2003 zur Verfügung stehen.

Wir bitten alle Systembetreuer, bei Gelegenheit die neuen Server einzutragen.

Beck

---

4. IT-Sicherheit

4.1 Verschlüsselung von E-Mails und Dateien

Hat man sich erst einmal von dem Gedanken verabschiedet, E-Mails seien allein deshalb authentisch, weil sie auf elektronischem Wege übermittelt werden, und sieht sie fortan mehr als das digitale Gegenstück zu einer Postkarte, dann kommt doch schnell der Wunsch auf, sensible Informationen auch einmal so zu versenden, dass wirklich nur der Absender und der Empfänger Kenntnis davon haben. Darüber hinaus möchte man auch gerne als Empfänger sicher sein, dass die Nachricht wirklich von dem jeweiligen Absender stammt.

Bei der Speicherung von Daten auf Festplatten und anderen Medien werden auch oft die Gefahren für die Vertraulichkeit der Daten übersehen. Der leider immer häufiger vorkommende Diebstahl von Rechnern - insbesondere Laptops sind da sehr beliebt -, aber auch Hackeinbrüche führen dazu, dass Daten in falsche Hände gelangen. Viele Betriebssysteme (z. B. Windows 9x oder MacOS vor Version X) bieten gar keine Möglichkeiten, Zugriffe auf Dateien einzuschränken. Aber auch Betriebssysteme, die Zugriffsrechte einschränken können (wie die verschiedenen UNIX-Derivate oder Windows NT, 2000 und XP), helfen nicht wirklich, denn schon der Umbau einer Festplatte in einen anderen Rechner, dessen Root- oder Administrator-Account im Zugriff des Angreifers ist, reicht aus, um alle Schutzmaßnahmen zu umgehen.

4.1.1 Verschlüsselung mit OpenSource-Software

Um all diese Vertraulichkeitsprobleme zu lösen, bedarf es mittlerweile keines geheimen Wissens und aufwändiger Software mehr, sondern dank einer Initiative des Bundeswirtschaftsministeriums

kann sich jeder der eigens dafür entwickelten frei verfügbaren OpenSource-Programme bedienen. Das Projekt, welches dahinter steht, nennt sich **GnuPP** (**G**NU **P**rivacy **P**rojekt, **`http://www.gnupp.org`**) und bietet die Möglichkeit, E-Mails, Dateianhänge, aber auch normale Daten und Verzeichnisse zu ver- und entschlüsseln. Das hierfür dienende Verschlüsselungsprogramm **GnuPG** (**G**NU **P**rivacy **G**uard) basiert auf dem internationalen Standard **OpenPGP** (RFC 2440) und ist vollständig kompatibel zu **PGP** („**P**retty **G**ood **P**rivacy"), was den Vorteil hat, dass die mit **GnuPP** verschlüsselte Daten problemlos auch mit **PGP** wieder entschlüsselt werden können und umgekehrt.

Übliche symmetrische Verschlüsselungsverfahren (Verschlüsselung und Entschlüsselung erfolgen mit einem einzigen Schlüssel) basieren auf einem geheimen Schlüssel, der sowohl Sender als auch Empfänger bekannt sein muss. Dies führt schnell zu dem Problem, wie dieser Schlüssel zwischen beiden Kommunikationspartnern so ausgetauscht werden kann, ohne dass ihn Dritte ausspähen. Die Lösung stellt ein auch bei **GnuPP** eingesetztes asymmetrisches Verschlüsselungsverfahren dar. Statt eines Schlüssels gibt es hier stets zwei Schlüsselhälften: Der öffentliche Schlüssel (**public key**) dient zum Austausch, der geheime Schlüssel (**private key**) verbleibt beim Anwender. Mit dem öffentlichen Schlüssel wird die Nachricht verschlüsselt und nur mit dem privaten Schlüssel kann diese wiederum entschlüsselt werden. Bei der Nachrichtenübermittlung wird somit der öffentliche Schlüssel des Empfängers dem Sender zur Verfügung gestellt, damit er in der Lage ist, die Nachricht für den Empfänger zu verschlüsseln, und nur der dazu passende private Schlüssel des Empfängers vermag diese wieder korrekt zu entschlüsseln. Dem Vorteil, dass hier die Übermittlung eines geheimen Schlüssels entfällt, steht als Nachteil einzig die höhere Rechenleistung gegenüber, die die Verarbeitung asymmetrischer Verschlüsselungsoperationen erfordert. Dies dürfte aber bei dem Leistungsstand moderner Rechnersysteme eine eher untergeordnete Rolle spielen.

Der erforderliche Schutz des sensitiven privaten Schlüssels erfolgt durch ein Passwort (Passphrase), welches natürlich entsprechend sorgfältig gewählt werden und möglichst nirgendwo niedergeschrieben sein sollte. Auch wenn **GnuPP** neben MS-Windows auch für diverse UNIX-Systeme verfügbar ist, soll in diesem Artikel nur der Einsatz unter Windows besprochen werden

Verschlüsselung von E-Mails

Zuerst erfolgt die Installation von **GnuPP**. Die hierfür erforderliche Datei für die Windows-Systeme findet sich am bekannten Ort:

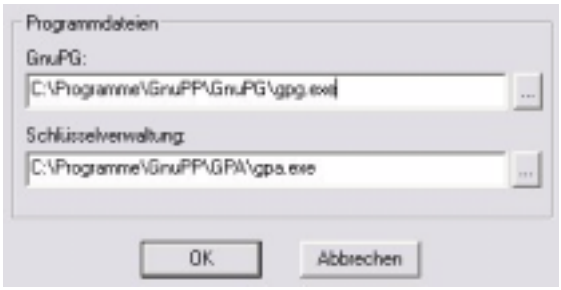
`http://www.gwdg.de/samba/windows/gnupp-1.1-de-installer.exe`

Die Installation von **GnuPP** dürfte problemlos ablaufen. Es sollten dabei nur die Standardeinstellungen übernommen werden. Als nächstes erfolgt die Installation der Plugins für die jeweiligen Mail-Programme; z. B. für Microsoft Outlook (2000, XP) das Plugin von **GDATA** (**`http://www3.gdata.de/gpg/`**) vom bekannten Ort:

`http://www.gwdg.de/samba/windows/GDATA_plugin_091-ger.exe`

Es gibt derzeit Plugins für diverse Mail-Programme, z. B. neben Outlook u. a. auch für **Mozilla** und die UNIX-Mailprogramme **KMail** (KDE) und **Sylpheed**.

Thema dieses Artikels soll zunächst die Anpassung für Microsoft Outlook sein. Bei der Installation des GDATA-Plugins sollte darauf geachtet werden, dass als zu installierende Komponente nur „**GDATA GnuPG-Plugin für Outlook**" ausgewählt wird; die weiteren Vorgaben können dann ohne Veränderung übernommen werden. Nach der Installation sollte Outlook auf jeden Fall neu gestartet werden. Alle weiteren Konfigurationen können nun direkt aus Outlook heraus erfolgen. Zu Beginn müssen die Pfade zu den Programmen **GPG** (**G**NU **P**rivacy **G**uard) und **GPA** (**G**NU **P**rivacy **A**ssistent, die Schlüsselverwaltung) im Menü **Extras > Optionen > Verschlüsselung > Erweitert** angepasst werden, da hier die durch die Installation vorgenommenen Voreinstellungen oftmals nicht stimmen. Nachfolgend ein Beispiel der Pfade unter Windows 98:



Über das Menü **Extras > GnuPG Schlüsselverwaltung** gelangt man zu dem **GPA** (**G**NU **P**rivacy **A**ssistent), in dem zunächst über die Schaltfläche „**Jetzt Schlüssel erzeugen**" die erforderlichen Schlüsselpaare generiert werden müssen. Hierzu werden der Name des Besitzers, seine E-Mail-Adresse und optional zusätzliche Bemerkungen eingetragen. Als nächstes erfolgt die Wahl eines Passwortes. Hier ist das Programm sehr anspruchsvoll, was die Güte des Kennwortes anbetrifft. Dabei sollten auch durchaus die Empfehlungen aus den GWDG-Nachrichten 9/2002 hinzugezogen werden. Auf Wunsch kann man eine Sicherheitskopie der Schlüssel anlegen lassen, die dann unter dem Namen **`pub_key.asc`** für den öffentlichen

und unter **sec_key.asc** für den privaten Schlüssel in einem Verzeichnis eigener Wahl erstellt werden. Die Dauer der Generierung der Schlüsselpaare steht in direkter Abhängigkeit zu der Schnelligkeit des jeweiligen Rechners. Über die Schaltfläche „**Fenster schließen**“ wird das Dialogfenster nach erfolgter Prozedur geschlossen. Nun kann auch der **GPA** beendet werden.

Wenn man nun nicht gleich seine E-Mail-Adressaten mit den ersten Verschlüsselungsversuchen behelligen möchte, kann man sich für derartige Testzwecke auch des digitalen Mail-Roboters „***Adele***“ (**adele@gnupp.de**) bedienen, ein hierfür eigens von der GnuPP-Organisation bereitgestellter Dienst.

Als erstes muss der eigene öffentliche Schlüssel an den Adressaten verschickt werden, was komfortabel über das Menü **Extras > Standardschlüssel in die Nachricht einfügen** erreicht wird. Ideal wäre es natürlich, sich hier einer PublicKey-Infrastruktur zu bedienen, indem der eigene öffentliche Schlüssel auf einem zentralen Key-Server abgelegt wird. Damit könnte auch zugleich die Echtheit dieser Schlüssel durch eine Zertifizierungsinstanz sichergestellt werden. Einen derartigen Dienst bietet derzeit der DFN-Verein (**http://www.dfn-pca.de**) an. Alternativ könnte man den öffentlichen Schlüssel aber auch auf der eigenen persönlichen Homepage ablegen, so dass Interessierte ihn sich herunterladen können.

Verfährt der Kommunikationspartner (z. B. die oben erwähnte *Adele*) auf die gleiche Weise, erhält man ebenfalls eine Nachricht mit seinem beigefügtem öffentlichen Schlüssel. Ist seine Nachricht bereits mit unserem öffentlichen Schlüssel verschlüsselt worden, müssen wir sie über das Menü **Extras > Entschlüsseln und Unterschrift prüfen** erst mit unserem privaten Schlüssel entschlüsseln, wozu wir nach dem dazugehörigen Passwort gefragt werden. Nachdem wir die Mail öffnen konnten, lässt sich der öffentliche Schlüssel unseres Kommunikationspartners über das Menü **Extras > Schlüssel hinzufügen** in unsere Schlüsselverwaltung integrieren. Jetzt können wir zum verschlüsselten Nachrichtenaustausch schreiten, indem über das Menü **Extras > Nachricht beim Senden verschlüsseln** der Verschlüsselungsmodus aktiviert wird. Sobald auf „**Senden**“ geklickt wird, öffnet sich die Schlüsselverwaltung und bietet die Möglichkeit, den öffentlichen Schlüssel unseres Adressaten (hier des Mail-Roboters *Adele*) auszuwählen:

Damit ist der verschlüsselte Nachrichtentransfer gesichert.

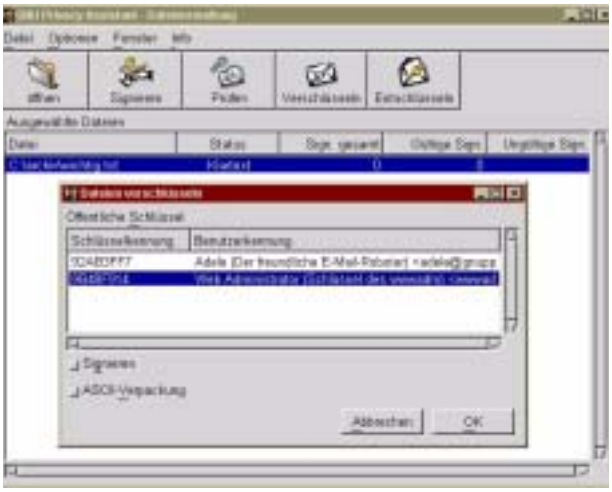
Um zudem auch noch die Gewissheit zu erhalten, dass die Nachricht authentisch ist, muss sie digital signiert werden. Signieren ist gleichbedeutend mit einer elektronischen Unterschrift, die besagt, dass die Nachricht wirklich von dem Absender ist und nicht unterwegs manipuliert wurde. Auch wenn die digitale Signatur von **GnuPP** nicht mit der offiziellen digitalen Signatur nach dem Signaturgesetz vom 22.5.2001 gleichzusetzen ist, erfüllt sie dennoch den gleichen Zweck. Das Signieren der Nachricht erfolgt mit dem eigenen privaten Schlüssel, dessen Echtheit dann jederzeit mit dem zu Verfügung stehenden öffentlichen Schlüssel überprüft werden kann. In Outlook erreicht man diese Funktion über das Menü **Extras > Nachricht beim Senden unterschreiben**. Beim Versenden wird die Nachricht mit dem eigenen privaten Schlüssel signiert und deshalb das dazugehörige Passwort abgefragt. Die Signatur rahmt die Nachricht nun gewissermaßen ein und stellt damit sicher, dass sie auf dem Übertragungsweg nicht verfälscht wird und somit von dem Absender stammen muss. Der Empfänger wird dann wiederum über das Menü **Extras > Entschlüsseln und Unterschrift prüfen** mit dem öffentlichen Schlüssel des Senders die digitale Unterschrift überprüfen.

Mit der Kombination von beiden Verfahren, dem Signieren mit dem eigenen privaten Schlüssel und der Verschlüsselung mit dem öffentlichen Schlüssel des Adressaten erhält man die optimale Sicherheit: Die Mail ist authentisch, kann also nur vom Absender kommen, sofern der öffentliche Schlüssel des Absenders passt. Sie ist weiterhin verschlüsselt mit dem öffentlichen Schlüssel des Adressaten und kann nur von diesem mit seinem privaten Schlüssel wieder entschlüsselt werden

Verschlüsselung von Dateien

GnuPP dient jedoch nicht nur zur Nachrichtenverschlüsselung, sondern vermag jede Datei oder jedes Verzeichnis im lokalen Dateisystem zu verschlüsseln. Durch Starten von **GPA** über **Start > Progamme > GnuPP > Gnu Privacy Assistent** gelangt man in die schon bekannte Schlüsselverwaltung von **GnuPP**. Über das Menü **Fenster > Dateiverwaltung** erhält man die Möglichkeit, Daten

auf dem eigenen Rechner zu verschlüsseln. Dabei wählt man über **Datei > Öffnen** die zu verschlüsselnde Datei aus. Mit Aktivierung der Schaltfläche „**Verschlüsseln**“ wird nach dem zu verwendenden Schlüssel gefragt. Wenn es der eigene sein soll, dann muss er hier ausgewählt werden. Andernfalls, sofern es sich um Dateianhänge für einen Adressaten handelt, sollte man natürlich dessen öffentlichen Schlüssel wählen. Als Ergebnis erhält man eine Datei gleichen Namens, allerdings mit der zusätzlichen Endung **`.gpg`** - in unserem Fall also die Datei **`wichtig.txt.gpg`**, die verschlüsselte Version von **`wichtig.txt`**.



Die Entschlüsselung geschieht in umgekehrter Weise, indem die entsprechende .gpg-Datei ausgewählt und dann die Schaltfläche „**Entschlüsseln**“ aktiviert wird. Erwartungsgemäß wird hierbei wieder das Passwort für den eigenen privaten Schlüssel abgefragt.

Passt alles zusammen, wird die Datei entschlüsselt und unter dem gleichen Namen allerdings ohne die Endung **`.gpg`** im gleichen Verzeichnis abgelegt. Auf diese Weise lassen sich wichtige Daten problemlos dem Zugriff Dritter entziehen. Möchte man gleich mehrere Dateien oder gar gesamte Verzeichnisse verschlüsseln, dann braucht man diese einfach vorher nur in ein ZIP-Format zu archivieren (s. hierzu die GWDG-Nachrichten 8/2002), um sie dann von **GnuPP** als eine Datei verschlüsseln zu lassen.

Insgesamt betrachtet bietet sich hier den Anwendern eine einfach zu handhabende und komfortable Möglichkeit, Daten zu verschlüsseln, und dass nicht nur für den Nachrichtenversand, sondern auch für die eigene lokale Datenhaltung, immer mit dem Ziel, Unbefugten den Zugriff zu verwehren. Da **GnuPP** weitaus mehr Funktionen bereithält, als sie hier in der Kürze dargestellt werden konnten, empfiehlt sich durchaus der Blick in die beiden ausführlichen und leicht verständlichen Anleitungen

`http://www.sicherheit-im-internet.de/download/einsteiger.pdf`

und

`http://www.sicherheit-im-internet.de/download/durchblicker1.1.pdf`

Reimann

4.1.2 Verschlüsselung von Dateien auf NTFS-Dateisystemen

Das Encrypting File System EFS

Die Verschlüsselung mit GnuPP ist ein offener und betriebssystemunabhängiger Standard. Insbesondere bei der Verschlüsselung oder Signierung von E-Mails oder Mailanhängen ist GnuPP bzw. das kompatible PGP das am weitesten verbreitete System. Zur Verschlüsselung von einzelnen Dateien oder ganzen Verzeichnissen im Routinebetrieb ist GnuPP allerdings trotz aller Fortschritte der oben beschriebenen Anwendungen doch relativ aufwändig.

Die neueren Microsoft-Betriebssysteme (Windows 2000 und Windows XP) bieten einen anderen Weg zur Verschlüsselung von Dateien durch das „Encrypting File System“ EFS. EFS ist integraler Bestandteil dieser Betriebssysteme. EFS setzt auf dem NTFS-Dateisystem auf und kann daher nur dort zur Verschlüsselung eingesetzt werden, wo auch NTFS eingesetzt wird. Dadurch ist dieses Verschlüsselungsverfahren mit älteren Microsoft-Betriebssystemen wie Windows 9x oder ME, die nur das VFAT-Dateisystem unterstützen, nicht einsetzbar. EFS ist demnach erst recht nicht mit Betriebssystemen anderer Hersteller oder Open-Source-Betriebssystemen kompatibel. Damit ist schon der wichtigste Nachteil von EFS bzw. ein wesentlicher Vorteil von GnuPP/PGP genannt.

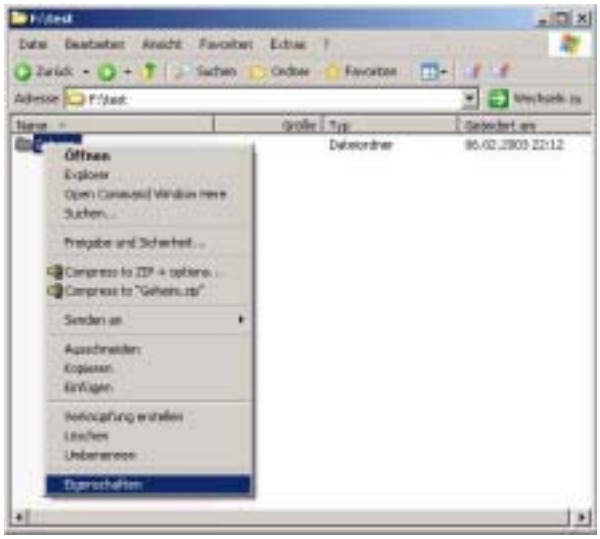
Der große Vorteil von EFS zeigt sich jedoch bei der täglichen Arbeit. EFS arbeitet für den Benutzer (fast) vollkommen transparent. Hat man einmal –

über die Kontextmenüs im Windows-Explorer – Dateien oder Verzeichnisse als verschlüsselt bzw. zu verschlüsseln konfiguriert, so sorgt das Betriebssystem dafür, das die Dateien beim Zugriff sogleich ent- bzw. verschlüsselt werden. Beim Zugriff über die Anwendungsprogramme merkt der Benutzer also nichts von der Verschlüsselung – solange die Rechnerleistung des Computers ausreicht.

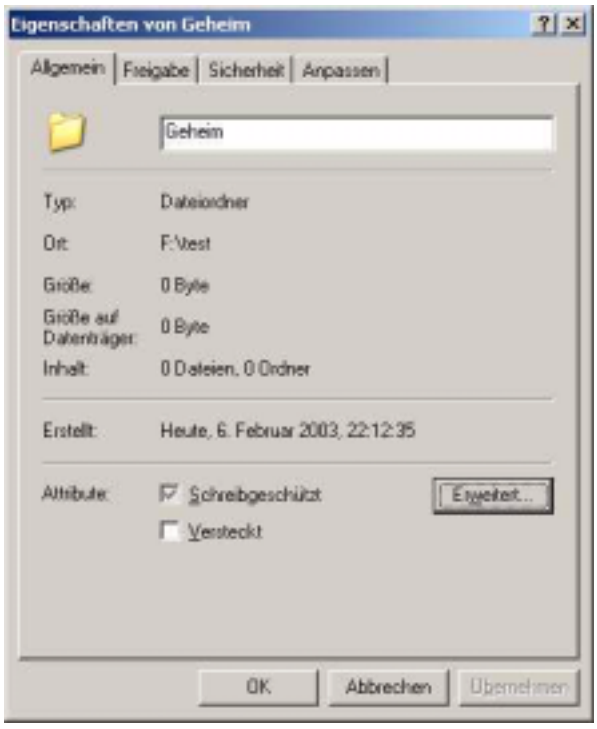
EFS steht nach einer Standardinstallation des Betriebssystems automatisch zur Verfügung. Auch Schlüsselgenerierung und Verwaltung ist so im Betriebssystem integriert, dass der Benutzer im Normalfall nichts davon mitbekommt. Auch das ist (zunächst) ein großer Vorteil des EFS.

Beispiel

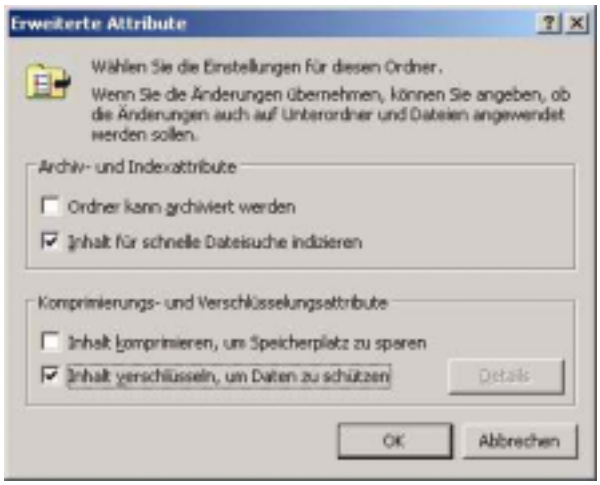
Um eine Datei oder ein Verzeichnis zu verschlüsseln (im nachstehenden Beispiel das Verzeichnis „Geheim“), wählt man es im Windows-Explorer aus und aktiviert im Kontextmenü (anklicken mit der rechten Maustaste) den Punkt „Eigenschaften“ (Klicken mit der linken Maustaste):



Darauf erscheint das Fenster „Eigenschaften“, in dem man jetzt auf die Schaltfläche „Erweitert“ klikken muss.



In dem daraufhin erscheinenden Fenster „Erweiterte Attribute“ wird der Menüpunkt „Inhalt verschlüsseln, um Daten zu schützen“ aktiviert.



Nachdem die beiden Fenster durch Klicken auf „OK“ wieder geschlossen wurden, ist die ausgewählte Datei bzw. das Verzeichnis (im Beispiel also das „Geheim“-Verzeichnis) verschlüsselt.

Anwendern, die Verschlüsselungstechnologie einsetzen wollen, empfiehlt Microsoft – die GWDG schließt sich dem an –, nach Möglichkeit, ganze Verzeichnisse und nicht einzelne Dateien zu verschlüsseln. Dadurch werden alle Dateien in den Verzeichnissen verschlüsselt und somit auch alle darin von Anwendungen möglicherweise erstellten temporären Dateien. Unverschlüsselte temporäre

Dateien können nach einem Fehlerabbruch der Anwendung versehentlich erhalten bleiben, so dass das durch die Verschlüsselung erstrebte Ziel der Datenvertraulichkeit verfehlt wird.

Wiederherstellungsoptionen und gemeinsame Nutzung verschlüsselter Dateien

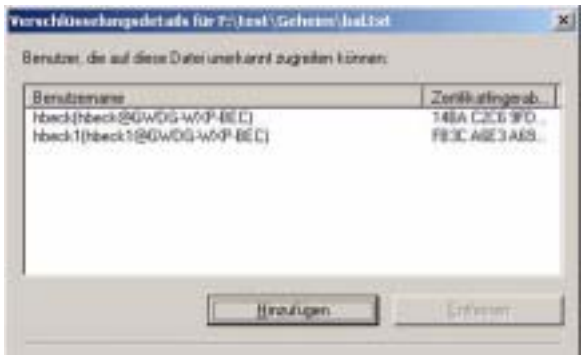
Verschlüsselung von Dateien bietet einen ausgezeichneten Schutz der Vertraulichkeit der Inhalte derselben, weil die Datei nur noch von demjenigen gelesen werden kann, der über den passenden Schlüssel verfügt. Gleichzeitig entsteht dadurch aber auch das Risiko, das Dateien unbrauchbar werden, wenn, aus welchem Grund auch immer die Schlüssel verloren gehen. Microsoft hat daher im EFS einen Mechanismus zur Wiederherstellung von Dateien nach Verlust von Schlüsseln vorgesehen.

EFS arbeitet dazu bei der Verschlüsselung mit einer Mischung von symmetrischen und asymmetrischen Verschlüsselungsverfahren. Die zu verschlüsselnde Datei wird zunächst mit einem symmetrischen Verfahren verschlüsselt (dem „File Encryption Key“ FEK). Dieser Schlüssel selbst wird dann mittels eines asymmetrischen Verfahrens verschlüsselt und gemeinsam mit der Datei gespeichert. Die Verschlüsselung des FEK erfolgt mittels des öffentlichen Schlüssels des Benutzers, der die Datei verschlüsselt. Aus diesem verschlüsselten FEK kann mit dem privaten Schlüssel des Benutzers der FEK wiedergewonnen werden. Mit dem FEK kann dann die Datei entschlüsselt werden.

Um eine Wiederherstellung (Entschlüsselung) einer Datei auch dann zu ermöglichen, selbst wenn der Besitzer seinen Schlüssel verloren hat, sieht das Betriebssystem „Wiederherstellungsagenten“ („Recovery Agents“) vor. Ist ein solcher Agent auf dem Rechner – oder bei Systemen in einem Active Directory für eine Domäne oder Organisationseinheit – konfiguriert, dann wird mit der Datei nicht nur der mit dem öffentlichen Schlüssel des Benutzers verschlüsselte FEK gespeichert. Zusätzlich wird eine mit dem öffentlichen Schlüssel des Agenten verschlüsselte Variante des FEKs mit der Datei gespeichert. Dadurch kann der FEK auch mittels des privaten Schlüssels des Agenten ermittelt werden und damit wiederum die Datei entschlüsselt werden. Dieses Verfahren ermöglicht auch die Konfiguration mehrerer Wiederherstellungsagenten.

Mit dem Begriff „Wiederherstellungsagent“ ist ein spezielles Benutzerkonto gemeint. Standardmäßig ist auf einem isolierten Rechner der lokale Administrator, bei Rechnern, die in Domänen integriert sind, der Domänenadministrator der Wiederherstellungsagent. Diese Rollenzuordnung kann aber auch anders konfiguriert werden. Die Festlegung dieser Rolle muss rechner- oder domänenbezogen erfolgen. Der Benutzer hat darauf keinen Einfluss.

Der für den Wiederherstellungsagenten verwendete Mechanismus kann auch dazu eingesetzt werden, um eine gemeinsame Nutzung verschlüsselter Dateien durch mehrerer Benutzer zu ermöglichen. Dazu muss der Eigentümer der Datei die öffentlichen Schlüssel der Benutzer kennen, denen er die Entschlüsselung ermöglichen will. Hierfür muss er in dem Fenster „Erweitere Attribute“ (s. o.) auf „Details“ klicken und erhält dann das untenstehende Fenster, in dem die Benutzer eingetragen werden können, die die Datei entschlüsseln dürfen.



Sicherheitsaspekte

Die bisherige Beschreibung des EFS hat (hoffentlich?) den Eindruck erweckt, dass EFS ein einfaches Hilfsmittel ist, um eine erhebliche Steigerung der Datensicherheit zu erreichen. Das ist aber leider nur die halbe Wahrheit, denn je nach Einsatzszenario gibt es doch erhebliche Einschränkungen und Probleme, auf die hier noch hingewiesen werden soll.

Ein zentrales Problem ist die Speicherung der privaten Schlüssel und deren Sicherung gegen Verlust und vor allem gegen unbefugten Zugriff. Zunächst einmal bietet EFS eine einfache und unkomplizierte Nutzung dieser Verschlüsselungstechnologie. Das Betriebssystem nimmt dem Nutzer alle komplexeren Aufgaben wie Schlüsselgenerierung und Schlüsselverwaltung ab. Für den Benutzer reicht der normale Windows-Anmeldevorgang und das Betriebssystem sorgt für die Bereitstellung der benötigten Schlüssel. Leider führt das aber auch zu der Konsequenz, dass jeder, der das Passwort für die Windows-Anmeldung kennt, auch den vollen Zugriff auf die verschlüsselten Dateien hat. Gegen Hacker schützt das System in dieser Konfiguration also nicht.

Noch kritischer sind in dieser Beziehung die privaten Schlüssel von Wiederherstellungsagenten, denn diese können ja – je nach Konfiguration – alle Dateien eines Rechners oder gar einer ganzen Domäne wieder entschlüsseln.

Gegen diese Problematik hilft letztlich nur eine externe Speicherung der Schlüssel (und gleichzeitige Löschung aus den sonst üblichen Aufbewahrungsorten im System), z. B. auf Disketten oder Smartcards, die dann ihrerseits wiederum sicher verwahrt werden müssen. Damit muss dann allerdings auf etwas Bequemlichkeit verzichtet werden. Für die privaten Schlüssel der Wiederherstellungsagenten ist dieses Vorgehen auf jeden Fall ein Muss (die Schlüssel gehören in einen Tresor).

Ein weiteres Problem stellen die Wiederherstellungsagenten dar, weil deren Zugriff nicht vom Benutzer verboten werden kann. Die Erzeugung dieser Schlüssel wird in der für einen Rechner oder eine Domäne verbindlichen Sicherheitsrichtlinie festgelegt. Der Benutzer muss sich dem zwangsweise unterwerfen. Für gewisse Szenarien ist das sicherlich die richtige Lösung (z. B. will man ja bei Ausfall oder Ausscheiden eines Mitarbeiters in einer Firma noch an die dienstlich erstellten Dokumente herankommen – da kann man sich nicht darauf verlassen, dass die Mitarbeiter das immer selbst richtig einstellen).

Ebenfalls ein Problem ist, dass nur Dateien auf einem NTFS-Dateisystem verschlüsselt abgelegt werden. Werden die Dateien auf ein Medium kopiert, das NTFS nicht unterstützt, werden die Dateien zwangsweise wieder entschlüsselt. Das trifft z. B. das Kopieren auf Disketten oder CDs. Auch wenn auf Dateien über Netze zugegriffen wird, werden die Dateien im Klartext übertragen (die Entschlüsselung erfolgt im I/O-System des Rechners auf dem sie gespeichert sind). So werden bei einer Übertragung als Mailanhang die Dateien ebenfalls entschlüsselt. Die Lösung, die Microsoft hier als Umgehung vorschlägt, ist, die verschlüsselten Dateien mit einem Backup-Programm, das NTFS hinreichend unterstützt, in ein Backup-Archiv auf Festplatte zu sichern und dann die so erzeugte Archivdatei zu kopieren oder zu verschicken. Vor dem Zugriff auf die Dateien muss dann allerdings das Archiv wieder mit dem entsprechenden Backup-Programm ausgepackt werden, und aus dem Archiv müssen die Dateien wieder in ein NTFS-Dateisystem restauriert werden. Für die Absicherung von Mailverkehr ist EFS daher offensichtlich kaum als praktikable Lösung anzusehen.

Soll die Verschlüsselungstechnologie nicht nur auf einem einzelnen Rechner, sondern in einer Domäne eingesetzt werden, so muss die Instanz zur Schlüsselverwaltung und Schlüsselgenerierung domänenweit zur Verfügung stehen. Auch dadurch kann die Bequemlichkeit etwas leiden, weil man statt der vom Betriebssystem einfach mal so nebenher erzeugten, selbstsignierten Schlüssel eine zentrale Zertifizierungsstelle benötigt.

Einsatz im Active Directory der GWDG

Im Windows-Netz der GWDG (Active Directory) werden für alle angeschlossenen Systeme der Verschlüsselungsdienst und insbesondere die zentrale Schlüsselzertifizierung und Schlüsselverwaltung ab voraussichtlich 1.4.2003 zur Verfügung stehen. Details dieses Dienstes werden in einer der nächsten GWDG-Nachrichten veröffentlicht.

Beck, Quentin

4.2 Aktuelle Viren, Würmer und Trojaner

Zu den Gründen, die uns daran hindern, im wissenschaftlichen Umfeld unsere Arbeit ungestört und effizient zu verrichten, gehören leider auch Angriffe aus einem feindlich gesonnenen Umfeld. Neben hochintelligenten Hackern, die versuchen, in unsere Computer einzubrechen, um sie unter ihre Kontrolle zu bringen, sind wir auch den Angriffen „niederen Getiers“, nämlich von Viren und Würmern ausgesetzt. Manchmal versuchen auch Trojanische Pferde sich einzuschleichen, die in ihrem Inneren böswillige Objekte verbergen, die uns ausspionieren oder bekämpfen wollen.

Mit diesem Artikel soll aus aktuellem Anlass ein grober Überblick über das Gefahrenpotenzial gegeben werden, das vor allem aus der Internet-Nutzung droht, und damit sollen insbesondere diejenigen PC-Benutzer sensibilisiert werden, die dieser wichtigen Thematik bisher leider gar keine oder nur wenig Beachtung geschenkt haben. In den nächsten Ausgaben der GWDG-Nachrichten soll dann detaillierter auf einzelne Gefahrenquellen und konkrete Handlungsempfehlungen für die Benutzer eingegangen werden.

4.2.1 Hacker

Hacker erhalten Zugang zu unseren Rechnern, indem sie sich ganz normal als Administrator anmelden, nachdem sie ein Passwort ausgespäht oder mit einem der im Internet erhältlichen Spezialprogramme geknackt haben. Auch versuchen sie, über die sogenannten „Ports“, den logischen Kommunikationskanälen des Rechners zur Außenwelt, einzudringen und sich so z. B. Administratorrechte zu verschaffen.

Unter dem oben genannten „Getier“ sind es die Würmer und Trojanischen Pferde, deren sich Hakker zur Vorbereitung Ihres Einbruchs in ein Rechnersystem auch gern bedienen.

4.2.2 Computerviren

„Echte“ Computerviren sind den aus Flora und Fauna bekannten Viren vergleichbar: Sie befallen einen Wirt (hier ein Computerprogramm) und bauen ihren genetischen Code (hier eine Folge von Com-

puterbefehlen) ein, so dass beim Ablauf des Programms Befehle ausgeführt werden, die schädliche Wirkungen haben. Auch sorgt dieser eingebaute Code für die Vermehrung des Virus: Er befällt weitere Programme in seiner Umgebung.

Zuerst waren es meist Programmviren und Bootsektorviren, die sich in unsere Computer einschlichen. Als dann beinahe an jedem Arbeitsplatz mit den Office-Produkten von Microsoft gearbeitet wurde, hatten über einige Jahre die (Word-)Makroviren ihre Hochzeit. Die Verbreitung „echter“ Viren hat in den letzten Jahren etwas abgenommen, dagegen die Ausbreitung von Würmern stark zugenommen, wobei als Ausbreitungsmedium das Internet dient. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht hier Statistiken, die z. B. für das Jahr 2001 angeben, das man es zu 52% mit Würmern, zu 28% mit Makroviren, zu 14% mit Bootsektorviren und zu 5% mit Trojanern zu tun hatte.

Würmer in der EDV-Welt sind eigenständige Programme, die sich über die Computernetze ausbreiten, in Rechner eindringen, sich dort vermehren, wobei sie ständig darauf bedacht sind, ihre Brut über die Computernetze auch in andere Rechner zu schicken. Bemerkbar durch Anrichtung eines Schadens machen sie sich erst, nachdem sie sich einige Zeit ausgebreitet haben.

4.2.3 Trojanische Pferde

Trojanische Pferde sind Programme mit fragwürdigem Nutzen, die man gutgläubig und in leichtsinniger Weise auf seinen Computer lädt. Ihr eigentlicher Zweck ist z. B., den Computer auszuspionieren: Sie geben Fremden Informationen – geheime Daten, Adressen, Passwörter – oder verraten einem Programmhersteller, dass man seine Software benutzt, ohne eine Lizenz zu besitzen. Das Bundesamt für Sicherheit in der Informationstechnik definiert wie folgt:

> „Trojanische Pferde sind Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen. Im Gegensatz zu Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.“

4.2.4 Aktuelle Situation

Für die letzten vier Monate gibt der Antiviren-Programm-Hersteller Sophos die Häufigkeitsverteilung der im jeweiligen Monat gemeldeten Viren wie folgt an:

Oktober 2002	November 2002	Dezember 2002	Januar 2003
W32/**Bugbear**-A: 77,6%	W32/**Bugbear**-A: 29,4%	W32/**Bugbear**-A: 15,8%	W32/Avril-B: 16,8%
W32/**Klez**-H: 6,2%	W32/Braid-A: 8,5%	W32/**Klez**-H: 10,9%	W32/Avril-A: 12,4%
W32/**Opaserv**-A: 2,5%	W32/**Klez**-H: 7,7%	Troj/Tubmo-A: 5,9%	W32/**Klez**-H: 12,1%
W32/Yaha-E: 1,1%	W32/**Opaserv**-A,C:10,5%	W32/**Klez**-G: 4,5%	W32/Sobig-A : 6,1%
W32/Badtrans-B: 0,8%	W32/Flcss: 4,6%	W32/**Opaserv**-G: 3,9%	W32/Yaha-E.K: 9,0%
W32/Nimda-D: 0,7%	W95/Spaces : 3,3%	W32/Nimda-D: 2,9%	W32/**Bugbear**-A: 5,6%
W32/**Opaserv**-C,D: 1,3%	W32/**Opaserv**-F: 62,5%	W32/**Opaserv**-A,F: 5,2%	W32/ElKern-C: 2,1%
W32/ElKern-C: 0,6%	W32/**Opaserv**-B: 2,1%	W32/Braid-A: 2,2%	W95/Spaces : 1,5%
W32/**Opaserv**-B: 0,5%	W32/**Opaserv**-D: 2,0%	W32/ElKern-C: 2,2%	W32/Flcss: 1,2%

An der (genormten) Namensgebung der Viren kann abgelesen werden, welchen Betriebssystemen die Viren gefährlich werden. Von vielen Viren treten in kurzer Zeit Varianten auf, deren Signaturen jeweils wieder neu in die Antiviren-Programme eingearbeitet werden müssen. Der Buchstabe hinter dem Virusnamen (beginnend mit A) zeigt die Variante an.

Insgesamt meldet Sophos, im Januar 2003 521 neue Viren, Würmer und Trojaner erkannt zu haben. Die Gesamtzahl der Viren, die Sophos bis jetzt aufgespürt und gegen die das Unternehmen Schutzmechanismen entwickelt hat, beträgt damit 79.538. (Die anderen Antiviren-Programm-Hersteller melden vergleichbare Zahlen.)

In Göttingen hatten wir im Januar nennenswerte Vorfälle mit den Würmern Bugbear (seit Ende September 2002 bekannt), Opaserv (seit Oktober 2002 bekannt) und SQLSlammer (seit 25. Januar 2003 bekannt), die im Folgenden geschildert werden sollen, um aufzuzeigen, wie vielfältig diese Plage ist und wie mühsam und zeitaufwendig es ist, ihrer Herr zu werden.

4.2.5 Bugbear

Der Wurm „Bugbear“ ist seit Ende September 2002 bekannt. Über große Entfernungen verbreitet er sich als Anhang von elektronischer Post (E-Mail-Adressen findet er auf seinem Wirtsrechner; er verfügt über einen großen Vorrat von Textteilen, aus denen er den Betreff und den Text formuliert. Er kann auch auf E-Mails in der Posteingabe antworten und verwendet dabei deren Textteile).

Durch eine Schwäche des Microsoft Internet Explorer kann ein Attachment (Anhang) geöffnet und ausgeführt werden, ohne dass es durch Doppelklicken gestartet wird. (Diese Schwäche kann durch Einbau eines von Microsoft empfohlenen Sicherheits-Patches beseitigt werden).

Nachdem der Wurm „Bugbear“ in einen Computer eingedrungen ist, macht er Netzwerkfreigaben von Computern in seiner Umgebung ausfindig. Über eine offene Laufwerksfreigabe kopiert sich der Wurm in den fremden Rechner. Der Wurm bemächtigt sich nicht nur der Laufwerksfreigaben, sondern auch der Druckerfreigaben. Bei diesen schickt er seinen Kode zum Drucker, welcher diesen druckt. Dabei können große Mengen Papier eines teuren Spezialdruckers verschwendet werden, Da der absendende Rechner dem Druckserver bekannt ist, kommt der Besitzer des PCs, auf dem sich „Bugbear“ eingerichtet hat, für die Kosten auf.

Da sich der Wurm „Bugbear“ im Rechner unter verschiedenen, auch zufällig erzeugten Namen auf der Festplatte abspeichert, sind Antiviren-Programme nicht in der Lage, den Wurm zu beseitigen. Auch die vielfältigen Einträge in der Registrierungsdatenbank und in diversen .INI-Konfigurationsdateien, in denen Befehle abgespeichert werden, die den Wurm gleich beim Betriebssystemstart aktivieren, können von einem Antivirus-Programm nicht korrigiert werden. Diese Korrekturen und das Löschen der Wurm-Dateien muss in mühsamer Handarbeit geschehen. Vergisst man ein Exemplar des Wurms, hat er sich beim nächsten Systemstart sehr schnell wieder ausgebreitet.

Damit der Wurm „Bugbear“ nicht so schnell erkannt wird, verfügt er über die Fähigkeit, die gängigsten Antiviren-Programme zu deaktiviren.

> „W32/Bugbear-A öffnet außerdem Port 36794 und sendet eine Benachrichtigungs-E-Mail über SMTP an eine externe Adresse, die vertrauliche Daten über den Computer des Opfers, wie z. B. Benutzername und Kennwort, enthält. Der Wurm kann versuchen festzustellen, ob ein Apache-1.3.26-Webserver vorhanden ist und diese Information an eine externe E-Mail-Adresse weiterleiten.“
> *(Auszüge aus der Information von Sophos)*

4.2.6 Opaserv

Der Netzwerk-Wurm (Network Crawler) „Opaserv“ ist seit Oktober 2002 bekannt.

Nachdem er in einen Computer eingedrungen ist, macht er Netzwerkfreigaben von Computern in seiner Umgebung ausfindig. PCs mit den Betriebssystemen Windows 95/98/ME, die ihre Freigaben mit Passwort abgesichert haben, teilt er mit, dass er leider nur ein Zeichen lange Passwörter kennt. Das Betriebssystem geht darauf ein und akzeptiert eines der nun vom Wurm ausprobierten, ein Zeichen langen Passwörter. Über die nun offene Laufwerksfreigabe kopiert sich der Wurm in den fremden Rechner.

Der Fehler des Betriebssystems Windows, ein nur aus einem Zeichen bestehendes Passwort zu akzeptieren, wurde bereits vor zwei Jahren bekannt und die Firma Microsoft empfiehlt seitdem, auch für diesen Fehler eine Sicherheitskorrektur in das Betriebssystem einzubauen. Leider ignorieren die meisten Besitzer von PCs diese Empfehlungen und bringen ihre Systeme nicht auf den sichersten Stand.

Wie der Wurm „Bugbear“ tarnt sich auch „Opaserv“ mit verschiedenen Namen und trägt sich in die Run-Befehle der Registrierungsdatenbank und in .INI-Dateien ein. Er kann somit nicht vom Antiviren-Programm beseitigt werden; dies muss in Handarbeit geschehen.

Gelingt die vollständige Beseitigung des Wurms, aber der oben genannte Sicherheits-Patch wurde noch nicht vorgenommen, kann es leicht passieren, dass der Wurm wieder eindringt, sobald der PC ans Netzwerk angeschlossen wird.

4.2.7 SQLSlammer

Seit dem 25. Januar 2003 nutzt der Wurm „Slammer“ eine sechs Monate alte Schwachstelle aus. Er beweist „einmal mehr, dass es äußerst notwendig ist, dass jeder seine Patches auf dem aktuellsten Stand hält“, so Gernot Hacker, Senior Technical Consultant bei Sophos.

> „W32/SQLSlam-A ist ein SQL-Wurm, der nicht gepatchte Microsoft SQL Server angreift, auf denen Windows 2000 läuft. Er kann auch Anwender von MSDE 2000 (Microsoft SQL Desktop Engine) angreifen. Der Wurm nutzt eine Pufferüberlauf-Schwachstelle des SQL Servers aus. Eine Erläuterung dieser Schwachstelle finden Sie auf der Microsoft Website. Anwender, die bereits SQL Server Service Pack 3 installiert haben, sind von diesem Wurm nicht betroffen.
>
> W32/SQLSlam-A erscheint als Paket am UDP

> Port 1434 und nutzt eine Pufferüberlauf-Schwachstelle aus, um kontinuierlich zufällige IP-Adressen zu erzeugen und sich an diese Adressen zu senden. Dadurch wird eine Distributed-Denial-of-Service (DDOS)-Attacke auf den betroffenen Computern ausgelöst, was zu erhöhtem Internetverkehr führt."
> *(Auszüge aus der Information von Sophos)*

Der letzte Halbsatz ist sehr vorsichtig formuliert. Tatsächlich kann „SQLSlammer" ein Computernetzwerk lahm legen, was im Göttinger Übertragungsnetz GÖNET auch prompt in Teilbereichen passierte – wegen des aufmerksamen Netzwerkadministrators der GWDG zum Glück nur für kurze Zeit.

Man kann seine Rechner vor diesem Wurm nur schützen, wenn man den Patch von Microsoft installiert. Hinweise von Microsoft zu dieser Thematik findet man auf der Microsoft-Website.

4.2.8 Schlussfolgerungen

Aus den obigen Beschreibungen lernen Sie, dass (neben der obersten Regel, Daten konsequent zu sichern) zu den grundlegenden Sicherheitsvoraussetzungen gehört, ein stets aktuell gehaltenes Antiviren-Programm auf allen Rechnern einzusetzen. Dieses kann Viren erkennen und sie an ihrer Verbreitung hindern, indem Kopiervorgänge virenbehafteter Dateien nicht zugelassen werden. Leider nisten sich manche Viren derart geschickt und vielfältig im System ein, dass es dem Virensuchprogramm nicht möglich ist, den Virus zu eliminieren. Zu diesem Zweck bieten die Hersteller von Antiviren-Programmen speziell zu bestimmten Viren Hilfsprogramme zu deren Beseitigung an.

Weiterhin sollten unbedingt die zur Verfügung stehenden Service-Packs und Sicherheits-Patches eingefahren werden. Hierzu bieten die Web-Seiten der GWDG in der Rubrik „Service > Sicherheit" vielfältige Informationen und Möglichkeiten, die Service-Packs und Patches herunterzuladen oder über das Netz direkt auf dem Computer zu installieren.

Zur Zeit schleichen sich die Viren und Würmer am häufigsten mit der elektronischen Post ein und E-Mail-Programme sowie Internet-Browser, die viele eingebaute Funktionen zur automatischen Erkennung und Ausführung von vielerlei „Spezialitäten" enthalten, machen es den Viren leicht einzudringen. Der Server der GWDG, der die E-Mail aus dem Internet entgegennimmt, prüft alle eingehenden Sendungen auf Viren. Man sollte unbedingt dessen Virenwarnungen beachten.

Aber auch diese „Wächterfunktion" kann von geschickten Programmierern umgangen werden, wie folgendes Beispiel zeigt:

4.2.9 Klez

In der Posteingangsliste findet man einen nicht weiter auffälligen Eintrag, eine Virenwarnung des Posteingangs-Servers liegt nicht vor. Man sieht sich die E-Mail an, sie enthält einen belanglosen Text oder ist völlig leer. Aber ehe man sich versieht, öffnet sich das Fenster des Web-Browsers, zeigt eine fremde Seite an und ein kleines Fenster meldet, dass zwei Dateien heruntergeladen werden. Ordentlicherweise hat man ein Antiviren-Programm installiert und aktualisiert. Dieses meldet nun „Virus Klez in herunterzuladender Datei gefunden. Kopiervorgang abgebrochen." Nach Klicken der Taste „OK" meldet sich das Antiviren-Programm nochmals mit gleicher Meldung. Hier versucht also ein Virus per E-Mail einzudringen, ohne in der E-Mail selbst enthalten zu sein. Stattdessen wird er automatisch – gleich im Doppelpack – heruntergeladen. Wohl dem, der ein aktuelles Antiviren-Programm auf seinem Rechner installiert hat!

4.2.10 Hoax

Trittbrettfahrer, die aus der Virenplage ein „eigenes Süppchen kochen", sind die Verbreiter der so genannten Hoaxes, die auch in Göttingen im letzten Monat vielfach aufgetreten sind.

Ein Hoax ist eine E-Mail mit typischerweise folgendem Text:

> „Liebe/r EDV-Experte/in,
>
> in letzer Zeit breitet sich ein äußerst gefährlicher Virus über die Computernetze aus, den die Antiviren-Programme der verschiedenen Hersteller noch nicht entdecken können. Der Virus löscht in etwa 14 Tagen alle Dateien Ihrer Festplatte. Um den Virus zu beseitigen, suchen sie auf Ihrer Platte nach einem Programm mit dem Namen xyz.exe. Wenn sie es finden, löschen Sie es sofort, denn es enthält den Virus. Schikken Sie diese Mail an alle Ihre Korrespondenzpartner weiter, um auch sie zu warnen!"

Hierzu ist zunächst zu sagen, dass man dem aktuellen Antiviren-Programm auf seinem Computer mehr vertrauen sollte als einer x-beliebigen Person irgendwo im Internet, die einem rät, eine wichtige Systemdatei zu löschen, mit der Folge, dass man sein Betriebsystem mehr oder weniger beschädigt.

Die beabsichtigte Wirkung eines Hoax, der sich im Schneeballsystem in den Netzen verbreiten soll, ist:

- Leute zu verunsichern,
- leichtgläubigen Menschen einen Schaden zuzufügen,
- Mitarbeiter von der Arbeit abzuhalten,

- die Postfächer der Mail-Server überlaufen zu lassen und
- die Computernetze mit Müll zu verstopfen.

Wie sollte man auf einen Hoax reagieren? Die betreffende Mail kann gelöscht werden, jedoch sollte man keine Dateien auf dem eigenen Computer löschen und an niemanden (außer vielleicht dem eigenen Systemadministrator) die Mail weiterschicken. Sie wollen doch nicht mit Ihrem guten Namen einen Brief unterschreiben, aufgrund dessen ein Kollege, mit dem Sie eigentlich ein gutes Verhältnis pflegen möchten, seinen Computer unbrauchbar macht?

4.2.11 Informationen

Zu dieser Thematik, mit der sich jeder befassen muss, der einen Rechner betreibt, finden Sie eingehende Informationen unter folgendem URL im Web-Angebot der GWDG:

`http://www.gwdg.de/service/sicherheit`

Unter der Rubrik „Computerviren“ gelangen Sie über sog. Links zu den Web-Seiten verschiedenen Antiviren-Programm-Hersteller, die Sie von Allgemein (Was kann man gegen Viren tun?) bis Speziell (Wie verhält sich ein bestimmter Virus, welchen Schaden richtet er an, wie lässt er sich beseitigen?) über Computerviren informieren. Besonders empfehlenswert ist das Angebot des Bundesamtes für Sicherheit in der Informationstechnik:

`http://www.bsi.de`

Über Hoaxes gibt das „Hoax-Info Newsletter-Archiv“ der TU Berlin besonders ausführlich Auskunft:

`http://www.tu-berlin.de/www/software/hoax/`

4.2.12 Die Situation in Göttingen

In den Instituten der Max-Planck-Gesellschaft wird generell und in den Instituten der Universität wird sicherlich auf 99% der PCs Antiviren-Software eingesetzt, denn diese Institutionen verfügen über entsprechende Campus-Lizenzen. Man kann die Programme über das Netz auf seinem Rechner installieren und teilweise auch an automatischer Aktualisierung teilnehmen.

Größere Virenvorfälle oder gar -Epidemien sind daher seit langer Zeit nicht mehr aufgetreten. Leider gibt es einzelne PC-Besitzer, die diesem Thema noch nicht die erforderliche Aufmerksamkeit schenken. Hier kommt es dann auch ab und an zum Virenunfall: manchmal totaler Datenverlust, meist aber ein großer bis sehr großer Zeitaufwand zur Wiederherstellung des Normalbetriebs.

Eyßell

---

5. Datenbanken

5.1 Die Max Planck Virtual Library und MPG-SFX

Seit dem 21. Oktober 2002 ist die **Max Planck Virtual Library (VLib)** freigeschaltet. Damit ging ein Informationsportal ans Netz, das – nach dem Prinzip des „One-Stop-Shop“ – eine Vielzahl dezentraler wissenschaftlicher Informationsressourcen unter einer gemeinsamen Suchoberfläche zugänglich macht. Zu erreichen ist die VLib unter

`http://vlib.mpg.de`

Dieses Angebot richtet sich insbesondere an Mitarbeiter und Gäste der Max-Planck-Gesellschaft und ermöglicht einen benutzerfreundlichen Zugang zu zahlreichen Informationsressourcen auf unterschiedlichen Plattformen und in vielfältigen Erscheinungsformen. Zu diesen Ressourcen zählen die Bibliothekskataloge der 75 verschiedenen Max-Planck-Institutsbibliotheken ebenso wie die von der MPG lizenzierten Datenbanken, ferner einige externe Bibliothekskataloge und eine Auswahl frei verfügbarer Datenbanken und Kataloge. Ein ebenfalls in das Informationsportal integrierter gemeinsamer Zeitschriftenkatalog der Max-Planck-Institute bietet einen Überblick über die in der MPG verfügbaren elektronischen und gedruckten Zeitschriftenbestände. Für Gastbenutzer ohne Zugangskennung ist mittels der VLib-Oberfläche eine Suche in einer Anzahl von frei verfügbaren Ressourcen – darunter die meisten der Bibliothekskataloge – möglich.

Zunächst geplant als gemeinsamer, jedoch verteilter Bibliothekskatalog für die Gesamtheit der Max-Planck-Institute – vom Konzept her vergleichbar mit der Suchmaschine des Kooperativen Bibliotheksverbundes Berlin-Brandenburg (KOBV) –, entwickelte sich im Verlauf des Projekts bald die Idee eines umfassenden Informationsportals, das nicht nur die Bibliothekskataloge, sondern möglichst alle für die MPG verfügbaren Informationsressourcen integrieren sollte.

Das Informationsportal Max Planck Virtual Library ist ein gemeinschaftliches Projekt verschiedener Gruppen innerhalb der Max-Planck-Gesellschaft,

an dem Vertreter der Bibliotheken und Informationsvermittlungsstellen, der Generalverwaltung, des Heinz Nixdorf Zentrums für Informationsmanagement in der Max-Planck-Gesellschaft (ZIM) sowie der GWDG beteiligt sind. Als Portalsoftware wird das Produkt Metalib der Firma Ex Libris verwendet; für die Beschaffung und Wartung der Hardware und die Systempflege ist die GWDG zuständig.

Die Max Planck Virtual Library bietet eine gleichzeitige Suchmöglichkeit in verschiedenen, heterogenen Ressourcen. Die Suchanfragen erfolgen in der Regel über das Z39.50-Protokoll. Bei Zielsystemen, die dieses Protokoll nicht unterstützen, kann eine Abfrage mittels des HTTP-Protokolls eingerichtet werden. Andere Ressourcen, die nicht auf diese Weise in die verteilte Suche eingebunden werden können, sind zumindest als Hyperlinks aus der VLib heraus erreichbar.

Das in die VLib-Oberfläche integrierte Max Planck Context Sensitive Linking ermöglicht eine direkte Lokalisierung des Volltextes – soweit Zugriff darauf besteht – sowie die Weiterbearbeitung des Suchergebnisses mit anderen verfügbaren Diensten. Hier ist die ebenfalls von Ex Libris vertriebene Software **SFX** im Einsatz. Dieser Service kann außerdem unter weiteren Suchoberflächen, z. B. OVID, genutzt werden.

Die Max Planck Virtual Library wird ständig weiter entwickelt. So wird demnächst die Personalisierung der Services weiter verbessert, und künftig sollen von hier aus auch auf lokale Ressourcen Fernzugriffe möglich sein. Ziel ist, Mitgliedern und Gästen der MPG Zugang zu allen verfügbaren wissenschaftlichen Ressourcen von überall aus anzubieten.

Nähere Informationen sind unter folgenden URLs zu finden:

http://www.gwdg.de/service/info-mpg/vlib

http://www.zim.mpg.de/projects/virtlib/index.html

Bruns

---

6. Peripherie

6.1 Farbdruck in Fotoqualität

Im letzten Jahr wurde der Betrieb des Farbsublimationsdruckers Mitsubishi S6800-40, der Grafiken im Format bis DIN-A3-Übergröße in Fotoqualität ausgeben konnte, eingestellt. Grund dafür war nicht der geringe Bedarf unserer Benutzer an einer derartigen Ausgabemöglichkeit, sondern vielmehr die zu hohen Verbrauchsmaterialkosten sowie die mittlerweile unzulänglichen Wartungsbedingungen. Als Ersatz wurde nun für den Bereich „Fotorealistischer Farbdruck“ von der GWDG ein thermischer Tintenstrahldrucker **HP Designjet 20PS** beschafft. Dieser Drucker ist hinsichtlich Verbrauchsmaterialkosten, Druckqualität und Einsatzmöglichkeit dem Sublimationsdrucker um einiges überlegen und stellt somit eine wesentliche Verbesserung dar.

Mit Hilfe des HP Designjet 20PS können Farbgrafiken in Foto- bzw. Offset-Druckqualität auf hochwertigem Fotopapier in den Formaten DIN A4 und DIN A3 ausgegeben werden. Insbesondere eignet er sich für besonders anspruchvolle Anwendungen wie z. B. für Vorlagen in der Druckvorstufe oder im Pre-Proof-Bereich.

Der HP Designjet 20PS verfügt über ein Sechsfarb-Tintensystem, das neben den vier Grundfarben Cyan, Magenta, Gelb und Schwarz zusätzlich noch die Farben Hell-Cyan und Hell-Magenta enthält. Das Drucksystem erreicht damit eine maximale Auflösung von 2400 dpi; verantwortlich dafür ist die hochentwickelte thermische Tintenstrahltechnik. So besitzt der Druckkopf für jede Farbe 304 Düsen, die kleinste Farbtröpfchen mit einem Volumen von bis zu vier Picolitern bei hoher Geschwindigkeit und äußerster Präzision auf das Medium Papier aufbringen. Durch Übereinanderplatzieren von bis zu 29 Tintentröpfchen auf einen Punkt - dem so genannten Color-Layering-Verfahren - gelingt es, ein überaus großes Farbspektrum aufs Papier zu bringen; 3500 echte Mischfarben sind so realisierbar. Selbst feine Linien werden scharf wiedergegeben und Farbübergänge gelingen sehr weich und harmonisch. Im Ergebnis entsteht eine feinkörnige Farbqualität, die das Niveau eines Offset-Drucks erreicht. Zudem sorgt ein integriertes automatisches Farbkalibrierungssystem für eine beständig gleichbleibende Farbqualität.

Der Drucker besitzt zwei Einzugsfächer, die bei der GWDG mit hochwertigem Fotopapier (240 g) in den Formaten DIN A4 und DIN A3 bestückt sind. Der auf dem Papier nicht bedruckbare Randbereich beträgt links und rechts jeweils 5 mm, oben 3 mm und unten 12 mm; damit verbleiben folgende **bedruckbare Bereiche**:

für DIN A4: 200 x 282 mm

für DIN A3: 287 x 405 mm

Der Drucker wird von einem Print-Server (PC unter Windows 2000) bedient. Mit der dort installierten RIP-Software (Raster Image Processor) werden die vom Benutzer abgeschickten Dateien bearbeitet und in das Ausgabeformat PCL3GUI für den Drukker umgewandelt. Der RIP unterstützt folgende **Datenformate**:

- PostScript (*.eps, *.ps, *.prn)
- PDF (*.pdf)
- JPEG (*.jpg)
- TIFF (*.tif)
- Windows-Bitmap (*.bmp)

In der Standardvoreinstellung werden die Bilder bzw. Grafiken auf die Größe des bedruckbaren Bereichs (s. o.) angepasst.

Gemäß der zwei Papierblattformate sind für den Drucker im Workstation-Cluster und PC-Netz der GWDG zwei **Druckerwarteschlangen** eingerichtet:

- **zcip4s20** für DIN A4, Fotopapier
- **zcip3s20** für DIN A3, Fotopapier

Unter UNIX können in diese Warteschlangen Dateien, die in einem der oben angegebenen Formaten geschrieben sind, zur weiteren Bearbeitung eingetragen werden; z. B. eine TIF-Datei **`bild27.tif`** mit dem Befehl

```
lpr -Pzcip4s20 bild27.tif
```

Unter Windows und Mac OS empfiehlt sich die Nutzung des im Netz von der GWDG bereitgestellten PostScript-Druckertreibers. Weitere Informationen dazu liefern folgende Internet-Seiten der GWDG:

Für Windows:

`http://www.gwdg.de/service/drucker/faq/index.html#Druckertreiber`

Für Mac OS:

`http://www.gwdg.de/service/drucker/faq/index.html#Drucken_MacOS`

Wegen der verhältnismäßig hohen Verbrauchsmaterialkosten pro Seite von 1 bis 2 Euro bei DIN A4 bzw. von 2 bis 4 Euro bei DIN A3 unterliegt das Drucken auf dem HP Designjet 20PS einer besonderen **Ablauforganisation**:

- Gedruckt wird nur im bedienten Betrieb, d. h. unter Aufsicht des Bedienpersonals der GWDG.
- Die Warteschlangen zcip4s20 und zcip3s20 werden nur für einzelne Dateien auf Anforderung des Benutzers freigegeben. Die engültige Ausgabe wird erst gestartet, nachdem der Benutzer die gewünschten Grafiken unter Angabe seiner Benutzeridentifikation, des Warteschlangen- und Dateinamens der GWDG mitgeteilt hat. Dies kann auf eine der drei folgenden Arten erfolgen: persönlich im Rechenzentrum bei der Information, telefonisch beim Schichtleiter der GWDG (Tel.: 0551/201-1543) oder mittels E-Mail an **`printservice@gwdg.de`**.
- Die erstellte Druckausgabe wird im Umschlag in das Ausgabefach des Benutzers abgelegt.
- Die Verweilzeit der Dateien in der Warteschlange beträgt maximal eine Woche; nicht abgeforderte Einträge werden danach aus der Warteschlange entfernt.

Als **Kosten** werden in Arbeitseinheiten (AE) berechnet:

150 mAE für eine DIN-A4-Seite

300 mAE für eine DIN-A3-Seite

Die wichtigsten technischen Daten des Druckers auf einen Blick:

Farbdrucker HP Designjet 20PS	
Druckverfahren	Thermischer Tintenstrahldrucker mit Sechsfarb-Tintensystem CMYKcm (Cyan, Magenta, Gelb, Schwarz, Hell-Cyan, Hell-Magenta)
Auflösung	für bestmögliche Druckqualität im Präsentations-Modus: Schwarz/Weiß: 600 x 600 dpi; Farbe: 2400 x 1200 dpi (Punkte/Zoll)
Druckzeit	2 Minuten pro Seite DIN A4, 4 Minuten pro Seite DIN A3,
Farbtechnologie	Offsetdruck-Emulation (SWOP, Euroscale, TOYO, DIC), ICC-Profile, RGB-Emulation, Automatische Farbkalibrierung
Speicher	16 MByte
Druckmedium	Hochglänzendes Fotopapier (240 g), Formate: DIN A4, DIN A3
Bedruckbarer Bereich	200 x 282 mm auf DIN-A4-Papier, 287 x 405 mm auf DIN-A3-Papier (Rand: links und rechts je 5 mm, oben 3 mm, unten 12 mm)
Druckersprache	PCL3GUI
Software	Adobe PostScript 3 mit HP-Software RIP
Unterstützte Formate	PostScript, PDF, JPEG, TIFF und Windows-Bitmap (BMP)

Wagenführ

---

7. Personalia

7.1 Neuer Mitarbeiter der GWDG

Seit dem 1. Februar 2003 ist Herr Uwe Nolte Mitarbeiter der GWDG. In der AG 3 „Wissenschaftliches Rechnen / Multimedia“ wird er für die Systemtechnik und Anwendungsumgebung der Service-PCs zuständig sein und Benutzerberatung im Bereich Grafikanwendungen und Druckausgabe durchführen.

Herr Nolte hat Physik und Mathematik an der Universität Göttingen studiert und das Physik-Diplom mit einer Arbeit aus dem Bereich der Astronomie im Jahre 1993 abgelegt. Vielen Nutzern der GWDG wird er gut bekannt sein durch seine Mitarbeit im DV-Bereich im MPI für Aeronomie und im Seminar für Ägyptologie und Koptologie der Universität Göttingen, als Softwareentwickler in der Gruppe Grubmüller des MPI für biophysikalische Chemie und vor allem als wissenschaftliche Hilfskraft bei der GWDG.

Bis zum 30. Juni 2003 arbeitet Herr Nolte halbtags, vorwiegend am Nachmittag, erst danach wird er eine volle Stelle besetzen. Sein Arbeitsplatz befindet sich im Zimmer U 37, er ist zu erreichen unter der Telefonnummer 0551/201-1547 und der E-Mail-Adresse unolte@gwdg.de.

Haan

8. Veranstaltungen

8.1 Kurse des Rechenzentrums von März bis April 2003

Datenbanksystem MS-Access, Einführung mit Übungen

(Dr. Th. Kneser)

Montag - Freitag, 3.3. - 7.3.2003, 9.00 - 12.00 Uhr

MS-Access ist sowohl für solche Anwender geeignet, die eine einfache Datenbank für den persönlichen Gebrauch erstellen wollen (Gruppe 1), als auch für IT-Fachleute, die eine komplexe Datenbank für eine größere Gruppe von Anwendern aufzubauen haben (Gruppe 2).

MS-Access bietet neben den herkömmlichen Datenmanagement-Tools Integrationsmöglichkeiten in das World Wide Web, um Datenaustausch über die Grenzen von Plattformen hinweg zu ermöglichen.

MS-Access-Datenbanken lassen sich z. B. bei höherem Sicherheitsbedarf in Datenbanken unter MS-SQL-Server übertragen, wobei die Oberfläche für den Anwender erhalten bleiben kann.

Der hier angekündigte Kurs vermittelt Kenntnisse für Anwender aus Gruppe 1 und behandelt dabei u. a. folgende Themen:

- Erstellen von Tabellen und Gliedern der Tabellen in Felder
- Definieren von Beziehungen
- Entwerfen von Abfragen
- Entwerfen von Formularen und Berichten
- Entwerfen von Makros
- Entwerfen von Datenbanken

Vorausgesetzt wird die Fähigkeit, die MS-Windows-Oberfläche zu handhaben.

Der Kurs findet im Kursraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Anmeldungen können bis zum 24.2.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **10** AE abgezogen.

UNIX für Fortgeschrittene

(Dr. R. Sippel)

Montag - Mittwoch, 3.3. - 5.3.2003, 9.15 - 12.00 Uhr und 13.00 - 15.30 Uhr

Der Kommandointerpreter der Korn-Shell umfaßt alle Elemente einer höheren Programmiersprache. Korn-Shell-Scripts und zahlreiche Hilfsprogramme bieten die Möglichkeit, String-Manipulation, Fileverarbeitung sowie die Programmierung komplizierter Algorithmen auf einfache Weise zu realisieren. Die Kursteilnehmer erwerben die Fähigkeit, eigenständig Korn-Shell-Scripts zu erstellen, mit deren Hilfe komplexe Programmabläufe gesteuert werden können.

Der Kurs umfasst folgende Themen:

- Grundlagen der Korn-Shell-Programmierung
- Verarbeitung von Standardeingabe und Standardausgabe
- Verarbeitung von Aufrufparametern
- Musterersetzung
- String-Manipulation
- Definition und Aufruf von Korn-Shell-Funktionen
- Hilfsprogramme zur Fileverarbeitung (sed, grep)
- Programm zur Tabellenverarbeitung (awk)
- Pipeline-Konzept
- Fehlerbearbeitung (Debugging)
- Verändern von Shell-Optionen

Die Teilnehmer sollten über Grundkenntnisse des Betriebssystems UNIX verfügen und mit einem UNIX-typischen Editor (z. B. vi oder Emacs) vertraut sein.

Der Kurs findet vormittags im Vortragsraum der GWDG statt; die Übungen werden an den Nachmittagen im Kursraum der GWDG, beides Am Faßberg, 37077 Göttingen-Nikolausberg, durchgeführt. Wegen der begrenzten Anzahl von Übungsplätzen ist die Teilnehmerzahl auf 15 beschränkt. Anmeldungen können bis zum 24.2.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **12** AE abgezogen.

Einführung in die Nutzung des Leistungsangebots der GWDG

(Dr. W. Grieger)

Mittwoch, 5.3.2003, 17.15 - 20.00 Uhr

Die GWDG ist das Hochschulrechenzentrum der Georg-August-Universität Göttingen und ein Rechen- und Kompetenzzentrum der gesamten Max-Planck-Gesellschaft. Der Kurs *„Einführung in die Nutzung des Leistungsangebots der GWDG“* soll sowohl die GWDG selber als auch ihr Leistungsangebot vorstellen und Wege beschreiben, die Dienstleistungen sinnvoll zu nutzen. Da es offensichtlich noch viele Wissenschaftler gibt, die

die GWDG gar nicht kennen oder sich scheuen, Dienstleistungen aus dem umfangreichen und deshalb vielleicht auch unübersichtlichen Angebot aus dem Bereich der Datenverarbeitung in Anspruch zu nehmen, richtet sich die Veranstaltung an diejenigen, die die GWDG und deren Dienstleistungen für die Universität Göttingen, die Max-Planck-Gesellschaft und andere wissenschaftliche Einrichtungen erstmalig kennenlernen wollen. Insbesondere können auch Studierende an dem Kurs teilnehmen. Aus diesem Grund werden auch keinerlei Kenntnisse und Erfahrungen auf dem Gebiet der Datenverarbeitung vorausgesetzt.

Der Kurs findet im gemeinsamen Schulungsraum von GWDG und SUB statt. Dieser befindet sich in der Niedersächsischen Staats- und Universitätsbibliothek, Platz der Göttinger Sieben 1, 37073 Göttingen, im Erdgeschoss. Eine Anmeldung sollte bis zum 26.2.2003 erfolgen. Abweichend von der sonstigen Regelung kann sie auch telefonisch unter der Nummer 201-1523 dem Dispatcher übermittelt werden. Die Teilnahme ist selbstverständlich kostenlos, es werden auch **keine** Arbeitseinheiten von den Institutskontingenten abgezogen.

Windows 2000 für Systembetreuer

(S. Quentin)

Montag - Dienstag, 10.3. - 11.3.2003, 9.15 - 12.30 Uhr und 13.30 - 16.00 Uhr

Dieser Kurs vermittelt Grundlagen für die Unterstützung des Betriebssystems Windows 2000 Professional und Server. Er wendet sich an Personen, die in ihrem Institut Systeme auf der Basis von Windows 2000 bzw. NT 4.0 betreuen.

Es werden u. a. folgende Themen behandelt:

- Überblick über die Architektur des Betriebssystems
- Installation
- Startvorgang
- NTFS-Dateisystem
- Konfiguration der Windows-2000-Umgebung
- Festplattenverwaltung und Ausfallsicherheit
- Systemüberwachung

Kenntnisse in der Bedienung von Windows-Oberflächen werden vorausgesetzt.

Der Kurs findet im Kursraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Anmeldungen können bis zum 3.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **8** AE abgezogen.

Bei Redaktionsschluss zeigte sich, dass dieser Kurs bereits vollständig belegt ist!

Administration von Windows-2000-Server und -Professional in der Active-Directory-Infrastruktur

(S. Quentin)

Mittwoch - Freitag, 12.3. - 14.3.2003, 9.15 - 12.15 Uhr und 13.30 - 16.00 Uhr

Der Kurs soll eine Einführung in die Administration und Konfiguration der Active Directory für Personen geben, die innerhalb ihrer Institute Windows-2000-Server und -Clients zu betreuen haben.

Folgende Themen werden behandelt:

- Einführung in Active-Directory-Services (ADS)
- Verwaltung/Management von Windows-2000-Client/Server
- Verwalten von Benutzerkonten
- Implementierung von Gruppenrichtlinien
- Bereitstellung von Software
- verteilte Ressourcen (Applikationen, Daten und Drucker im Netz)

Kenntnisse zu den im Kurs „*Windows 2000 für Systembetreuer*“ behandelten Themen sowie das im Kurs „*Grundlagen der Netzwerktechnik*" vermittelte Wissen werden vorausgesetzt.

Der Kurs findet im Kursraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Anmeldungen können bis zum 5.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **12** AE abgezogen.

Bei Redaktionsschluss zeigte sich, dass dieser Kurs bereits vollständig belegt ist!

Web Publishing II

(M. Reimann)

Montag - Dienstag, 17.3. - 18.3.2003, 9.15 - 12.00 Uhr und 13.30 - 15.30 Uhr

Gedacht als Fortsetzung des Kurses „*Web Publishing I*“ sollen hier einige Techniken zur Erstellung wirkungsvoller Web-Auftritte vertieft werden. Dabei werden der Einsatz von Stilvorlagen (CSS), die eine deutlichere Trennung von inhaltlicher Strukturierung und visueller Formatanweisung ermöglichen, ebenso zur Sprache kommen wie die Realisierung dynamischer Web-Inhalte durch client-seitige Skripttechniken.

Unter Berücksichtigung der in diesen Themenbereichen üblichen raschen Entwicklung sind folgende Kursinhalte geplant:

- Seitenrahmen (Frames)
- Stilvorlagen CSS (Cascading Style Sheets)

- fortgeschrittene Layouttechniken
- Realisierung dynamischer Web-Inhalte mit JavaScript
- Übungen an ausgewählten Beispielen

Anwenderkenntnisse in Windows und/oder UNIX und Grundkenntnisse in der Erstellung von Web-Seiten werden vorausgesetzt.

Der Kurs findet im Kursraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Anmeldungen können bis zum 10.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **8** AE abgezogen.

Grafik I: Grundlagen der grafischen Datenverarbeitung

(Dr. K. Heuer)

Montag, 17.3.2003, 13.30 - 16.30 Uhr

Grafische Datenverarbeitung steht für ein umfassendes Einsatzfeld von Rechenanlagen zur Erzeugung und Verarbeitung unterschiedlichster Grafiken. Die modular aufgebauten Kurse *„Grafik I“* bis *„Grafik IV“* versuchen, einen Einblick in verschiedene Aspekte dieses Gebiets zu vermitteln.

Grundlagen der grafischen Datenverarbeitung werden im ersten Teil *„Grafik I“* vorgestellt; Stichworte sind: Vektor- und Rastergrafik, grafische Dateiformate, Farbmodelle, Ausgabegeräte, führende Hardware- und Software-Hersteller, Kurzübersicht über grafische Anwendungssoftware und nützliche Hilfsprogramme. Hinzu kommt ein Ausblick auf die weiteren Kursteile. Empfohlen wird je nach Interesse der Besuch eines oder mehrerer der folgenden Kursteile *„Grafik II“* bis *„Grafik IV“*.

Der Kurs findet im Vortragsraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg**,** statt. Die Teilnehmerzahl ist auf 20 Personen beschränkt. Eine Anmeldung kann bis zum 10.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **2** AE abgezogen.

Grafik II: Drucken bei der GWDG - Wie geht das?

(Dr. K. Heuer)

Dienstag, 18.3.2003, 13.30 - 16.30 Uhr

Die GWDG bietet ihren Nutzern unterschiedlichste grafische Ausgabegeräte an, angefangen von Monochrom- und Farblaserdruckern über Großformatdrucker zur Postererstellung bis hin zur Farbdiaerstellung auf Filmrecordern.

Die Ansteuerung fast aller Geräte erfolgt mit zentraler Hard- und Software über Druckerwarteschlangen, die von vielen Client-Rechnern mit unterschiedlichen Betriebssystemen direkt beschickt werden können.

Der Kurs erläutert das Betriebskonzept der GWDG und versetzt die Teilnehmer in die Lage, die Warteschlangen und die dazu gehörigen Geräte auf ihren eigenen Arbeitsplatzrechnern oder auf GWDG-Rechnern zu nutzen. Hierbei wird dargestellt, welche Einfluss-, Einstell- und Kontrollmöglichkeiten bestehen, aber auch, welche Fehlerquellen zu beachten sind und wie Fehler vermieden werden können.

Vorausgesetzt werden Grundkenntnisse in mindestens einem der folgenden Betriebssysteme: MacOS, Windows (95/98/NT/2000), UNIX. Der Besuch des Kurses *„Grafik I“* am Vortag wird empfohlen.

Der Kurs findet im Vortragsraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Die Teilnehmerzahl ist auf 20 Personen beschränkt. Eine Anmeldung kann bis zum 11.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **2** AE abgezogen.

Grafik III: Zeichen- und Designprogramm CorelDRAW

(Dipl.-Math. H. Wagenführ)

Mittwoch - Donnerstag, 19.3. - 20.3.2003, 9.15 - 12.00 Uhr und 13.30 - 16.30 Uhr

CorelDRAW ist ein universelles Grafikprogrammsystem zum Anfertigen und Bearbeiten von Zeichnungen. Für die Bereiche Grafik, Gestaltung und Darstellung hat sich CorelDRAW als eines der wichtigsten Werkzeuge etabliert.

Der Kurs gibt einen Einstieg in die vielseitigen Möglichkeiten von CorelDRAW. Stichworte sind: Werkzeuge, Freihandzeichnen, geometrische Figuren, Text, Clip-Art und Symbole, Import und Export von Grafiken, Dateiverwaltung, Objektbearbeitung, Drucken.

An einfachen Beispielen werden die wichtigsten Werkzeuge von CorelDRAW vorgestellt. Die erworbenen Kenntnisse werden durch praktische Übungen am Rechner vertieft. Elementare Kenntnisse von Windows-Oberflächen werden vorausgesetzt.

Der Kurs findet im Kursraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Die Teilnehmerzahl ist auf 18 Personen beschränkt. Eine Anmeldung kann bis zum 12.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **8** AE abgezogen.

Grafik IV: Präsentationen - Poster, Dia, Folie

(Dipl.-Math. H. Wagenführ)

Freitag, 21.3.2002, 9.15 - 12.00 Uhr

Der Kurs gibt Anleitungen zur Erstellung von Präsentationen auf dem Rechner; folgende Präsentationsformen bzw. Ausgabemedien werden berücksichtigt:

- großformatiger Druck, Poster
- Farbdiapositiv
- Transparentfolie
- Bildschirmpräsentation

Neben den grundsätzlichen Kriterien hinsichtlich Darstellung und Design wird insbesondere die Steuerung der Ausgabe anhand einfacher Beispiele unter MS-Windows (CorelDRAW, PowerPoint) erläutert. Elementare Kenntnisse von Windows-Oberflächen werden vorausgesetzt.

Der Kurs findet im Vortragsraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Die Teilnehmerzahl ist auf 18 Personen beschränkt. Eine Anmeldung kann bis zum 14.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **2** AE abgezogen.

Führung durch das Rechnermuseum

(Dipl.-Ing. M. Eyßell)

Freitag, 21.3.2003, 10.00 - 12.00 Uhr

Die GWDG hat 1980 mit dem Aufbau einer Sammlung begonnen, die einen Überblick über die Entwicklungsgeschichte von Rechenanlagen geben soll. Die Sammlung besteht aus einigen vollständigen Rechnerkomponenten, die in der Eingangshalle ausgestellt sind, sowie einer großen Zahl von kleineren Objekten, die in den Gängen gezeigt werden. Die Exponate zeigen die Entwicklung der Technologie von Schaltkreisen, Speichern, Ein- und Ausgabegeräten von den Anfängen bis zum aktuellen Stand der Datenverarbeitungstechnik auf.

Das Angebot der Führung durch das Rechnermuseum wendet sich an Benutzer, die über die vorgenommenen Beschriftungen der Ausstellungsstücke hinausgehende Informationen haben wollen, sich für die Funktion der Teile interessieren und die Einordnung der Exponate in die Entwicklungsgeschichte der Datenverarbeitungstechnik erklärt bekommen möchten.

Treffpunkt: Eingangshalle der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg. Anmeldungen können bis zum 14.3.2003 erfolgen. Vom Institutskontingent werden **keine** Arbeitseinheiten abgezogen.

Anwendungen in Lotus Notes

(S. Greber, Dr. W. Grieger)

Dienstag - Mittwoch, 25.3. - 26.3.2003, 9.15 - 16.30 Uhr

Die Verwendung von Groupware-Lösungen in den wissenschaftlichen Instituten und Abteilungen wird auf Grund der zunehmenden Datenvielfalt und Datenkomplexität immer wichtiger. Ein Groupware-System wird von der Firma IBM mit dem Software-Produkt Lotus Notes/Domino angeboten, das in diesem Kurs vorgestellt werden soll. Weiter bietet die GWDG den zugehörigen Server-Dienst auch allen Instituten an.

Die folgenden Themen werden behandelt:

- Was ist Groupware?
- das Lotus-Notes/Domino-System
- Terminplanung, Gruppenkalender
- Aufgaben-, Adressverwaltung
- Synchronisation mit PDAs

Darüber hinaus werden zur Verwaltung von Dokumenten jeglicher Art innerhalb des Lotus-Notes/Domino-Systems spezielle Datenbanken verwendet. Jede Datenbank kann verschieden gestaltet werden:

- Gestaltungselemente mit dem Domino Designer
- Veröffentlichung der Datenbanken im WWW

Elementare Kenntnisse von Windows-Oberflächen werden vorausgesetzt.

Der Kurs findet im Kursraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Anmeldungen können bis zum 18.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **8** AE abgezogen.

Installation und Administration von UNIX-Systemen

(Dr. K. Heuer, Dr. R. Sippel)

Dienstag - Freitag, 1.4. - 4.4.2003, 9.30 - 12.00 Uhr und 13.30 - 16.30 Uhr

Ziel des Kurses ist es, die Teilnehmer zu befähigen, UNIX-Systeme zu installieren und zu administrieren. Der Kurs ist als eine allgemeine Einführung konzipiert und beschränkt sich nicht auf spezielle UNIX-Derivate.

Berücksichtigte Systeme sind, in alphabetischer Reihenfolge, AIX, Compaq/Tru64 UNIX, FreeBSD, IRIX, Linux und Solaris.

Folgende Themen werden angesprochen:

- Aufbau von UNIX-Systemen
- Dateisysteme
- Installationsvorgang
- Kernel-Anpassung
- systemnahe Werkzeuge
- Konfigurationsdateien
- Netzwerkkonfiguration
- Benutzerverwaltung
- Konfiguration des X-Window-Systems
- Run-Level / Single- und Multi-User-Mode
- System-Startup-Prozeß
- Systemsicherheit
- Backup-Verfahren

Die Vorträge werden durch Übungen ergänzt, bei denen die Teilnehmer Gelegenheit haben, Erlerntes auszuprobieren und zu vertiefen. Gute UNIX-Grundkenntnisse werden vorausgesetzt.

Der Kurs findet vormittags im Vortragsraum und an den Nachmittagen im Kursraum der GWDG statt, beides Am Faßberg, 37077 Göttingen-Nikolausberg. Anmeldungen können bis zum 25.3.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **16** AE abgezogen.

Grundkurs UNIX/Linux mit Übungen

(Dipl.-Phys. J. Hattenbach)

Dienstag - Donnerstag, 8.4. - 10.4.2003, 9.15 - 12.00 Uhr und 13.30 - 16.00 Uhr

Der Kurs bietet Anfängern eine grundlegende Einführung in einfache Arbeiten unter Betriebssystemen der UNIX-Familie. Dabei wird versucht, eine gemeinsame Basis der unterschiedlichen UNIX-Systeme auf den Workstations der GWDG darzustellen. Die Einführung umfaßt folgende Themen:

- Struktur eines UNIX-Systems, Prozesse
- die Korn-Shell als einfache Kommandooberfläche
- die allgemeine Kommandosyntax
- das hierarchische Filesystem
- die Benutzung des Editors Emacs
- einige nützliche UNIX-Kommandos
- die Verknüpfung von Prozessen, Pipelines
- Hintergrundprozesse
- einfache Programmierung der Korn-Shell, Profiles
- Testen eigener C- und Fortran-Programme

Die Übungen finden auf einer DECalpha-Station unter dem Betriebssystem Digital UNIX, vormals OSF/1, statt und sollen die vorgetragenen Themen vertiefen.

Der Kurs findet vormittags im Großen Seminarraum des Max-Planck-Instituts für biophysikalische Chemie statt; die praktischen Übungen werden mit maximal 16 Teilnehmern an den Nachmittagen im Kursaum der GWDG, beides Am Faßberg, 37077 Göttingen-Nikolausberg, durchgeführt. Anmeldungen können bis zum 1.4.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **12** AE abgezogen.

PowerPoint

(M. Reimann)

Donnerstag - Freitag, 24.4. - 25.4.2003, 9.15 - 12.00 Uhr und 13.30 - 15.30 Uhr

Ziel dieses Kurses ist der wirkungsvolle Aufbau einer Folien-Präsentation zur Begleitung eines wissenschaftlichen Vortrages. Dabei sollen die Erstellung von Entwurfsvorlagen, die Aufbereitung und Einbindung von Grafiken ebenso behandelt werden wie die verschiedenen Präsentationsmöglichkeiten und natürlich Fragen zum themen- und zielgruppenorientierten Layout und Design.

Folgende Themen sind geplant:

- Einsatzbereich von Präsentationen
- das Zusammenspiel von PowerPoint und MS-Office
- grundlegende Arbeitstechniken
- Gestaltungstipps und inhaltliche Konzeption einer Präsentation
- Erstellen von Entwurfsvorlagen und Präsentationslayout
- Erstellen und Einbinden von Diagrammen, Illustrationen und Zeichenobjekten
- Einsatz von Animationseffekten
- Bildschirm- und Internet-Präsentationen

Der Kurs findet im Kursraum der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg, statt. Anmeldungen können bis zum 17.4.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent 8 AE abgezogen.

Führung durch das Rechnermuseum
(Dipl.-Ing. M. Eyßell)

Freitag, 25.4.2003, 10.00 - 12.00 Uhr

Die GWDG hat 1980 mit dem Aufbau einer Sammlung begonnen, die einen Überblick über die Entwicklungsgeschichte von Rechenanlagen geben soll. Die Sammlung besteht aus einigen vollständigen Rechnerkomponenten, die in der Eingangshalle ausgestellt sind, sowie einer großen Zahl von kleineren Objekten, die in den Gängen gezeigt werden. Die Exponate zeigen die Entwicklung der Technologie von Schaltkreisen, Speichern, Ein- und Ausgabegeräten von den Anfängen bis zum aktuellen Stand der Datenverarbeitungstechnik auf.

Das Angebot der Führung durch das Rechnermuseum wendet sich an Benutzer, die über die vorgenommenen Beschriftungen der Ausstellungsstücke hinausgehende Informationen haben wollen, sich für die Funktion der Teile interessieren und die Einordnung der Exponate in die Entwicklungsgeschichte der Datenverarbeitungstechnik erklärt bekommen möchten.

Treffpunkt: Eingangshalle der GWDG, Am Faßberg, 37077 Göttingen-Nikolausberg. Anmeldungen können bis zum 18.4.2003 erfolgen. Vom Institutskontingent werden **keine** Arbeitseinheiten abgezogen.

SAS - Grundlagen
(Dipl.-Math. H. Wagenführ)

Montag - Mittwoch, 28.4. - 30.4.2003, 9.15 - 12.00 Uhr und 13.30 - 16.30 Uhr

SAS (Statistical Analysis System) ist ein universelles Programmsystem, das mit gleicher Benutzeroberfläche und gleicher Syntax sowohl auf Großrechnern und Workstations als auch auf Personal Computern läuft. In einem System integriert SAS u. a. Datenspeicherung, Datenzugriff, Datenverwaltung, Abfrage und Änderung von Daten, vielfältige Möglichkeiten der Datenanalyse, Berichterstellung und die grafische Darstellung. Als höhere Programmiersprache mit umfangreichen Makromöglichkeiten unterstützt SAS den Anwendungsprogrammierer. Eine Vielzahl einfach zu handhabender Anwendungsroutinen (Prozeduren) für verschiedene Anwendungsbereiche erleichtert die Arbeit. Insbesondere sind für den Bereich der statistischen Datenanalyse die wichtigsten Verfahren, wie z. B. Regressions-, Varianz-, Faktoren-, Diskriminanz-, Clusteranalyse etc., in Form von SAS-Prozeduren realisiert.

Der Kurs vermittelt einen Überblick über die vielseitigen Möglichkeiten des SAS-Systems. Anhand einfacher Beispiele werden die grundlegenden Bestandteile eines SAS-Jobs vorgestellt; dabei werden die Logik der Programmverarbeitung und das Konzept der SAS-Dateien eingehend erläutert. Weitere Themen sind Anweisungen und Prozeduren des SAS-Systems für Informationsrückgewinnung, Datenmanagement und statistische Auswertung.

Der Besuch des Kurses empfiehlt sich sowohl für neue Anwender als auch für Anwender, die bereits Grundkenntnisse im SAS-System besitzen und diese erweitern wollen. Die Teilnehmer sollten über elementare Datenverarbeitungskenntnisse und Grundkenntnisse zu einem Betriebssystem verfügen.

Der Kurs findet vormittags im Vortragsraum und nachmittags mit praktischen Übungen im Kursraum der GWDG, beides am Faßberg, 37077 Göttingen-Nikolausberg, statt. Anmeldungen können bis zum 21.4.2003 erfolgen. Pro Teilnehmer werden vom zugehörigen Institutskontingent **12** AE abgezogen.

8.2 Kurse des Rechenzentrums von Mai bis Dezember 2003

Die Teilnahme ist für die Mitarbeiter aus Instituten der Universität Göttingen und der Max-Planck-Gesellschaft im Rahmen der Kontingentierungsregelung für die Inanspruchnahme von Leistungen der GWDG möglich. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

Anmeldungen können per Brief oder per Fax unter der Nummer 0551-21119 an die

GWDG
Kursanmeldung
Postfach 2841
37018 Göttingen

oder per E-Mail an die Adresse auftrag@gwdg.de mit der Subject-Angabe „Kursanmeldung“ erfolgen.

Wegen der Einbeziehung der Kurse in das Kontingentierungssystem der GWDG können telefonische Anmeldungen nicht vorgenommen werden. Eine schriftliche Anmeldung durch den Gruppenmanager oder Geschäftsführenden Direktor des zugehörigen Instituts ist erforderlich. Die Anmeldefrist endet jeweils 7 Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit dem Dispatcher (Tel.: 0551-201-1523, E-Mail: auftrag@gwdg.de) möglich.

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu 8 Tagen vor Kursbeginn erfolgen. Bei späteren Absagen werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht.

Aktuelle kurzfristige Informationen zu den Kursen sind im WWW unter dem URL

`http://www.gwdg.de/service/kurse`

bei den Monatsübersichten zu beachten.

Kurs	Vortragende	Termin	AE
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	5.5.03 9.15 - 12.30 Uhr	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	6.5.03 9.15 - 12.30 und 13.30 - 16.15 Uhr	4
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	9.5.03 9.15 - 12.00 Uhr	2
Excel für Anfänger	Hame	13.5. - 14.5.03 9.15 - 12.00 und 14.00 - 16.00 Uhr	8
Programmierung von Parallelrechnern	Prof. Haan, Dr. Schwardmann	19.5. - 21.5.03 9.15 - 12.15 und 14.00 - 17.00 Uhr	12
Photoshop für Fortgeschrittene	Töpfer	22.5. - 23.5.03 9.30 - 16.00 Uhr	8
Führung durch das Rechnermuseum	Eyßell	23.5.03 10.00 - 12.00 Uhr	0
Einführung in das Computeralgebra-System Mathematica	Dr. Schwardmann	27.5. - 28.5.03 9.00 - 12.00 und 14.00 - 16.00 Uhr	8
Einführung in SPSS	Hame	3.6.03 9.15 - 12.00 und 14.00 - 16.00 Uhr	4
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	4.6.03 17.15 - 20.00 Uhr	0
Sicherheit im Internet für Anwender	Reimann	5.6. - 6.6.03 9.15 - 12.00 und 13.30 - 15.30 Uhr	8
Grundkurs UNIX/Linux mit Übungen	Hattenbach	17.6. - 19.6.03 9.15 - 12.00 und 13.30 - 16.00 Uhr	12
Datenschutz - Verarbeitung personenbezogener Daten auf den Rechenanlagen der GWDG	Dr. Grieger	20.6.03 9.15 - 12.00 Uhr	2
Führung durch das Rechnermuseum	Eyßell	20.6.03 10.00 - 12.00 Uhr	0
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	30.6.03 9.15 - 12.30 Uhr	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	1.7.03 9.15 - 12.30 und 13.30 - 16.15 Uhr	4
Outlook	Reimann	3.7. - 4.7.03 9.15 - 12.00 und 13.30 - 15.30 Uhr	8
PDF-Dateien: Erzeugung und Bearbeitung	Dr. Baier, Koch	8.7. - 9.7.03 9.15 - 12.00 und 13.00 - 15.00 Uhr	8
Grundlagen der Bildbearbeitung mit Photoshop	Töpfer	21.8. - 22.8.03 9.30 - 16.00 Uhr	8
Führung durch das Rechnermuseum	Eyßell	22.8.03 10.00 - 12.00 Uhr	0
Einführung in die Programmiersprache Fortran 90/95	Dr. Schwardmann	25.8. - 26.8.03 9.00 - 12.00 und 14.00 - 16.00 Uhr	8
Web Publishing I	Reimann	28.8. - 29.8.03 9.15 - 12.00 und 13.30 -15.30 Uhr	8
Grundkurs UNIX/Linux mit Übungen	Hattenbach	2.9. - 4.9.03 9.15 - 12.00 und 13.30 - 16.00 Uhr	12
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	3.9.03 17.15 - 20.00 Uhr (Schulungsraum der SUB)	0
Arbeiten mit CAD, Grundlagen	Witt	8.9. - 12.9.03 8.30 - 16.00 Uhr (am 08.09. ab 10.00 Uhr, am 12.09. bis 14.00 Uhr)	20
Windows 2000 für Systembetreuer	Quentin	15.9. - 16.9.03 9.15 - 12.30 und 13.30 - 16.00 Uhr	8
Administration von Windows-2000-Server und -Professional in der Active-Directory-Infrastruktur	Quentin	17.9. - 19.9.03 9.15 - 12.15 und 13.30 - 16.00 Uhr	12
Führung durch das Rechnermuseum	Eyßell	19.9.03 10.00 - 12.00 Uhr	0
Methoden und Werkzeuge der Gensequenzanalyse: GCG, EMBOSS, STADEN	Dr. Bohrer, Dr. Liesegang	22.9. - 25.9.03 9.30 - 12.30 und 13.30 - 16.30 Uhr	16
Das Internet als Werkzeug für die Biowissenschaften	Dr. Liesegang	26.9.03 9.30 - 12.30 und 13.30 - 16.00 Uhr	4
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	29.9.03 9.15 - 12.30 Uhr	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	30.9.03 9.15 - 12.30 und 13.30 - 16.15 Uhr	4

Kurs	Vortragende	Termin	AE
Web Publishing II	Reimann	1.10. - 2.10.03 9.15 - 12.00 und 13.30 - 15.30 Uhr	8
Programmierung von Parallelrechnern	Prof. Haan, Dr. Schwardmann	6.10. - 8.10.03 9.15 - 12.15 und 14.00 - 17.00 Uhr	12
Führung durch das Rechnermuseum	Eyßell	10.10.03 10.00 - 12.00 Uhr	0
Anwendungen in Lotus Notes	Greber, Dr. Grieger	14.10. - 15.10.03 9.15 - 16.30 Uhr	8
Grafik I: Grundlagen der grafischen Datenverarbeitung	Dr. Heuer	20.10.03 13.30 - 16.30 Uhr	2
Grafik II: Drucken bei der GWDG - Wie geht das?	Dr. Heuer	21.10.03 13.30 - 16.30 Uhr	2
Grafik III: Zeichen- und Designprogramm CorelDRAW	Wagenführ	22.10. - 23.10.03 9.15 - 12.00 und 13.30 - 16.30 Uhr	8
Grafik IV: Präsentationen - Poster, Dia, Folie	Wagenführ	24.10.03 9.15 - 12.00 Uhr	2
Datenbanksystem MS-Access, Einführung mit Übungen	Dr. Kneser	27.10. - 31.10.03 9.00 - 12.00 Uhr	10
UNIX für Fortgeschrittene	Dr. Sippel	27.10. - 29.10.03 9.15 - 12.00 und 13.00 - 15.30 Uhr	12
XML	Reimann, Koch	4.11. - 6.11.03 9.15 - 12.00 und 13.30 - 15.30 Uhr	12

Kurs	Vortragende	Termin	AE
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	7.11.03 9.15 - 12.00 Uhr	2
Grundkurs UNIX/Linux mit Übungen	Hattenbach	11.11. - 13.11.03 9.15 - 12.00 und 13.30 - 16.00 Uhr	12
Führung durch das Rechnermuseum	Eyßell	14.11.03 10.00 - 12.00 Uhr	0
Photoshop für Fortgeschrittene	Töpfer	25.11. - 26.11.03 9.30 - 16.00 Uhr	8
Sicherheit im Internet für Anwender	Reimann	27.11. - 28.11.03 9.15 - 12.00 und 13.30 - 15.30 Uhr	8
SAS - Grundlagen	Wagenführ	2.12. - 4.12.03 9.15 - 12.00 und 13.30 - 16.30 Uhr	12
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	3.12.03 17.15 - 20.00 Uhr	0
Installation und Administration von UNIX-Systemen	Dr. Heuer, Dr. Sippel	9.12. - 12.12.03 9.30 - 12.00 und 13.30 - 16.30 Uhr	16
Führung durch das Rechnermuseum	Eyßell	12.12.03 10.00 - 12.00 Uhr	0
PowerPoint	Reimann	16.12. - 17.12.03 9.15 - 12.00 und 13.30 - 15.30 Uhr	8

9. Autoren dieser Ausgabe

Name	Artikel	E-Mail-Adresse	Telefon-Nr.
Dr. Holger Beck	• Neue Nameserver im GÖNET • Verschlüsselung von Dateien auf NTFS-Dateisystemen	hbeck@gwdg.de	0551/201-1554
Anke Bruns	• Die Max Planck Virtual Library und MPG-SFX	abruns1@gwdg.de	0551/201-1519
Manfred Eyßell	• Aktuelle Viren, Würmer und Trojaner	meyssel@gwdg.de	0551/201-1539
Prof. Dr. Oswald Haan	• Neuer Mitarbeiter der GWDG	unolte@gwdg.de	0551/201-1547
Thomas Körmer	• Video-Server der GWDG	tkoerme@gwdg.de	0551/201-1555
Dr. Thomas Otto	• Meilenstein auf dem Weg zur Langzeit-Archivierung: Inbetriebnahme eines verteilten Bandroboter-Systems am 28.1.2003	totto@gwdg.de	0551/201-1828
Stefan Quentin	• Verschlüsselung von Dateien auf NTFS-Dateisystemen	squenti2@gwdg.de	0551/201-1816
Michael Reimann	• Verschlüsselung mit OpenSource-Software	mreiman1@gwdg.de	0551/201-1826
Harald Wagenführ	• Farbdruck in Fotoqualität	hwagenf@gwdg.de	0551/201-1537