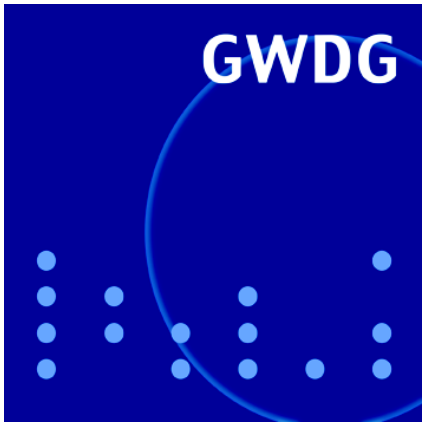



**Sicherheit im GÖNET**

**Sicherheitskonzept für Notebooks**

**Sicherheitslöcher und Software-Aktualisierung**

**ArcGIS 9.0**

# GWDG Nachrichten

# 10 / 2004

**Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen**

## Inhaltsverzeichnis



**GWDG-Nachrichten für die Benutzer des Rechenzentrums**

**ISSN 0940-4686**

27. Jahrgang, Ausgabe 10 / 2004

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

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

Redaktion und Herstellung: Dr. Thomas Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de

## 1. Neue Informationen zur Sicherheit in Netzen

Sicherheitsvorfälle in Datennetzen durch Viren, Würmer und Trojanische Pferde sind eine Plage, von der weder das GÖNET noch die Max-Planck-Institute verschont geblieben sind. In den GWDG-Nachrichten wurde darüber schon wiederholt berichtet. Fast alle Vorfälle hätten vermieden werden können, wenn rechtzeitig Vorsorgemaßnahmen ergriffen worden wären. Auch im September 2004 kam es wieder zu einer Einbruchsserie, bei der ca. 20 Rechner im GÖNET betroffen waren. Dabei wurden einmal mehr Nachlässigkeiten der Rechnerbetreiber (fehlende oder zu schwache Kennwörter und fehlende Softwarekorrekturen) ausgenutzt, um Rechner im GÖNET als Umschlagplatz von Hackergruppen zu missbrauchen.

Die GWDG hat mit Informationsveranstaltungen, Workshops, Schulungen, WWW-Angeboten, Sicherheitsdiensten und Artikeln in den GWDG-Nachrichten Administratoren und Endnutzer beim Selbstschutz vor Gefahren in der vernetzten IT-Landschaft unterstützt. Jetzt stellt die GWDG hierzu zwei weitere Papiere zur Verfügung:

1. An den „normalen“ Netzwerkteilnehmer richtet sich das Faltblatt „Sicherheit im GÖNET - Sicherheitshinweise für Netzteilnehmer im GÖNET“. Wir möchten darin auch die EDV-Laien für die vorhandenen Sicherheitsprobleme sensibilisieren und ihnen mit kurzen Texten Hilfen an die Hand geben, die wichtigsten Sicherheitsvorkehrungen treffen zu können.

   Dieses Faltblatt ist nachstehend in der aktuellen Version 1.0 abgedruckt und bei der GWDG in gedruckter Form oder elektronisch unter

   **`http://www.gwdg.de/service/sicherheit/info/faltblatt.pdf`**

   erhältlich. Zwei Exemplare sind dieser Ausgabe der GWDG-Nachrichten zusätzlich beigefügt.

2. In vielen Fällen konnten die Schädlinge in die Netze eindringen, weil diese durch Notebooks und andere mobile Rechner eingeschleppt wurden. Die GWDG hat daher zusätzlich ein Sicherheitskonzept für solche Rechner verfasst.

   Das „Sicherheitskonzept für Notebooks und andere mobile Rechner“ richtet sich an Netzwerkbetreuer und Administratoren. Es ist auf dem WWW-Server der GWDG unter

   **`http://www.gwdg.de/service/sicherheit/info/notebookkonzept.html`**

   zu finden und wird ebenfalls nachfolgend abgedruckt.

Beck

---

## 2. Sicherheit im Netz – Sicherheitshinweise für Netzteilnehmer im GÖNET

### 2.1 Auch Ihr Rechner ist gefährdet

Rechner am Internet sind vielfältigen Gefährdungen ausgesetzt.

- **Viren und Würmer** gefährden die Stabilität und Integrität der Rechner und Netze.
- **Trojanische Pferde** werden von Viren und Würmern hinterlassen und von Internetseiten unbeabsichtigt heruntergeladen und spähen vertrauliche Informationen (Kennwörter, Kreditkarteninformationen, Banktransaktionen, …) aus.
- Einbrecher (**Hacker**) dringen über Schwachstellen im Betriebssystem oder über schon vorhandene Trojanische Pferde in Rechner ein, um dort vorhandene Daten auszuspähen oder Rechner zu missbrauchen.

Auch GÖNET-Teilnehmer erleben immer öfter böse Überraschungen, wenn ihr Rechner wegen solcher Kompromittierungen nicht mehr funktionsfähig ist, der Rechner nicht mehr genutzt werden kann und die Wiederherstellung viel Zeit kostet.

Weitergehende Schäden haben die bisherigen Angriffe glücklicherweise nicht verursacht. Aber schon

- **die nächste Virenattacke** könnte nicht nur Netze und Mailserver überlasten, sondern zu Totalverlusten von Daten führen,
- **das nächste Trojanische Pferd** könnte Zugriff auf sensible Daten erlauben,
- **der nächste Einbrecher** könnte Ihren Rechner nicht nur als illegale Tauschbörse für Filme und Software, sondern auch als Server für Kinderpornographie missbrauchen und Sie müssen beweisen, dass Sie den nicht selbst eingerichtet haben.

Nachstehend wollen wir Ihnen Informationen geben, die Ihnen helfen, Ihren Rechner vor solchen Gefahren zu schützen.

**Denken Sie daran: Wenige Minuten genügen, um Ihren Rechner zu schützen.**

## 2.2 Sichere Konfiguration und Umgang

Stellen Sie das Betriebssystem und Anwendungen so ein, dass Ihr Rechner Schadprogrammen und Angreifern möglichst **wenig Angriffsfläche** bietet! Installieren Sie nur die benötigten Dienste!

Stellen Sie sicher, dass für alle Benutzer, insbesondere aber für Benutzer mit Administrationsrechten nicht zu erratende **Kennwörter** verwendet werden! Ein Angreifer kann tausende Kennwörter in Sekundenbruchteilen ausprobieren.

Konfigurieren Sie **Netzwerkanwendungen** wie **Internetbrowser** oder **Mailprogramm** so, dass auf WWW-Seiten oder in Mails enthaltene Programme nicht ungewollt und unbemerkt ausgeführt werden können! Hinweise, wie Sie die gängigen Programme einrichten sollten, finden Sie unter

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

### 2.2.1 Software-Update

Moderne Software ist so komplex, dass sie nicht fehlerfrei sein kann. Softwarefehler werden immer wieder von Viren und Würmern wie auch Hackern als Angriffpunkte genutzt.

Softwarehersteller veröffentlichen immer wieder Korrekturen für solche Fehler. Diese Korrekturprogramme (Patches) müssen so zeitig wie möglich installiert werden, um zu verhindern das neue Viren oder Angriffsprogramme diese Fehler innerhalb kürzester Zeit ausnutzen.

Für einige Betriebssysteme – insbesondere für die neueren Windows-Versionen – bieten die Hersteller automatische Installationen dieser Korrekturen über das Internet an. **Nutzen Sie möglichst diese Dienste und aktualisieren Sie Betriebssystem und Software!**

Für Windows ab Version 2000 können Sie den **Software-Update-Server der GWDG** nutzen (siehe **`http://sus.gwdg.de`**). Bei älteren Windows-Betriebssystemen müssen Sie Korrekturen manuell installieren. Informationen hierzu finden Sie unter

**`http://www.gwdg.de/service/sicherheit/aktuell/sec-inst.html`**

## 2.3 Viren, Würmer, Trojanische Pferde

Das Land Niedersachsen wie auch die Max-Planck-Gesellschaft haben **Sammellizenzen für Antivirensoftware** erworben. Die entsprechende Software kann daher auf allen dienstlich genutzten Rechnern sowie auf den Rechnern aller Studierenden der Universität eingesetzt werden.

**Schützen Sie sich, indem Sie dieses Angebot nutzen!**

Neue Schädlinge werden fast täglich in Umlauf gesetzt. Nur ständig aktualisierte Antivirensoftware kann daher den nötigen Schutz bieten.

**Halten Sie Ihre Antivirensoftware aktuell!**

Die von der Max-Planck-Gesellschaft und von der Universität Göttingen lizenzierte Software sowie Beschreibungen für die Installation und Aktualisierung derselben finden Sie unter

**`http://antivir.gwdg.de`**

Viele Viren werden über Massenmails verteilt. Gehen Sie **vorsichtig mit Mailanhängen** um! Öffnen Sie diese nur, wenn Sie sich über die Herkunft und den Inhalt im Klaren sind!

Der **Mailserver der GWDG** filtert alle mit bekannten Viren behafteten Mails aus. Nutzen Sie den Mailserver der GWDG oder einen anderen Mailserver, der Sie vor Viren schützt!

Manche Würmer dringen über von Virenscannern nicht überwachte Schnittstellen in den Rechner ein. Lassen Sie den Virenscanner daher **regelmäßig die Festplatte nach Viren durchsuchen!**

**Nicht alle Internetseiten sind seriös**. Wegen eines unsicher konfigurierten Browsers können Sie sich daher Trojanische Pferde und andere Schädlinge einhandeln. Viele dieser Schädlinge kann ein regelmäßiger Virenscan finden. Noch wichtiger ist, einen sicheren bzw. sicher konfigurierten Browser zu benutzen. Hinweise dazu finden Sie unter

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

## 2.4 Personal Firewall

Angreifer aus dem Internet schlagen oft schneller zu, als die Nutzer die nötigen Softwarekorrekturen (gerade bei neuen Rechnern) aus dem Netz herunter laden können. Hier – und generell als zusätzliche Verteidigungslinie – hilft ein „Personal Firewall“ genanntes Filterprogramm, das Zugriffe aus dem Netz heraus abwehrt.

Mit Windows XP und Windows 2003 wird eine solche Firewall mitgeliefert. Für ältere Windows-Versionen gibt es frei verfügbare Firewalls. Auch andere Betriebssysteme bieten entsprechende Filterprogramme an.

Anleitungen und weitere Informationen finden Sie unter

**`http://www.gwdg.de/service/sicherheit/aktuell/persfw.html`**

**Nutzen Sie die verfügbaren Firewallfunktionalitäten**, um eine Grundsicherung der Rechner zu erreichen!

### 2.5 Firewallfunktionen im GÖNET

Angriffe aus dem Internet oder auch von infizierten Rechnern im GÖNET können auch an den Vermittlungsstellen (Routern) des GÖNET abgewehrt werden.

Für die meisten Rechner lässt sich mit wenigen Regeln der Schutz gegenüber Angriffen erheblich verbessern. Die GWDG bietet den Instituten an, den Bedürfnissen der Institute angepasste Regeln auszuarbeiten und zu implementieren.

Sprechen Sie uns an (Kontakt: itsz@gwdg.de) und **nutzen Sie diese Schutzfunktionen!**

### 2.6 Private IP-Adressen

Nutzen Sie die Netzanbindungen Ihres Rechners zum E-Mail-Lesen und Internetsurfen, benötigen darüber hinaus aber keine spezielleren Internetdienste? Für die meisten Rechner trifft das zu.

Dann können auch Sie so genannte „private IP-Adressen“ für Ihren Rechner verwenden. Diese Adressen bieten den Vorteil, dass sie prinzipbedingt nicht aus dem Internet angegriffen werden können. Nähere Informationen hierzu finden Sie unter

```
http://www.gwdg.de/service/
      netze/goenet/privatenetze.html
```

### 2.7 Notebooks und mobile Rechner

Rechner, die zeitweise innerhalb und zeitweise außerhalb des GÖNET am Netz betrieben werden, haben wiederholt zu schweren Sicherheitsproblemen im GÖNET geführt, weil durch solche Rechner Schädlinge ins GÖNET eingeschleppt wurden, die am Internetzugang eigentlich blockiert wurden.

**Prüfen Sie Notebooks und mobile Rechner auf ihre Integrität, bevor Sie diese an das GÖNET anschließen!**

Ein ausführliches Konzept für den sicheren Betrieb von Notebooks und mobilen Rechnern finden Sie unter

```
http://www.gwdg.de/service/
   sicherheit/info/notebookkonzept.html
```

### 2.8 Informationsangebote der GWDG

Die GWDG bietet Ihnen vielfältige Informationen zum Thema IT-Sicherheit an.

Sie finden allgemeine Informationen unter

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

und aktuelle Informationen unter

```
http://www.gwdg.de/aktuell
```

Über die **Mailingliste GWDG-SEC** informiert die GWDG Sie über aktuelle Sicherheitsprobleme. Mehr zu dieser Liste finden Sie unter

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

Die GWDG bietet viele Schulungen an. Nutzen Sie auch die **Kurse zu Sicherheitsfragen!** Das Kursangebot finden Sie unter

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

Beck

---

## 3. Sicherheitskonzept für Notebooks und andere mobile Rechner

### 3.1 Gefährdungslage

Die Flut der digitalen Schädlinge, denen Rechner im Internet ausgesetzt sind, gefährdet auch immer wieder die Netze der Max-Planck-Institute und der Universität Göttingen. Diese Kompromittierung ereignet sich trotz der Absicherung des internen Netzes gegenüber dem Internet durch eine Firewall.

Ursachen für diese Sicherheitsprobleme sind meist ungenügend abgesicherte Notebooks von Mitarbeitern und Gästen und andere Rechner, die abwechselnd innerhalb und außerhalb des Intranets betrieben werden. Außerhalb des Intranets erfolgte Infektionen solcher mobilen Rechner mit Schadroutinen werden dann ins Intranet eingeschleppt und gefährden dort andere Systeme, die ansonsten durch die Firewall geschützt wären.

### 3.2 Lösungsvorschläge

In vielen Firmen und Behörden wird diesem Problem begegnet, in dem solche mobilen Rechner generell nicht zugelassen werden. Ein solches Verbot lässt sich in unserem Umfeld von Forschung und Lehre nicht realisieren. Hier ist davon auszugehen, dass die Forscher ihre Arbeit zu Hause fortsetzen und mit dem mitgenommenen Rechner auch online arbeiten. Ebenso werden immer wieder Gastwissenschaftler ihre Rechner mitbringen und für unterschiedliche Dauer ihren Rechner im Institut anschließen wollen und sollen.

Prinzipiell müssen zwei Arten mobiler Rechner unterschieden werden:

- Rechner von Mitarbeitern und Gästen, die über längere Zeiträume immer wieder an das interne Netz angeschlossen werden und

- Rechner von Gästen, die nur für kurze Zeit einen Netzzugang im Institut benötigen.

Grund für diese Fallunterscheidung ist, dass im ersten Fall dem Nutzer zugemutet werden kann, den mobilen Rechner gemäß den Vorgaben des Instituts sicher zu betreiben, während dies einem Kurzzeitgast kaum zugemutet werden kann.

### 3.2.1 Regeln für längerfristig ans Netz anzuschließende Rechner

Rechner, die über einen länger dauernden Zeitraum am internen Netz betrieben werden sollen, müssen strengen Konfigurationsregeln genügen. Hier gelten die gleichen Grundregeln wie für alle anderen Rechner im Intranet:

- Sichere Konfiguration von Betriebssystem und Anwendungen
- Zeitnahe Installation von sicherheitsrelevanten Softwarekorrekturen
- Einsatz von Antivirensoftware
- Einsatz einer „Personal Firewall“

**Sichere Konfiguration von Betriebssystemen und Anwendungen**

Der erste hier zu beachtende Punkt ist die Verwendung sicherer Passwörter. Fehlende oder leicht zu erratende Passwörter werden von verschiedenen Würmern, aber auch von Hackern immer wieder ausgenutzt. Sichere Passwörter sollten eine Länge von acht oder mehr Zeichen haben. Ein Passwort sollte aus einer Mischung von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen. Voreinstallierte Passwörter sollten bei Übernahme des Systems umgehend geändert werden.

Betriebssystem- und Anwendungssoftware (insbesondere Webbrowser und Mailclient) sollten so konfiguriert werden, dass keine Programme unbeabsichtigt ausgeführt werden können. Aktive Inhalte von Webseiten oder in Mails dürfen, wenn überhaupt, dann zumindest nicht ungeprüft ausgeführt werden. (Musterkonfigurationen siehe **`http://www.gwdg.de/service/sicherheit`**).

Die Benutzung der Rechner sollte mit möglichst minimalen Benutzerrechten erfolgen. Insbesondere sollte nicht regulär mit administrativen Rechten gearbeitet werden.

**Zeitnahe Installation von sicherheitsrelevanten Softwarekorrekturen**

Wenn man von Massenmail-Viren absieht, waren für fast alle Sicherheitsvorfälle der letzten Zeit Fehler der Betriebssystemsoftware oder systemnaher Anwendungssoftware das Einfallstor. Eine rechtzeitige Installation veröffentlichter Softwarekorrekturen hätte den überwiegenden Teil dieser Sicherheitsvorfälle verhindert.

Insbesondere für die neueren Windows-Betriebssystem (Windows 2000, Windows XP und Windows 2003) kann die Softwareaktualisierung durch den „Windows-Updatedienst“ automatisiert werden. Die Softwareaktualisierung kann über Server von Microsoft oder über eigene Software-Update-Server (z. B. den SUS-Server der GWDG, siehe **`http://sus.gwdg.de`**) erfolgen.

Für ältere Windows-Betriebssysteme sind manuelle Installationen nötig. Dabei ist vom Systemadministrator auf entsprechende Ankündigungen vom Hersteller selbst oder von anderen Institutionen (z. B. auf der Mailingliste GWDG-SEC der GWDG, siehe **`http://www.gwdg.de/service/sicherheit/aktuell`**) zu achten und entsprechend zu reagieren.

Bei langsamen Netzanbindungen außerhalb des Institutsnetzes kann im Heimbetrieb auf eine Aktualisierung verzichtet werden, wenn eine Aktualisierung am nächsten Tag bzw. nach dem Wochenende im Institutsnetz erfolgt.

**Einsatz von Antivirensoftware**

Auf allen Rechnern sind eine Antivirensoftware und eine automatische Aktualisierung derselben einzurichten. Die Max-Planck-Gesellschaft wie auch die Universität verfügen über entsprechende Sammellizenzen, die eine Einrichtung auf allen Rechner der Institute bzw. auf dienstlich genutzten Rechnern erlauben (siehe **`http://antivir.gwdg.de`**). Bei Rechnern von Gästen sollten die Besitzer sich schriftlich verpflichten, lizenzpflichtige Software, wie die vom Institut zur Verfügung gestellten Virenscanner, nach Verlassen des Instituts zu deinstallieren.

Die Antivirensoftware sollte so eingestellt werden, dass eine Prüfung auf neue Signaturen mehrmals täglich erfolgt. Die erste Prüfung sollte möglichst unmittelbar nach dem Starten des Rechners erfolgen.

Auch hier kann auf eine automatische Aktualisierung im Heimbetrieb verzichtet werden, falls eine Aktualisierung am nächsten Tag bzw. nach dem Wochenende gewährleistet ist.

Zu einer Antivirensoftware gehört ein Hintergrundwächter (On-Access-Scanner), der permanent aktiviert sein sollte und ein Eindringen von Viren verhindern soll. Es wurden jedoch immer wieder Fälle beobachtet, in denen Viren oder Würmer auf vom Hintergrundwächter nicht kontrollierten Wegen eingedrungen sind. Es ist daher notwendig, regelmäßig eine explizite Durchsuchung der Festplatten nach Viren durchzuführen (On-Demand-Scan). Dies trifft ganz besonders auf alle Rechner zu, die

zeitweise außerhalb des internen Netzes betrieben werden. Bei mobilen Rechnern sollte bei jeder Rückkehr ins interne Netz der (On-Demand-) Virenscanner gestartet und ein Suchlauf über alle lokalen Laufwerke durchgeführt werden.

**Einsatz einer „Personal Firewall“**

Die Filterung von Netzverkehr auf jedem Rechner durch eine „Personal Firewall“ ist eine zusätzliche Sicherheitsmaßnahme, die zumindest von mobilen Rechnern im Betrieb außerhalb des internen Netzes gefordert wird.

UNIX und verwandte Betriebssystem verfügen über entsprechende mitgelieferte oder frei verfügbare Software. Windows verfügt ab Windows XP über eine integrierte Personal Firewall. Bei älteren Windows-Versionen sollten im Internet verfügbare Zusatzprodukte (z. B. Kerio Firewall) installiert werden.

Die Firewall sollte so eingestellt werden, dass grundsätzlich alle eingehenden Verbindungsaufbauten verboten werden. Die interne Firewall von Windows XP leistet genau diese Funktion, sofern sie aktiviert ist. Eine geeignet Konfiguration der Kerio Firewall ist unter

**`http://www.gwdg.de/service/sicherheit/aktuell/persfw.html`**

beschrieben.

Soweit nicht dringende Gründe dagegen sprechen, sollte die Firewall auch während des Betriebs im internen Netz eingeschaltet bleiben. Dort bietet sie einen zusätzlichen Schutz und es ist somit sichergestellt, dass die Firewall auch im externen Betrieb aktiviert bleibt.

**Organisation und Verantwortlichkeiten**

Mitarbeiter sind auf die Einhaltung dieser Regeln für die von ihnen genutzten Rechner zu verpflichten.

Der Gastgeber ist für die Einhaltung der Sicherheitsregeln seitens des Gastes voll verantwortlich. Er kann für die Information über die Sicherheitsregeln und eine gegebenenfalls notwendige Überprüfung des Laptops auf die IT-Servicegruppe verweisen. Gäste sind auf die Einhaltung der Regeln zu verpflichten. Soweit Gästerechner bereits über eine geeignete Konfiguration verfügen (z. B. auch mit anderen als im Institut üblichen Virenscannern), können diese an das interne Netz angeschlossen werden. Besteht keine Klarheit über die Konformität der Konfiguration, so ist eine Überprüfung vorzunehmen.

#### 3.2.2 Regeln für nur kurzzeitig am Netz anzuschließende Rechner

Sind Gäste nur für sehr kurze Zeit am Institut, so kann man eine Umkonfiguration der Rechner (und eine Überprüfung durch das Institutspersonal) nach den obigen Regeln meist nicht verlangen. Rechner, die den Sicherheitsanforderungen nicht zweifelsfrei entsprechen, dürfen nicht an das interne Netz angeschlossen werden. Soll Gästen dennoch diese Möglichkeit geboten werden, so ist dafür ein separates Netz einzurichten, das gegenüber dem internen Netz ebenfalls durch eine Firewall abgetrennt wird.

Kleinere Abweichungen in der Behandlung eines solchen Netzes im Vergleich zum Internet sind insoweit möglich, dass aus diesem Netz ggf. auf im Internet nicht verfügbare Informationsdienste zugegriffen werden darf (z. B. interne Telefonlisten, Zugriff auf Informationsdienste über den Proxy-Server des Instituts u. ä).

Ein solches Netz kann als virtuelles LAN innerhalb der Netzwerkinfrastruktur realisiert werden.

### 3.3 Zugangskontrolle beim Netzanschluss

Die bisherigen Ausführungen zeigen Regeln für eine sichere Konfiguration von Rechnern und die Erlaubnis zum Netzzugang auf. All diese Maßnahmen stellen jedoch kein technisches Hindernis für einen die Regeln verletzenden Anschluss von unerwünschten Rechnern am lokalen Netz dar. In den meisten Netzen sind erfahrungsgemäß auch keine technischen Maßnahmen implementiert, die verhindern können, dass beliebige Rechner an beliebige Netze angeschlossen werden können.

Die technischen Möglichkeiten, um den Anschluss beliebiger Rechner an ein Netz zu verhindern, sind bisher sehr gering. Einige Hersteller bieten eine häufig „Port Security“ genannte Funktionalität an, die auf Basis von MAC-Adressrestriktionen an Switchports verhindert, das Rechner mit unbekannten MAC-Adressen eine Netzwerkverbindung erhalten. Technisch versierte Nutzer können diesen Schutz allerdings umgehen, indem sie die MAC-Adresse ihres Rechners per Software geeignet einstellen. Dennoch empfiehlt sich die Nutzung dieser Funktionalität zumindest für Anschlüsse in öffentlich zugänglichen Bereichen.

Eine neuere und zuverlässigere Entwicklung sind 802.1X-fähige Switches. Mit 802.1X-Funktionen kann die Freischaltung von Netzwerkports an Switches an eine Authentifizierung mit Benutzername und Kennwort oder Zertifikate gebunden werden. Hier ist eine Fälschung derzeitig nicht möglich. Allerdings ist die Zugangskontrolle hier an den Nut-

zer und nicht an das System gebunden. Diese Möglichkeit der Zugangskontrolle sollte mittelfristig genutzt werden.

## 3.4 Sicherer Betrieb von Funknetzen

Drahtlose Netze finden immer größere Verbreitung. Gerade für mobile Rechner im Allgemeinen und Gäste im Besonderen bieten Sie einen einfachen Zugangsweg zum Netzanschluss. Aber Funknetze bedürfen prinzipbedingt hinsichtlich der Sicherheit einer höheren Aufmerksamkeit als kabelgebundene Netzwerke. Der Betrieb eines Funk-LAN ohne Verschlüsselungs- und Zugangskontrolle stellt ein großes Sicherheitsrisiko dar. **Für ein sicheres Funk-LAN sind daher die nachstehenden Regeln zu beachten:**

### 3.4.1 Verschlüsselung, Firewall und Zugriffe

- Die Access-Points eines Funknetzes sollten immer, z. B. durch ein virtuelles LAN (VLAN), vom Institutsnetz getrennt betrieben werden.
- Ist eine Verbindung aus dem Funk-LAN zu Diensten innerhalb des Instituts erforderlich, so ist der Zugriff durch eine Firewall oder ACL entsprechend abzusichern und zusätzlich eine Identifikation der Personen durch geeignete Authentifizierung erforderlich.
- Die Benutzer eines Funk-LAN müssen durch eine Firewall oder ACL vor direkten Zugriffen aus dem Internet geschützt werden.
- Der Datenaustausch im Funknetz sollte überdies nur verschlüsselt erfolgen, damit ein „Ausspähen“ von Daten und Passwörtern nicht möglich ist. Zur verschlüsselten Übertragung auf der Funknetzseite sind derzeit die folgenden Verfahren geeignet:

| Verschlüsselungsverfahren | Sicherheitsniveau |
|---|---|
| VPN (IPSEC, 3DES, AES ) | Höchste Sicherheit |
| 802.1X & EAP (Varianten mit dynamischen WEP-Keys) | Sehr hohe Sicherheit |
| SSL Gateway | Sehr hohe Sicherheit |
| WPA | Hohe Sicherheit |
| WEP | Geringe Sicherheit |

### 3.4.2 Zugangskontrollen im Funk-LAN

- Ausschließlich Benutzer mit gültigem Benutzernamen/Passwort oder Schlüssel wird der Zugang zum Funk-LAN gewährt. Häufig wechselnde Benutzergruppen wie z. B. Gäste bekommen Kurzzeit-Accounts, deren Zugriff auf sicherheitsrelevante Bereiche durch geeignete Maßnahmen verhindert werden muss.
- Ein Funknetz, welches lediglich den Zugang zum Internet ermöglichen soll, wird als prinzipiell unsicher eingestuft und erhält die gleiche Sicherheitsstufe, wie das unsichere Internet. Diese Variante eines Funk-LAN kann, bei einer etwaigen Firewall zum Internet, in einer DMZ betrieben werden.

## 3.5 Einwahl- und VPN-Zugänge

Bei externen Rechnern, die über einen Einwahl- oder VPN-Zugang an das Institutsnetz angebunden werden, ist die gleichen Problematik zu sehen, wie bei mobilen Rechnern, die zeitweise direkt im Institutsnetz betrieben werden. Auch diese Rechner werden in verschiedenen Sicherheitszonen betrieben und können so zu einer Gefährdung des Institutsnetzes werden.

Wegen dieses Gefährdungspotentials müssen auch hier die Regeln für mobile Rechner angewandt werden, insbesondere sind analog zu mobilen Rechnern entweder die externen Rechner entsprechend sicher zu konfigurieren oder es ist ein separates Netz, dessen Übergänge zum internen Netz durch Firewallfunktionalität zu kontrollieren sind, für diese Zugänge zu konfigurieren.

Beck

## 4. Sicherheitslöcher und Software-Aktualisierung

Gerade in der heutigen Zeit wird es immer wichtiger, sein Betriebssystem auf dem aktuellen Stand zu halten, denn der Zeitraum zwischen der Veröffentlichung von Schwachstellen und dem Aufkommen von Schadroutinen, die diese ausnutzen, wird immer kürzer. Aktuell trifft das auf einen schwerwiegenden **Fehler in der Verarbeitung von JPEG-Grafiken** zu. Dieses Mitte September veröffentlichte Problem betrifft sowohl Windows als auch diverse Anwendungsprogramme und ermöglicht Angreifern, letztlich die Kontrolle über fremde Rechner zu erlangen. Dazu genügt es bereits, eine entsprechend präparierte Grafik auf einer Webseite bzw. innerhalb einer Mail zu betrachten. Ursache dafür ist die **fehlerhafte Grafikbibliothek „gdiplus.dll“**, die erstmals in Windows XP, Windows 2003 und in dem dazugehörigen Internet Explorer ihren Einsatz fand und im Service Pack 2 für Windows XP (s. auch die GWDG-Nachrichten 9/2004) inzwischen korrigiert wurde. Da die Programme aus den moderneren Office-Versionen XP und 2003 ebenfalls auf diese Komponente angewiesen sind, bringen sie die dazugehörige Bibliothek einfach selber mit, da sie ja durchaus auch auf älteren Windows-Systemen (z. B. Windows 2000) ablauffähig sein müssen. Genau das kann aber dazu führen, dass ein ansonsten nicht verwundbares System wie eben z. B. Windows 2000 nun plötzlich doch angreifbar wird, nur weil eine Office-Version installiert wurde, die genau diese fehlerhafte Grafikbibliothek integriert hat. Für uns Anwender bedeutet dies, dass wir uns nicht nur um den aktuellen Stand der Betriebssysteme und des Internet Explorers kümmern müssen, sondern unser Augenmerk auch vermehrt auf die Release-Stände der jeweiligen Office-Anwendungen zu richten haben.

Zwar können die Schädlinge, die diese JPEG-Schwachstelle ausnutzen, mittlerweile auch von Virenscannern erkannt werden, aber immer nur dann, wenn die präparierten Grafiken auch in irgendeiner Form auf die Festplatte gelangen und somit der Hintergrundwächter eine Chance hat, darauf zu reagieren. Wird eine Grafik in Form einer Web-Seite oder innerhalb einer E-Mail geladen, dann gelangt sie zwar in den Browser-Cache der temporären Internet-Dateien, allerdings ist dann der schädigende Programmcode aus der Grafik bereits auch schon ins System gelangt. Zudem sind viele Scanner so eingestellt, dass sie wohl nach ausführbaren Dateien mit der Endung „**.exe**“, „**.com**“, „**.vbs**“ etc. fahnden, nicht aber jedoch nach Bilddateien mit der Endung „**.jpg**“. Erschwerend kommt dabei noch hinzu, dass es gerade bei diesem Grafikformat völlig egal ist, wie die Endung lautet, da der Browser dieses Bildformat selbst dann immer noch als JPEG erkennt. Daraus ergibt sich die dringende Maßnahme, den Virenscanner möglichst so einzustellen, dass er auf jeden Fall alle Dateitypen untersucht. Bei **Norman Virus Control** ist dies erfreulicherweise nicht nötig, da er Grafikdateien von sich aus überprüft. Bei **Sophos Anti-Virus** hingegen gelingt dies erst, wenn im Programm **Sophos Anti-Virus** über die Schaltfläche **Ändern** dort auch der Menüpunkt „**Alle Dateien**“ aktiviert wird.


Weil man sich aus den oben genannten Gründen auf die Virenscanner alleine nicht verlassen sollte, ist es dringend erforderlich, die von Microsoft seit Mitte September veröffentlichten Sicherheits-Updates einzufahren. Dabei können die betroffenen Betriebssysteme Windows XP und Windows 2003 komfortabel über den SUS-Server der GWDG (s. auch die GWDG-Nachrichten 5/2003) aktualisiert werden. Ein Anleitung, wie das eigene System dazu konfiguriert werden muss, findet sich unter

```
http://sus.gwdg.de
```

Gleiches gilt auch für die anfällige Version 6 SP1 des Internet Explorers. Aufwändiger wird es hingegen leider bei den betroffenen Office-Produkten, da hier der SUS-Server bislang noch keine Unterstützung liefert. Somit bleiben dem Anwender nur zwei Lösungswege:

- Die automatische Aktualisierung über den Office-Update-Service von Microsoft direkt:

  ```
  http://officeupdate.microsoft.com
  ```


  Durch Aktivieren des Eintrags „**Suchen nach Updates**“ wird der Release-Stand der installierten Office-Umgebung ermittelt und die erforderlichen Korrekturen vorgeschlagen. Damit das geschehen kann, wird zuerst das Active-X-Steuerelement „**Office Update Installation Engine**“ zur Installation vorgeschlagen, was selbstver-

ständlich von dem Benutzer explizit erlaubt werden muss und was als Browser zwangsläufig den Internet Explorer voraussetzt.

- Das manuelle Einfahren der bereitgestellten Korrekturdateien: Hierzu ist bei Office XP zunächst das Service Pack 3 erforderlich, um danach die eigentliche Korrektur einzufahren. Bei Office 2003 genügt bereits die Installation des Service Pack 1, um für diese JPEG-Schwachstelle nicht mehr anfällig zu sein. Den jeweiligen Release-Stand erfährt man übrigens, indem eine beliebige Office-Anwendung - z. B. Word - gestartet, in der Menüzeile auf das Fragezeichen „**?**“ gegangen und dort der Eintrag „**Info**“ aktiviert wird. Hier steht die Version und das installierte Service Pack ganz oben in dem Fenster, z. B.:

  ```
  Microsoft Office Word 2003
  (11.6359.6360) SP1
  ```

  wobei „SP“ für „Service Pack“ steht.

Die einzelnen Korrekturdateien und Service Packs können selbstverständlich auch bei der GWDG herunter geladen werden. Welche Korrekturen genau benötigt werden und woher sie bezogen werden können, erfährt man auf der folgenden Webseite:

```
http://www.gwdg.de/service/
        sicherheit/aktuell/gdi.html
```

Bemüht man sich also, sein Betriebssystem und auch seine Anwendungen stets auf dem aktuellen Stand zu halten und den Virenscanner entsprechend zu konfigurieren und zu aktualisieren, dann sollten solche Gefahren wie diese hier in der Verarbeitung von JPEG-Grafiken eher weniger Schrekken verbreiten. Ist man darüber hinaus auch noch flexibel in der Browserwahl, dann hilft der Einsatz von Alternativen zum Internet Explorer - wie z. B. Firefox oder Mozilla - die Angriffe zu parieren, die ganz gezielt den Microsoft-Browser ins Visier genommen haben.

Reimann

---

# 5. ArcGIS 9.0 – Was ist neu?

## 5.1 Die wichtigsten Neuerungen

In ArcGIS 9.0 wurde eine große Funktionsbibliothek für Daten-Processing angelegt. Eine bessere Integration der Toolbox in ArcMap und im ArcCatalog wurde hergestellt. Die ausführbaren Werkzeuge in ArcToolbox können nun visuell zu Prozessmodellen zusammengesetzt werden. Dies kann des weiteren mit externen Anwendungen gekoppelt und in einer Kommandozeile ausgeführt oder in Skripten zusammengefasst werden.

Folgende Skriptsprachen wurden integriert:

- Python
- VBScript

Im Labelbereich gab es auch Erneuerungen wie Labelmanager für alle Label, Labelausrichtung für Polygone, neue Textformating Tags und die Möglichkeit des Umfließen eines Textes um Grafikelemente.

Der Rasterbereich wurde ebenfalls mit neuen Elementen versehen:

- Die Raster-Layer-Files können nun einschließlich der Übertragung der Symbolik importiert werden.
- Der Export von Rasterdaten mit zahlreichen Einstellungsmöglichkeiten wurde ermöglicht.
- Des weiteren wurden neue Rasterkataloge in der Geodatabase eingebunden.

## 5.2 Weitere Neuerungen

Unter anderem wurden zahlreiche Tastatur-Shortcuts, die Printvorschau, eine GPS-Tollbar, ein schnellerer Start und der XML-Import und -Export von Daten und Schemata integriert.

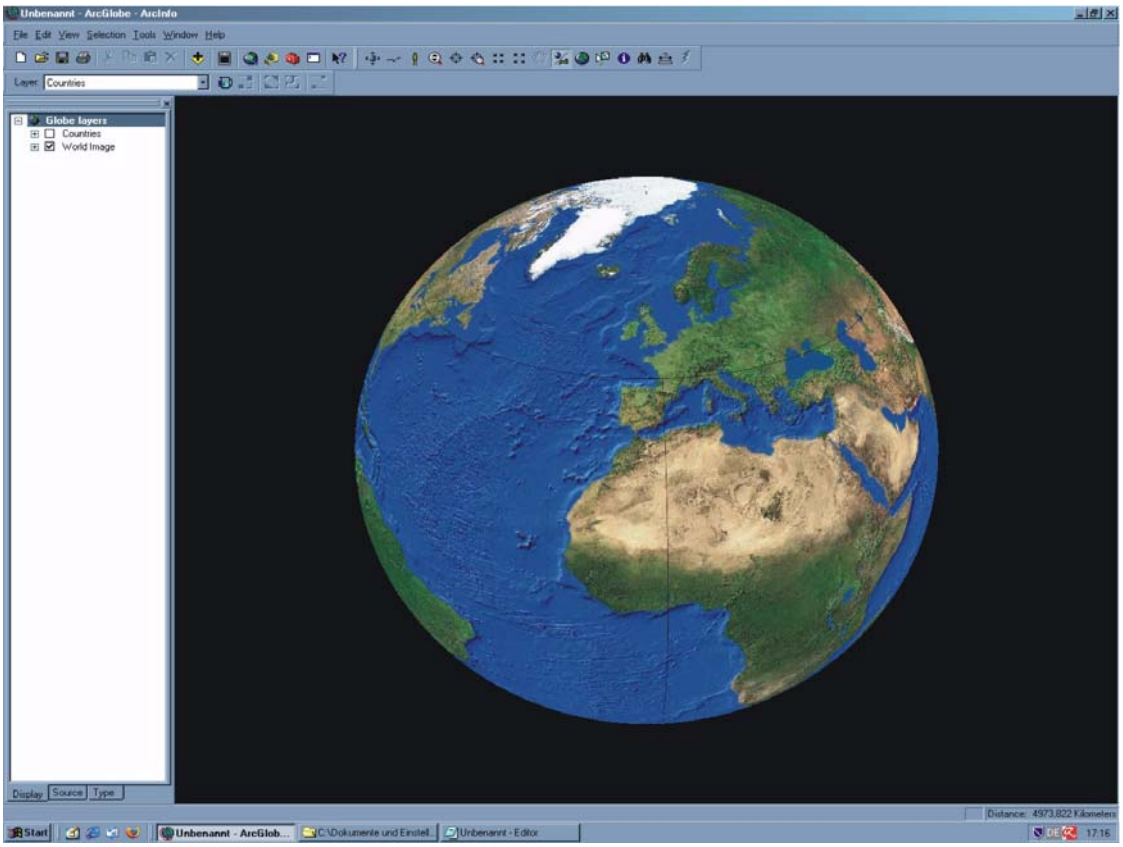
## 5.3 Eine weitere Visualisierungsanwendung: ArcGlobe

Durch die von ArcGlobe (s. Abb.) erzeugten Caching-Strukturen ist es möglich, umfangreiche GIS-Datenbestände, vor allem große Rasterdatenmengen, performant und interaktiv live zu präsentieren.

Die hierfür benötigten Werkzeuge sind integriert und entsprechen den gewohnten Werkzeugen von ArcMap und ArcScene.

ArcGlobe ist im Gegensatz zu ArcScene für große Datenmengen und die Integration aus verschiedenen Datenquellen bzw. Auflösungen in einer Anwendung ausgearbeitet worden.

Axmann




# 6. Kurse des Rechenzentrums

## 6.1 Allgemeine Informationen zum Kursangebot der GWDG

### 6.1.1 Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

### 6.1.2 Anmeldung

Anmeldungen können schriftlich 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. Für die schriftliche Anmeldung steht unter

**`http://www.gwdg.de/service/nutzung/antragsformulare/kursanmeldung.pdf`**

ein Formular zur Verfügung. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager - eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu authorisierte Person - oder Geschäftsführenden Direktor des Instituts vorgenommen werden. 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. Eine Anmeldebestätigung wird nur an auswärtige Institute oder auf besonderen Wunsch zugesendet. Falls eine Anmeldung wegen Überbelegung des

Kurses nicht berücksichtigt werden kann, erfolgt eine Benachrichtigung.

### 6.1.3 Kosten bzw. Gebühren

Die Kurse sind - wie die meisten anderen Leistungen der GWDG - in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

### 6.1.4 Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu 8 Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

### 6.1.5 Kursorte

Die meisten Kurse finden in Räumen der GWDG oder des Max-Planck-Instituts für biophysikalische Chemie statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Fassberg, 37077 Göttingen, der Große Seminarraum im Allgemeinen Institutsgebäude dieses Instituts. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL

**`http://www.gwdg.de/gwdg/standort/lageplan`**

zu finden. Der gemeinsame Schulungsraum von GWDG und SUB befindet sich im Untergeschoss der Niedersächsischen Staats- und Universitätsbibliothek, Platz der Göttinger Sieben 1, 37073 Göttingen.

### 6.1.6 Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL

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

zu finden. Anfragen zu den Kursen können an den Dispatcher per Telefon unter der Nummer 0551 201-1524 oder per E-Mail an die Adresse auftrag@gwdg.de gerichtet werden. Zweimal jährlich wird ein Katalog mit dem aktuellen GWDG-Kursprogramm versendet. Interessenten, die in den Verteiler aufgenommen werden möchten, können dies per E-Mail an die Adresse gwdg@gwdg.de mitteilen.

## 6.2 Kurse 2004

### 6.2.1 Kurse von November bis Dezember 2004 in thematischer Übersicht

**EDV-Grundlagen und Sonstiges**

| Kurse | Termine | Vortragende |
|---|---|---|
| Einführung in die Nutzung des Leistungsangebots der GWDG | • 08.12.2004 | Dr. Grieger<br>Dr. Grieger |
| Führung durch das Rechnermuseum | • 12.11.2004<br>• 10.12.2004 | Eyßell<br>Eyßell<br>Eyßell |

**Betriebssysteme**

| Kurse | Termine | Vortragende |
|---|---|---|
| Grundkurs UNIX/Linux mit Übungen | • 07.12.2004 - 09.12.2004 | Hattenbach |
| Schnellkurs UNIX für Windows-Benutzer mit Übungen | • 29.11.2004 - 30.11.2004 | Dr. Bohrer |
| Installation und Administration von UNIX-Systemen | • 14.12.2004 - 17.12.2004 | Dr. Heuer, Dr. Sippel |
| UNIX für Fortgeschrittene | • 22.11.2004 - 24.11.2004 | Dr. Sippel |

**Netze / Internet**

| Kurse | Termine | Vortragende |
|---|---|---|
| Sicherheit im Internet für Anwender | • 02.12.2004 | Reimann |

**Sonstige Anwendungssoftware**

| Kurse | Termine | Vortragende |
|---|---|---|
| Datenbanksystem MS Access, Einführung mit Übungen | • 22.11.2004 - 26.11.2004 | Dr. Kneser |
| PowerPoint | • 21.12.2004 - 22.12.2004 | Reimann |
| SAS - Grundlagen | • 09.11.2004 - 11.11.2004 | Wagenführ |
| Mit StarOffice zum Schwarzen Loch | • 12.11.2004 | Dr. Grieger |

**Programmiersprachen**

| Kurse | Termine | Vortragende |
|---|---|---|
| Programmierung von Parallelrechnern | • 02.11.2004 - 04.11.2004 | Prof. Haan,<br>Dr. Schwardmann |

### 6.2.2 Kurse von November bis Dezember 2004 in chronologischer Übersicht

| Kurs | Vortragende | Termin | Anmelde-schluss | AE |
|---|---|---|---|---|
| Programmierung von Parallel-rechnern | Prof. Dr. Haan, Dr. Schwardmann | 02.11.2004 - 04.11.2004<br>09.15 - 12.15 Uhr und<br>14.00 - 17.00 Uhr | 26.10.2004 | 12 |
| SAS - Grundlagen | Wagenführ | 09.11.2004 - 11.11.2004<br>09.15 - 12.00 Uhr und<br>13.30 - 16.30 Uhr | 02.11.2004 | 12 |
| Führung durch das Rechner-museum | Eyßell | 12.11.2004<br>10.00 - 12.00 Uhr | 05.11.2004 | 0 |
| Mit StarOffice zum Schwarzen Loch | Dr. Grieger | 12.11.2004<br>09.15 - 12.00 Uhr | 05.11.2004 | 2 |
| Datenbanksystem MS Access, Einführung mit Übungen | Dr. Kneser | 22.11.2004 - 26.11.2004<br>09.00 - 12.00 Uhr | 15.11.2004 | 10 |
| UNIX für Fortgeschrittene | Dr. Sippel | 22.11.2004 - 24.11.2004<br>09.15 - 12.00 Uhr und<br>13.15 - 15.30 Uhr | 15.11.2004 | 12 |
| Schnellkurs UNIX für Windows-Benutzer mit Übungen | Dr. Bohrer | 29.11.2004 - 30.11.2004<br>13.30 - 16.30 Uhr | 22.11.2004 | 4 |
| Sicherheit im Internet für Anwender | Reimann | **Neue Uhrzeit!**<br>02.12.2004<br>09.15 - 12.00 Uhr | 25.11.2004 | 2 |
| Grundkurs UNIX/Linux mit Übungen | Hattenbach | 07.12.2004 - 09.12.2004<br>09.15 - 12.00 Uhr und<br>13.30 - 16.00 Uhr | 30.11.2004 | 12 |
| Einführung in die Nutzung des Leistungsangebots der GWDG | Dr. Grieger | 08.12.2004<br>17.15 - 20.00 Uhr | 01.12.2004 | 0 |
| Führung durch das Rechner-museum | Eyßell | 10.12.2004<br>10.00 - 12.00 Uhr | 03.12.2004 | 0 |
| Installation und Administration von UNIX-Systemen | Dr. Heuer, Dr. Sippel | 14.12.2004 - 17.12.2004<br>09.30 - 12.00 Uhr und<br>13.30 - 16.30 Uhr | 07.12.2004 | 16 |
| PowerPoint | Reimann | 21.12.2004 - 22.12.2004<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 14.12.2004 | 8 |

## 6.3 Kurse 2005

### 6.3.1 Kurse von Januar bis Dezember 2005 in thematischer Übersicht

**EDV-Grundlagen und Sonstiges**

| Kurse | Termine | Vortragende |
|---|---|---|
| Datenschutz - Verarbeitung personenbezogener Daten auf den Rechenanlagen der GWDG | • 01.07.2005 | Dr. Grieger |
| Einführung in die Nutzung des Leistungsangebots der GWDG | • 02.03.2005<br>• 18.05.2005<br>• 31.08.2005<br>• 07.12.2005 | Dr. Grieger<br>Dr. Grieger<br>Dr. Grieger<br>Dr. Grieger |
| Einführung in Aufbau und Funktionsweise von PCs | • 17.01.2005<br>• 02.05.2005<br>• 13.09.2005 | Eyßell<br>Eyßell<br>Eyßell |
| Einführung in die Bedienung von Windows-Oberflächen | • 18.01.2005<br>• 03.05.2005<br>• 14.09.2005 | Eyßell<br>Eyßell<br>Eyßell |
| Führung durch das Rechnermuseum | • 14.01.2005<br>• 11.02.2005<br>• 11.03.2005<br>• 08.04.2005<br>• 13.05.2005<br>• 10.06.2005<br>• 08.07.2005<br>• 02.09.2005<br>• 30.09.2005<br>• 04.11.2005<br>• 09.12.2005 | Eyßell<br>Eyßell<br>Eyßell<br>Eyßell<br>Eyßell<br>Eyßell<br>Eyßell<br>Eyßell<br>Eyßell<br>Eyßell<br>Eyßell |

**Betriebssysteme**

| Kurse | Termine | Vortragende |
|---|---|---|
| Linux: KDE-Desktop und Anwendungen | • 25.04.2005 - 26.04.2005 | Dr. Schwardmann |
| UNIX/Linux-Windows-Systemintegration mit SAMBA | • 16.06.2005 - 17.06.2005 | Dr. Heuer |
| Grundkurs UNIX/Linux mit Übungen | • 10.05.2005 - 12.05.2005<br>• 08.11.2005 - 10.11.2005 | Hattenbach<br>Hattenbach |

**Betriebssysteme**

| Kurse | Termine | Vortragende |
|---|---|---|
| Schnellkurs UNIX für Windows-Benutzer mit Übungen | • 07.02.2005 - 08.02.2005<br>• 04.07.2005 - 05.07.2005<br>• 11.09.2005 - 12.09.2005<br>• 28.11.2005 - 29.11.2005 | Dr. Bohrer<br>Dr. Bohrer<br>Dr. Bohrer<br>Dr. Bohrer |
| Installation und Administration von UNIX-Systemen | • 19.04.2005 - 22.04.2005<br>• 13.12.2005 - 16.12.2005 | Dr. Heuer, Dr. Sippel<br>Dr. Heuer, Dr. Sippel |
| UNIX für Fortgeschrittene | • 13.05.2005 - 15.05.2005<br>• 05.12.2005 - 07.12.2005 | Dr. Sippel<br>Dr. Sippel |
| Windows 2000/XP/2003 in kleinen Netzwerken | • 14.03.2005 - 15.03.2005<br>• 10.10.2005 - 11.10.2005 | Quentin<br>Quentin |
| Die Windows-Active-Directory-Domäne | • 16.03.2005 - 18.03.2005<br>• 12.10.2005 - 14.10.2005 | Quentin<br>Quentin |

**Netze / Internet**

| Kurse | Termine | Vortragende |
|---|---|---|
| Sicherheit im Internet für Anwender | • 15.04.2004<br>• 16.09.2005<br>• 16.12.2005 | Reimann<br>Reimann<br>Reimann |
| Web Publishing I | • 09.02.2005 - 10.02.2005<br>• 31.08.2005 - 01.09.2005 | Reimann<br>Reimann |
| Web Publishing II | • 02.03.2005 - 03.03.2005 | Reimann |
| Web Publishing III - PHP | • 01.11.2005 - 03.11.2005 | Koch, Reimann |

**Grafische Datenverarbeitung**

| Kurse | Termine | Vortragende |
|---|---|---|
| Arbeiten mit CAD, Grundlagen | • 05.09.2005 - 09.09.2005 | Witt |
| CorelDRAW - Grundlagen | • 12.04.2005 - 13.04.2005<br>• 18.10.2005 - 19.10.2005 | Wagenführ<br>Wagenführ |
| Grundlagen der Bildbearbeitung mit Photoshop | • 28.02.2005 - 01.03.2005<br>• 25.08.2005 - 26.08.2005 | Töpfer<br>Töpfer |
| Photoshop für Fortgeschrittene | • 27.04.2005 - 28.04.2005<br>• 04.10.2005 - 05.10.2005 | Töpfer<br>Töpfer |

**Sonstige Anwendungssoftware**

| Kurse | Termine | Vortragende |
|---|---|---|
| Datenbanksystem MS Access, Einführung mit Übungen | • 23.05.2005 - 27.05.2005<br>• 05.12.2005 - 09.12.2005 | Dr. Kneser<br>Dr. Kneser |
| Einführung in das Computeralgebra-System Mathematica | • 14.06.2005 - 15.06.2005 | Dr. Schwardmann |
| Anwendungen in Lotus Notes | • 07.06.2005 - 08.06.2005 | Greber, Dr. Grieger |
| MindMapping mit MindManager | • 13.07.2005 | Reimann |
| Outlook - Mailing und Groupware | • 09.06.2005 - 10.06.2005 | Reimann |
| PDF-Dateien: Erzeugung und Bearbeitung | • 12.01.2005 - 13.01.2005<br>• 06.07.2005 - 07.07.2005 | Dr. Baier, Koch<br>Dr. Baier, Koch |
| PowerPoint | • 18.05.2005 - 19.05.2005<br>• 22.11.2005 - 23.11.2005 | Reimann<br>Reimann |
| Projektplanung mit MS Project | • 06.10.2005 | Reimann |
| Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN | • 04.04.2005 - 07.04.2005<br>• 26.09.2005 - 29.09.2005 | Dr. Bohrer, Dr. Liesegang<br>Dr. Bohrer, Dr. Liesegang |
| Nutzung fortschrittlicher Datenbanken zur Charakterisierung von Proteinen | • 08.04.2005<br>• 30.09.2005 | Dr. Liesegang<br>Dr. Liesegang |
| SAS - Grundlagen | • 28.06.2005 - 30.06.2005 | Wagenführ |
| Mit StarOffice zum Schwarzen Loch | • 11.11.2005 | Dr. Grieger |

**Programmiersprachen**

| Kurse | Termine | Vortragende |
|---|---|---|
| Einführung in die Programmiersprache Fortran 90/95 | • 29.08.2005 - 30.08.2005 | Dr. Schwardmann |
| Programmierung von Parallelrechnern | • 31.05.2005 - 02.06.2005<br>• 29.11.2005 - 01.12.2005 | Prof. Haan, Dr. Boehme, Dr. Schwardmann<br>Prof. Haan, Dr. Boehme, Dr. Schwardmann |

### 6.3.2 Kurse von Januar bis Dezember 2005 in chronologischer Übersicht

| Kurs | Vortragende | Termin | Anmelde-schluss | AE |
|---|---|---|---|---|
| PDF-Dateien: Erzeugung und Bearbeitung | Dr. Baier, Koch | 12.01.2005 - 13.01.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 05.01.2005 | 8 |
| Führung durch das Rechner-museum | Eyßell | 14.01.2005<br>10.00 - 12.00 Uhr | 07.01.2005 | 0 |
| Einführung in Aufbau und Funktionsweise von PCs | Eyßell | 17.01.2005<br>10.00 - 12.00 Uhr | 10.01.2005 | 2 |
| Einführung in die Bedienung von Windows-Oberflächen | Eyßell | 18.01.2005<br>09.15 - 12.30 Uhr und<br>13.30 - 16.00 Uhr | 11.01.2005 | 4 |
| Schnellkurs UNIX für Windows-Benutzer mit Übungen | Dr. Bohrer | 07.02.2005 - 08.02.2005<br>13.00 - 16.00 Uhr | 31.01.2005 | 4 |
| Web Publishing I | Reimann | 09.02.2005 - 10.02.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 02.02.2005 | 8 |
| Führung durch das Rechner-museum | Eyßell | 11.02.2005<br>10.00 - 12.00 Uhr | 04.02.2005 | 0 |
| Grundlagen der Bildbearbeitung mit Photoshop | Töpfer | 28.02.2005 - 01.03.2005<br>09.30 - 16.00 Uhr | 21.02.2005 | 8 |
| Einführung in die Nutzung des Leistungsangebots der GWDG | Dr. Grieger | 02.03.2005<br>17.00 - 20.00 Uhr | 23.02.2005 | 0 |
| Web Publishing II | Reimann | 02.03.2005 - 03.03.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 23.02.2005 | 8 |
| Führung durch das Rechner-museum | Eyßell | 11.03.2005<br>10.00 - 12.00 Uhr | 04.03.2005 | 0 |
| Windows 2000/XP/2003 in kleinen Netzwerken | Quentin | 14.03.2005 - 15.03.2005<br>09.00 - 15.00 Uhr | 07.03.2005 | 8 |
| Die Windows-Active-Directory-Domäne | Quentin | 16.03.2005 - 18.03.2005<br>09.00 - 15.00 Uhr<br>(am 18.03. bis 13.00 Uhr) | 09.03.2005 | 10 |
| Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN | Dr. Bohrer,<br>Dr. Liesegang | 04.04.2005 - 07.04.2005<br>09.30 - 12.30 Uhr und<br>13.30 - 16.30 Uhr | 28.03.2005 | 16 |
| Nutzung fortschrittlicher Datenbanken zur Charakterisierung von Proteinen | Dr. Liesegang | 08.04.2005<br>09.30 - 12.30 Uhr und<br>13.30 - 16.00 Uhr | 01.04.2005 | 4 |
| Führung durch das Rechner-museum | Eyßell | 08.04.2005<br>10.00 - 12.00 Uhr | 01.04.2005 | 0 |
| CorelDRAW - Grundlagen | Wagenführ | 12.04.2005 - 13.04.2005<br>09.15 - 12.00 Uhr und<br>13.30 - 16.30 Uhr | 05.04.2005 | 8 |

| Kurs | Vortragende | Termin | Anmelde-schluss | AE |
|---|---|---|---|---|
| Sicherheit im Internet für Anwender | Reimann | 15.04.2005<br>09.15 - 12.00 Uhr | 08.04.2005 | 2 |
| Installation und Administration von UNIX-Systemen | Dr. Heuer,<br>Dr. Sippel | 19.04.2005 - 22.04.2005<br>09.30 - 12.00 Uhr und<br>13.30 - 16.30 Uh | 12.04.2005 | 16 |
| Linux: KDE-Desktop und Anwen-dungen | Dr. Schwardmann | 25.04.2005 - 26.04.2005<br>09.00 - 12.00 Uhr und<br>13.00 - 16.00 Uhr | 18.04.2005 | 8 |
| Photoshop für Fortgeschrittene | Töpfer | 27.04.2005 - 28.04.2005<br>09.30 - 16.00 Uhr | 20.04.2005 | 8 |
| Einführung in Aufbau und Funktionsweise von PCs | Eyßell | 02.05.2005<br>09.15 - 12.30 Uhr | 25.04.2005 | 2 |
| Einführung in die Bedienung von Windows-Oberflächen | Eyßell | 03.05.2005<br>09.15 - 12.30 Uhr und<br>13.30 - 16.00 Uhr | 26.04.2005 | 4 |
| Grundkurs UNIX/Linux mit Übungen | Hattenbach | 10.05.2005 - 12.05.2005<br>09.15 - 12.00 Uhr und<br>13.30 - 16.00 Uhr | 03.05.2005 | 12 |
| Führung durch das Rechner-museum | Eyßell | 13.05.2005<br>10.00 - 12.00 Uhr | 06.05.2005 | 0 |
| PowerPoint | Reimann | 18.05.2005 - 19.05.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 11.05.2005 | 8 |
| Einführung in die Nutzung des Leistungsangebots der GWDG | Dr. Grieger | 18.05.2005<br>17.00 - 20.00 Uhr | 11.05.2005 | 0 |
| Datenbanksystem MS Access, Einführung mit Übungen | Dr. Kneser | 23.05.2005 - 27.05.2005<br>09.00 - 12.00 Uhr | 16.05.2005 | 10 |
| UNIX für Fortgeschrittene | Dr. Sippel | 23.05.2005 - 25.05.2005<br>09.15 - 12.00 Uhr und<br>13.15 - 15.30 Uhr | 16.05.2005 | 12 |
| Programmierung von Parallelrech-nern | Prof. Dr. Haan,<br>Dr. Boehme,<br>Dr. Schwardmann | 31.05.2005 - 02.06.2005<br>09.15 - 12.15 Uhr und<br>13.30 - 16.30 Uhr | 24.05.2005 | 12 |
| Anwendungen in Lotus Notes | Greber,<br>Dr. Grieger | 07.06.2005 - 08.06.2005<br>09.00 - 16.00 Uhr | 31.05.2005 | 8 |
| Outlook - Mailing und Groupware | Reimann | 09.06.2005 - 10.06.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 02.06.2005 | 8 |
| Führung durch das Rechner-museum | Eyßell | 10.06.2005<br>10.00 - 12.00 Uhr | 03.06.2005 | 0 |
| Einführung in das Computeralgebra-System Mathematica | Dr. Schwardmann | 14.06.2005 - 15.06.2005<br>09.00 - 12.00 Uhr und<br>13.00 - 16.00 Uhr | 07.06.2005 | 8 |

| Kurs | Vortragende | Termin | Anmelde-schluss | AE |
|---|---|---|---|---|
| UNIX/Linux-Windows-System-integration mit SAMBA | Dr. Heuer | 16.06.2005 - 17.06.2005<br>09.30 - 12.00 Uhr und<br>13.30 - 16.30 Uhr<br>(am 17.06. bis 12.00 Uhr) | 09.06.2005 | 6 |
| SAS - Grundlagen | Wagenführ | 28.06.2005 - 30.06.2005<br>09.15 - 12.00 Uhr und<br>13.30 - 16.30 Uhr | 21.06.2005 | 12 |
| Datenschutz - Verarbeitung perso-nenbezogener Daten auf den Rechenanlagen der GWDG | Dr. Grieger | 01.07.2005<br>09.00 - 12.00 Uhr | 24.06.2005 | 2 |
| Schnellkurs UNIX für Windows-Benutzer mit Übungen | Dr. Bohrer | 04.07.2005 - 05.07.2005<br>13.00 - 16.00 Uhr | 27.06.2005 | 4 |
| PDF-Dateien: Erzeugung und Bearbeitung | Dr. Baier, Koch | 06.07.2005 - 07.07.2005 | 29.06.2005 | 8 |
| Führung durch das Rechner-museum | Eyßell | 08.07.2005<br>10.00 - 12.00 Uhr | 01.07.2005 | 0 |
| MindMapping mit MindManager | Reimann | 13.07.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 06.07.2005 | 4 |
| Grundlagen der Bildbearbeitung mit Photoshop | Töpfer | 25.08.2005 - 26.08.2005<br>09.30 - 16.00 Uhr | 18.08.2005 | 8 |
| Einführung in die Programmier-sprache Fortran 90/95 | Dr. Schwardmann | 29.08.2005 - 30.08.2005<br>09.00 - 12.00 Uhr und<br>13.00 - 16.00 Uhr | 22.08.2005 | 8 |
| Einführung in die Nutzung des Leistungsangebots der GWDG | Dr. Grieger | 31.08.2005<br>17.00 - 20.00 Uhr | 24.08.2005 | 0 |
| Web Publishing I | Reimann | 31.08.2005 - 01.09.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 24.08.2005 | 8 |
| Führung durch das Rechner-museum | Eyßell | 02.09.2005<br>10.00 -12.00 Uhr | 26.08.2005 | 0 |
| Arbeiten mit CAD, Grundlagen | Witt | 05.09.2005 - 09.09.2005<br>09.00 - 16.00 Uhr<br>(am 05.09. ab 10.00 Uhr;<br>am 09.09. bis 13.00 Uhr) | 29.08.2005 | 18 |
| Schnellkurs UNIX für Windows-Benutzer mit Übungen | Dr. Bohrer | 12.09.2005 - 13.09.2005<br>13.00 - 16.00 Uhr | 05.09.2005 | 4 |
| Einführung in Aufbau und Funktionsweise von PCs | Eyßell | 13.09.2005<br>09.15 - 12.30 Uhr | 06.09.2005 | 2 |
| Einführung in die Bedienung von Windows-Oberflächen | Eyßell | 14.09.2005<br>09.15 - 12.30 Uhr und<br>13.30 - 16.00 Uhr | 07.09.2005 | 4 |

| Kurs | Vortragende | Termin | Anmelde-schluss | AE |
|---|---|---|---|---|
| Sicherheit im Internet für Anwender | Reimann | 16.09.2005<br>09.15 - 12.00 Uhr | 09.09.2005 | 2 |
| Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN | Dr. Bohrer,<br>Dr. Liesegang | 26.09.2005 - 29.09.2005<br>09.30 - 12.30 Uhr und<br>13.30 - 16.30 Uhr | 19.09.2005 | 16 |
| Nutzung fortschrittlicher Datenbanken zur Charakterisierung von Proteinen | Dr. Liesegang | 30.09.2005<br>09.30 - 12.30 Uhr und<br>13.30 - 16.00 Uhr | 23.09.2005 | 4 |
| Führung durch das Rechnermuseum | Eyßell | 30.09.2005<br>10.00 - 12.00 Uhr | 23.09.2005 | 0 |
| Photoshop für Fortgeschrittene | Töpfer | 04.10.2005 - 05.10.2005<br>09.30 - 16.00 Uhr | 27.09.2005 | 8 |
| Projektplanung mit MS Project | Reimann | 06.10.2005<br>09.15 - 12.00 Uhr und<br>13.00 -15.00 Uhr | 29.09.2005 | 4 |
| Windows 2000/XP/2003 in kleinen Netzwerken | Quentin | 10.10.2005 - 11.10.2005<br>09.00 - 15.00 Uhr | 03.10.2005 | 8 |
| Die Windows-Active-Directory-Domäne | Quentin | 12.10.2005 - 14.10.2005<br>(am 14.10. bis 13.00 Uhr) | 05.10.2005 | 10 |
| CorelDRAW - Grundlagen | Wagenführ | 18.10.2005 - 19.10.2005<br>09.15 - 12.00 Uhr und<br>13.30 - 16.30 Uhr | 11.10.2005 | 8 |
| Web Publishing III - PHP | Koch, Reimann | 01.11.2005 - 03.11.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 25.10.2005 | 12 |
| Führung durch das Rechnermuseum | Eyßell | 04.11.2005<br>10.00 - 12.00 Uhr | 28.10.2005 | 0 |
| Grundkurs UNIX/Linux mit Übungen | Hattenbach | 08.11.2005 - 10.11.2005<br>09.15 - 12.00 Uhr und<br>13.30 - 16.00 Uhr | 01.11.2005 | 12 |
| Mit StarOffice zum Schwarzen Loch | Dr. Grieger | 11.11.2005<br>09.00 - 12.00 Uhr | 04.11.2005 | 2 |
| PowerPoint | Reimann | 22.11.2005 - 23.11.2005<br>09.15 - 12.00 Uhr und<br>13.00 - 15.00 Uhr | 15.11.2005 | 8 |
| Schnellkurs UNIX für Windows-Benutzer mit Übungen | Dr. Bohrer | 28.11.2005 - 29.11.2005<br>13.00 - 16.00 Uhr | 21.11.2005 | 4 |
| Programmierung von Parallelrechnern | Prof. Dr. Haan,<br>Dr. Boehme,<br>Dr. Schwardmann | 29.11.2005 - 01.12.2005<br>09.15 - 12.15 Uhr und<br>13.30 - 16.30 Uhr | 22.11.2005 | 12 |
| Datenbanksystem MS Access, Einführung mit Übungen | Dr. Kneser | 05.12.2005 - 09.12.2005<br>09.00 - 12.00 Uhr | 28.11.2005 | 10 |

| Kurs | Vortragende | Termin | Anmelde-schluss | AE |
|---|---|---|---|---|
| UNIX für Fortgeschrittene | Dr. Sippel | 05.12.2005 - 07.12.2005<br>09.15 - 12.00 Uhr und<br>13.15 - 15.30 Uhr | 28.11.2005 | 12 |
| Einführung in die Nutzung des Leistungsangebots der GWDG | Dr. Grieger | 07.12.2005<br>17.00 - 20.00 Uhr | 30.11.2005 | 0 |
| Führung durch das Rechner-museum | Eyßell | 09.12.2005<br>10.00 - 12.00 Uhr | 02.12.2005 | 0 |
| Installation und Administration von UNIX-Systemen | Dr. Heuer,<br>Dr. Sippel | 13.12.2005 - 16.12.2005<br>09.30 - 12.00 Uhr und<br>13.30 - 16.30 Uhr | 06.12.2005 | 16 |
| Sicherheit im Internet für Anwender | Reimann | 16.12.2005<br>09.15 - 12.00 Uhr | 06.12.2005 | 2 |

## 7. Betriebsstatistik September 2004

### 7.1 Nutzung der Rechenanlagen

| Rechner | Zahl der Prozessoren | CPU-Stunden |
|---|---|---|
| DECalpha | 12 | 892,97 |
| IBM RS/6000 SP | 224 | 75.948,47 |
| IBM Regatta | 96 | 21.667,34 |
| Linux Parallel | 198 | 133.340,51 |

### 7.2 Betriebsunterbrechungen

| Rechner/PC-Netz | Störungen | | System-pflege | |
|---|---|---|---|---|
| | Anzahl | Stunden | Anzahl | Stunden |
| UNIX-Cluster | 0 | | 0 | |
| IBM SP/Regatta | 0 | | 0 | |
| Linux Parallel | 0 | | 0 | |
| PC-Netz | 5 | 64,00 | 1 | 2,00 |
| Nameserver | 0 | | 0 | |
| Mailer | 0 | | 1 | 0,30 |

## 8. Autoren dieser Ausgabe

| Name | Artikel | E-Mail-Adresse / Telefon-Nr. |
|---|---|---|
| Monika Axmann | • ArcGIS 9.0 – Was ist neu? | maxmann1@gwdg.de<br>0551 201-1842 |
| Dr. Holger Beck | • Neue Informationen zur Sicherheit in Netzen | Holger.Beck@gwdg.de<br>0551 201-1554 |
| Dr. Holger Beck | • Sicherheit im Netz – Sicherheitshinweise für Netzteilnehmer im GÖNET | Holger.Beck@gwdg.de<br>0551 201-1554 |
| Dr. Holger Beck | • Sicherheitskonzept für Notebooks und andere mobile Rechner | Holger.Beck@gwdg.de<br>0551 201-1554 |
| Michael Reimann | • Sicherheitslöcher und Software-Aktualisierung | mreiman1@gwdg.de<br>0551 201-1826 |