Nr. 70 | Juni 2006

DFN mitteilungen

Urheberrecht in der Informationsgesellschaft – eine Zwischenbilanz

«Licht an» für die vierte Generation des Wissenschaftsnetzes in Deutschland

Dienstleistungen für Voice-over-IP

DFN-AAI - Kontrollierter Zugang zu geschützten Ressourcen

INHALT

VORWORT

WISSENSCHAFTS-NETZ

INTERNATIONAL

CAMPUS

RECHT

SICHERHEIT

DFN-VEREIN

Impressum

Herausgeber
Verein zur Förderung eines Deutschen Forschungsnetzes e.V.
DFN-Verein
Stresemannstr. 78, 10963 Berlin
Tel 030 - 88 42 99 - 24
Fax 030 - 88 42 99 - 70
Mail dfn-verein@dfn.de
WWW http://www.dfn.de
ISSN 0177-6894

Redaktion
Kai Hoelzner (kh)

Gestaltung
VISIUS Designagentur
www.visius-design.de

Druck
Trigger Offsetdruck

VORWORT

Vor wenigen Wochen fand in Form eines Festkolloquiums am DESY in Hamburg die offizielle Einweihung des X-WiN statt. Als vierte Generation des nationalen Forschungsnetzes für die Wissenschaft in Deutschland ersetzt das X-WiN seinen technischen Vorgänger, das Gigabit-Wissenschaftsnetz. Mit dem X-WiN verfügen die Hochschulen und Forschungseinrichtungen in Deutschland erstmals über ein eigenes Glasfaser-Netz für ihre Datenkommunikation.

Das Kernnetz des X-WiN wurde nach zweijähriger Vorbereitungszeit bereits zu Beginn diesen Jahres in Betrieb genommen. Mehr als fünfhundert Hochschulen und Forschungseinrichtungen werden seitdem mit einer Infrastruktur versorgt, die Grid-Computing und internationale Wissenschaftskooperationen ebenso ermöglicht, wie sie den einzelnen Wissenschaftler oder Studierenden mit speziell auf die Bedürfnisse in den Hochschulen und Forschungseinrichtungen zugeschnittenen Kommunikationsdienstleistungen unterstützt.

Für die 2,5 Millionen Nutzer an den Hochschulen und in der Forschung wird sich das X-WiN in den kommenden Jahren als eines der wichtigsten Werkzeuge für die tägliche wissenschaftliche Arbeit bewähren. Anschlüsse von derzeit bis zu 10 Gigabit/s und ein Kernnetz mit Terabit-Kapazität, das sich zwischen 46 Kernnetzstandorten aufspannt, machen das X-WiN zu einem der leistungsfähigsten Kommunikationsnetze weltweit.

Eine Kommunikationsinfrastruktur wie das X-WiN wird am Markt nicht fertig konfektioniert angeboten. Es bedarf intensiver Planung, vieler Abstimmungen und eines immenses Pensums an Arbeit, bis ein solches Netz in Betrieb gehen kann. Mindestens ebenso bemerkenswert wie seine Leistungsparameter ist daher die Tatsache, dass das X-WiN von der Wissenschaft unter dem Dach des DFN-Vereins in Eigenregie aufgebaut wurde und betrieben wird.

Mein Dank gilt daher an dieser Stelle allen Mitgliedern und Mitarbeitern des DFN-Vereins ebenso wie den den Kooperationspartnern und den Unterstützern des Deutschen Forschungsnetzes, die mit ihrem Engagement zum Gelingen des Projektes X-WiN beigetragen haben.

Ihr Wilfried Juling

Prof. Dr. Wilfried Juling
Vorsitzender des Vorstands
des DFN-Vereins

«Licht an» für die vierte Generation des Wissenschaftsnetzes in Deutschland

Kurz vor Erscheinen dieser Ausgabe der DFN-Mitteilungen fand am 3. Mai 2006 die feierliche Inbetriebnahme des X-WiN statt. Mit dem X-WiN verfügen die Hochschulen und Forschungseinrichtungen in Deutschland erstmals über ein eigenes Glasfaser-Netz für ihre Datenkommunikation. Anschlusskapazitäten von bis zu 10 Gigabit pro Sekunde und dazwischen frei skalierbare Kernnetzkapazitäten, die kumuliert bis in den Terabit-Bereich erweitert werden können, machen das X-WiN zu einem der leistungsfähigsten Netze weltweit. Ob beim Aufbau von Grids, bei der Kopplung von Forschungszentren und Hochschulen in ganz Europa oder bei der Installation von VPNs für internationale Science-Communities - dank der Leistungsfähigkeit und Flexibilität des X-WiN eröffnen sich neue Anwendungsszenarien zur Umsetzung des e-Science-Grid-Paradigmas in Deutschland.

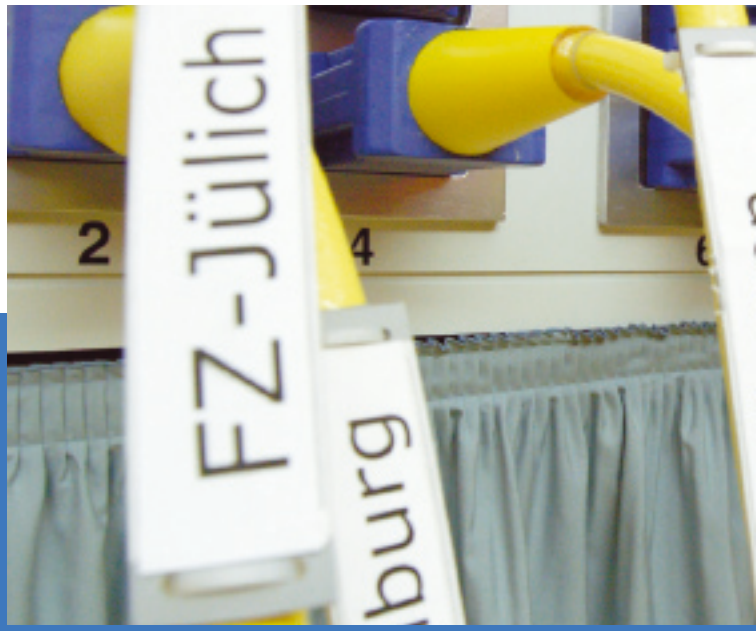
Nach zweijähriger intensiver Planung und Vorbereitung und der Bewältigung eines großen Pensums an Arbeit wurde das Netz mit einem Festakt am Deutschen Elektronen-Synchrotron eingeweiht. Mehr als einhundert Mitgliedsvertreter, Freunde und Kooperationspartner des Deutschen Forschungsnetzes kamen in Hamburg zusammen, um die Inbetriebnahme des Netzes gemeinsam zu begehen.

Der Generalsekretär des Wissenschaftsrats, Min.-Dir. Wedig von Heyden, attestierte dem DFN-Verein in seinem eingangs der Veranstaltung verlesenen Grußwort, mit dem X-WiN eine exzellente Kommunikationsinfrastruktur geschaffen zu haben. Dies, so von Heyden, ist die Voraussetzung für einen international konkurrenzfähigen Forschungs- und Lehrbetrieb. Dem DFN-Verein sei es mit dem X-WiN gelungen, der aktuellen Entwicklung in der Welt der Netzwerke mehr als einen Schritt voraus zu sein. Auch wenn die Worte "Gemeinsam sind wir stark" bislang nicht das offizielle Motto des DFN-Vereins sind, habe es der Verein dennoch gerade dem starken Gemeinschaftswillen seiner Mitglieder zu verdanken, dass mit dem X-WiN eines der weltweit leistungsfähigsten und modernsten Kommunikationsnetze realisiert ist.

Prof. Dr. Gerhard Peter, Vorsitzender der Mitgliederversammlung, ging in seiner anschließenden Ansprache auf den Übergang vom G-WiN zum X-WiN ein. Dieser sei zu vergleichen mit großen Migrationsprojekten wie dem Umzug des Münchner Flughafens von Riem zum Franz-Josef-Strauss-Airport. Gleichsam über Nacht wurde eine hochkomplexe Struktur ausgetauscht, ohne dass es bei den Fluggesellschaften zu nennenswerten Beeinträchtigungen des Flugbetriebs gekommen wäre. Innerhalb nur eines Tages hatte München einen neuen Airport. Die Umschaltung vom G-WiN zum X-WiN wurde in der Neujahrsnacht 2006 in ähnlich erfolgreicher Weise durchgeführt. Über 700 Einrichtungen sind seitdem über ein völlig neues Netz miteinander verbunden, ohne dass die Nutzer von diesem Netzwechsel etwas mitbekommen hätten.

Prof. Dr. Wilfried Juling, Vorstandsvorsitzender des DFN-Vereins, nimmt unter dem Applaus von mehr als hundert angereisten Mitgliedsvertretern und Kooperationspartnern des DFN das X-WiN in Betrieb.

Insgesamt mehr als 700 wissenschaftliche Einrichtungen in Deutschland sind mit dem X-WiN untereinander und mit Wissenschaftlern aus der ganzen Welt verbunden.



Fotos: Jens Nestvogel

Dank seines Potenzials zu fast beliebiger Leistungssteigerung und dank seiner Flexibilität, die auch die Einrichtung optischer VPN erlaubt, sei das X-WiN geeignet, innovative Anwendungen und Nutzungsszenarien im Bereich Grid, aber auch beim eLearning oder beim Knowledge-Management - kurzum im gesamten Bereich der e-Science - optimal zu unterstützen. Prof. Dr. Reinhard Maschuw, Vorstandsmitglied des Forschungszentrums Karlsruhe, stellte dazu fest, dass der Zugang zu den ständig wachsenden Datenmengen in all diesen Bereichen eine ständig wachsende Bandbreite bei der Übertragung ebenso erfordert wie ein hohes Maß an Flexibilität, Sicherheit und die ständig optimale Verfügbarkeit "on the spot".

Die anschließende symbolische Inbetriebnahme des Netzes wurde vom Vorstandsvorsitzenden des DFN-Vereins, Prof. Dr. Wilfried Juling vorgenommen. Unter dem Applaus der mehr als hundert Gäste griff Juling zu einem im Maßstab zehn zu eins angefertigten Datenkabel, das in einen überdimensionalen Switch eingesteckt wurde. In der anschließenden Ansprache wandte sich Juling noch einmal allen Mitgliedern, Freunden und Kooperationspartnern zu, die das Wissenschaftsnetz seit inzwischen 22 Jahren gemeinschaftlich betreiben. Seinen besonderen Dank übermittelte er auch den ehemaligen Vorstandsmitgliedern Prof. Heinz-Gerd Hegering und Prof. Eike Jessen, die den Aufbau des X-WiNs während ihrer letzten Amtsperiode als Vorstand über weite Strecken vorbereitet haben.

Den Abschluss des offiziellen Eröffnungsaktes bildeten drei Festvorträge. Klaus Ullmann, Geschäftsführer des DFN-Vereins, sprach über das 'X-WiN als vierte Generation des Wissenschaftsnetzes in Deutschland'. Dr. Hans Döbbeling, der in Cambridge die Geschäftsführung der europäischen Netzwerkorganisation Dante Ltd. inne hat, kontrastierte diesen Vortrag anschließend mit einer Einführung in die 'pan-europäische Vernetzung mit GÉANT2'. Zum Abschluss des Festaktes sprachen Dr. Volker Gülzow vom Deutschen Elektronen-Synchrotron und Prof. Dr. Martin Erdmann von der RWTH Aachen noch einmal aus Sicht der Nutzer über das Thema 'Bandbreite, unverzichtbar für den wissenschaftlichen Erfolg am Beispiel des CMS-Experimentes'. (*k.h.)*

Ein Transskript des Festvortrags von Dr. Hans Döbbeling wurde dem DFN-Verein freundlicherweise für die Veröffentlichung in den DFN-Mitteilungen zur Verfügung gestellt und findet sich in dieser Ausgabe. Für die kommende, im November erscheinende Ausgabe ist die Veröffentlichung des Beitrags von Dr. Volker Gülzow und Prof. Dr. Martin Erdmann geplant.

Laudatoren und Vortragende (v.l.n.r.): Prof. Dr. Reinhard Maschuw, Dr. Hans Döbbeling, Min.-Dir. Wedig von Heyden und Prof. Dr. Wilfried Juling. Reihe 2, rechts aussen: Klaus Ullmann

Das Netz lernt sprechen

DFN-Dienstleistungen für Voice-over-IP

Die wachsende Verbreitung von Voice-over-IP (VoIP) zeigt es deutlich: der Siegeszug des „Telefonierens über das Internet" hat längst begonnen. Die Vorteile der Nutzung eines gemeinsamen Netzes für Sprache und Daten überzeugen nicht zuletzt auch viele DFN Einrichtungen. So verwundert es wenig, dass die Zahl der DFN Einrichtungen, die eine VoIP-Telefonanlage häufig zusätzlich zu einer klassischen Telefonanlage betreiben, im vergangenen Jahr deutlich zugenommen hat.

Diese Entwicklung wird der DFN-Verein durch eine Reihe von VoIP-Dienstleistungen unterstützen. Das Hauptaugenmerk richtet sich dabei im Gesamtangebot auf die Integration von VoIP, klassischer Telefonie und Videokonferenz-Lösungen. Technische Übergänge zwischen den VoIP-Dienstleistungen und den DFN-Diensten DFNFernsprechen und DFNVideoConference schaffen einen Mehrwert für viele Einrichtungen, die bereits einen der beiden Dienste einsetzen.

Die Dienstleistung DFNVoIPBreakout

In zwei Monaten ist die Betriebsaufnahme der Dienstleistung für VoIP geplant. Da trotz zunehmender Bedeutung von VoIP immer noch die weitaus meisten Telefonate in die öffentlichen Telefonnetze geroutet werden, beginnt der DFN-Verein mit dem Betrieb der Dienstleitung DFNVoIPBreakout. DFNVoIPBreakout realisiert für Einrichtungen mit VoIP-Telefonanlage einen Gateway (sogenannter Breakout), mit dem Telefonate, die aus der VoIP-Welt kommen, mit Zielen im Festnetz oder in den Mobilfunknetzen verbunden werden können. Die Umsetzung der unterstützten VoIP-Protokolle SIP und H.323 auf die gängigen Protokolle im Festnetz und in den Mobilfunknetzen findet im Gateway statt.

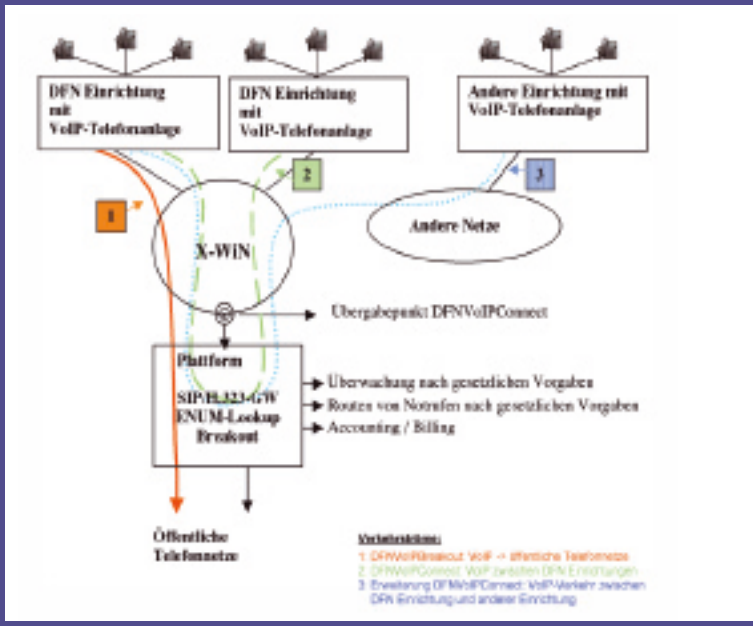
Der Zugang zum Breakout wird über eine Plattform von T-Systems realisiert. Die SIP/H.323-Telefonate werden über die VoIP-Telefonanlage der Einrichtung zur Plattform geroutet. In entgegengesetzter Richtung werden die Telefonate von der Plattform zur VoIP-Telefonanlage der Einrichtung geführt. Eine direkte Anbindung von VoIP-Telefonen an die Plattform wird nicht unterstützt. Die Plattform sorgt zusätzlich für das korrekte Routen der Notrufe nach den gesetzlichen Bestimmungen der Bundesnetzagentur. T-Systems garantiert darüber hinaus das Einhalten der gesetzlichen Bestimmungen für den Betrieb von Telekommunikationsnetzen.

Die Dienstleistung DFNVoIPBreakout ist technisch und administrativ in den Dienst DFNFernsprechen integriert. So erfolgt die Rechnungsstellung für Telefonate, die über den Breakout geführt werden, zusammen mit der Rechnungsstellung für DFNFernsprechen. Dennoch können auch Einrichtungen ohne DFNFernsprechen die neue Dienstleistung DFNVoIPBreakout nutzen.

Die Dienstleistung DFNVoIPConnect

Viele DFN Einrichtungen setzen VoIP bereits im Regelbetrieb ein. Ein Telefonat zwischen zwei VoIP-fähigen DFN Einrichtungen bleibt allerdings selten in der VoIP-Welt, fast immer wird ein Teil des Telefonats über die öffentlichen Telefonnetze geführt. Der Grund dafür liegt in der Ausstattung der Einrichtungen mit VoIP-Telefonanlagen, die sich durch Hersteller, Typ und Protokoll unterscheiden.

Zur Unterstützung des „reinen" VoIP-Verkehrs zwischen DFN Einrichtungen wird z. Zt. eine Connect-Funktion realisiert. Die entsprechende Dienstleistung DFNVoIPConnect unterstützt die Kommunikation über VoIP für DFN Einrichtungen unabhängig von Hersteller, Typ und Protokoll (SIP, H.323) der beteiligten VoIP-Telefonanlagen. Die Signalisierung wird ebenfalls über die Plattform der T-Systems durchgeführt, die für die Umsetzung der Signalisierungsprotokolle ein SIP/H.323-Signalling-Gateway anbietet. Das korrekte Routen von Notrufen nach den gesetzlichen Bestimmungen der Bundesnetzagentur wird garantiert. Ein Pilotbetrieb für DFNVoIPConnect befindet sich in Vorbereitung.



Erweiterung der Dienstleistung DFNVoIPConnect um ENUM

Auch außerhalb des DFN-Vereins ist der Siegeszug von VoIP nicht mehr aufzuhalten, inzwischen bieten viele DSL-Anbieter auch im Privatkundenmarkt VoIP an. Daher soll es in Zukunft auch möglich sein, aus dem DFN-Verein heraus mit Teilnehmern außerhalb des DFN-Vereins (Firmen oder Privatpersonen) über VoIP zu telefonieren. Im Gegensatz zur klassischen Telefonie reicht bei VoIP die Kenntnis der Telefonnummer für die Adressierung eines Teilnehmers jedoch nicht aus, zusätzlich muss auch die Kommunikationsadresse bekannt sein. Abhilfe schafft das ENUM-Protokoll, das mit Hilfe des bekannten Domain Name Service (DNS) eine Abbildung der Telefonnummer auf die Kommunikationsadresse vornimmt; Bedingung ist allerdings, dass auch der angerufene Teilnehmer ENUM unterstützt.

Die um ENUM erweiterte Connect-Funktion unterscheidet sich abgesehen von der Art der Adressierung nicht von der Connect-Funktion: der Verbindungsaufbau wird ebenfalls über die Plattform von T-Systems realisiert. Wie bei DFNVoIPConnect wird auch hier das SIP/H.323-Signalling-Gateway angeboten und das korrekte Routen der Notrufe nach den gesetzlichen Bestimmungen der Bundesnetzagentur gewährleistet. Die Realisierung der Erweiterung soll nach dem abgeschlossenen Pilotbetrieb der Connect-Funktion erfolgen.

ENUM

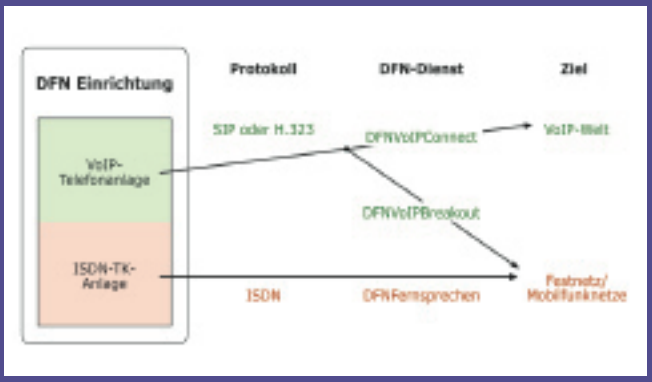
ENUM ist die Abkürzung von „telephone **nu**mber **m**apping“ und beschreibt eine Vorschrift für die Abbildung einer Telefonnummer auf eine Internet Domain. Z.B. wird aus +49308842990 => 0.9.9.2.4.8.8.0.3.9.4.e164.arpa. Unter dieser Domain können Kommunikationsadressen für verschiedene Applikationen abgelegt werden, insbesondere Informationen, wie die entsprechende Telefonnummer über VoIP erreicht werden kann. Über den sogenannten ENUM-Lookup kann mit Hilfe des DNS die Kommunikationsadresse einer VoIP-Telefonanlage oder eines VoIP-Telefons gefunden werden.
In sehr vielen Ländern der Welt wird ENUM pilotmäßig eingesetzt. In Österreich und Deutschland läuft bereits ein Regelbetrieb. Die DENIC eG ist in Deutschland für den Wirkbetrieb unter der Domain 9.4.e164.arpa zuständig. Der DFN-Verein ist Registrar für ENUM-Domains.
http://www.dfn.de/content/de/dienstleistungen/domain/enum/

Renate Schroeder

DFN-Verein
schroeder@dfn.de

Gesamtangebot

Durch Einsatz von DFNVoIPBreakout und DFNVoIPConnect können DFN Einrichtungen zukünftig ihren gesamten VoIP-Verkehr an die Plattform routen. Dort wird entschieden, ob das betreffende Telefonat über VoIP zugestellt werden kann oder über den Breakout in das öffentliche Telefonnetz geroutet werden muss (grüne Komponenten). Zusammen mit dem vorhandenen Angebot DFNFernsprechen für traditionelle Telefonanlagen (rote Komponenten) lässt sich das zukünftige Gesamtangebot in der folgenden Skizze darstellen.



Die Migration in Richtung VoIP erfolgt in den Einrichtungen schrittweise. Einrichtungen, die zusätzlich zur ISDN-TK-Anlage eine VoIP-Telefonanlage betreiben, können nach und nach ihre ISDN-Telefone abschalten und VoIP-Endgeräte anschließen. Das Angebot eines verknüpften Dienstes DFNFernsprechen/VoIP mit einer daraus resultierenden gemeinsamen Rechnungsstellung unterstützt diese sanfte Migration.

Betreibermodell

Bei Bedarf ist der Betrieb eines sogenannten Betreiber- bzw. Portmodells geplant. Dabei betreibt eine Einrichtung nur die VoIP-Telefone; der Betrieb der VoIP-Telefonanlage wird von einem Anbieter übernommen. Mehrere Einrichtungen können sich dadurch eine Telefonanlage oder ein Bündel von Telefonanlagen teilen. Durch ein Mandantensystem wird das gemeinsame System so verwaltet, dass jede Einrichtung nur die eigene Umgebung wahrnimmt und administrieren kann. Das Betreibermodell eignet sich insbesondere für kleinere Anwender oder Einrichtungen, die nicht das Personal für den Betrieb einer VoIP-Telefonanlage zur Verfügung stellen können.

Rechtliche Situation bei VoIP

Wie für die klassische Telefonie gilt auch für VoIP das Telekommunikationsgesetz und die Telekommunikationsüberwachungsverordnung. Nicht zuletzt vor diesem Hintergrund hat sich der DFN-Verein entschieden, mit einem Anbieter, der T-Systems, zusammenzuarbeiten, die die zur Einhaltung der gesetzlichen Vorschriften notwendige Systemtechnik vorhält.

Aktuelles aus dem Wissenschaftsnetz

DFN-PKI: Auslagerung großer Erfolg

Die Möglichkeit, den Betrieb der eigenen Zertifizierungsstelle (CA) an den DFN-Verein auszulagern, findet großen Zuspruch. Nur knapp fünf Monate nach Beginn des Regelbetriebs haben bereits mehr als 40 Einrichtungen davon Gebrauch gemacht. Vorteil dieser Lösung ist für die Anwender, dass sie keine spezielle Hard- und Software-Infrastruktur betreiben müssen und zudem der lokale Personalaufwand reduziert wird. Die Auslagerung der CA an den DFN-Verein ist für Einrichtungen, die den DFNInternet Dienst nutzen, ohne zusätzliches Entgelt verfügbar.

Wie im Rahmen der letzten DFN-Mitgliederversammlung angekündigt, besteht in der DFN-PKI ab Juli 2006 auch die Möglichkeit zum einfachen Bezug von Zertifikaten in großen Stückzahlen, wodurch die Nutzung der bekannten Webschnittstellen für einzelne Zertifikate ergänzt wird. Grundsätzlich gibt es dafür zwei unterschiedliche Verfahren: zum einen ein Self-Service Verfahren, bei dem die Schlüssel beim Nutzer erzeugt werden und das zugehörige Zertifikat umgehend ausgestellt wird, zum anderen ein Batch-Verfahren, bei dem die Schlüssel bei der Zertifizierungsstelle erzeugt werden. Voraussetzung in beiden Fällen ist, dass die Policy-Anforderungen an die Identifizierung der Nutzer eingehalten werden.

Informationen zur DFN-PKI finden Sie unter www.dfn.de/pki. Für Rückfragen stehen wir unter pki@dfn.de zur Verfügung.

2,7 Petabyte Verkehrsvolumen

Das ins X-WiN importierte monatliche Datenvolumen ist im April 2006 wiederum kräftig gestiegen und betrug annähernd 2,7 Petabyte. Mehr als 640 Terabyte davon entfielen auf die Übergabepunkte in das GÉANT2, das damit deutlich aus der ansonsten harmonischen Verteilung der Anteile am Importvolumen herausragt. Insgesamt haben im April 424 Anwender und 278 Mitnutzer den DFN-Internet-Dienst genutzt.

Bereits fünf 10 Gbit/s-Anschlüsse geschaltet

Im Mai wurden drei weitere 10 Gbit/s-Anschlüsse an das X-WiN geschaltet. Nach dem Forschungszentrum Karlsruhe und RWTH Aachen sind nun auch das DESY in Hamburg sowie die TU Dresden und das LRZ München mit 10 Gbit/s angeschlossen. Die derzeit höchste Klasse im DFN-Internet-Dienst hat einen spürbaren Anteil am Verkehrsaufkommen im X-WiN. So nahm der „Verbrauch" der beiden „Zehner" in Karlsruhe und Aachen im April mit einem Datenexport von mehr als 360 Terabyte einen Spitzenplatz bei der Netznutzung ein.

Neue MCUs und Test eines Webconferencing-Tools für DFNVC

Der DFN-Verein hat für den Dienst DFNVideoconference (DFNVC) zwei Codian MCUs mit je 40 Video- und Audio-Ports beschafft. Wesentlicher Vorteil der neuen MCUs für den Nutzer ist die Durchführung von Konferenzen ohne vorherige Auswahl von Service-Definitionen. Bis Mitte Juni erfolgt die Integration der MCUs in das DFNVC-Dienstangebot, anschließend startet der Pilotbetrieb.
Außerdem steht ab Mitte Juni ein Recorder mit fünf Ports zur Verfügung. Der Recorder ermöglicht die parallele Aufzeichnung von fünf MCU-Konferenzen, die anschließend über Quicktime oder Real Player abgerufen werden können.
Für die Erweiterung des Videokonferenzdienstes um ein einfaches Webconferencing Tool wurde das Produkt Breeze von Macromedia (Adobe) ausgewählt. Breeze erfüllt mit einer Reihe von Features die wesentlichen Anforderungen an den Austausch von Audio, Video und Daten in einer Webkonferenz und ist sehr einfach über Browser und Flash zu bedienen. Zur Zeit ist eine Server-Teststellung eingerichtet. Die Aufnahme des Pilotbetriebs ist für Anfang Juli geplant.

http://www.vc.dfn.de/

Phase Zwei beim X-WiN-Ausbau steht bevor

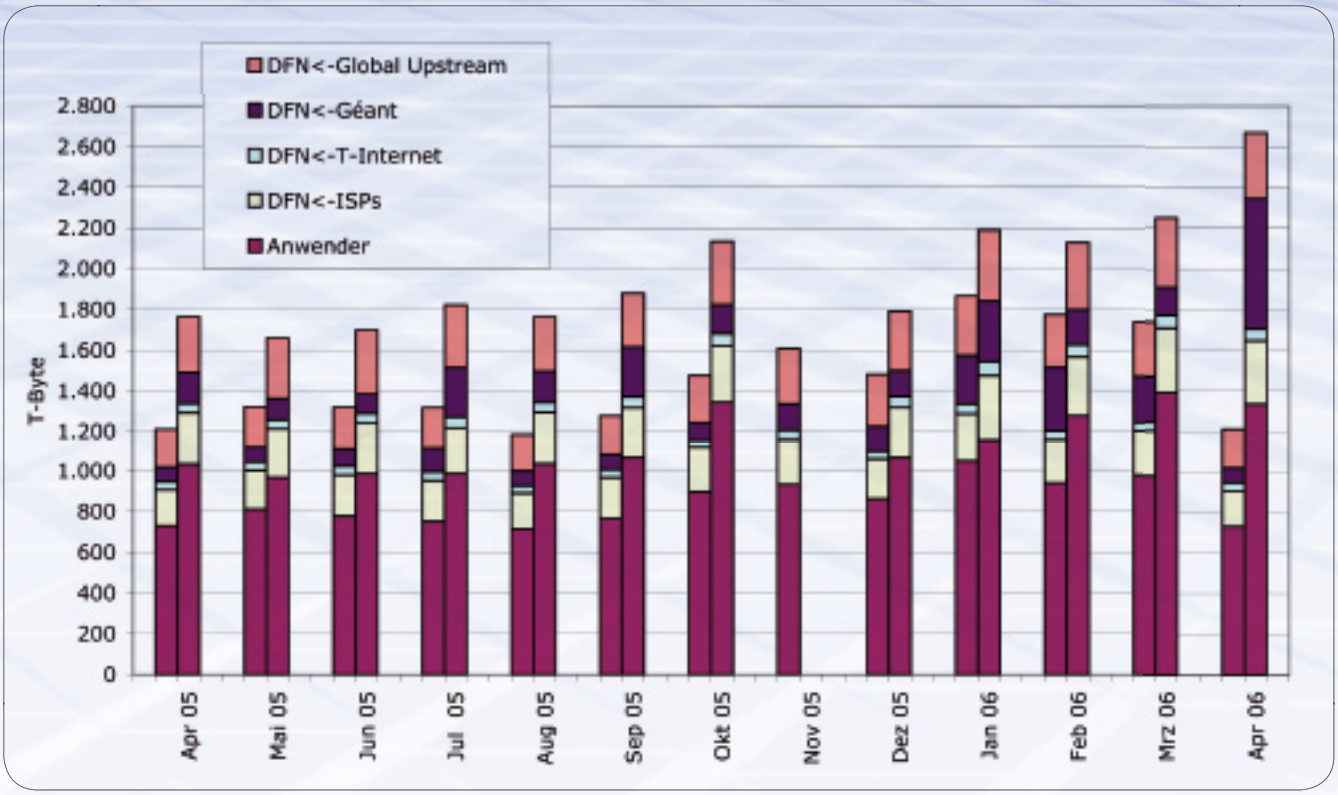
Ab Juli tritt das X-WiN in seine zweite Ausbauphase, in der es zu einem Re-Design der Routerplattform kommen wird. Künftig werden vier CISCO CRS1 Router an den zentralen Knotenpunkten des Netzes die Verbindungen der Ring-Trassen untereinander bewältigen. Um eine reibungslose Migration vom G-WiN auf das X-WiN gewährleisten zu können, bildete das X-WiN in seiner ersten Ausbaustufe die logische Struktur des Vorgängernetzes ab. In der zweiten Ausbaustufe erfolgt nun die Anpassung an die physikalische Topologie des X-WiN, die einzelne Verbindungen aus dem Vorgänger-Netz überflüssig macht.

Erfolgreiches VIOLA-Review 2006

Am 30. März 2006 fand das zweite Review für das Projekt VIOLA statt, um mit verschiedenen Gutachtern, Vertretern des BMBF sowie des Projektträgers im DLR die bisherigen Ergebnisse aus VIOLA und die noch offenstehenden Aufgaben für das dritte Projektjahr zu diskutieren. Sowohl im Netzbereich, als auch im Middleware- und Anwendungsbereich wurden den Projektbeteiligten von den Gutachtern sehr gute Ergebnisse bescheinigt. Empfohlen wurde u.a. eine Intensivierung der Zusammenarbeit mit den EU-Projekten. Das erfolgreiche Review-Meeting hat dazu geführt, dass alle für VIOLA bereitgestellten Finanzmittel für das dritte Projektjahr entsperrt wurden.

http://www.viola-testbed.de/

Entwicklung des importierten Datenvolumens (linke Balken: Vorjahresvolumina)



Sesam öffne dich

DFN-AAI bietet kontrollierten Zugang zu geschützten Ressourcen

Ulrich Kähler

DFN-Verein
kaehler@dfn.de

Mit dem Anwachsen der Informationsmengen im Internet existieren auch immer mehr Informationen, die nicht für die Öffentlichkeit bestimmt sind, sondern nur definierten Gruppen von Nutzern zugänglich gemacht werden sollen. Auf Anregungen aus dem Bibliotheksbereich (BMBF-finanziertes AAR-Projekt) und den deutschen Grids und in Kooperation mit zahlreichen interessierten Wissenschaftseinrichtungen arbeitet der DFN-Verein derzeit an dem Aufbau einer Infrastruktur für Authentifizierung und Autorisierung (AAI), mit der die bisherigen Verfahren für den kontrollierten Zugang zu Informationen nicht nur vereinfacht, sondern auch vereinheitlicht werden.

Um die Versorgung mit elektronischer Fachinformation an deutschen Hochschulen, Forschungseinrichtungen und wissenschaftlichen Bibliotheken nachhaltig zu verbessern, finanziert die Deutsche Forschungsgemeinschaft seit 2004 den Erwerb sogenannter Nationallizenzen. Ziel ist es, Wissenschaftlern und Studierenden den kostenlosen Zugang zu Datenbanken zu ermöglichen. Es ist noch nicht endgültig geklärt, wie dieser kostenlose Zugang organisatorisch und technisch gelöst werden soll. Mit einer DFN-weiten AAI wäre nicht nur für die Nationallizenzen der DFG eine Lösung geschaffen. Eine Vielzahl ähnlicher Anforderungen im Bereich der Wissenschaften könnten mit einer solchen Infrastruktur erfüllt werden. So betreibt z. B. das Netzwerk für die Erkennung von Veränderungen der Stratosphäre (NDSC) über die ganze Erde verteilt mehr als 70 hochsensible Messstationen zur Überwachung des physikalischen und chemischen Zustandes der Stratosphäre und der oberen Troposphäre. Untersucht wird unter anderem die Veränderung des Ozon-Gehaltes der Lufthülle. Für eine gewisse Zeit, in der Wissenschaftler aus vielen Ländern von ihren Heimatforschungsinstituten aus die Messdaten auswerten, sind die Messergebnisse geschützt und werden dann später der Öffentlichkeit zur Verfügung gestellt. Basis für das Funktionieren dieser internationalen Kooperation ist das Vorhandensein nationaler Infrastrukturen für Authentifizierung und Autorisierung (AAI).

Bisherige Ad-Hoc-Lösungen

Bislang wird die Authentifizierung und Autorisierung in der Regel unter Verwendung von Benutzerkennungen und Passwörtern direkt beim Anbieter von Informationen (im Folgenden „Anbieter" genannt), z.B. einem Verlag oder einem Software-Vertrieb, durchgeführt. Der Anbieter hat keine regelmäßigen Informationen darüber, ob ein Student noch eingeschrieben ist und beispielsweise eine Campus-Lizenz beim Kauf einer Software in Anspruch nehmen darf. Auf Seiten der Nutzer besteht das Problem, dass eine bestimmte Menge an Passwörtern dazu führt, dass das jeweils Benötigte im entscheidenden Moment nicht zur Hand ist.

Andere Verfahren wie die IP-Adressenprüfung funktionieren nicht von zu Hause bzw. auf Reisen, weshalb Nutzer ausschließlich aus dem Institut heraus auf Informations- und Dienstleistungsangebote zugreifen können. Indem IP-Adressenprüfungen nicht personenbezogen organisiert sind, ergeben sich auch erhebliche Unsicherheitsfaktoren. In der Praxis wird die IP-Adresslösung häufig mit einer Vielzahl fantasievoller Einzellösungen kombiniert. Hier sind Gruppenkennungen oder die Kombination von IP- und Passwortschutz zu nennen. Häufig werden auch VPN-Tunnel eingesetzt, um eine Nutzung von Instituts-Accounts von zu Hause aus zu ermöglichen.

Unterschiedliche Anforderungen mit gemeinsamer Lösung

Grundsätzliches Problem aller skizzierten Szenarien ist, dass es dem Anbieter einer Dienstleistung oder Information überlassen bleibt, Authentifizierung und Autorisierung eines Nutzers durchzuführen. Das Problem besteht darin, dass der Anbieter hierfür nicht über die nötigen Informationen verfügt, da diese in der Regel in den Wissenschaftseinrichtungen als den DFN-Anwendern (im Folgenden als „Anwender" bezeichnet) liegen, denen die Nutzer angehören.

Die drei beteiligten Partner haben hierbei unterschiedliche Anforderungen:

1. Die **Anbieter** suchen Schutz vor unberechtigtem Zugriff auf ihre Ressourcen bei einem möglichst geringen Aufwand.
2. Die **Anwender** möchten ihren Nutzern berechtigten Zugriff gewähren und dabei ebenfalls möglichst geringen Aufwand betreiben.
3. Die **Nutzer** benötigen einerseits einen ortsunabhängigen Zugriff und möchten andererseits mehrere Angebote nach nur einmaliger Authentifizierung nutzen (Single Sign-On).

Als Lösung bietet sich der Aufbau einer Infrastruktur zur Authentifizierung und Autorisierung (AAI) an, die den kontrollierten Zugriff auf geschützte Ressourcen ermöglicht. Grundidee hierbei ist die räumliche und logische Trennung von Authentifizierung und Autorisierung. Während der Anwender,

der über die aktuellen personenbezogenen Daten verfügt, gut geeignet ist, die Identifizierung durchzuführen und den Nutzer damit zu authentifizieren, sollte die Autorisierung, also die Gewährung des Zugriffs, dem Anbieter überlassen bleiben.

Der Anmeldewunsch eines Nutzers, der sich bei einem Anbieter einwählt, wird zum Zwecke der Identifizierung zu seiner Heimateinrichtung (Anwender) umgeleitet. Die Identifizierung des Nutzers erfolgt dort mit den beim Anwender üblichen Verfahren, z.B. mittels User-ID und Passwort, Chipkarte oder Token. Der Anwender meldet dem Anbieter daraufhin die erfolgreiche Authentifizierung. Der Anbieter kann nun bei Bedarf weitere Daten über den Nutzer anfordern, etwa wenn er wissen muss, ob der Nutzer Student, Wissenschaftler oder Gasthörer einer Hochschule ist. Weit größeres Interesse besteht unter Umständen auch an der Art der Authentifizierung, um zu prüfen, ob erhöhten Sicherheitsansprüchen genüge getan wurde. So verlangt der Zugriff auf medizinische Informationsbestände in der Regel relativ starke Authentifizierungen auf einem hohen Sicherheitsniveau, während es für die Online-Bestellung einer Software in der Regel genügt, sich mit ID und Passwort zu identifizieren.

Auf der Basis einer zwischen Anwender und Anbieter geschlossenen Lizenzvereinbarung kann der Anbieter anhand der Daten, die ihm die Hochschule liefert, entscheiden, ob er dem Nutzer Zugriff gewährt. Beispielsweise kann es erforderlich sein, dass der Anbieter vom Anwender die Attribute „Mitarbeiter“ und „Chemiker“ geliefert bekommt, um den Zugriff auf eine pharmazeutische Datenbank zu erlauben.

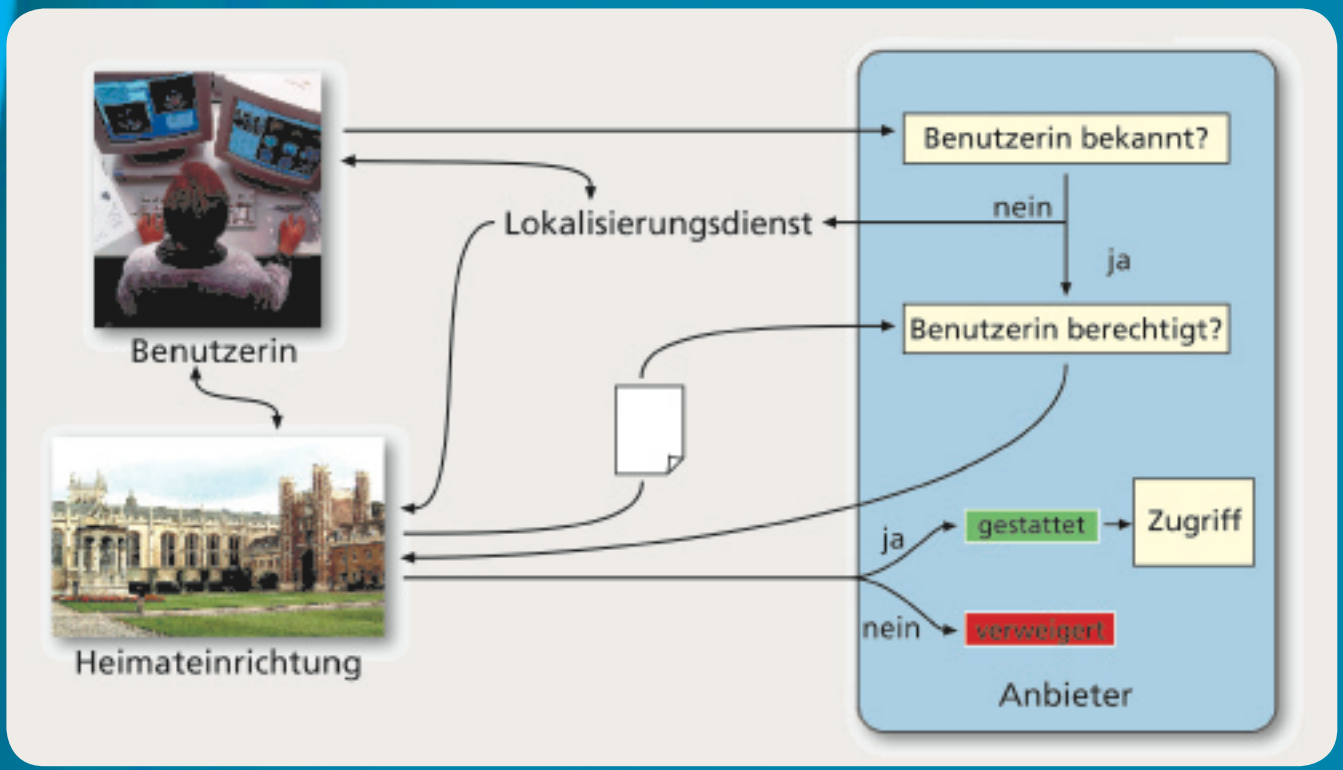
Voraussetzungen für den Aufbau einer AAI

Für den Betrieb einer AAI gelten mehrere Voraussetzungen. Zunächst muss ein Vertrauensverhältnis zwischen Anwendern und Anbietern etabliert werden. Darüber hinaus müssen eine Public-Key-Infrastruktur und ein Identity-Management-System beim Anwender verfügbar sein. Da es in den meisten Anwendungsfällen für eine AAI um geldwerte Leistungen geht, die von den Anwendern bezahlt werden müssen, bedarf es vertraglicher Regelungen zwischen den Anbietern, etwa den Verlagen für digitale Medien und den Anwendern.

Regeln innerhalb der DFN-AAI

In der DFN-AAI müssen die Verantwortungen und Modalitäten der Kommuniktion zwischen den beteiligten Partnern geregelt werden. Dies geschieht mithilfe von vertraglichen Vereinbarungen zwischen DFN-Verein, Anwendern und Anbietern, die die Verlässlichkeit der Kommunikationbeziehungen und des Datenaustausch zum Gegenstand haben. Bestehende oder zukünftige Lizenzvereinbarungen über die Nutzung von Informationsinhalten zwischen den Beteiligten sind dabei nicht betroffen und behalten weiterhin ihre Berechtigung.

‚Prinzip-AAI‘



Bei der DFN-AAI tritt der DFN-Verein als zentraler Vertragspartner für alle Teilnehmer auf. Für die Anwender bedeutet die Teilnahme an der DFN-AAI, dass sie mit Abschluss *eines* Vertrages kontrollierten Zugang zu *verschiedenen* Anbietern bekommen. Umgekehrt erreichen Anbieter mit *einem* Kontrakt Zugang zu einer Vielzahl von Anwendern. Im Falle der eingangs geschilderten Nationallizenz der DFG würde dies bedeuten, dass der Anbieter der Nationallizenz nicht mehr Hunderte von IP-Adressen von Anwendern (hier Hochschulen) verwalten muss, sondern mit einer einzigen Vereinbarung über den DFN-Verein als zentralen Betreiber der AAI die Gesamtheit der Hochschulen erreicht würde.

Die Verträge, die der DFN-Verein in diesem Zusammenhang mit den Anbietern und Anwendern schließt, regeln unter anderem die Qualitätsanforderungen an das Identity-Management, die Ausgestaltung der technischen Schnittstellen, den Austausch von Attributen und das Vorgehen bei Verstößen. Darüber hinaus übernimmt der DFN-Verein zentrale betriebliche Aufgaben. Hierzu gehört der Betrieb eines Testsystems, die Verwaltung von Metadaten der teilnehmenden Anwender und Anbieter und der Betrieb eines Lokalisierungsdienstes (Where-Are-You-From-Server - WAYF). Außerdem wird der DFN-Verein Beratung und Schulungen anbieten sowie die internationale Vertretung der Anwender übernehmen.

Zur technischen Realisierung wird in der DFN-AAI das Programmpaket „Shibboleth" eingesetzt. Shibboleth ist eine Entwicklung der US-amerikanischen INTERNET2-Initiative und beruht auf den international gängigen Standards HTTP, XML, XML Schema (XSD), XML Signatur (XMLDisg), SOAP sowie SAML 1.1 (später 2.0). Shibboleth besteht im Wesentlichen aus zwei Software-Komponenten, die für die Seite der Anbieter sowie für die Seite der Einrichtungen konzipiert wurden. Der Einsatz von Shibboleth gewährleistet die vollständige Kompatibilität z.B. zu internationalen Verlagen, die den Zugriff vieler ihrer Datenbestände über Shibboleth organisieren.

PKI als Voraussetzung von AAI

Der Betrieb einer AAI setzt an mehreren Stellen gesicherten Datenverkehr zwischen dem Anbieter, dem Anwender und gegebenenfalls dem Nutzer voraus: so kommen zur Sicherung der Kommunikation zwischen den beteiligten Rechnern Server-Zertifikate zum Einsatz. Für bestimmte Anwendungen ist es notwendig, dass sich der Nutzer an seiner Heimateinrichtung unter erhöhten Sicherheitsanforderungen identifiziert. Hier kommen personenbezogene Zertifikate zum Einsatz.

Eine solche Infrastruktur für die Verteilung und Verwaltung von Zertifikaten (DFN-PKI) wurde in den vergangenen Jahren erfolgreich im DFN aufgebaut und kann für AAI-Zwecke sofort eingesetzt werden.

Anforderungen an das Identity-Management

Zur Nutzung des Dienstes DFN-AAI ist es seitens des Anwenders nötig, dass er den Identity-Provider-Teil des Shibboleth-Systems an seiner Einrichtung betreibt. Dieser Teil von Shibboleth regelt den Verkehr zwischen Anbieter und dem beim Anwender vorhandenen Identity-Management-System. Standardmäßig ist ein Anschluss an LDAP- und SQL-basierten Verzeichnissen vorgesehen. Weitere Schnittstellen können mit Hilfe von Java-Scripten hinzugefügt werden. Welche Art von Identity-Management-System der Anwender einsetzt, spielt keine Rolle, solange eine entsprechende Schnittstelle zu Shibboleth vorhanden ist.

Die Teilnahme an der DFN-AAI stellt Qualitätsanforderungen an die betriebliche Organisation des Identity-Management-Systems in Bezug auf Verlässlichkeit, Aktualität und Ausfallsicherheit. Eine detaillierte Spezifikation der Anforderugen ist zur Zeit in Arbeit.

Ausblick

DFN-AAI wird derzeit unter Mitwirkung einer Vielzahl von interessierten Einrichtungen und Informations- bzw. Dienstleistungsanbietern aus den Bereichen Bibliothekswesen, Grid und e-Leaning zu einem betriebsbereiten Dienst ausgebaut. Eine Testinstallation des Shibboleth-Systems kann bereits jetzt am LRZ München, an der Universität Freiburg und in der Geschäftsstelle des DFN-Vereins verwendet werden. Interessenten für die Teilnahme an diesem Testbetrieb wenden sich bitte an den Autor dieses Artikels unter: aai@dfn.de.

Das DFN-Labor – Qualitätssicherung im Wissenschaftsnetz

Birgit König
birgit.koenig@dfn.de

Dr. Stephan Kraft
stephan.kraft@dfn.de

Seit mehr als 12 Jahren besteht das am Regionalen Rechenzentrum (RRZE) der Universität Erlangen-Nürnberg angesiedelte DFN-Labor. Über die Zeit hat sich nicht nur der Name von „B-WiN Labor" über „G-WiN Labor" in „DFN-Labor" geändert, sondern auch die Aufgaben wurden neuen Anforderungen, neuer Hardware und neuen Technologien angepasst.

So hat das DFN-Labor das G-WiN von seiner Inbetriebnahme bis zu seinem Ende im Dezember 2005 aktiv begleitet. Qualitätskontrolle, Dienstgüteüberwachung, Verkehrsflussmessungen, Hardwaretests waren u.a. Aufgaben, die das Labor für den DFN-Verein wahrgenommen hat.

Im Laufe der bisherigen Arbeiten wurden verschiedene Systeme entwickelt, die bereits im G-WiN erfolgreich zum Einsatz kamen.

IP-Performance Measurement System

Ein Beispiel der Forschungs- und Entwicklungsarbeit ist das vom Labor entwickelte IPPM-Messsystem, welches erst in jüngster Zeit den Namen Hades (Hades Active Delay Evaluation System) bekam.

Basierend auf den Ansätzen der IETF wurde 1998 in der Working Group IPPM ein umfangreiches Rahmenwerk verabschiedet. Dazu wurde im Labor ein System entwickelt, welches qualitätsrelevante Daten wie One-Way Delay (Paketlaufzeit), One-Way Delay Variation (Laufzeitschwankung) und Packet Loss (Paketverluste) ermittelt.

Eine Sendestation erzeugt Gruppen von UDP-Paketen (UDP: User Datagram Protocol) in konfigurierbaren Abständen, versieht jedes Paket mit einem aktuellen Zeitstempel und einer Sequenznummer und sendet sie zu einer Empfangsstation. Diese wiederum bestimmt die aktuelle Empfangszeit und schreibt die gesammelten Daten in eine Datei. Daraus lassen sich One-Way Delay, Delay Variation und Paketverluste auf den einzelnen Messstrecken bestimmen.

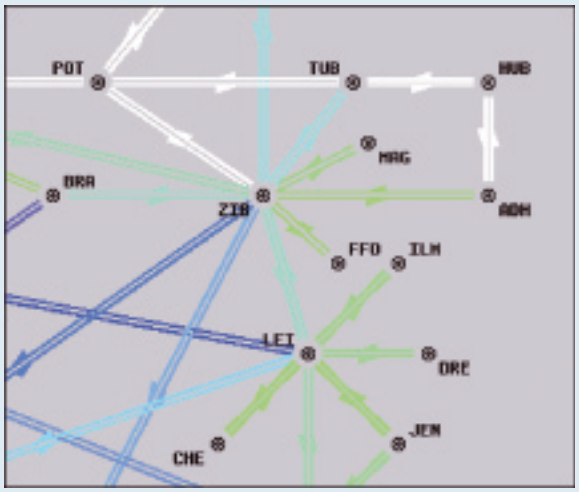


Abbildung 1: Webdarstellung der IPPM-Messungen im X-WiN (Auszug)

Für die IP-Performance Messungen im G-WiN Nachfolgenetz X-WiN wurden auch die neu hinzugekommenen Kernnetzstandorte mit Mess-Equipment ausgestattet. Während es im G-WiN nur 27 Kernnetzstandorte gab, sind es im X-WiN fast 50. In einer überarbeiteten graphischen Darstellung (siehe Abbildung 1), die der neuen Topologie Rechnung trägt, werden auch im X-WiN vollvermaschte Messungen von One-Way Delay, One-Way Delay Variation und Packet Loss durchgeführt. Da es im X-WiN bereits erste Standorte ohne Router gibt, wird sich die Weiterentwicklung von Hades vor allem mit dem Thema IP-Dienstgüteüberwachung auf Layer 2 (data link layer) beschäftigen.

Hades geht mittlerweile im Rahmen eines EU-Projektes auch internationale Wege: Mit diesem erfolgreichen Messsystem nimmt das DFN-Labor am EU-Projekt GÉANT2 teil. Die speziellen Aufgaben liegen in den Teilprojekten JRA1 (Joint Research Activity) und SA3 (Service Activity). Während in JRA1 verschiedene Methoden zur Bestimmung der Performance hinsichtlich Verwendung und Nutzbarkeit verglichen werden sollen, konzentriert sich das Teilprojekt SA3 darauf, ein verteiltes Performance Monitoring System zur Überwachung der Dienstgüte einzurichten und in Betrieb zu nehmen. JRA1 dient somit als Entwicklungsphase und Wegbereiter für die in SA3 geplante Betriebsphase.

Ein Ergebnis des JRA1-Projektes war der Einsatz des im DFN-Labor entwickelten IPPM-Messsystems innerhalb Europas und darüber hinaus. Ziel ist es nun, das entwickelte Messsystem auch im europäischen Wissenschaftsnetz GÉANT2 und in den USA zu verbreiten.

Über zwanzig Messgeräte sind bereits an Standorten innerhalb Europas und in den USA installiert (siehe Abbildung 3). Davon sind mehr als 15 schon im Einsatz und liefern Messergebnisse von den Verbindungen innerhalb des europäischen Netzes.

Das DFN-Labor besteht momentan aus sechs Mitarbeitern (v.l.n.r.): Dr. Stephan Kraft, Ralf Kleineisel, Birgit König, Roland Karch, Verena Venus, Jochen Reinwand

Qualitätskontrolle durch SNMP-Daten Auswertung

Im Rahmen der Qualitätskontrolle im G-WiN wurden Managementdaten der SDH/WDM-Plattform (SDH: Synchronous Digital Hierarchy, WDM: Wavelength Division Multiplexing) und Daten aus anderen und eigenen Informationsquellen ausgewertet, aufeinander abgebildet und der DFN-Geschäftsstelle zur Verfügung gestellt. Dazu hat das Labor ein Programmsystem entwickelt, welches auf Basis der an den G-WiN-Routern abgefragten SNMP-Daten (SNMP: Simple Network Management Protocol) eine Auswertung der täglichen Verfügbarkeit vornimmt und diese hinsichtlich des Ausfallverursachers beurteilt.

Im Gegensatz zum G-WiN, in dem die Qualitätskontrolle durch Abfrage und Auswerten der SNMP-Daten vorrangig dazu diente, die Managementdaten des Carriers zu kontrollieren, wird das SNMP-Auswertungssystem im X-WiN als eigenständiges System zur Bestimmung der Verfügbarkeit des Netzes genutzt.

In Abbildung 2 sieht man einen Auszug der SNMP-Daten Auswertung für einen Tag. „D“ steht für einen Fehler am DFN-Equipment und „U“ für einen Ausfall auf Leitungsebene.

```
##############################################################
 Auswertung für 2006/04/23
##############################################################

[...]

*** Leitung STM16/HUA0040_BIR_DUI
    von POS0/1 cr-koeln1 (Interface-ID: 333)
    nach POS0/3 cr-essen1 (Interface-ID: 338)
    DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD 13:00
    DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD 24:00

*** Leitung GE/HUA0188_HAN_POT
    von GigabitEthernet0/2 cr-hannover1 (Interface-ID: 347)
    nach GigabitEthernet0/2 ar-potsdam2 (Interface-ID: 400)
    ..................................................... 12:00
    ..................................................... 24:00

*** Leitung STM04/HUA0051_FRA_ZIB
    von POS1/0 cr-berlin1 (Interface-ID: 53)
    nach POS13/0 cr-frankfurt1 (Interface-ID: 90)
    ....................UUUUUUUUUUUUUUUUUUUUUUUUU 12:00
    U.................................................. 24:00

[...]

D ... Fehler am DFN-Equipment
U ... Leitungsstoerung
```

Abbildung 2: Viertelstündliche SNMP-Datenauswertung ausgewählter X-WiN Verbindungen

Accountingsystem (Verkehrsflussmessungen)

Das Labor verarbeitet Accountingdaten aus den Routern des WiNs. Zur Analyse dieser Daten hinsichtlich der Darstellung von Verkehrsbeziehungen sind auch eine Reihe anderer administrativer Tätigkeiten nötig. Insbesondere die Ermittlung der aktuellen Netztopologie und die Zuordnung der Accountingdaten zu den Kunden ist ein wesentlicher Bestandteil des vom Labor entwickelten Accountingsystems.

Als nächster Schritt wird ein Umzug von cflowd auf flow-tools angestrebt. Diese Tools sammeln die von den Routern exportierten Netflow-Daten. Diese Daten werden von dem im Labor entwickelten System ausgewertet, in einer Datenbank abgelegt und anschließend visualisiert. Ein Redesign der Topologiedatenbank und neue Hardware sollen zu einer Performancesteigerung des Systems führen.

Zusätzlich zu den Verkehrsstatistiken werden im Labor auch die Clusteranschlüsse und die Mitnutzeranschlüsse analysiert.

Informationen, Kontakt und Literatur

Mehr Informationen zur Arbeit des DFN-Labors, den entwickelten Systemen und den laufenden IPPM-Messungen finden Sie unter http://www.win-labor.dfn.de. Bitte entnehmen Sie dort auch die entsprechenden Kontaktdaten.

- http://www.ietf.org/
- http://www.ietf.org/html.charters/ippm-charter.html
- http://www.rfc.org.uk/cgi-bin/lookup.cgi?rfc=3393
- http://www.geant2.net/
- http://www.caida.org/tools/measurement/cflowd/
- http://www.splintered.net/sw/flow-tools/

Abbildung 3: Übersicht über IPPM-Messstationen innerhalb Europas und darüber hinaus

Nachgefragt.

Redaktion: Was war der Anstoß für die Entwicklung ihres erfolgreichen IPPM-Messsystems?

Dr. Stephan Kraft: Ausgangspunkt war eine Diplomarbeit mit dem Thema „Implementation eines Programms zur Bestimmung der Dienstgüte in IP-Netzen" eines Studenten der Erlanger Universität. Diese wurde im Labor betreut. Die Idee der Arbeit basierte auf Ansätzen der IETF. In der Working Group IP Performance Metrics (IPPM) wurde dazu 1998 ein umfangreiches Rahmenwerk verabschiedet.

Redaktion: Und von der Idee bis zur ersten Messstation ...?
Dr. Stephan Kraft: ... war viel Entwicklungsarbeit nötig. Zusätzlich zur eigentlichen Programmierung kamen auch noch Tests mit verschiedenen Zeitquellen und die Zusammenstellung geeigneter Mess-PCs.

Redaktion: Wann haben sie die erste Messstation in Betrieb genommen?

Dr. Stephan Kraft: Die erste Messstation wurde im Sommer 2002 in Erlangen in Betrieb genommen. Mit der letzten Messstation in Stuttgart im November 2003 waren die Kernnetzknoten des G-WiNs komplett ausgestattet.

Redaktion: Wie sieht es im neuen Netz, im X-WiN, aus?

Dr. Stephan Kraft: Die neuen Standorte haben mittlerweile alle eine von uns installierte und konfigurierte Messbox inklusive einer GPS-Antenne bekommen. Die Messstationen sind zu einem großen Teil bereits in Betrieb. Durch die neue Topologie des Kernnetzes im Gegensatz zum G-WiN musste unsere graphische Darstellung an die neuen Bedürfnisse angepasst werden.

Redaktion: Gibt es IPPM-Messungen nur im Kernnetz?

Dr. Stephan Kraft: Nein. Eine Messstation kann mit mehreren Netzkarten ausgestattet werden. Die erste wird mit dem X-WiN verbunden, die zweite kann an einen Switch des Kunden angeschlossen werden.

Redaktion: Welcher Nutzen ergibt sich für den Kunden?

Dr. Stephan Kraft: Der Kunde kann somit die Performance seines Anschlusses, also bis zur Einrichtung selbst, beobachten und damit mehr Informationen über die jeweilige Ende-zu-Ende Dienstgüte bekommen. Darüber hinaus besitzt das DFN-Labor einige mobile Messstationen mit PZF-Zeitsynchronisation, die flexibel an verschiedenen Standorten eingesetzt werden können. Damit ist es möglich, bei Kunden, die beispielsweise Probleme mit der Videokonferenzübertragung haben, gezielt auf Fehlersuche im (Kunden-)Netz zu gehen.

Redaktion: Wo kann man die Messergebnisse sehen?

Dr. Stephan Kraft: Das Labor stellt auf seiner Homepage (http://www.win-labor.dfn.de) unter der Rubrik IPPM Hintergrundinformationen und eine graphische Darstellung des gesamten Netzes zur Verfügung. Zusätzlich können einzelne Messergebnisse für auszuwählende Standorte bzw. Messstrecken angezeigt werden.

Redaktion: Wie genau ist das System?

Dr. Stephan Kraft: Die Genauigkeit der NTP-Synchronizität mittels GPS liegt bei ca. 7 µs. One-Way Delays im X-WiN liegen im Bereich von 10 ms.

Redaktion: Wie zeitnah ist das Messsystem?

Dr. Stephan Kraft: Die graphische Darstellung des gesamten Netzes erneuert sich alle 10 min automatisch. Das OWD einer Verbindung wird dabei aus dem Median der letzten 21 angekommenen Pakete zum Zeitpunkt des Updates der Kartendarstellung ermittelt. Als Weiterentwicklung bzw. Ergänzung des eigentlichen Systems gibt es seit einiger Zeit auch ein Alarmsystem, das bei Unregelmäßigkeiten wie beispielsweise Paketverlusten eine Alarm auslöst. Angedacht ist ein dreistufiges Alarmsystem, wobei die erste Stufe weitestgehend realisiert ist. Das heißt, es existiert ein einfaches Warnsystem, das genau dann aktiv wird, wenn gesetzte Schwellwerte für OWD und Packet Loss überschritten werden.

Redaktion: In welcher Weise wird das System weiterentwickelt?

Dr. Stephan Kraft: In einer zweiten Stufe des Alarmsystems sollen ergänzende Eigenschaften wie Fehlereingrenzung und Filtern der Alarme nach administrativen Bereichen hinzukommen. Die dritte Stufe sieht ein adaptives Alarmsystem vor, so dass beispielsweise im Falle eines regelmäßigen, zeitlich abhängigen Delayanstiegs keine Alarmierung erfolgt. Andere Stichworte für die Zukunft sind On-Demand-Messungen, Protokoll- und gerätespezifische Messungen, IPv6 und Multicast.

Performance-Monitoring für Europas Forschungsnetz

Sibylle Schweizer-Jäckle

DFN-Verein
E-Mail: schweizer@dfn.de

Für die Netzüberwachung und das Performance Monitoring existieren eine Reihe verschiedenartiger Werkzeuge. Jedes Forschungsnetzwerk benutzt eine andere Untermenge davon, um Informationen über den Status seiner Netzwerkinfrastruktur zu erhalten. Teilweise kommen Eigenentwicklungen zum Einsatz, teilweise werden bereits existierende Entwicklungen derart modifiziert, dass sie in das Umfeld des jeweiligen Forschungsnetzes passen. Bei internationalen Verbindungen, die in der Regel über mindestens zwei nationale Forschungsnetze und das europäische Forschungsnetz geführt werden, ist es daher sehr schwierig, die Performance der gesamten Verbindung zu beurteilen.
Mit dem Aufbau von GÉANT2, dem aktuellen europäischen Forschungsnetz, startete im September 2004 im Rahmen der „Joint Research Activities" (JRA) auch ein Entwicklungsprojekt für den Aufbau eines Performance-Monitoring-Systems (JRA1). Bei diesem Projekt werden im wesentlichen drei Hauptziele verfolgt:

- Die Netzwerkmanagement- und Performance-Informationen sollen über ein spezifiziertes Interface für verschiedene Gruppen bereitgestellt werden. Darunter fallen z.B. die Betriebsgruppen von GÉANT2 und das europäische PERT (Performance Enhancement Response Team), das z.B. in Fällen verminderter Übertragungsqualität tätig wird. Darüber hinaus benötigen auch nationale Forschungsgruppen und solche von regionalen bzw. Campus-Netzwerken sowie viele Anwender mit hohem Datenvolumen z.B. in GRIDs ein Performance-Monitoring-System.
- Die Menge der zu erfassenden Netzwerkmanagement- und Performance-Daten soll deutlich erhöht werden. Dabei sind Verbindungsauslastung, Verbindungskapazität, One-Way-Delay, Delay-Variation, erreichter Durchsatz, Interface-Fehler und Paketverluste von besonderem Interesse.
- Werkzeuge zum Sammeln und Verarbeiten von Netzwerkmanagement- und Performance-Daten, die zu verschiedenen Netzen gehören, sollen entwickelt und implementiert werden. Vorhandene Werkzeuge sollen verbessert und den Nutzerbedürfnissen angepasst werden. Die größte Herausforderung liegt dabei darin, die Interoperabilität mit allen bestehenden Messsystemen zu gewährleisten.

Mittlerweile hat JRA1 gemeinsam mit den beiden US-amerikanischen Initiativen ESnet (Energy Sciences network) und Internet2 einen ersten Prototyp ihrer Netzüberwachungsarchitektur freigegeben. Dieser Prototyp namens perfSONAR (Performance focused Service Oriented Network monitoring ARchitecture) besteht aus einer Kombination aus Messwerkzeugen, Datenspeicher, Sicherheitsdiensten, Topologieinformationen und Visualisierungswerkzeugen.
Der DFN-Verein arbeitet aktiv an den Entwicklungen zu perfSONAR mit. Ein Schwerpunkt liegt bei den Messwerkzeugen. Hierzu wurden die aus dem G-WiN bekannten IPPM-Messungen (IP-Performance-Measurement) zur Bestimmung von One-Way-Delays, Delay-Variation und Paketverlusten weiterentwickelt. Für Available-Bandwidth-Messungen wurden bestehende Werkzeuge für den Einsatz in perfSONAR angepasst.
Ein anderer Schwerpunkt des DFN-Vereins liegt bei der Entwicklung von Visualisierungswerkzeugen. Hierzu wird neben anderen Visualisierungswerkzeugen das aus dem G-WiN bekannte CNM (Customer Network Management) weiterentwickelt. In der Prototypversion wird die Auslastung und Kapazität der Verbindungen von GÉANT2, Uninett (norwegisches Forschungsnetz), SWITCH (Forschungsnetz der Schweiz), Surfnet (Niederländisches Forschungsnetz) und Esnet graphisch dargestellt. Weitere Forschungsnetze sollen ebenso folgen wie weitere Netzcharakteristika, z.B. Delay, Jitter, Paketverluste und Available Bandwidth (verfügbare Bandbreite).
PerfSONAR ermöglicht es zum ersten Mal, Daten aus unterschiedlichen Netzwerken auf einheitliche Weise zu präsentieren. Der erste Schritt, um Netzwerk Performance von Endnutzer zu Endnutzer verfügbar zu machen, ist erfolgt. Fehlersuchen bei Transferproblemen werden dadurch stark vereinfacht.
EGEE (Enabling Grids for E-SciencE) kann als Teilnehmer der Prototyp-Phase bereits aus perfSONAR Nutzen ziehen. Über ein perfSONAR Interface erhält EGEE Daten zur weiteren Analyse.
Bereits bei der Entwicklung dieses Prototyps wurde eng mit Forschungsteams aus USA zusammengearbeitet. Diese unterstützten nicht nur die Entwicklung dieses Systems, sondern setzen es auch in ihren eigenen Netzwerken ein. Damit können bereits auf zwei Kontinenten Daten auf einheitliche Weise dargestellt werden.

Weitere Informationen unter http://www.geant2.net/

Paneuropäische Vernetzung mit GÉANT2

Insgesamt 12.000 Kilometer an Leitungen verbinden die nationalen Forschungsnetze Europas untereinander. Damit ist GÉANT2 das größte Netzwerk, das je für Forscher in Europa aufgebaut wurde. Die nationalen Forschungsnetze sind zu fünfzig Prozent an der Finanzierung dieses Netzes beteiligt, weitere fünfzig Prozent steuert die EU-Kommission bei, die bis zum Jahr 2008 93 Millionen Euro in das Projekt investieren wird. Hand in Hand mit nationalen Forschungsnetzen wie dem X-WiN bietet der europäische Forschungsbackbone ausreichend Kapazitäten, um auch sehr große Datenmengen etwa von Radioteleskopen oder vom Large Hadron Collider des CERN europaweit zustellen zu können.

Längst sind es nicht mehr nur die klassischen Disziplinen wie die Teilchenphysik oder die Radioastronomie, die sich über GÉANT2 und die Forschungsnetze europaweit verlinken, um gemeinsam zu forschen, entfernte Rechner anzusteuern oder auf globale Informationsbestände zuzugreifen. Durch Roaming-Dienste, Autorisierungs- und Authentifizierungs-Infrastrukturen, durch Voice-over-IP und Videoconferencing stellen die Forschungsnetze heute auch für jene Wissenschaftler eine unverzichtbare Arbeitsgrundlage dar, die sich bislang nicht als Intensivnutzer der Forschungsnetze definierten.

Dr. Hans Döbbeling

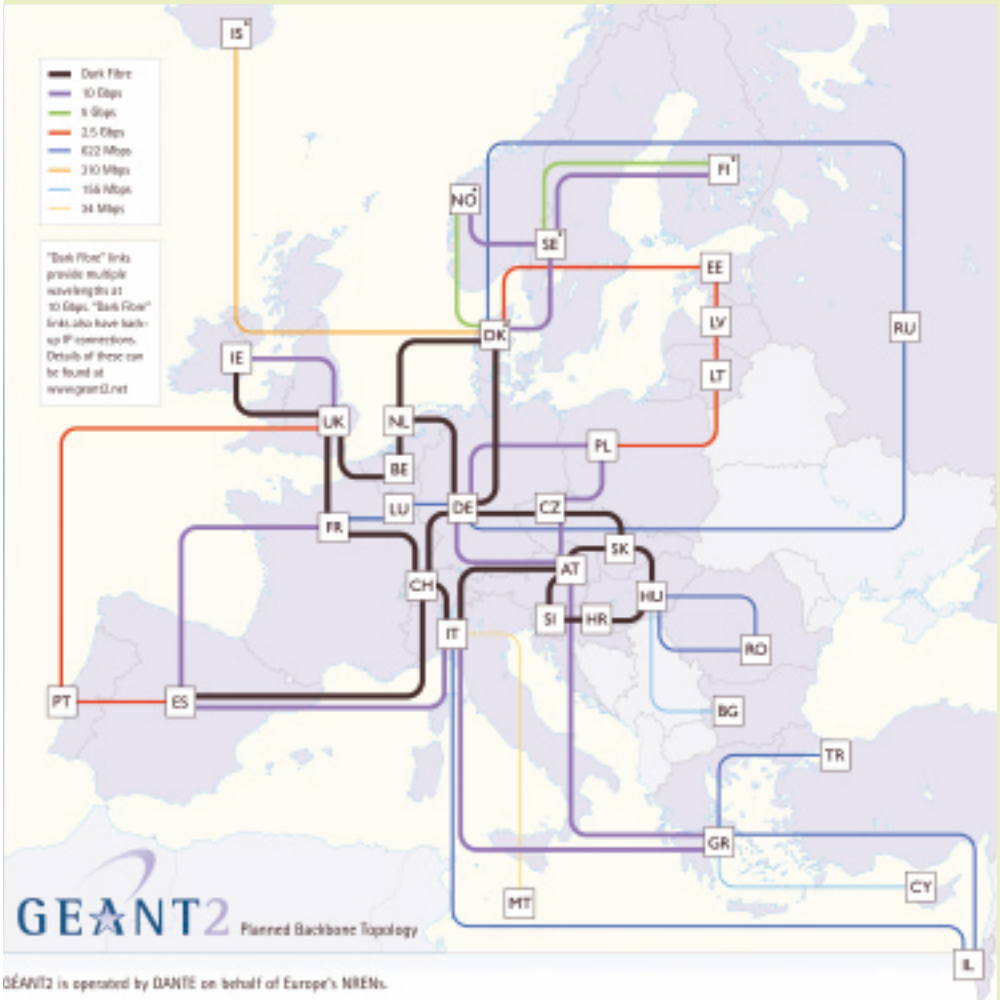
Geschäftsführer DANTE Ltd.

Enge Verbindungen zwischen DANTE und DFN

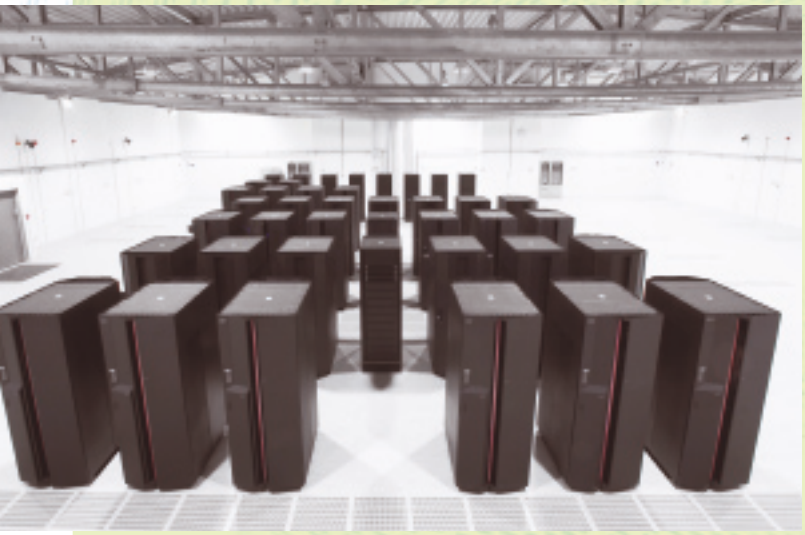
Als Shareholder von DANTE Ltd. ist der DFN-Verein seit je her eng mit dem paneuropäischen Forschungsnetz verbunden. Bereits während der ersten Generation des Wissenschaftsnetzes in Deutschland war der Blick der Netzwerker des DFN wie auch vieler Kollegen auf die Nachbarstaaten in Europa gerichtet. Dies führte 1993, also noch zu Zeiten des X.25-WiN, zur Gründung der in Cambridge ansässigen Firma DANTE Ltd. Der DFN-Verein hat bei dieser Gründung eine entscheidende Rolle gespielt und in Person seines Geschäftsführers Klaus Ullmann auch während eines Großteils der Unternehmensgeschichte den ‚Chairman of the Board' gestellt.

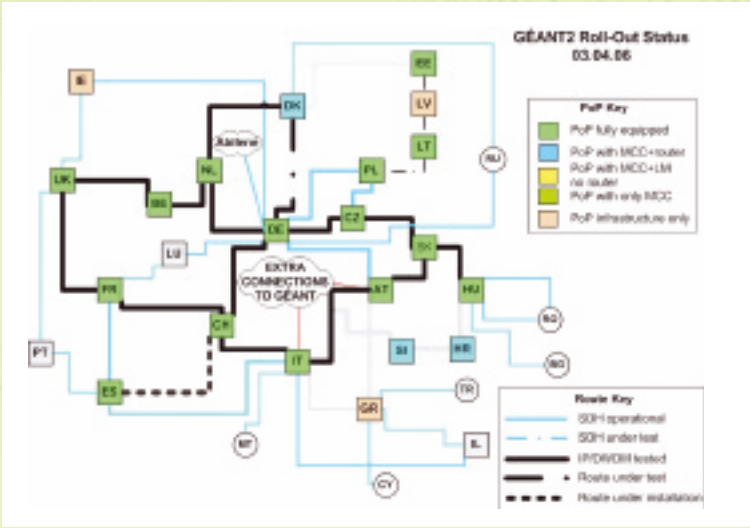
DANTEs Aufgabe ist die Bereitstellung der europaweiten Verbindungen zwischen nationalen Forschungsnetzen und der Aufbau von globalen Verbindungen zwischen Europa und anderen Weltregionen. DANTE leistet dies über eine Reihe von Projekten, welche von der Europäischen Kommission gefördert werden.

Knapp 50% der Kosten für den Betrieb des Netzes, die sich auf etwa 40 Millionen Euro pro Jahr belaufen, werden von der Kommission beigesteuert. Der Rest wird von den Konsortialmitgliedern, das sind die dreißig am Projekt beteiligten nationalen Forschungsnetze, über die Entgelte für die von DANTE bezogenen Dienste finanziert.



Parallel zu den Generationen des WiN und zu denen anderer vergleichbarer nationaler Netze existierten auf europäischem Niveau die Trans European Networks TEN und als deren Nachfolger die GÉANT-Netze. Als siebte Generation des europäischen Forschungs-Backbones wurde im Juni vergangenen Jahres in Luxemburg das GÉANT2 eingeweiht, dessen schrittweise Inbetriebnahme zügig voran geht: 90% der Verbindungen zwischen den europäischen NRENs (National Research and Education Networks) sind bereits im Betrieb. Die ersten Verbindungen konnten im Dezember 2005 zwischen der Schweiz,





Im DEISA-Projekt vernetzen sich Supercomputing-Zentren europaweit.

Italien und Deutschland in Betrieb genommen werden. Während das X-WiN gleichsam über Nacht das G-WiN abgelöst hat, erstreckt sich der Wechsel von GÉANT1 zu GÉANT2 über einige Monate, ist aber gleichermaßen für die Endbenutzer transparent.

Dark Fiber als Basis für hybride Netze

Ebenso wie beim X-WiN handelt es sich auch beim GÉANT2 um ein hybrides Netzwerk, das neben klassischen IP-Paketdiensten auch verbindungsorientierte Dienste anbietet. Dies wird realisiert, indem sich das NREN Konsortium, durch DANTE vertreten, die langfristigen Nutzungsrechte auf „Dark-Fiber" sichert und eine eigene Transmissionsplattform auf diesem Faserpaar unterhält, bzw. von einer dritten Partei unterhalten lässt. Ist die Anfangsinvestition in Verstärker, Dispersionskompensation und Multiplexoren einmal getan, wird der Ausbau des DWDM Systems um weitere Übertragungskanäle wirtschaftlich sehr günstig.

Motivation für diesen Schritt ist u.a. der kostengünstige und selbstorganisierte Zugang zu mehr Bandbreite. GÉANT2 und die europäischen Forschungsnetze wollen einzelnen wissenschaftlichen Disziplinen, europäischen Projekten, Grid-Initiativen oder verteilten Organisationen eigene private Netze bereitstellen. Das Schlagwort in diesem Zusammenhang lautet "OPNs", optische private Netze.

Beispiele für derartige OPNs sind das für die Analyse der CERN LHC Experimente benötigte Netz, die Verbindung europäischer Supercomputer im DEISA Projekt und die Zusammenführung radioastronomischer Daten zwecks Korrelation der Messungen.

Vorreiter der Entwicklung hin zu hybriden Infrastrukturen in Europa waren u.a. die Forschungsnetze der deutschen Nachbarn Schweiz, Holland und Polen. Die Marktsituation für Glasfaser-Leitungen ermöglichte hier am frühesten den Umstieg von angemieteter Bandbreite auf gekaufte bzw. langfristig angemietete Fasern. Neben DFN und GÉANT2 wechseln derzeit eine Reihe weiterer Netze zu diesem Betriebsmodus. So wird das britische SuperJanet5 ebenso über Dark Fiber verfügen wie Frankreichs Renater4, das skandinavische NordUNET, Tschechiens CESNET oder das serbisch-montenegrinische AMREJ.

Stand der Vernetzung

Der Netzplan zeigt, was GÉANT2 bislang erreicht hat. Die Hälfte der insgesamt 30 Projektteilnehmer werden unter Verwendung von Dark Fiber an das GÉANT2 angeschlossen. 18 Verbindungen von insgesamt 12.000 km Länge sind dabei eingerichtet. Bis auf drei Faserstrecken, welche Ljubljana und Zagreb mit Wien und Budapest verbinden sollen, ist die optische Plattform von GÉANT2 installiert und in Betrieb. Die anderen 15 Projektteilnehmer sind über gemietete Wellenlängen- oder SDH-Verbindungen in die GÉANT2-Infrastruktur eingebettet.

Einer der Gründe für den schrittweisen Umstieg auf die neue Netzgeneration liegt im sehr komplexen Ausschreibungs- und Beauftragungsverfahren. Die Ausschreibung und Anmietung der Fasern gestaltet sich auf europäischer Ebene ungleich schwieriger als auf nationaler Ebene. Ein in Europa fein aufgeteilter Markt für Glasfasern sorgt dafür, dass allein acht Lieferanten das Netz mit den nötigen Leitungen versorgen. Auf nationaler Ebene in Deutschland mussten für die Bereitstellung der im Kernnetz verwendeten Glasfasern lediglich drei Lieferanten beauftragt werden.

Im Bereich der Vermittlungstechnik wurde beim Aufbau des GÉANT2 das gleiche kostenbewusste Verfahren angewendet wie beim X-WiN: die Router aus dem Vorgängernetz wurden wieder verwendet. Da gegenüber dem GEANT1 eine Reihe von POPs verlegt werden mussten, war das Recycling jedoch mit einer Sequenz

von Router-Umzügen verbunden, bei der eine größere Menge der eingesetzten Juniper-Router von Hauptstadt zu Hauptstadt transportiert wurden. Wie bei Umstieg vom G-WiN zum X-WiN ist es dabei gelungen, den normalen IP-Betrieb weiterzuführen, ohne dass die Endnutzer in den europäischen Hochschulen etwas vom Umbau der Plattform bemerkt hätten.

Aktuell werden zusätzliche Verbindungen für das LCG Netz installiert. Leitungen dieser Art existieren bereits zwischen Genf und Frankfurt sowie zwischen Genf und Mailand. Entsprechende Arbeiten für den DEISA-Verbund sind in Vorbereitung.

Ausbau der Dienst-Plattform

Das GÉANT2 Projekt besteht nicht nur in der Beschaffung und Bereitstellung der Netzwerkplattform und der darauf aufbauenden Dienste. Eine wichtige Komponente stellt die internationale Kooperation bei der Entwicklung neuer Dienste dar. Dies geschieht in den sogenannten Joint Research Activities (JRAs). Der Ausbau der Dienstplattform ist neben dem technischen Paradigmen-Wechsel beim Umstieg auf eine hybride Plattform die zweite wesentliche Neuerung gegenüber der Vergangenheit. So werden über das GÉANT2 ein Roaming-Dienst, ein gemeinsames Security-Konzept und ein Netzwerk-Monitoring angeboten. Darüber hinaus existiert eine Testplattform für Bandwith on Demand.

Insbesondere im Bereich der Dienste zeigen sich deutlich die Synergien, die zwischen den nationalen Forschungsnetzen und GÉANT2 entstehen. DANTE kann in den JRAs auf die Erfahrung aus mehr als 30 teilnehmenden Nationen zurückgreifen. So spielt etwa das DFN beim Aufbau einer Monitoring-Umgebung unter dem Projetktitel perfSONAR eine wichtige Rolle. Hierbei handelt es sich um einen Netzwerk-Monitoring-Dienst, der Verbindungen über mehrere Verwaltungsdomänen und verschiedene Hardware-Plattformen hinweg erfasst. Dies wird mittels eines standardisierten Systems von Web-Services erreicht. Jede Netzdomäne muss die entsprechenden Dienste für ihre Verbindungen und ihre Hardware-Plattform beitragen. So entstehen übergreifende Informationen, welche als Basis von Netzwerkzustandskarten, als Dienstnachweis oder zur Fehlerbehebung weiterverarbeitet werden können.

Das Netzüberwachungs-System perfSONAR ist in europäischer Zusammenarbeit entstanden. Gleichzeitig ist es Ergebnis einer Kooperation mit der Internet2-Initiative und dem nordamerikanischen Energy Sciences Network (ESnet). Wie wichtig ein Monitoring-Tool für die multinationale Zusammenarbeit der Netze untereinander und mit GÉANT2 ist, zeigt sich, wenn man etwa die Einzelverbindungen eines Optischen Privaten Netzwerks betrachtet, welches zum Beispiel eine Verbindung zwischen dem GridKA in Karlsruhe und dem Rutherford Appleton Laboratory (RAL) bei Oxford realisieren soll. Sie besteht aus einer Komponente Karlsruhe (FZK) - Frankfurt/Main des X-WiN mit Technik des chinesischen Herstellers Huawei, einer Komponente des GÉANT2 auf der Strecke Frankfurt/Main - London mit Alcatel-Geräten und einer SuperJanet5-Komponente mit einer optischen Plattform des amerikanischen Herstellers Ciena.

Globale Vernetzung

Neben der europäischen Vermaschung investiert DANTE Ltd. auch erhebliche Mittel zur globalen Vernetzung. Aus den von GÉANT1 übernommenen drei 2.5 GB/s Verbindungen nach Nordamerika werden zwei, später sogar drei 10GB/s Verbindungen, wobei das nordamerikanische Internet2 seinerseits vergleichbare transatlantische Kapazitäten bereitstellt. Am anderen Ende der Skala steht eine in Zusammenarbeit mit dem Indischen Forschungsnetz ERNET erarbeitete und von der Europäischen Kommission geförderte 45 MB/s Verbindung nach Indien - eine Verbindung, die pro Jahr mehr kostet, als eine der oben genannten transatlantischen Strecken.

Flankiert wird die Entwicklung der globalen Verbindungen des GÉANT2 durch eine Reihe von der EU bezuschusster Vernetzungs-projekte, bei denen DANTE ebenfalls der koordinierende Partner ist. Mit ALICE, EuMedConnect, TEIN2, und ORIENT werden Verbindungen nach Lateinamerika, Nordafrika, Südostasien und China aufgebaut. Im Rahmen von ALICE und EuMedConnect werden darüber hinaus in Südamerika und rund ums Mittelmeer völlig neue Infrastrukturen für die Vernetzung der teilnehmenden Staaten untereinander geschaffen. Hierüber wurde die in den letzten Ausgaben der DFN-Mitteilungen verschiedentlich berichtet. Gemeinsame Absicht von Europäischer Kommission und Projektteilnehmern ist die Förderung der Entwicklung von regionalen Netzverbünden, die sich zu Partnern für das Europäische Wissenschaftsnetz entwickeln sollen.

Ausblick

Parallel zur Overlay-Struktur eines GÉANT2 bieten die optischen Systeme auf nationaler Ebene die Möglichkeit, NRENs wie zum Beispiel das X-WiN und das polnische PIONIER direkt zu verbinden und unmittelbar aneinander anzuschließen. Insbesondere Deutschland hat aufgrund seiner geographischen Lage eine interessante Rolle in Bezug auf derartige sogenannte Cross-Border-Leitungen.

Auch wenn nationale Netzwerke und das pan-europäische GÉANT2 Unterschiede aufweisen - erstere sind auf die Anbindung möglichst vieler Einrichtungen optimiert, letzteres hingegen auf das Überwinden großer Strecken - können die nationalen Forschungsnetze künftig zunehmend Kapazitäten für den transeuropäischen Datenverkehr bereitstellen und eröffnen damit gänzlich neue Dimensionen für die Vernetzung der Wissenschaftler Europas. Vor diesem Hintergrund wird deutlich, dass das hier skizzierte Hand-in-Hand-Gehen nationaler und transnationaler Netze nur als Prolog für die künftige globale Vernetzung der Wissenschaften angesehen werden kann.

CESNET – NREN of the Czech Republic

Dr. Jan Gruntorád, CSc.

Member of the Board of Directors and the CEO of CESNET,
Member of the Board of Directors DANTE

CESNET 10-year history

The *CESNET* association is currently financed mainly from the resources of the governmental Committee for Research and Education and the resources of the members of the association. The association performs research and development in the area of information and communication technologies, and builds and maintains the national multigigabit optical network, *CESNET2,* designed for research and educational purposes.

Looking into the history, it is hardly imaginable that before the "velvet revolution" of 1989 there were no computer networks in former Czechoslovakia. However, shortly after an explosive development was initiated focused mainly on the academic sphere, fueled also by international help. With the help of a US foundation, a node of *EARN (European Academic and Research Network,* the European branch of the *BITNET)* was set up in the Computing Center of the Czech Technical University in Prague in 1990. Based on the international 19.2 kbps link to Austria, the Internet officially entered Czechoslovakia in 1992.

A year later, after the split of the country, the originally shared academic network was split into the Slovak SANET *(Slovak Academic NETwork)* and Czech CESNET *(Czech Education and Scientific NETwork).* Due to the gradual commercialization of CESNET network activities, in 1994, the Ministry for Youth, Education and Sports appointed the Board of CESNET to decide on its future. The solution was to create a standalone entity that would ensure the operation and development of the network.

On 6 March 1996, *CESNET* was established as an Association of Legal Entities that represented all Universities and Academy branches in the country. The association supported the distributed network environment that quickly evolved and also was one of the founding members of the CZ.NIC association, maintaining the national domain .cz, as well as the NIX.CZ association, which is responsible for the operation of neutral exchange point interconnecting domestic Internet providers.

The networking research was supported by *CESNET* from the very beginning, therefore the Czech Republic was the only country from the former communist bloc that became a participant of the European research project *TEN-34* in 1996. The *CESNET* association participated also in the follow-up TEN-155 project which meant a significant improvement in the backbone network capacity, based on ATM (Asynchronous Transfer Mode).

The fast development of the optical *CESNET* network lead to the first 2.5 Gbps backbone line using the PoS *(Packet-over-SONET)* technology that was put into operation already in 2000, when transfer lines of such capacity, dedicated entirely to IP traffic, were rare even in the most developed countries.

However, at that time it became clear that it would not be possible to implement a gigabit network based on leased transfer services with the available budget. The association therefore looked for a more economical method of achieving its goals: the solution was the rental of dark fibers. This approach, referred to as the CEF *(Customer-Empowered Fiber)* networks, is nowadays widely used but at the beginning on the 21st century CESNET was one of its pioneers in the worldwide scope.

In 2001, a trans-European network called *GÉANT,* successor of the TEN-155, was launched, and the Czech Republic became a part of the core with three 2.5/10 Gbps international connections. Related to this development, a renamed *CESNET2* network was officially launched. Its backbone lines brought 2.5 Gbps to nine of the most important university cities. In the comparative study of European scientific and research networks carried by the TERENA association, CESNET2 was evaluated as the third largest network in Europe at that time.

Towards a modern multigigabit network

The WDM *(Wavelength Division Multiplexing)* technology allowed transferring several independent signals in a single fiber therefore the evolution of the network continued: the new generic network structure was designed in 2002 based on the backbone formed by DWDM *(Dense WDM)* rings. The CEF principle imposed limitations on optical line transfer range therefore CESNET developed methods called NIL *(Nothing In-Line)* that are based mainly on utilization of various types of amplifiers and their combinations. The original NIL modular amplifier, tested in CESNET2 up to the distances exceeding 300 km, is called PC Light and is considerably cheaper than commercial amplifiers.

The first DWDM line (Prague – Brno) was deployed in 2004, providing several independent lines with transfer speeds of 10 and 1 Gbps. During 2005, the line was upgraded to the Prague – Brno – Olomouc –Hradec Králové – Prague 10Gbps DWDM ring based on 32-channel ROADM *(Reconfigurable Add-Drop Multiplexer)* technology.

One of top NRENs worldwide

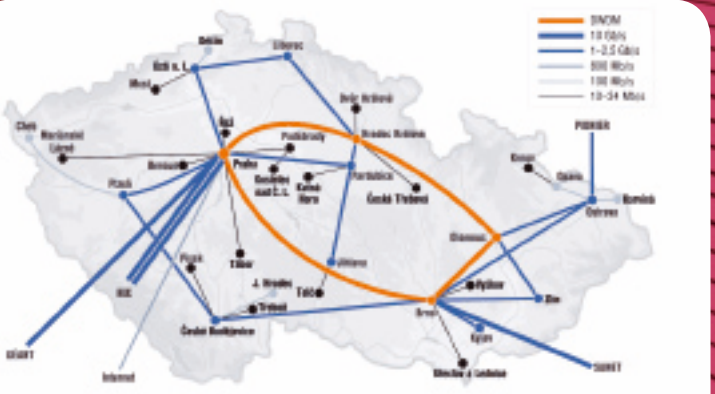
CESNET2 is technologically comparable to other NRENs in developed countries. External connectivity capacity has increased 100fold from 300 Mbps in 2001 to 35.3 Gbps in 2005. Contrary to other new EU member states' NRENs, *CESNET2* is not only a sink of external data, instead it exports 1.7 times more data than enters the network. According the latest *TERENA kompendium 2005* the number of universities and research institutes with at least 1 Gbps is in the new EU member states higher than in the former EU-15; the Czech TU is connected to *CESNET2* by 10 Gbps.

CESNET association acts as a representative of the Czech Republic in the *GN2* project and *CESNET2* is connected to GEANT2 by 10 Gbps optical line. The association has participated in numerous other EU research projects, such as DataGrid, EGEE, 6NET, SCAMPI, LOBSTER, and SEEFIRE. The international cooperation does not end here: the association has been an international partner of *Internet2* since 1999.

CESNET association is also a founding member of GLIF *(Global Lambda Integrated Facility)* in which lightpaths (based on individual wavelengths) may be provided end-to-end on demand. Parallel to *CESNET2*, the association started to develop a purely experimental optical *CzechLight* network, connected to the international GLIF infrastructure. This network is designed for experimenting with optical transfer technologies and on-demand circuit provision. The network is utilized within selected applications with extreme bandwidth demands.

Conclusion

The strategic goal of CESNET is to maintain its position as a technical innovator in the area of computer networks, both in the Czech and worldwide perspective. This is the only way of giving the CESNET the ability to efficiently develop the national research and education network, offering the local academic community top-class services to implement projects that are demanding in terms of communication services and to maintain full cooperation with international partners.



CESNET association and CESNET2 network

CESNET (Czech Education and Scientific NETwork) is an association of all universities of the Czech Republic and the Czech Academy of Science. Its main goals are operate and develop a high-speed national research and education network, CESNET2, participate in analogous projects at European and global levels, carry out original research in the area of networking technologies and their applications and actively seek, adapt and develop corresponding applications.

CESNET2 network is the backbone network connecting scientific, research and higher-education facilities in the Czech Republic. Main features of CESNET2 are gigabit backbone (POS and Ethernet) including DWDM ring Praha – Brno – Olomouc – Hradec Králové – Praha, redundant topology with low hop numbers for main nodes, high-speed connection to GÉANT2 European research backbone and to commodity Internet, deployment of advanced optical technology (nothing-in-line, single fibre) and advanced IP services (MPLS, multicast, IP version 6).

CESNET celebrates 10th anniversary

On the occasion of the tenth anniversary of its establishment, CESNET organized the first international conference 6 - 8 March in Prague. Over 100 leading professionals from the Internet research area from 15 European countries and the United States have gathered at this event. The conference was officially inaugurated by the Minister of Youth, Education and Sport of the Czech Republic who appreciated the long-term stable contribution of the association to the research, development and education at both the national and international levels.

Keynote speech was given by Klaus Ullmann, Chairman of the Board of Directors of the DANTE association, coordinating GN2 project (co-funded by the EU) responsible for creating the modern pan-European network GÉANT2 to interconnect national research and education networks; and director of the German national research network, DFN (Das Deutsche Forschungsnetz). The importance of cooperation and a systematic approach within science and research support via a top-notch communication and information environment in a pan-European context was stressed. Next, the CEO of the CESNET association, Jan Gruntorád, evaluated the ten-year history of the association in the view of future prospects and research tasks.

Lectures at the two-day conference covered a very wide range of issues – from optical signal transmissions and amplification, application of programmable hardware within high-speed data transmission, to highly-specialized distributed network applications, and middleware. Among the applications of cutting-edge computer networks the grids were the main topic of discussion.

CESNET Conferences 2006 also witnessed the first high-definition video (HDV) conference in the Czech Republic, and one the first public HDV demonstrations in Europe. The lecture hall of the Charles University, equipped with a borrowed prototype of an HD projector featuring a full resolution of 1920 x 1080, was connected via academic high-speed networks with the Research Channel site in Seattle (USA, Washington State). The 30-minute lecture was transmitted between the two points in a compressed 25 Mbps data flow.
Details on the conference, including presentations of individual lecturers in various formats of choice, including video in both standard and high-definition qualities, are available at www.ces.net/conference06/.

Hochgeschwindigkeitsnetz zwischen EU und China

Ein neues chinesisch-europäisches Hochgeschwindigkeitsnetz wird die Kommunikation und die Zusammenarbeit zwischen 45 Millionen Forschern und Studierenden in Europa und China erheblich erleichtern. Das ORIENT-Projekt (Oriental Research Infrastructure to European NeTworks), das von der Europäischen Union, China und den nationalen Forschungs- und Bildungsnetzen in Europa mitfinanziert wird, soll in Zukunft allen Forschungsgebieten (einschließlich Radioastronomie, nachhaltiger Entwicklung, Meteorologie und Datenverarbeitung in Gitterverbundnetzen) in Europa und China zu Gute kommen, indem es den Informationsfluss zwischen Europa und China steigert.

In einer Landverbindung über Sibirien wird ORIENT Europas GÉANT2 mit den chinesischen Forschungsnetzen CERNET und CSTNET zusammenführen. Noch in diesem Jahr werden auf diese Weise 200 chinesische Universitäten und Forschungsinstitute mittels einer Übertragungsgeschwindigkeit von bis zu 2,5 Gbit/s mit GÈANT2 und somit mit allen Wissenschaftseinrichtungen in Europa verbunden. Die Koordinierung übernehmen in Europa die Forschungsnetzorganisation DANTE und in China das Netzwerk CERNET.

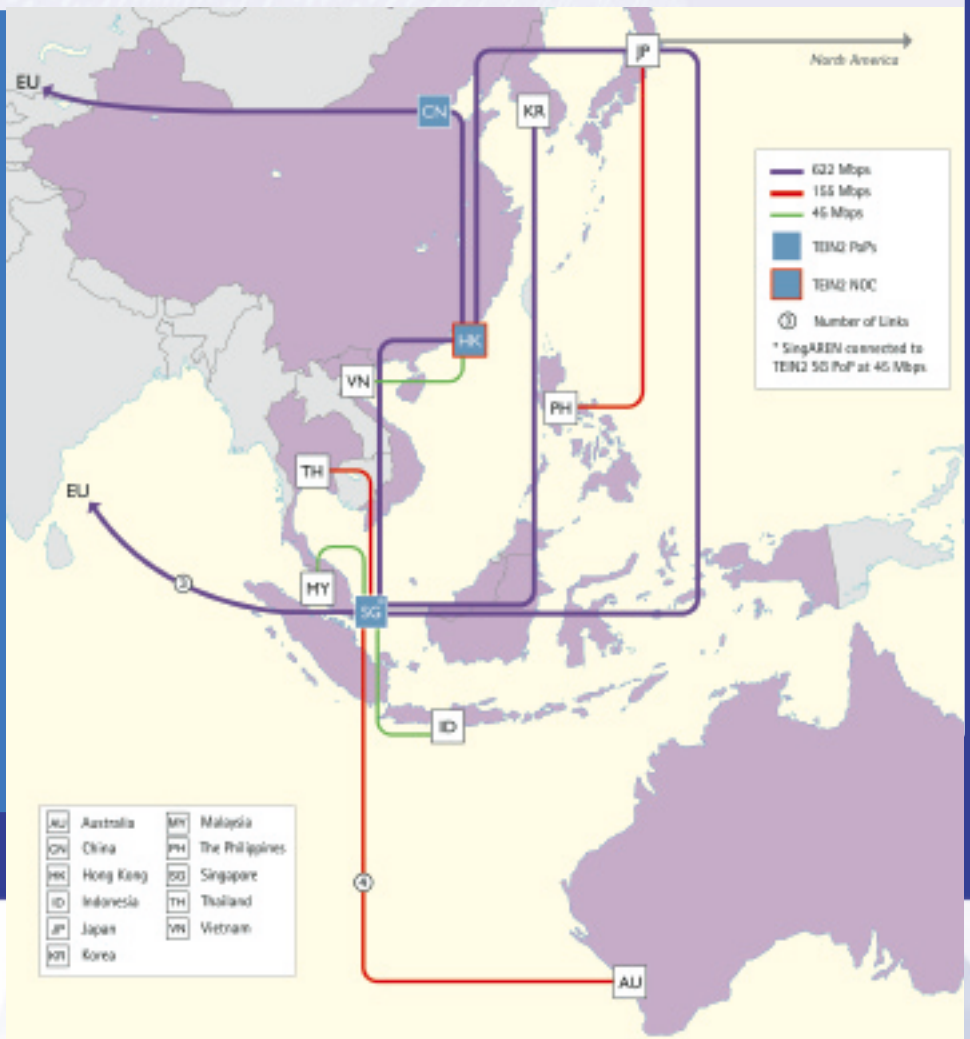
Das Projekt lief am 1. März 2006 an. Die Laufzeit beträgt drei Jahre. Die Finanzierung der Netzverbindung erfolgt aus drei Quellen: 50 % der Projektkosten werden von CERNET übernommen, 25 % von den nationalen Forschungs- und Bildungsnetzen in Europa und die restlichen 25 % von der Europäischen Kommission.

Bereits bestehende chinesisch-europäische Forschungsprojekte sehen der ORIENT-Verbindung erwartungsvoll entgegen. Zwei Beispiele hierfür sind das EUChinaGrid, welches europäische Grid-Infrastrukturen nach China ausdehnen und somit die Außenanbindung des Europäischen Forschungsraums unterstützen wird, oder das Radioastronomieprojekt EXPReS, mit dem europäische und chinesische Radioteleskope miteinander verbunden werden.

ORIENT ergänzt TEIN2, die seit Dezember 2005 aktive Verbindung in den asiatisch-pazifischen Forschungsraum. Mit 622 Mbit/s verbindet TEIN2 zehn Länder, darunter auch China, und fördert so die regionale Zusammenarbeit. Jedes Netz profitiert von dem Verbund, weil die Kapazität der Aussenanbindung erhöht wird und bei Ausfall auch Ersatzverbindungen bereitstehen. *(k.h.)*

CERNET

CERNET stellt Internetdienste für chinesische Universitäten, Institute, Schulen und andere gemeinnützigen Organisationen bereit und bedient somit 200 Standorte in 31 Provinzen auf dem chinesischen Festland. Des weiteren verfügt CERNET über verschiedene globale Verbindungen nach Nordamerika, Asien und in den Pazifikraum und umfasst somit ca. 1 300 Universitäten und Institutionen und ca. 15 Mio. Endnutzer. CERNET bietet eine nationale Netzplattform, auf der zahlreiche große nationale Netztechnologieprojekte durchgeführt werden, und unterstützt zudem viele Anwendungen, darunter Online-Bewerbungen für über 1 500 Universitäten, Fernunterricht, digitale Bibliotheken, Gitterverbundnetze, Videokonferenzen und Voice-over-IP-Lösungen.



Verbindungen zwischen den Forschungsnetzen im asiatisch-pazifischen Raum im Rahmen des Projektes TEIN2

Prüfungsanmeldung per Internet – wie geht denn das?

Michail Bachmann
Humboldt-Universität zu Berlin
michail.bachmann@cms.hu-berlin.de

Franziska Löser
Humboldt-Universität zu Berlin
franziska.loeser@cms.hu-berlin.de

Mit der Einführung der modularisierten Studiengänge hat sich die Arbeitsbelastung der Prüfungsbüros vervielfacht. Dass dieser Mehraufwand bei stagnierendem oder gar sinkendem Personalstand nicht bewältigt werden kann, ist offensichtlich. Um die Mitarbeiter des Prüfungsamtes von solchen Routineaufgaben zu entlasten und ihnen die Zeit zu geben, sich auf notwendige Arbeiten zu konzentrieren, musste ein Ausweg geschaffen werden. Der folgende Artikel soll einen kurzen Überblick über das dafür eingesetzte System geben.

Vorgeschichte

Die Verwaltung und Organisation der Prüfungen erfolgen an der Humboldt-Universität dezentral. Jede Fakultät entwickelte so für sich Lösungen, die auf ihre Bedürfnisse zugeschnitten waren. Spätestens mit der Einführung der modularisierten Studiengänge vervielfachte sich aber die Arbeitsbelastung der Prüfungsämter. Die erhöhten Anforderungen konnten oftmals von der bisherigen Software nicht mehr erfüllt werden. Ein Ersatz wurde notwendig.

Die Studierendenverwaltung war bereits zentral organisiert. Zu diesem Zweck wird eine Software der Firma HIS GmbH[1] – das SOS-System[2] – verwendet. Außerdem gehört zum Portfolio der HIS GmbH auch Software zur Prüfungsverwaltung, genannt HISPOS. Ende 2003 wurde beschlossen, dieses POS-System[3] universitätsweit – zuerst für Studiengänge mit Lehramtsoption, danach für alle anderen – einzuführen.

Da an einigen deutschen Hochschulen die Studierenden bereits erfolgreich Selbstbedienungsfunktionen nutzen und damit eine deutliche Verbesserung der Servicequalität erreicht werden konnte, wurde beschlossen, auch an der Humboldt-Universität ein Selbstbedienungssystem für Studierende einzuführen – das QIS-System[4].

Dafür wurde Anfang 2005 eine Projektgruppe gegründet, die die Fakultäten bei der Einführung von QIS unterstützen soll. Nachdem ein im Juni 2005 an zwei Fakultäten durchgeführtes Pilotprojekt zufriedenstellende Resultate erbrachte, wurde beschlossen, QIS – so weit schon möglich und gewünscht – universitätsweit einzuführen und diese Funktionalität weiteren Fakultäten zur Verfügung zu stellen. Ab Januar 2006 können sich ca. 4000 Studierende von fünf Fakultäten mit Hilfe von QIS zu ihren Prüfungen des Semesters 2005/2006 anmelden.

Systemaufbau

Um ausgewählte Funktionen der eingesetzten Verwaltungssoftware auch über das Internet nutzen zu können, wird eine von der HIS GmbH entwickelte Lösung verwendet.

Sie ist in der Programmiersprache Java geschrieben und als Servlet implementiert. Als direkte Ausführungsumgebung wird fast ausschließlich von der Apache Software Foundation geschriebene Open-Source-Software eingesetzt: der Webserver httpd[5], der Servletcontainer Tomcat[6], das Vorlagensystem (template engine) Velocity[7] und der für die PDF-Erzeugung zuständige FOP[8].

Der Aufbau des Systems folgt der klassischen Dreiteilung in Frontend, Applikation und Datenbank. Als Frontend dienen zwei Apache-Webserver. Mit Hilfe von keepalived[9] wird sichergestellt, dass bei Ausfall eines Servers der andere dessen Aufgaben automatisch übernimmt. Neben der Bereitstellung von statischen Inhalten (Grafiken, CSS, HTML-Seiten) erledigen die Webserver noch einige andere Aufgaben: Die Verschlüsselung der Verbindung zum Nutzer mit Hilfe des Apache-Moduls mod_ssl[10] gewährleistet die Vertraulichkeit der Dateneingabe. Das Apache-Modul mod_jk[11] baut die Verbindung zu den dahinter liegenden Tomcat-Applikationsservern auf, wobei es gleichzeitig für eine gleichmäßige Verteilung der Last auf die einzelnen Applikationsserver sorgt und Ausfälle für den Nutzer transparent abfängt. Die Authentifizierung der Nutzer erfolgt über den CMS-Account gegen einen LDAP-Server (zentrales Accountverzeichnis). Eine Prüfungsanmeldung wird an einen POS-Server übergeben, der die Eingaben auf Plausibilität prüft und letztendlich die Anmeldung zur Prüfung in die Datenbank schreibt. Jedes Schreiben in die Datenbank muss durch die Eingabe einer TAN (Transaktionsnummer) vom Nutzer autorisiert werden.

Der logische Aufbau des Systems – wobei insbesondere der Sicherheitsaspekt eine Rolle spielt – wird in Abbildung 1 dargestellt: Den Kern des Systems bildet der Datenbankserver, der alle Studierenden- und Prüfungsdaten enthält. Der Zugriff auf diese Datenbank erfolgt über Anwendungen der HIS GmbH, die teilweise auf PCs der Verwaltung, zum größten Teil jedoch auf Terminalservern laufen. Alle diese Systeme befinden sich im besonders geschützten inneren Verwaltungsnetzwerk.

Da das innere Verwaltungsnetz durch die Einführung von QIS einerseits natürlich nicht plötzlich der ganzen Welt offen stehen soll, andererseits jedoch für das Funktionieren der Prüfungsanmeldungen ein direkter Zugriff auf die Datenbank erforderlich ist, wird das HU-QIS-System in eine so genannte Demilitarisierte Zone (DMZ) ausgelagert. Diese DMZ ist ein spezieller Teil des Netzwerks, die – durch den äußeren und inneren Paketfilter (Firewall) kontrolliert – einen sicheren Zugriff auf die QIS-Server und das innere Verwaltungsnetz ermöglicht.

Außerhalb des äußeren Paketfilters befindet sich das Universitätsnetz, in dem sich z. B. der zentrale Accountserver und die diversen PC-Pools der Universität befinden.

Das Universitätsnetz ist über das HU-Gate an das Internet angeschlossen. Eine Anmeldung zu einer Prüfung, z. B. von zu Hause oder aus einem Internetcafe ist damit problemlos möglich.

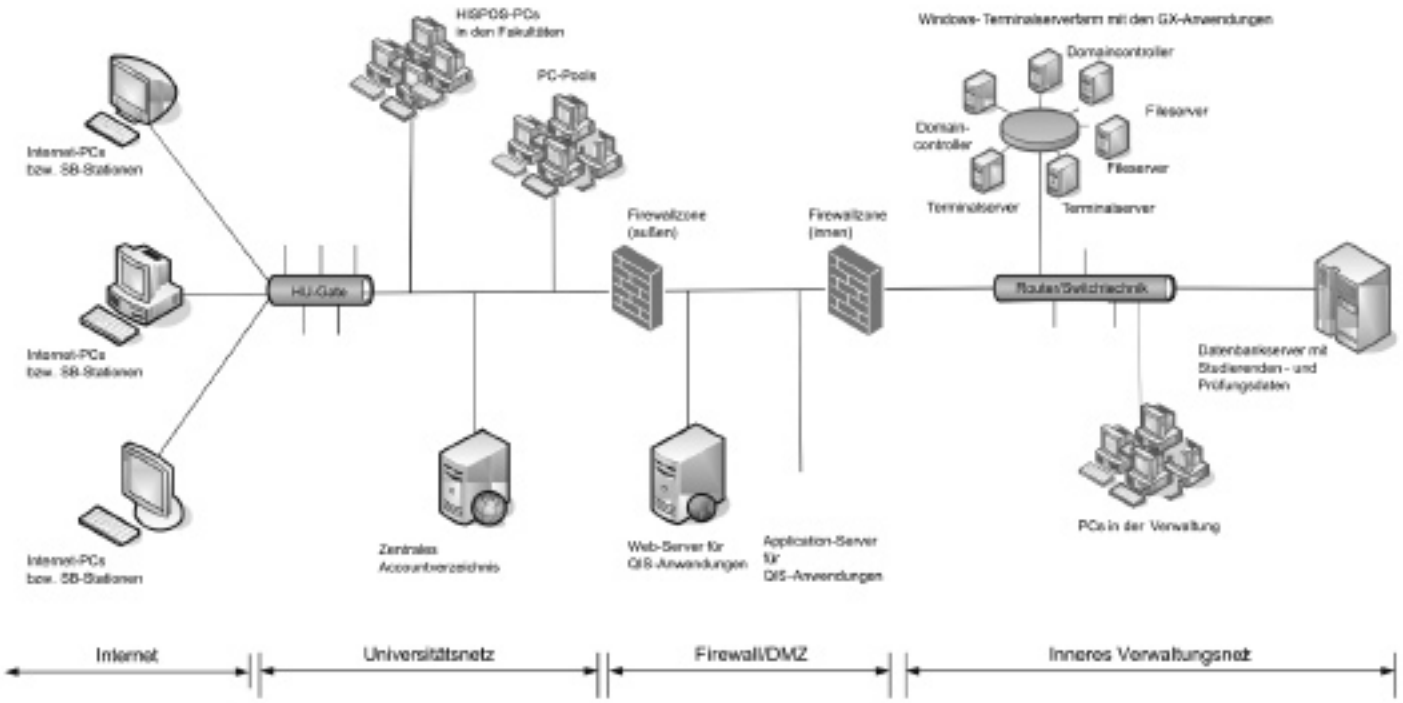


ABBILDUNG 1 (Systemaufbau)

Funktionsweise

Um das HU-QIS-System nutzen zu können, müssen – neben dem Studium an der Humboldt-Universität – noch einige Voraussetzungen erfüllt sein.

Da die Prüfungsanmeldung über das Internet angeboten wird, benötigt man selbstverständlich einen Zugriff auf einen an das Internet angeschlossenen PC. Das können der eigene Rechner zu Hause, ein Laptop im HU-WLAN, ein PC in einem der PC-Pools oder auch ein Rechner in einem Internetcafe am anderen Ende der Welt sein.

Da so ein Zugriff auf die Studierendendaten theoretisch von überall auf der Welt erfolgen kann, muss dieser Zugriff natürlich besonders abgesichert sein. Diese Absicherung erfolgt auf mehreren Ebenen: Auf der untersten Ebene ist die Verbindung zwischen dem Computer des Nutzers und den HU-QIS-Servern verschlüsselt, ein Abhören der Zugangsdaten also nicht so leicht möglich. Um sich am HU-QIS-System anzumelden, wird der Account beim Computer- und Medienservice (CMS) der Humboldt-Universität verwendet. Dieser Ansatz hat mehrere Vorteile: Es wird ein bereits existierender Account verwendet, die Studierenden werden also nicht mit einem weiteren Login und Passwort belastet. Gleichzeitig wird sichergestellt, dass das Passwort sicher genug ist. Es hat sich leider in der Vergangenheit immer wieder gezeigt, dass oftmals zu einfache Passworte benutzt wurden, womit natürlich die Sicherheit nicht mehr gewährleistet werden kann.

Ein weiterer Vorteil: Die wichtigsten Funktionen die den Account betreffen (z. B. das Zurücksetzen vergessener Passworte) stehen den Studierenden über ein Web-Interface rund um die Uhr von überall her zur Verfügung.

ABBILDUNG 2 (Prüfungsanmeldung)

Um die Zugriffssicherheit weiter zu erhöhen, wird das vom Online-Banking bekannte TAN-Verfahren verwendet. Dabei bekommt der Studierende vorher eine Liste mit zufällig erzeugten Zahlen zugeschickt. Bei jeder An- bzw. Abmeldung einer Prüfung muss eine TAN als Bestätigung eingegeben werden, dass die Anfrage wirklich von der dazu berechtigten Person stammt. Diese TAN ist danach verbraucht und kann nicht mehr verwendet werden. Durch den Einsatz der kombinierten Passwort-TAN-Authentifizierung wird eine hohe Sicherheit gegen unbefugte Datenveränderung erreicht.

Aussehen

Nach diesen doch eher theoretischen Betrachtungen soll an dieser Stelle ein Eindruck vermittelt werden wie eine Prüfungsanmeldung aus Studierendensicht abläuft:

Startseite

Nach Eingabe der Adresse http://qis.hu-berlin.de/ gelangt man auf die Startseite des HU-QIS-Systems. Hier kann man sich über das Login-Formular am System anmelden. Außerdem werden auf dieser Seite aktuelle Informationen veröffentlicht.

Nach erfolgreicher Anmeldung erhält man den Zugriff auf das eigentliche HU-QIS-System. Die Funktionen lassen sich in zwei Bereiche aufteilen: zum Einen die eigentliche Prüfungsanmeldung und zum Anderen verschiedene Übersichten zum Verlauf des Studiums.

Prüfungsanmeldung

Folgt man dem ersten Link »Prüfungsanmeldung«, so gelangt man auf eine Seite, die rechtliche Informationen zum Verlauf der Anmeldung enthält. Nachdem man die Kenntnisnahme durch die Eingabe einer TAN quittiert hat, gelangt man zum Kernstück der Prüfungsanmeldung – dem Prüfungsbaum. Dieser Prüfungsbaum stellt eine grafische Darstellung der Prüfungsordnung, nach der das jeweilige Studium absolviert werden soll, dar. Je nach Prüfungsordnung ist das ein mehr oder weniger komplexes System von einzelnen Prüfungen, Modulen und Konten. Einzelne Prüfungen können zu Modulen zusammengefasst werden, diese wiederum werden einzelnen Konten zugeordnet, bis am Ende der angestrebte Abschluss winkt.

Im Prüfungsbaum ist nicht nur erkennbar, ob man sich zu einer Prüfung anmelden kann, bereits angemeldet oder wieder zurückgetreten ist, sondern es ist auch auf einen Blick erkennbar, ob bereits absolvierte Prüfungen bestanden, nicht bestanden oder endgültig nicht bestanden sind.

Um sich zu einer Prüfung anmelden zu können, muss man durch den Prüfungsbaum navigieren, indem man die Überschriften anklickt. Nachdem man auf diese Weise bis zur gewünschten Prüfung vorgedrungen ist, folgt man nun dem Link zum favorisierten Prüfungstermin. Daraufhin wird man mit der Frage konfrontiert, ob man sich denn wirklich zu dieser Prüfung anmelden möchte. Nachdem man seine Absichten durch die Eingabe einer TAN und einen Klick auf »Anmelden« bestätigt hat, versucht das System, die Prüfungsanmeldung durchzuführen. Sollten nun alle Voraussetzungen für die Anmeldung zu dieser Prüfung erfüllt sein, gibt das System eine Bestätigung zurück und man erhält außerdem eine Übersicht, zu welchen Prüfungen man sich bei dieser Sitzung angemeldet hat. Andernfalls wird eine Warnung ausgegeben, aus der ersichtlich ist, warum die Anmeldung fehlgeschlagen ist. Das könnte z.B. an noch nicht erbrachten Leistungen liegen oder schlicht daran, dass die Frist zur Anmeldung bereits abgelaufen ist. Inhaltliche Unstimmigkeiten sind jedoch nur mit dem zuständigen Prüfungsamt zu klären. Man sollte daher trotz Online-Anmeldung nicht bis zum letzten Tag mit der Anmeldung warten.

Selbstverständlich kann man sich auf demselben Weg auch wieder von einer Prüfung abmelden.

ABBILDUNG 3 (Prüfungsbaum)

ABBILDUNG 4 (Angemeldete Prüfungen (HTML))

ABBILDUNG 5 (Angemeldete Prüfungen (PDF))

Übersichten

Neben der Möglichkeit, sich zu Prüfungen an- und abzumelden, wird für die Studierenden eine Reihe von Übersichten zur Verfügung gestellt.

Derzeit können folgende Übersichten abgerufen werden: »Angemeldete Prüfungen« und »Leistungsspiegel«.

Mit der Übersicht »Angemeldete Prüfungen« bekommen Studierende alle Prüfungen, zu denen sie angemeldet sind, auf einen Blick angezeigt.

Bei der Übersicht »Leistungsspiegel« können sich die Studierenden einen Überblick über die bisher erbrachten Leistungen verschaffen. Es werden alle bereits absolvierten Prüfungen inklusive Bewertung aufgelistet.

Diese angeführten Übersichten sind für die Darstellung im WWW optimiert. Da jedoch oftmals eine ansprechendere Darstellung gewünscht wird, besteht die Möglichkeit aus diesen Übersichten auch PDF-Dateien zu erzeugen, die zum Ausdrucken besser geeignet sind.

An dieser Stelle sei jedoch gleich darauf hingewiesen, dass diese Ausdrucke keinen offiziellen Charakter haben, sondern nur der persönlichen Information dienen. Es wäre zwar vorstellbar, weitere Bescheinigungen – auch offiziellen Charakters – mit Hilfe des HU-QIS-Systems zu erzeugen. Die Gültigkeit solcher selbst ausgedruckten Bescheinigungen ist jedoch naturgemäß nur schwer zu belegen. Es gibt für dieses Problem allerdings Lösungsansätze seitens der HIS GmbH, die jedoch bisher erst experimentell sind.

Abschluss und Ausblick

Durch den Einsatz von Online-Prüfungsanmeldungen wird eine spürbare Entlastung der einzelnen Prüfungsbüros von Routineaufgaben und – daraus folgend – eine gleichzeitige Erhöhung der Servicequalität für die Studierenden erwartet. Eine Reduzierung der Wege- und Wartezeiten ermöglicht ein Studium, das weniger von verwaltungstechnischem Aufwand geprägt ist.

Für die Zukunft ist geplant, weitere Selbstbedienungsfunktionen – nicht nur im Prüfungsbereich – online bereitzustellen. Abiturienten sollen die Gelegenheit erhalten, ihre Bewerbungen für ein Studium an der Humboldt-Universität online abzugeben. Studierende sollen u. a. Adressänderungen online durchführen, Veranstaltungen belegen oder individuelle Stundenpläne erstellen können.

Anmerkungen

1 http://www.his.de/
2 Studierendenorganisationssoftware
3 Prüfungsorganisationssoftware
4 Qualitätssteigerung der Hochschulverwaltung im Internet durch Sebstbedienung
5 http://httpd.apache.org/
6 http://tomcat.apache.org/
7 http://jakarta.apache.org/velocity/
8 http://xmlgraphics.apache.org/fop/
9 http://www.keepalived.org/
10 http://www.modssl.org/
11 http://jakarta.apache.org/

Urheberrecht in der Informationsgesellschaft – eine Zwischenbilanz

Ass. jur. Jan K. Köcher

Forschungsstelle Recht im DFN
recht@dfn.de

http://www.dfn.de/recht

Mit dem Einzug moderner digitaler Kommunikationstechnologie in den Alltag der Menschen, wurde das Urheberrecht vor neue Herausforderungen gestellt. Das Urheberrecht dient dem Schutz der schöpferischen Leistung der Kreativen. Voraussetzung für den Schutz ist, dass sich die schöpferische Leistung in irgendeiner Weise Ausdruck verschafft hat und eine bestimmte Gestaltungshöhe erreicht, an die jedoch keine allzu großen Anforderungen gestellt werden. Die bloße Idee unterliegt hingegen grundsätzlich keinem Schutz. Der Schutz des Urhebers eines Werks umfasst neben der wirtschaftlichen Verwertung seines Arbeitsergebnisses, seine persönliche Beziehung zum Werk. Diese Beziehung wird beispielsweise durch eine ungefragte Entstellung gestört, gegen die der Urheber rechtlich vorgehen kann. Die Brisanz im Zusammenhang mit der aktuellen Diskussion um das Urheberrecht, liegt jedoch in dem Schutz der wirtschaftlichen Verwertung des schöpferischen Ergebnisses. Relevante Verwertungshandlungen wie etwa die Vervielfältigung, öffentliche Aufführung oder Verbreitung eines Werkes bedürfen grundsätzlich der Zustimmung des Urhebers, die meist gegen Entrichtung eines Entgelts für die jeweilige Nutzung erteilt wird. Das Urheberrecht sieht von diesem Grundsatz seit jeher Ausnahmen aus Gründen des Allgemeinwohls vor. So darf beispielsweise ein Lehrer für seine Klasse zum Unterrichtsgebrauch Vervielfältigungen in der erforderlichen Anzahl auch ohne Zustimmung des Urhebers herstellen. Dies ist jedoch nur eine von mehreren sog. „Schranken" des Urheberrechts, die durch die Erlaubnis der zustimmungsfreien Nutzung zu den gesetzlich definierten Zwecken, das Recht des Urhebers einschränken. Als Ausgleich für diese erlaubnisfreie Nutzung erhält der Urheber in der Regel eine pauschale Vergütung, die für ihn durch Verwertungsgesellschaften wie z. B. VG Wort, GEMA etc. wahrgenommen wird.

Durch die zunehmende Digitalisierung hat sich das Recht zur zustimmungsfreien Nutzung innerhalb der Schranken für die Urheber, insbesondere aber für die Verwertungsindustrie, zunehmend zu einem Dorn im Auge entwickelt. Im Bereich der Vervielfältigungen etwa, stellt die Digitaltechnologie eine günstige, wenig aufwendige und hochqualitative Möglichkeit der Erstellung von Kopien dar. Von der Seite der Rechteinhaber wird deshalb das Bedürfnis nach einer weitgehenden Einschränkung oder gar der Abschaffung von Schranken und der gleichzeitige gesetzliche Schutz technischer Kontrollmechanismen (Digital Rights Management) an die Politik herangetragen. Ziel ist eine im digitalen Zeitalter möglichst undurchbrochene Kontrollmöglichkeit in Bezug auf den Zugriff und die Verwendung urheberrechtlich geschützter Werke. Hierbei stören Schranken, die einen zustimmungsfreien Gebrauch von Werken erlauben. Auf der anderen Seite hat die Politik die mit den Schranken verbundenen Belange des Allgemeinwohls im Auge zu behalten. Hierzu zählen insbesondere die zahlreichen Schranken des Urheberrechts zu Gunsten von Bildung und Wissenschaft zur Gewährleistung der Informationsversorgung. Dem könnte zwar entgegengehalten werden, dass die Öffentliche Hand dies auch durch eine bessere finanzielle Ausstattung und der damit gegebenen Möglichkeit des Einkaufs der Informationen erreichen könnte. Diese Argumentation erkennt jedoch nicht das Ungleichgewicht in der Marktstruktur, das durch das unbedingte und alternativlose Angewiesensein in Wissenschaft und Forschung auf bestimmte Informationen und die gleichzeitig konkurrenzlose Verwertung auf der Angebotsseite entsteht, weshalb auch in einer digitalen Informationsgesellschaft das Bedürfnis nach Einschränkungen des Urheberrechts aus Gründen des Allgemeinwohls besteht.

1.) Europäische Vorgaben durch die Richtlinie 2001/29/EG

Den unterschiedlichen Interessen im Angesicht der technischen Entwicklung sollte die europäische „Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft" vom 22. Mai 2001 gerecht werden. Hierbei ist anzufügen, dass dieses Süppchen nicht allein auf EU-Ebene gekocht wurde, da die Richtlinie teils auch der Umsetzung internationaler Verpflichtungen durch WIPO-Verträge (WIPO = World Intellectual Property Organization) diente. Dem Kontrollbedürfnis der Urheber und Verwerter wird Rechnung getragen, indem den Mitgliedstaaten in der EU bindend vorgegeben wird, technische Schutzmechanismen rechtlich effektiv gegen Durchbrechung und Umgehung zu schützen. Andererseits wird an den Schranken zu Gunsten des Allgemeinwohls im Grundsatz festgehalten. Dies gilt im Bereich der Vervielfältigung insbesondere für die weiter aufrecht erhaltene Möglichkeit der Herstellung digitaler Kopien.

Bedeutsam für Forschung, Wissenschaft und Bildung ist zudem die im digitalen Kontext ohne Zustimmung des Urhebers ermöglichte Zugänglichmachung von Werken zur Veranschaulichung für einen abgegrenzten Kreis von Personen zu Unterrichtszwecken oder für Zwecke der wissenschaftlichen Forschung. Dies erleichtert den (netzbasierten) Informationsaustausch innerhalb von Forscherteams ungemein und eröffnet dem E-Learning neue Perspektiven.

Eine weitere bedeutsame Neuerung im Bereich der Schranken ist die für öffentlich zugängliche Bibliotheken, Bildungseinrichtungen, Museen oder Archive zu nichtkommerziellen Zwecken ermöglichte Wiedergabe oder Zugänglichmachung von in den Beständen enthaltenen Werken zu Zwecken der Forschung oder privater Studien auf eigens hierfür eingerichteten Terminals in den Räumlichkeiten der Einrichtungen.

Allerdings ist der Spagat, der durch die Richtlinie auf dem Weg zu einem Urheberrecht in der Informationsgesellschaft beschritten wird, unübersehbar. Einerseits soll durch den bindend vorgesehenen rechtlichen Schutz technischer Kontrollmechanismen, den Forderungen der Rechteinhaber nach einem restriktiven Urheberrecht als Reaktion auf die technischen Möglichkeiten entsprochen werden. Andererseits sollen die durch das Gemeinwohl bedingten Schranken des Urheberrechts auch unter den geänderten technischen Voraussetzungen erhalten bleiben und an die Veränderungen moderat angepasst werden. Da die Nutzung von Werken aufgrund einer entsprechenden Einschränkung des Urheberrechts (Schranke) regelmäßig keiner Zustimmung eines Rechteinhabers bedarf, geraten die Schranken als Durchbrechung des Kontrollprinzips in Konflikt mit der Konzeption des Selbstschutzes der Rechteinhaber durch den Einsatz technischer Kontrollmechanismen. Die Lösung erfolgt in der Richtlinie zuungunsten der Schranken, da die Durchbrechung, Entfernung oder Umgehung technischer Kontrollmechanismen auch im Falle eines an sich durch Schranken erlaubten Gebrauchs verboten ist. Zur Durchsetzung des erlaubten Gebrauchs gegenüber dem Einsatz technischer Schutzmechanismen ist lediglich ein gegebenenfalls einklagbarer Anspruch auf Ermöglichung des Gebrauchs vorgesehen. Im Falle der digitalen Privatkopie wurde die Entscheidung über die Einführung eines solchen Anspruchs in das Ermessen der Mitgliedstaaten gestellt. Bei Einsatz von technischen Kontrollmechanismen wurde der Spagat somit klar zu Gunsten der Selbstschutzinteressen der Rechteinhaber entschieden. Aus Sicht des Allgemeinwohls kommt erschwerend hinzu, dass die durch den technischen Fortschritt veränderten Arbeitsabläufe in Bildung, Wissenschaft und Forschung, in den entsprechenden Schranken, wenn überhaupt, nur halbherzig Berücksichtigung gefunden haben.

Die zwingenden Vorgaben der Richtlinie mussten durch die EU-Mitgliedstaaten vor dem 22. Dezember 2002 in nationales Recht umgesetzt werden.

2.) Die Umsetzung in deutsches Recht

Der durch die beschriebene Spagatsituation bestehende Konflikt zwischen den Interessen der Rechteinhaber, der Allgemeinheit und der Verbraucher, ließ eine schnelle Lösung nicht erwarten, so dass die Umsetzung der Richtlinie in deutsches Recht aufgrund des aufkommenden Zeitdrucks in zwei so genannte „Körbe" aufgeteilt wurde. Nach diesem Plan sollen die zwingenden Bestandteile der Richtlinie in einem „ersten Korb" umgesetzt werden, während streitige Bereiche, bei denen den Mitgliedstaaten Regelungsspielräume zustehen, begleitet von einer ausführlichen Diskussion einem „zweiten Korb" überlassen werden sollen.

a) Der „erste Korb"

Die Umsetzung im ersten Korb erfolgte durch das „Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft" vom 10.09.2003. Aus Nutzersicht standen im Mittelpunkt der Diskussionen vor allem die Zukunft der Privatkopie und die Einführung der neuen durch die Richtlinie ermöglichten Schranke zur zustimmungsfreien Zugänglichmachung von Teilen eines Werkes in Intranets zu Forschungs- und Unterrichtszwecken in einem neuen Paragraf 52a Urheberrechtsgesetz.

Im Zusammenhang mit der Privatkopie und dem Schutz technischer Schutzmechanismen, wurde das durch die Richtlinie eingeräumte Ermessen so ausgeübt, dass nur Kopien auf Papier oder ähnlichen Trägern rechtlich gegen den Einsatz von Kopierschutzmechanismen durchgesetzt werden können. Für digitale Kopien gilt dies nicht, so dass durch das gesetzliche Verbot der Umgehung das Recht auf Privatkopie beim Einsatz von Kopierschutzmaßnahmen praktisch auf die analoge Kopie beschränkt wird.

Ein wichtiger Meilenstein war die Schaffung der neuen Schranke in Paragraf 52a Urheberrechtsgesetz. Durch die in Grenzen ermöglichte Zugänglichmachung von veröffentlichten Teilen eines Werkes, wurden die Voraussetzungen für mehr Rechtssicherheit in Bezug auf E-Learning Anwendungen und die vernetzte Arbeit von Forscherteams geschaffen. Dabei sah es kurz vor Abschluss des Gesetzgebungsverfahrens so aus, dass die Einführung dieser neuen Beschränkung des Urheberrechts an den, vor allem durch die Verwertungsindustrie, geäußerten Bedenken scheitern könnte. In dieser kritischen Phase hat die Forschungsstelle Anfang 2003 im Auftrag des DFN-Verein eine an die zuständigen Ministerien gerichtete Stellungnahme zur Unterstützung des Vorhabens erstellt, in der die besondere Bedeutung einer solchen Schranke für die Zukunft der vernetzten Forschung herausgehoben wurde. Letztlich gelang die Einführung der neuen Schranke, jedoch mit dem Wermutstropfen, dass den Bedenken der Verwerter mit einer Befristung des Paragrafen bis zum 31.12.2006 entgegengekommen wurde. Dies hat die Wirkung, dass die Schranke ohne eine Verlängerung automatisch zum 1.1.2007 außer Kraft tritt. Für eine vorausschauende Arbeit an Wissenschafts-, Forschungs- und Bildungseinrichtungen sind dies keine guten rechtlichen Rahmenbedingungen.

b) Der „zweite Korb"

Der sog. „zweite Korb" soll wie gesagt die streitigen Punkte aufgreifen, bei denen die Richtlinie den Mitgliedstaaten Ausgestaltungsspielraum belässt. Das Vorhaben ist bis dato noch nicht abgeschlossen. Den Auftakt bildete ein Symposium zum Urheberrecht in der Informationsgesellschaft des Bundesministeriums der Justiz im September 2003. Bereits hier wurde deutlich, dass die Fronten

in Bezug auf die Schranken weiter verhärtet sind. Von der Seite der Rechteinhaber wird trotz des erreichten Schutzes technischer Kontrollmechanismen, ein restriktiveres Urheberrecht gefordert, indem teilweise die Abschaffung der digitalen Privatkopie und die wesentliche Einschränkung des erlaubnisfreien Gebrauchs von geschützten Werken über die Schranken des Urheberrechts gefordert wird. Die Nutzerseite möchte hingegen die Erhaltung des durch die Schranken ermöglichten Gebrauchs aus Gründen des Allgemeinwohls erhalten und eine Anpassung an die durch die Digitalisierung veränderten Arbeitsbedingungen erreichen. Die Forderungen der Rechteinhaber nach einer weiteren Zurückdrängung des in den Schranken zum Ausdruck kommenden Allgemeinwohlgedankens, hat weite Teile von Wissenschaft, Bildung und Forschung auf den Plan gerufen. Unter Beteiligung des DFN-Verein und seiner Forschungsstelle Recht, wurde zusammen mit einer Reihe weiterer Organisationen am 5. Juli 2004 durch die Verabschiedung der „Göttinger Erklärung" das Aktionsbündnis „Urheberrecht für Bildung und Wissenschaft" ins Leben gerufen und kontinuierlich aufgebaut. Erklärtes gemeinsames Ziel darin, ist der Einsatz für ein Urheberrecht, das auch in einer digitalisierten und vernetzten Gesellschaft den Zugang zu Informationen für Bildung und Wissenschaft zu fairen Bedingungen sicherstellt. Bis dato wurde die Göttinger Erklärung von 6 großen Wissenschaftsorganisationen, annähernd 300 Fachgesellschaften, Verbänden und Institutionen und mehr als 4000 Einzelpersonen unterzeichnet.

aa) Erster Referentenentwurf

Ein erster Referentenentwurf des federführenden Bundesministeriums der Justiz wurde am 27. September 2004 veröffentlicht. Anknüpfend an diesen Entwurf veröffentlichte das Aktionsbündnis am 26. November eine ausführliche juristische Expertise, die im Bündnis unter Federführung der Forschungsstelle Recht im DFN entstanden ist. Die darin enthaltene Kritik an den Vorschlägen des Justizministeriums knüpfte in erster Linie an der teilweise praxisfernen Ausgestaltung der Schranken zu Forschungs- und Bildungszwecken angesichts der technologischen Entwicklungen an.

So ist beispielsweise nicht nachvollziehbar, warum der Versand von Kopien durch Bibliotheken mittels Telefax unter den weiteren Voraussetzungen immer zulässig sein soll, während der Versand als grafische Datei mittels E-Mail nur dann zulässig sein soll, wenn der entsprechende Verlag kein eigenes kommerzielles elektronisches Angebot betreibt. Elektronische Angebote der Verlage bieten weitaus mehr Komfort und Verwendungsmöglichkeiten als die Zusendung einer grafischen Datei, deren Zusendung per E-Mail zudem mit der Sendung eines Faxes technisch vergleichbar ist. Ein weiteres Kuriosum war im Zusammenhang mit der durch Paragraf 52b des Entwurfs geplanten Ermöglichung der elektronischen Wiedergabe vorhandener Werke an Terminals, die Beschränkung des gleichzeitig ermöglichten Zugangs auf die Zahl der tatsächlich als „Hardware" in den Regalen vorhandenen Werke.

Ein weiterer wesentlicher Schwerpunkt der Kritik richtete sich gegen die oftmals komplizierte Ausgestaltung von Regelungen mit 5 Ausnahmen und jeweils wieder mindestens 2 Unterausnahmen, so dass selbst studierten Juristen das Verständnis oft schwer fällt. Angesichts dessen, dass Gesetze im Prinzip für die Bürger und damit auch für Nichtjuristen geschaffen werden, ist dies ein Armutszeugnis.

Nicht zuletzt wurde das Augenmerk auf die erst im ersten Korb eingeführte Schranke in Paragraf 52a Urheberrechtsgesetz gerichtet, die durch die Befristung zum 31.12.2006 und die Nichtberücksichtigung im Entwurf leise zu sterben droht.

bb) Zweiter Referentenentwurf

Der erste Referentenentwurf wurde durch einen zweiten Referentenentwurf des Bundesjustizministeriums aufgrund der durch die Neuwahl im Herbst 2005 veränderten politischen Situation abgelöst. In seinen Grundstrukturen weicht der zweite Referentenentwurf, der Anfang Januar 2006 der Öffentlichkeit präsentiert wurde, nicht wesentlich von dem ersten Entwurf ab. In Bezug auf die Schranken sticht jedoch heraus, dass die kuriose Beschränkung auf die Anzahl der angeschafften Exemplare bei der Wiedergabe an Terminals aus Paragraf 52b des Entwurfs gestrichen wurde. Daneben wurden insbesondere für den Bildungsbereich Anregungen in dem Entwurf übernommen.

cc) Regierungsentwurf

Nach einer kurzen Abstimmung zwischen den Ministerien, wurde ein Regierungsentwurf für den sog. „Zweiten Korb" am 22. März 2006 durch die Bundesregierung beschlossen. In den genannten Bereichen ergaben sich im Prinzip keine Veränderungen. Im weiteren Verlauf muss der Entwurf das parlamentarische Gesetzgebungsverfahren durchlaufen. Überraschungen sind hier durchaus noch möglich, da der derzeitige Entwurf auch Gegenwind aus den Fraktionen der Koalitionspartner erfährt. Zudem gibt es aus der Presse Verlautbarungen, dass nun doch eine Verlängerung des Paragrafen 52a Urheberrechtsgesetz über den 31.12.2006 hinaus erwogen werde.

3.) Weiteres Vorhaben: Umsetzung der „Durchsetzungsrichtlinie"

Zudem wurde im Januar 2006 ein weiterer Referentenentwurf des Bundesministeriums der Justiz zur Umsetzung einer weiteren europäischen Richtlinie mit Bezug zum Urheberrecht öffentlich. Die so genannte „Durchsetzungsrichtlinie" mit der offiziellen Bezeichnung 2004/48/EG, verfolgt die Verbesserung der Stellung der Rechteinhaber beim Kampf gegen Produktpiraterie. Der Referentenentwurf des Justizministeriums sieht in einem geänderten Paragrafen 101 Urheberrechtsgesetz, einen Anspruch der Rechteinhaber gegenüber Dritten auf Auskunft über die Identität eines Verletzers auch dann vor, wenn der Dritte in gewerblichem Ausmaß Dienstleistungen erbringt, die für eine rechtsverletzende Tätigkeit genutzt werden. Letztendlich geht es darum, dass beispielsweise Platten- und Filmunternehmen von Access-Providern anhand aufgeschnappter IP-Adressen Name und Anschrift des entsprechenden Kunden wegen einer angenommenen Urheberrechtsverletzung herausverlangen können, was bislang rechtlich nicht möglich ist.

In Bezug auf dieses Vorhaben hat die Forschungsstelle Recht am 28. Februar 2006 eine Stellungnahme gegenüber dem Bundesministerium der Justiz abgegeben. Kern der darin enthaltenen Kritik ist einerseits die sehr vage gehaltene Formulierung des Entwurfs. Aus der bisherigen Formulierung lässt sich nicht zweifelsfrei bestimmen, wann von der Erbringung von Dienstleistungen durch den Dritten in gewerblichem Ausmaß ausgegangen werden muss. Des Weiteren droht durch die vage Ausgestaltung der vorgesehenen Eingrenzungskriterien eine Überflutung der Provider mit Anfragen. Als größtes Problem stellt sich jedoch die Verfügbarkeit der für die Auskunfterteilung erforderlichen Daten bei den Providern dar. Aus Gründen des Datenschutzes müssen Daten wie die IP-Adresse und der Zeitpunkt ihrer Zuteilung beim Provider grundsätzlich gelöscht werden, sofern diese nicht für die Abrechnung erforderlich sind. Entsprechend sind bereits von Seiten der Rechteinhaber Forderungen laut geworden, dass die zur Terrorismusbekämpfung und Verfolgung von schweren Straftaten geplante Vorratsdatenspeicherung von Telekommunikationsdaten auch zur Ermöglichung von Klagen durch die Musik- und Filmindustrie fruchtbar gemacht wird. Ob hierbei noch das Verhältnis gewahrt bleibt, ist indes noch fragwürdiger als bei der Vorratsdatenspeicherung zu Sicherheitsinteressen, da letztlich jeder Telekommunikationsnutzer als potentiell Verdächtiger behandelt wird.

„Big Brother“ im Hörsaal

Rechtliche Grenzen der Videoüberwachung an Hochschulen

Noogie C. Kaufmann
Rechtsanwalt, Master of Arts

Forschungsstelle Recht im DFN

E-Mail: recht@dfn.de

Gestohlene Bücher, demolierte Hörsäle und aufgebrochene Spinde gehören zum Alltag an deutschen Hochschulen. Aus Gründen der Abschreckung und Aufklärung derartiger Straftaten ordnen Rektoren und Präsidenten verstärkt den Einsatz von Videokameras an. Doch die Installation und auch die Aufzeichnungen müssen im Einklang mit den Buchstaben des Gesetzes stehen. Die Nichtbeachtung kann handfeste Folgen haben: Es droht unter anderem ein Beweisverwertungsverbot, wonach trotz Videonachweis vom Übeltäter kein Ersatz verlangt werden kann.

Bereits im Jahre 1907 hat der Gesetzgeber im Kunsturheberrechtsgesetz (KUG) ein grundsätzliches Verbot von Bildaufnahmen von Menschen ohne deren Einwilligung statuiert. Da zu diesem Zeitpunkt noch keine Videotechnik existierte, wurde auf Bundesebene Anfang 2000 der Paragraf 6b in das Bundesdatenschutzgesetz (BDSG) eingefügt. Diese Norm regelt nunmehr die Voraussetzungen für den Einsatz von „Big Brother“. Da die Regelungen in den jeweiligen Ländern nahezu identisch sind, wird vorliegend nur auf Paragraf 6b BDSG eingegangen.

Das BDSG kommt jedoch nur zur Anwendung, soweit nicht hoheitliche Träger aktiv werden. Soll beispielsweise eine Überwachung eines öffentlichen Platzes erfolgen, gilt dafür das jeweilige Polizeigesetz des Landes; für den Einsatz bei Versammlungen ist das Versammlungsgesetz die rechtliche Grundlage. Weiter muss es sich um „öffentlich zugängliche Räume“ handeln. Entgegen des Wortlautes ist das Merkmal jedoch weit zu verstehen, da darunter alle Bereiche verstanden werden, die kraft ihrer Funktion von jedermann betreten werden dürfen. Unterschieden wird ferner zwischen der reinen Beobachtung mittels einer Kamera durch Menschen und der anschließenden Aufzeichnung; mithin dem „Konservieren“ der Bilder auf Bildträgern. Hauptmerkmal von Paragraf 6b BDSG ist die dort festgezurrte Interessenabwägung der Belange der Hochschule auf der einen Seite und mit den Belangen der Studenten beziehungsweise der Bediensteten auf der anderen Seite. Anschaulich und auch verständlich normiert hat der Gesetzgeber die Interessen der Hochschule, die vornehmlich in der Wahrnehmung des allgemeinen Hausrechts liegen. Bei den betroffenen Personen spricht das Gesetz sehr allgemein und nebulös von deren „schutzwürdigen Interessen“. Gemeint ist damit vornehmlich das Recht am eigenen Bild, was bereits zur Einführung des KUG führte, und dem allgemeinen Persönlichkeitsrecht, das Art. 2 Absatz 1 in Verbindung mit Art. 1 Absatz 1 Grundgesetz (GG) schützt. Diese beiden sich gegenüberstehenden Interessen sind stets in eine Abwägung zu bringen und entscheiden darüber, ob überhaupt eine Kamera installiert werden darf, an welchem Ort, ob Aufzeichnungen gemacht werden und wie lange die gläsernen Augen aktiviert sein dürfen. In den allermeisten Fällen erfolgt der Einsatz von „Big Brother“ zur Verfolgung von Straftaten, was erst einmal vom Hausrecht der Hochschule gedeckt ist.

Zulässiger Einsatz – vielfaches ist zu beachten

Um dem Recht am eigenen Bild und dem allgemeinen Persönlichkeitsrecht seitens der Betroffenen gerecht zu werden, müssen aber vorab vier Punkte beachtet werden. Erst dann ist ein Einsatz statthaft. Zum ersten muss die Überwachung auf Bereiche beschränkt werden, in denen es in der Vergangenheit mehrfach zu Straftaten gekommen ist. Keine Einwände bestehen etwa, wenn in der Bibliothek nachweislich Bücher auf seltsame Weise verschwinden. Gleiches gilt für die Entwendung von technischem Equipment. Soll aber „Big Brother“ im Hörsaal eingesetzt werden, dient das mitnichten der Strafverfolgung und ist folglich rechtswidrig. Zum zweiten hat eine zeitliche Begrenzung des Einsatzes zu erfolgen, die sich an den tatsächlichen Gegebenheiten zu orientieren hat. Schließt die Bücherei um 20 Uhr, hat auch die Kamera ab diesem Zeitpunkt „Sendepause“. Zum dritten ist dafür Sorge zu tragen, dass nur berechtigtes Personal Zugang zu den Monitoren und zu eventuell vorgenommen Aufzeichnungen hat. Dafür müssen ausreichende Sicherheitsmaßnahmen ergriffen werden. Unzulässig ist etwa, dass wissenschaftliche Mitarbeiter oder sonstige Verwaltungsbedienstete in den Monitorraum marschieren können. Und viertens ist das berühmte „Ultima-Ratio-Prinzip“ zu beachten. Existieren andere Mittel, um Diebstahl, Vandalismus und Co. Herr zu werden, müssen diese Maßnahmen ergriffen werden; der Einsatz von Vi-

deokameras ist dann rechtswidrig. Dabei spielen auch Kosten eine Rolle. So haben sich beispielsweise einige Polizeipräsidien gegen den Einsatz von Kameras an Plätzen mit einer hohen Kriminalitätsrate entschieden, da eine verstärkte Präsenz von Streifenpolizisten ebenso wirksam war und dabei weniger Kosten verursacht wurden, als sie beim Kauf von Kameras und dem Personaleinsatz zur Überwachung angefallen wären. Soweit alle vier Voraussetzungen vorliegen und der Einsatz somit rechtmäßig ist, muss ferner noch deutlich auf die Überwachung hingewiesen werden. Erforderlich, aber auch ausreichend, sind dabei grafische Darstellungen. Soweit nicht nur eine reine Überwachung erfolgt, sondern auch eine Aufzeichnung, schreibt Paragraf 6b Absatz 3 BDSG letztens noch vor, dass die Daten unverzüglich zu löschen sind, wenn sie nicht mehr benötigt werden. Praktisch verhält es sich beispielsweise so, dass Aufzeichnungen vom Vortag nach Durchsicht am darauf folgenden Tag dann zu vernichten sind, wenn keine besonderen Vorkommnisse registriert wurden.

„Freispruch" trotz bewiesener Straftat

Im Falle eines Prozesses kann die Nichteinhaltung von Paragraf 6b Bundesdatenschutzgesetz beziehungsweise der jeweiligen Landesregelungen bei den Hochschulverantwortlichen für ein böses Erwachen sorgen. Grund dafür ist das so genannte Beweisverwertungsverbot, wonach trotz Nachweis der Straftat auf dem Videoband der Übeltäter nicht zum Schadensersatz verurteilt wird, da die Aufzeichnung vom Gericht schlichtweg nicht berücksichtigt werden darf. Die Richter müssen dann so tun, als wäre das Band gar nicht existent. Da die Hochschule zum Beweis der Straftat verpflichtet ist und diesen nicht führen kann, verlässt der Schädiger den Gerichtssaal im Extremfall als Sieger. Exemplarisch sei auf eine Entscheidung des Oberlandesgerichts (OLG) Köln verwiesen (Urteil vom 5.7.2005, Az. 24 U 12/05, abgedruckt in „Neue Juristische Wochenschrift" 2005, S. 2997). Im dortigen Fall kam es in einem Mehrfamilienhaus wiederholt zu Vandalismus an den im Keller stehenden Waschmaschinen, die der Vermieter dort zur Verfügung gestellt hatte. Um den Täter bei weiteren Attacken zu überführen, installierte der Eigentümer heimlich eine Videokamera, die rund um die Uhr aktiviert war. Nachdem ein Mieter dabei ertappt wurde, wie er eine fremde Waschmaschine mit Fußtritten „bearbeitet" hatte, erhob der Vermieter Klage auf Zahlung von Schadensersatz für die Reparatur der Maschinen. Zum Beweis legte er die Videoaufzeichnungen vor, die den Beklagten tatsächlich als Täter entlarvten. Gleichwohl wies das OLG die Klage ab. Begründung: Die heimliche Installation eine Videokamera, mit der „rund um die Uhr" Aufzeichnungen gefertigt wurden, stelle einen so schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht des Beklagten dar, dass es als rechtswidriges Beweismittel einzustufen sei und nicht verwertet werden könne. In der vorzunehmenden Abwägung der gegenseitigen Interessen hob das Gericht zwar auch das Interesse des Vermieters an seinem Eigentum hervor. Dieses hätte aber auch durch eine offene Überwachung erreicht werden können, da dann der Täter wohl von weiteren Beschädigungen abgesehen hätte.

Rootkits – Die Tarnkappen der Angreifer

Das eigene System macht eigentlich gerade nichts. Das sagen zumindest der Task Manager und der fast leere Desktop. Aber die Festplatte scheint nie zur Ruhe zu kommen und auch die Lichter der Netzwerkkarte blinken ohne Unterlass.

Bald treffen Beschwerden von Kollegen und Bekannten ein: Man soll doch bitte keine Mails mit Werbung verschicken. Ein Kollege meint, dass das System bestimmt mit einem Virus infiziert sei. Die Anti-Viren Software beharrt aber auch nach Aktualisierung der Signaturen darauf, dass das System frei von Viren ist.

Schließlich wird das System von einem Experten genauer untersucht und es stellt sich heraus, dass jemand über das Netzwerk eingebrochen ist und ein „Rootkit" installiert hat. Mit Hilfe des Rootkits wurden die Programme versteckt, die für das Verschicken der unerwünschten Werbe-Mail verantwortlich sind.

Was ist ein Rootkit?

Ein Angreifer bricht in ein System ein, indem er verschiedene Sicherheitslücken ausnutzt. Um nun auf dem System unentdeckt zu bleiben, werden spezielle Programme eingesetzt: sogenannte Rootkits. Ein Rootkit dient nicht der Ausnutzung einer Sicherheitslücke, durch die der Angreifer Zugriff zum System erlangen kann. Es ist auch nicht die Hintertür, die erneuten Zugriff über das Netzwerk für den Angreifer ermöglicht. Das Rootkit dient ausschließlich der Verschleierung der Aktivitäten des Angreifers auf dem System und soll in der Regel alle Dateien, Verzeichnisse, Prozesse und Netzwerk-Verbindungen des Angreifers unsichtbar machen.

Die Geschichte der Rootkits begann in den 80'er Jahren auf UNIX-Systemen [1]. Es wurden Logfiles verändert und die Ausgaben zum Status des Systems manipuliert, um die Accounts der Angreifer zu verheimlichen. Das Ziel war, auch später noch Zugriff als „root" zu haben, dem Administratoren-Account auf UNIX und Linux Systemen. Hieraus entstand der Name „Rootkit". Bald tauschten die Angreifer auch diverse Systemprogramme aus, um bestimmte Verbindungen, Dateien und Prozesse aus deren Ausgabe verschwinden zu lassen. Nachdem Rootkits sich auch auf Linux Systemen verbreitet hatten, kamen Mitte der 90'er Jahre erstmals neuartige Rootkits auf, die den Kern des Betriebssystems manipulierten. Da das Betriebssystem die Schnittstelle aller regulären Programme zur Hardware ist, kann ein solches Rootkit an einer zentralen Stelle jegliche Manipulation vornehmen und ist sehr schwer zu entdecken. Diese Entwicklung wurde bald von Linux wieder zurück getragen auf UNIX-Betriebssysteme wie Solaris und verschiedene BSD-Varianten. Ende der 90'er Jahre verbreiteten sich Rootkits schließlich auch auf Windows Systemen. Mittlerweile gibt es kaum ein Betriebssystem, auf dem es nicht irgendeine Version eines Rootkits gibt. Die bei weitem aktivste Entwicklung findet im Umfeld von Windows und Linux statt.

Wer installiert Rootkits?

Das Ausnutzen von Sicherheitslücken wurde in den letzten Jahren dadurch erleichtert, dass die dafür notwendigen Programme und Werkzeuge frei verfügbar und teilweise auch leicht zu bedienen sind. Die gleiche Entwicklung findet bei Rootkits statt. Vor einigen Jahren war noch erhebliches Expertenwissen notwendig, um ein Rootkit erfolgreich einsetzen zu können. Aktuelle Rootkits helfen bei der Installation, besitzen integrierte Hintertüren, die automatisch versteckt werden und sind insgesamt auch deutlich schwerer zu finden. Hat ein Angreifer Zugriff zum System erlangt, muss daher immer mit der Installation eines Rootkits gerechnet werden.

Andreas Bunten

DFN-CERT
Heidenkampsweg 41
20097 Hamburg

bunten@dfn-cert.de
http://www.dfn-cert.de/

Die in Rootkits entwickelten Techniken werden mittlerweile auch durch Würmer, Viren und Spyware eingeschleust, um Anti-Viren Software effektiver auszuweichen. Zuweilen kommen Rookits aus ganz unerwarteten Quellen: Manche Audio CDs und Video DVDs verwenden einen Kopierschutz, der versucht, Software zu installieren, sobald die CDs bzw. DVDs in ein Laufwerk eines Windows Systems eingelegt werden. Diese Software verhält sich wie ein Rootkit und dient leider auch „echter" Schadsoftware als Versteck [2][3].

Wie können Rootkits aufgespürt werden?

Ein aktuelles Rootkit, das den Kern des Betriebssystems manipuliert, kann den Angreifer sehr effektiv verstecken. Durch Manipulation einer geeigneten Funktion im Kern können beispielsweise bestimmte Dateien unsichtbar gemacht werden. Da alle regulären Programme in der Regel die gleichen Schnittstellen zum Betriebssystem verwenden, werden diese Dateien damit auch für alle Programme versteckt. Obwohl die Entdeckung eines Rootkits dadurch sehr schwer ist, gibt es mittlerweile eine Reihe von Werkzeugen dafür. Diese verwenden in der Regel eine oder mehrere der folgenden Vorgehensweisen.

Signatur-basierte Suche

Nach bereits bekannten Rootkits kann im Speicher und auf der Festplatte mit Hilfe von Signaturen gesucht werden. Eine Signatur eines Rootkits kann dabei eine typische Folge von Bytes sein. Das Werkzeug „determine" sucht z.B. im Kernelspeicher eines Linux Systems auf diese Weise nach dem Rootkit Adore-NG. Das Programm „chkrootkit" sucht nach Signaturen verschiedener Rootkits auf UNIX und Linux Systemen.

Dies ist auch die typische Vorgehensweise von Anti-Viren Software und kann auf verschiedene Weisen von einem Rootkit unterlaufen werden. Der Zugriff auf die Festplatte kann vom Rootkit manipuliert werden und prinzipiell auch der Zugriff auf den Speicher des Systems. Schreibt das Rootkit keine Daten auf die Festplatte, kann es so nicht gefunden werden. Mit Hilfe einer Signatur können nur bereits bekannte Rootkits gefunden werden. Wurde das Rootkit verändert oder modifiziert es sogar selbstständig den eigenen Programmcode, ist die Suche nach einer festen Signatur erfolglos.

Suche mit generischen Signaturen

Anstatt ein festes Muster zu beschreiben, kann eine Signatur auch generisch ein Rootkit-typisches Verhalten angeben. Damit sollen auch bisher unbekannte und leicht modifizierte Rootkits entdeckt werden. Typisch für ein Rootkit ist beispielsweise der Trick, Programme in Alternate Data Streams auf Windows Systemen zu verstecken. Das NTFS-Dateisystem ermöglicht es, Daten in Alternate Data Streams für den Benutzer unsichtbar zu speichern. Da in der Regel nur Meta-Informationen auf diese Weise

Werkzeuge zum Entdecken und Entfernen von Rootkits

Linux / UNIX	
determine	http://stealth.openwall.net/rootkits/removal/
chkrootkit	http://www.chkrootkit.com/
patchfinder	http://www.phrack.org/phrack/59/p59-0x0a.txt
Windows	
RootkitRevealer	http://www.sysinternals.com/Utilities/RootkitRevealer.html
BlackLight	http://www.f-secure.com/blacklight/
Klister	http://invisiblethings.org/tools/klister-0.4.zip
Strider GhostBuster	http://research.microsoft.com/rootkit/
Patchfinder2	http://invisiblethings.org/tools/PF2/
Vice	http://www.rootkit.com/project.php?id=20
System Virginity Verifier	http://invisiblethings.org/tools/svv/

abgelegt werden, suchen z.B. die Werkzeuge „RootkitRevealer“ und „BlackLight“ in Alternate Data Streams nach ausführbaren Programmen.

Generische Signaturen führen zu vermehrten Falschmeldungen, da die Signaturen oft nicht nur auf Rootkits sondern auch auf nicht standardkonforme, legitime Programme passen. Wird in einem Rootkit eine neue Technik implementiert, kann es auch durch eine generische Signatur nicht gefunden werden.

Vergleichende Suche

Mit der sog. „Cross-View-Methode“ wird die gleiche Information über das System auf verschiedenen Wegen eingeholt und verglichen. Ergibt sich eine Differenz, liegt wahrscheinlich eine Manipulation des Systems vor. Der eine Weg ist dabei die Standard-Methode, der andere greift direkt auf die internen Strukturen des Betriebssystems zu und verwendet nicht die normalen Schnittstellen.

Eine vergleichende Suche kann z.B. nach versteckten Dateien in einem Verzeichnis durchgeführt werden. Unter Linux / UNIX werden die Dateien in einem Verzeichnis mit dem Befehl „ls“ aufgelistet, wobei u.a. der oft von Rootkits manipulierte Systemaufruf getdents() verwendet wird. Mit dem Programm „debugfs“ kann das Dateisystem analysiert werden, ohne dass die üblichen Systemaufrufe wie getdents() verwendet werden. Tauchen Dateien in der Ausgabe von debugfs auf, aber nicht bei ls, wurden diese von einem Rootkit versteckt.

Ein weiteres Beispiel ist die Untersuchung der gerade aktiven Prozesse, deren Liste zuerst durch einen Standard-Befehl ermittelt wird. Diese Liste wird dann mit den Daten verglichen, die ein Programm direkt aus den entsprechenden Strukturen des Betriebssystems gewinnt. So geht z.B. das Werkzeug „klister“ unter Windows vor. Weitere Werkzeuge, die zumindest teilweise vergleichend suchen, sind „RootkitRevealer“, „Blacklight“ und „Strider GhostBuster“.

Die vergleichende Suche kann nur schwer vom Rootkit umgangen werden und ist dadurch sehr hilfreich. In der Regel kann damit aber nur die Manipulation selbst aufgedeckt werden, ohne dabei Hinweise auf das vorliegende Rootkit zu erlangen.

Suche nach Anomalien / Test der System-Konsistenz

Bei der Suche nach Anomalien wird allgemein nach Inkonsistenzen im System gesucht. Dies können z.B. Abweichungen bei Standard-Parametern oder zentralen Datenstrukturen im Kern des Betriebssystems sein. Ein Beispiel für einen zu überprüfenden Parameter ist der Zeiger auf die „Interrupt Descriptor Table“, die eine zentrale Rolle bei der Ausführung von Systemaufrufen einnimmt. Der Zeiger hat typischer Weise einen bestimmten Wert, aber manche Rootkits lassen den Zeiger auf eine eigene Datenstruktur zeigen, um so den Kontrollfluss zu verändern [6]. Unter Windows werden Konsistenztests bzgl. derartiger Manipulation z.B. vom „System Verginity Verifier“ durchgeführt und unter Linux durch „Kstat2“.

Ein weiterer Konsistenztest kann durch die Messung der mittleren Laufzeit von Systemaufrufen erfolgen. Die Idee dabei ist, dass die Manipulationen eines Rootkits im Kern des Betriebssystems zur Laufzeit einen nicht unbeträchtlichen Mehraufwand erfordern. Es werden dafür in der Regel Referenzwerte von der gleichen Version des Betriebssystems mit den gleichen Treibern erstellt und diese mit aktuellen Messungen verglichen. Tatsächlich ist der von manchen Rootkits verursachte Mehraufwand so groß, dass auch sehr ungenaue Referenzwerte ausreichen, um die manipulierten Systemaufrufe zu entdecken. Der Konsistenztest wird unter Linux und unter Windows durch die gleichnamigen Programme „Patchfinder“ realisiert. Ähnliche Suchen nach Anomalien werden durch die Werkzeuge „vice“ und dem „System Virginity Verifier“ durchgeführt.

Die Konsistenztests bzw. die Suche nach Anomalien sind hilfreiche Mittel auf der Suche nach Rootkits. Aber auch hier sind Falschmeldungen durch schlecht implementierte, legitime Software möglich und, wie bei der vergleichenden Suche, wird nur die Manipulation aufgedeckt und nicht das Rootkit selbst.

Weitere Beispiele zur Suche nach Rootkits auf UNIX und Linux Systemen sind im Artikel „Rootkits: Techniken und Abwehr“ des 10. DFN-CERT Workshop zu finden [6]. Es gibt kein Werkzeug, dass jedes Rootkit finden kann. In der Regel müssen daher eine Reihe von Programmen verwendet werden, um einen sinnvollen Test auf Rootkits durchzuführen.

Rootkits wieder loswerden

Wurde ein Rootkit gefunden, soll es in der Regel vom System entfernt werden. Viele der oben genannten Werkzeuge ermöglichen dies auf bequeme Weise, aber in der Praxis trifft man dabei u.a. auf folgende Probleme:

1. Manche Rootkits setzen sich sehr tief im System fest und ein unbedarftes Entfernen (z.B. durch Umbenennung von Dateien) kann dazu führen, dass das System nicht mehr startfähig ist.
2. Anti-Rootkit Werkzeuge erkennen oft legitime Programme als vermeintliche Rootkits.
3. Ist ein System längere Zeit durch Sicherheitslücken verwundbar, brechen oft verschiedene Angreifer parallel ein und installieren unterschiedliche Rootkits und Hintertüren.

Vor allem aufgrund des letzten Punktes kann man nie wirklich sicher sein, dass alle Rootkits und die damit versteckten Hintertüren entdeckt wurden. Als erste Reaktion kann daher zwar das gefundene Rootkit mit einem geeigneten Werkzeug oder manuell unschädlich gemacht werden, aber die einzig konsequente Reaktion kann danach nur eine Neuinstallation sein. Diese Ansicht wird mittlerweile auch bei Microsoft vertreten [4]. Damit das möglich ist, wird vor allem ein gutes Backup sowohl der Benutzer-Daten als auch des Systems benötigt. In größeren Rechnerpools sollten einzelne Systeme schnell und ohne Aufwand automatisiert neu installiert werden können. Nur so kann effektiv auf einen Einbruch und die Installation eines Rootkits reagiert werden, damit der Schaden minimiert wird.

Der Angreifer kann aber nicht nur auf dem betroffenen System selbst aufgespürt werden. Da ein Angreifer immer etwas mit dem System vor hat, wird sich diese Aktivität auch bald im Netzwerkverkehr niederschlagen. Der Netzwerkverkehr kann mit Hilfe von Intrusion Detection Systemen oder einfach nur durch die Kontrolle der Netflows beobachtet werden, um an zentraler Stelle eine frühe Warnung zu erhalten.

Beispiel für eine vergleichende Suche nach Rootkits (Cross View) auf einem Linux System

Es besteht ein erster Verdacht, dass ein Einbruch in ein Linux-System stattgefunden hat. Der Inhalt von /tmp wird kontrolliert:

```
webhamster:~# ls -al /tmp
total 24
drwxrwxrwt   6 root root 4096 2006-02-18 01:18 .
drwxr-xr-x  21 root root 4096 2006-01-03 02:11 ..
drwxrwxrwt   2 root root 4096 2006-02-17 15:14 .ICE-unix
drwx------   2 root root 4096 2006-02-17 15:35 ssh-UZhejn9506
-r--r--r--   1 root root   11 2006-02-17 15:34 .X0-lock
drwxrwxrwt   2 root root 4096 2006-02-17 15:34 .X11-unix
```

Beim genaueren Hinsehen stellt man fest, dass der Link-Count des Verzeichnisses 5 und nicht 6 sein müsste. Für eine vergleichende Suche kann jetzt mit dem Werkzeug „debugfs“ auf das Dateisystem zugegriffen werden, ohne die üblichen Schnittstellen zu verwenden:

```
webhamster:~# debugfs /dev/sda1
debugfs 1.37 (21-Mar-2005)
debugfs:  ls -l /tmp

 808001   41777 (2)      0      0    4096 18-Feb-2006 00:52 .
      2   40755 (2)      0      0    4096  3-Jan-2006 02:11 ..
 243117   41777 (2)      0      0    4096 17-Feb-2006 15:34 .X11-unix
 243118   41777 (2)      0      0    4096 17-Feb-2006 15:14 .ICE-unix
 938006   40755 (2)  21037  27421    4096 17-Feb-2006 15:30 owned
 340099   40700 (2)      0      0    4096 17-Feb-2006 15:35 ssh-UZhejn9506
 808240  100444 (1)      0      0      11 17-Feb-2006 15:34 .X0-lock
```

Es existiert tatsächlich ein weiteres Verzeichnis in /tmp. Dieses kann auch mit Hilfe von „debugfs“ kopiert werden, so dass es auch wieder bei normalem Zugriff sichtbar ist:

```
debugfs:  rdump /tmp /root/test
debugfs:  quit
webhamster:/tmp# ls -al /root/test/tmp
total 28
drwxrwxrwx  6 root  root  4096 2006-02-18 01:08 .
drwxr-xr-x  3 root  root  4096 2006-02-18 01:10 ..
drwxrwxrwx  2 root  root  4096 2006-02-17 15:14 .ICE-unix
drwxr-xr-x  4 21037 27421 4096 2006-02-17 15:30 owned
drwx------  2 root  root  4096 2006-02-17 15:35 ssh-UZhejn9506
-r--r--r--  1 root  root    11 2006-02-17 15:34 .X0-lock
drwxrwxrwx  2 root  root  4096 2006-02-17 15:34 .X11-unix
```

Bei Untersuchung des so versteckten Verzeichnisses stellt sich heraus, dass die Angreifer das Kernel-basierte Rootkit Adore-NG installiert haben.

Insgesamt kann die Entwicklung der Rootkits und der Werkzeuge zu ihrer Entdeckung als eine Art Wettrennen gesehen werden. Es ist sinnvoll, sich mit der aktuellen Entwicklung zu befassen und sich z.B. frühzeitig mit den Werkzeugen vertraut zu machen. Immer auf dem aktuellsten Stand zu sein kostet aber viel Zeit und Aufwand. Ein zuverlässiges Backup, eine solide Infrastruktur und feste Kontrolle über das Netzwerk liefern eine allgemeine Grundabsicherung, mit der das Wettrennen aus einem bequemen Abstand verfolgt werden kann.

Tipps zum Umgang mit Sicherheitsvorfällen und Hinweise zum Finden von Rootkits sowie Referenzen zu den oben genanngen Werkzeugen sind auf den Incident Response Seiten des DFN-CERT zu finden [5].

Referenzen

[1] „HIDING OUT UNDER UNIX“
http://www.phrack.org/phrack/25/P25-06

[2] „DVD-Kopiersperre Alpha-DVD: Update oder Uninstaller“
http://www.heise.de/newsticker/meldung/print/71115

[3] „Sony BMGs Kopierschutz mit Rootkit-Funktionen“
http://www.heise.de/security/news/meldung/print/65602

[4] „Microsoft Says Recovery from Malware Becoming Impossible“
http://www.eweek.com/article2/0,1895,1945808,00.asp

[5] „Incident Response“
http://www.dfn-cert.de/dfncert/incident-response/

[6] „Rootkits: Techniken und Abwehr“, DFN-CERT Workshop, Februar 2003
http://www.dfn-cert.de/team/bunten/rootkits_ws2003.pdf

Erfolgreicher DFN-CERT-Workshop

Anfang März 2006 veranstaltete das DFN-CERT den mittlerweile 13. Workshop „Sicherheit in vernetzten Systemen". Den rund 320 Teilnehmern wurde ein abwechslungsreiches Programm präsentiert, das viele aktuelle Themen der IT-Sicherheit beleuchtete. Der bekannte Firewall-Experte Bill Cheswick eröffnete die zweitägige Veranstaltung im Congress Centrum Hamburg mit seinem humorvollen aber im weiteren Verlauf auch sehr nachdenklich stimmenden Vortrag über den „virenverseuchten Computer seines Vaters". Es folgten Vorträge aus dem Bereich Kryptographie (u.a. von Werner Koch, dem Entwickler des Verschlüsselungsprogramms „GnuPG") und zum Thema Open-Source-Firewalls. Kontrovers diskutiert wurde nach dem Vortrag von Jörg Helbach (GI) zum Thema „Internetwahlen in der Praxis".

Am zweiten Tag lag der Schwerpunkt bei den Themen Honeypots und Voice over IP. Christian Wieser von der Universität Oulu in Finnland deckte auf, dass die meisten VoIP-Systeme noch nicht ausgereift sind. Den Abschluss bildeten zwei Vorträge zu den Themen Forensik und Windows Rootkits. Die Vortragsfolien und weitere Informationen zur Veranstaltung finden Sie unter https://www.dfn-cert.de/events/ws/2006/

Schon mal vormerken: Der nächste DFN-CERT-Workshop findet am 7. und 8. Februar 2007 wieder in Hamburg statt.

Übersicht über die Mitgliedseinrichtungen und Organe des DFN-Vereins

(Stand 6/2006)

Laut Satzung fördert der DFN-Verein die Schaffung der Voraussetzungen für die Errichtung, den Betrieb und die Nutzung eines rechnergestützten Informations- und Kommunikationssystems für die öffentlich geförderte und gemeinnützige Forschung in der Bundesrepublik Deutschland. Der Satzungszweck wird verwirklicht insbesondere durch Vergabe von Forschungsaufträgen und Organisation von Dienstleistungen zur Nutzung des Deutschen Forschungsnetzes.

Als Mitglieder werden juristische Personen aufgenommen, von denen ein wesentlicher Beitrag zum Vereinszweck zu erwarten ist oder die dem Bereich der institutionell oder sonst aus öffentlichen Mitteln geförderten Forschung zuzurechnen sind.

Die Organe des DFN-Vereins sind

- die Mitgliederversammlung
- der Verwaltungsrat
- der Vorstand

Sitz des Vereins ist Berlin.
Die **Mitgliederversammlung** ist u.a. zuständig für die Wahl der Mitglieder des Verwaltungsrates, für die Genehmigung des Jahreswirtschaftsplanes, für die Entlastung des Vorstandes und für die Festlegung der Mitgliedsbeiträge. Derzeitiger Vorsitzender der Mitgliederversammlung ist Prof. Dr. Gerhard Peter, FH Heilbronn.

Verwaltungsrat
Der Verwaltungsrat beschließt über alle wesentlichen Aktivitäten des Vereins, insbesondere über die technisch-wissenschaftlichen Arbeiten, und berät den Jahreswirtschaftsplan. Für die 8. Wahlperiode bis Ende 2008 sind Mitglieder des Verwaltungsrates:

- Prof. Dr. Claudia Eckert, Fraunhofer-Institut für Sichere Telekooperation, Darmstadt
- Vis. Prof. Geerd-Rüdiger Hoffmann, Deutscher Wetterdienst
- Prof. Dr. Wilfried Juling, Universität Karlsruhe
- Dr. Klaus-Peter Kossakowski, PRESECURE Consulting GmbH, Telgte
- Prof. Dr. Reinhard Maschuw, Forschungszentrum Karlsruhe
- Prof. Dr. Wolfgang E. Nagel, TU Dresden
- Prof. Dr. Bernhard Neumair, GWDG Göttingen
- Dr. Frank Nolden, Universität Leipzig (Kanzler)
- Dr.-Ing. Christa Radloff, Universität Rostock
- Prof. Dr. Gerhard Schneider, Universität Freiburg
- Manfred Seedig, Universität Kassel
- Günter Springer, TU Ilmenau
- Prof. Dipl.-Ing. Herbert Wiese, FH Esslingen

Vorstand
Der Vorstand des DFN-Vereins im Sinne des Gesetzes wird aus dem Vorsitzenden und den beiden stellvertretenden Vorsitzenden des Verwaltungsrates gebildet. Derzeit sind dies Prof. Dr. Wilfried Juling, Vorsitz, sowie Prof. Dr. Bernhard Neumair und Dr. Frank Nolden.

Der Vorstand wird beraten von einem Technischen Ausschuss (TA), einem Betriebsausschuss (BA), und einem Ausschuss für Recht und Sicherheit (ARSi), der zugleich auch als Jungendschutzbeauftragter für das DFN fungiert.

Der Vorstand bedient sich zur Erledigung laufender Aufgaben einer **Geschäftsstelle** mit Standorten in Berlin und Stuttgart. Sie wird von einer Geschäftsführung geleitet.
Als Geschäftsführer wurden vom Vorstand Klaus Ullmann und Jochem Pattloch bestellt.

Der DFN-Verein hat derzeit folgende Mitglieder:

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Fachhochschule Aalen
Albstadt	Fachhochschule Albstadt-Sigmaringen
Amberg	Fachhochschule Amberg-Weiden
Aschaffenburg	Fachhochschule Aschaffenburg
Augsburg	Fachhochschule Augsburg
	Universität Augsburg
Bamberg	Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Berliner Elektronenspeicherring-Gesellschaft für Synchrotronstrahlung mbH (BESSY)
	BBB Management GmbH
	Bundesanstalt für Materialforschung und -prüfung (BAM)
	Bundesinstitut für Risikobewertung
	CDU Bundesgeschäftsstelle
	Deutsche Telekom AG
	Deutscher Beamtenbund (DBB)
	Deutsches Herzzentrum
	Deutsches Historisches Museum (DHM) GmbH
	Deutsches Institut für Normung e.V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	Alice-Salomon-Fachhochschule für Sozialarbeit und Sozialpädagogik Berlin
	Fachhochschule für Technik und Wirtschaft
	Fachhochschule für Wirtschaft
	Fachinformationszentrum Chemie GmbH (FIZ Chemie)
	Institut für Nachrichtentechnik
	Fraunhofer Heinrich-Hertz-Institut für Nachrichtentechnik
	Freie Universität Berlin (FUB)
	Hahn-Meitner-Institut Berlin GmbH (HMI)
	Humboldt-Universität Berlin (HUB)
	IT-Dienstleistungszentrum
	Konrad-Zuse-Zentrum für Informationstechnik Berlin (ZIB)
	Landesbetrieb für Informationstechnik (LIT)
	Robert-Koch-Institut
	Stiftung Preußischer Kulturbesitz
	Stanford-Universität in Berlin
	Technische Fachhochschule Berlin (TFH)
	Technische Universität Berlin (TUB)
	Umweltbundesamt
	Universität der Künste
	Forschungsverbund Berlin e.V.
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum für Sozialforschung gGmbH (WZB)
	T-Systems Enterprise Services GmbH
Biberach	Fachhochschule Biberach, HS für Bauwesen und Wirtschaft
Bielefeld	Fachhochschule Bielefeld
	Universität Bielefeld
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische FH Rheinland-Westfalen-Lippe
	Fachhochschule Bochum,
	Technische FH Georg Agricola für Rohstoffe, Energie und Umwelt
	Ruhr-Universität Bochum
Böblingen	Staatliche Akademie für Datenverarbeitung
Bonn	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
	Bundesministerium für Verkehr, Bau- und Stadtentwicklung
	Deutsche Forschungsgemeinschaft
	Deutscher Akademischer Austauschdienst e.V. (DAAD)
Bonn	Deutsches Zentrum für Luft und Raumfahrt
	Universität Bonn
	IZ Sozialwissenschaften
	Zentrum für Informationsverarbeitung und Informationstechnik
	Bundesministerium des Innern
Borstel	FZB, Leibniz-Zentrum für Medizin und Biowissenschaften
Brandenburg	Fachhochschule Brandenburg
Braunschweig	Biologische Bundesanstalt für Land- und Forstwirtschaft
	Bundesforschungsanstalt für Landwirtschaft (FAL)
	Fachhochschule Braunschweig/Wolfenbüttel
	Gesellschaft für Biotechnologische Forschung mbH (GBF)
	Hochschule für Bildende Künste
	Physikalisch-Technische Bundesanstalt (PTB)
	Technische Universität Braunschweig
Bremen	Hochschule Bremen
	International University Bremen GmbH
	Universität Bremen
Bremerhaven	Hochschule Bremerhaven
	Stadtbildstelle Bremerhaven
	Stiftung Alfred-Wegener-Institut für Polar- und Meeresforschung (AWI)
Chemnitz	Technische Universität Chemnitz
Clausthal	Clausthaler Umwelttechnik-Institut GmbH (CUTEC)
	Technische Universität Clausthal-Zellerfeld
Coburg	Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus
Darmstadt	European Space Agency (ESA)
	Fachhochschule Darmstadt
	Gesellschaft für Schwerionenforschung mbH (GSI)
	Merck KGaA
	Technische Universität Darmstadt
	T-Systems Enterprise Services GmbH
Deggendorf	Fachhochschule Deggendorf
Detmold	Lippische Landesbibliothek
Diepholz	Private Fachhochschule für Wirtschaft und Technik
Dortmund	Fachhochschule Dortmund
	Universität Dortmund
Dreieich	PanDacom Networking AG
Dresden	Forschungszentrum Rossendorf e.V.
	Hannah-Arendt-Institut für Totalitarismusforschung e.V.
	Hochschule für Bildende Künste
	Hochschule für Technik und Wirtschaft (FH)
	Leibniz-Institut für Festkörper- und Werkstofforschung e.V.
	Leibniz-Institut für Polymerforschung Dresden e.V.
	Sächsische Landesbibliothek
	Technische Universität Dresden
Düsseldorf	Fachhochschule Düsseldorf
	Landesamt für Datenverarbeitung und Statistik des Landes NRW
	Heinrich-Heine-Universität Düsseldorf
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Joh. A. Lasco Bibliothek - Große Kirche Emden
Erfurt	Fachhochschule Erfurt
	Universität Erfurt
Erlangen	Universität Erlangen-Nürnberg
Essen	Rheinisch-Westfälisches Institut für Wirtschaftsforschung
	Universität Duisburg-Essen
Esslingen	Fachhochschule Esslingen, Hochschule für Technik
Flensburg	Fachhochschule Flensburg
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Die Deutsche Bibliothek Frankfurt

Frankfurt/M.	Deutsches Institut für Internationale Pädagogische Forschung
.	Fachhochschule Frankfurt am Main
	Fachinformationszentrum Technik e. V. (FIZ Technik)
	Juniper Networks
	KPN EuroRings B.V.
	Phil.-Theol. Hochschule St. Georgen e. V.
	Universität Frankfurt am Main
Frankfurt/O.	Europa-Universität Viadrina Frankfurt/Oder
	IHP Innovations for High Perfomance Microelectronics/ Institut für innovative Mikroelektronik
Freiberg	TU/Bergakademie Freiberg
Freiburg	Universität Freiburg
Fulda	Fachhochschule Fulda
Furtwangen	Fachhochschule Furtwangen
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Gatersleben	Institut für Pflanzengenetik und Kulturpflanzenforschung
Geesthacht	GKSS-Forschungszentrum Geesthacht GmbH
Gelsenkirchen	Fachhochschule Gelsenkirchen
Gießen	Fachhochschule Gießen-Friedberg
	Universität Gießen
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GwDG)
	IWF, Wissen und Medien gGmbH
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	Universität Greifswald
Hagen	FernUniversität in Hagen
	Fachhochschule Südwestfalen, Fachhochschule für Technik und Wirtschaft
Halle/Saale	Martin-Luther-Universität Halle-Wittenberg
	Institut für Wirtschaftsforschung Halle
Hamburg	Bundesamt für Seeschiffahrt und Hydrographie (BSH)
	Deutsches Elektronen Synchrotron (DESY)
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	Hochschule für angewandte Wissenschaften Hamburg
	Heinrich-Pette-Institut für Experimentelle Virologie und Immunologie
	Hewlett Packard GmbH
	Hochschule für Bildende Künste
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg-Harburg
	Helmut-Schmidt-Universität, Universität der Bundeswehr Hamburg
	Universität Hamburg
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe (BGR)
	Evangelische Fachhochschule Hannover
	Fachhochschule Hannover
	Hochschule für Musik und Theater Hannover
	Hochschul-Informations-System-GmbH
	Medizinische Hochschule Hannover
	Niedersächsisches Landesamt für Bergbau, Energie und Geologie
	Gottfried Wilhelm Leibniz Bibliothek - Niedersächsische Landesbibliothek
	Tierärztliche Hochschule Hannover
	Universität Hannover
	Universitätsbibliothek Hannover und Technische Informationsbibliothek (TIB)
Heide	FH Westküste
Heidelberg	Network Laboratories, NEC Europe Ltd.
	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	Universität Heidelberg
Heilbronn	Fachhochschule Heilbronn
Heyrothsberge	(Institut der Feuerwehr Sachsen-Anhalt)
Hildesheim	Fachhochschule Hildesheim/Holzminden/Göttingen Hochschule für angewandte Wissenschaft und Kunst
	Universität Hildesheim
Hof	Fachhochschule Hof
Ilmenau	Technische Universität Ilmenau
Ingolstadt	Fachhochschule Ingolstadt
Jena	Fachhochschule Jena
	Friedrich-Schiller-Universität Jena
	Leibniz-Institut für Altersforschung e.V. (FLI)
	Institut für Physikalische Hochtechnolgie e.V.
Jülich	Forschungszentrum Jülich GmbH
Kaiserlautern	Fachhochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	Hochschule Karlsruhe
	Fachinformationszentrum (FIZ Karlsruhe)
	Forschungszentrum Karlsruhe GmbH
	Technische Universität Karlsruhe
	Universität Karlsruhe
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Fachhochschule Kempten
	DIZ Zentrum für Hochschuldidaktik der bayerischen Fachhochschulen
Kiel	Fachhochschule Kiel
	Leibniz-Institut für Meereswissenschaften
	Institut für Weltwirtschaft
	Universität Kiel
Koblenz	Fachhochschule Koblenz
	Universität Koblenz-Landau
	Landesbibliothekszentrum Rheinland-Pfalz
Köln	Deutsches Institut für medizinische Dokumentation und Information (DIMDI)
	Deutsche Sporthochschule Köln
	Fachhochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln
	Universität zu Köln
Köthen	Hochschule Anhalt (FH) (Köthen, Bernburg, Dessau)
Konstanz	Universität Konstanz
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e.V.
Landshut	Fachhochschule Landshut
Leipzig	Fachhochschule Leipzig der Deutschen Telekom AG
	Hochschule für Grafik und Buchkunst
	Hochschule für Technik, Wirtschaft und Kultur Leipzig (FH)
	Institut für Troposphärenforschung e.V.
	Mitteldeutscher Rundfunk
	Umweltforschungszentrum Leipzig-Halle GmbH
	Universität Leipzig
Lemgo	Fachhochschule Lippe und Höxter
Ludwigshafen	Fachhochschule Ludwigshafen, HS für Wirtschaft
Lübeck	Fachhochschule Lübeck
	Universität zu Lübeck
Lüneburg	Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Institut für Neurobiologie
	Otto-von-Guericke-Universität Magdeburg
Mainz	Fachhochschule Mainz
	Universität Koblenz-Landau
	Universität Mainz
Mannheim	Hochschule Mannheim
	TÜV Energie- und Systemtechnik GmbH

Mannheim	Baden-Württemberg
	Universität Mannheim
	Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW)
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Universität Marburg
Merseburg	Fachhochschule Merseburg
Mittweida	Hochschule Mittweida, University of Applied Sciences
Mosbach	Berufsakademie Mosbach, Staatl. Studienakademie
München	Bayerische Staatsbibliothek Bibliotheksverbund Bayern
	DECUS München e.V.
	Fachhochschule München
	Fraunhofer-Gesellschaft (FhG) e. V.
	GSF-Forschungszentrum für Umwelt und Gesundheit GmbH
	IFO-Institut für Wirtschaftsforschung e.V.
	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft e.V., (MPG)
	SIEMENS AG
	Technische Universität München
	Universität der Bundeswehr München
Müncheberg	Zentrum für Agrarlandschafts- und Landnutzungsforschung (ZALF) e.V.
Münster	Fachhochschule Münster
	Institut für Angewandte Informatik an der Universität Münster
	Universität Münster
Neu Ulm	Fachhochschule Neu Ulm
Neubrandenburg	Hochschule Neubrandenburg
Nordhausen	Fachhochschule Nordhausen
Nürnberg	Fachhochschule Nürnberg
	Kommunikationsnetz Franken e.V.
Nürtingen	Hochschule für Wirtschaft und Umwelt
Oberursel	Dimension Data Germany AG & Co. KG
Oberwolfach	Mathematisches Forschungsinstitut gGmbH
Offenbach/Main	Deutscher Wetterdienst Offenbach
Offenburg	Fachhochschule Offenburg, HS für Technik und Wirtschaft
Oldenburg	Landesbibliothek Oldenburg
	Universität Oldenburg
Osnabrück	Fachhochschule Osnabrück
	Universität Osnabrück
Paderborn	HNF Heinz Nixdorf MuseumsForum GmbH
	Universität Paderborn
Passau	Universität Passau
Peine	Deutsche Gesellschaft zum Bau und Betrieb von Endlagern für Abfallstoffe mbH
Potsdam	Deutsches Institut für Ernährungsforschung Bergholz-Rehbrücke
	Fachhochschule Potsdam
	GeoForschungsZentrum Potsdam
	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam Institut für Klimafolgenforschung e.V. (PIK)
	Universität Potsdam
Ratingen	SUN Microsystems GmbH
Recklinghausen	InfoTech Gesellschaft für Informations- und Datentechnik mbH
Regensburg	Fachhochschule Regensburg
	Universität Regensburg
Rosenheim	Fachhochschule Rosenheim
Rostock	Institut für Ostseeforschung
	Universität Rostock
Saarbrücken	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Fachhochschule Bonn Rhein-Sieg
Sankt Ingbert	Comchat AG-Security
Schmalkalden	Fachhochschule Schmalkalden
Schwäbisch-Gmünd	Pädagogische Hochschule
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Senftenberg	Fachhochschule Lausitz
Siegen	Universität Siegen
Speyer	Deutsche Hochschule für Verwaltungswissenschaften
Stralsund	Fachhochschule Stralsund
Straeten	GasLINE
Stuttgart	Cisco Systems GmbH
	DaimlerCrysler AG
	Hochschule der Medien
	Hochschule für Technik
	Nextira One Deutschland GmbH
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte
Trier	Fachhochschule Trier
	Universität Trier
Tübingen	Friedrich-Loeffler-Institut Bundesforschungsinstitut für Tiergesundheit
	Universität Tübingen
Ulm	Fachhochschule Ulm, Hochschule für Technik
	Universität Ulm
Vechta	Hochschule Vechta
Wachtberg	Forschungsgesellschaft für angewandte Naturwissenschaften e.V.
Weidenbach	Fachhochschule Weihenstephan
Weimar	Bauhaus-Universität Weimar
Weingarten	Fachhochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz, Fachhochschule für Wirtschaft und Technik
Wiesbaden	Fachhochschule Wiesbaden
	Statistisches Bundesamt
Wessling	T-Systems Solutions for Research GmbH
Wildau	Technische Fachhochschule Wildau
Wilhelmshaven	Fachhochschule Oldenburg/Ostfriesland/Wilhelmshaven
Wismar	Hochschule Wismar
Witten	Universität Witten/Herdecke
Wolfenbüttel	Herzog-August-Bibliothek
Worms	Fachhochschule Worms
	Wissenschaftliche Bibliothek der Stadt Worms
Würzburg	Fachhochschule Würzburg-Schweinfurt
	Universität Würzburg
Wuppertal	Bergische Universität Wuppertal
Zittau	Hochschule für Technik und Wirtschaft Zittau/Görlitz (FH)
	Internationales Hochschulinstitut
Zwickau	Westsächsische Hochschule Zwickau (FH)

termine

7. bis 9. Juni 2006, Heilbronn
20. DFN-Arbeitstagung über Kommunikationsnetze
http://www.dfn.de

9. bis 12. Juni 2006, Toronto, Kanada
IEEE International Conference on Multimedia and Expo
http://www.ieee.org

15. Juli 2006, Venedig, Italien
International Workshop on Algorithmic Aspects of Wireless Sensor Networks
http://ru1.cti.gr/algosensors06/

16. bis 18. September 2006, Waikoloa, USA
IEEE International Conference on Information Reuse and Integration
http://www.sis.pitt.edu/~iri06

17. bis 18. Oktober 2006, Berlin
45. DFN-Betriebstagung
http://www.dfn.de

22. bis 28. Oktober 2006, Santa Barbara, USA
ACM Multimedia Conference
http://mmdb.ece.ucsb.edu/acmmm06/

29. bis 30. Oktober 2006, Split/Dubrovnik, Kroatien
International Conference on Software, Telecommunications and Computer Networks
http://www.fesb.hr/SoftCOM

6. Dezember 2006, Bonn
53. DFN-Mitgliederversammlung
http://www.dfn.de

7. bis 8. Februar 2007, Hamburg
14. DFN-CERT Workshop
http://www.dfn-cert.de/