DFN mitteilungen

35 Jahre Deutsches Forschungsnetz

Im Wandel der Zeit

Peering-Strategie im X-WiN
Kommunizieren ohne Grenzen

Informationssicherheit im DFN
Das Motto: Prävention, Detektion, Reaktion

9 770177 689001

Impressum

Herausgeber: Verein zur Förderung
eines Deutschen Forschungsnetzes e. V.

DFN-Verein
Alexanderplatz 1, 10178 Berlin
Tel.: 030 - 88 42 99 - 0
Fax: 030 - 88 42 99 - 370
Mail: dfn-verein@dfn.de
Web: www.dfn.de

ISSN 0177-6894

Redaktion: Maimona Id
Lektorat: Angela Lenz
Gestaltung: Labor3 | www.labor3.com
Druck: Druckerei Rüss, Potsdam

Fotonachweis
Titelfoto: © chepkoelena / iStockphoto
Seite 6/7 © Koldunov / iStockphoto
Seite 42/43 © BDMcIntosh / iStockphoto
Umschlag Rückseite: © ortodoxfoto / Adobe Stock

Prof. Dr. Hans-Joachim Bungartz
Vorstandsvorsitzender im DFN-Verein,
Dekan der Fakultät für Informatik der TU München sowie Mitglied des Direktoriums des LRZ

Viele von uns werden die Feierlichkeiten zum dreißigjährigen Bestehen des DFN-Vereins noch in lebhafter Erinnerung haben – insbesondere die Festveranstaltung im Französischen Dom am Vortag der 68. Mitgliederversammlung. Und schon ist der nächste runde – na gut, halbrunde – Geburtstag da: Der DFN-Verein wird 35.

Und so halten wir kurz inne, blicken zurück und nach vorn. Für den Rückblick haben wir einen der Grandseigneurs gewinnen können – DFN-Urgestein, wie es urgesteiniger (und manchmal auch uriger) nicht mehr geht: Heinz-Gerd Hegering, der den Verein und das Wissenschaftsnetz weit mehr geprägt hat, als es die (durchaus stattlichen) zwölf Jahre Verwaltungsrat und neun Jahre Vorstand zum Ausdruck bringen. Und – wie man es nicht anders von ihm gewohnt ist – sagt er nicht nur etwas, sondern er hat auch etwas zu sagen.

Bei der Bestandsaufnahme inklusive eines Blicks in die Zukunft muss der aktuelle Vorstand ran. Nach nunmehr fast acht Jahren Vorstandsvorsitz ist es für mich immer wieder spannend zu sehen, wie das Gebälk des Deutschen Forschungsnetzes im Sturm der Zeiten arbeitet und ächzt, aber doch jeder Belastungsprobe standhält; wie verschiedene, zuweilen divergierende Interessenslagen immer wieder das gemeinsame Ganze auf die (meist wohlbekannte) Probe stellen, am Ende sich dann aber doch das Solidarprinzip sowie die Erkenntnis des Mehrwerts für alle durchsetzen; wie immer wieder neue Technologien, Möglichkeiten, Dienste und Aufgaben hochpoppen, ohne dass Bestehendes dadurch obsolet würde. Und so liefert die Lektüre des Beitrags von Heinz-Gerd Hegering auch für die heute für den Verein Verantwortung tragenden Personen das eine oder andere Déjà-vu.

Aber keine Sorge, es geht nicht nur um Selbstreflexion – zu viel tut sich gerade an den verschiedenen „Fronten“. Und so gibt es auch in diesem Heft eine Fülle spannender Beiträge rund um die Themen Netz, Internationales, Sicherheit, Recht und vieles mehr.

Lassen Sie mich zum Abschluss noch ein paar Worte des Dankes sagen. Getreu dem bewährten bayerischen Motto „ned g’schimpft is g’lobt g’nug“ (ich hoffe, alle aus der DFN-Familie kommen hier ohne Übersetzung aus …) kommt der Dank in der Hektik des Alltags immer etwas zu kurz. Ich bedanke mich herzlich bei unseren Mitgliedern und Anwendern für ihre Verbundenheit; bei denjenigen unter diesen, die sich auf den verschiedenen Podien (Beirat, Betriebsausschuss, ARuS, Verwaltungsrat etc.) ehrenamtlich für den Verein engagieren und dabei ein ums andere Mal Partikularinteressen hintanstellen; bei unseren nationalen und internationalen Partnern; bei der Politik, die offenbar (natürlich vollkommen zurecht) ein derart gutes Bild vom DFN-Verein hat, dass man uns auch komplexe Aufgaben überträgt; und – last, aber nun wirklich alles andere als least – bei den Mitarbeiterinnen und Mitarbeitern unserer Geschäftsstelle, die jeden Tag die Grundlage dafür schaffen, dass dem DFN-Verein national wie international derart großes Vertrauen entgegengebracht wird.

Wir – ich darf hier im Namen des Vorstandes und der Geschäftsführung sprechen – freuen uns mit ungeminderter Leidenschaft auf die vor uns liegenden Aufgaben zur gedeihlichen Fortentwicklung des Deutschen Forschungsnetzes.

Herzlichst,
Ihr Hans-Joachim Bungartz


1


2


3


4


5


6


7


8


9


10


11


12


13


14


15


16


17

Unsere Autoren dieser Ausgabe im Überblick

1 Heinz-Gerd Hegering, Leibniz-Rechenzentrum, LRZ (heinz-gerd.hegering@lrz.de); **2** Hans-Joachim Bungartz, Technische Universität München (bungartz@in.tum.de); **3** Stephan Peinkofer, Leibniz-Rechenzentrum, LRZ (stephan.peinkofer@lrz.de); **4** Helmut Reiser, Leibniz-Rechenzentrum, LRZ (helmut.reiser@lrz.de); **5** Henry Kluge, DFN-Verein (kluge@dfn.de); **6** Stefan Piger, DFN-Verein (piger@dfn.de); **7** Barbara Diederich, DFN-Verein (diederich@dfn.de); **8** Kim Gush, Council for Scientific and Industrial Research, CSIR (kgush@csir.co.za); **9** Maimona Id, DFN-Verein (id@dfn.de); **10** Leonie Schäfer, DFN-Verein (schaefer@dfn.de); **11** Ralf Gröper, DFN-Verein (groeper@dfn.de); **12** Dennis-Kenji Kipker, Universität Bremen (kipker@uni-bremen.de); **13** Marc Brendel, Universitätsrechenzentrum Heidelberg (marc.brendel@urz.uni-heidelberg.de); **14** Maximilian Hoecker, Universitätsrechenzentrum Heidelberg (maximilian.hoecker@urz.uni-heidelberg.de); **15** Andree Müller, Universitätsrechenzentrum Heidelberg (andree.mueller@urz.uni-heidelberg.de); **16** Marten Tiessen, Forschungsstelle Recht im DFN (tiessen@uni-muenster.de); **17** Charlotte Röttgen, Forschungsstelle Recht im DFN (roettgen@dfn.de).

Inhalt

Wissenschaftsnetz

International

Sicherheit

Campus

Recht

DFN-Verein

Wissenschaftsnetz

Daten, Dienste, Digitalisierung – 35 Jahre DFN

DFN wurde heuer 35 Jahre alt. Für manch einen ein Grund zur Gewissenserforschung: Hatte ich die richtigen Ziele, Partner und Freunde? Der DFN hat es sich einfach gemacht und einen Autor gefragt, der seit 1985 mit dem DFN verbandelt ist und lange Jahre als Vertreter eines Großnutzers (LRZ) dem Betriebsausschuss, dem Verwaltungsrat und dem Vorstand angehörte. Die Darstellung fällt darum notgedrungen subjektiv aus. Bei der hohen Innovationsrate der letzten gut drei Dekaden und der ihm eigenen Agilität des DFN-Vereins bietet sich eine Fülle von Material an, das nur zu einem kleinen Teil hier genannt werden kann.

Text: **Heinz-Gerd Hegering** (ehem. stellv. Vorsitzender des DFN-Vereins, ehem. Vorsitzender des Direktoriums des LRZ)

Aus der Mitte der Wissenschaft: Am 12. Januar 1984 wurde das Deutsche Forschungsnetz (DFN) gegründet. Zum Gründungsvorstand gehörten Prof. Dr. Zander (2. v. li.), Prof. Dr. Szyperski (3. v. li.) und Prof. Dr. Jessen (nicht im Bild). Das Hahn-Meitner-Institut zählte zu den 11 Gründungsmitgliedern, vertreten durch den damaligen Geschäftsführer Dr. Nettesheim (1. v. li.). Klaus Ullmann (1. v. rechts) war einer der ersten Geschäftsführer des DFN-Vereins.

Vergegenwärtigen wir uns kurz die Situation zur Gründungszeit in den 1980er Jahren. Das typische Versorgungskonzept der Datenverarbeitung war damals noch charakterisiert durch zentralorientierte Mainframes mit einer herstellerspezifischen Netzanbindung von Fernstapelstationen und Dialoggeräten, die über Multiplexer oder erste Knotenrechner konzentriert wurden. SNA, Transdata oder CDCNet waren Beispiele solcher Architekturen. Herstellerneutrale Protokollstandards über alle Schichten hinweg waren noch nicht entwickelt. X.25 war zwar bereits als Ergebnis eines englischen Forschungsprojektes definiert und pilotmäßig in SERCNet, dem Vorläufer des späteren englischen Wissenschaftsnetzes JANET, eingesetzt, aber bei der Bundespost wurde soeben erst der Datex-P-Dienst mit Anschlussraten von 50 Baud bis 64 kbit/s aufgebaut. In den USA war gerade das Internet Activities Board (IAB) gegründet worden, das ARPANET hatte seine Bewährungsprobe längst bestanden, das Stanford Research Institute (SRI) arbeitete an neuen Protokollspezifikationen.

1982 wurde am LRZ deutschlandweit das erste 10-Mbit-Ethernet installiert (100m Koax-Kabel und vier Transceiver kosteten damals fast 100.000 DM!). Die ersten Arbeitsplatzrechner (PSI 80 von Kontron oder M24 von Olivetti) mit den verschiedensten Betriebssystemen und Terminalemulationen (Anschlussrate von 9,6 kbit/s) kamen auf den Markt. Die Arbeitsplatzsystem- und Netz-Förderprogramme CIP, WAP oder später NIP, die für die Gesamtdurchdringung der Universitäten mit IT geschaffen wurden, waren noch nicht wirksam, die deutschen Hochschulen waren von einer systematischen und flächendeckenden Vernetzung noch deutlich entfernt. Das wurde erst besser nach dem ersten Netzmemorandum der Kommission für IT-Infrastruktur (KfR) der DFG aus dem Jahr 1986. Dennoch empfahl bereits 1981 eine SRI-Studie auch für Deutschland den Aufbau eines Wissenschaftsnetzes. Eine Informationsreise des Bundesministeriums für Forschung und Technologie (BMFT) in die USA bekräftigte die Empfehlung. Dies führte 1982 zur Gründung eines Arbeitskreises, der ein deutsches Forschungsnetz vorbereiten sollte. Dabei sollten die laufenden Planungen für einen norddeutschen Rechnerverbund und die bei der GMD (frühere Gesellschaft für Mathematik und Datenverarbeitung mbH) unter Eckardt Raubold entstandene Planskizze für ein deutsches Verbundnetz einfließen.

„Stößchen“ – ein Prosit auf das erste Wissenschaftsnetz des DFN-Vereins X.25 WiN: Prof. Dr. Dieter Haupt, Vorsitzender des DFN-Vereins (vorne li.), Dipl.-Ing. Klaus Werner, Präsident der Oberpostdirektion Telekom Berlin (vorne re.).

Schließlich kam es am 12. Januar 1984 zur Gründung des „Vereins zur Förderung eines Deutschen Forschungsnetzes e. V.“, kurz „DFN-Verein“. Zu den Gründungsmitgliedern zählten neben der GMD und dem HMI die DFVLR (heute DLR), die Fraunhofer-Gesellschaft (FhG), die Universitäten Hamburg, Karlsruhe und TU Berlin sowie die Industriefirmen IBM, Nixdorf, Siemens und Philips. Es wurde ein erster Verwaltungsrat bestimmt mit vier Repräsentanten aus den Hochschulen, drei Vertretern der außeruniversitären staatlichen Forschung und zwei Vertretern aus der Industrie. Aus ihnen ging der erste DFN-Vorstand hervor: Prof. Dr. Eike Jessen, Prof. Dr. Norbert Szyperski und Dr. Hagen Hultzsch. Bei der feierlichen Gründungsveranstaltung am 30. März 1984 in Schloss Birlinghoven war Forschungsminister Dr. Heinz Riesenhuber anwesend.

Das erste Wissenschaftsnetz ging mit 64 kbit/s an den Start, heute sind es bis zu 200 Gbit/s.

Die ersten Jahre vergingen mit intensiven technischen Diskussionen über die richtige Plattform für ein produktives deutsches Wissenschaftsnetz. Damals wurde in Deutschland zeitgleich an vier Ansätzen konkurrierend gearbeitet: Einige Standorte mit IBM-Systemen wie Heidelberg oder IPP in Garching setzten auf das von IBM gesponserte EARN (European Academic Research Network). Karlsruhe baute auf einen Link zum CSNet (Computer Science Network) in den USA. Dortmund versuchte, die gerade aufkommenden UNIX-Rechner mit EUnet zu vernetzen, und der DFN-Verein favorisierte die international genormten OSI-Protokolle und er stand dabei nicht isoliert da. Ich erinnere an das von der GMD geführte Protokollprojekt PIX, das OSA-Projekt oder die vom Bundesinnenminister eingeleiteten Standardisierungsverfahren EHKP (Einheitliche Höhere Kommunikationsprotokolle) für die öffentliche Verwaltung, deren Schnittstellen eine Zeit lang sogar bei öffentlichen Ausschreibungen gefordert wurden. In Nordrhein-Westfalen wurde gar ein EHKP-basiertes Verwaltungsnetz betrieben. Auch in den USA boomte auf wissenschaftlichen Kongressen der Religionskrieg OSI versus Internet. 1990 stellte der Vertreter des BMFT in einer Mitgliederversammlung (MV) klar, dass die Zuwendungen des Bundes an die OSI-Orientierung gebunden seien. Bei einer vorherigen MV hatte der DFN-Vorsitzende jedoch zu Protokoll gegeben: „DFN plant, einen IP-Knoten in Deutschland einzurichten. Da die Bedeutung von IP in der Zukunft zurückgehen wird, muss auf eine geordnete Überführung von Internet-Anwendungen geachtet werden. Dazu werden entsprechende Gespräche mit der Internetorganisation in den USA aufgenommen.“ Anmerkung: Erst 1994 fiel im DFN die Entscheidung für IPnG und damit für das Ende der OSI-Entwicklung. Als Folge bildeten damals EUnet (Dortmund), XLINK (Karlsruhe) und der DFN-Verein gemeinsam ein Konsortium zum Betrieb von DE-NIC (Zentrale Registrierungsstelle für alle Domains mit Endung .de).

In den ersten sechs Jahren plante der DFN-Verein ein erstes produktives Wissenschaftsnetz und entwarf ein umfangreiches Entwicklungsprogramm, denn man musste ja die vielen herstellerspezifischen Systeme auf einer gemeinsamen Protokoll-Suite abbilden. Im Laufe der Zeit wurden beim DFN dann verschiedene Netzplattformen eingesetzt.

Schwarz auf weiß – Vertrag zur Errichtung und zum Betrieb des X.25 WiN: Am 7. September 1989 in Bonn unterschrieben Prof. Dr. Eike Jessen als Vorsitzender des DFN-Vereins (rechts), Friedrich Winkelhage als Stellvertretender Vorsitzender (Mitte) sowie der Bundesminister für Post und Telekommunikation, Dr. Christian Schwarz-Schilling (links).

Das Wissenschaftsnetz X.25 WiN, 1990 bis 1998 – der erste privatwirtschaftliche Dienstleistungsvertrag der DBP macht es möglich

Am 7. September 1989 schloss der DFN-Verein einen zehnjährigen Vertrag mit der Deutschen Bundespost (DBP) ab. Dieser war der erste privatwirtschaftliche Dienstleistungsvertrag der DBP. 1990 ging das erste deutsche Wissenschaftsnetz WiN in Betrieb – mehr als doppelt so leistungsfähig wie die stärksten damals in Deutschland angebotenen kommerziellen Netze.

Doppelt so leistungsfähig wie damalige kommerzielle Netze – das erste Wissenschaftsnetz WiN: Netzdarstellung aus den DFN-Mitteilungen Heft Nr. 37 - 3/95

WiN war ein X.25-basiertes VPN mit geplant 100 Anschlüssen je 9,6 kbit/s und 125 Anschlüssen je 64 kbit/s. Die spätere Aufstockung auf 1,92 Mbit/s wurde ab 1992 in Aussicht gestellt. X.25 definierte ein paketvermittelndes Netz zwischen Knotenrechnern mit virtuellen oder permanenten Verbindungen. Der Zugang der Endgeräte war in den Normen X.3/X.28/X.29 geregelt. Die über der Schicht 3 liegenden Protokolle (Transport und Anwendungen) mussten vom DFN bereitgestellt werden, als Dienste wurden Dialog, RJE, DFN-FT bzw. FTAM und X.400 angeboten. Die europäische Anbindung erfolgte über das X.25-Netz IXI ab 1990. Zu den USA wurde ab 1991 zunächst eine 64 kbit/s-Leitung errichtet. In die Zeit fällt auch die Gründung von RARE (1986) und von DANTE (1993), einem der Vorläufer des europäischen Wissenschaftsnetzes GÉANT. 1991 wurde WiN durch ERWiN erweitert, wodurch 51 Teilnehmer aus den neuen Bundesländern Zugang bekamen. Das WiN hatte 1993 einen Durchsatz von 120 GByte/Monat. Der X.25-Dienst endete am 31. Dezember 1998.

Das Breitbandwissenschaftsnetz B-WiN, 1996 bis 2000 – freie Fahrt auf der Autobahn der Wissenschaft

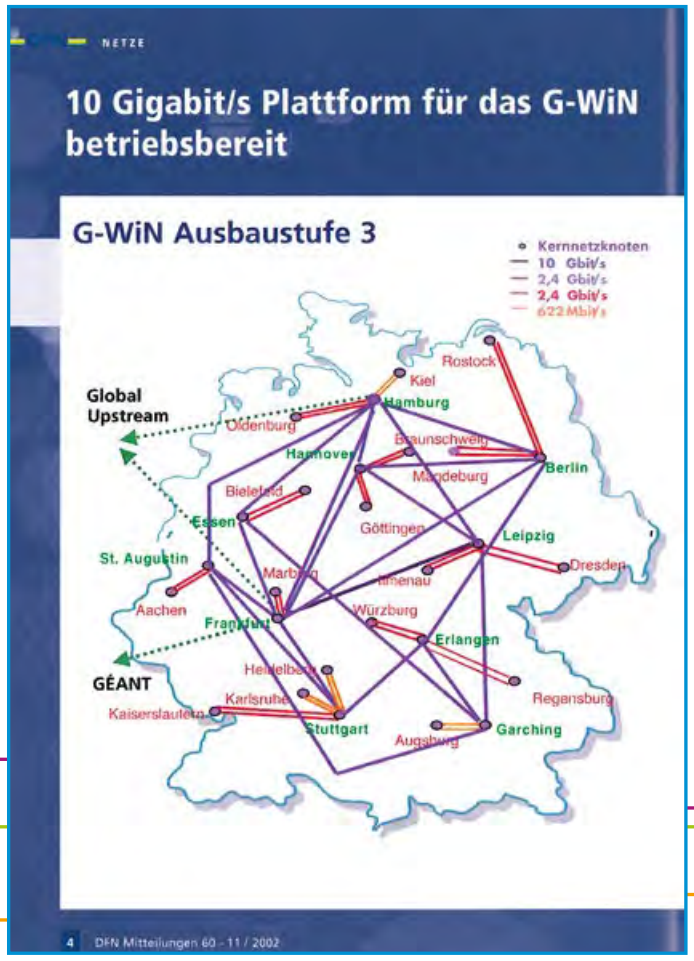
Es zeigte sich sehr schnell, dass die Übertragungsraten und -kapazitäten im WiN dem Bedarf der Wissenschaft nicht gerecht wurden. Ab 1992 kamen deshalb Überlegungen zu sich anbahnenden Hochgeschwindigkeitsdatennetzen (HDN) oberhalb 2 Mbit/s auf. Bei diesem Ansinnen verhielt sich die Telekom lange Zeit ausgesprochen zögerlich, da sich einige Herren aus der Monopolistenwelt des schmalbandigen Fernsprechdienstes nicht vorzustellen vermochten, dass es je ein so großes Datenkommunikationsaufkommen geben könnte, das solche hohen Bandbreiten

„Mega!" – Mit dem Breitband-Wissenschaftsnetz (B-WiN) wachsen die Netzkapazitäten zu Beginn auf 34 Mbit/s: Netzdarstellung aus den DFN-Mitteilungen Heft Nr. 41 - 6/96

rechtfertigt. Ich erinnere mich, dass ein bereits fixierter Termin mit dem DFN-Vorsitzenden vom Ministerium kurzfristig abgesagt wurde mit dem vertraulichen Hinweis, dass man einem anerkannten Wissenschaftler die Peinlichkeit eines offiziellen Ge-

sprächs über einen unseriösen Sachverhalt ersparen wolle. Doch die Technikentwicklung war rasant und die Entwicklung der Datennetze in den USA auch. Und bald wurde auch bei uns über WANs (34–155 Mbit/s) mit ATM/ SDH und MANs (DQDB und FDDI) diskutiert. Zu allen Optionen wurden bereits Testbeds eingerichtet.

Voraussetzung für die nächsten technischen Innovationssprünge und eine X-WiN-Plattform, wie wir sie heute kennen, war die Verleihung der Befugnis für die Wissenschaft, eigene Übertragungswege zu errichten und zu betreiben. Das Monopol hatte bis dato die Deutsche Bundespost. Am 4. September 1995 unterzeichnete der Vorstand des DFN-Vereins und der Vorstand der DeTeSystem Nürnberg, einer Tochter der Deutschen Telekom AG, in Bonn den Vertrag zur Errichtung, Betrieb und Management des Breitband-Wissenschaftsnetzes (B-WiN) mit zunächst 34 Mbit/s (ATM über SDH). Die Betriebsaufnahme erfolgte im März 1996 mit 50 Anschlüssen je 34 Mbit/s und drei Anschlüssen je 155 Mbit/s. Damit fanden die jahrelangen Bemühungen des DFN-Vereins, der Wissenschaft in Deutschland die dringend benötigten „schnellen" Datennetze zur Verfügung stellen zu können, ein positives



Raten bis 2,5 Gbit/s und ein IP-Dienst im Gigabit-Netz G-WiN: Darstellung aus den DFN-Mitteilungen Heft Nr. 60 - 11/2002

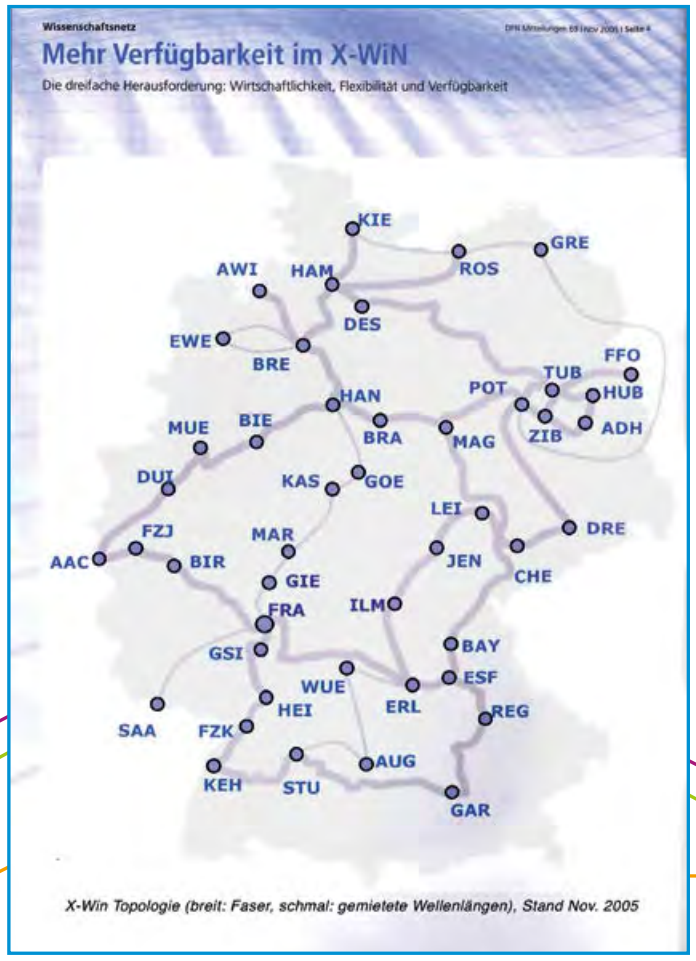
Ende. Mit dem B-WiN verfügte die Wissenschaft in Deutschland über eine Kommunikationsinfrastruktur, die verschiedenen Aspekten Rechnung trug: die Übertragungskapazität wurde dem exponentiell steigenden Wachstum gerecht; neue Dienste vor allem im Bereich der Multimedia-Kommunikation konnten entwickelt und eingesetzt werden; die Wissenschaftskommunikation in Deutschland hatte nun Anschluss an internationale Entwicklungen. 1997 gab es die erste 622-Mbit/s-Verbindung, und im Testbed schaffte man mit dieser Technik sogar den damaligen Weltrekord mit 2,5 Gbit/s. Mit dem B-WiN konnte der DFN-Verein endlich mit dem Leistungsstand der USA gleichziehen.

Das Gigabit-Netz G-WiN, 2001 bis 2005 – ATM ist nun überflüssig

Die Planung für einen B-WiN-Nachfolger begann 1998. Die ATM-Technik war zu komplex und die Flexibilität der ATM-Schicht wurde nicht wirklich gebraucht. Mittlerweile löste IP auch in Deutschland immer stärker die anderen Protokolle ab. Man strebte die Technik SDH über WDM an mit Raten bis 2,5 Gbit/s und darüber direkt dann den IP-Dienst. Die Ausschreibung für das G-WiN erfolgte 2000: Für 650 Zugangsleitungen wurden die Kosten für alle Bandbreiten abgefragt und damit das Kernnetz optimiert. Ab 1. Januar 2001 ging das G-WiN dann stufenweise und problemlos in Betrieb, es wurde Ende 2005 abgeschaltet.

Die Netzplattform X-WiN ab 2006 – neuartige Struktur im Baukastensystem

Damals tauchte folgende revolutionäre Idee neu auf, massiv vertreten durch den damaligen technischen Geschäftsführer Klaus Ullmann und den jetzigen Geschäftsführer Jochem Pattloch: Anstelle einer Netzausschreibung sollte ein Baukasten an technischen Optionen für eine Plattform entwickelt werden, um Dienste bedarfsgerecht gestalten zu können und so die gesamte Fertigungstiefe in der Hand zu haben. Ausgeschrieben wurden 2004 vier Lose (Fasern, Wellenlängen, Veredelung, Überwachung). Es wurden die Preise für alle Optionen und 70



Revolutionär und bedarfsgerecht – erstmalig mathematische Optimierung der Kernnetztopologie: Darstellung der Netzplattform X-WiN aus den DFN-Mitteilungen Heft Nr. 69 - 11/2005

Standorte in einer 70 x 70-Matrix abgefragt. Mit diesen Informationen erfolgten am ZIB eine mathematische Optimierung und die Berechnung der Kernnetztopologie nach Wirtschaftlichkeitskriterien. Es war das erste Mal, dass bei einem Netzentwurf die Planung nicht mit der Vorgabe von Kernnetzknoten begann. Diese Ausschreibung wurde in großer Transparenz durchgeführt. Sie war nicht nur wegen des strukturell neuartigen Ansatzes bemerkenswert, sondern auch wegen des Ergebnisses. Der unerwartete Gewinner eines Loses war eine Firma eines fernöstlichen Landes, was einen unterlegenen Anbieter veranlasste, wenn auch vergeblich, einen Prozess vor der Vergabekammer zu führen. Das bescherte damals dem DFN-Verein einen unfreiwilligen Besuch im Bundeskanzleramt, wo wir uns zu Sicherheitsbedenken zu äußern hatten.

Am 1. Januar 2006 starte das X-WiN ohne Probleme mit zunächst 47 Kernnetzknoten. Ethernet- und SDH-Schnittstellen wurden angeboten sowie ein VPN-Dienst. Das Fasernetz wurde laufend erweitert und die Topologie optimiert. 2012 erfolg-

DIENSTE

Die Kommunikationsdienste des DFN sind für die Zwecke von Wissenschaft und Forschung maßgeschneidert und werden in Abstimmung mit den Nutzern weiter entwickelt. Ziel ist es, diese möglichst gut in die informatorischen Prozesse der Hochschulen und Forschungseinrichtungen zu integrieren sowie die besonderen Anforderungen an die Dienstqualität zu berücksichtigen. Die Entstehung dieser Dienste hing einerseits von den Netzplattformen ab, andererseits spiegelten sie die Technologieentwicklung bei Geräten und Netzen wider und die sich daraus ergebenden Anwendungsmöglichkeiten und Einsatzszenarien.

Die folgende Liste gibt die aktuellen DFN-Dienste in der Reihenfolge der Betriebsaufnahme wieder:

- DFN-CERT (1993),
- DFNInternet(1994),
- DFN-PKI (1996),
- WiNShuttle (1995, Einstellung bis zum 31.12.2021),
- DFNFernsprechen (1998) und seit 2007 mit VoIP),
- DFNBackup (2001, eingestellt 2018),
- DFN-SAP (2001, Einstellung bis zum 31.12.2019),
- DFNconf (2001, neue Generation ab 2018),
- DFNRoaming/eduroam (2003),
- DFNNetNews (2003),
- DFN-VPN (2005),
- DFN-ListServ (2005),
- DFN-AAI (2007),
- DFNTerminplaner (2011),
- eduGAIN (2011),
- DFN-MailSupport (2011),
- DFN-Cloud (2014).

Neben den Netzplattformen mit der Internet-Konnektivität bieten vermutlich die Dienste DFNconf, DFN-AAI und eduroam einen besonderen Mehrwert für die Vielzahl von DFN-Mitgliedseinrichtungen und DFN-Nutzern. Mit eduroam ermöglicht DFN dem reisenden Wissenschaftler ohne zusätzliche Anmeldung weltweit den Zugang zum Wissenschaftsnetz. Der DFN-AAI stellt eine Authentifizierungs- und Authorisierungsinfrastruktur bereit, mittels derer die Verlässlichkeit von Kommunikationsbeziehungen zwischen mehreren Partnern sichergestellt wird.

te eine Erneuerung der Fasertopologie und der zugrunde liegenden DWDM-Technik. Die Netzverfügbarkeit wurde per Design durch Redundanzen auf mehreren Ebenen verbessert.

Von Menschen für Menschen

Ich komme nicht umhin, heute dankbar einige Namen zu nennen, die unmittelbar mit der Geburtstagsfeier unseres DFN-Vereins zu tun haben. Ich meine zunächst einmal die Personen, die von Anfang an dabei waren. Aus der DFN-Geschäftsstelle sind dies Gisela Maiß und Carola Schulz alias Domke. Herzlichen Dank für 35 Jahre Treue und gute Dienste in unserer Gemeinschaft. Wann immer ich mit der Geschäftsstelle zu tun hatte – einer bestens organisierten und hochgradig motivierten Truppe – bestach mich neben der Professionalität stets auch die freundliche Atmosphäre eines gut geführten Familienbetriebs. Nicht unschuldig an diesem Erscheinungsbild waren zwei Männer, die von der ersten Stunde an den Geist der Geschäftsstelle prägten: der administrative Geschäftsführer Dr. Klaus-Eckart Maass, der die ersten 20 DFN-Jahre bis zu seinem Ruhestand 2003 wirkte, und der international bestens vernetzte technische Geschäftsführer Klaus Ullmann, der im März 2011 an seinem Schreibtisch überraschend zusammenbrach und starb. Er war die technische Kapazität des deutschen Wissenschaftsnetzes und auch leitend bei RARE, DANTE und TERENA tätig beim Aufbau der europäischen Wissenschaftsnetze während mehrerer Generationen. Obwohl von der Sache her stets überzeugend und führungsstark, zeichnete beide Geschäftsführer eine gewisse Bescheidenheit aus. Sie gerierten sich mehr als primi inter pares denn als Chefs, eine Eigenschaft, die die beiden jetzigen Geschäftsführer Jochem Pattloch und Dr. Christian Grimm nach meiner Beobachtung in vorbildlicher Weise von ihren Vorgängern übernommen haben. Zurückblickend muss ich sagen, dass wir viele großartige Persönlichkeiten hatten, die das anfangs noch zarte Pflänzchen DFN hochgepäppelt, unterstützt und groß gemacht haben. Pars pro toto nenne ich für das BMFT Prof. Dr. Güntzsch, Dr. Rupf und Dr. Vogel, aus der Industrie Dr. Hultzsch (damals EDS, später Telekom-Vorstand) und den ersten DFN-Vorsitzenden Prof. Dr. Szyperski (Mannesmann Kienzle), aus der Gründerzeit noch die Kollegen Prof. Dr. Zander (HMI Berlin) und Prof. Dr. Dr. Fischer-Appelt (Universität Hamburg). Wir hatten stets großes Glück bei der Besetzung der bislang dreizehn Verwaltungsräte und auch bei der Besetzung der Vorstandspositionen, wobei Prof. Dr. Jessen mit fünf Amtsperioden den Vogel abschoss. Seit 2011 hatten wir mit der Kanzlerin der TU Berlin, Prof. Dr. Gutheil, die erste Dame in der Vorstandsriege. Doch damit will ich es genug sein lassen.

Aus meinem persönlichen Rückblick auf 35 Jahre DFN – im zwischenmenschlichen Bereich würde man vielleicht auch von einer Liebeserklärung sprechen – ist eine Werbeveranstaltung für den DFN-Verein geworden. Das entspricht auch meiner Überzeugung: Die Quantität und Qualität der durch den DFN in den (nur) 35 Jahren geschaffenen technischen und fachlichen Kommunikationsmöglichkeiten und des dazugehörigen Anwendungs- und Nutzungsumfelds sind beachtenswert. Dabei wurde in der Vergangenheit des DFN ganz offensichtlich dem Leitspruch des Dominikaners Père Henri Didon (1840–1900), des Priors des Collège d'Arcueil, gefolgt. Der Leitspruch lautete: „Citius, altius, fortius, melius", also „schneller, höher, stärker, besser", was ja bekanntlich auch zum Motto der neuzeitlichen Olympischen Spiele wurde. Damit sind wir seit Jahren auf Augenhöhe mit den fortschrittlichsten Nationen – wenn es den DFN-Verein nicht schon gäbe, man müsste ihn erfinden!

Ich schließe mit dem Wunsch: Lieber DFN-Verein, vivas, crescas, floreas ad multos felicesque annos! ◆

Der Netzpionier – als der DFN-Verein laufen lernte

Aufregend muss es in den Pionierzeiten des DFN-Vereins gewesen sein. Am 12. Januar 1984 wurde der Verein zur Förderung eines Deutschen Forschungsnetzes e. V. als Selbsthilfeorganisation der Wissenschaft gegründet. Dass das Netz damals seinen Kinderschuhen entwachsen ist, rasch auf Augenhöhe mit den internationalen Spitzennetzen konkurrieren konnte und heute zu den leistungsfähigsten Forschungsnetzen weltweit gehört, daran hat Prof. Dr. Heinz-Gerd Hegering einen entscheidenden Anteil. Erfahren im Umgang mit Notfällen und Katastrophen war er als Kommandant der Freiwilligen Feuerwehr Garching bei München ohnehin. Und auch beim DFN-Verein löschte er so manchen Brandherd und scheute sich nicht, seine Kolleginnen und Kollegen zur Räson zu rufen und Tacheles zu reden, wenn es nötig war. „Hart aber herzlich" trug er dazu bei, den DFN-Verein auf Erfolgskurs zu halten.

Steuerte den DFN-Verein auch in unruhigen Zeiten: Prof. Dr. Heinz-Gerd Hegering *(Foto © Privatarchiv)*

35 Jahre DFN: Welche Erinnerungen kommen Ihnen da spontan in den Sinn?

Neben der rasanten Technikentwicklung auf dem Gebiet der Kommunikation mitsamt ihren gesellschaftspolitischen und prozessrelevanten Auswirkungen sind es zuallererst die Menschen im DFN, an die ich mich erinnere. In seinen nur 35 Jahren hat der DFN sehr viel erlebt und bewirkt dank der Visionen einiger früher Vordenker, die bereits Anfang der 1980er Jahre über die gerade aufkommenden technischen Möglichkeiten einer rechner- und netzgestützten Datenkommunikation nachdachten, aber auch dank vieler großartiger Menschen, die an diese Visionen glaubten, sie mutig aufgriffen und auch umsetzten gegen viele anfängliche Widerstände. Damit legten sie die Basis für die selbstbestimmte Solidargemeinschaft „Verein zur Förderung eines Deutschen Forschungsnetzes". Einer von ihnen ist Eike Jessen, mein Münchner Kollege, der leider am 18. März 2015 verstarb, nachdem er über 30 Jahre Motor und Seele des DFN gewesen ist. Seit der ersten Stunde unseres Vereins lag ihm dessen Geschick sehr am Herzen. Er bekleidete nicht ohne Grund am längsten und am häufigsten Vorstandspositionen im DFN-Verein. Neben seiner hohen technischen Kompetenz und strukturierten Herangehensweise zur Zielerreichung, bestach er vor allem durch sein Geschick bei Konfliktlösungen – sowie einer Beharrlichkeit, der wir Kollegen uns kaum entziehen konnten.

> „Es sind zuallererst die Menschen im DFN, an die ich mich erinnere"

Das klingt ja fast so, als hätten Sie es zumindest mal versucht – sich zu entziehen.

Hiermit bekenne ich öffentlich: 1998 reisten wir mit einer kleinen DFN-Delegation nach Washington. Thema war die Kofinanzierung der USA-Verbindung. Als wir nach zwölfstündigem Verhandlungsmarathon bei der National Science Foundation (NSF), dem United States Department of Energy (DoE) sowie in

einem Büro des Weißen Hauses am späten Abend von Herrn Jessen nochmals zu einer Nachtsitzung und zu einem Brainstorming aufgefordert wurden, da gingen Herr Dr. Vogel vom BMBF und ich nicht etwa versehentlich im Verkehrsdschungel der US-Metropole verloren, sondern wir hatten uns unbemerkt und vorsätzlich abgesetzt, um ein DFN-freies Bier in Georgetown zu trinken. Aber als Katholik weiß ich natürlich, dass mir diese Sünde nie vergeben werden kann – denn ich bereue sie nicht.

Was waren rückblickend bedeutende Meilensteine für den DFN?

Ein bedeutender Schritt für den DFN war sicherlich die „Verleihung", also die Befugnis oder das Recht für die Wissenschaft selber Weitverkehrsleitungen zu errichten und zu betreiben. Bis dahin bestand das ausschließliche Recht nur für den Monopolisten Deutsche Bundespost. Das erste DFN-Netz, das X.25-WiN, entstand noch unter der Federführung der Deutschen Bundespost Telekom mit anfänglich 64 kbit/s – für die Wissenschaft lächerlich wenig. Zur selben Zeit hatte der DFN entschieden, einen IP-Knoten einzurichten und entschied sich damit gegen die OSI-Protokolle. Der DFN-Verein beantragte 1994 die Verleihung und scheute sich auch nicht, das Bundeskanzleramt dazu einzuschalten. Tatsächlich gab es dann im Juli 1995 eine gemeinsame Presseerklärung der Bundesminister Dr. Jürgen Rüttgers (Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, BMBF) und Dr. Wolfgang Bötsch (Bundesministerium für Post und Telekommunikation, BMPT) mit der Überschrift „ Freie Fahrt auf der Autobahn der Wissenschaft", in der die Verleihung angekündigt wurde und auch eine Anschubfinanzierung von 80 Millionen DM zum beschleunigten Aufbau eines 155 Mbit/s-Netzes außerhalb des Tarifgefüges der Telekom AG. Das war die Geburtsstunde des eigenen DFN-Netzes. Zuvor hatte der DFN jedoch eine Menge Überzeugungsarbeit zu leisten gehabt. Natürlich war das eine politische Entscheidung auf höchster Ebene, um die Liberalisierung voranzutreiben. Und das hat funktioniert.

> „Das war die Geburtsstunde des eigenen DFN-Netzes"

Das BMBF und das BMPT hatten also einen großen Anteil an den Geschicken des DFN. Nicht zuletzt auch durch die Mitfinanzierung des BMBF.

In den Anfangsjahren erhielt der DFN eine Anschubfinanzierung vom Bund zur Planung und zum Aufbau einer Netzinfrastruktur. Man kann sagen, das damalige BMFT schenkte dem jungen DFN ein eigenes, selbstverantwortliches Fördermodell. Der DFN finanzierte sich schon damals zum Teil aus den Entgelten und Mitgliedsbeiträgen. Die sogenannte Fehlbedarfsfinanzierung vom Bund diente bis 2004 dazu, bei Bedarf einen finanziellen Ausgleich zu schaffen, etwa für die Investitionsbeschaffung der nächsten Generation des Wissenschaftsnetzes – jeder Innovationssprung kostete natürlich Geld – oder für das mit dem Bundesministerium abgestimmte Rahmenprogramm. In den ersten 20 Jahren bekam der DFN-Verein nicht nur Zuwendungen für den Netzaufbau und -betrieb, sondern auch für Forschungs- und Entwicklungsprojekte. Damit war der DFN nicht nur Zuwendungsempfänger, sondern auch Projektträger. Ein Vorteil für den Verein, denn die Projekte waren maßgeschneidert für die DFN-Bedarfe. Dazu gehörten unter anderen Themen wie Breitband-Infrastrukturen, betriebsunterstützende Dienste, Netzmanagement, Unterstützung und Gewährleistung sicherer Netzdienste, Verfügbarkeit und Dienstqualität oder aber Rechtsrahmen für IT-Dienste.

Wie kam es zehn Jahre später zur Beendigung der Mitfinanzierung?

Der DFN-Verein hatte laufen gelernt, er war selbstbewusst und wollte seine eigenen Entscheidungen treffen. Tatsache war, dass ab 2004 die Fehlbedarfsfinanzierung vom Bund aufgekündigt wurde und damit etwa zehn Prozent im Budget des DFN-Vereins fehlten. Die große Frage war, wie das ausgeglichen werden sollte.

Wie wirkte sich das auf den DFN-Verein aus? Kann man hier auch von Emanzipierungsbestrebungen des DFN sprechen?

Unbedingt – sowohl extern als auch intern. Wir hatten zu der Zeit eine stark heterogene Mitgliederstruktur, darunter FHs und Unis, Großforschungseinrichtungen und Industrieforschung. Unsere Mitgliederzahl war seit der Gründung 1984 von elf auf fast 400 Mitglieder (Stand: 1999) gestiegen, nicht zuletzt durch den Beitritt der Wissenschaftseinrichtungen der ehemaligen DDR 1991 gab es einen ordentlichen Schub. Wir verstanden uns als Selbsthilfeorganisation der Wissenschaft und als Interessensvertretung gegenüber staatlichen Einrichtungen, nationalen und internationalen Organisationen und Herstellern sowie Dienstleistungsanbietern. Es gab eine Reihe von Themen, die den Verein viele Jahre, und zwar teils sehr emotional und kontrovers, beschäftigten. Ein Thema jedoch erwies sich als Dauerbrenner und war ein Diskussionsfass ohne Boden – die Entgeltstruktur für die Mitgliedschaft und für die Nutzung von Netzplattformen und Diensten, insbesondere nachdem die Finanzierung des Bundes wegfiel. Da ging es arm versus reich, klein gegen groß, Umlageverfahren gegen Nutzungsorientierung, Einzelanschlüsse

> „Wir verstanden uns als Selbsthilfeorganisation der Wissenschaft"

„Bad Cop“ und „good Cop“ oder Yin und Yang: Prof. Dr. Heinz-Gerd Hegering und Prof. Dr. Eike Jessen ergänzten sich im Vorstand hervorragend.

versus Gemeinschaftsanschlüsse, um nur einige Kontroversen zu nennen. All das bot ja genügend Zündstoff und Versuchung und betraf auch die Frage der Integration oder Unabhängigkeit von Regionalanbietern oder Ländernetzen. BelWü in Baden-Württemberg war hier lange Zeit ein heißes Eisen, aber auch zeitweise NRW oder Rheinland-Pfalz. Auch der Versuch, Wissenschaftsnetze in das enge Korsett von Verwaltungsnetzen zu zwingen, hat uns zeitweise beschäftigt, sogar im sonst so vorbildlichen Bayern. Es gab immer Mitmenschen, die es einem nicht so leicht machten, seinem DFN-Enthusiasmus ungebremst zu folgen, die vorgetragene Vorschläge sehr (manchmal zu) kritisch hinterfragten und denen es gelegentlich nicht leicht fiel, den Begriff Solidargemeinschaft mit Leben zu füllen.

Jetzt machen Sie mich aber neugierig.

Ich werde hierzu natürlich keine Namen nennen, aber durch ein intensives Studium der MV-Protokolle lässt sich diese Kandidatenmenge leicht eingrenzen. Auch dieser Gruppe bin ich heute persönlich sehr dankbar, weil sie mir nachhaltig Gelegenheit gegeben hat, an meiner Geduld, Toleranz, Kritikfähigkeit, aber auch der Überredungs- bzw. Überzeugungskunst zu arbeiten.

Alles Eigenschaften, die Sie offensichtlich gut gebrauchen konnten als Vorstandsmitglied.

Die lokalen und regionalen Planungen bargen natürlich die latente Gefahr von Abwanderungstendenzen. Dies führte in der Folge zu einer verstärkten Reisediplomatie von uns Vorstandskollegen, um besonders abwanderungs¬gefährdete DFN-Mitglieder bei der Stange zu halten. Bei den vielen Besuchen bei Länderreferenten, Ministern und Hochschulrektoren konnte ein Vorstandsduo durchaus gekonnt gelegentlich die aus Fernseh-Krimis bekannte Vorgehensmethodik „good guy – bad guy“ einsetzen, wobei ich es jetzt der geschätzten Leserschaft überlasse, über die Rollenverteilung zu spekulieren (Anmerkung der Redaktion: alles andere als die Rolle des „good guy“ ist bei Herrn Prof. Hegering schwerlich vorstellbar). Diese insgesamt komplexe Gesamtthematik führte oft zu sehr hitzigen Auseinandersetzungen in den MVs, die manchmal fast an die Gürtellinie gingen. Ein noch harmloses Beispiel ist folgende Protokollnotiz: „Herr X hält es für sehr problematisch, dass mit der Einrichtung Y ein Gemeinschaftsanschluss besteht, deren Vertreter ein Mitglied des Vorstandes des DFN ist, und dass sogar der Vorstandsvorsitzende zu einer der nutzenden Einrichtungen zählt …“

Trotz der leidenschaftlichen Auseinandersetzungen schienen die gemeinsamen Interessen letztendlich im Vordergrund zu stehen.

Ein Begriff, der in den Diskussionen oft strapaziert wurde, allerdings oft auch mit Erfolg, war der der Solidargemeinschaft, bei dem häufig die größeren Einrichtungen nachgaben, obwohl es bekannt war, dass die höheren Leistungskategorien im Netz ohnehin einen relativ weit höheren Kostendeckungsbeitrag aufbrachten. Die konkret resultierende Entgeltstruktur und die dabei angewandten Kriterien änderten sich häufig im Laufe der Zeit, abhängig von der Technik der Netzplattformen, von deren Anbietern, von der Marktkonkurrenz, von der Zuwendungsstruktur oder der aktuellen Mitgliederstruktur. Es war wichtig, dem DFN-Verein ein institutionelles Selbstverständnis und Selbstwertgefühl zu geben, das den Mitgliedern insbesondere während des höchst schwierigen Umbaus des Vereins in Richtung einer selbstbestimmten und selbstfinanzierten Zukunft die Zuversicht gab, auch große Vorhaben stemmen zu können.

„Wichtig waren ein institutionelles Selbstverständnis und Selbstwertgefühl“

Auch aktuell wird dieses Thema wieder intensiv diskutiert. Unabhängig von der bereits beschlossenen Anpassung der Höhe der Entgelte ab dem Jahr 2020 erteilten die Mitglieder dem Vorstand den Auftrag, auch die Gestaltung der Regelungen des Entgeltmodells zu prüfen. Ich sage ja, ein Dauerbrenner. ◆

Auf ein Wort: Perspektiven und Chancen für den DFN-Verein

Mögliche Antworten auf die Fragen, ob der DFN-Verein noch zeitgemäß ist oder ob es strategisch besser ist, sich entweder auf das Netz oder die Dienste zu konzentrieren, fallen wohl so vielfältig aus wie die Zusammensetzung seiner Mitglieder und Teilnehmer. So unterschiedlich die Interessen und Schwerpunkte auch sein mögen, das Prinzip der Solidargemeinschaft und damit das gegenseitige Vertrauen dürfen als Basis nicht aus der Mode kommen. Hans-Joachim Bungartz, seit 2011 Vorstandsvorsitzender des DFN-Vereins, hat dazu und zur zukünftigen Entwicklung des DFN-Vereins einen ganz klaren Standpunkt.

Text: **Hans-Joachim Bungartz** (Vorstandsvorsitzender im DFN-Verein)

35 Jahre sind eine lange Zeit in einem IT-Hochtechnologiebereich. Und so muss sich der DFN-Verein natürlich die bzw. der Frage stellen, ob die eigene Verfasstheit, das Betreiben eines eigenen Netzes für die Wissenschaft, das über die Jahre gewachsene und stetig erweiterte Portfolio an Diensten, das – momentan ja auf dem Prüfstand stehende – Entgeltmodell, eines der großen Vereinsthemen dieses Jahres, bis hin zu den – im vergangenen Sommer bekanntlich erneuerten – Preisschildern noch zeitgemäß sind. Beide letztgenannten Aspekte haben offenkundig mit Geld zu tun und oft wird die Debatte auch primär ums Geld geführt. Doch das Nachdenken muss weitergreifen, es muss uns schließlich bis hin zu der Kernfrage führen, ob der DFN-Verein insgesamt noch zeitgemäß ist. Denn was vor 35 Jahren aus einem bestimmten technologischen, wirtschaftlichen und wissenschaftspolitischen Kontext heraus ins Leben gerufen wurde und sich seitdem prächtig entwickelt hat, muss ja nicht zwangsläufig heute oder in Zukunft immer noch die bestmögliche Antwort auf die Bedarfe der Wissenschaftslandschaft in Deutschland sein. Nicht oft, auch nicht immer öfter, aber dann und wann tritt tatsächlich jemand an uns mit diesen Fragen heran: „Habt ihr die Grundsatzfrage auf dem Radar, und habt ihr eine Antwort?“ Und deshalb an dieser Stelle ein überzeugtes zweifaches „Ja!“ – Ja, wir stellen uns diese Frage im Vorstand, in der Geschäftsführung immer und immer wieder, wir haben

Findet Antworten auf wichtige Fragen: Prof. Dr. Hans-Joachim Bungartz *(Foto © Maimona Id/DFN)*

nicht das Selbstverständnis von Lordsiegelbewahrern und wir drehen auch durchaus an Stellschrauben; und ja, bisher können zumindest wir nicht erkennen, dass irgendetwas fundamental falsch liefe oder dass sich an den Randbedingungen etwas so fundamental geändert hätte, dass Teile oder das Ganze des DFN-Vereins obsolet geworden wären. Das zweimalige „Ja!" mag nicht überraschen, aber es ist das aktuell abgerufene Ergebnis eines kontinuierlich ablaufenden Denkprozesses – kein stereotyper Automatismus.

Ja zum Wir – das Prinzip Solidargemeinschaft

Zunächst nochmals kurz zum Geld, dann wird das – zumindest in diesem Beitrag – kein Thema mehr sein. Wer sachlich und verantwortungsvoll auf die Beträge in den Entgelttabellen des Vereins schaut (auch in der 2018 angepassten und ab 2020 geltenden Form) und dabei erstens die heutige Bedeutung der Vernetzung für die Wissenschaftseinrichtungen, zweitens die Mehrwerte durch das Wissenschaftsnetz sowie die damit verbundenen Dienste und drittens die Relationen zu den Gesamtbudgets der Einrichtungen im Blick hat, der kann eigentlich nicht fundamental ins Zweifeln kommen. Und so höre ich es auch immer wieder bestätigend, in Gesprächen mit Vertreterinnen und Vertretern der Leitungsebene unserer Mitgliedseinrichtungen. Natürlich kann man immer optimieren, an der Verteilung schrauben, hier oder da eine Einsparung erzielen; nein, man kann nicht nur, man muss sogar, und wir tun das selbstverständlich auch, zum Beispiel, indem der Automatisierungsgrad beim Betrieb der Dienste weiter erhöht wird. Zu diesem Zweck wird aktuell die Einführung eines DFN-Self-Service-Portals forciert, auf der Betriebstagung im kommenden Herbst soll der Prototyp dafür vorgestellt werden. Die Ausgabenseite ist also fest im Blick. Aber ein Mehr an Funktionalität und Qualität hat eben seinen Preis. Argumente wie „Im IT-Bereich wird doch eigentlich alles billiger." sind zwar schnell gesagt und finden auch ihr Publikum, im Grunde tun sie aber nur eins – sie diskreditieren diejenigen, die sie gebrauchen. Ein kurzer Blick auf die Entwicklung von IT-Budgets reicht. Der Umgang mit dem Argument „Ich habe viel günstigere Alternativen." erscheint auf den ersten Blick diffiziler, ist es aber im Grunde gar nicht. Denn wo das Annehmen eines solchen Angebots dem Einzelnen hilft und die Solidargemeinschaft nicht über Gebühr belastet – kein Problem! Der DFN-Verein hat und will kein Monopol. Wo die Sache allerdings heftig auf Kosten der anderen geht und das „cherry picking" ausufert oder auszuufern droht, geht's halt nicht – ich kann auch nicht eigenmächtig weniger Steuern zahlen, bloß weil ich das eine oder andere Trottoir nicht nutze. Das ist das Prinzip einer Solidargemeinschaft, die natürlich immer wieder auf dem Prüfstand stand, wie ja auch Heinz-Gerd Hegering in seinem Beitrag treffend artikuliert. Die Gemeinschaft hat sich aber aus mehr als guten Gründen immer wieder für den Erhalt dieses Prinzips ausgesprochen. Und das bedeutet nun mal, dass keiner und keine das „Ich kann aber billiger" zum alleinigen Motto für das eigene Handeln ausrufen darf; zumindest nicht, solange man Teil der Gemeinschaft bleiben will.

„Was habe ich von der Kohle, wenn ich im Off sitze?"

Mir stellt sich in diesem pekuniären Kontext noch eine ganz andere Frage: Sind besagte Angebote wirklich günstiger oder preiswerter oder sind sie einfach nur billiger? Zwei Aspekte bzw. Beispiele hierzu, erstens: Zum einen vernehme ich wiederholt von einer Mitgliedseinrichtung am Ort A, dass der Anbieter X immer attraktivere Angebote in Sachen Bandbreite mache; jüngst nochmals ein deutlicher Nachlass. Davor könne man die Augen eigentlich nicht mehr verschließen. Zum anderen erlebe ich es aber hautnah, wie jener Anbieter X seit nunmehr über anderthalb Jahren größte Probleme hat, seine in Angeboten und Verträgen dem DFN-Verein gegenüber zugesicherten Verpflichtungen in Sachen Teilnehmeranbindung und Leistungssteigerung zu erfüllen bzw. dies in Teilen klar nicht geschafft hat. Natürlich gibt es Instrumente, wie Konventionalstrafen, aber was habe ich von der Kohle, wenn ich im Off sitze (abgesehen davon, dass man vielleicht den einen oder anderen Controller damit beglücken kann, dass man toll was gespart habe)? Das relativiert die angeblich so attraktiven Angebote dann schon etwas. Zweitens: Am Ort B übernimmt schon seit langer Zeit Anbieter Y die Versorgung. Und so wurde ich vom Vertreter einer Mitgliedseinrichtung dort gerade jüngst ziemlich heftig bearbeitet, der Verein möge doch bitte nicht irgendwelche „Zwangskategorien" einführen, man sei vor Ort nun mal anderweitig bestens mit Bandbreite versorgt. Kurze Zeit später erfahre ich dann, dass eben dieser Anbieter Y bei GÉANT wegen direkter Konnektivität angefragt hat. Das gibt einem schon zu denken. Man kann jetzt verschiedener Meinung sein, ob das ein Eingeständnis von Unvermögen, ein bisschen unverschämt oder einfach nur grenzenlos blöd ist – für Qualität und Nachhaltigkeit der Dienstleistungen des Anbieters Y spricht es jedoch in keinem Fall. Nein, also ich würde mich nicht in die Hände von X oder Y begeben. Aber das sind jetzt lediglich zwei Snapshots, die keinesfalls repräsentativ sein müssen.

Mit gutem Beispiel voran – Mut zum Diskurs und zur Selbstreflexion

Aber nun zum Nicht-Monetären, zu der eingangs formulierten Frage: „Passt das alles noch?". Die Verfasstheit des DFN-Vereins ist

schon ganz gut und alles andere als nicht mehr zeitgemäß. Und sie gilt anderswo durchaus als beispielhaft oder als „Best Practice“, wie man neudeutsch sagt. Bei der Neuaufstellung von HIS beispielsweise wurden externe Berater engagiert und diese Berater ließen sich dann ihrerseits vom DFN-Verein beraten. Sie ließen sich vor allem deshalb vom DFN-Verein beraten, weil der überall als Musterbeispiel in Sachen Selbstorganisation in der Wissenschaft anerkannt ist. Und auch wenn für „HIS 2.0“ am Ende nicht der Weg eines Vereins, sondern der einer Genossenschaft gewählt wurde, so ist doch nicht zu verkennen, dass der DFN-Verein sehr genau angeschaut wurde. Oder als für die Implementierungsphase des Nationalen Hochleistungsrechnens – NHR – operative Unterstützung gesucht wurde, wandte sich die Politik an den DFN-Verein. So schlecht kann das alles also nicht sein. Aber die Verfasstheit als Verein erfordert eben von den Mitgliedern auch ein aktives Sich-Einbringen, ein Agieren als Vereinsmitglieder. Ja, das „Verein-Sein“ kann anstrengend sein. Alle sind gefordert, alle bestimmen mit, aber alle müssen auch irgendwie mitziehen.

Dann die Frage nach dem eigenen Netz: Für die Gegenwart und die nahe Zukunft ist die ganz klar positiv zu beantworten. Ob das immer so bleiben wird, ist dagegen offen. Da muss man selbstredend immer wieder darauf schauen; und wenn's

„Wir sind der Verein“

anders besser geht, machen wir's anders. Und wie das halt so ist: Während der eine hinterfragt, ob das Betreiben des Netzes noch sinnvoll sei und sich der Verein nicht lieber auf die Dienste konzentrieren solle, stellt die andere ein „Schuster, bleib bei deinen Leisten!“ in den Raum. Will sagen: Warum macht ihr immer mehr Dienste und konzentriert euch nicht einfach auf euer Kerngeschäft, das Netz? Wobei die zweite Person, „ihr“, hier mit Bedacht gewählt ist, denn hierin liegt schon ein erster Fehler. Es ist eben nicht: „Hier ich, dort ihr, der Verein – das anonyme System, die ominöse Matrix“, sondern: „Wir sind der Verein.“ Wenn die Mitgliedschaft einen Dienst will – ob nun Bottom-up-initiiert oder auf Vorschlag der Vereinsleitung – und beschließt, dann kommt der. Und sonst kommt er eben nicht. Und somit ist die Einheit aus Netz und Diensten nicht notwendig etwas für die Ewigkeit; aber für den Augenblick schon.

„Verbundaktivitäten lösen das alleinige Werkeln ab“

„Wo geht's hin?“ – Lust auf kommende Herausforderungen, Spaß an neuen Aufgaben

Doch jetzt noch ein paar Gedanken zu „Wo geht's hin?“ Auf einen Nenner gebracht: Das mit dem Schuster und den Leisten wird kaum zu schaffen sein. Denn die Komplexität und die Vielfalt werden weiter zunehmen.

Erstens: die Internationalisierung – Europa wird immer mehr zum Heimstadion, der Übergang zu GÉANT verkörpert keine wirkliche Außenanbindung mehr, sondern ist eher Binnenanbindung. Was sich aktuell auf der europäischen Bühne im Hinblick auf die Vorbereitungen des neunten Rahmenprogramms tut, sei es nun unter dem Dach von EDI (European Data Infrastructure) oder EOSC (European Open Science Cloud), wird unmittelbare Auswirkungen auf Anforderungen, Nutzer und Nutzungsarten des Netzes haben. Mit den Vergabeverfahren auf europäischer Ebene, wie es im Rahmen des GÉANT-IaaS-Vergabeverfahrens erstmals im größeren Stil erprobt wurde, werden die Partizipationsmöglichkeiten an verschiedensten Clouds für einzelne Einrichtungen vielfältiger, aber eben auch komplizierter werden. Internationale Großexperimente und Großprojekte sowie die Pläne zum Exascale-Computing werden über ihre singulären Bedarfe die Netzlandschaft prägen.

Und auch hier ist die Liste länger und bunter geworden und sie enthält neben dem üblichen Allzeitverdächtigen CERN/LHC inzwischen etliche weitere Einträge, wie z. B. SKA, ITER, EuroHPC oder Copernicus. Der Siegeszug von eduroam setzt sich fort, und eine „Edu-ID“ wird erprobt. All das kann nur gelingen mit einem leistungsfähigen Netz samt passendem Angebot an Mehrwertdiensten, national geplant und umgesetzt und international abgestimmt.

Zweitens: die Kollaborationen – Lokale oder regionale Versorgungsverbünde, standortweite und institutionenübergreifende Konzepte, ortsübergreifende Strategien innerhalb von Wissenschaftsgemeinschaften, Exzellenzcluster und Zukunftskonzepte im Rahmen der Exzellenzstrategie, sektorenübergreifende lokale Zusammenarbeit (z. B. mit Start-ups in Technologieparks oder mit der industriellen Forschung im Rahmen von On-campus-Konzepten), etc. etc. Wieder so eine Auflistung, die alles andere als vollständig ist und die sich beinahe beliebig ergänzen ließe. Immer mehr lösen Verbundaktivitäten das alleinige Werkeln ab, sei es nun aus fachlichen oder aus primär strategischen Gründen. Für den DFN-Verein heißt das zunächst, dass dies alles technisch unterstützt werden muss. Dann kommen aber auch formale Fragen auf, die sich vor zehn oder zwanzig Jahren vielleicht noch nicht oder noch nicht in dieser Heftigkeit gestellt haben: Wer darf und wer darf nicht? Oder konkret: Wie lange ist ein Spin-off einer universitären Arbeitsgruppe noch irgendwie „Uni“ und ab wann ist er dann „Industrie“? Wie sind Konditionen zu definieren, und wie kann man das alles in transparente Regeln fassen? Auch dies ein Aspekt, der aktuell im Rahmen der Diskussionen um das Ent-

geltmodell virulent geworden ist – und mit dem Universitäten, Hochschulen und andere Wissenschaftseinrichtungen ja keinesfalls nur beim Netz konfrontiert sind. Auch hier muss die Devise sein: ermöglichen, nicht verhindern; Flexibilität so lange zulassen, wie sie die Allgemeinheit im Verein nicht über Gebühr strapaziert.

Drittens: nationale Infrastrukturen – Lange waren Infrastrukturen ja nicht gerade en vogue, oft galt das die Wissenschaft Unterstützende nicht wirklich als zur Wissenschaft gehörig. Noch beim 91b-Verfahren im Rahmen der Forschungsbauten- und Großgeräteförderung für die Forschung musste jeder Großrechnerantrag immer auch gegen den Generalverdacht der „Infrastruktur" ankämpfen: „Das nutzen ja mehrere Wissenschaftsdomänen, da fehlt ja die kohärente Programmatik, das ist ja Infrastruktur" – igitt sozusagen. Die erste Abhilfe war bekanntlich die Einführung der Programmatisch-strukturellen Linie „HPC" und tatsächlich wurde manches besser, aber nicht alles. Aber nun der Doppelschlag – das Hochleistungsrechnen wird als Nationale Infrastruktur (NHR, s. o.) eingeführt und die Nationale Forschungsdateninfrastruktur (NFDI) trägt das ehemals stigmatisierende „I" sogar im Namen. Nun sind weder HPC noch Forschungsdaten per se „Netz", aber ebenso klar ist, dass beide unmittelbar mit dem Netz zu tun haben, ja, das Netz existenziell brauchen. Beim HPC hat das ja schon Tradition, doch aktuell ist es sichtbar wie selten zuvor. EuroHPC definiert Anforderungen an das europäische Netz und umgekehrt wird GÉANT nach aktueller Planung nicht unerhebliche Mittel über EuroHPC beziehen. In Deutschland hat das Gauß-Zentrum, quasi in Vorbereitung der Exascale-Aktivitäten, die Konnektivität der drei Standorte Stuttgart, Jülich und Garching untereinander ausgebaut. Und NHR soll ja eine verteilte Kompetenz- und Kapazitäteninfrastruktur werden, keinesfalls eine Menge quasi baugleicher Generalversorger – was ebenfalls eine spürbare Zunahme an Netzverkehr bedeuten wird. Auch wenn im NFDI-Dunstkreis noch an erstaunlich vielen Stellen zu hören ist: „Wieso, das Netz ist doch da?", werden der Datenfokus insgesamt wie die Systematisierung, Nutzbarmachung und Nutzung des rasant wachsenden Schatzes an Forschungsdaten ein signifikantes Mehr an Netzverkehr mit sich bringen. Schon über die letzten Jahre – darüber wurde und wird ja regelmäßig berichtet – ist ein durchschnittliches Wachstum des integrierten Datenvolumens von ca. 30 Prozent pro Jahr zu beobachten. Weniger wird das nicht werden. Und es geht ja nicht nur um die Bandbreite: Die sich gerade findenden und konstituierenden NFDI-Konsortien werden auch Dienste wie AAI etc. benötigen. Insgesamt spricht viel dafür, dass diese mit einer gewissen Institutionalisierung einhergehenden Infrastrukturen zu einem weiteren Zusammenrücken führen werden – auch, aber keinesfalls nur in Netzhinsicht. Der DFN-Verein steht diesen strukturbildenden Entwicklungen offen gegenüber, gestaltet den Prozess im Falle NHR ja sogar aktiv mit. Dies bedeutet aber keinesfalls eine Verwässerung der Identität, eine zu weite Abkehr des Schusters von seinen Leisten also. Der DFN-Verein will weder HPC-Versorger noch NHR-Verein werden. Von den anderen kann (und will vermutlich) aber auch niemand den DFN-Verein geben.

„Das ist ja Infrastruktur, igitt"

„Maßgeschneidert, nicht von der Stange – das Wissenschaftsnetz"

Viertens: Sicherheit – Auch hier besteht ein nicht zu leugnender Bedarf an Mehr – nicht zuletzt, weil immer mehr digital wird und somit digital geschützt werden muss, aber auch aufgrund rechtlicher Rahmenbedingungen wie der DSGVO (Datenschutz-Grundverordnung), dem TKG (Telekommunikationsgesetz) oder der Richtlinien für Kritische Infrastrukturen. Und so wird uns die strategische Weiterentwicklung der Sicherheits- und CERT-Dienste im DFN-Verein weiter beschäftigen – mit dem Primärinteresse des Schutzes unserer eigenen Infrastruktur, aber dann durchaus auch mit der Perspektive weiterer Angebote für die DFN-Teilnehmer. Security Operations ist das Schlagwort, Risikomanagement das Ziel – um in der Trias aus Prävention, Erkennung und Abwehr noch schneller und effektiver zu werden.

Fünftens: Recht – Gerade eben bei der Sicherheit kamen rechtliche Aspekte ja schon zur Sprache und auch darüber hinaus gilt: Auch in diesem Bereich wird Routine die Ausnahme bleiben, werden immer mehr zu bedenkende Aspekte oder zu klärende Fragestellungen aufschlagen – ob man das will oder nicht.

Mir fiele schon noch Stoff für sechstens, siebtens und darüber hinaus ein, aber dabei möchte ich es jetzt mal bewenden lassen beziehungsweise (und das ist jetzt fast wie bei Inspector Columbo – das Beste kommt zum Schluss, quasi schon fast nach dem Abgang) eins möchte ich schon noch erwähnen: das Kerngeschäft des DFN-Vereins, das Wissenschaftsnetz. Auch hier wird der Fortschritt der Technologie weitere Dinge ermöglichen und uns zugleich vor neue Herausforderungen stellen. Und so gehe ich sicher davon aus, dass man auch in Zukunft ein „Wissenschaftsnetz" nicht so schnell wird von der Stange kaufen können, dass die deutsche Wissenschaftslandschaft das Wissenschaftsnetz und den DFN-Verein auch weiterhin brauchen wird. ◆

InHPC-DE-Projekt: Multi-100-Gbit-Vernetzung des Supercomputing in Deutschland

Die drei nationalen Höchstleistungsrechner sind im Rahmen des Gauss Center for Supercomputing (GCS) eng gekoppelt und bieten Forschern aus allen wissenschaftlichen Bereichen die mit Abstand leistungsfähigste Systeminfrastruktur in ganz Europa. GCS setzt sich zusammen aus dem High Performance Computing Center Stuttgart (HLRS), dem Jülich Supercomputing Centre (JSC) sowie dem Leibniz-Rechenzentrum in Garching (LRZ). Mit dem Projekt InHPC-DE wird die Integration der drei Standorte deutlich verbessert, um die Grundlage für ein ganzheitliches und gleichzeitig verteiltes Versorgungskonzept auf der Ebene Tier-0/1 zu bilden. Ein nationales, virtuelles Zentrum für Höchstleistungsrechnen, das technisch und organisatorisch eine einheitliche und nahtlose Nutzung der HPC-Services ermöglicht, ist das Ziel. Für die Vernetzung zwischen den Zentren mit mehrfach 100 Gbit/s ist der Aufbau einer technischen Infrastruktur notwendig. Im Rahmen des Projektes werden die dafür notwendigen Prozesse und Tools entwickelt.

Text: **Stephan Peinkofer, Helmut Reiser** (Leibniz-Rechenzentrum, LRZ)

1. Ausgangslage

Bis Anfang 2018 war das LRZ über einen redundanten Clusteranschluss mit einer Bandbreite von 2x20 Gbit/s an das X-WiN des Deutschen Forschungsnetzes (DFN) angebunden. Die Anbindung erfolgte mittels zweier Border-Router am Campus Garching, wobei der eine mit einem 2x10-Gbit/s-Trunk am X-WiN Super-Core in Garching und der andere mit einem 2x10-Gbit/s-Trunk in Erlangen angebunden war (vgl. Abb.1). An diese beiden Border-Router waren dann wiederum zwei weitere Rechenzentrums-Router im Rechnergebäude des LRZ mit je 2x10 Gbit/s angeschlossen. Das Rechnergebäude des LRZ besteht aus sechs Rechnerräumen, verteilt auf drei Stockwerken. Um die Verkabelung zwischen den einzelnen Räumen im Rahmen zu halten, waren die einzelnen HPC-Systeme und die zentralen Speichersysteme, eine weitere Ebene unter den Hausroutern, als Inseln an die RZ-Router angebunden. Das Inselkonzept zog sich auch durch die Layer-2- und 3-Ebenen, so dass sich jedes HPC- und Speichersystem in eigenen VLANs und Subnetzen befand. Typischerweise waren die Uplinks zwischen

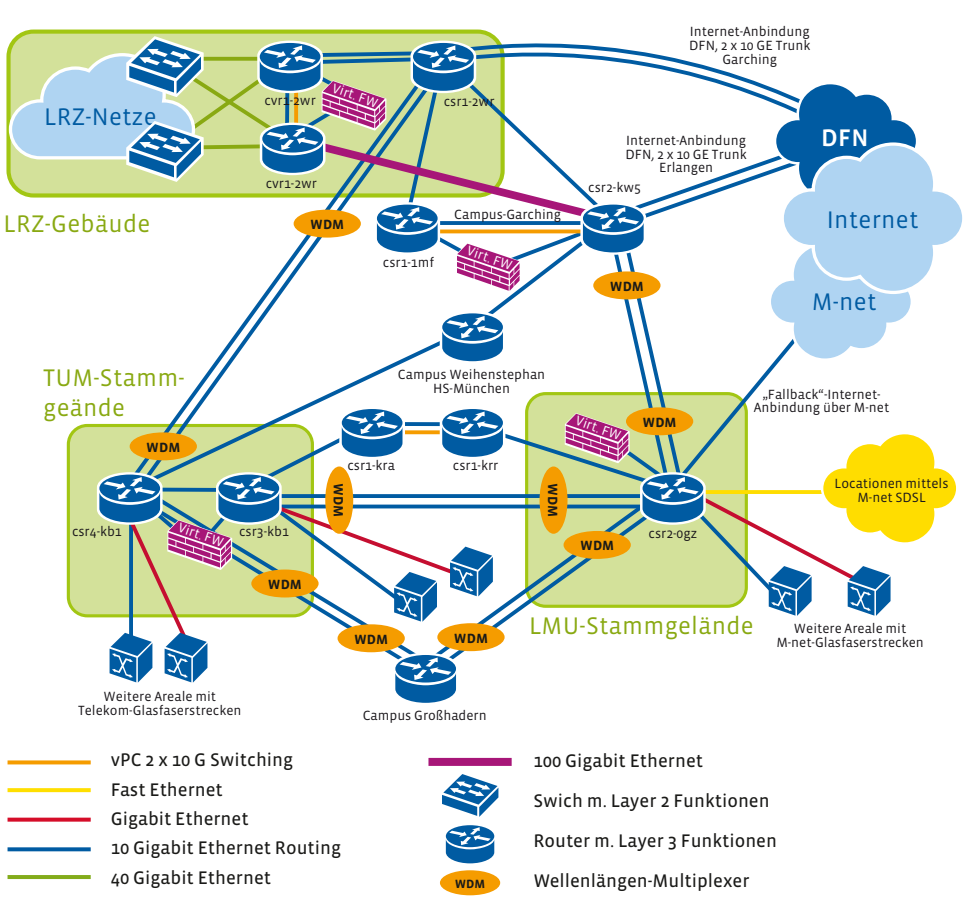


Abbildung 1: Backbone des Münchner Wissenschaftsnetzes (MWN) mit Übergang ins X-WiN

INHPC-DE GLIEDERT SICH IN VIER ARBEITSPAKETE (AP)

- AP1 Netzinfrastruktur hat die Vernetzung der Zentren mit 100 Gbit/s zum Ziel und schafft damit die technische Basis für weitere Forschungsaktivitäten.
- AP2 Datenmanagement entwickelt Lösungen für die stärkere Integration auf der Datenebene, untersucht Hochleistungsdatentransportmechanismen sowie die enge Koppelung der Storage-Systeme an den Zentren.
- AP3 Workflows unterstützt die Wissenschaftler mit dem Ziel, ihre Arbeitsabläufe und Berechnungen einfach zwischen den drei Systemen zu migrieren.
- AP4 Datenaufbereitung und Visualisierung stärken die Integration der Visualisierungsinfrastruktur zwischen den Zentren und ermöglichen komplexe Ergebnisdaten räumlich verteilt und kollaborativ zu visualisieren und an verschiedenen Standorten gemeinsam an der Visualisierung zu arbeiten und über große Distanzen die Ergebnisse der Forschung auszutauschen und gemeinsam zu bearbeiten.

2x10 Gbits/s und 4x40 Gbit/s dimensioniert, was sich zum Bottleneck zwischen den Inseln entwickelt hat. Zudem waren viele dieser Inseln über eine zentrale Firewall mit einer 2x10-Gbit/s-Anbindung geschützt. Das schränkte die Bandbreite weiter ein. Da das LRZ seit 2016 am Aufbau einer zentralen Software-defined Speicherplattform mit höchster Bandbreite für HPC- und Big-Data-Anwendungen arbeitet, wurde die alte Netztopologie zunehmend zu einem Flaschenhals, den es aufzulösen galt.

2. Vorarbeiten: Science DMZ und Referenz Data Transfer Nodes (DTNs)

Im Bereich der Nutzbarmachung von Hochgeschwindigkeitsvernetzungen mit 100 Gbit/s im Wissenschaftsbereich leistet das Energy Science Network (ESnet) bereits seit einigen Jahren umfassende Pionierarbeit und stellt seine Erkenntnisse, Erfahrungen und Best Practices auf einer Website (http://fasterdata.es.net/) weltweit der Wissenschaft zur Verfügung. In 2013 wurde das Architekturkonzept der Science DMZ entwickelt. Diese Blaupause für die Wissenschaftler ermöglicht es, ein für schnellen Datenaustausch optimiertes, dediziertes Netzsegment aufzubauen (siehe auch DFN Mitteilungen Ausgabe 94, Artikel „Campus Edge für Big Data“).

Ein Problem beim Aufbau einer 100-GE-WAN-Infrastruktur ist eine entsprechende Gegenstelle für Bandbreitentests zu finden, von der man möglichst sicher annehmen kann, dass sie für 100 Gbit/s optimiert ist. In Europa bietet GÉANT zwei entsprechende Referenz-DTNs an, einer davon ist in Paris und der andere in London platziert. Diese wurden während der Tests genutzt.

3. Realisierung von 100 GE: Leaf & Spine; Außenanbindung

Um die beschriebenen Defizite zu beheben, hat das LRZ zwei Architekturansätze evaluiert.

Der erste Ansatz bestand aus der Auflösung des Inselkonzepts und der Implementierung von zwei großen (>256 Ports), skalierbaren 100-GE-L3-Switches als redundante Core-Fabric („Fat Core“), an die alle HPC- und Speichersysteme direkt angeschlossen werden. Die großen Vorteile dieser Architektur sind die geringe Komplexität und ein Datenverkehr, der – auch mit L3 Routing zwischen den Subnetzen der HPC und Speichersysteme – in diesen Switches meist komplett non-blocking ist. Allerdings mit dem Nachteil, dass erhebliche Investitionen in die Nachinstallation einer strukturierten MPO-Verkabelung notwendig sind, da am LRZ die Systeme über sechs Räume verteilt sind. Zudem sind die Preise für die notwendigen Enterprise-Switchsysteme relativ hoch. Dazu kommt, dass eine schnelle und flexible Skalierung mit einem Fat Core nicht so einfach umzusetzen ist.

Der zweite Ansatz basiert auf der sogenannten Leaf-Spine-Architektur. Die Grundidee ist, dass man das Netz in Spine- und Leaf-Schichten teilt. An den Switches der Leaf-Schicht sind die Endgeräte angeschlossen und jeder Leaf Switch hat eine oder mehrere Verbindungen zu jedem Switch in der Spine-Schicht. Somit ist jedes Endgerät maximal drei Hops von jedem anderen Endgerät entfernt. Theoretisch ließe sich diese Architektur beliebig skalieren, indem man weitere Spine Layers hinzufügt. Die vom LRZ evaluierte und implementierte Leaf-Spine- Architektur ist in Abb. 2 dargestellt. Insgesamt vier Switches mit je 64 Ports verteilt auf zwei Brandabschnitte bilden den Spine Layer. Zehn Switches mit je 64 Ports und zwei mit je 32 Ports bilden den Leaf Layer und sind als redundante Pärchen auf die Rechnerräume verteilt. Jeder Leaf ist mit 8x100 GE an den Spine angebunden, was eine aggregierte Bandbreite von 1,6 Tbit/s von jedem redundanten Leaf-Paar in den Spine Layer ergibt. Zusätzlich sind zwei Switches als Border Leaf implementiert, um einen definierten Übergabepunkt zwischen der Leaf-Spine-Fabric und dem restlichen RZ-Netz zu haben. Diese sind mit je 4x100 GE an den Spine Layer und je 2x100GE an den Border-Routern sowie je 2x100 GE an den Rechenzentrumsroutern angeschlossen.

Mit diesem Ansatz ist wesentlich weniger Nachverkabelung zwischen den Räumen erforderlich. Durch den Einsatz der vom Hersteller für diese Switches zertifizierten QSFP-100-SRBD-Transceiver lässt sich im Vergleich zu den üblichen QSFP-100-SR4-Transceivern der Verkabelungsaufwand noch weiter um den Faktor 4 reduzieren. Im Gegensatz zum Fat Core, der i. d. R. non-blocking ist, wurde zwischen den einzelnen Leaf-Paaren ein Blockingfaktor von 7:1 gewählt, da die angeschlossenen Speichersysteme maximal 200 Gbit/s – verteilt auf mehrere Leafs – liefern können. Zudem erlaubt die Architektur den Blockingfaktor jederzeit bedarfsgetrieben über die Uplink-Anzahl zu skalieren. Darüber hinaus sind die Kosten für die benötigten 32- und 64-Port-Switches inkl. Transceiver und Kabel für die Anbindung spürbar geringer als für die Enterprise Switches, die für die Fat Core-Lösung nötig wären. Ein Nachteil ist die deutlich höhere Gesamtkomplexität. Da die Leaf-Spine-Architektur nicht nativ mit Ethernet realisiert werden kann (loopfreie Topologie, Spanning Tree), kommt zur Implementierung eine Reihe von zusätzlicher Technologien wie z. B. VXLAN und ECMP zum Einsatz. Zudem will das LRZ nicht auf eine Separierung der einzelnen HPC und Speichersysteme in verschiedene VLANs und Subnetze verzichten. Um zu vermeiden, dass damit sämtlicher Traffic zwischen den einzelnen HPC- und Speichersystemen über die LRZ-Rechenzentrumsrouter, und damit aus der Fabric, hinaus- und wieder hineingeleitet werden muss, sind auch auf Layer 3 entsprechende fortgeschrittene Technologien wie z. B. BGP-EVPN, VRF, Route Leaking u. a. nötig.

Auch die Außenanbindung musste für das Projekt auf mindestens 100 GE erhöht werden. Eigene dedizierte Links oder VPNs zwischen den Zentren wurden sehr schnell zugunsten einer Erhöhung des jeweiligen „normalen" X-WiN-Anschlusses verworfen. Ein breitbandiger X-WiN-Zugang bringt allen Nutzern Vorteile und nicht nur denen, die an einem der GCS-Zentren angeschlossen sind. Jedes Zentrum wurde mit 2x100 GE an das X-WiN angeschlossen. Das Upgrade konnte, nach Beschaffung entsprechender Komponenten bei den Sites und beim DFN, schnell realisiert werden. Durch die hohe Bandbreite im X-WiN Super Core und die direkte Anbindung der Zentren daran sind 100 GE auch Ende zu Ende realisierbar.

3.1 Implementierung und Anbindung der 100-GE-Data-Transfer-Nodes

Als DTNs für das InHPC-DE Projekt kommen drei aktuelle auf Linux X86_64 basierte Server mit Mellanox-ConnectX-4- und -5-Netzwerkkarten zum Einsatz.

Bei der Auswahl von Hardware für 100-GE-DTNs sind einige Grundregeln zu beachten. Bedingt durch die heutigen Multi-Core-Architekturen werden mehrere parallele TCP Streams benötigt, um einen 100-GE-Link zu saturieren. Ist man auf eine möglichst hohe Single Stream Performance angewiesen, empfiehlt sich der Einsatz einer CPU mit möglichst hoher Taktrate. Sofern die Applikation nicht die Leistung einer zweiten CPU benötigt, ist in diesem Fall auch ein Single CPU System vorzuziehen, da man dadurch negative Performanceeffekte vermeidet, die durch die NUMA-Architektur entstehen können.

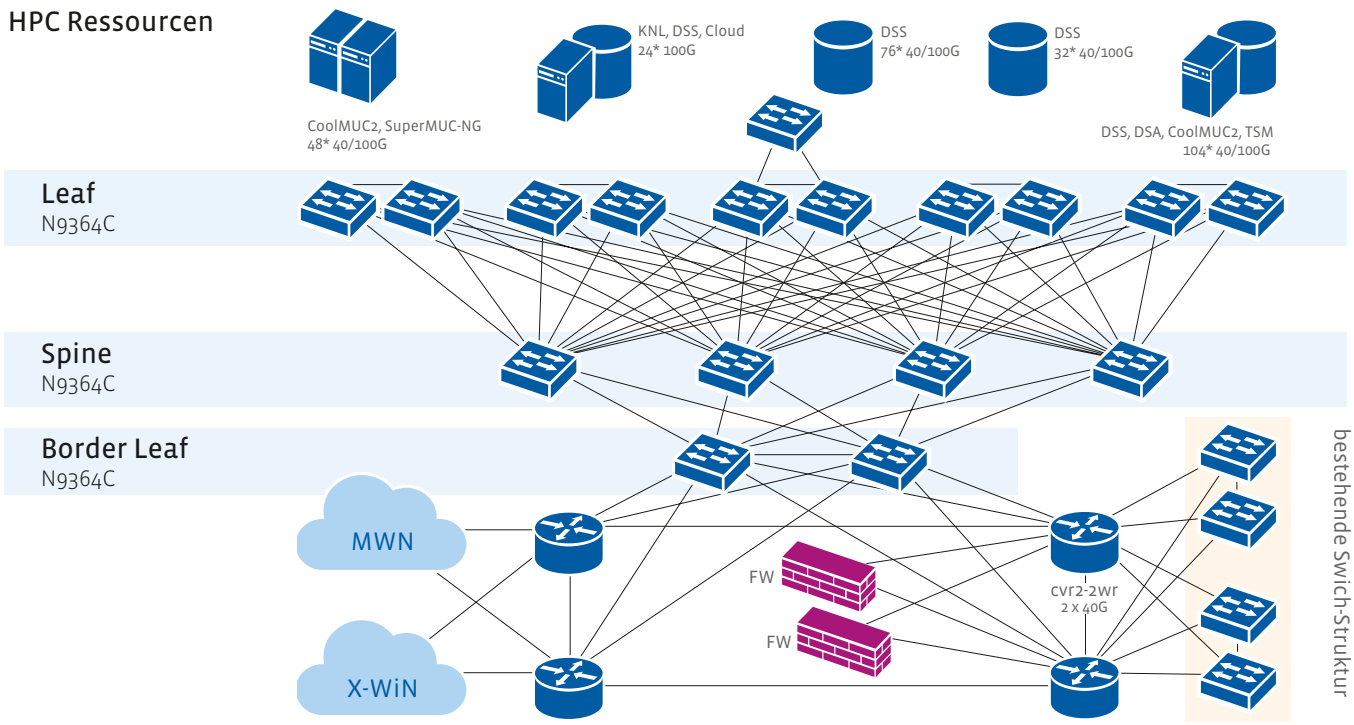


Abbildung 2: Leaf & Spine Architektur

4. Evaluation der Netzinfrastruktur-Transfergeschwindigkeit

Für eine erste Evaluation der 100-GE-Netzinfrastruktur wurden synthetische Bandbreitenmessungen zwischen GÉANT DTNs in London und Paris sowie den drei GCS-Zentren und weiteren Sites mit 40/100-GE-Netzanbindung durchgeführt. Diese Tests zeigten sehr schnell, dass 100 GE nicht auf Anhieb erreichbar waren, und halfen, versteckte Probleme in der Infrastruktur zu identifizieren.

4.1 100-GE-Bandbreitenmessungen mit iperf3

Im Projekt kommt zur Bandbreitenmessung das Tool iperf3 zum Einsatz. Die Wahl von iperf3 begründet sich durch dessen gute Stabilität und einen Output im JSON Format, der es leichter macht, die Ergebnisse weiter aufzubereiten. Eine oftmals übersehene Einschränkung von iperf3 ist die Implementierung als Single-threaded Applikation. Daher ist eine einzelne Messung, auch wenn mehrere TCP Streams parallel verwendet werden, immer auf die Performance eines einzelnen CPU-Kerns limitiert. Somit ist für eine Saturierung einer 100-GE-Leitung mit aktueller Hardware ein Test mit mindestens vier iperf3 Prozessen parallel erforderlich.

4.2 Optimierung des Durchsatzes der Data Transfer Nodes

Um die Data Transfer Nodes für die geplanten 100-GE-WAN-Datentransfers zu optimieren, mussten einige Konfigurationsanpassungen im BIOS und im Betriebssystem der DTNs vorgenommen werden, mit dem Ziel, die Latenzen bei der Interrupt-Behandlung möglichst klein und konstant zu halten. Dazu müssen im BIOS die sogenannten P- und C-States sowie das Hyperthreading ausgeschaltet werden.

Um die im BIOS abgeschalteten P- und C-States auch im Betriebssystem zu deaktivieren, kommen die Kernel-Kommandozeilenparameter

```
intel_idle.max_cstate=0
processor.max_cstate=0
intel_pstate=disable
```

zum Einsatz.

Darüber hinaus wurden folgende Anpassungen am Linux TCP-Stack vorgenommen:

Maximale TCP-Puffergröße: TCP erlaubt dem Sender über das Congestion Window, eine von ihm dynamisch festgelegte Menge von Daten zu senden, bevor er auf die Bestätigung des Empfangs wartet. Die Größe dieses Fensters lässt sich mit dem sogenannten Bandwidth Delay Product (BDP) berechnen:
Bandbreite des Links [bit/s] x Round Trip Time [s] = Bandwidth Delay Product [bit]

Bei einer Bandbreite von 100 Gbit/s und einer Round Trip Time (RTT) von 23 ms, was in etwa der Netzstrecke München/London entspricht, ergibt sich so ein BDP von ca. 275 MB.

Die maximale Größe des Congestion Windows wird bei Linux durch die maximale TCP-Puffergröße bestimmt, welche auf maximal 2 GB limitiert ist. Daher ist die Empfehlung für 100-GE-DTNs die maximale TCP-Puffergröße auf 2 GB zu setzen. Das wird über die Parameter:

```
net.ipv4.tcp_rmem
net.ipv4.tcp_wmem
net.core.rmem_max
net.core.wmem_max
in /etc/sysctl.conf
```

erreicht.

TCP Paketscheduler: Als weitere Maßnahme wurde der TCP Paketscheduler auf Fair Queuing geändert. Dies erfolgt über den Parameter:

```
net.core.default_qdisc = fq in der
Datei /etc/sysctl.conf.
```

Eine weitere Tuningmaßnahme ist der Einsatz von **Jumbo Frames**. Mit Jumbo Frames wird oftmals eine MTU von 9000 bezeichnet. Allerdings sind prinzipiell alle Ethernet Frames, die größer sind als 1500 Bytes, Jumbo Frames. Die fehlende Standardisierung ist der große Nachteil von Jumbo Frames. Zwar gibt es mittlerweile einige Verfahren, wie das Betriebssystem die maximale MTU auf einem Pfad zwischen zwei Hosts relativ zuverlässig erkennen kann, allerdings sind diese Verfahren nicht perfekt, und wenn es zu Problemen kommt, ist die Fehlersuche relativ schwierig. Der Einsatz von Jumbo Frames sollte also wohlüberlegt sein.

4.3 Ergebnisse der Netzinfrastrukturevaluation

Die Bandbreitentests wurden zwischen den GCS-Sites und GÉANT DTNs vorgenommen. Nach anfänglichen Problemen, wo nur 40 bis 50 Gbit/s erreichbar waren, wurden die in dieser Arbeit beschriebenen Konfigurationen vorgenommen. Mit einer MTU von 9000 waren zwischen einem DTN in Jülich und einem DTN in Garching ca. 90 Gbit/s bei synthetischen Lasttests in beide Richtungen erreichbar. Zwischen Garching und dem GÉANT DTN in Paris konnten ca. 96 Gbit/s und zum DTN in London konnten ca. 90 Gbit/s, jeweils in beide Richtungen, übertragen werden. Bei einer MTU von 1500 konnten von Jülich nach Garching ca. 90 Gbit/s, für Verkehr von Garching nach Jülich ca. 88 Gbit/s gemessen werden. Bei ersten Tests von Garching nach Stuttgart haben wir ca. 95 Gbit/s und von Stuttgart nach Garching ca. 75 Gbit/s gemessen. Bei allen Tests wurden acht iperf3-Prozesse mit je acht parallelen TCP Streams genutzt.

5. Ausblick

Als nächster Projektschritt werden Datentransfer- und -management-Applikationen gefunden und getestet, welche die vorhandene Netzbandbreite über mehrere parallele TCP Streams und Betriebssystemprozesse auch ausnutzen können. Dazu werden in den nächsten Monaten diverse Werkzeuge wie z. B. Globus Online, GridFTP, Unicore FTP, iRODS und FTS evaluiert werden. ◆

Netze, Bälle, Datenströme – oder wie die Fußball-WM ins X-WiN kam

Im Sommer 2018 wurde die Leidensfähigkeit deutscher Fußballfans, aber auch die Leistungsfähigkeit des Deutschen Forschungsnetzes auf die Probe gestellt. Wenig überraschend nutzten auch Teilnehmer am X-WiN die Möglichkeit, Spiele der Fußball-WM online per Videostreaming zu verfolgen. Insbesondere die (wenigen) Spiele der deutschen Nationalmannschaft waren sehr deutlich in den Auslastungsdiagrammen des Wissenschaftsnetzes sichtbar. Wie finden solche Live-Übertragungen oder generell Wissenschaftsdaten weltweit ihr Ziel? Einen Einblick in die Welt der Verbindungen zwischen den Teilnetzen des Internets, das sogenannte Internet Transit bzw. Peering, gibt es auf den folgenden Seiten.

Text: **Henry Kluge, Stefan Piger** (DFN-Verein)

Foto © skynesher/iStockphoto

Das weltweite Internet besteht aus einer Vielzahl unabhängiger Netze. Jedes dieser Netze hat einen Betreiber, der die Strategie der Verkehrsführung innerhalb seines Netzes vorgibt und die reibungslose Kommunikation zwischen seinen Nutzern sicherstellt. Im Jargon des Internets werden diese abgegrenzten Netze Autonomous Systems oder kurz AS genannt und erhalten eine weltweit eindeutige AS-Nummer. Diese bildet zusammen mit dem Routingprotokoll BGP (Border Gateway Protocol) die Grundstruktur der Vermittlungsinfrastruktur des Internets und ermöglicht den Austausch von Routinginformationen, die für eine Ende-zu-Ende-Kommunikation notwendig sind.

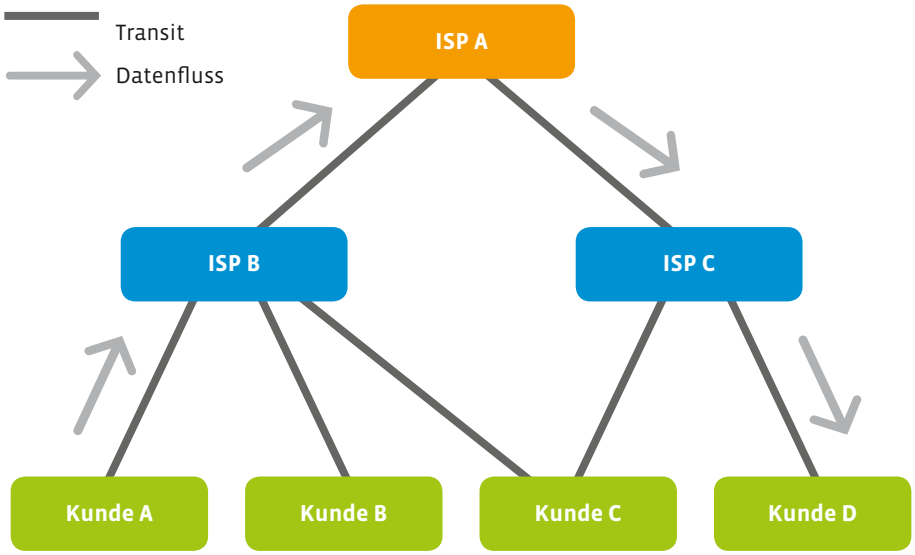


Abbildung 1: Datenfluss zwischen Endpunkten im Internet (nur Transit)

Der Erfolg des Internets liegt wesentlich darin begründet, dass Nutzer weltweit kommunizieren können, ohne sich Gedanken darüber machen zu müssen, an welches Netz sie oder ihr jeweiliger Kommunikationspartner angebunden sind. Diesem Ansatz fühlt sich auch der DFN-Verein verpflichtet und verfolgt daher für seinen Dienst DFNInternet das Ziel, exzellente Konnektivität nicht nur zwischen Einrichtungen seiner Community bereitzustellen, sondern auch zu den anderen Zielen des Internets.

Durch die Größe und Ausdehnung des heutigen Internets ist es allerdings unrealistisch, dass sich alle Netze direkt miteinander verbinden können. Das Ziel, die einzelnen Netze sowohl kosteneffizient als auch mit hoher Leistungsfähigkeit direkt oder indirekt miteinander zu koppeln, führte zu zunehmend komplexen technischen und administrativen Strukturen, die im Folgenden näher beleuchtet werden sollen.

Netze verknüpfen: die (kommerzielle) Welt des Peerings

Wie stellt nun aber ein Netzbetreiber (Internet Service Provider – ISP) sicher, dass Pakete mit Zielen außerhalb des eigenen Netzes ihr jeweiliges Ziel erreichen? Im einfachsten Fall reicht es aus, das eigene Netz mit dem eines anderen Netzbetreibers zu verbinden, der vertraglich garantiert und technisch sicherstellt, dass über ihn alle Ziele des Internets erreicht werden können. Netzbetreiber, die gegen Entgelt IP-Verkehr durch das eigene Netz leiten, werden Transit- oder auch Upstream-Provider genannt. In Abbildung 1 hat diese Rolle Provider A inne, über den Provider B Verkehr von Kunde A zu Kunde D via Provider C leitet.

Dieses Modell ist zwar einfach und klar strukturiert, jedoch muss für die genutzte Bandbreite bezahlt werden, und auch die Policy zur Wahl der besten Routen ist nur eingeschränkt beeinflussbar. Zudem werden die Transit-Provider in dieser Topologie zu kritischen Infrastrukturen, deren Ausfall weite Teile des Internets isolieren würde.

Die Lösung dieses Problems sind direkte Kopplungen von Netzen. Diese direkten technischen Verbindungen werden im Jargon als Peering bezeichnet und reduzieren die Abhängigkeit von Transit-Providern erheblich. Wie in Abbildung 2 dargestellt, kann der Verkehr zwischen Kunden von Peers den direkten Weg über das Peering nehmen und muss nicht mehr zwingend den über den Transit-Provider nehmen. Gleichzeitig erhöhen Provider B und Provider C dadurch ihre Resilienz gegen Ausfälle einzelner Links deutlich, da es nun einen weiteren Weg zwischen ihnen gibt. Der direkte Weg zwischen den Providern verbessert typischerweise auch die für die Endanwender wichtigen Antwortzeiten deutlich und ermöglicht eine flexible Routingstrategie.

Wie aber baut nun ein Netzbetreiber ökonomisch effizient und technisch skalierbar Peerings zu möglichst vielen attraktiven Netzen auf? Im Internet haben sich dafür zwei Modelle durchgesetzt, die auch frei kombiniert werden können.

Der einfachste Weg ist die direkte Kopplung von Routern (auch als Provider Edge- oder PE-Router bezeichnet) der beiden Peering-Partner. Diese Art des Peerings wird als Private Network Interconnection oder PNI bezeichnet und findet bevorzugt in Carrier-neutralen Datenzentren statt. Diese auch als Colocation-Center bezeichneten Einrichtungen stehen allen Netzbetreibern für die Anmietung von Flächen und Datenverbindungen untereinander offen. Durch die dem PNI-Modell inhärente

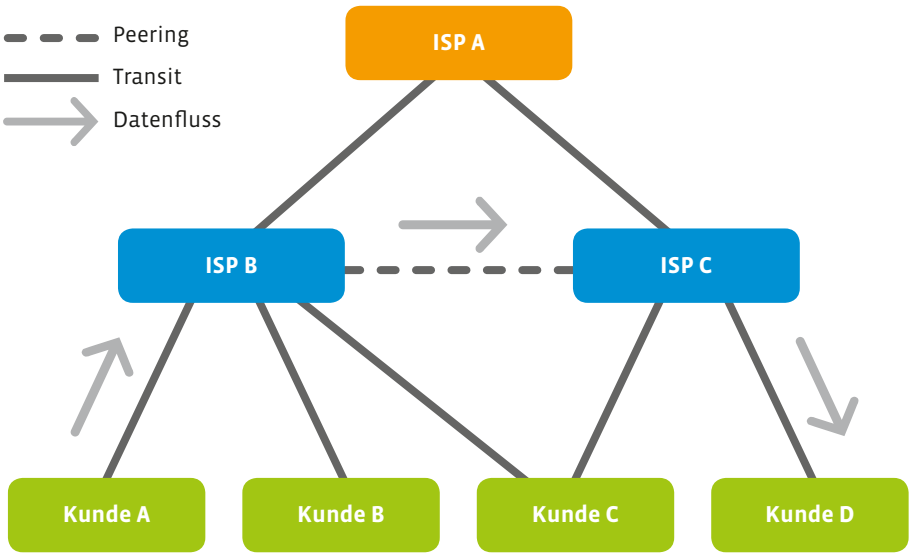


Abbildung 2: Datenfluss zwischen Endpunkten im Internet (mit Peering)

1:1-Beziehung zwischen Netzen und die schiere Anzahl von etwa 86.000 Autonomous Systems im Internet skaliert dieses Modell jedoch nicht ausreichend und wird daher vorwiegend für die Kopplung mit relevant großen Partnern verwendet.

Um dieses Skalierungsproblem zu umgehen, hat sich weltweit eine große Anzahl von Austauschpunkten etabliert, die als Internet eXchange Point (IXP) oder auch Commercial Internet eXchanges (CIX) bezeichnet werden. An diesen Austauschpunkten „treffen" sich Internet Service Provider mit ihren Netzen und schließen sich an eine eigens dafür etablierte Netzwerkinfrastruktur auf Basis von Layer-2-Switches an, über die sie dann Verkehr mit allen dort angeschlossenen Netzen austauschen können. Diese Art der Anbindung wird als Public Peering Interconnection (PPI) bezeichnet. Diese PPI können durch den Aufbau einer individuellen BGP-Session zum Austausch der Routinginformationen oder zur Nutzung eines typischerweise am IXP bereitgestellten Route-Servers etabliert werden. Limitierender Faktor ist hierbei nur die Bandbreite des vom ISP genutzten Netzwerkinterfaces.

Als Sonderform hat sich in den letzten Jahren das sogenannte Remote Peering herausgebildet, bei dem der Anschluss des PPI nicht direkt am IXP, sondern über eine separate angemietete Datenverbindung zwischen IXP und ISP erfolgt.

Neben dem in Deutschland bekanntesten Internet Exchange DE-CIX in Frankfurt/Main, existieren weltweit mehrere Hundert weitere IXP wie z. B. der AMS IX (Amsterdam), LINX (London) oder LAIIX (Los Angeles). [Quelle: Wiki oder http://www.ix-f.net/]

„Drum prüfe, wer sich ewig bindet" – Überlegungen zur Peering-Strategie

Aber was ist nun die optimale Peering-Strategie? Darauf gibt es leider keine universelle Antwort, da sie von mehreren für jedes Netz individuellen Faktoren abhängt. Den wichtigsten Einfluss auf eine strategische Ausrichtung haben im Regelfall die Kosten.

Diese hängen beim IP-Transit direkt von der genutzten Bandbreite ab. Im Internet hat sich dazu ein Berechnungsmodell durchgesetzt, das einen Preis für das 95. Perzentil der in einem Monat genutzten Maximalbandbreite berechnet. Dieses Abrechnungsmodell verhindert, dass kurzfristige Spitzenlasten preisbildend für den ganzen Monat sind.

Die Kosten für PNI und PPI ergeben sich direkter. Bei PNI trägt jeder Peer die Kosten für seine Router-Schnittstellen selber. Es entstehen „nur" noch Kosten für die Aufstellung des Routers (Miete für die Aufstellfläche, Kosten für Spannungsversorgung und Klimatisierung) sowie für die Verbindung zwischen den Router-Schnittstellen. Im günstigsten Fall ist dies lediglich eine Glasfaserverbindung (Cross-Connect) innerhalb eines Colocation-Centers. Beim PPI kommt zu diesen Kosten noch ein monatliches Entgelt für die Netzwerkschnittstelle

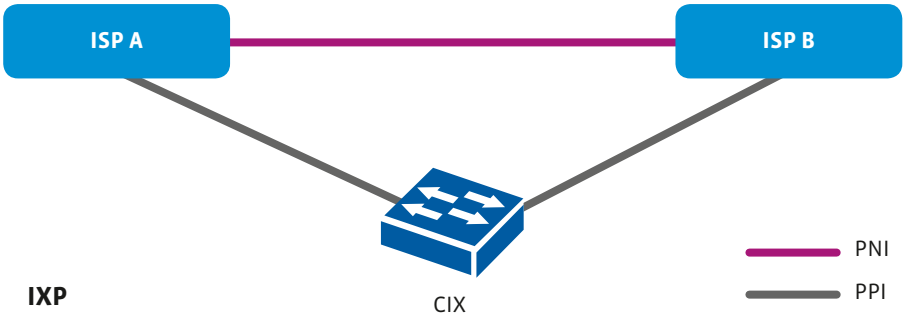


Abbildung 3: Peering-Modelle

am IX hinzu, das auf Basis der technischen Bandbreite berechnet wird.

Für die Strategie spielen neben den Kosten noch Faktoren wie die Größe des eigenen Netzes bzw. dessen Attraktivität für mögliche Peers eine wichtige Rolle. Die Attraktivität eines Netzes als Peer erhöht sich dabei mit der Anzahl der über diese erreichbaren und für die potenziellen Partner interessanten Dienste sowie mit der Anzahl der angebundenen Endnutzer (im Internet-Jargon auch als Eyeballs bezeichnet). Letztlich entscheidet in erster Linie diese Attraktivität über die Bereitschaft anderer Netzbetreiber, mit dem eigenen Netz zu peeren.

Zusätzlich sollte jeder Netzbetreiber eine Risikobewertung vornehmen, um zu klären, welche Ausfallzeiten er für einzelne oder ganze Teile des Internetzugangs seinen Nutzern zumuten kann. Daraus folgend ist eine Strategie ableitbar, die aus der Kombination der o. g. Modelle eine angemessene Redundanz seiner Außenanbindungen sicherstellt.

Schließlich sind noch globale aktuelle Entwicklungen im Internet-Transit und Peering-Markt in die eigene Strategie einzubeziehen. Wurde zur Jahrtausendwende noch ein Großteil des Internet-Verkehrs über die Transit-Provider geführt, ist jetzt ein Trend hin zu direkten (PNI) oder Verbindungen über Internet Exchanges (PPI) zu verzeichnen. Eine dominierende Rolle spielen in dieser Entwicklung die großen Content Networks und Cloud-Provider wie Amazon, Apple, Facebook, Google, Microsoft und Netflix, deren Ziel eine möglichst direkte Verbindung zu ihren Endnutzern ist. Dazu bauen einige dieser Konzerne inzwischen eigene globale Backbone-Netze auf und verbinden diese mit den weltweit relevanten Internet Exchanges bzw. bieten in Colocation-Centers direkte Peering-Verbindungen an. Diese generelle Tendenz der Unterscheidung von Transport und Content begann bereits vor 20 Jahren mit dem Aufkommen von Content Delivery Networks. Anbieter wie Akamai, EdgeCast und Limelight spezialisierten sich auf eine weltweit verteilte Bereitstellung von Inhalten insbesondere für Fernsehanstalten und Nachrichtenanbieter aber auch für Internetshops. Hierfür werden sogenannte Caches eingesetzt, die Kopien von Daten an möglichst vielen IXP zur Verfügung stellen.

Eine wichtige Konsequenz aus dieser Entwicklung ist die abnehmende Bedeutung der globalen Transit-Provider, die im Jargon auch als Tier-1-Carrier bezeichnet werden. Indem ein zunehmender Anteil des Contents direkt an die Netze mit Endnutzern geführt wird, sinkt der Anteil dieser Carrier am weltweiten Datenverkehr kontinuierlich. Während diese Entwicklung eine für sich genommen erst einmal begrüßenswerte Senkung der Kosten für die Abwicklung von Verkehr mit anderen Netzen mit sich bringt, stellt sie doch auch eine Gefahr für die Neutralität des Internets dar. Während die globalen Transit-Provider Verkehr jeglicher Provenienz durch ihre Netze leiten, sind die reinen Content-Provider nur ihren eigenen Daten verpflichtet. Sollte diese Entwicklung durch die Reduktion der Einnahmen der Transit-Carrier zu einer fortgesetzten Atrophie ihrer Netzkapazitäten führen, könnte das Internet ultimativ zu einer Vielzahl geographisch verteilter und nur schlecht miteinander vernetzter Inseln zerfallen. Einzig die Content-Provider wären weiterhin in der Lage, Inhalte mit hoher Kapazität weltweit bereitzustellen.

Und nun konkret: die Peering Strategie des DFN

Was sind nun die Ziele, die der DFN-Verein bei der Verbindung mit anderen Netzen verfolgt? Im Wesentlichen sind dies die gleichen, die auch beim Ausbau des Wissenschaftsnetzes verfolgt werden: höchste Leistungsfähigkeit beim Austausch von Daten mit den für seine Teilnehmer relevanten Netzen bei gleichzeitig höchster Verfügbarkeit der Konnektivität und ebensolcher Kosteneffizienz. Eine hohe Leistungsfähigkeit der einzelnen Außenanbindungen zu erreichen, erscheint auf den ersten Blick recht einfach: Man muss „nur“ dafür sorgen, dass ausreichend Übertragungskapazität vorhanden ist. Aber wie viel ist bzw. wird in der näheren Zukunft ausreichend sein? Welche Netze (Autonomous Systems) sind für die Teilnehmer am X-WiN relevant und wie entwickeln sich Volumen und Charakteristik des Datenverkehrs?

Zur Beantwortung dieser Fragen betreibt der DFN-Verein eine spezialisierte Analyse-Plattform, mittels derer die Verkehre auf der IP-Plattform kontinuierlich erfasst und statistisch ausgewertet werden. Dabei werden im ersten Schritt Daten über das Volumen erhoben, das über die Anschlüsse zu anderen Netzen (PNI) sowie zu Internet-Exchanges (PPI) und IP-Transit-Providern fließt. Diese Volumendaten geben jedoch allein keine Auskunft darüber, mit welchen AS wie viele Daten ausgetauscht werden.

Zur Ermittlung der individuellen Zuordnung einzelner Verkehrsströme zu Netzen werden von den Routern im Wissenschaftsnetz Informationen im NetFlow-Format erhoben. Mithilfe dieser Daten, die sowohl die beteiligten AS, die Verkehrsrichtung und das Datenvolumen beinhalten, lassen sich dann fundierte Entscheidungen über die Notwendigkeit von neuen Peerings und deren Dimensionierung treffen. Weiterhin lassen sich mit diesen Daten und der Beobachtung der Entwicklung des Internetmarktes auch Prognosen über künftig benötigte Übertragungskapazitäten ableiten.

Damit beim Ausfall einzelner Anbindungen keine für den Nutzer spürbaren Einschränkungen entstehen, werden wo möglich Internet Service Provider auf mehreren Wegen angebunden. Hier wird neben unterschiedlichen Peering-Arten (PPI und PNI) und Anbietern (DE-CIX, ECIX und BCIX) insbesondere eine geographische Verteilung angestrebt.

PEERING POLICY

Im Peering-Ökosystem ist es üblich über eine sogenannte Peering Policy die Voraussetzungen und Rahmenbedingungen für ein Peering zu formulieren. Inhalt ist typischerweise die generelle „Politik“ des Peerings, die in 4 Klassen unterteilt werden kann:

- → Open: Peering mit jedem ISP an jedem verfügbaren IXP ohne weitere Voraussetzungen,
- → Selective: Peering grundsätzlich mit jedem ISP an ausgewählten IXP mit Voraussetzungen wie z. B. einem minimal zu erreichenden Datenvolumen,
- → Restrictive: Peering nur unter strikter Einhaltung von Voraussetzungen (typisch für Tier-1 Provider),
- → No Peering: Generelle Ablehnung von Peering.

Der DFN-Verein verfolgt eine selektive Policy mit der Ausnahme, generell nicht mit anderen Wissenschaftsnetzen zu peeren, da deren Anbindung über GÉANT erfolgt.

Auch die Versorgung mit IP-Transit-Kapazität wird über eine geographische Verteilung innerhalb Deutschlands gesichert. Darüber hinaus werden immer Verträge mit mindestens zwei unterschiedlichen Transit-Carriern abgeschlossen, um Auswirkungen durch Probleme innerhalb eines Carrier-Netzes auf die Teilnehmer am X-WiN zu minimieren. Mit diesem Ansatz wird nicht nur eine sehr hohe Robustheit gegen lokale Unterbrechungen erreicht, sondern auch noch die Latenz zwischen den Teilnehmern am Wissenschaftsnetz und dem jeweiligen Peer reduziert.

Da sich die Verkehre über die Außenanbindungen des X-WiN genau wie der Gesamtverkehr laufend verändern, müssen diesbezügliche Analysen kontinuierlich durchgeführt werden, um Trends frühzeitig erkennen zu können. Darüber hinaus ist eine laufende Beobachtung der Marktentwicklungen sowohl für Colocation-Centers und Internet-Exchanges als auch der dort angesiedelten und für die Teilnehmer am X-WiN relevanten ISP erforderlich, um eine strategische Planung von Präsenzen an Peering-Lokationen vornehmen zu können.

Zur Sicherstellung einer hohen Kosteneffizienz wird angestrebt, Autonomous Systems mit relevantem Datenverkehr von IP-Transit auf PPI umzustellen. Wenn auch hier Verkehrsvolumina mit Peaks von mehreren Gbit/s erreicht werden, wird die Möglichkeit eines Private Network Interconnects geprüft. Selbst wenn hierbei ein relativ hoher kommunikativer und technischer Initialaufwand typisch ist, rentiert sich dieser in kurzer Zeit durch die Minimierung der laufenden Kosten des IP-Transits und für Interfaces an IXP für PPI.

Neben den absoluten Zahlen von übertragenen Daten können auch strategische Überlegungen zur Auswahl der Peeringpartner eine Rolle spielen. In erster Linie werden hier die Nähe zur Wissenschafts-Community in Deutschland und der potenzielle Nutzen für diese als Entscheidungskriterien herangezogen.

In diesem Kontext ist es auch jenseits einer rein technischen Betrachtung des Internetverkehrs hilfreich, Kontakte mit ISP und anderen Mitspielern im Internetbusiness aufzubauen und zu pflegen. Auf „Branchen“-Veranstaltungen, über Mailinglisten oder persönliche Kontakte lassen sich sowohl potenzielle Peering-Partner finden als auch neue Entwicklungen frühzeitig erkennen.

Der DFN-Verein verfolgt eine selektive Policy mit der Ausnahme, generell nicht mit anderen Wissenschaftsnetzen zu peeren, da deren Anbindung über GÉANT erfolgt.

Vernetzung mit der globalen Wissenschaft

Die effiziente Vermittlung von Datenverkehr seiner Teilnehmer mit kommerziellen ISPs ist sicherlich wichtig für den DFN-Verein. Aber die konstituierende Aufgabe des DFN-Vereins ist die Vernetzung seiner Community, national und international. Innerhalb Deutschlands ist die Situation einfach, da die Verbindungen zwischen seinen Teilnehmern direkt über das X-WiN geführt werden können. Aber wie werden Daten zwischen nationalen Wissenschaftsnetzen (im Jargon „National Research and Educations Networks“, NREN) ausgetauscht? Wie der Begriff NREN schon andeutet, arbeiten die Wissenschaftsnetze in der Regel ausschließlich auf der jeweiligen nationalen Ebene, was eine direkte Vernetzung mit den NRENs nicht-benachbarter Länder deutlich erschwert. In Europa wurde dafür eigens eine Organisation der NRENs gegründet, die für die Vernetzung innerhalb Europas, aber auch von Europa mit den außereuropäischen NRENs zuständig ist – die GÉANT Association. Schon der Vorläufer dieser Organisation DANTE („Delivering Advanced Network Technology to Europe“) betrieb das europäische Overlay-Network GÉANT und seine Vorgänger. Dieses Netz verfügt über Standorte in den meisten Ländern der EU und verbindet die dortigen NRENs über ein eigenes Weitverkehrsnetz miteinander. Daneben verbindet GÉANT die europäischen NRENs über eine Vielzahl von angemieteten Verbindungen mit den NRENs in Nord- und Südamerika, Afrika, dem Nahen und Mittleren Osten sowie Asien (vgl. https://map.geant.org).

Warum aber betreibt man diesen Aufwand und verlässt sich nicht auf kommerzielle Carrier? Dafür gibt es historische, aber auch gute aktuelle Gründe. Ausgangspunkt zu Beginn der 90er Jahre war das Ziel einer qualitativ hochwertigen Vernetzung europäischer NRENs sowohl im Hinblick auf die verfügbare Übertragungskapazität als auch die Latenz zwischen Teilnehmern. Auch gute Verbindungen in die USA waren schon damals wichtig. Zur Zeit der Gründung von DANTE war diese Forderung durch kommerzielle IP-Transit-Verbindungen selbst innerhalb der damaligen EU gar nicht oder nicht kosteneffizient erfüllbar. Heute haben sich die Grenzen der EU verschoben, sodass aktuelle Herausforderungen eher die performante Anbindung der Länder des Balkans sind. Zunehmend liegen die Herausforderungen aber auch im außereuropäischen Bereich, da wissenschaftliche Projekte inzwischen weltweit kollaborieren. So müssen Teleskope der europäischen Südsternwarte in Chile angebunden oder Verbünde von Hochenergiephysikern in Europa und Japan unterstützt werden. Auch die weltweite Verteilung von Erdbeobachtungsdaten des europäischen Copernicus-Projekts stellt eine Aufgabe dar, der sich die europäischen NRENs und damit GÉANT zu stellen haben.

Eine zunehmend strategische Funktion erhält GÉANT für die NRENs und damit den DFN-Verein im Kontext der Entwicklung des kommerziellen Umfelds. Wie im ersten Abschnitt dargelegt, scheinen die Tier-1-Carrier aktuell durch den Ausbau der Netze der Content-Provider marginalisiert zu werden. Damit steht zu befürchten, dass künftig für den Ausbau von deren Netzen weniger Investitionsmittel zur Verfügung stehen werden und darunter am Ende die Leistungsfähigkeit der Tier-1-Netze leiden wird. Mit einer eigenen leistungsfähigen Vernetzungsinfrastruktur verfügt die Wissenschaft damit über ein unabhängiges Standbein und sichert die eigene Konnektivität auch unter sich ändernden globalen Rahmenbedingungen.

Die Außenanbindungen des X-WiN

Aus den in den vorigen Abschnitten dargestellten strategischen Zielen ergibt sich die geographische Architektur der Außenanbindungen des X-WiN (vgl. Abbildung 4). Aktuell unterhält der DFN-Verein drei X-WiN-Standorte in Carrier-neutralen Colocation-Centers in Deutschland. Diese befinden sich in Düsseldorf und Frankfurt/Main beim Anbieter interxion sowie in Hamburg bei GlobalConnect und werden für direkte, d. h. PNI-Verbindungen zu anderen Netzen genutzt. Darüber hinaus bestehen dort Verbindungen zu den lokalen Internet Exchanges, in Düsseldorf zu ECIX, in Frankfurt/Main zu DE-CIX Frankfurt sowie zu DE-CIX Hamburg in Hamburg. Eine Anbindung des in Berlin ansässigen BCIX wird aktuell über eine Dark-Fibre-Verbindung vom X-WiN-Standort an der TU Berlin aus realisiert.

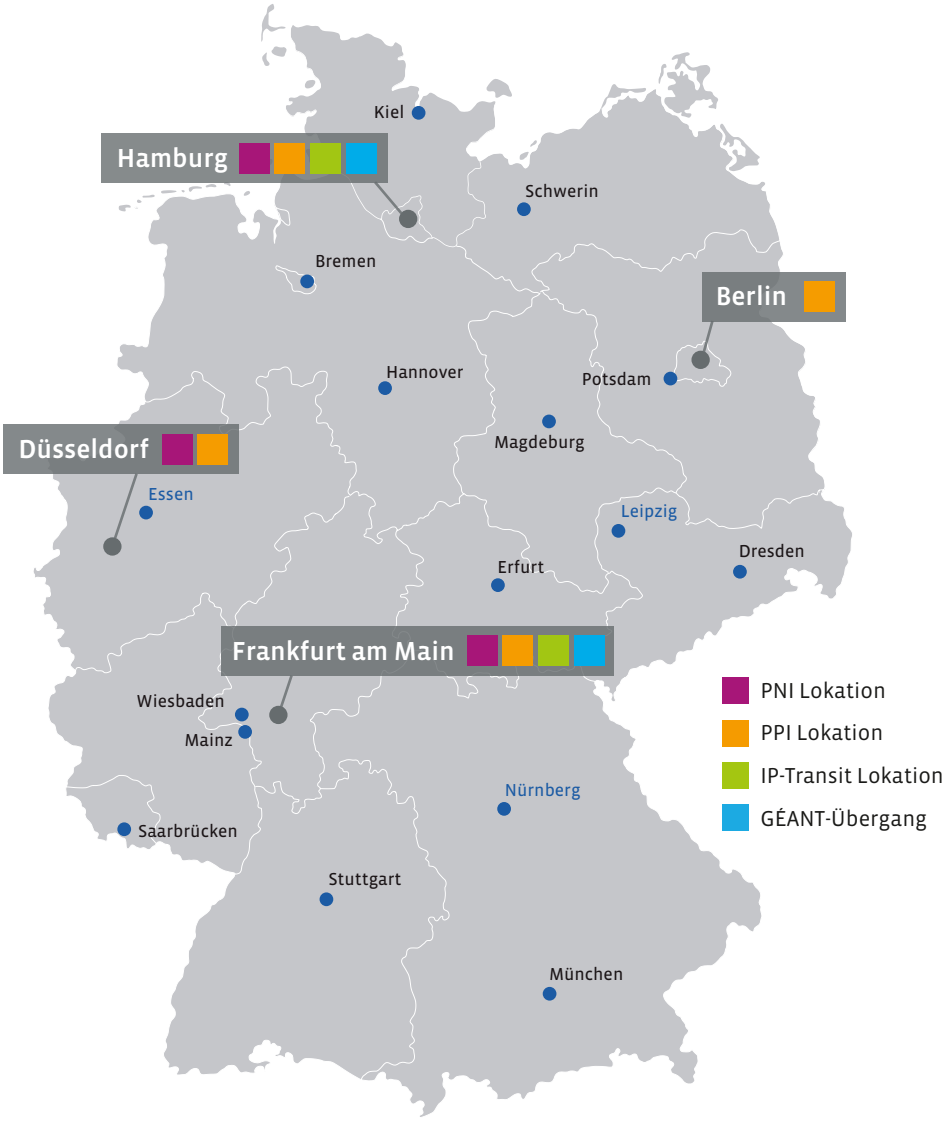


Abbildung 4: Peering-Lokationen des X-WiN in Deutschland

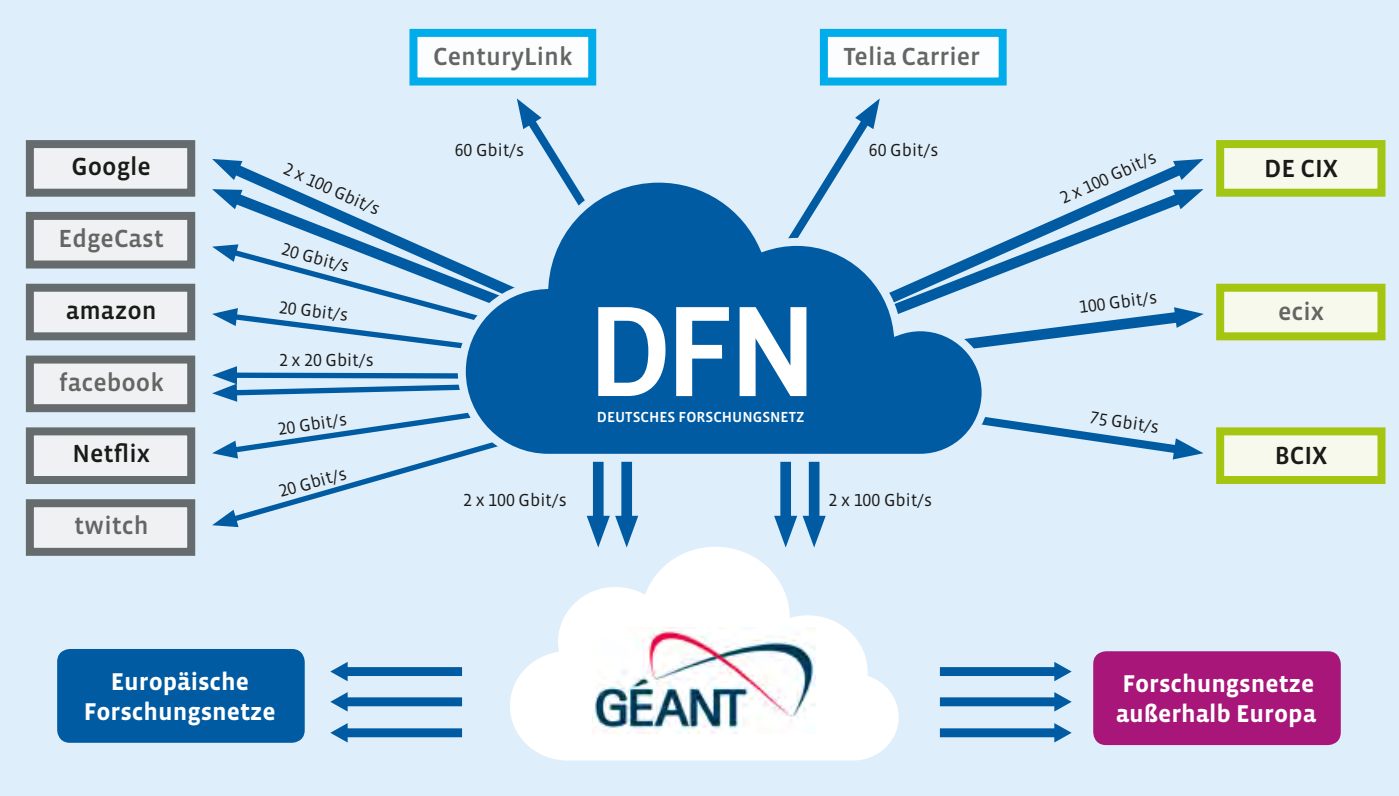


Abbildung 5: Außenanbindungen des X-WiN

Die Auswahl der IP-Transit-Anbieter für das Wissenschaftsnetz erfolgt auf der Basis der regelmäßig von GÉANT durchgeführten Ausschreibungen dieses Dienstes.

Die Netzübergänge der aktuellen Provider Telia Carrier und CenturyLink befinden sich in Frankfurt/Main und Hamburg. Zum europäischen Wissenschaftsnetz GÉANT erfolgt der Anschluss über Colocation-Center in Frankfurt/Main und Hamburg.

Die Gesamtkapazität der Außenanbindungen des X-WiN beträgt aktuell 1.215 Gbit/s (vgl Abbildung 5). Davon entfallen auf PNI 320 Gbit/s, auf PPI 375 Gbit/s und auf IP-Transit 120 Gbit/s. Mit insgesamt 400 Gbit/s (je 200Gbit/s in Frankfurt/Main und Hamburg) ist das X-WiN mit dem europäischen Wissenschaftsnetz GÈANT verbunden.

Entwicklung des Verkehrs über die Außenanbindungen des X-WiN

Aber spiegelt die Entwicklung der Verkehre über die Außenanbindungen des X-WiN die genannten Entwicklungen in der kommerziellen Welt wider und lässt sich die behauptete wachsende Bedeutung von internationalen Verbindungen zwischen NRENs verifizieren?

Seit Inbetriebnahme der ersten Netzgeneration des X-WiN im Jahre 2006 zeichnet der DFN-Verein die übertragenen Datenvolumina getrennt nach technischen Übergängen monatlich auf. Daraus lassen sich für die Außenanbindungen des X-WiN Trends über die letzten 13 Jahre analysieren, die wenig überraschend dem Wachstum des gesamten Verkehrs im X-WiN entsprechen. Wurden im Jahr 2006 etwa 2,3 Petabyte in Summe über die Außenanbindungen übertragen, waren es im Jahr 2018 bereits knapp 66,7 PB, was einem Faktor von etwa 30 und damit einem mittleren jährlichen Wachstum von 32 % entspricht.

Interessanter noch als diese absoluten Zahlen ist aber die unterschiedliche Entwicklung der verschiedenen Kategorien (vgl. Abbildung 6). Während der Verkehr über die IP-Transit-Anbindungen in dieser Zeit um einen Faktor von 7 zugenommen hat, stieg der Verkehr über die Peerings des X-WiN um einen Faktor von 38,4 an. Den größten Zuwachs aber hat der Verkehr zwischen dem X-WiN und den über GÉANT erreichbaren NRENs erfahren. Hier wurde ein Faktor von knapp 75 erreicht.

Gut nachvollziehen lässt sich diese Entwicklung auch bei Betrachtung der Verkehrsanteile, die über die Außenanbindungen des X-WiN in den einzelnen Monaten abgewickelt wurden (vgl. Abbildung 7). So hatte der IP-Transit-Verkehr im Januar 2006 noch einen Anteil von 48 % (Peering 35 %, GÉANT 17 %) am Gesamtverkehr über die Außenanbin-

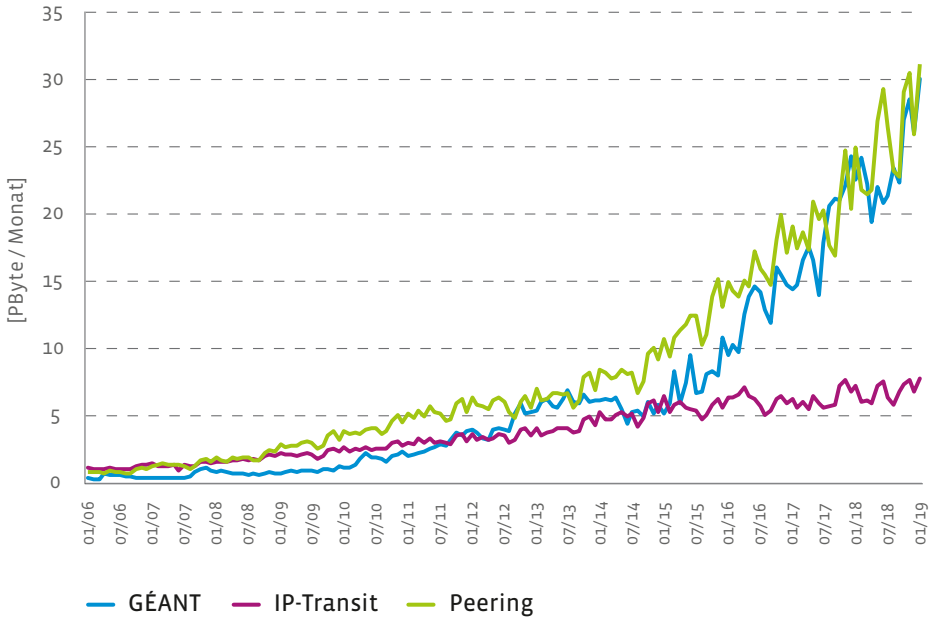


Abbildung 6: Verkehrsvolumina über Außenanbindungen nach Anbindungstyp im X-WiN

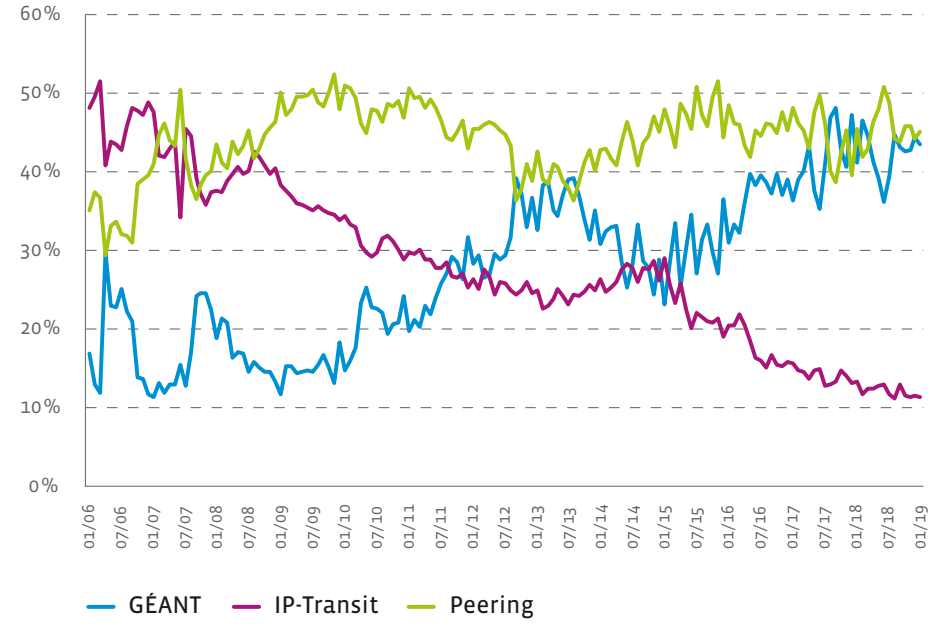


Abbildung 7: Anteile Verkehrsvolumina über Außenanbindungen nach Anbindungstyp im X-WiN

dungen des X-WiN, im November 2018 waren es nur noch 12 % (Peering 44 %, GÉANT 44 %).

Es bleibt insgesamt festzustellen, dass die Marginalisierung von Verkehr über IP-Transit, sprich über die sogenannten Tier-1-Carrier, auch im X-WiN stattfindet. Dieser Verkehr wird stattdessen zunehmend über Peerings abgewickelt. Die zweite und vielleicht die wichtigere Erkenntnis ist aber, dass der Verkehr zu anderen Forschungsnetzen, sowohl in Europa aber auch weltweit, in den letzten 13 Jahren relativ zum Gesamtverkehr noch deutlich stärker gewachsen ist als der „kommerzielle“ Verkehr. Dies untermauert noch einmal die Bedeutung von Forschungsnetzen und deren internationaler Vernetzung

Wie schon am Anfang des Artikels angedeutet, stellt das X-WiN jedoch auch für nicht rein wissenschaftlichen Datenverkehr ausreichend Kapazitäten zur Verfügung. Der generelle Trend, bewegte Bilder über das Internet zu beziehen, zeigte sich eindrucksvoll über die beim WM-Fußballspiel Deutschland – Südkorea an den Außenanbindungen gemessenen 195 Gbit/s Peak-Datenrate des u. a. von ARD/ZDF genutzten CDN Akamai.

Fazit

Die Peering-Strategie des DFN-Vereins – und damit die Außenanbindung des X-WiN – hat seit Inbetriebnahme des X-WiN vor 13 Jahren eine kontinuierliche Entwicklung durchlaufen, nun ist ein solider Reifegrad erreicht.

Ausgereifte Werkzeuge zur Analyse des Datenverkehrs und eingespielte Prozesse bei der Beobachtung von Trends im Markt und bei der Etablierung neuer Peerings sorgen auch in Ausnahmesituationen für stets bedarfsgerechte Dimensionierung der Außenanbindungen. Die Geo-Redundanz wichtiger Peerings sichert eine hochverfügbare Erreichbarkeit relevanter Netze.

Der DFN-Verein ist somit zuversichtlich, auch für die nächsten 13 Jahre des X-WiN angemessene Außenanbindungen bereitstellen zu können. ◆

Willkommen im DFN-Verein – Start für NHR-Geschäftsstelle

Die Nachfrage nach Rechenleistung hat in vielen Forschungsbereichen enorm zugenommen. So hat sich die Gemeinsame Wissenschaftskonferenz (GWK) von Bund und Ländern im Herbst 2018 auf die Förderung eines koordinierten überregionalen Verbundes von Hochleistungsrechenzentren der Ebene 2 verständigt. Mit der neuen Geschäftsstelle des Strategieausschusses für Nationales Hochleistungsrechnen (NHR) unter dem Dach des DFN-Vereins ist nun der Startschuss gefallen.

Text: **Barbara Diederich** (DFN-Verein, Leiterin NHR-Geschäftsstelle)

Am 1. April 2019 nahm die Geschäftsstelle des Strategieausschusses für Nationales Hochleistungsrechnen (NHR) ihre Arbeit auf. Als einer der zentralen Akteure der nationalen Forschungsinfrastrukturen erklärte sich der DFN-Verein auf Anfrage der Gemeinsamen Wissenschaftskonferenz (GWK) bereit, die Geschäftsstelle des Strategieausschusses in der Gründungsphase des künftigen NHR-Verbunds im Verein anzusiedeln und damit den Aufbau zu unterstützen. Das gemeinsam vom BMBF und dem DFN-Verein initiierte Projekt mit dem Titel „Geschäftsstelle für den Strategieausschuss in der Gründungsphase des NHR“ hat eine Laufzeit von zwei Jahren.

In vielen Wissenschaftsbereichen ist der Einsatz von Hochleistungsrechnern mittlerweile unverzichtbar, beispielsweise in Simulationsverfahren der Grundlagen- und Klimaforschung oder der Material- und Lebenswissenschaften. In der anwendungsorientierten Forschung sind die Bereiche Künstliche Intelligenz (KI) und Big Data auf HPC-Infrastrukturen angewiesen.

Um der zunehmenden Bedeutung und der steigenden Nachfrage nach Hochleistungsrechnen gerecht zu werden, hat sich die GWK im Herbst 2018 auf die gemeinsame Förderung eines koordinierten Verbundes des NHR durch Bund und Länder verständigt. Ziel ist es, die Rechenzentren der Ebene 2 in einer gemeinsamen Struktur zusammenzufassen und ein zukunftsfähiges Netzwerk von Hochleistungsrechnern zu errichten. Wissenschaftlerinnen und Wissenschaftler der deutschen Hochschulen sollen somit deutschlandweit und bedarfsgerecht auf die für ihre Forschung benötigte Rechenkapazität zugreifen können. Ein weiterer Schwerpunkt ist die Stärkung der Methodenkompetenz durch koordinierte Aus- und Weiterbildung der Nutzerinnen und Nutzer sowie insbesondere des wissenschaftlichen Nachwuchses. Die GWK folgt damit den Empfehlungen des Wissenschaftsrats von 2015 zur Finanzierung des Nationalen Hoch- und Höchstleistungsrechnens.

Insgesamt stellen Bund und Länder bis zu 62,5 Millionen Euro jährlich bereit. Geplant ist ein Förderzeitraum von grundsätzlich zehn Jahren, eine Weiterförderung ist möglich. Zwischenevaluierungen der Zentren und des NHR-Verbundes sind ebenfalls vorgesehen. Die Aufnahme in die Förderung soll in einem wettbewerblichen und wissenschaftsgeleiteten Auswahlverfahren in mehreren Runden erfolgen. Um die Einzelheiten des Verfahrens zu erarbeiten, wird die GWK einen Strategieausschuss einsetzen, dem sowohl wissenschaftliche Mitglieder als auch Vertreterinnen und Vertreter von Bund und Ländern angehören. Der Ausschuss wird unter anderem Empfehlungen zum Ausschreibungskonzept und den Förderkriterien, zur Evaluierung und Auswahl der NHR-Zentren sowie zu den zukünftigen Strukturen aussprechen. Die Begutachtung der Anträge der Zentren wird durch die Deutsche Forschungsgemeinschaft (DFG) erfolgen. Auf dieser Basis empfiehlt der Strategieausschuss der GWK Zentren zur Förderung. Die ersten NHR-Zentren werden voraussichtlich bis 2020 ermittelt.

Vorgesehen ist, dass die GWK in ihrer Sitzung am 3. Mai 2019 die wissenschaftlichen Mitglieder des Strategieausschusses beruft und die Vertretungen von Bund und Ländern bestellt. Die Geschäftsstelle wird den Strategieausschuss in der zweijährigen Gründungsphase des NHR-Verbunds bei seiner Arbeit administrativ unterstützen. ◆

Solar Digital Doorways – an entryway to information literacy

South Africa has not only an abundance of sunshine but also of struggling low-income communities. There is a huge disparity in the country between rich and poor, educated and illiterate. An ongoing need exists for facilities that afford opportunities to develop computer literacy and provide access to information. Many small towns and villages in South Africa are challenging to get to in terms of their remoteness. They are frequently affected by unstable or unavailable grid power. The Digital Doorway1 (DD) is a type of digital library or computer lab, fully powered by solar, and able to be deployed in some of the remotest towns and villages in the country. So it's a great complement to the various offers of the National Research and Education Networks (NRENs).

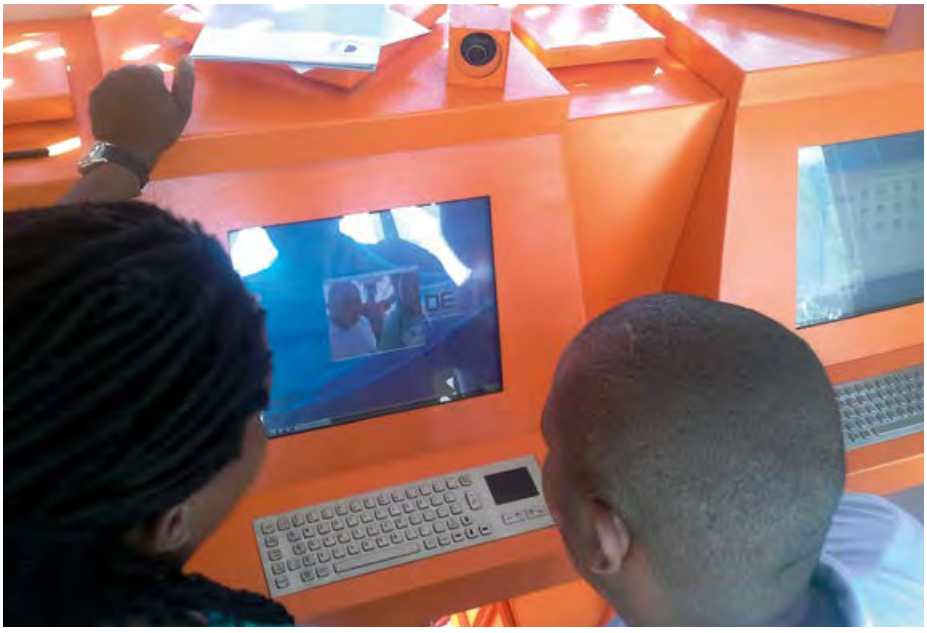
Text: **Kim Gush** (Council for Scientific and Industrial Research, CSIR)

Photograph showing the first solar-powered container Digital Doorway to be installed *(Foto © CSIR)*

"Self-learning" and "learning through exploration and play" – the DD Concept

A joint collaboration between South Africa's CSIR2 (Centre for Scientific and Industrial Research) and various government departments such as the Department of Science & Technology (DST) and the Department of Rural Development & Land Reform (DST, DRDLR) the Digital Doorway initiative commenced way back in 2002. The initial idea was one of "self-learning" and "learning through exploration and play", mainly in the fields of computer basics, mathematics and physical science. Figure 1 illustrates how this technology solution has developed over the years

with various hardware iterations being produced. One of the most versatile and successful versions being the solar-powered containerised unit currently installed around the country and still being rolled out in 2019. The system is a self-contained ICT lab and off-grid Wifi access point and content repository, provided as a free-resource to anyone within the vicinity.



Users at one of the internal user terminals *(Foto © Ingwapele Technologies)*

A tiny power house – the technology basics

The DD housing was designed to meet a number of challenges related to assembly, insulation, transportation, vandal and theft prevention and functionality.

Solar panels, deep-cycle batteries, solar charge controller and inverter provide power to the equipment, with connectivity being supplied via VSAT or Cellular (3G/LTE) depending on availability. The basic computer topology consists of a media server (content server), user terminals, Wifi access point and Internet modem. The steel plate that makes up the user terminals is laser-cut, welded and powder-coated. ISO-panels (a combination of Chromadek and Polistyrene) and other materials are cut and assembled into the housing structure. Solar panels are attached to the roof and each assembly is fitted with the various hardware components. After wiring, software installation, customisation and testing, the container is ready for transportation to site. A flat-bed truck delivers the container to site where it is lowered into place, final setup is initiated and the system is ready to be used.

Free and open-source – content and applications

One of the goals of the project is to allow users access to informative, entertaining and education information, both via the Internet and locally cached content in case of connectivity failure. This is achieved through a media server containing free and open-source applications and content. Smart phones have become extremely popular with young and old alike and the DD media server and WiFi access point provides a convenient hub of information at no cost to the user. Users connect their phone to the public access point at the container and point their browser to a specific web-page (hosted locally) for convenient access to a selection of content categories.

The content includes an ever-growing body of educational and informative material in a number of different fields from agriculture to engineering. Cached content includes a local encyclopaedia, learning materials, videos, PDF books and interactive material (e.g. PHET science simulations3).

Access to the Internet over WiFi is made available via a voucher system that entitles each user to one hour free Internet before they need to renew their voucher. This imposed restriction helps prevents the Internet connection being dominated by just a few individuals.

The “champion” assists the users – social challenges and feedback

The Digital Doorway initiative is a complex socio-technical challenge. Providing high-tech equipment in low-income remote areas requires adequate servicing and maintenance. A custodian of the site is appointed to oversee the computer installation. This so-called “champion” is responsible for locking and unlocking the housing, providing basic assistance to users, keeping the unit clean and providing feedback to the help-desk on issues arising at the site. The champions require training on computer basics and Digital Doorway specifics. This is an opportunity for these volunteers to improve their skills and possibly begin a career in information and computer technologies.

For many, the DD is the only traditional computer they have access to. Feedback from users within the villages provides valuable information about aspects of the installation that are not working properly (e.g. Internet going down) as well as very positive and encouraging remarks.

Real-time monitoring through a custom-designed dashboard

One of the big challenges for these installations is providing servicing and maintenance of the equipment over the long term. The network is serviced by a help-desk and maintenance team and relies on telephonic feedback from the on-site champion, as well as real-time monitoring of the network status through a custom-designed dashboard. The dashboard provides a visual map of the network with colour-coded representations of the status of the equipment. The monitoring is dependent on reliable connectivity to the site. While LTE equipment is suitable for most installations, certain sites are out of cellular coverage range and satellite is currently the only viable alternative. Support and maintenance teams rely on a suite of open-source tools for monitoring, asset tracking, site management and ticket logging. This is illustrated in the figure below.

Many hurdles, but much more benefit – Future and conclusion

Successfully providing computer equipment and access to useful and relevant information resources in low-income rural areas is no easy task. From unpredictable road access to equipment maintenance difficulties, financial constraints and social challenges, the hurdles are many. Any provision of complex technologies should be undertaken with adequate resources allocated to the administration and long-term support of those technologies. Where these hurdles are cleared, solar-powered containerised ICT solutions are a viable means of improving access to computer infrastructure and information, providing new opportunities for those willing to use them. ◆

Refs:

1. http://www.digitaldoorway.org.za
2. http://www.csir.co.za
3. https://phet.colorado.edu/en/simulations/category/physics

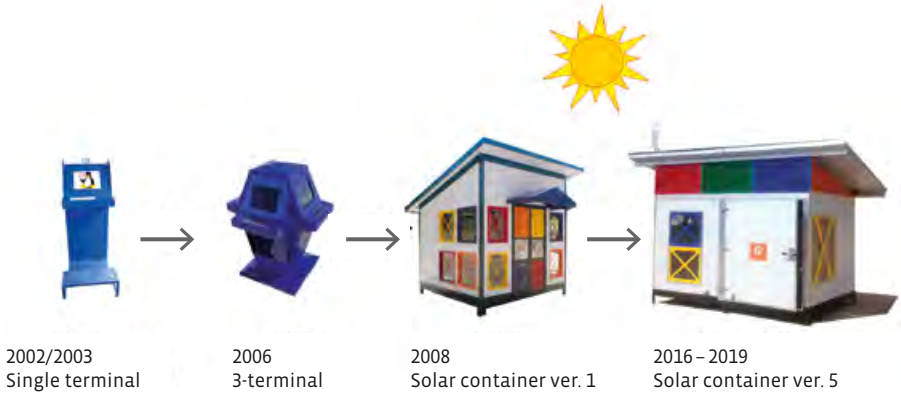


Figure 1: Digital Doorway technology iterations

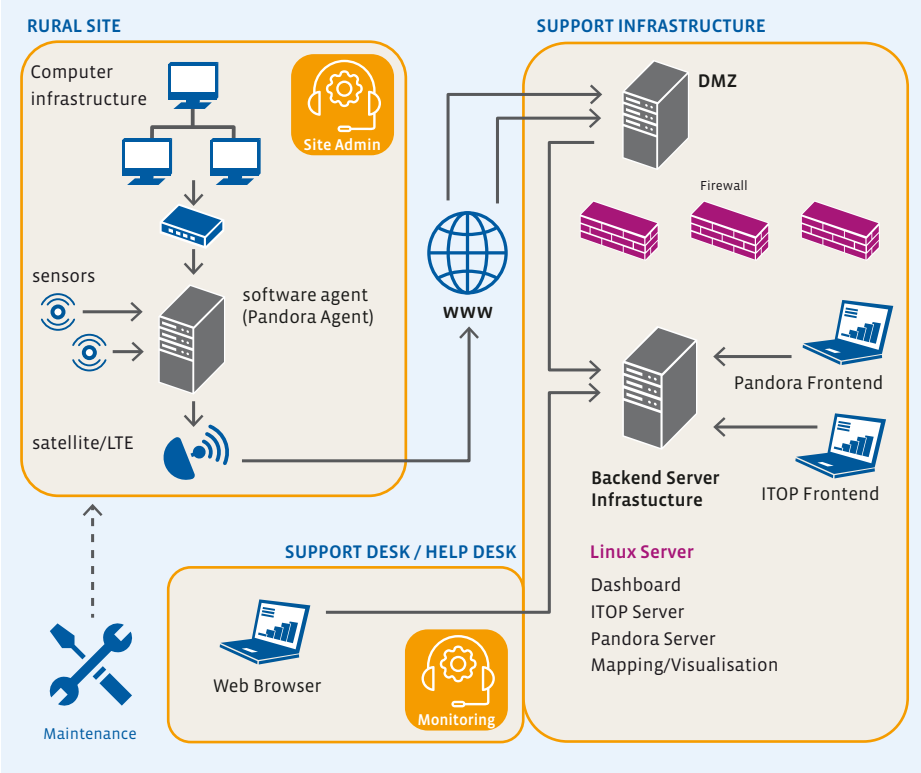


Figure 2: A suite of open-source tools for monitoring, asset tracking, site management and ticket logging

The Council for Scientific and Industrial Research, commonly known as the CSIR, is a world-class African research and development organisation established through an Act of Parliament in 1945. The CSIR undertakes directed, multidisciplinary research and technological innovation that contributes to the improved quality of life of South Africans. The CSIR's shareholder is the South African Parliament, held in proxy by the Minister of Science and Technology.

Der Netzwerker

Diplomat im Dienste der Forschungsnetze: Dr. Boubakar Barry ist CEO von WACREN *(Foto © WACREN)*

Dr. Boubakar Barry ist mit der Mission angetreten, die aktuellen Bandbreiten im Forschungs- und Bildungsbereich West- und Zentralafrikas zu verzehnfachen. Seit mehr als 13 Jahren hat sich der studierte Kernphysiker und Spezialist für Datenverarbeitung dem Thema Kommunikationsnetze verschrieben. Der Aufbau des Backbone-Netzes WACREN, West and Central African Research and Education Network, sowie die Anbindung und Unterstützung der Nationalen Forschungsnetze ist nicht nur eine Lebens-, sondern auch eine echte Herkulesaufgabe. Mit dem DFN-Verein entwickelt er ein Programm zur Kapazitätsentwicklung und Wissensvermittlung, das junge NRENs in West- und Zentralafrika dabei unterstützt, einen nachhaltigen Business- und Strategieplan zu entwickeln. Vor welchen Herausforderungen diese jungen Forschungsnetze, insbesondere WACREN, heute stehen, erzählt er im Interview. Dabei gibt es erstaunliche Parallelen zu den Anfängen des DFN-Vereins.

Als Netzwerkexperte haben Sie 2006 damit begonnen, eine Kommunikationsinfrastruktur für West- und Zentralafrika aufzubauen, seit 2013 sind Sie Chief Executive Officer (CEO) von WACREN. Was waren bisher Ihre größten Herausforderungen?

Wir sind als Wissenschaftsnetz noch sehr jung, sowohl WACREN als auch unsere NRENs. Das Thema ist neu in unseren Ländern. Um Regierungsvertreter von den Vorteilen zu überzeugen, muss ich einiges an Überzeugungsarbeit leisten. Mitunter braucht das sehr viel Zeit, unzählige Versammlungen und Konferenzen. Die Lobbyarbeit nimmt darum seit vielen Jahren einen Großteil meiner Tätigkeit in Anspruch. In den ersten Jahren, als wir noch kein Netz hatten, bin ich ständig umhergereist und habe viele Regierungsminister, Uni-

versitätspräsidenten und Direktoren von Rechenzentren getroffen, um sie zu überzeugen, den Aufbau der nationalen Forschungsnetze politisch und finanziell zu unterstützen. In unseren Regierungen gibt es eine große Fluktuation. Wenn ich endlich ein gewisses Verhandlungsniveau erreicht hatte, wechselte der entsprechende Minister,

> „Um Regierungsvertreter von den Vorteilen zu überzeugen, muss ich einiges an Überzeugungsarbeit leisten“

ein anderer kam und ich musste wieder ganz von vorne beginnen. Aber in Togo und der Elfenbeinküste waren wir sehr erfolgreich, das beruht auf persönlichen Beziehungen. Mit der Ministerin der Elfenbeinküste hatte ich schon zu tun, als sie noch Universitätsprofessorin war.

Ihr Plan ist, die aktuellen Bandbreiten für Forschungs- und Bildungseinrichtungen zu erhöhen. Auf welche Schwierigkeiten stoßen Sie dabei?
Nach wie vor ein großes Problem ist die Bereitstellung von Konnektivität mit ausreichenden Bandbreiten durch die hiesigen Internetanbieter am Markt. Ihre Monopolstellung führt dazu, dass es keinerlei Marktöffnung und damit Preisregulierung gibt. Das Internet ist viel zu teuer, das können sich unsere Universitäten und Forschungseinrichtungen einfach nicht leisten. Dazu kommt, dass die angebotenen Bandbreiten für Forschungszwecke viel zu gering sind. Das führt dazu, dass unsere Forscher im Prinzip isoliert sind, sowohl untereinander als auch, was die Teilnahme an weltweiten Forschungsprojekten angeht. Zum Beispiel verfügt die Universität in Abidjan/Elfenbeinküste mit rund 80 000 Studierenden über lediglich 100 Mbps, die Hochschule in Lomé/Togo mit etwa 50 000 Studierenden über weniger als 50 Mbps. Das ist leider die Regel. Für Forschungsvorhaben wie das Radioteleskopprojekt Square Kilometre Array (SKA), dessen Partner Ghana ist, und für viele andere Einrichtungen, die im Bereich Climate Change oder Genomix arbeiten, benötigen wir dringend Hochgeschwindigkeitsverbindungen. Darum ist es unser Ziel, die Bandbreiten mindestens zu verzehnfachen und vor allem weniger dafür zu bezahlen.

Wie wollen Sie das erreichen?
Mit einem langen Atem. Jahrelang standen wir in zähen Verhandlungen mit den Providern. Ständig fragten sie uns, wie viel Geld uns zur Verfügung stünde, erst dann könne man uns die Kosten nennen. Wir aber benötigten zuerst einen konkreten Preis für eine Kapazität von 10 Gbps, um wegen der Finanzierung mit unseren Mitgliedern reden zu können. Wir drehten uns ständig im Kreis – eine klassische Huhn-Ei-Situation. Die großen Bandbreiten, die langen Laufzeiten, das ging total über deren Horizont, da sie Kapazitäten von maximal 50 Mbps und Laufzeiten von höchstens drei Jahren gewohnt sind. Deren Politik ist ganz einfach: Bei einer langen Laufzeit multiplizieren sie die Kosten einfach dement-

> „Die großen Bandbreiten, die langen Laufzeiten, das ging über deren Horizont“

sprechend. Aber eigentlich sollte der Betrag logischerweise sinken. Immer wieder kam die misstrauische Frage, was wir überhaupt mit so viel Bandbreite anfangen wollen. In einigen Wochen sind wir endlich so weit, dass wir einen für uns befriedigenden Vertrag unterschreiben können. Das waren sehr langwierige und schwierige Verhandlungen.

Wie haben Sie das letztendlich geschafft?
Im Regionalverbund der NRENs sind wir zwar ein starker Ansprechpartner für die Provider, aber erst mit der finanziellen Unterstützung von AfricaConnect2 war es uns möglich, mit ihnen auf Augenhöhe über langfristige, stabile und kostengünstige Verträge zu verhandeln. Mit einem Gesamtbudget von 26,6 Millionen Euro (davon 20 Millionen von der Europäischen Kommission), aufgeteilt in drei Cluster für Ost- und Südafrika, West- und Zentral- sowie Nordafrika, unterstützt das Projekt die Entwicklung von nationalen und regionalen Forschungsnetzen auf dem Kontinent. WACREN ist der Cluster 2, hier reden wir über etwa 12 Millionen Euro Budget.

Was hat momentan Priorität für Sie?
Neben dem Aufbau des physikalischen Netzes müssen wir parallel das Angebot der Services, wie zum Beispiel Internet, Videoconferencing, eduroam oder Cybersecurity, vorantreiben. Wir denken auch über Cloud Services wie Hosting

> „Wir wollen unseren Einrichtungen zeigen, welche Vorteile wir im Gegensatz zu den privaten Anbietern haben“

nach, mit unserem Cluster in Lagos/Nigeria haben wir einen Piloten gestartet. Wir wollen unseren Einrichtungen zeigen, welche Vorteile wir im Gegensatz zu den privaten Anbietern haben – nämlich bedarfsgerechtere und vor allem günstigere Angebote. Damit die Einrichtungen die Qualität der Services testen können, stellen wir diese ein paar Monate gratis zur Verfügung und bieten anschließend Verträge an. Diese können wir unseren Anwendern nur deshalb so günstig anbieten, weil wir über AfricaConnect2 die Unterstützung haben.

Es geht also sehr schnell vorwärts.
Und das erzeugt wiederum ganz andere Probleme. Gemessen an den vielen komplexen Aufgaben, haben wir nur sehr geringe Personalressourcen. Bisher schaffen es nur wenige NRENs, ihre Leute in

Vollzeit zu beschäftigen, deren CEOs beispielsweise arbeiten oft nur halbtags. Das sind in der Regel Uniprofessoren, IT-Direktoren, allgemein Techis. Sie werden von ihren Institutionen den NRENs in Teilzeit zur Verfügung gestellt, müssen aber ihre eigentliche Arbeit zusätzlich erledigen. Von Businessplänen oder Ähnlichem haben sie wenig Ahnung. „Capacity Building“, der Aufbau von Wissen, Strukturen und Fähigkeiten, ist hier das Stichwort: Was wir benötigen, sind nicht nur ausreichend Mitarbeiterinnen und Mitarbeiter in Vollzeit, sondern auch, diese möglichst gut auf ihre künftigen Aufgaben vorzubereiten – insbesondere wenn die Services jetzt richtig ins Laufen kommen. Darum haben wir in letzter Zeit sehr viele Workshops, insbesondere auf der technischen Seite, angeboten.

Zusätzlich entwickeln wir derzeit ein Capacity-Building-Programm für WACREN, damit unter anderem unsere CEOs lernen, Wirtschafts- und Strategiekonzepte für ihre NRENs zu erstellen. Das ist auch der Grund meines Besuchs in Berlin. Der erste Workshop soll schon im Oktober in Kooperation

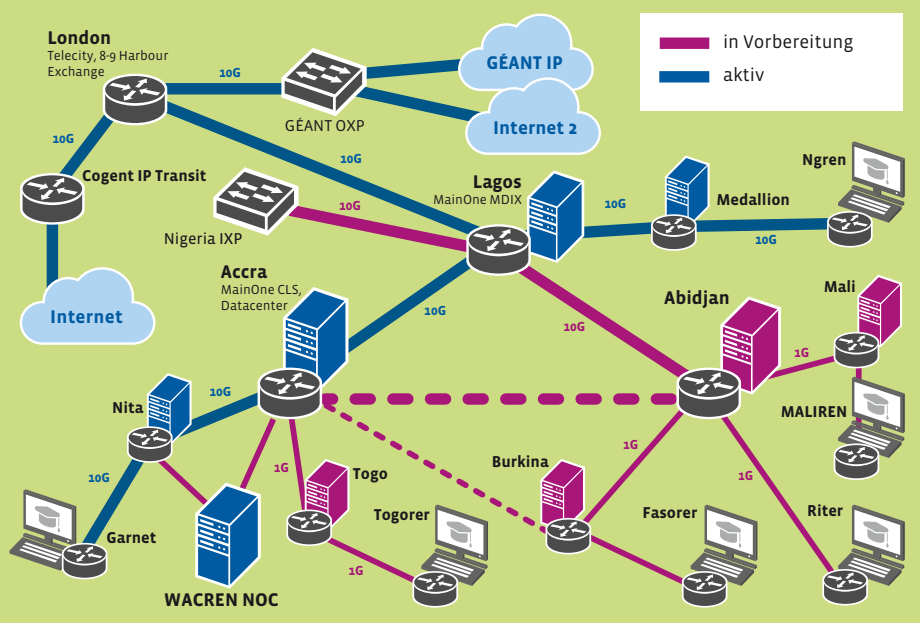
> „Lange bevor es ein physikalisches Netz gab, haben wir es geschafft, ein humanes Netzwerk aufzubauen“

mit dem DFN-Verein in Ghana stattfinden. Das ist großartig. Wir würden uns freuen, wenn der DFN-Verein in der dritten Phase von AfricaConnect vielleicht sogar assoziierter Partner wird.

Was sind rückblickend Ihre größten Erfolge?

Lange bevor es ein physikalisches Netz gab, haben wir es geschafft, ein humanes Netzwerk aufzubauen, das Netzwerk einer sehr starken Gemeinschaft in West- und Zentralafrika. Ich glaube, das ist das Wichtigste. Mittlerweile gehören 13 Länder in der Region zu WACREN, am Ende der Projektlaufzeit werden es 16 sein. Wo vorher eine NREN-Wüste war, konnten wir in vielen Ländern Decision Maker, wie Minister, Operatoren und Provider, überzeugen und sogar an einen Tisch bringen. Wir haben ihnen gezeigt, dass wir nicht nur Kunden für Bandbreite sind, sondern starke Partner.

Das Interview führten
Maimona Id und **Leonie Schäfer**



Aktueller Stand der WACREN-Netzwerkarchitektur (März 2019)

AFRICACONNECT2

Ziel: Die Aufgabe von AfricaConnect2 ist es, die Entwicklung, Konsolidierung und den Betrieb leistungsfähiger nationaler und regionaler Netze für Wissenschaft, Forschung und Lehre in Afrika zu unterstützen und Verbindungen zum europäischen Netzwerk GÉANT herzustellen. Dazu gehört unter anderem, die Konnektivität zu verbessern und damit den wissenschaftlichen weltweiten Austausch Afrikas zu fördern. GÉANT übernimmt im Cluster 2 sowie dem Nachfolgecluster 3 administrative, finanzielle und operationale Aufgaben. Das Projekt verfolgt einen modularen Ansatz und umfasst drei geografische Cluster mit ihren jeweiligen regionalen Netzwerkorganisationen:

- ASREN in Nordafrika,
- WACREN in West- und Zentralafrika,
- UbuntuNet Alliance in Ost- und Südafrika.

→ Förderzeitraum: 3,5 Jahre,
→ Fördersumme: Das Gesamtbudget beträgt 26,6 Millionen Euro, davon stellt die Europäische Kommission 20 Millionen bereit. Die regionalen Netze leisten jeweils eine Eigenbeteiligung, die sich bei WACREN auf rund 2,5 Millionen Euro beläuft.

Kurzmeldungen

GN4-3 – GÉANT-Projekt geht in die nächste Phase über

Das europäische Wissenschaftsnetz GÉANT steht für eine erfolgreiche europaweite Zusammenarbeit und wird im Rahmen von Horizon 2020 gefördert. Das aktuelle GÉANT-Projekt GN4-3 startete im Januar 2019 mit einer Laufzeit von 48 Monaten und 39 Projektpartnern. Die zuvor beendete Projektphase GN4-2 erhielt von der EU-Kommission im März erneut die Bewertung „Exzellent". GN4-3 verfügt über ein Budget von 119 Mio. Euro bestehend aus 77 Mio. Euro Förderung durch die EU und 42 Mio. Euro Eigenanteil der beteiligten Partner.

Das Projekt GN4-3N hat zusätzlich die Aufgabe, den weiteren Ausbau des gesamteuropäischen Netzwerks zu planen und dafür möglichst langfristige Verträge für die Anmietung von Glasfaserleitungen zu vereinbaren. Hier ist ein Budget von rund 63 Mio. Euro inklusive einer EU-Beteiligung von 50 Mio. Euro vorgesehen.

Ziel der GÉANT-Partner ist es, den Stand der Technik in den Bereichen Networking und Service Innovation voranzutreiben. Das GÉANT-Netzwerk verbindet heute Europas Forschungsnetze (NRENs) mit Geschwindigkeiten von bis zu 500 Gbit/s und erreicht NRENs in mehr als der Hälfte aller Länder weltweit.

Das aktuelle GÉANT-Projekt GN4-3 beinhaltet folgende Schwerpunkte:

- die Weiterentwicklung und den Betrieb des europäischen Forschungs- und Bildungsnetzes bei gleichzeitiger Verbesserung der Kosteneffizienz,
- Unterstützung höchster Datenkapazität für kommende Großprojekte, wie die nächste Ausbaustufe des Teilchenbeschleunigers Large Hadron Collider (LHC) und des Radioteleskops Square Kilometre Array (SKA),
- Verbreitung von Big Data-Anwendungen in der Wissenschaft,
- Unterstützung von Exascale-Höchstleistungsrechnen durch optimale Vernetzung,
- Beitrag zu einem integrierten Dienste-Angebot europäischer e-Infrastrukturen,
- Föderierte Trust- und Identity-Lösungen, die Anwendern die nahtlose Nutzung der angebotenen e-Infrastruktur-Dienste ermöglichen.

Es werden jedoch nicht nur technische Schwerpunkte gesetzt. Ein wichtiger Aspekt ist die Förderung der Community-Aktivitäten zwischen Forschern und Forschungsnetzen. Ein Highlight ist beispielsweise die jährlich stattfindende TNC-Veranstaltung – The Networking Conference. Sie ist die größte europäische Konferenz der Forschungs- und Bildungsnetzwerke mit zuletzt etwa 800 Teilnehmern; sie findet dieses Jahr im Juni in Tallinn statt (https://tnc19.geant.org/).

Darüber hinaus bietet das GÉANT Community-Programm mit seinen Task Forces (TFs) und Special Interest Groups (SIGs) viele Möglichkeiten der Beteiligung an den aktuellen Projekten von GÉANT. ◆

Nach der Ausschreibung ist vor der Ausschreibung – kommerzielle Cloud Services in OCRE

Im dritten Quartal dieses Jahres findet im Projekt OCRE (Open Clouds for Research Environments) erneut eine europaweite Ausschreibung kommerzieller Cloud Services statt. In der Rolle des zentralen Beschaffers leitet die Dachorganisation der europäischen Forschungsnetze GÉANT diesen Prozess. Die Vorbereitungen dazu laufen bereits seit Januar 2019.

Konkret werden folgende Leistungen ausgeschrieben:

- Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS),
- Earth Observation Services (Infrastrukturen für die Auswertung von bspw. COPERNICUS- Satelliten- Daten),
- Virtual Learning Environment (VLE)-Lösungen und Lern-Management-Systeme.

Forschungseinrichtungen, Hochschulen und Universitäten erhalten die Möglichkeit, zentral koordinierte kommerzielle Cloud Services in ihrer Einrichtung anzubieten. Damit entfällt der initiale Aufwand des Ausschreibungsverfahrens für sie.

Erstmalig haben europäische Forschungsnetze bereits 2016 ihre Anforderungen an kommerzielle Cloud Services zusammengetragen. Die Laufzeit der daraus resultierenden Rahmenvereinbarungen ist auf vier Jahre begrenzt worden und endet mit Ablauf des Jahres 2020. Im aktuell anstehenden Verfahren sollen die in 2016 gesammelten Informationen sowie die bereits während der praktischen Umsetzung gemachten Erfahrungen für den Fortbestand des Bezugsweges sorgen.

Sie benötigen weitere Informationen oder haben grundsätzliche Fragen? Sie sind auf der Suche nach spannenden Anwendungsszenarien oder möchten mit uns und anderen Einrichtungen über das Thema „Clouds im wissenschaftlichen Umfeld" diskutieren? Dann registrieren Sie sich über den folgenden Link http://cloud.dfn.de/ocre für die Teilnahme auf unserer Mailingliste! Übrigens wird zurzeit die finale Leistungsbeschreibung formuliert: Nehmen Sie über cloud@dfn.de Kontakt mit uns auf und sorgen Sie dafür, dass Ihre Bedarfe rechtzeitig darin berücksichtigt werden können! ◆

Sicherheit

Prävention, Erkennung und Reaktion – Informationssicherheit im DFN

Sowohl die Teilnehmer am Deutschen Forschungsnetz als auch die Geschäftsstelle des DFN-Vereins unterliegen, insbesondere im Bereich der Informationssicherheit, sich wandelnden externen sowie internen Anforderungen. Diese ergeben sich aus der steigenden Komplexität der einzelnen Dienste sowie der Digitalisierung von immer mehr Geschäftsprozessen, die ohne die informationstechnischen Systeme zum Erliegen kommen. Die Aspekte Verfügbarkeit, Integrität und Vertraulichkeit dieser Dienste und der dort verarbeiteten Daten gehören zu den klassischen Säulen der Informationssicherheit. Der DFN-Verein bietet den Teilnehmern in Zusammenarbeit mit dem DFN-CERT nicht nur einen Anschluss an das Wissenschaftsnetz, die internationalen Forschungsnetze sowie das öffentliche Internet, sondern auch eine Vielzahl von sicherheitsorientierten Zusatzdiensten, die überwiegend ohne zusätzliches Entgelt im Dienst DFNInternet enthalten sind.

Text: **Ralf Gröper** (DFN-Verein)

Foto © D-Keine/iStockphoto

An der Hochschule Pellworm geht gar nichts mehr: Das Immatrikulationsamt müht sich vergeblich, auf die Studierendendaten zuzugreifen. Das Institut für Hochenergiephysik kann die aktuellen Messdaten des CERN-Teilchenbeschleunigers Large Hadron Collider plötzlich nicht mehr herunterladen. Die Biologen verpassen wegen des IT-Ausfalls die Deadline für die elektronische Einreichung eines Papers für das Nature Magazine. Was ist passiert? Ein Angriff auf die Informationssysteme hat die Hochschule – trotz umfangreicher präventiver Sicherheitsmaßnahmen – lahmgelegt. Potenzielle Angreifer sind viele denkbar: Ist es eine exmatrikulierte Studentin, die sich an der Hochschule rächen will, oder gar eine kriminelle Vereinigung, die die Hochschule erpressen möchte? Obwohl das Krisenmanagement der Uni greift – der Angriffsvektor kann mithilfe einer Logfile-Analyse identifiziert, die Infektion der betroffenen Systeme entfernt und die kritischen Systeme können erfolgreich wieder in Betrieb genommen werden – entsteht ein signifikanter Schaden: Nicht nur finanziell, auch die Reputation der Hochschule leidet erheblich. Ein fiktiver Fall an einer fiktiven Hochschule, der aber durchaus realistisch erscheint und zeigt, wie wichtig es ist, Managementsysteme für Informationssicherheit und Datenschutz kontinuierlich weiterzuentwickeln und zu verbessern.

Anforderungen an die Informationssicherheit

Die Anforderungen an die Informationssicherheit sind in den vergangenen Jahren an vielen Stellen gestiegen. Das betrifft nicht nur die Umsetzung einer Vielzahl an Einzelmaßnahmen wie beispielsweise einem organisierten Patch-Management oder der Einführung einer VPN-Richtlinie, sondern darüber hinaus oft auch die formale Nachweisbarkeit des erreichten Sicherheitsniveaus.

Externe Faktoren

Externe Anforderungen an die Informationssicherheit lassen sich unter dem Stichwort „Compliance" – damit ist die Einhaltung von Gesetzen und Richtlinien, aber auch von freiwilligen Kodizes gemeint – zusammenfassen. Die für den DFN-Verein und seine Teilnehmer relevanten Regeln ergeben sich unter anderem aus den folgenden Gesetzen, die der Gesetzgeber entweder komplett neu erlassen oder in den vergangenen Jahren zumindest deutlich erweitert und verändert hat:

- **IT-Sicherheitsgesetz:** Die DFN-PKI, aber auch viele Teilnehmer wie Universitätskliniken, gelten als Kritische Infrastrukturen (KRITIS) und unterliegen damit besonderen Anforderungen.
- **EU-Datenschutzgrundverordnung, DSGVO:** Auch wenn die deutschen Datenschutzgesetze bereits vor der Einführung der DSGVO ein hohes Datenschutzniveau sichergestellt hatten, ergeben sich durch das Gesetz erweiterte Anforderungen.
- **Telekommunikationsgesetz, TKG:** Das TKG wurde im Rahmen des IT-Sicherheitsgesetzes ebenfalls angepasst. Hieraus ergeben sich Auswirkungen sowohl auf die Dienste des DFN-Vereins als auch auf die seiner Teilnehmer.
- **Telemediengesetz, TMG:** Zu den im TMG geregelten Telemedien gehören (nahezu) alle Angebote im Internet. Auch dieses Gesetz wurde angepasst, sodass die Anforderungen an Dienstanbieter steigen.

Interne Faktoren

Interne Quellen für steigende Anforderungen an die Informationssicherheit sind ebenfalls zu beobachten. Diese setzen sich unter anderem aus den folgenden Aspekten zusammen:

- **Erhöhte Komplexität der Dienste:** Selbst wenn die Anforderungen an das Sicherheitsniveau nicht steigen, wächst aufgrund der steigenden Komplexität der bereitgestellten Dienste der Aufwand, der getrieben werden muss, um das Sicherheitsniveau konstant sicherzustellen.
- **Wachsende Anforderungen an die Verfügbarkeit:** Die Anforderungen an die Verfügbarkeit der informationstechnischen Dienste ist in den vergangenen Jahren kontinuierlich gestiegen. Geschäftsprozesse, die beispielsweise vor einigen Jahren noch analog auf Karteikarten durchgeführt wurden, sind nun vollständig IT-gestützt, wie etwa die Studierendenverwaltung mithilfe der Immatrikulationsämter.
- **Steigende Anforderungen an die Integrität und Vertraulichkeit:** Die Integrität der Daten ist Voraussetzung für viele Kernprozesse an Hochschulen. So muss beispielsweise sichergestellt werden, dass Prüfungsergebnisse den betreffenden Studierenden korrekt zugewiesen und nicht nachträglich manipuliert werden können. Die Anforderungen an die Vertraulichkeit ergeben sich durch die Datenschutzgesetze, aber insbesondere auch aus der Notwendigkeit, die Reputation der

DIE DREI ÜBERGEORDNETEN DFN-ZIELE IN DER INFORMATIONSSICHERHEIT:

→ **Schutz des X-WiN und der DFN-Serverinfrastruktur:** Der DFN-Verein betreibt das X-WiN und die Infrastruktur für die weiteren DFN-Dienste im Auftrag von Forschung und Lehre in Deutschland. Aus diesem Grund ist es wichtig, diese Infrastrukturen zu schützen, das heißt Probleme zu erkennen und zu lösen, die sich auf die Verfügbarkeit auswirken könnten. Dieses stellen wir durch die DFN Security Operations sicher.

→ **Schutz der am DFN teilnehmenden Organisationen:** Der DFN schützt nicht nur die eigenen Infrastrukturen, sondern auch die IT-Landschaft der Teilnehmer. Der DFN-Verein informiert über Schwachstellen in IT-Systemen und kann auf Sicherheitsvorfälle reagieren und daran arbeiten, sie zu entschärfen, um die Teilnehmer und deren Nutzer zu schützen.

→ **Hilfe für am DFN teilnehmende Organisationen, um sich selbst zu schützen:** Der DFN-Verein bietet nicht nur direkten Schutz, sondern ermöglicht auch den Zugang zu einer Reihe zusätzlicher sicherheitsbezogener Dienste. Damit können die Teilnehmer ihre eigenen Informationssicherheitsprozesse um geeignete Aspekte erweitern.

Einrichtung zu schützen – ein kompletter Datenbankabzug der Prüfungsergebnisse einer Hochschule von einem öffentlichen Server birgt nicht zuletzt das Risiko eines negativen Medienechos.

Um diese Anforderungen nachhaltig umsetzen zu können, wird ein Informationssicherheitsmanagementsystem (ISMS) benötigt, das auf der Basis erlangter Erfahrungen und auf dem jeweiligen Stand der Technik kontinuierlich weiterentwickelt werden muss. Es kann sich an etablierten Standards, wie ISO27001 oder BSI-Grundschutz, ausrichten und durch eigene Best Practices gestützt werden. Ebenso fordert die DSGVO die Einführung eines Managementsystems für den Datenschutz. In jedem Fall werden Dienste und Daten von außen benötigt, um die Maßnahmen, die sich aus den Managementsystemen ergeben, umsetzen zu können. Das unterstützt der DFN-Verein durch eine Reihe von Diensten, die gemeinsam die Prävention, Erkennung und Abwehr von Sicherheitsvorfällen bei den Teilnehmern, aber auch beim DFN selber, zum Ziel haben. Die zugehörige Toolchain wird als „Security Operations“ bezeichnet.

Security Operations im DFN

Die sicherheitsbezogenen DFN-Dienste in den Kategorien „Prävention“, „Erkennung“ und „Reaktion“ greifen ineinander und unterstützen dabei die lokalen Managementsysteme, Risiken zu minimieren. Ein Risiko besteht aus dem Produkt der Eintrittswahrscheinlichkeit eines Schadens sowie der Höhe des Schadens. Risiken zu minimieren bedeutet also, einen oder beide Faktoren zu minimieren:

- durch **Prävention**: Sie senkt die Eintrittswahrscheinlichkeit.
- durch schnellstmögliche **Detektion** eines Sicherheitsvorfalls und eine effiziente **Reaktion**: Sie minimieren die Schadenshöhe, falls der Schaden trotz Prävention eintritt.

Nach Eintritt eines Sicherheitsvorfalls gilt es außerdem, seine Ursachen aufzuklären, um die Eintrittswahrscheinlichkeit zukünftiger ähnlich gearteter Sicherheitsvorfälle durch angepasste Präventivmaßnahmen nachhaltig senken zu können. Dafür betreiben der DFN-Verein und das DFN-CERT eine Reihe von Tools mit darauf basierenden Diensten im Bereich der Informationssicherheit.

Wie diese Dienste im Rahmen eines geeigneten Managementsystems in einer Institution sinnvoll eingesetzt werden können, unterscheidet sich stark von Einrichtung zu Einrichtung. Gefördert durch den DFN-Verein gibt es einen regen Erfahrungsaustausch unter den Teilnehmern. Darüber hinaus steht das DFN-CERT mit seiner Expertise vielen Einrichtungen mit Rat und Tat zur Seite, die ein Managementsystem für Informa-

Status	Prävention	Detektion	Reaktion
Derzeit verfügbar	• Schwachstellenmeldungen • Netzwerkprüfer • DFN-MailSupport • DFN Trusted Identity-Dienste (DFN-PKI, DFN-AAI, eduroam) • Grundsätzliche Verschlüsselung von Kommunikationen der weiteren DFN-Zusatzdienste (VoIP, DFNconf, ...) • Awareness und Schulung (Tutorien, Konferenzen, Tagungen, Publikationen	• Automatische Warnmeldungen • DFN-DoS-Analyseplattform	• Incident Response • DFN DoS-Basisschutz • DoS-Schutz des X-WiN
in Vorbereitung		• DFN-SOC-Tools (Einführungsphase DFN-intern, Dienst für Teilnehmer in der Konzeptphase)	• Dediziertes Security Operations Center (Konzeptphase)

Tabelle 1: DFN-Dienste und Tools mit Sicherheitsbezug

tionssicherheit oder Datenschutz einführen oder ausbauen wollen.

Eine Übersicht über diese Dienste findet sich in Tabelle 1 sowie auf den Webseiten des DFN-Vereins unter https://www.cert.dfn.de/secops/. Die weiterführenden Links verweisen direkt auf jeden der hier aufgeführten Dienste.

Ausblick

Das Werkzeug zur zentralen Erkennung von Angriffen auf Basis von Threat Intelligence[1] wird derzeit in Kooperation mit dem DFN-CERT aufgebaut. Es soll zunächst das bereits bestehende hohe Schutzniveau (siehe BSI-Grundschutz-Zertifizierung des DFN-MailSupport-Dienstes) in der DFN-eigenen Serverlandschaft besonders bei der Erkennung von Angriffen weiter verbessern. Von der hierfür aufgebauten Infrastruktur zur Auswertung von Log- und anderen Rohdaten und zum (selbstverständlich datenschutzkonformen) Abgleich mit den aus der Threat Intelligence gewonnenen sogenannten Indicators of Compromise (IoC)[2] sollen zukünftig auch Teilnehmer am DFN profitieren.

Für die Realisierung des Angebots ist eine detaillierte Anforderungsanalyse notwendig, die eine Befragung der DFN-Teilnehmer beinhaltet (siehe hierzu „Fünf Fragen an die Teilnehmer“). Die Infrastruktur, die derzeit aufgebaut wird, ist darauf ausgelegt, Alarme automatisch zu generieren und den jeweiligen Dienstverantwortlichen zuzustellen. Zukünftig ist es vorstellbar, dieses in einem Security Operations Center (SOC) zu zentralisieren und die Qualität der Alarme durch manuelle Voranalyse weiter zu verbessern oder höhere Verfügbarkeitsanforderungen in Richtung 24/7-Betrieb umzusetzen. Das wird aber nur durch die vertrauensvolle Kooperation mehrerer Einrichtungen umgesetzt werden können – allein schon aufgrund von finanziellen Aspekten. Der DFN-Verein ist bereit, hier mit dem DFN-CERT eine zentrale Rolle einzunehmen, um der Wissenschaftslandschaft in Deutschland eine angemessene Antwort auf die steigenden Risiken der Informationssicherheit zu geben. ◆

FÜNF FRAGEN AN DIE TEILNEHMER:

- Haben Sie ein SOC oder haben Sie darüber nachgedacht, eines einzurichten oder einzukaufen?
- Können Sie sich grundsätzlich vorstellen, dem DFN-CERT Zugriff zu Log-Daten zur Angriffserkennung und -aufklärung zu gewähren?
- Dürfte der DFN-Verein bzw. das DFN-CERT Dritte (z. B. kommerzielle Anbieter) als Unterauftragnehmer miteinbeziehen? Falls ja: Nur deutsche/europäische Anbieter? Anbieter aus Drittstaaten?
- Wünschen Sie einen erweiterten Dienst (z. B. 24/7-Erreichbarkeit, manuelle Voranalyse der Alarme durch ein gemeinsames SOC) gegen zusätzliches regelmäßiges Entgelt?
- Wünschen Sie einen Basisdienst, bei dem nur ein kleineres regelmäßiges Entgelt anfällt für die notwendige lokale Sensorik in Ihrem Netz? Hinweis: Hierbei wird die Erkennungsrate niedriger und/oder die False-Positive Rate höher sein als beim erweiterten Dienst mit manueller Voranalyse.

Antworten bitte per E-Mail (sicherheit@dfn.de) oder telefonisch direkt an Ralf Gröper (030-884299-337) geben.

1 Threat Intelligence ist evidenzbasiertes Wissen über eine bestehende oder sich abzeichnende Bedrohung für informationstechnische Systeme.
2 Indicators of Compromise (IoC) sind die technischen Merkmale eines Angriffs auf informationstechnische Systeme. Sie sind Teil der Threat Intelligence.

Datenverkehr kennt keine Grenzen – Cybersecurity-Regulierung international

Cybersicherheit ist ein Thema jenseits von Landesgrenzen. Dies wird nicht nur anhand der regelmäßig wiederkehrenden Vorfälle in verschiedenen Nationalstaaten deutlich, sondern ist vielmehr eine dem grenzüberschreitenden Datenverkehr innewohnende Tatsache. In den letzten Jahren haben es sich deshalb zahlreiche Länder, aber auch die Europäische Union zum Ziel gemacht, neue und teils umfassende gesetzliche Vorgaben zur Cybersicherheit aufzustellen. Der vorliegende Beitrag gibt einen Überblick über die bisherigen gesetzgeberischen Initiativen in der EU, in Deutschland, Russland, China sowie den USA und stellt die verschiedenen Ansätze einander vergleichend gegenüber.

Text: **Dennis-Kenji Kipker** (Universität Bremen)

Foto © sakura/adobestock

I. Deutschland und Europäische Union

Die deutsche und europäische Gesetzgebung in der Cybersicherheit hängen eng miteinander zusammen – dies ist letztlich auch der Tatsache geschuldet, dass das IT-Sicherheitsgesetz (IT-SiG, 2015) in Deutschland nur in etwa ein Jahr vor der EU-Richtlinie zur Netz- und Informationssicherheit (NIS-RL, 2016) in Kraft getreten ist, sodass die Entwicklungen rund um den deutschen Rechtsakt auch das entsprechende EU-Gesetzgebungsverfahren beeinflussen konnten. Darüber hinaus hat die Europäische Union in den vergangenen Jahren zwei weitere Gesetzesentwürfe zur Cybersicherheit vorgelegt, deren Verabschiedung zum Zeitpunkt der Erstellung dieses Beitrages noch aussteht: die EU-Cybersecurity-Verordnung (sog. „Cybersecurity Act“) und den Vorschlag für die Verordnung zur Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit.

1. Deutsches IT-Sicherheitsgesetz

Ziel des am 25. Juli 2015 in Kraft getretenen IT-SiG ist die signifikante Verbesserung der IT-Sicherheit in Deutschland. Als Artikelgesetz enthält es selbst keine unmittelbaren Vorgaben für Unternehmen und Bürger, sondern modifiziert verschiedene Einzelvorschriften wie zum Beispiel das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG). Ergänzt werden die Vorgaben des IT-SiG durch die BSI-Kritisverordnung (BSI-KritisV), die als vom Bundesministerium des Innern (BMI) erlassenes „Behördenrecht“ den Anwendungsbereich der gesetzlichen IT-Sicherheitspflichten konkretisiert. Das IT-SiG wird 2019 durch das IT-SiG 2.0 erweitert, ein erster Referentenentwurf dieses Gesetzes wurde Anfang April veröffentlicht.

2. EU-Richtlinie zur Netz- und Informationssicherheit 2016/1148

Auch das europäische Recht der Cybersicherheit ist nicht in einem einzelnen Gesetz geregelt, sondern findet sich über zahlreiche allgemeine und bereichsspezifische Vorschriften mit einem unterschiedlichen Detaillierungsgrad verteilt.[1] In diesem Zusammenhang besonders hervorzuheben ist die EU-Richtlinie 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“ (NIS-RL), die im August 2016 in Kraft getreten ist und die politische Cybersicherheitsstrategie der EU nach schwerwiegenden IT-Sicherheitsvorfällen wie „WannaCry“ und „Petya“ auf eine klare gesetzliche Grundlage stellt. Die NIS-RL dient laut der EU-Kommission als globaler Ansatz, um gemeinsame Mindestanforderungen für Betreiber wesentlicher und digitaler Dienste festzulegen. Neu ist dabei insbesondere die Regulierung der digitalen Dienste, wozu Suchmaschinen, Online-Marktplätze und Cloud-Computing-Anbieter gehören. Die NIS-RL wurde mit dem „Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 06.06.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ im April 2017 in das nationale Recht überführt.

3. EU-Cybersecurity-Verordnung (Entwurf)

Mit der neuen EU-Cybersicherheitsstrategie wurde im September 2017 zugleich auch der Entwurf eines neues Rechtsakts vorgestellt, die Verordnung „über die EU-Cybersicherheitsagentur (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit)“, gemeinhin auch als „Cybersecurity-Verordnung“ oder „Cybersecurity Act“ bezeichnet. Kernelement des Gesetzesentwurfs, der im März 2019 vom Europäischen Parlament angenommen wurde und voraussichtlich noch im Frühjahr 2019 verabschiedet wird, ist die Schaffung eines europaweit einheitlichen Zertifizierungsrahmens für die IT-Sicherheit von Produkten und Diensten der Informations- und Kommunikationstechnik, um die Sicherheit und das Vertrauen in den digitalen

[1] Eine entsprechende Auflistung findet sich im „IT-Security NAVIGATOR“ wieder, der als Forschungsprojekt in Kooperation der Universität Bremen mit VDE|DKE entstanden ist, siehe https://www.itsecuritynavigator.de/.

Binnenmarkt zu stärken wie auch den gemeinsamen europäischen Markt weiter zu harmonisieren. Inhaltlich wird bei der Zertifizierung zwischen einer Selbstbewertung der Konformität durch den Hersteller oder Anbieter sowie einer Drittzertifizierung unterschieden. Generell ist ein Durchlaufen des Zertifizierungsverfahrens freiwillig, es sei denn, dass IKT-Produkte oder -Dienste im Zusammenhang mit Kritischen Infrastrukturen betrieben werden. Für die Zertifizierung wird zwischen den drei Anforderungsniveaus „niedrig", „mittel" und „hoch" unterschieden. Die Selbstbewertung durch den Hersteller oder Diensteanbieter ist dabei nur für das Zertifizierungsniveau der Sicherheitsstufe „niedrig" möglich.

4. EU-Verordnung zur Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit (Entwurf)

Ein weiterer aktueller Gesetzesentwurf auf EU-Ebene trägt den Titel „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren". Im Zentrum dieses Verordnungsentwurfs steht die Schaffung eines neuen EU-Kompetenzzentrums für Cybersicherheit, das vorrangig der europäischen Forschung in diesem Bereich dienen soll, indem es Nutzer aus der gesamten Union sowohl aus der Industrie als auch aus dem öffentlichen Sektor sowie aus der Forschung und Wissenschaft durch seine fachliche Kompetenz und finanzielle Fördermaßnahmen unterstützt. Die Abgrenzung zur eher im operativen Feld tätigen ENISA soll dadurch gewährleistet werden, dass sich das Kompetenzzentrum in erster Linie auf die Wissenschaft fokussiert.

II. Russische Föderation

Die beiden russischen Cybersicherheitsstrategien – Cybersecurity Doctrines – stammen aus den Jahren 2000[2] und 2016[3]. Während das erste Dokument kaum für die Cybersicherheit relevante Informationen enthält, greift die zweite Cybersecurity Doctrine das Thema umfassend auf und bildet zugleich auch die politische Grundlage für das neue russische Cybersicherheitsgesetz. Auffällig ist in diesem Zusammenhang, dass Russland nicht wie die EU vor allem den Schutz von wirtschaftlichen Interessen in den Mittelpunkt stellt, sondern in seinem Handeln insbesondere auf die Lenkung politischer Interessen in Staat und Gesellschaft sowie auf militärische Ziele ausgerichtet ist. Dies begründet auch die enge Verknüpfung der russischen Cybersicherheitsstrategie mit der allgemeinen nationalen Sicherheitsstrategie der Russischen Föderation[4].

Das neue russische Cybersicherheitsgesetz „Federal Law on Security of Critical Russian Federation Information Infrastructure"[5] ist am 1. Januar 2018 in Kraft getreten und greift die Vorgaben der Cybersecurity Doctrine aus 2016 verbindlich auf. Dabei sollen nicht nur die kritischen Informationsinfrastrukturen des Landes abgesichert werden, sondern es soll vielmehr das Fundament gelegt werden für ein funktionierendes staatliches Informationssicherheitssystem, das sich der Erkennung, Vorbeugung und Beseitigung der Folgen von Cyber-Angriffen gegen die IT-Strukturen der Russischen Föderation verschrieben hat, gelegt werden. Inhaltlich schaffen die neuen gesetzlichen Regelungen mit dem deutschen IT-SiG und mit der EU-NIS-RL teils vergleichbare Vorgaben[6], indem einerseits verschiedene Rechte und Pflichten für Diensteanbieter bestimmt werden, die andererseits mit einem Ausbau behördlicher Kontroll- und Weisungsrechte zur Überprüfung der neuen gesetzlichen Anforderungen einhergehen. Gegenüber dem IT-SiG sowie der NIS-RL erfährt das Gesetz in seinem Anwendungsbereich eine Ausdehnung, indem auch die Sektoren Verteidigung, Bergbau und Chemie explizit den kritischen Informationsinfrastrukturen zugerechnet werden.

[2] Information Security Doctrine of the Russian Federation, approved by President of the Russian Federation Vladimir Putin on September 9, 2000, abrufbar unter: https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (Stand: 11.02.2019). [3] Decree of the President of the Russian Federation No. 646 of December 5, 2016, abrufbar unter: http://www.mid.ru/en/foreign_policy/official_documents// asset_publisher/CptICkB6BZ29/content/id/2563163 (Stand: 11.02.2019). [4] Decree of the President of the Russian Federation No. 683 of December 31, 2015. [5] No. 187 FZ. [6] Siehe dazu auch schon Kipker, ZD-Aktuell 2016, 05261; Kipker, ZD-Aktuell 2016, 05363; Kipker, MMR-Aktuell 2017, 394677.

III. Volksrepublik China

China gehört weltweit zu jenen Staaten, die das Thema Cybersicherheit bereits seit Jahrzehnten adressieren. Zwar wurde die öffentliche Diskussion hierüber bisher vorwiegend durch das 2016 verabschiedete und im Juni 2017 in Kraft getretene chinesische Cybersicherheitsgesetz (Chinese Cybersecurity Law, CSL) geprägt, jedoch existieren im Reich der Mitte unzählige Vorschriften mit IT-Sicherheitsbezug. Beispielhaft seien an dieser Stelle nur die Computer Information System Security Protection Regulations of the People's Republic of China aus dem Jahr 1994 genannt. Auffällig bei einer Betrachtung der chinesischen Gesetzgebung ist, dass eine Vielzahl unterschiedlichster, teils bereichsspezifischer Vorschriften zur gleichen Zeit erarbeitet wird, so zum Beispiel aktuell das chinesische Kryptografiegesetz. Hierdurch wird es gerade ausländischen Unternehmen erschwert, einen adäquaten Überblick über das dortige Compliance-Gefüge zu erlangen. Eine zweite Besonderheit liegt im Charakter chinesischer Gesetze: Während hierzulande nicht selten möglichst konkrete Gesetze angestrebt werden, erfüllen entsprechende chinesische Vorschriften stärker die Funktion eines allgemeinen Rechtsrahmens, der vorwiegend durch untergesetzliches Behördenrecht und durch technische Normen und Standards ausgefüllt wird. Im Bereich Cybersicherheit ist für die technische Konkretisierung der rechtlichen Vorgaben vor allem das Chinesische Nationale Normungskomitee zur technischen Standardisierung der Informationstechnologie (TC 260) zu nennen, das unmittelbar der chinesischen Cyber-Sicherheitsbehörde CAC untersteht.

Im Zusammenhang mit dem Chinese Cybersecurity Law stellen sich aktuell verschiedene Einzelprobleme dar, die zum Teil auch aus der faktischen Wirkung des Gesetzes über Landesgrenzen hinweg resultieren. So war in den vergangenen Monaten immer wieder von einer flächendeckenden „Abschaltung" von VPN-Verbindungen zwischen Deutschland und China die Rede, mit der Folge, dass sensible Unternehmensdaten von in China tätigen ausländischen Konzernen zukünftig nur noch per „analoger Botenpost" auf USB-Sticks zwischen den Ländern transferiert werden könnten, was erhebliche Einbußen in der internationalen Wettbewerbsfähigkeit zur Folge hätte. Auf längere Sicht steht in diesem Zusammenhang ferner die Frage im Raum, wie sich die Nutzung chinesisch-staatlich lizensierter VPNs durch ausländische Unternehmen entwickelt. So will das chinesische Ministry of Industry and Information Technology (MIIT) die nationalen Anbieter von Telekommunikationsdiensten dazu verpflichten, in Zukunft keine ungenehmigten VPNs in ihren Netzwerken zu nutzen. Auch ist zu vermuten, dass das chinesische Kryptografiegesetz nach seinem Inkrafttreten erhebliche Auswirkungen auf transnationale Datenübermittlungen haben wird.

Für deutsche und EU-Unternehmen relevant ist neben der Frage der zukünftigen Handhabung von VPN-Verbindungen die neue chinesische Produktzertifizierung, die verhältnismäßig strenge Regeln für IT-Importe nach China schafft. Laut CSL müssen teils verschiedene Behörden „kritische Netzwerkausrüstung" und „spezifische Cybersicherheitsprodukte" überprüfen und zertifizieren, bevor sie auf dem chinesischen Markt vertrieben oder innerhalb Chinas eingesetzt werden dürfen. Welche Produkte hiervon im Einzelnen betroffen sind, regelt ein erstmals im Jahr 2017 veröffentlichter Produktkatalog, der unter anderem Router, Switches, Server, Firewalls und Anti-Spam-Produkte ab einer festgelegten Leistungsgrenze aufzählt. Für von der chinesischen Zertifizierungspflicht betroffene deutsche Unternehmen haben die neuen Bestimmungen zur Folge, dass sie bei einer akkreditierten und für die IT-Sicherheitszertifizierung zuständigen Stelle in China einen entsprechenden Zertifizierungsantrag einreichen müssen.

Hervorzuheben ist ferner auch die im CSL enthaltene Pflicht zur Datenlokalisierung, soweit es um solche Daten geht, die im Rahmen des Betriebs von kritischen Informationsinfrastrukturen anfallen. So wird in Art. 37 des Gesetzes festgeschrieben, dass derlei Datenbestände grundsätzlich im chinesischen Inland zu speichern sind – es sei denn, ein Auslandsdatentransfer ist aus zwingenden Gründen notwendig. Unklar ist zurzeit außerdem, ob die Pflicht zur Datenlokalisierung zukünftig über die in Art. 31 CSL definierten kritischen Informationsinfrastrukturen hinaus erweitert wird.

IV. Vereinigte Staaten von Amerika

Auch die Cybersecurity-Rechtsetzung in den USA zeichnet sich dadurch aus, dass zurzeit kein einheitliches Gesetz zur IT-Sicherheit existiert, sondern sich die entsprechenden Compliance-Vorgaben sowohl aus politischen Strategien wie auch aus verbindlichen gesetzlichen Anforderungen ergeben – sowohl auf Bundesebene wie auch auf Ebene der einzelnen Bundesstaaten.[7] Dazu kommen verschiedene Selbstregulierungsmaßnahmen der freien Wirtschaft. Als grundlegende politische Strategie wurde 2016 der „Cybersecurity National Security Action Plan" (CNAP) veröffentlicht, der längerfristige Maßnahmen und Strategien zum Schutz gegen Cyberangriffe vorsieht. 2013 wurde die Executive Order 13636 „Improving Critical Infrastructure Cybersecurity" erlassen, die Maßnahmen speziell zum Schutz kritischer Infrastrukturen enthält. Darüber hinaus fördert der „Cybersecurity Enhancement Act" von 2014 die freiwillige Zusammenarbeit von staatlichen und privaten Stellen zur Verbesserung der IT-Sicherheit im Sinne einer Public-private Partnership (PPP). Unter der Trump-Administration wurde im November 2018 zudem der „Cybersecurity and Infrastructure Security Agency Act" verabschiedet, und gegenwärtig wird im US-Senat ein neuer „IoT Cybersecurity Improvement Act" diskutiert.

Auf föderaler Ebene existiert in den USA eine Reihe von sektorspezifischen Vorschriften zur Cybersicherheit. Beispielhaft zu nennen sind hier der „Health Insurance Portability and Accountability Act" (HIPAA, 1996) für den Bereich der Gesundheitsdaten, der „Financial Services Modernization Act" (Gramm-Leach-Bliley Act, 1999 inkl. der Safeguards Rule, 2003) für den Bereich der persönlichen Finanzinformationen, der „Federal Information Management Act" (FISMA, 2002) für die Datenverarbeitung durch Bundesbehörden und der „Cybersecurity Information Sharing Act" (CISA, 2015) zum Austausch IT-sicherheitsbezogener Informationen zwischen Regierung und Unternehmen. Auf Ebene der einzelnen Bundesstaaten ist insbesondere Kalifornien als nationaler Vorreiter in Sachen IT-Sicherheits- und Datenschutzregulierung hervorzuheben. So wurde hier jüngst das erste IoT Cybersecurity-Gesetz erlassen, das 2020 in Kraft treten wird.[8]

V. Fazit und Ausblick

Cybersicherheit ist nicht nur ein technisch-organisatorisches, sondern vor allem auch ein juristisches Thema, was aber erst in den letzten Jahren mehr und mehr deutlich geworden ist, indem globale Herausforderungen die Nationalstaaten zur Förderung der Cybersicherheitsregulierung bewegen. Dabei werden zahlreiche und durchaus verschiedene inhaltliche Ansätze verfolgt, die von punktuellen, themen- und branchenspezifischen Regelungen bis hin zu ganzheitlichen Regulierungsansätzen reichen, die auch Datenschutz- und Zertifizierungsfragen in sektoren- und branchenübergreifender Hinsicht adressieren, reichen. So weit die jeweilige nationalstaatliche Regulierung aber auch geht, wird man nicht umhinkommen, ebenso auf transnationaler Ebene weitere Vorgaben und Richtlinien zu schaffen, um den grenzüberschreitenden Cybersicherheitsbedrohungen angemessen zu begegnen. Hier leistet die EU mit ihrem aktuellen Maßnahmenkatalog wertvolle Pionierarbeit. Aber auch Nationalstaaten wie Israel zeigen mit dem Entwurf eines neuen Cybersicherheitsgesetzes „Memorandum on Cyber Protection and the National Cyber Directorate Act, 5778-2018", der explizit auch den internationalen Informationsaustausch einbezieht, den Weg auf, in welche Richtung es in Zukunft beim Thema Cybersicherheit und Recht gehen wird. ◆

[7] Dazu ausführlich Fischer/Kipker/Voskamp, in: Kipker (Hrsg.), Cybersecurity: Rechtshandbuch, Kap. 16 (im Erscheinen). [8] Vgl. die Ergänzung des California Civil Code in Sections 1798.91.04–06.

Sicherheit aktuell

DFN-CERT: Gestiegene Zahl an Datenlecks und Phishing-Kampagnen

Die Anfang des Jahres unter dem Namen „Collection #1“ veröffentlichte Sammlung von mehreren hundert Millionen Datensätzen mit gültigen E-Mail-Adressen (und oft auch Passwörtern im Klartext) zeigt einen neuen Trend im Datenhandel auf: Sammlungen aus verschiedenen Datenlecks werden massenhaft zusammengefasst angeboten und vertrieben. Unter dem Schutz der imaginären Anonymität des Darknets kann alle Welt solche Daten veräußern und die Qualität der Sammlungen ist oft entsprechend mäßig. In den Sammlungen finden sich viele Daten aus Jahre zurückliegenden Vorfällen, Duplikate und etliche Einträge unterschiedlicher E-Mails mit identischem, scheinbar zufälligem Passwort. Letzteres lässt darauf schließen, dass die Daten zum Teil konstruiert oder die zugehörigen Passworte noch nicht dechiffriert wurden – möglicherweise, um die zum Verkauf angebotene Sammlung künstlich aufzublähen. Einige der Datenhändler beobachten den Markt genau und halten neue Datensätze zurück, bis sich die Aufregung über die massiven Datenlecks in den Medien gelegt hat. Auf diese Weise lassen sich frische Daten besser verkaufen. Über das DFN-CERT werden in jedem Fall, in dem das Incident Response Team Zugriff auf derartige Daten erhält, Informations-E-Mails an die Administratoren der betroffenen Einrichtungen gesendet. Das Hasso-Plattner-Institut in Potsdam bietet darüber hinaus einen Dienst an (https://sec.hpi.uni-potsdam.de/ilc/search?lang=de), mit dem Betroffene die eigene E-Mail-Adresse prüfen können.

Foyer des HPI Potsdam *(Foto © HPI/Kay Herschelmann)*

Die schiere Menge an Daten ermöglicht aber auch andere „Geschäftsmodelle“, was sich beispielsweise an der deutlich gestiegenen Zahl an gezielten Phishing-Kampagnen im vergangenen Jahr zeigt. Hierbei werden Anwender über oft sehr überzeugend gestaltete E-Mails zum Aufruf ebenso schlüssiger Webseiten verleitet und geben dort unbedarft ihre Benutzerdaten an. Die sensitiven Daten werden im Hintergrund gespeichert, die betroffenen Nutzer werden auf die eigentliche Log-in-Seite weitergeleitet und dort zum Teil auch automatisch eingeloggt. Das System versorgt sich selbst mit neuen Daten, die weiterverkauft, zum Versenden unerwünschter Werbemails oder von Erpressungstrojanern verwendet werden können. Oft werden die Daten auch benutzt, um die Online-Adressbücher der betroffenen Nutzer abzugreifen und so an gültige neue E-Mail-Adressen und potenzielle neue Angriffsziele zu kommen. Der Vorgang bleibt häufig unbemerkt und zeigt sich erst in der nächsten Runde der Kampagne, in der die auf diese Weise erhaltenen Daten verwendet werden, um noch überzeugendere Nachrichten zu senden und die Reichweite der Kampagne zu vergrößern.

Die Werkzeuge für solche Kampagnen stehen mittlerweile offen im Netz. Mit Tools wie „Modlishka“ und „evilginx2“ können ohne großen Aufwand eigene Phishing-Kampagnen gestaltet werden. Dieses könnte eine Chance zur Schaffung eines Bewusstseins für das Problem mittels einer „ethischen“ Phishing-Kampagne sein, die auf die eigene Institution zugeschnitten ist. Durch sorgfältig vor- und nachbereitete Kampagnen wird das Problem wesentlich präsenter als durch einen im täglichen Nachrichtenfluss untergehenden Bericht zu einem weiteren Datenleck oder einer neuen Phishing-Kampagne.

Bei Problemen mit Phishing-Kampagnen hilft das DFN-CERT gern bei der Eindämmung des Problems durch Kontakt zu den jeweiligen Hostern und Providern. Betroffene haben die Möglichkeit, die entsprechende E-Mail oder einen Link zur Kampagnenseite an cert@dfn-cert.de mit der Bitte um Unterstützung weiterzuleiten. ◆

eduroam: TLS und SSLs

Seit dem 30. Juni 2018 entspricht das Transport-Layer-Security-(TLS-)Protokoll in der Version 1.0 bzw. das Secure-Socket-Layer-(SSL-)Protokoll in der Version 3.1 nicht mehr dem Payment Card Industry Data Security Standard (PCI DSS). Diese Sicherheitsprotokolle werden nicht nur im Bereich der Bezahlsysteme eingesetzt. Im Rahmen des Dienstes eduroam kommen diese Protokolle in den RADIUS-Servern bei der Authentifizierung der eduroam-Nutzer und bei der Absicherung der Kommunikationswege zwischen den RADIUS Security (RadSec) Client/Servern zum Einsatz.

Die DFN-Geschäftsstelle in Berlin hat in den letzten Monaten bereits reagiert und die Infrastruktur RadSec Client/Server angepasst. Die RadSec Client/Server bieten nun das sichere Protokoll TLS1.2 an. Wegen der Abwärtskompatibilität werden weiterhin auch die Protokolle TLS1.1 und TLS1.0 erforderlich sein, um die Kommunikation zwischen den RadSec Client/Servern des DFN-Vereins und den Einrichtungen, die den Dienst eduroam anbieten, abzusichern.

Scans in der eduroam-Infrastruktur in den letzten Wochen, durchgeführt von der DFN-Geschäftsstelle in Berlin, haben gezeigt, dass viele Einrichtungen auf ihren RadSec Client/Servern das TLS1.2 nicht unterstützen. Jede Einrichtung, die eduroam anbietet, kann mit folgendem Kommandoaufruf prüfen, ob der RadSec Client/Server bereits das TLS1.2 unterstützt:

openssl s_client -connect ihre_radsecproxy_ip_adresse:2083 -tls1_2

Wenn TLS1.2 nicht unterstützt wird, antwortet das openssl-Kommando mit der Ausgabe, hier als Auszug dargestellt:

SSL-Session:
Protocol: TLSv1.2
Cipher: 0000
Master Key:

Sind Master Key und Cipher angegeben, so wird das TLS1.2 unterstützt und es ist nichts weiter zu unternehmen. Andernfalls sollte der RadSec Client/Server alsbald mit einer aktuellen openssl Library › 1.0.0 verlinkt werden.

TLS1.2 für den Einsatz in RADIUS Servern gestaltet sich schwieriger, da das Keying aus dem TLS1.2-Standard offensichtlich nicht in allen RADIUS Servern korrekt übernommen wurde. Aber auch viele vor allem ältere eduroam Clients unterstützen das TLS1.2 nicht. Somit ist davon abzuraten, TLS1.2 auf RADIUS zu aktivieren.

Bisher sind keine Angriffsvektoren bei TLS1.0 bzw.TLS1.1, die in eduroam ausgenutzt werden können, bekannt.

Weitere Informationen zu den Schwachstellen in TLS1.0 können unter folgendem Link genauer recherchiert werden:
https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls ◆

DFN-PKI: Übergang der DFN-PKI von Generation 1 zu Generation 2

Ende Juni/Anfang Juli 2019 (abhängig von der konkreten CA) läuft die erste Generation der DFN-PKI Global aus. Die DFN-PCA hat in der Vergangenheit alle Teilnehmer auf dieses Datum vorbereitet. Die zweite Generation der DFN-PKI steht seit November 2016 zur Verfügung. Am 2. September 2018 war die Anzahl der aktiven Zertifikate in der zweiten Generation erstmals größer als die in der ersten Generation.

Trotzdem wird das Ablaufen einer größeren Anzahl noch nicht ausgetauschter Zertifikate in den nächsten Wochen voraussichtlich zu einem erhöhten Arbeitsaufwand beim Teilnehmerservice führen. ◆

DFN-PKI: Diskussionsgruppe dfnpki-d

Um den Teilnehmern der DFN-PKI ein Forum zum Austausch zu geben, wurde die E-Mail- Diskussionsliste „dfnpki-d“ eingerichtet. Wir möchten hiermit die Verbreitung von Wissen und Informationen rund um die Nutzung von X-509-Zertifikaten in Wissenschaft und Forschung fördern und laden Sie ein, die Liste zu abonnieren und aktiv mitzudiskutieren. ◆

DFN-CERT: Emotet – neue Tendenzen der Schadsoftware und statische Analyse der verwendeten bösartigen Makros

Emotet ist bereits 2014 entdeckt worden, unterscheidet sich allerdings in vielen Facetten von anderer Schadsoftware. Ein Merkmal dieser Schadsoftware ist, dass sich sowohl ihre Eigenschaften als auch die Durchführung der Angriffe ständig ändern. So richten sich die Angriffe nicht nur gegen Endanwender, sondern stellen auch für Firmen und Universitäten eine große Bedrohung dar. Weiterhin wird Emotet aktuell dazu verwendet, zusätzliche Schadsoftware nachzuladen, die sich auch aktiv in Netzwerken verbreiten kann.

Als Reaktion auf Emotet sind vom DFN-CERT zwei Beiträge erschienen: Unter dem Link https://www.dfn-cert.de/aktuell/emotet-beschreibung.html werden die Facetten und Eigenschaften zusammengefasst, die diese Schadsoftware so besonders machen. Dieser Artikel beinhaltet u. a. zahlreiche weiterführende Links, z. B. zur Allianz für Cybersicherheit, die eine gute und umfassende Zusammenfassung der Maßnahmen zum Schutz vor Emotet veröffentlicht hat.

Die initiale Infektion erfolgt in der Regel über ein Microsoft-Office-Dokument mit bösartigen Makros. In einem weiteren Beitrag unter https://www.dfn-cert.de/aktuell/malicious-macros-emotet.html zeigen wir daher, wie diese Makros extrahiert und analysiert werden können. ◆

KONTAKT

Wenn Sie Fragen oder Kommentare zum Thema „Sicherheit im DFN“ haben, schicken Sie bitte eine E-Mail an **sicherheit@dfn.de**

MITARBEIT AN DIESER AUSGABE DER SICHERHEIT AKTUELL:

DFN-CERT: Jürgen Brauckmann, Stefan Kelm, Jan Kohlrausch, Klaus Möller, Martin Waleczek
DFN-Verein: Heike Ausserfeld, Ralf Gröper, Ralf Paffrath

heiCLOUD – die Brücke zwischen Forschung und IT-Dienstleistung

Mit heiCLOUD wurde an der Universität Heidelberg ein Cloud-Angebot etabliert, das speziell an die Bedürfnisse von Forschung und Lehre angepasst ist. Im Sinne des Konzepts Infrastructure-as-a-Service können Wissenschaftlerinnen und Wissenschaftler innerhalb weniger Minuten eigenständig virtuelle IT-Ressourcen beziehen, konfigurieren und verwenden. Die flexible Abrechnung über ein On-Demand-Modell ermöglicht es hierbei, ein nachhaltig finanziertes Angebot bereitzustellen. Seit diesem Frühjahr steht heiCLOUD nun auch als föderierter Dienst in der DFN-Cloud zur Verfügung.

Text: **Marc Brendel, Dr. Maximilian Hoecker, Andree Müller** (Universitätsrechenzentrum (URZ) der Universität Heidelberg)

Forscherinnen und Forscher benötigen einen hohen Grad an Autonomie, um effektiv arbeiten zu können. Dies gilt nicht nur auf inhaltlicher Ebene, sondern auch im Hinblick auf die IT, die inzwischen zentrales Element einer zunehmend digitalisierten Forschung geworden ist. Sie möchten häufig direkten Zugriff auf ihre Hardware haben, um schnell auf Bedarfsänderungen im aktuellen Vorhaben zu reagieren und die IT-Infrastruktur entsprechend anpassen zu können. Gleichzeitig ist jedoch nicht überall genügend Raum und Personal vorhanden, um Server oder Servercluster sicher, nachhaltig und zuverlässig betreiben zu können. Im schlimmsten Fall werden für ein Forschungsprojekt eigentlich hochkritische Systeme in leicht zugänglichen oder nicht ausreichend gekühlten Räumlichkeiten aufgestellt, häufig ohne Redundanz oder Absicherung durch eine unterbrechungsfreie Stromversorgung. Dem essenziellen Bedürfnis nach wissenschaftlicher Selbstbestimmung gerecht zu werden und gleichzeitig eine sichere, nachhaltige und verlässliche IT-Umgebung für die Gesamtorganisation zu schaffen, stellt für zentrale IT-Dienstleister an Hochschulen und Forschungseinrichtungen eine spannende Herausforderung dar.

Private-Cloud-Lösung vereint Selbstbestimmung mit Sicherheit

Das Universitätsrechenzentrum Heidelberg (URZ) hat den Dienst heiCLOUD entwickelt, um genau dieser Herausforderung effektiv begegnen zu können. Die heiCLOUD baut eine Brücke zwischen Forschung und IT-Dienstleistung: Das Rechenzentrum kann die einzelnen Komponenten der Cloud in seinen gesicherten, zentralen Serverräumen betreiben, sie mit einem Expertenteam vor Ort stets auf dem neuesten technischen Stand halten und kontinuierlich um neue Funktionen und Dienstleistungen erweitern. Gleichzeitig können Wissenschaftlerinnen und Wissenschaftler IT-Ressourcen durch das zugrunde liegende Infrastructure-as-a-

DAS SAGEN DIE ANWENDER

„Wir nutzen die heiCLOUD, um der internationalen Forschungsgemeinschaft im Bereich der Astronomie und Astrophysik Daten von synthetischen sternbildenden Wolken zur Verfügung zu stellen, die aus hochpräzisen numerischen Simulationen auf hochparallelen Supercomputern generiert wurden. Diese Daten werden zum Vergleich mit und zur astrophysikalischen Interpretation von Beobachtungsdaten aus erd- und weltraumgestützten Observatorien verwendet."

Prof. Dr. Ralf S. Klessen,
Professor für Theoretische Astrophysik,
Zentrum für Astronomie der
Universität Heidelberg
http://www.ita.uni-heidelberg.de/~ralf

„Wir verwenden die heiCLOUD vor allem, um unsere veralteten, momentan noch laufenden Server nach und nach zu ersetzen, wobei unser miRNA Datenbank-(Web-)Server als Erstes in die heiCLOUD verschoben wurde. Eine Kalkulation der Kosten und der anfallenden Aufwendung zum Erhalt eigener Server erbrachte letztendlich, dass die Verwendung der Server in der heiCLOUD viel mehr Vorteile und kaum Nachteile einbringt.

Dr. Carsten Sticht,
Bioinformatik und Statistik,
Medizinische Fakultät Mannheim
der Universität Heidelberg
http://mirwalk.umm.uni-heidelberg.de

„Am Heidelberg Institute for Geoinformation Technology (HeiGIT) betreiben wir unter dem Label openrouteservice eine Vielzahl frei nutzbarer Geodienste auf Open-Source-Basis. Über ein Webinterface und eine API können unter anderem Routen berechnet, Distanzmatritzen erstellt oder Erreichbarkeitsanalysen durchgeführt werden. Durch Verwendung der heiCLOUD lässt sich dieses Angebot flexibel skalieren und ausbauen."

Prof. Dr. Alexander Zipf,
Geographisches Institut der
Universität Heidelberg
https://openrouteservice.org

Service-Konzept so verwenden und verwalten, als stünden die genutzten IT-Komponenten in den eigenen Räumlichkeiten. Um Sicherheit, Aktualität, Hochverfügbarkeit und Funktionsfähigkeit der Infrastruktur selbst müssen sie sich nicht mehr kümmern. Zudem verbleiben alle gespeicherten Daten in den besonders geschützten Räumen des Rechenzentrums. Die Nutzerinnen und Nutzer werden durch das heiCLOUD-Team individuell beraten und unterstützt.

Über das webbasierte Dashboard der heiCLOUD oder eine REST-API können heiCLOUD-User selbsttätig virtualisierte IT-Infrastruktur – wie virtuelle Maschinen, Block- und Objektspeicher oder Netzwerkkomponenten – erstellen, konfigurieren und verwalten. Während Beschaffungsprozesse für physische Hardware oft wochen- oder monatelang dauern und viel bürokratischen Aufwand bedeuten, stehen die Komponenten aus der Cloud im besten Fall innerhalb weniger Minuten zur Verfügung. Ändern sich die IT-Bedürfnisse eines Forschungsprojekts, können die virtuellen Komponenten sofort angepasst und flexibel neu strukturiert und skaliert werden. Gleichzeitig entfallen viele Unannehmlichkeiten, die mit dem Betrieb physischer Hardware einhergehen, wie regelmäßige Wartungen, der Tausch von defekten Komponenten oder gar die Migration eines Servers auf neuere Hardware. Der Platz, den sonst Serverschränke einneh-

men würden, kann eventuell produktiver – etwa für Arbeits- und Laborflächen – genutzt werden.

On-Demand – Forschungs-Cloud mit nachhaltigem Geschäftsmodell

Die Beschaffung physischer Hardware bringt für Forschungsprojekte oft auch finanzielle Nachteile mit sich: So werden Server häufig zu Beginn eines Forschungsprojekts gekauft und sind dabei meist überdimensioniert, um möglichen Bedarfsschwankungen begegnen zu können. Verkleinert sich dann der IT-Bedarf des Projekts unerwartet, bleiben redundante Hardwareressourcen zurück. Zudem darf für Forschungsprojekte beschaffte Hardware häufig nicht für andere Zwecke verwendet werden, da dies den Vorgaben des Drittmittelgebers widerspricht – sofern überhaupt eine Beschaffung von Hardware aus Drittmitteln möglich ist.

Die Leistungen aus der heiCLOUD hingegen werden im On-Demand-Modell monatlich verbrauchsbezogen abgerechnet und müssen nicht im Vorfeld eingekauft werden. Benötigt das Forschungsvorhaben weniger IT-Ressourcen, sinken auch die IT-Kosten. Für dauerhaft betriebene Dienste können die Nutzer alternativ auch ein Prepaid-Modell wählen, bei dem die Kosten im Voraus abgerechnet werden. Auch der Kauf von heiCLOUD-Coins, einer Art Guthaben, das nicht an bestimmte Ressourcen gebunden ist, ist möglich und entspricht dem etablierten Bezahlmodell der Verwaltungen in Form einer Einmalzahlung. Da heiCLOUD eine Dienstleistung ist, können so auch virtuelle IT-Ressourcen in Drittmittelprojekten genutzt werden, für die vom Mittelgeber keine direkte Beschaffung physischer Hardware vorgesehen ist. Unabhängig vom Einsatz bietet die heiCLOUD ein selbstentwickeltes Billing-Dashboard, das heiCLOUD-Nutzern bzw. deren Kostenverantwortlichen eine stundengenaue Übersicht über die aktuellen und vergangenen Kosten und Guthaben gewährt. Grafiken bieten Einsicht in die Nutzung der verschiedenen Ressourcen und Dienstleistungen und ermöglichen so eine effektive, transparente Kostenkontrolle.

Das der heiCLOUD zugrunde liegende Geschäftsmodell ist nicht profitorientiert, sondern allein darauf ausgerichtet, den Dienst nachhaltig und langfristig zu finanzieren. Alle Erlöse fließen ausnahmslos in den Erhalt und den Ausbau der Cloud mit neuen Technologien und neuer Hardware. Hierdurch haben heiCLOUD-User die Garantie, dass ihre virtuelle Infrastruktur dauerhaft Bestand hat und dabei stetig aktualisiert und erweitert wird.

TECHNISCHE HINTERGRÜNDE

Die heiCLOUD besteht aus mehreren Clustern, die mithilfe der Open-Source-Software OpenStack® und Ceph betrieben werden. Im Netzwerk kommen Open-Networking-Switches in Kombination mit Cumulus® Linux® zum Einsatz. Folgende IaaS-Leistungen werden derzeit angeboten:

- Virtuelle Maschinen: Es stehen verschiedene Instanztypen (von 512 MB Hauptspeicher und einer CPU bis zu 200 GB Hauptspeicher und 40 vCPUs) zur Verfügung. Als Betriebssysteme sind standardmäßig Images für Ubuntu, CentOS und Windows abrufbar, es können jedoch auch eigene Images hochgeladen und verwendet werden.
- Block- und Objektspeicher: Jede virtuelle Maschine verfügt automatisch über 30 GB flüchtigen Blockspeicher als Root-Laufwerk. Zusätzlicher nichtflüchtiger Blockspeicher in Form von virtuellen Volumes kann jederzeit direkt an die Instanz angebunden werden. Über das Netzwerk lassen sich zudem beliebige externe Datenquellen einbinden. Für die Nutzung des Objektspeichers steht eine Swift-Schnittstelle zur Verfügung.
- Netzwerke: Virtuelle Netzwerke, Subnetze und Router lassen sich flexibel und vollkommen autonom erstellen. Jedes Projekt verfügt über die Möglichkeit, eigene projektinterne Netzwerke zu konfigurieren. Instanzen, die sich im selben internen Subnetz befinden, können direkt auf Layer 2 miteinander kommunizieren. Die Netzwerke sind sowohl zwischen den Projekten als auch projektintern vollständig voneinander isoliert und erlauben somit auch die mehrfache Nutzung beliebiger, frei konfigurierbarer Adressbereiche. Die Verwendung von IPv4 wird in heiCLOUD vollständig unterstützt, die Implementierung von IPv6 (intern und extern) befindet sich aktuell in Vorbereitung.
- Firewalls: Mithilfe von Sicherheitsgruppen und Sicherheitsregeln können Stateful Firewalls auf Instanzebene realisiert und zur Laufzeit beliebig angepasst werden.

An der Universität Heidelberg haben inzwischen ganz unterschiedliche Anwendungsfälle aus Forschung und Lehre ihren Platz in der heiCLOUD gefunden. So nutzen wissenschaftliche Projekte aus verschiedenen Fachdisziplinen die Cloud-Infrastruktur – von der Geographie über die Medizin und Lebenswissenschaften bis hin zur Linguistik und den Geisteswissenschaften. Darüber hinaus kommt die heiCLOUD auch in der Lehre zum Einsatz, etwa bei der Auswertung von Vorlesungen oder für statistische Erhebungen. Und auch in der wissenschaftsnahen Verwaltung werden inzwischen viele Anwendungen rein Cloud-basiert betrieben, zum Beispiel in den Bereichen der Prüfungsverwaltung, der Arbeitssicherheit oder der Kundenbetreuung.

Für alle Teilnehmer am X-WiN nutzbar

Inzwischen wurde die heiCLOUD als föderierter Dienst in die DFN-Cloud aufgenommen und ist somit über Heidelberg hinaus an allen Teilnehmereinrichtungen des Deutschen Forschungsnetzes zu günstigen Konditionen nutzbar. Dabei folgt sie den Grundprinzipien der DFN-Cloud: Als Dienst, der die besonderen Bedürfnisse von Forschung und Lehre berücksichtigt, wird die heiCLOUD nicht nur wissenschaftsnah zur Verfügung gestellt, sondern auch in gemeinsamem Austausch mit den Usern weiterentwickelt. Sie wird so immer weiter auf den Einsatz im wissenschaftlichen Kontext spezialisiert.

In naher Zukunft wird das Angebot der heiCLOUD um zwei neue Dienstleistungsvarianten erweitert: Zum einen sollen vGPU-VMs für GPU-intensive Anwendungsfälle (etwa für die Visualisierung von Forschungsdaten oder die Berechnung neuronaler Netze) integriert werden. Außerdem sollen durch geplante Ergänzungen im Netzwerkbereich sowohl DNS-as-a-Service als auch öffentliche IPv6-Adressen nutzbar gemacht werden. Mittelfristig sollen weitere infrastrukturnahe Servicekonzepte, wie Platform-as-a-Service oder hoch verfügbare Datenbanken, Teil des heiCLOUD-Portfolios werden. Übergeordnetes Ziel dieser Bemühungen ist es, die heiCLOUD als eine nachhaltige, sichere und wissenschaftsnahe Private Cloud weiter zu stärken und auszubauen.

Mehr Informationen zur heiCLOUD: https://heicloud.uni-heidelberg.de

Anfang vom Ende?

Die Entwicklung der EU-Urheberrechtsreform

Im September 2018 hat das EU-Parlament über die EU-Urheberrechtsrichtlinie abgestimmt, über die nun im Trilog-Verfahren mit Rat und Kommission weiterverhandelt wird. Die Richtlinie ist stark umstritten. Während die einen das Ende des freien Internets prognostizieren, freuen sich die anderen auf den langersehnten Schutz ihrer Werke. Umstritten sind dabei insbesondere die Regelungen zum Data-Mining, Upload-Filter und neuem Presse-Leistungsschutzrecht. Dieser Beitrag soll einen Überblick über die wichtigsten Streitpunkte geben und darstellen welche Auswirkungen die geplante Reform haben könnte.

Text: **Marten Tiessen** (Forschungsstelle Recht im DFN)

I. Gesetzgebungsverfahren

Die Diskussion über eine Modernisierung des EU-Urheberrechts aufgrund der fortschreitenden Digitalisierung dauert nun schon einige Jahre an. Hintergrund der Diskussion sind die durch die Digitalisierung entstandenen neuen Nutzungsmöglichkeiten urheberrechtlich geschützter Werke durch Plattformen wie Facebook, Google oder YouTube. Rechteinhaber beanstandeten in der Vergangenheit immer wieder, dass durch diese Plattformen Werke millionenfach genutzt werden, ohne dass dem eine angemessene Vergütung der Rechteinhaber gegenübersteht. Die Plattformbetreiber würden hingegen an den hochgeladenen Inhalten Milliarden verdienen. Dabei entstünde ihrer Meinung nach eine sogenannte Value Gap (Wertlücke), die es durch eine Reform des Urheberrechts zu schließen gilt. Durch die Gesetzesänderung sollen Plattformbetreiber verpflichtet werden, für die Nutzung der Werke eine angemessene Vergütung zu zahlen.

Das Europäische Parlament (Louise Weiss Building) in Straßburg *(Foto © Pietro NAJ-OLEARI)*

Der Anstoß zur EU-Richtlinie geht auf die Initiative des damaligen EU-Kommissars für Digitales, Günther Oettinger, zurück. Mit seiner Forderung nach einem stärkeren Schutz der Rechteinhaber setzte er sich in der EU-Kommission durch, die im Herbst 2016 einen ersten Entwurf einer neuen Urheberrechtsrichtlinie verfasste. In diesem Jahr stimmten auch die Mitgliedstaaten und das Europäische Parlament über die geplante Richtlinie ab. Die Länder einigten sich im EU-Ministerrat im Mai 2018 auf eine gemeinsame Position zur Richtlinie. Im Parlament versuchte der CDU-Politiker Axel Voss als zuständiger Berichterstatter, die

geplante Richtlinie durchzusetzen. Er befürwortete dabei sowohl die Verpflichtung zu Upload-Filtern sowie ein unionsweites Leistungsschutzrecht für Presseverleger. Nachdem der erste Entwurf Kritik erfahren hatte und auch im Plenum abgelehnt wurde, wurde der Entwurf erneut überarbeitet. In seiner jetzigen Fassung wurde er von der Mehrheit des EU-Parlaments am 12.09.2018 angenommen. Um sich auf eine finale Position der Richtlinie zu verständigen, befinden sich Vertreter des EU-Parlaments, des EU-Rats und der EU-Kommission zurzeit noch in Trilog-Verhandlungen. Die Richtlinie soll aber noch vor der Europawahl im Mai 2019 beschlossen werden.

II. Inhalt der aktuellen Fassung des EU-Parlaments

Die „Richtlinie über das Urheberrecht im digitalen Binnenmarkt" will zukunftstaugliche Regeln aufstellen, um den Rechteinhabern ein möglichst hohes Maß an Schutz zu bieten und die Klärung von Rechten zu erleichtern, gerade bei der digitalen und länderübergreifenden Nutzung von Werken. Dabei soll die Ausübung und Durchsetzung der Nutzungsrechte an Werken und sonstigen Schutzgegenständen auf Plattformen von Online-Diensteanbietern reguliert und mehr Transparenz bei Verträgen mit Urhebern und ausübenden Künstlern geschaffen werden. Die Reform umfasst auch verschiedene Ausnahmen für die Bereiche Bildung, Forschung und zum Erhalt des Kulturerbes. Kontrovers diskutiert wurde aber insbesondere über die neuen Vorschriften zu Text- und Data-Mining (1.), zum neuen Presse-Leistungsschutzrecht (2.) und zur Haftung von Plattformbetreibern (3.).

1. Text- und Data-Mining

Die Reform sieht vor, dass eine neue europaweite urheberrechtliche Schranke für das Text- und Data-Mining geschaffen wird. Beim Text- und Data-Mining werden große Mengen an Daten automatisch ausgewertet, um übergeordnete Erkenntnisse aus dem Gesamtkorpus zu gewinnen. Einen Teil des Datenkorpus werden häufig auch urheberrechtlich geschützte Werke ausmachen. Zwar sind die Sachinformationen in diesen Werken nicht urheberrechtlich geschützt, für die in der Vorbereitung oder im Prozess des Minings entstehenden Vervielfältigungen wäre hingegen grundsätzlich eine Erlaubnis des Urhebers erforderlich. Bei Tausenden von Werken, die in einem Datensatz enthalten sein können, würde das Einholen jeder Erlaubnis die Verarbeitung geradezu unmöglich machen. Durch die geplante Schranke soll diese Erlaubnis aber entbehrlich sein. Eine Schranke stellt im Urheberrecht einen Ausnahmetatbestand dar, durch den das absolute Recht des Urhebers in besonderen Fällen zugunsten vorrangiger anderer Interessen gesetzlich eingeschränkt wird, in diesem Fall zugunsten der Wissenschaft und Forschung. Art. 3 des Entwurfs begrenzt diese Ausnahme aber auf die nicht-kommerzielle wissenschaftliche Forschung. Neben der für alle Mitgliedstaaten verpflichtenden Schranke aus Art. 3 des Entwurfs stellt Art. 3a des Entwurfs es den Mitgliedstaaten frei, darüber hinaus noch weitere Ausnahmetatbestände für Data Mining zu anderen Zwecken zu schaffen. Voraussetzung für die Anwendung der Schranken ist, dass der Nutzer bereits Zugang zu den Werken hat, denn der Zugang zu den Werken wird von der Schranke nicht mitumfasst.

In Deutschland wurde eine ähnliche Schranke bereits durch die nationale Urheberrechtsreform im März 2018 eingeführt.[1] Im Gegensatz zur nationalen Regelung, die eine Vergütung für die Nutzung vorsieht, bleibt es nach dem Richtlinienentwurf des Parlaments den Mitgliedstaaten selbst überlassen, ob sie für die Nutzung eine Vergütungspflicht normieren. Die Kommission sah in ihrem ursprünglichen Entwurf noch ausdrücklich die vergütungsfreie Nutzung vor. Es bleibt daher abzuwarten, was nach den Trilog-Verhandlungen im finalen Entwurf stehen wird. Für die Rechteinhaber und Verlage geht die deutsche Schranke schon zu weit, eine erlaubnis- und vergütungsfreie Nutzung stößt dementsprechend auf noch größere Kritik. Die Wirtschaft bemängelt wiederum die Beschränkung der Schranke aus Artikel 3 auf nicht-kommerzielle Forschungszwecke. Von dieser Zweckbeschränkung ist auch der Datenjournalismus betroffen, der sich nicht auf die Schranke berufen kann. Ob eine zusätzliche Data-Mining-Schranke für den privaten Sektor geschaffen wird und wie diese dann gestaltet wird, bleibt nach jetzigem Stand den Mitgliedstaaten selbst überlassen. Profiteur der Schranke aus Artikel 3 des Entwurfs ist auf jeden Fall die europäische Wissenschaft. Eine potentielle Vergütungsfreiheit würde die Forschung mit großen Datensätzen sogar noch weiter vereinfachen.

2. Presse-Leistungsschutzrecht

Ein Kernthema der Reform ist die Einführung eines Leistungsschutzrechts für Presseverleger. Ein Leistungsschutzrecht ist ein dem Urheberrecht verwandtes Schutzrecht, was nicht auf einer eigenen schöpferischen Leistung beruht, sondern einer Leistung, die lediglich im Zusammenhang mit urheberrechtlich geschützten Werken steht. So werden vor allem bestimmte technisch und finanziell aufwendige Leistungen geschützt, durch die ein urheberrechtlich geschütztes Werk der Öffentlichkeit vermittelt wird. Darunter fällt neben dem Leistungsschutzrecht für Presseverleger beispielsweise das Schutzrecht der Tonträgerhersteller oder Datenbankhersteller. Die Regeln für Urheberrechte sind zu weiten Teilen auf Leistungsschutzrechte übertragbar.

Das Leistungsschutzrecht für Presseverleger aus Art. 11 des Entwurfs sieht einen Schutz der digitalen Nutzung von Presseveröffentlichungen vor. Der europäische Gesetzgeber sieht die mediale Vielfalt in Europa durch das Ungleichgewicht zwischen

[1] siehe hierzu Mörike, Es ist vollbracht, DFN-Infobrief Recht 08/2017

UPDATE:

Nachdem die Trilog-Verhandlungen erfolgreich abgeschlossen werden konnten und das Europäische Parlament dem aus den Verhandlungen entstandenen finalen Entwurf mehrheitlich zugestimmt hat, wurde die Urheberrechtsrichtlinie in ihrer finalen Version am 15. April 2019 durch den Rat der Europäischen Union beschlossen. Die Mitgliedstaaten haben jetzt zwei Jahre Zeit, die Richtlinie in nationales Recht umzusetzen.

Die beschlossene Urheberrechtsrichtlinie weicht in einigen Teilen von dem hier besprochenen Entwurf des Europäischen Parlaments ab. Auch hat sich die Nummerierung der Artikel verschoben, sodass beispielsweise aus dem umstrittenen Artikel 13 inzwischen Artikel 17 geworden ist. Die wesentlichen Punkte des Parlamentsentwurfs sind aber auch in die endgültige Fassung eingeflossen.

Presseverlagen und mächtigen Plattformen gefährdet. Die Übernahme von Nachrichtenausschnitten durch Suchmaschinenbetreiber oder News-Aggregatoren bedrohe seiner Ansicht nach die unternehmerische Leistung der Verlage. Mit dem neuen Leistungsschutzrecht will er sicherstellen, dass die Presseverlage für die digitale Nutzung ihrer Veröffentlichungen in Zukunft vergütet werden. In erster Linie geht es dabei um die Nutzung kleiner Textausschnitte („Snippets“) oder Überschriften durch Dienste wie Google News. Durch das Leistungsschutzrecht sollen solche Anbieter gezwungen werden, die Lizenzen von den Verlagen für die Nutzung von Snippets zu erwerben. Art. 11 des Entwurfs erlegt den Mitgliedstaaten daher auf, Bestimmungen zu erlassen, durch die die Presseverlage die Rechte für die digitale Nutzung ihrer Presseveröffentlichungen erhalten. Eine Ausnahme schafft der Gesetzgeber in Absatz 2a für Hyperlinks, neben denen einzelne Wörter stehen. Außerdem fallen die in den Nachrichten veröffentlichten Tatsachen oder Sachinformationen nicht in den Schutzbereich des Art. 11 der Reform. Die Rechte sollen fünf Jahre nach Veröffentlichung der Artikel erlöschen. Außerdem ist beabsichtigt, dass die Urheber an den Einnahmen, die durch die sekundäre Nutzung der Veröffentlichungen entstehen, angemessen beteiligt werden. Ein solches Presse-Leistungsschutzrecht ist für den deutschen Gesetzgeber nicht neu. Mit dem achten Gesetz zur Änderung des Urheberrechtsgesetzes vom 7. März 2013 wurde in Deutschland aus ähnlichen Gründen ein solches Leistungsschutzrecht bereits eingeführt. Das heftig umstrittene Gesetz hat bis heute nicht den gewünschten Erfolg erbracht. Gerade Google News konnte nicht gezwungen werden, entgeltliche Lizenzvereinbarungen mit den einzelnen Verlagshäusern zu schließen. Viele der großen Verlage gewährten Google News eine kostenlose Lizenz, da sie sonst nicht weiter auf Google News gelistet worden wären. Die Listung, gegen die sich die Verlage auch ohne Leistungsschutzrecht hätten wehren können, stellte für die Verlage aber nie ein Problem dar, sondern lag schon immer im eigenen finanziellen Interesse der Verlage, die durch die Listung ihre Bekanntheit steigern und den Leserkreis erweitern. Ziel des Leistungsschutzrechts war es lediglich an den Werbeeinnahmen der News-Aggregatoren zu partizipieren. Zu solchen Lizenzvereinbarungen ist es aber nicht gekommen. Trotz des ausbleibenden Erfolgs des Gesetzes hat sich die EU-Kommission das deutsche Leistungsschutzrecht neben dem spanischen zum Vorbild für ihr Projekt genommen. Der EU-Gesetzgeber will aber weiter gehen als der deutsche Gesetzgeber, der in seiner Fassung die Verwendung einzelner Wörter oder kleinster Textausschnitte von dem Leistungsschutzrecht ausgenommen hat.

3. Haftung von Online-Plattformen

Art. 13 des Entwurfs enthält ein neues Vergütungs- und Haftungsregime für die Nutzung geschützter Inhalte durch große Plattformbetreiber. Dabei richtet er sich ausschließlich an Plattformen, bei denen einer der Hauptzwecke darin besteht, wesentliche Mengen an von Nutzern dieser Dienste hochgeladenen beziehungsweise bereitgestellten urheberrechtlich geschützten Inhalten zu speichern, der Öffentlichkeit zugänglich zu machen oder als Stream wiederzugeben. Unter solche sogenannten Online-Inhaltsweitergabedienste fallen insbesondere große Plattformen wie YouTube, Facebook, Instagram, Vimeo, SoundCloud etc. Kleinstunternehmen, kleine und mittlere Unternehmen sind von der Definition ebenso ausgenommen wie auch Diensteanbieter, die nicht zu gewerblichen Zwecken tätig sind (z. B. Wikipedia), oder Anbieter von Online-Diensten, bei denen die Inhalte mit Zustimmung aller betroffenen Rechtsinhaber hochgeladen werden (z. B. bildungsbezogene oder wissenschaftliche Verzeichnisse). Auch fallen individuelle Cloud-Dienste, Open-Source-Entwicklungsplattformen und Online-Markplätze nicht unter die Bestimmungen des Art. 13.

Anders als zuvor soll nach der neuen Rechtslage nicht mehr der Grundsatz „notice and take down“ gelten.[2] Danach haften zurzeit die Plattformbetreiber nicht direkt für die Inhalte ihrer Plattform, es sei denn sie haben Kenntnis von der Rechtswidrigkeit des Inhalts. Werden sie auf rechtswidrige Inhalte aufmerksam gemacht, entsteht die Pflicht, diese Inhalte unverzüglich zu entfernen oder den Zugang zu ihnen zu

[2] Ausführlicher hierzu Herring, Host-Provider – Risikoreiche Gastgeberrolle?, DFN-Infobrief Recht 02/2011.

sperren. Eine allgemeine Überwachungspflicht des Plattformbetreibers besteht allerdings grundsätzlich nicht.

An diesem System will der europäische Gesetzgeber aber nicht festhalten: Zukünftig sollen Online-Inhaltsweitergabedienste selbst für die Inhalte ihrer Plattform voll haften. Der neu entworfene Art. 13 der Richtlinie stellt klar, dass der Dienst des Plattformbetreibers selbst eine Handlung der öffentlichen Wiedergabe darstellt. Rechtsgrundlage dieser Nutzungshandlung sollen nach Art. 13 Abs. 1 S. 2 faire und angemessene Lizenzverträge mit den Rechteinhabern sein. In der Lizenzvereinbarung sollen auch die Haftungsbedingungen für Inhalte der Plattformnutzer festgelegt werden, sofern diese nicht gewerblich handeln (Abs. 2).

Während in den ersten Entwürfen die umstrittene gesetzliche Verpflichtung zu Maßnahmen, die die Einhaltung der Lizenzvereinbarung gewährleisten (sprich: Upload-Filtern) noch geplant war, ist im neuesten Entwurf davon nicht mehr die Rede. Dennoch ist fraglich, ob eine faktische – wenngleich keine rechtliche – Pflicht zur Implementierung von Filtern bestehen würde. Anders ließen sich Rechtsverstöße bei großen Plattformen, auf denen sekündlich neue Inhalte hochgeladen werden, kaum überprüfen und vermeiden. Es liegt im Interesse des Betreibers ein solches Haftungsrisiko möglichst gering zu halten. Die ihm entstehenden, nicht unerheblichen Kosten für Entwicklung und Implementierung von Filter-Software wird der Betreiber jedoch selbst tragen müssen.

Die Plattform YouTube benutzt schon seit einiger Zeit die Filtersoftware „ContentID“, auch ohne rechtliche Pflicht, die eigenen Inhalte zu überprüfen. Liegt allerdings erstmal eine bestimmte Rechtsverletzung vor, so soll der Anbieter laut OLG Hamburg (Urteil v. 01.07.2015, Az. 5 U 87/12) auch sicherstellen, dass der Inhalt nicht erneut rechtswidrig hochgeladen wird („stay down“). Hier sei im Falle YouTubes auch der Einsatz der ContentID-Software sowie Wortfilter zumutbar. Eine solche sekundäre Filterpflicht wird voraussichtlich auch nach der EU-Urheberrechtsreform weiterhin bestehen.

Ein grundsätzliches Problem von Upload-Filtern ist allerdings, dass sie nicht immer exakt arbeiten und unter Umständen auch solche Inhalte filtern, die nicht geschützt sind. Kritiker befürchten daher, dass es durch die Filter zu einem „Overblocking“ kommen wird. Denn den Filtern wird es im Einzelfall nicht immer gelingen, automatisch zu erkennen, ob die Voraussetzungen von gesetzlichen Schrankenbestimmungen oder einer freien Benutzung vorliegen. Von einem Overblocking könnten daher gerade auch Zitate, Parodien oder Persiflagen betroffen sein, deren Nutzung aufgrund gesetzlicher Ausnahmeregelungen zulässig ist. Um die Nutzung von Werken für Zitate, Parodien, etc. in hochgeladenen Inhalten zu vereinfachen und bisherige Rechtsunsicherheiten zu beseitigen, soll zwar nach dem Erwägungsgrund 21b des Parlamentsentwurfs eine neue spezifische Ausnahme für diese Anwendungsfälle eingeführt werden. Doch auch diese sieht eine umfangreiche Verhältnismäßigkeitsprüfung im Einzelfall vor, sodass eine rechtsfehlerfreie, maschinelle Anwendung der Ausnahme zumindest unwahrscheinlich bleibt.

Für den Fall, dass Inhalte ungerechtfertigt gesperrt oder entfernt werden, sollen die Mitgliedstaaten nach Absatz 2b wirksame und zügige Beschwerde- und Rechtsbehelfsmechanismen zur Verfügung stellen.

III. Fazit und Ausblick

Die geplanten Änderungen im Urheberrecht betreffen zumindest mittelbar jeden Internetnutzer. Zwar ist noch nicht klar, welche Auswirkungen die Reform auf das Angebot der großen Internetdienstanbieter haben wird. Kritiker der Reform, wie YouTube-CEO, Susan Wojcicki, die angekündigt hatte, unter Umständen Millionen YouTube-Kanäle in Europa zu schließen, befürchten aber, dass durch die Haftungserweiterung zahlreiche Internetdienste eingestellt oder reduziert werden müssen. Ob die Einführung eines europaweiten Leistungsschutzrechts anderes hervorbringen wird als das nationale in Deutschland, kann zumindest bezweifelt werden, da die Interessenlage ähnlich ist. Die Hochschulen und Forschungseinrichtungen sind durch die Reform nicht nur mittelbar betroffen: Die neuen Regelungen zum Data Mining könnten unmittelbaren Einfluss auf Wissenschaft und Forschung haben. Allerdings werden die Änderungen aufgrund der bereits geltenden nationalen Schranken nicht so weitreichend sein wie in anderen Ländern. Wird allerdings in der endgültigen Fassung die Vergütungsfreiheit ausdrücklich fixiert, wäre die Anwendung weiter vereinfacht. Die Hochschule oder Forschungseinrichtung müsste dann nicht genauer untersuchen, an welche Verwertungsgesellschaft oder in welcher Höhe sie zu zahlen hat.

Im Gegensatz zu der im letzten Jahr verbindlich in Kraft getretenen Datenschutzgrundverordnung soll das Urheberrecht durch eine Richtlinie erneuert werden. Richtlinien wirken im Gegensatz zu Verordnungen in den Mitgliedstaaten in der Regel nicht unmittelbar und müssen erst durch den nationalen Gesetzgeber umgesetzt werden. Anders als die Datenschutzgrundverordnung, die das Datenschutzrecht von Grund auf neu strukturiert hat, sollen mit der neuen Richtlinie die bisher bestehenden Regelungen zum Urheberrecht nur ergänzt werden.

Es bleibt aber auch abzuwarten, zu welchem Ergebnis die Trilog-Verhandlungen kommen werden. Schon jetzt zeichnet sich ab, dass nicht alle Bestimmungen des Parlamentsentwurfs in den endgültig verhandelten Entwurf übernommen werden. Allerdings wird es voraussichtlich zu keinen großen inhaltlichen Veränderungen mehr kommen, da alle drei EU-Institutionen sich in den wesentlichen Punkten in ihren Entwürfen einig sind. ◆

(K)ein Ende in Sicht?

Vom Datenschutz und von Wettbewerbsverstößen

Die wettbewerbsrechtliche Abmahnfähigkeit fehlerhafter Datenschutzerklärungen ist seit der DSGVO ein großes Thema. Der vorliegende Beitrag will aktuelle Entwicklungen in Rechtsprechung und Gesetzgebung aufzeigen. Im Fokus stehen dabei insbesondere die jüngsten Entscheidungen des LG Bochum und des LG Würzburg zu dem Thema. Während das LG Bochum die wettbewerbsrechtliche Abmahnfähigkeit fehlerhafter Datenschutzerklärungen verneint, bejaht das LG Würzburg diese hingegen. Klärung könnten jüngste gesetzgeberische Entwicklungen bringen.

Text: **Charlotte Röttgen** (Forschungsstelle Recht im DFN)

Foto © FabioFilzi/iStockphoto

Bereits lange vor ihrem Wirksamwerden im Mai 2018 stach in der medialen Berichterstattung das Thema der Abmahnungen aufgrund fehlerhafter Datenschutzerklärungen hervor. Insbesondere kleineren Unternehmen und Websitebetreibern graute vor den vermeintlich drohenden rechtlichen und wirtschaftlichen Konsequenzen. In der öffentlichen Debatte wurden teilweise regelrechte Abmahn-Wellen prophezeit – die bislang jedoch ausgeblieben sind. Grund dafür ist, dass die Jurisprudenz die Normen der DSGVO uneinheitlich auslegt. Konkret geht es um die Frage, ob die in Kapitel 8 der DSGVO enthaltenen speziellen Regelungen der Rechtsdurchsetzung abschließend sind oder ob etwa das Wettbewerbsrecht daneben anwendbar bleibt. Mit anderen Worten: Handelt ein Unternehmer unlauter im wettbewerbsrechtlichen Sinn, wenn er gegen die Standards der DSGVO verstößt? Mit den Urteilen des LG Bochum und des LG Würzburg sind in der jüngeren Vergangenheit zwei inhaltlich voneinander abweichende Entscheidungen ergangen, welche die Abmahnfähigkeit von Datenschutzverstößen nach der DSGVO behandeln. Möglicherweise könnte nunmehr der Bundesgesetzgeber das Thema im Rahmen des zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes (DSAnPUG) einer Klärung zuführen.

I. Hintergrund

Möchte ein Mitbewerber gegen unlauteres Verhalten seines Konkurrenten vorgehen, steht ihm der Weg der wettbewerbsrechtlichen Abmahnung offen. Die Voraussetzung dafür, dass ein Verhalten wettbewerbsrechtlich nach § 3a UWG (Gesetz gegen den unlauteren Wettbewerb) abgemahnt werden kann ist, dass ein Marktteilnehmer gegen eine Marktverhaltensregelung verstoßen haben muss und hierdurch spürbar die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern beeinträchtigt hat. Abmahnberechtigt sind nach § 8 Abs. 3 UWG u.a. Mitbewerber. Unter einer Marktverhaltensregelung versteht man eine Norm, die zumindest auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln. Einige Landgerichte und Oberlandesgerichte haben auf Grundlage der alten Datenschutzgesetze einzelne datenschutzrechtliche Normen als Marktverhaltensregelungen qualifiziert (etwa § 4a Abs. 1 BDSG a.F., in dem Vorgaben zur datenschutzrechtlichen Einwilligungserklärung enthalten waren) und deren grundsätzliche Abmahnfähigkeit nach § 3a UWG bejaht.

Anders als die alte Datenschutz-RL bestimmt die DSGVO die Rechtslage in den Mitgliedstaaten unmittelbar und hat einen grundsätzlich abschließenden Charakter. Deshalb entflammte eine Diskussion zu der Frage, ob neben den in der DSGVO selbst vorgesehenen Sanktionsmöglichkeiten auch solche aus anderen Gesetzen, im konkreten Fall aus dem UWG, anwendbar seien. Die Meinungen hierzu sind bis heute gespalten. Gehen die einen von einem abschließenden Charakter von Kapitel 8 DSGVO aus, das spezielle Regelungen der Rechtsdurchsetzung enthält und insbesondere keine Aktivlegitimation von Mitbewerbern vorsieht, halten die anderen das UWG neben der DSGVO für anwendbar und sehen daher teilweise ein erhöhtes Risiko für wettbewerbsrechtliche Abmahnungen durch Mitbewerber.

Die datenschutzrechtlichen Neuerungen, die mit der Einführung der DSGVO in deutsches Recht einhergegangen sind, beinhalten insbesondere einen erweiterten Pflichtenkatalog aufseiten der Verantwortlichen für die Verarbeitung personenbezogener Daten. Nicht zuletzt aufgrund des teils abstrakt anmutenden Wortlautes der nunmehr nach der DSGVO einzuhaltenden Informationspflichten bestehen bis heute vielfach Bedenken, ob die Umsetzung der eigenen Datenschutzerklärung rechtskonform ist. Vor dem Hintergrund der bisherigen Rechtsprechung wurde von manchen Medien prophezeit, dass die DSGVO dem Markt von „Abmahnanwälten“ zu einem Wachstum verhelfen werde. Obwohl die Rechtslage bislang nicht eindeutig geklärt ist, ist entgegen dieser Befürchtungen eine „Abmahnwelle“ ausgeblieben.

II. Urteil des LG Bochum

Das LG Bochum (Urteil vom 07.08.2018, Az. I-12 O 85/18) hatte kürzlich über die mitbewerberseitige Abmahnfähigkeit von Datenschutzverstößen zu entscheiden, wobei es die Rechtslage erstmals auf Grundlage der DSGVO beurteilen musste. In der Sache stritten die Parteien, die über das Internet Waren aus dem Bereich Druckerzeugnisse, Autokleber, Textilien, Bürobedarf und Werbemittel an Verbraucher vertrieben, im Wege des einstweiligen Rechtsschutzes u.a. darüber, ob der Verfügungskläger als Mitbewerber des Verfügungsbeklagten Unterlassung von Handlungen verlangen konnte, die gegen die DSGVO verstoßen. Der Verfügungskläger machte einen Unterlassungsanspruch geltend, da der Verfügungsbeklagte auf seiner Website nicht die erforderlichen Informationspflichten nach Art. 13 DSGVO für die Verbraucher bereitgehalten hatte. Der Verfügungskläger beanstandete u.a. das Fehlen der Namen und Kontaktdaten des für die Datenverarbeitung Verantwortlichen und seines Datenschutzbeauftragten sowie von Angaben zu der Speicherdauer personenbezogener Daten. Das LG Bochum entschied in dem Eilverfahren hinsichtlich des Anspruchs nach der DSGVO zugunsten des Verfügungsbeklagten und wies den Anspruch ab. Das Gericht begründete seine Entscheidung damit, dass dem Verfügungskläger die erforderliche Aktivlegitimation fehle, um Datenschutzverstöße von Mitbewerbern zu ahnden. Es schloss sich in seiner Argumentation der Meinung in der Rechtswissenschaft an, die von einem abschließenden Charakter der Art. 77–84 DSGVO ausgeht. Da in diesen Normen eine Aktivlegitimation von Mitbewerbern nicht vorgesehen ist und aufgrund des abschließenden Charakters daneben keine weiteren Ansprüche – etwa aus UWG

– ausgeschlossen sind, gibt es keine weitere rechtliche Möglichkeit von Mitbewerbern, Verstöße gegen die DSGVO abzumahnen.

III. Urteil des LG Würzburg

Das LG Würzburg (Az. 11 O 1741/18 UWG) hat mit Beschluss vom13.09.2018 hingegen die Frage nach der wettbewerbsrechtlichen Abmahnfähigkeit von Datenschutzverstößen durch Mitbewerber anders beurteilt. In der Sache begehrte ein Rechtsanwalt von einer Mitbewerberin, es zu unterlassen, ihre Kanzlei-Website ohne eine Datenschutzerklärung zu betreiben, die den Anforderungen der DSGVO entspricht. Der Antragsteller war der Ansicht, dass die Datenschutzerklärung auf der Website der Antragsgegnerin gegen die Vorgaben der DSGVO verstoße, weil es insbesondere an Informationen über Art, Zweck und Umfang der Verarbeitung personenbezogener Daten sowie über die Betroffenenrechte fehle. Das Gericht gab dem Begehr des Antragstellers statt und erließ eine einstweilige Verfügung gegen die Antragsgegnerin. In seiner Begründung folgt das LG Würzburg, anders als das LG Bochum, der Argumentation nach alter Rechtslage. Es bejahte den Marktverhalten-regelnden Charakter der streitgegenständlichen Normen der DSGVO gem. § 3a UWG und nahm auch die Aktivlegitimation des Antragsstellers als Mitbewerber an.

Es lässt sich also festhalten, dass sich die Wertungen der beiden Landgerichtsentscheidungen diametral entgegenstehen. De lege lata ist eine endgültige Klärung der Rechtslage damit erst durch die höchstrichterliche Rechtsprechung zu erwarten. Bis dahin kann allerdings noch einige Zeit vergehen.

IV. Aktuelle Entwicklungen des Gesetzgebers

Auf Bundesebene bereitet der Gesetzgeber derzeit das zweite Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG) vor. Mit dem Gesetzentwurf sollen bisher noch nicht erfolgte Anpassungen in bereichsspezifischen datenschutzrechtlichen Regelungen des Bundes an die Vorgaben der DSGVO vorgenommen werden. Der bisherige Entwurf sieht u.a. Änderungen in 152 bereichsspezifischen Gesetzen vor. Darüber hinaus könnten im Rahmen der Gesetzesnovelle auch Korrekturen oder Ergänzungen des BDSG vorgenommen werden, die zur Klärung von Rechtsfragen beitragen, die seit dem Wirksamwerden der DSGVO aufgekommen sind oder die im Zeitpunkt des ersten Gesetzgebungsprozesses[1] übersehen wurden. So haben der federführende Ausschuss für Innere Angelegenheiten und der Wirtschaftsausschuss des Bundesrates etwa in ihren Empfehlungen für den Bundesrat den Vorschlag unterbreitet, einen § 44a in das BDSG einzufügen. Die Norm soll ausdrücklich klarstellen, dass die Normen der DSGVO keine geschäftlichen Handlungen im Sinne des UWG darstellen. Dieser Vorschlag zeigt, dass die unklare Rechtslage hinsichtlich des Verhältnisses von DSGVO und UWG von dem Bundesgesetzesgeber gesehen wird und möglicherweise bereits in naher Zukunft regulative Maßnahmen ergriffen werden könnten, die diesen Zustand beseitigen. Allerdings ist an dieser Stelle zu betonen, dass das Gesetzgebungsverfahren (Stand Oktober 2018) noch im Gange ist und daher noch keine validen Aussagen zu der Gesetzesnovelle gemacht werden können.

V. Zusammenfassung und Konsequenzen für Hochschulen und wissenschaftliche Einrichtungen

Zusammenfassend lässt sich das Folgende festhalten: Die Frage danach, ob Verstöße gegen die DSGVO – insbesondere fehlerhafte Datenschutzerklärungen – von Mitbewerbern mithilfe des Wettbewerbsrechts abgemahnt werden können, ist nach wie vor sehr umstritten. Die jüngsten Entwicklungen in der Rechtsprechung weisen noch keine Tendenz zugunsten der einen oder anderen Bewertung auf, im Gegenteil. Aktuell ist die Bewertung zugunsten einer Anwendbarkeit des UWG auf DSGVO-Verstöße so wahrscheinlich wie jene, dass die DSGVO-Normen abschließend sind und Mitbewerber keine Ansprüche nach UWG geltend machen können. Der Ausschuss-Vorschlag des Bundesrates könnte, sofern er sich im Gesetzgebungsprozess durchsetzt, zu einer baldigen Klärung der Frage führen. Dann wäre per Gesetz ausdrücklich klargestellt, dass die Normen der DSGVO keine Vorschriften gem. § 3a UWG darstellen und damit nicht geeignet sind, eine Abmahnung durch Mitbewerber zu begründen.

Die Thematik ist auch für Hochschulen und Forschungseinrichtungen relevant. Auch sie sind dem Wettbewerbsrecht unterworfen, soweit sie am Markt teilnehmen. Daher können sie grundsätzlich von Mitbewerbern abgemahnt werden, sofern sie sich unlauter i.S.d. UWG verhalten. Nicht zuletzt aufgrund der aktuell unklaren Rechtslage ist es angeraten, ein besonderes Augenmerk auf die Rechtskonformität der eigenen Datenschutzerklärungen und Datenverarbeitungsvorgänge mit der DSGVO zu legen. ◆

[1] Leinemann, Auf die Plätze, fertig, los, DFN-Infobrief-Recht 10/2017.

DFN unterwegs

Der Begriff Netz ist schon Teil unseres Namens. Und gut vernetzt sind auch unsere Mitarbeiterinnen und Mitarbeiter – weit über die Grenzen unserer technischen Infrastruktur. Wo wir überall unterwegs sind, zeigen wir hier.

Michael Röder ist unter anderem verantwortlich für die DFN-Cloud-Services. Eines seiner Highlights war bisher …

… das OCRE Face-2-Face Kick-Off-Meeting in Utrecht am 12. und 13. März 2019:
„Das Treffen war der Auftakt zum Projekt, das im Januar 2019 gestartet ist. Im Rahmen von OCRE werden für die kommenden vier Jahre Ausschreibungsverfahren vorbereitet und realisiert. Ziel ist, den Erwerb von kommerziellen Cloud Services für öffentliche Einrichtungen aus Europas Wissenschaft und Forschung zu vereinfachen. Im Rahmen des Meetings hatten alle Projektbeteiligten die Möglichkeit, ihre eigenen Erwartungen zu schildern und sich von Beginn an in das Projekt einzubringen. Zur Meet-and-Greet-Session waren außerdem diverse Cloud Service Provider eingeladen worden. Diese nutzten bereits im Vorfeld die Chance, sich über Verfahrensmechanismen zu informieren. Insbesondere für große Projekte mit einer längeren Laufzeit sowie einem räumlich verteilten Projektteam ist ein initiales Treffen mit allen Beteiligten ein toller gemeinsamer Anfang, der die künftige Zusammenarbeit erheblich erleichtert."

Hubert Waibel ist beim DFN zuständig für das Network Operations Center (NOC). Einer seiner bisherigen Veranstaltungshöhepunkte war …

… der 2. CLAW-Crisis Management Workshop in Málaga am 12. und 13. November 2018:
„Wie gut ist ein Forschungsnetz auf Netzwerk- oder Cyberkrisen vorbereitet? Und wie wird eine Krise überhaupt definiert? Diese und zahlreiche andere Fragen diskutierten rund sechzig Teilnehmerinnen und Teilnehmer von Forschungsnetzen rund um den Globus – überwiegend aus den Bereichen Informationssicherheits-Management, den Computer Emergency Response Teams (CERTs), den Network Operating Centern (NOC) sowie der Presse- und Öffentlichkeitsarbeit. Organisiert wurde das Event bereits das zweite Mal von GÉANT. Die Keynote vermittelte gleich zu Beginn spannende Einblicke in die Stress-Biologie und beantwortete die Frage, unter welchen Umständen Menschen in Krisensituationen ihr Verhalten beeinflussen können, um über sich hinauszuwachsen und beste Ergebnisse zu erzielen – und wie wichtig ein harmonisches Krisenteam für die Bewältigung einer Krise ist. Höhepunkt des zweitägigen Workshops war jedoch das Proben des Ernstfalles. Bei der Krisen-Simulationsübung galt es, trotz des massiven Drucks – obwohl jeder wusste, dass es eine Simulation ist – als Team so gut wie möglich zu kommunizieren und zu funktionieren, um die Ursache der Krise zu identifizieren und zu bewältigen. Der größte Lerneffekt entstand jedoch aus den zahlreichen Pannen und Fehlern, die gemacht wurden."

DFN live: Wissen teilen, Erfahrungen weitergeben

Der DFN-Verein lebt von der Expertise und Erfahrung seiner Mitglieder und Teilnehmer am Deutschen Forschungsnetz. Mit zahlreichen Veranstaltungen, Tutorien, Tagungen und Workshops bietet der DFN-Verein ein Forum für einen lebendigen Austausch und Wissenstransfer.

Mitgliederversammlung

Mit über 300 institutionellen Mitgliedern engagiert sich die überwiegende Mehrzahl der deutschen Hochschulen und Forschungseinrichtungen sowie der forschungsnahen Unternehmen im DFN-Verein. Das breite Mandat seiner Gemeinschaft und das in ihn gesetzte Vertrauen gehören zu den Stärken des Vereins. Zweimal jährlich treffen sich dessen Vertreter zur Mitgliederversammlung (MV), um die Zukunft des Deutschen Forschungsnetzes zu gestalten.

Zum Vorsitzenden der 77. Mitgliederversammlung, die am 4. und 5. Dezember 2018 im Wissenschaftszentrum Bonn stattfand, wurde Hartmut Hotzel, Leiter des Rechenzentrums an der Bauhaus-Universität Weimar, gewählt. Eines der Topthemen war das gemeinsam vom BMBF und dem DFN-Verein initiierte Projekt zur Gründung einer Geschäftsstelle des Strategieausschusses für Nationales Hochleistungsrechnen (NHR). Aufgrund seiner Expertise im Bereich von nationalen Forschungsinfrastrukturen trat die Gemeinsame Wissenschaftskonferenz (GWK) bereits im vergangenen Sommer mit der Bitte an den Verein heran, das Vorhaben maßgeblich zu unterstützen. Mit Inbetriebnahme der Geschäftsstelle am 1. April 2019 ist das Projekt offiziell gestartet. Es hat eine Laufzeit von zwei Jahren.

Ein weiteres wichtiges Thema war der Prüfauftrag des Entgeltmodells, mit dem die 76. Mitgliederversammlung den Vorstand beauftragt hatte. Die Analyse sah vor, die Nachhaltigkeit und Zukunftsfähigkeit des bestehenden Entgeltmodells zu prüfen, unter anderem hinsichtlich der bedarfsgerechten Versorgung kleiner Einrichtungen, der Fairness und des Solidarprinzips sowie der Marktsituation. In seinem detaillierten Zwischenbericht gab Geschäftsführer Jochem Pattloch den aktuellen Stand wieder. Einen spannenden Einblick in ihre aktuellen Forschungsergebnisse gaben am Vorabend der MV Prof. Dr. Richard Bamler vom DLR mit seinem Vortrag „Big Data und KI-Verfahren in der Erdbeobachtung“ und Prof. Dr. Heiner Kuhlmann von der Rheinischen Friedrich-Wilhelms-Universität Bonn mit seiner Präsentation zum Exzellenzcluster PhenoRob.

Nachhaltige Landwirtschaft: Prof. Dr. Heiner Kuhlmann weiß, was Pflanzen wollen *(Foto © Maimona Id / DFN-Verein)*

TERMIN

Die nächste Mitgliederversammlung findet am **3. und 4. Juni 2019** in Berlin statt.

Volle Reihen, voller Erfolg: die DFN-Betriebstagung im Frühjahr 2019
(Foto © Heike Ausserfeld / DFN-Verein)

TERMIN

Die 71. DFN-Betriebstagung findet am **24. und 25. September 2019** im Seminaris CampusHotel Berlin statt.

Betriebstagung

Zweimal im Jahr treffen sich Mitarbeiterinnen und Mitarbeiter der am Wissenschaftsnetz X-WiN teilnehmenden Institutionen, Vertreter der Mitgliedsorganisationen sowie andere an den Fachthemen des DFN-Vereins Interessierte zur zweitägigen Betriebstagung, um sich fachlich weiterzubilden und Erfahrungen auszutauschen. In den insgesamt neun Foren, unter anderem Sicherheit, AAI, IP über WiN, Multimedia oder Clouddienste, werden die Teilnehmerinnen und Teilnehmer über neue Entwicklungen informiert und diskutieren Fragen, die sich aus dem Einsatz von DFN-Diensten ergeben.

Mit mehr als 300 Teilnehmerinnen und Teilnehmern gehörte die Veranstaltung am 19. und 20. März 2019 zu den bisher publikumsstärksten Betriebstagungen. Einen gelungenen Auftakt bestritt Keynote Speaker Olaf Erber vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinem Vortrag zum Thema „Sichere Nutzung öffentlicher Clouds und Mindeststandards zur RZ-Sicherheit“. Auf ebenso großes Interesse stieß der Vortrag „Cloud Journey and Agile Transformation of DB Systel“ im Forum Clouddienste. Darin erläuterte René Schneider wie der Deutschen Bahn der Transformationsprozess in die Welt der Clouddienste geglückt ist. Die Teilnehmerinnen und Teilnehmer erhielten einen Einblick, wie die Einführung von modernen Technologien wie Cloud Services mit Hilfe von strukturellen Änderungen der Organisationsform unter Einbezug der Belegschaft gelingen kann.

DFN-Konferenz „Datenschutz“

Seit 2012 veranstaltet das DFN-CERT im Auftrag des DFN-Vereins jährlich die DFN-Konferenz „Datenschutz“. Ziel ist unter anderem die Beratung und der Austausch der für die Einhaltung und die praktische Umsetzung des Datenschutzes Verantwortlichen in Forschungs- und Bildungsinstitutionen sowie Behörden. Zugleich bietet die Veranstaltung die Möglichkeit, Anforderungen mit Vertretern der Datenschutzaufsichtsbehörden und eingeladenen Experten aus der Datenschutzpraxis zu diskutieren.

Ganz im Fokus der 7. DFN-Konferenz „Datenschutz“, die am 20. und 21. November 2018 im Grand Elysée Hotel Hamburg stattfand, stand die Datenschutz-Grundverordnung (DSGVO). So zog Dr. Jan K. Köcher, Datenschutzauditor der DFN-CERT Services GmbH, in seiner Keynote eine erste Bilanz aus 180 Tagen DSGVO aus Sicht der Hochschulen und der Forschung. Die Veranstaltung besuchten 142 Teilnehmerinnen und Teilnehmer.

TERMIN

Die 8. DFN-Konferenz „Datenschutz“ findet am **5. und 6. Dezember 2019** im Hotel Park Inn Alexanderplatz in Berlin statt.

DFN-Konferenz „Sicherheit in vernetzten Systemen“

Im Auftrag des DFN-Vereins veranstaltet das DFN-CERT jedes Jahr die Konferenz „Sicherheit in vernetzten Systemen“. Mit ihrem technischen und wissenschaftlichen Fokus sowie einer großen Vielfalt an Beiträgen und Diskussionen hat sich die Veranstaltung als eine der größten deutschen Tagungen für Informationssicherheit etabliert.

Die Konferenz am 6. und 7. Februar 2019 im Grand Elysée Hotel Hamburg war mit mehr als 330 Teilnehmerinnen und Teilnehmern sehr gut besucht und bot eine breites Spektrum an Themen. Sie reichten von sehr technischen Demos beispielsweise zur Live-Erkennung von Angriffsmustern in Logdaten mittels Threat Intelligence bis hin zu einem juristischen Übersichtsvortrag zu internationalen Cybersecurity-Gesetzgebungen. Ein wiederkehrendes Thema war die Einführung von Informationssicherheits-Managementsystemen (ISMS) in Hochschulen und Forschungseinrichtungen sowie die Integration des ISMS mit den Datenschutzmanagementsystemen (DSMS).

Themenvielfalt ist ihre Stärke: die DFN-Konferenz in Hamburg *(Foto © Nina Bark/ DFN-Verein)*

TERMIN

Die 27. DFN-Konferenz „Sicherheit in vernetzten Systemen“ findet am **24. und 25. Februar 2020** im Grand Elysée Hotel Hamburg statt.

Aktuelle Informationen rund um das Deutsche Forschungsnetz und seine Veranstaltungen erhalten Sie auch regelmäßig in unserem Newsletter.
Den DFN-Newsletter können Sie unter **www.dfn.de** abonnieren.

Überblick DFN-Verein

(Stand: 06/2019)

Fotos © jackijack/fotolia

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. Sitz des Vereins ist Berlin.

Die Geschäftsstelle

Geschäftsstelle
Standort Berlin (Sitz des Vereins)
DFN-Verein e. V.
Alexanderplatz 1
D-10178 Berlin
Telefon: +49 (0)30 884299-0

Geschäftsstelle
Standort Stuttgart
DFN-Verein e. V.
Lindenspürstraße 32
D-70176 Stuttgart
Telefon: +49 (0)711 63314-0

Die Organe

Mitgliederversammlung
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, HS Heilbronn.

Verwaltungsrat
Der Verwaltungsrat beschließt alle wesentlichen Aktivitäten des Vereins, insbesondere die technisch-wissenschaftlichen Arbeiten und berät den Jahreswirtschaftsplan. Für die 12. Wahlperiode sind Mitglieder des Verwaltungsrates:

Dr. Rainer Bockholt
(Rheinische Friedrich-Wilhelms-Universität Bonn)

Prof. Dr. Hans-Joachim Bungartz
(Technische Universität München)

Prof. Dr. Gabi Dreo Rodosek
(Universität der Bundeswehr München)

Prof. Dr. Rainer W. Gerling
(Max-Planck-Gesellschaft München)

Dr.-Ing. habil. Carlos Härtel
(GE Global Research)

Prof. Dr. Odej Kao
(Technische Universität Berlin)

Prof. Dr.-Ing. Ulrich Lang
(Universität zu Köln)

Prof. Dr. Joachim Mnich
(Deutsches Elektronen-Synchrotron Hamburg)

Dr. Karl Molter
(Hochschule Trier)

Dr.-Ing. Christa Radloff
(Universität Rostock)

Prof. Dr.-Ing. Ramin Yahyapour
(Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen)

Christian Zens
(Friedrich-Alexander-Universität Erlangen-Nürnberg)

Dr. Harald Ziegler
(Heinrich-Heine-Universität Düsseldorf)

Der Verwaltungsrat hat als ständige Gäste

einen Vertreter der Hochschulrektorenkonferenz:

Prof. Dr. Monika Gross
(Präsidentin der Beuth Hochschule für Technik Berlin)

eine Vertreterin der Hochschulkanzlerinnen und -kanzler:

Dr. Andrea Bör
(Kanzlerin der Freien Universität Berlin)

einen Vertreter der Kultusministerkonferenz:

Jürgen Grothe
(SMWK Dresden)

den Vorsitzenden der jeweils letzten Mitgliederversammlung:

Prof. Dr. Gerhard Peter
(Hochschule Heilbronn)

den Vorsitzenden des ZKI:

Hartmut Hotzel
(Bauhaus-Universität Weimar)

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. Hans-Joachim Bungartz
Vorsitz

Dr. Rainer Bockholt
Stellv. Vorsitzender

Christian Zens
Stellv. Vorsitzender

Der Vorstand wird beraten vom Strategischen Beirat, einem Betriebsausschuss (BA) und einem Ausschuss für Recht und Sicherheit (ARuS).

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 Dr. Christian Grimm und Jochem Pattloch bestellt.

Die Mitgliedereinrichtungen

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Technische Hochschule Aschaffenburg
Augsburg	Hochschule für angewandte Wissenschaften, Fachhochschule Augsburg
	Universität Augsburg
Bad Homburg	Dimension Data Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	Berliner Institut für Gesundheitsforschung/Berlin Institut of Health
	Beuth Hochschule für Technik Berlin – University of Applied Sciences
	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
	Bundesanstalt für Materialforschung und -prüfung
	Bundesinstitut für Risikobewertung
	Campus Berlin-Buch GmbH
	Deutsche Telekom AG Laboratories
	Deutsche Telekom IT GmbH
	Deutsches Herzzentrum Berlin
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin (FUB)
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hochschule für Technik und Wirtschaft – University of Applied Sciences
	Hochschule für Wirtschaft und Recht
	Humboldt-Universität zu Berlin (HUB)
	International Psychoanalytic University Berlin
	IT-Dienstleistungszentrum
	Konrad-Zuse-Zentrum für Informationstechnik (ZIB)
	Museum für Naturkunde
	Robert Koch-Institut
	Stanford University in Berlin
	Stiftung Deutsches Historisches Museum
	Stiftung Preußischer Kulturbesitz
	Technische Universität Berlin (TUB)
	Umweltbundesamt
	Universität der Künste Berlin
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum Berlin für Sozialforschung gGmbH (WZB)
Biberach	Hochschule Biberach
Bielefeld	Fachhochschule Bielefeld
	Universität Bielefeld
Bingen	Technische Hochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Hochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Hochschule Georg Agricola
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern
	BundesminIsterium für Umwelt, Naturschutz u. nukleare Sicherheit
	Deutsche Forschungsgemeinschaft (DFG)
	Deutscher Akademischer Austauschdienst e. V. (DAAD)
	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
	Deutsches Zentrum für Neurodegenerative Erkrankungen e. V.
	Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.
	ITZ Bund
	Rheinische Friedrich-Wilhelms-Universität Bonn
Borstel	FZB, Forschungszentrum Borstel – Leibniz Lungenzentrum
Brandenburg	Technische Hochschule Brandenburg
Braunschweig	Leibniz-Institut DSMZ – Deutsche Sammlung von Mikroorganismen und Zellkulturen GmbH
	Helmholtz-Zentrum für Infektionsforschung GmbH
	Hochschule für Bildende Künste Braunschweig
	Johann-Heinrich von Thünen-Institut, Bundesforschungs-institut für Ländliche Räume, Wald und Fischerei
	Julius Kühn-Institut Bundesforschungsinstitut für Kulturpflanzen
	Physikalisch-Technische Bundesanstalt (PTB)
	Technische Universität Carolo-Wilhelmina zu Braunschweig
Bremen	Hochschule Bremen
	Hochschule für Künste Bremen
	Jacobs University Bremen gGmbH
	Universität Bremen
Bremerhaven	Alfred-Wegener-Institut, Helmholtz-Zentrum für Polar- und Meeresforschung (AWI)
	Hochschule Bremerhaven
	Stadtbildstelle Bremerhaven
Chemnitz	Technische Universität Chemnitz
	TUCed – Institut für Weiterbildung GmbH
Clausthal	Technische Universität Clausthal
Coburg	Hochschule für angewandte Wissenschaften, Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus-Senftenberg
Darmstadt	Deutsche Telekom IT GmbH
	European Space Agency (ESA)
	Evangelische Hochschule Darmstadt
	GSI Helmholtzzentrum für Schwerionenforschung GmbH
	Hochschule Darmstadt
	Merck KGaA
	Technische Universität Darmstadt
Deggendorf	Technische Hochschule
Dortmund	Fachhochschule Dortmund
	Technische Universität Dortmund

Dresden	Evangelische Hochschule Dresden
	Helmholtz-Zentrum Dresden-Rossendorf e. V.
	Hannah-Arendt-Institut für Totalitarismusforschung e. V.
	Hochschule für Bildende Künste Dresden
	Hochschule für Technik und Wirtschaft
	Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden e. V.
	Leibniz-Institut für Polymerforschung Dresden e. V.
	Sächsische Landesbibliothek – Staats- und Universitätsbibliothek
	Technische Universität Dresden
Dummersdorf	Leibniz – Institut für Nutztierbiologie (FBN)
Düsseldorf	Hochschule Düsseldorf
	Heinrich-Heine-Universität Düsseldorf
	Information und Technik Nordrhein-Westfalen (IT.NRW)
	Kunstakademie Düsseldorf
	Robert-Schumann-Hochschule
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Hochschule Emden/Leer
Erfurt	Fachhochschule Erfurt
	Universität Erfurt
Erlangen	Friedrich-Alexander-Universität Erlangen-Nürnberg
Essen	RWI – Leibniz-Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Europa-Universität Flensburg
	Hochschule Flensburg
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Deutsche Nationalbibliothek
	Deutsches Institut für Internationale Pädagogische Forschung
	Frankfurt University of Applied Science
	Johann Wolfgang Goethe-Universität Frankfurt am Main
	Philosophisch-Theologische Hochschule St. Georgen e. V.
	Senckenberg Gesellschaft für Naturforschung
Frankfurt/O.	IHP GmbH – Institut für innovative Mikroelektronik
	Stiftung Europa-Universität Viadrina
Freiberg	Technische Universität Bergakademie Freiberg
Freiburg	Albert-Ludwigs-Universität Freiburg
	Evangelische Hochschule Freiburg
	Katholische Hochschule Freiburg
Freising	Hochschule Weihenstephan
Friedrichshafen	Zeppelin Universität gGmbH
Fulda	Hochschule Fulda
Furtwangen	Hochschule Furtwangen – Informatik, Technik, Wirtschaft, Medien
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH
	Leibniz-Rechenzentrum d. Bayerischen Akademie der Wissenschaften
Gatersleben	Leibniz-Institut für Pflanzengenetik und Kulturpflanzenforschung (IPK)
Geesthacht	Helmholtz-Zentrum Geesthacht Zentrum für Material- und Küstenforschung GmbH
Gelsenkirchen	Westfälische Hochschule
Gießen	Technische Hochschule Mittelhessen
	Justus-Liebig-Universität Gießen
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GwDG)
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	Universität Greifswald
	Friedrich-Loeffler-Institut, Bundesforschungsinstitut für Tiergesundheit
Hagen	Fachhochschule Südwestfalen, Hochschule für Technik und Wirtschaft
	FernUniversität in Hagen
Halle/Saale	Leibniz-Institut für Wirtschaftsforschung Halle e. V.
	Martin-Luther-Universität Halle-Wittenberg
Hamburg	Bundesamt für Seeschifffahrt und Hydrographie
	Deutsches Elektronen-Synchrotron (DESY)
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	DFN – CERT Services GmbH
	HafenCity Universität Hamburg
	Helmut-Schmidt-Universität, Universität der Bundeswehr
	Hochschule für Angewandte Wissenschaften Hamburg
	Hochschule für Bildende Künste Hamburg
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg
	Universität Hamburg
	Xantaro Deutschland GmbH
Hameln	Hochschule Weserbergland
Hamm	SRH Hochschule Hamm
	Hochschule Hamm-Lippstadt
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe
	Hochschule Hannover
	Gottfried Wilhelm Leibniz Bibliothek – Niedersächsische Landesbibliothek
	Gottfried Wilhelm Leibniz Universität Hannover
	HIS Hochschul-Informations-System eG
	Hochschule für Musik, Theater und Medien
	Landesamt für Bergbau, Energie und Geologie
	Medizinische Hochschule Hannover
	Technische Informationsbibliothek
	Stiftung Tierärztliche Hochschule
Heide	Fachhochschule Westküste, Hochschule für Wirtschaft und Technik
Heidelberg	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	NEC Laboratories Europe GmbH
	Ruprecht-Karls-Universität Heidelberg
Heilbronn	Hochschule für Technik, Wirtschaft und Informatik Heilbronn
Hildesheim	Hochschule für angewandte Wissenschaft und Kunst Fachhochschule Hildesheim/Holzminden/Göttingen
	Stiftung Universität Hildesheim
Hof	Hochschule für angewandte Wissenschaften Hof – FH
Idstein	Hochschule Fresenius gGmbH
Ilmenau	Technische Universität Ilmenau
Ingolstadt	DiZ – Zentrum für Hochschuldidaktik d. bayerischen Fachhochschulen
	Hochschule für angewandte Wissenschaften FH Ingolstadt
Jena	Ernst-Abbe-Hochschule Jena
	Friedrich-Schiller-Universität Jena

	Leibniz-Institut für Photonische Technologien e. V.
	Leibniz-Institut für Alternsforschung – Fritz-Lipmann-Institut e. V. (FLI)
Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Hochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	FIZ Karlsruhe - Leibnitz-Institut für Informationsinfrastruktur
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe – Technik und Wirtschaft
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Hochschule für angewandte Wissenschaften, Fachhochschule Kempten
Kiel	Christian-Albrechts-Universität zu Kiel
	Fachhochschule Kiel
	Institut für Weltwirtschaft an der Universität Kiel
	Helmholtz-Zentrum für Ozeanforschung Kiel (GEOMAR)
	ZBW – Deutsche Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft
Koblenz	Hochschule Koblenz
Köln	Deutsche Sporthochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Katholische Hochschule Nordrhein-Westfalen
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln gGmbH
	Technische Hochschule Köln
	Universität zu Köln
Konstanz	Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)
	Universität Konstanz
Köthen	Hochschule Anhalt
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e. V.
Landshut	Hochschule Landshut – Hochschule für angewandte Wissenschaften
Leipzig	Deutsche Telekom, Hochschule für Telekommunikation Leipzig
	Helmholtz-Zentrum für Umweltforschung – UFZ GmbH
	Hochschule für Grafik und Buchkunst Leipzig
	Hochschule für Musik und Theater „Felix Mendelssohn Bartholdy“
	Hochschule für Technik, Wirtschaft und Kultur Leipzig
	Leibniz-Institut für Troposphärenforschung e. V.
	Mitteldeutscher Rundfunk
	Universität Leipzig
Lemgo	Technische Hochschule Ostwestfalen-Lippe
Lübeck	Technische Hochschule Lübeck
	Universität zu Lübeck
Ludwigsburg	Evangelische Hochschule Ludwigsburg
Ludwigshafen	Hochschule für Wirtschaft und Gesellschaft Ludwigshafen
Lüneburg	Leuphana Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Leibniz-Institut für Neurobiologie Magdeburg
Mainz	Hochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Katholische Hochschule Mainz
	Universität Koblenz-Landau
Mannheim	Hochschule Mannheim
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	TÜV SÜD Energietechnik GmbH Baden-Württemberg
	Universität Mannheim
	ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung GmbH
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Philipps-Universität Marburg
Merseburg	Hochschule Merseburg (FH)
Mittweida	Hochschule Mittweida
Mülheim an der Ruhr	Hochschule Ruhr West
Müncheberg	Leibniz-Zentrum für Agrarlandschafts- u. Landnutzungsforschung e. V.
München	Bayerische Staatsbibliothek
	Hochschule für angewandte Wissenschaften München
	Hochschule für Philosophie München
	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e. V.
	Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt GmbH
	ifo Institut – Leibniz-Institut für Wirtschaftsforschung e. V.
	Katholische Stiftungshochschule München
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft
	Technische Universität München
	Universität der Bundeswehr München
Münster	Fachhochschule Münster
	Westfälische Wilhelms-Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neu-Ulm	Hochschule für Angewandte Wissenschaften, Fachhochschule Neu-Ulm
Nordhausen	Hochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
Nürtingen	Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen
Nuthetal	Deutsches Institut für Ernährungsforschung Potsdam-Rehbrücke
Oberwolfach	Mathematisches Forschungsinstitut Oberwolfach gGmbH
Offenbach/M.	Deutscher Wetterdienst (DWD)
Offenburg	Hochschule Offenburg
Oldenburg	Carl von Ossietzky Universität Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Bundesgesellschaft für Endlagerung mbH (BGE)
Pforzheim	Hochschule Pforzheim – Gestaltung, Technik, Wirtschaft und Recht
Potsdam	Fachhochschule Potsdam

	Helmholtz-Zentrum, Deutsches GeoForschungsZentrum – GFZ
	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam-Institut für Klimafolgenforschung (PIK)
	Universität Potsdam
Regensburg	Ostbayerische Technische Hochschule Regensburg
	Universität Regensburg
Reutlingen	Hochschule Reutlingen
Rosenheim	Hochschule für angewandte Wissenschaften – Fachhochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	Cispa Helmholtz-Zentrum i.G.
	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn Rhein-Sieg
Schenefeld	European X-Ray Free-Electron Laser Facility GmbH
Schmalkalden	Hochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Siegen	Universität Siegen
Sigmaringen	Hochschule Albstadt-Sigmaringen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Hochschule Stralsund
Stuttgart	Cisco Systems GmbH
	Duale Hochschule Baden-Württemberg
	Hochschule der Medien Stuttgart
	Hochschule für Technik Stuttgart
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte Tautenburg
Trier	Hochschule Trier
	Universität Trier
Tübingen	Eberhard Karls Universität Tübingen
	Leibniz-Institut für Wissensmedien
Ulm	Technische Hochschule Ulm
	Universität Ulm
Vechta	Universität Vechta
	Private Hochschule für Wirtschaft und Technik gGmbH
Wadern	Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH (LZI)
Weimar	Bauhaus-Universität Weimar
	Hochschule für Musik FRANZ LISZT Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz
Weßling	T-Systems Solutions for Research GmbH
Wiesbaden	Hochschule RheinMain
	Statistisches Bundesamt
Wildau	Technische Hochschule Wildau
Wilhelmshaven	Jade Hochschule Wilhelmshaven / Oldenburg / Elsfleth
Wismar	Hochschule Wismar
Witten	Private Universität Witten / Herdecke gGmbH
Wolfenbüttel	Ostfalia Hochschule für angewandte Wissenschaften
	Herzog August Bibliothek
Worms	Hochschule Worms
Wuppertal	Bergische Universität Wuppertal
	Kirchlische Hochschule Wuppertal/Bethel
Würzburg	Hochschule für angewandte Wissenschaften – Fachhochschule Würzburg-Schweinfurt
	Julius-Maximilians-Universität Würzburg
Zittau	Hochschule Zittau / Görlitz
Zwickau	Westsächsische Hochschule Zwickau

DFN mitteilungen
bieten Hintergrundwissen zu Themen aus der Welt der Kommunikationsnetze und des DFN-Vereins

DFN infobrief recht
informiert über aktuelle Entwicklungen und Fragen des Medien- und Informationsrechtes

DFN newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

Alle Publikationen können Sie hier abonnieren:
https://www.dfn.de/publikationen/