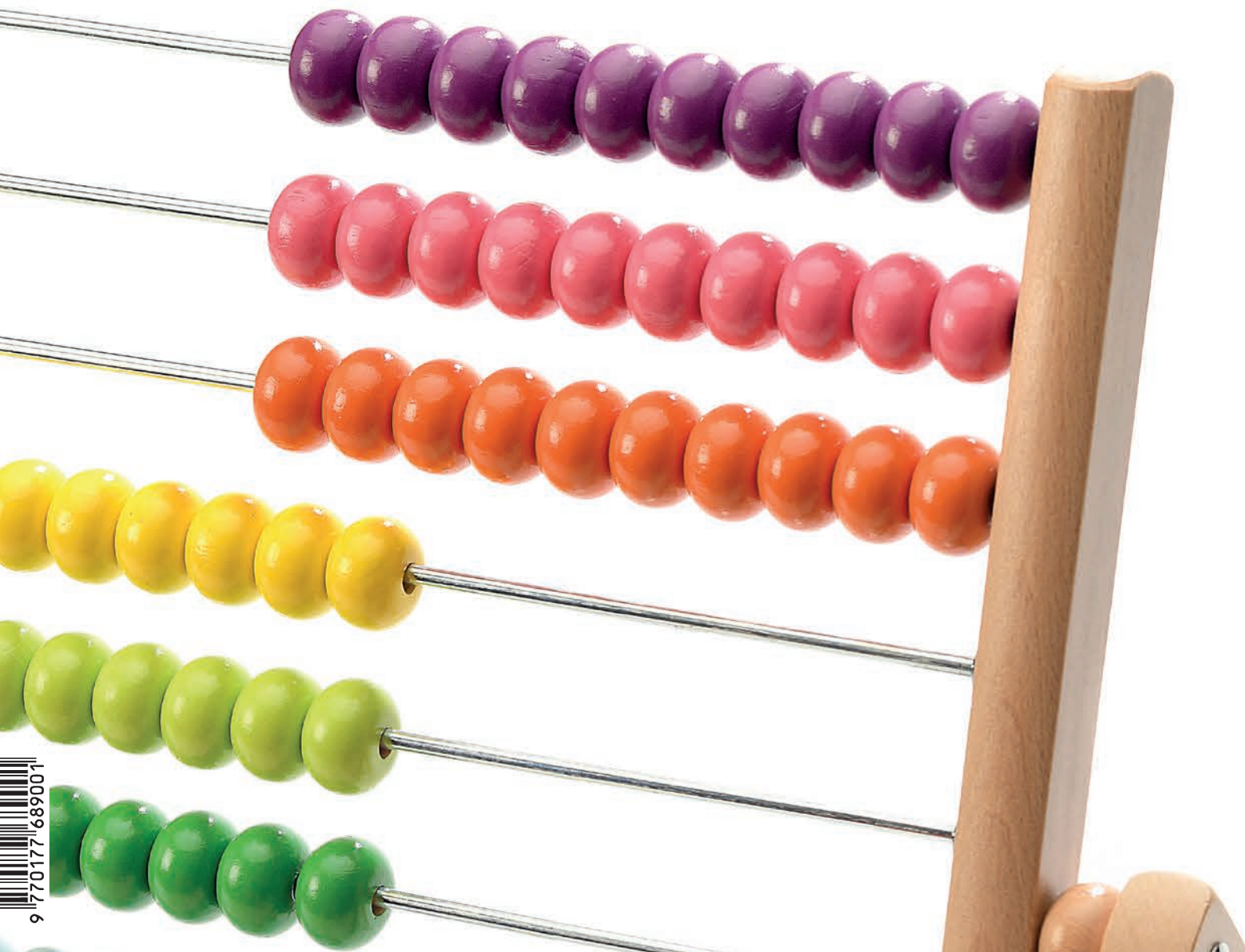
DFN mitteilungen

Die Rechnung geht auf
Aufbruchstimmung im NHR

The Next Generation
neue Infrastruktur für easyroam

Kampf gegen Phishing
DNS-basierter Schutz in DFN.Security



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: presse@dfn.de
Web: www.dfn.de

ISSN 0177-6894

Redaktion: Maimona Id, Nina Bark
Lektorat: Angela Lenz
Gestaltung: Labor3 | www.labor3.com
Druck: Druckerei Rüss, Potsdam
© DFN-Verein 12/2023

Fotonachweis
Titel: uwimages / Adobe Stock
Rückseite: Rawpixel.com / Adobe Stock

Dr. Rainer Bockholt
Direktor des Hochschulrechenzentrums der Rheinischen Friedrich-Wilhelms-Universität Bonn | Seit 2014 Stellvertretender Vorstandsvorsitzender im DFN-Verein | Seit 2014 Mitglied im Vorstand der „Zentren für Kommunikation und Informationsverarbeitung e. V." (ZKI)

Ein Hoch auf die Gemeinschaft – insbesondere auf den DFN-Verein und seine außergewöhnliche Mitgliedergemeinschaft, an der ich das Privileg habe, beteiligt zu sein: seit 20 Jahren als Mitgliedsvertreter der Rheinischen Friedrich-Wilhelms-Universität Bonn und seit 2014 als Stellvertretender Vorstandsvorsitzender des DFN-Vereins.

Die ersten Wochen und Monate im damals neuen Amt waren für meinen Geschmack etwas beschaulich – aber das sollte sich schnell ändern. Stichwort „Leistungssteigerung": Elendig lange Bereitstellungszeiten von Upgrades auf Teilnehmerseite führten zu Eskalationsgesprächen bis in die Vorstandsetagen der Lieferanten. Aber das endgültige Aus der „Komfortzone" im Vorstand war gekommen, als die Kostendeckung und Kostenumlage des Netzes und seiner Dienste auf den Prüfstand gestellt wurden. Es bestand zum ersten Mal seit der Unabhängigkeit des DFN-Vereins die Notwendigkeit, ein nachhaltiges und zukunftsfähiges Entgeltmodell zu entwickeln – eine Herkulesaufgabe, die uns im Verein jahrelang beschäftigen sollte. Möglichst alle mitnehmen, Wogen glätten, Kompromisse finden, das waren schwierige, aber wichtige Aufgaben für uns.

Hier zeigte sich aber auch, was für eine Gemeinschaft wir trotz aller Unterschiede und verschiedenen Interessen sind: bis ins Mark solidarisch, resilient und stark. So beruht auch die neue Entgeltordnung, die 2020 von der Mitgliederversammlung mit großer Mehrheit beschlossen wurde, ebenfalls auf den Kernprinzipien „fair, solidarisch und bedarfsgerecht". Der damit verbundene Willensbildungsprozess und der gemeinsam getragene Konsens waren und sind beispielhaft für den DFN-Verein. Mehr Mitbestimmung geht nicht! Diesen Zusammenhalt habe ich stets geschätzt, nie war er wichtiger als heute.

Zeit Abschied zu nehmen. In meinem bisherigen Berufsleben ist der DFN-Verein etwas Einmaliges, in dem ich auch persönlich sehr viel Bestätigung gefunden habe: So durfte ich unter anderem den Betriebsausschuss weiterentwickeln zu einem Kreis, der sich mit seinem geballten Erfahrungsreichtum intensiv mit innovativen Ideen, Entwicklungen und Technologien auseinandersetzt und damit den Vorstand optimal beraten kann.

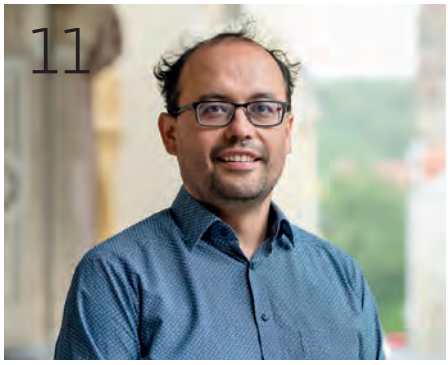
Die Gewissheit, an etwas wirklich Gutem beteiligt zu sein, etwas bewirken zu können mit Gleichgesinnten, für die Wissenschaftscommunity und mit ihr, hat dazu geführt, dass mich in den neun Jahren nicht ein einziges Mal so etwas wie Amtsmüdigkeit überkommen hat. Ganz im Gegenteil.

Ein riesiges „Danke!", auch im Namen meiner Vorstandskollegen, für das große Vertrauen, das uns jahrelang aus der Mitgliederschaft entgegengebracht wurde sowie für das außerordentliche Engagement und den großen Gestaltungswillen im Verein. Dem neuen Verwaltungsrat und Vorstand wünsche ich eine glückliche Hand, ein weiterhin offenes Ohr für die Community und genauso viel Freude und Begeisterung, wie ich sie in all den Jahren erfahren habe.

Ihr Rainer Bockholt

Inhalt

Die Rechnung geht auf – mit dem NHR-Verein
Aufbruchstimmung im Hochleistungsrechnen



Ein Quantensprung für das Hochleistungsrechnen
Warum Supercomputer Zeitmaschinen sind, verrät Prof. Dr. Thomas Kühne

Wer hat an der Uhr gedreht? Zeitsynchronisation mit PTP
Präzision und Genauigkeit bis in den Sub-Nanosekundenbereich

Wissenschaftsnetz

International

Forschung

Sicherheit

Campus

Flexibel lehren und lernen – mit bwLehrpool
Neuzugang in den Föderierten Diensten der DFN-Cloud

Recht

DFN-Verein

Autorinnen und Autoren dieser Ausgabe im Überblick

1 Dr. Barbara Diederich, NHR-Verein (barbara.diederich@nhr-verein.de); **2** Maimona Id, DFN-Verein (id@dfn.de); **3** Lars Fischer, NORDUnet (lars@nordu.net); **4** Dr.-Ing. Susanne Naegele-Jackson, Friedrich-Alexander-Universität Erlangen-Nürnberg (susanne.naegele-jackson@fau.de); **5** Sascha Schweiger, Friedrich-Alexander-Universität Erlangen-Nürnberg (sascha.schweiger@fau.de); **6** Martin Seidel, Friedrich-Alexander-Universität Erlangen-Nürnberg (martin.m.seidel@fau.de); **7** Jochen Becker, Technische Universität Darmstadt (jochen.becker@tu-darmstadt.de); **8** Long Yang Paffrath, DFN-Verein (lypaffrath@dfn.de); **9** Ralf Paffrath, DFN-Verein (paffrath@dfn.de); **o. Abb.** Christine Kahl, DFN-CERT (kahl@dfn.de); **10** Steffen Ritter, Hochschule Offenburg (steffen.ritter@hs-offenburg.de); **11** Dr. Dirk von Suchodoletz, Universität Freiburg (dirk.von.suchodoletz@rz.uni-freiburg.de); **12** Klaus Palenberg, Forschungsstelle Recht im DFN (klaus.palenberg@uni-muenster.de); **13** Johannes Müller, Forschungsstelle Recht im DFN (johannes.mueller@uni-muenster.de)

Die Rechnung geht auf – mit dem NHR-Verein

Aufbruchstimmung im Hochleistungsrechnen: Die erste Konferenz des NHR-Vereins ist ein voller Erfolg. Die Etablierung der internationalen Veranstaltungsreihe ist jedoch nur ein Baustein. Um Forschenden in Deutschland Hochleistungsrechenkapazitäten flächendeckend und bedarfsgerecht zur Verfügung stellen zu können, entwickelt der NHR-Verein die gemeinsame Koordinationsstruktur stetig weiter.

Text: **Barbara Diederich** (NHR-Verein)

Ein Highlight der NHR Conference ist das Panel „Women in HPC: Empowering future careers“, bei dem u. a. Elizabeth Robertson (DLR), Prof. Dr. Juliane Siegeris (HTW Berlin), Moderatorin Tania Carlin und Cristina Manzano (Forschungszentrum Jülich) diskutieren, wie wissenschaftliche Karrieren für Frauen im HPC-Bereich attraktiver gestaltet werden können (v. li.) | *Foto: ALOI.PHOTO*

Wissenschaftlicher Austausch über Disziplingrenzen hinweg: Am Zuse Institut (ZIB) in Berlin trafen sich vom 18. bis 20. September 2023 Expertinnen und Experten des High Performance Computings (HPC) zur ersten „NHR Conference“ des Vereins für Nationales Hochleistungsrechnen, NHR-Verein. Ziel der künftig jährlich stattfindenden internationalen Veranstaltung ist es, den Austausch der HPC-Community untereinander sowie mit den Fachleuten der neun NHR-Zentren zu fördern. Schwerpunkte dieses Jahr waren die Forschungsbereiche Life Science, Atomistic Simulation und Agent-based Simulation.

Hochkarätige Vorträge von Robert Axtell (George Mason University, Fairfax, Virginia), Karissa Sanbonmatsu (Los Alamos National Laboratory, New Mexico), Helmut Grubmüller (Universität Göttingen) und Mohammed AlQuraishi (Columbia University, New York) sowie eine Vielzahl spannender Kurzvorträge und Posterpräsentationen sorgten für angeregte Diskussionen unter den 170 Teilnehmenden. Auch die Stipendiatinnen und Stipendiaten der NHR Graduate School nutzten die Gelegenheit zum Erfahrungsaustausch mit den Fachleuten.

Die abschließenden Podiumsdiskussionen gaben wichtige Impulse für die Weiterentwicklung des NHR-Verbundes: Unter der Überschrift „NHR: HPC for Science“ diskutierte Rolf Krause mit seinen Gästen die aktuellen Herausforderungen im Hochleistungsrechnen. Das von Tania Carlin moderierte Podium „Women in HPC: Empowering future careers“ befasste sich mit der Frage, wie wissenschaftliche Karrieren für Frauen im HPC-Bereich attraktiver gestaltet werden können. Ziel des NHR-Verbundes ist es, das bestehende Entwicklungspotenzial an dieser Stelle auszuschöpfen.

Die Verknüpfung der wissenschaftlichen Konferenz mit den anschließenden Gremien- und Arbeitsgruppentreffen des NHR-Vereins bot sowohl für die teilnehmenden Nutzerinnen und Nutzer der Hochleistungsrechner als auch für die Verantwortlichen an den NHR-Zentren, die für den Betrieb der Rechner, die Vergabe der Rechenressourcen und die Beratungsangebote zuständig sind, einen großen Mehrwert. Fazit der ersten NHR-Konferenz: Die Teilnehmenden, die Vortragenden, das vielfältige Programm und nicht zuletzt die tolle Atmosphäre am ZIB und das gute Wetter machten die Veranstaltung zu einem vollen Erfolg.

Die „NHR Conference ’24“ findet im kommenden Jahr Anfang September in Darmstadt statt.

Meilensteine in der Koordination und Weiterbildung

Die Etablierung der Konferenzreihe ist nur ein Baustein der NHR-Aktivitäten zur Unterstützung von Forschenden im HPC. Im Rahmen der NHR Graduate School fördert der NHR-Verein jährlich junge Talente mit einem Stipendium und einem breiten Ausbildungsprogramm. Neben der Bereitstellung von Rechenkapazitäten sieht der NHR-Verein seine Verantwortung insbesondere

> Im Ergebnis können mehr Projekte schneller, energieeffizienter und somit nachhaltiger gerechnet werden.

in der Stärkung der Kompetenz zur effizienten und effektiven Nutzung der Hochleistungsrechner. Das Kurs- und Beratungsangebot reicht von der Antragstellung über grundlegende Einführungen der jeweiligen Rechnernutzung und den optimalen Einsatz

NHR CONFERENCE '23 | HIGH PERFORMANCE COMPUTING | 18.–20.09.2023

Gut besucht: Mit seiner Konferenz fördert der NHR-Verein den internationalen Austausch im HPC

Dr. Karissa Sanbonmatsu, Los Alamos National Laboratory

DER NHR-VEREIN AUF EINEN BLICK

11/2018 Beschluss der Gemeinsamen Wissenschaftskonferenz (GWK) über die gemeinsame Förderung des Nationalen Hochleistungsrechnens (NHR) durch Bund und Länder

04/2019 – 12/2021 Von BMBF und DFN-Verein initiiertes Projekt „Geschäftsstelle für den Strategieausschuss in der Gründungsphase des NHR“

01/2020 Ausschreibung der NHR-Förderung durch die Deutsche Forschungsgemeinschaft (DFG).

01/2021 Beginn der Förderung des NHR (62,5 Mio. €/Jahr, Förderzeitraum zunächst 10 Jahre).

08/2021 Gründung des Vereins für Nationales Hochleistungsrechnen, NHR-Verein e. V.

Zentrale Ziele der Förderung sind

1. die flächendeckende und bedarfsgerechte Bereitstellung von Hochleistungsrechenkapazitäten für wissenschaftliche Forschung an Hochschulen,
2. die Förderung der standortübergreifenden und interdisziplinären Zusammenarbeit in einer gemeinsamen Koordinationsstruktur, die für eine deutschlandweite Nutzung geöffnet ist,
3. die Stärkung der Methodenkompetenz der Nutzerinnen und Nutzer, die Förderung des wissenschaftlichen Nachwuchses sowie die Aus- und Weiterbildung im Wissenschaftlichen Rechnen,
4. die Förderung und Weiterentwicklung des Wissenschaftlichen Rechnens.

fachspezifischer Standardsoftware auf dem Hochleistungsrechner bis hin zur Unterstützung bei Effizienzoptimierung und Verbesserung von Software. Im Ergebnis können mehr Projekte schneller, energieeffizienter und somit nachhaltiger gerechnet werden. Davon profitieren am Ende alle in der Community.

Die NHR-Zentren unterscheiden sich nach wissenschaftlichen Schwerpunkten. Jedes Zentrum verfügt über Expertise in einem spezifischen Anwendungsbereich. Auf diese

> Die Angebote des NHR richten sich explizit an Fachbereiche, die die Möglichkeiten des HPC bislang kaum ausschöpfen.

Weise werden die entsprechenden Kompetenzen im NHR-Verbund koordiniert und stehen für eine schnelle und maßgeschneiderte Beratung bereit. Die Angebote des NHR richten sich nicht mehr nur an die traditionellen Anwendungsgebiete wie beispielsweise die Physik, sondern auch an Fachbereiche, die die Möglichkeiten des Hochleistungs-

NHR CONFERENCE '23 | HIGH PERFORMANCE COMPUTING | 18.–20.09.2023

Prof. Dr. Andrea Walther,
Humboldt-Universität zu Berlin

Marvin Kaster,
Stipendiat der NHR Graduate School, TU Darmstadt

Prof. Dr. Robert Axtell,
George Mason University, Fairfax, Virginia

rechnens bislang kaum ausschöpfen oder für ihre Forschung noch nicht entdeckt haben. Hier versucht der NHR-Verein, Abhilfe zu schaffen.

Eine Hürde für viele Forschende an deutschen Hochschulen ist die Antragstellung: Die Nutzung der Hochleistungsrechner ist für sie zwar kostenfrei, Voraussetzung ist jedoch ein Antrag, der nach einem wissenschaftsgeleiteten Verfahren bewertet und bewilligt werden muss. Dies kann auf potenzielle Erstantragstellende zunächst abschreckend wirken. Um diese Hürde so niedrig wie möglich zu gestalten, bietet der NHR-Verein seit Oktober 2023 die Möglichkeit, ein sogenanntes NHR-Starter-Projekt zu beantragen. In diesem Rahmen kann ein Antrag einmalig ohne detaillierte Angaben zu Rechenzeitbedarf und technischen Anforderungen eingereicht werden. Die Antragstellung beinhaltet von Beginn an das Angebot für eine Beratung zur Nutzung der Ressourcen. Ziel der Starterprojekte ist es, Forschenden während der einjährigen Projektlaufzeit die Vorteile der effizienten Nutzung von HPC-Rechnern zu vermitteln und sie zu befähigen, einen Antrag im Standardverfahren zu stellen.

Seit Oktober 2023 gibt es ein gemeinsames Onlineportal der NHR-Zentren. Über die Plattform JARDS kann die Ressourcennutzung zentral beantragt werden (siehe Kasten zu JARDS).

KI im Hochleistungsrechnen fördern

Eine neue und schnell wachsende Gruppe sind die Forschenden im Bereich Künstliche Intelligenz (KI), die einen zunehmenden Bedarf an Rechenressourcen haben, deren Softwarepakete und Methoden aber noch an die Betriebsumgebung einer HPC-Infrastruktur sowie an die zugehörigen Speichersysteme angepasst werden müssen. Um auch diese Gruppe von Anfang an optimal betreuen zu können, hat der NHR-Verbund mit Beteiligung des Gauss Centre for Supercomputing (GCS) eine KI-Informationsoffensive gestartet. Mit einführenden Webinaren, regelmäßig stattfindenden Fragestunden (QA-Café) sowie weiteren Angeboten möchten die NHR-Zentren KI-Anwenderinnen und -Anwender an die umfangreichen Möglichkeiten heranführen und zeigen, dass die bestehende HPC-Infrastruktur ihren Anforderungen entspricht und einen großen Teil des Bedarfes bereits jetzt abdecken kann.

Mit einem breiten Angebot an Anwendungsgebieten sind die NHR-Zentren noch vor drei Jahren in einem kompetitiven Verfahren um die NHR-Förderung durch Bund und Länder gegeneinander angetreten. Heute haben sie eine fachliche Schwerpunktsetzung sowie eine erfolgreiche Kooperationskultur entwickelt. Dieses Zusammenwachsen zu einem Verbund in echter Partnerschaft kommt nun den Wissenschaftlerinnen und Wissenschaftlern zugute – in Form eines breiten Angebots an Kompetenzen, bestmöglicher Beratung und maßgeschneiderten Lösungen für die verschiedenen Anwendungsgruppen. ◆

Informationen zum NHR-Verein finden Sie unter:
https://www.nhr-verein.de/

Informationen zur KI-Offensive finden Sie unter:
https://www.nhr-verein.de/ki-auf-hochleistungsrechnern

ATOMISTIC SIMULATION | LIFE SCIENCE | AGENT-BASED SIMULATION

Prof. Dr. Gerhard Wellein, stellvertretender NHR-Vorsitzender, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Prof. Dr. Christof Schütte, NHR-Vorstandsvorsitzender, Freie Universität Berlin

Fotos S. 7-9: ALOI.PHOTO

Mit JARDS Rechenzeit beantragen

JARDS (Joint Application Review and Dispatch Service) ist eine Software für die HPC-Ressourcenvergabe. Die PHP-basierte Web-Anwendung wird seit 2014 federführend vom Jülich Supercomputing Centre (JSC) entwickelt. Mit JARDS werden insbesondere die komplexen Vergabeprozesse in den verschiedenen Phasen unterstützt: HPC-Nutzende können in der Beantragungskomponente (JARDS.application) ihren Rechenzeit- und Speicherbedarf spezifizieren und begründen. Über die Begutachtungskomponente (JARDS.review) können die Mitarbeitenden der Rechenzentren die technischen und wissenschaftlichen Begutachtenden einem Rechenzeitantrag zuweisen und per E-Mail einladen. Das ausgeklügelte, rollenbasierte Zugriffsmodell ermöglicht es den Begutachtenden, anschließend die Bewertungen direkt in der Onlineplattform zu erstellen und zu bearbeiten. Darüber hinaus können Mitglieder der Vergabegremien Zugriff auf alle für sie relevanten Anträge und Gutachten erlangen. In der dritten Komponente (JARDS.project) besteht die Möglichkeit, Projekte zu verwalten: Beispielsweise können Berichte hochgeladen, Publikationen Projekten zugeordnet oder die aktuellen Ressourcen-Verbräuche eingesehen werden.

JARDS wird seit vielen Jahren am John von Neumann Institute for Computing (NIC), am Gauss Centre for Supercomputing e. V. (GCS), an der RWTH Aachen sowie an weiteren Standorten erfolgreich für den Vergabeprozess eingesetzt. Um auch Nutzenden des Vereins für Nationales Hochleistungsrechnen – NHR-Verein e. V. einen einheitlichen Zugang zur Beantragung von Rechenzeit zu ermöglichen, steht seit dem 2. Oktober 2023 eine entsprechende deutschlandweite Plattform zur Verfügung. Diese deckt den Bedarf aller neun NHR-Zentren ab: So können hier Rechenzeitprojekte unterschiedlicher Größenordnungen (Normal- und Großprojekte) beantragt werden, sodass die verschiedenen Ressourcen-Anforderungen berücksichtigt werden. Zur Vorbereitung größerer Anträge an einem spezifischen Zentrum können entsprechende Testprojekte beantragt werden. Für neue Nutzende (z. B. aus dem Bereich des maschinellen Lernens oder der Künstlichen Intelligenz) steht über die „NHR Starter“-Kategorie ein niederschwelliger Beantragungsweg zur Verfügung. Hierbei wird ein festes Kontingent bei einem der NHR-Zentren eingerichtet. Während Normalprojekte in der Regel fortlaufend beantragt werden können, starten die Großprojekte jeweils zum Quartalsbeginn.

Da JARDS zum ersten Mal für so eine große Anzahl an HPC-Zentren zum Einsatz kommt, wurde die Software in den vergangenen zwei Jahren unter der Leitung der RWTH Aachen und in enger Abstimmung mit dem JSC sowie den beteiligten NHR-Zentren an die Bedürfnisse des NHR-Verbunds angepasst und weiterentwickelt. Zu den neuen Features gehören beispielsweise verbesserte Funktionalitäten für die Zuweisung der Begutachtenden, zur automatischen Benachrichtigung über den Status eines Gutachtens, zum Verschieben der Anträge in ein anderes Quartal oder für mehrjährige Projekte. Darüber hinaus wurde das feingranulare Zugriffsmodell um eine Schnittstelle erweitert, die die Projekteinrichtung für die lokalen HPC-Zentren vereinfacht. ◆

Text: **Tim Cramer**, IT Center der Rheinisch-Westfälischen Technischen Hochschule (RWTH) Aachen, Kontakt: **cramer@itc.rwth-aachen.de**

Informationen auf Zenodo:
JARDS - Joint Application, Review and Dispatch Service von Carsten Karbach, Andreas Galonska, Matthias Richerzhagen et al.
https://doi.org/10.5281/zenodo.8031686

Zugang zu JARDS für NHR-Nutzende:
https://jards.nhr-verein.de

Ein Quantensprung für das Hochleistungsrechnen

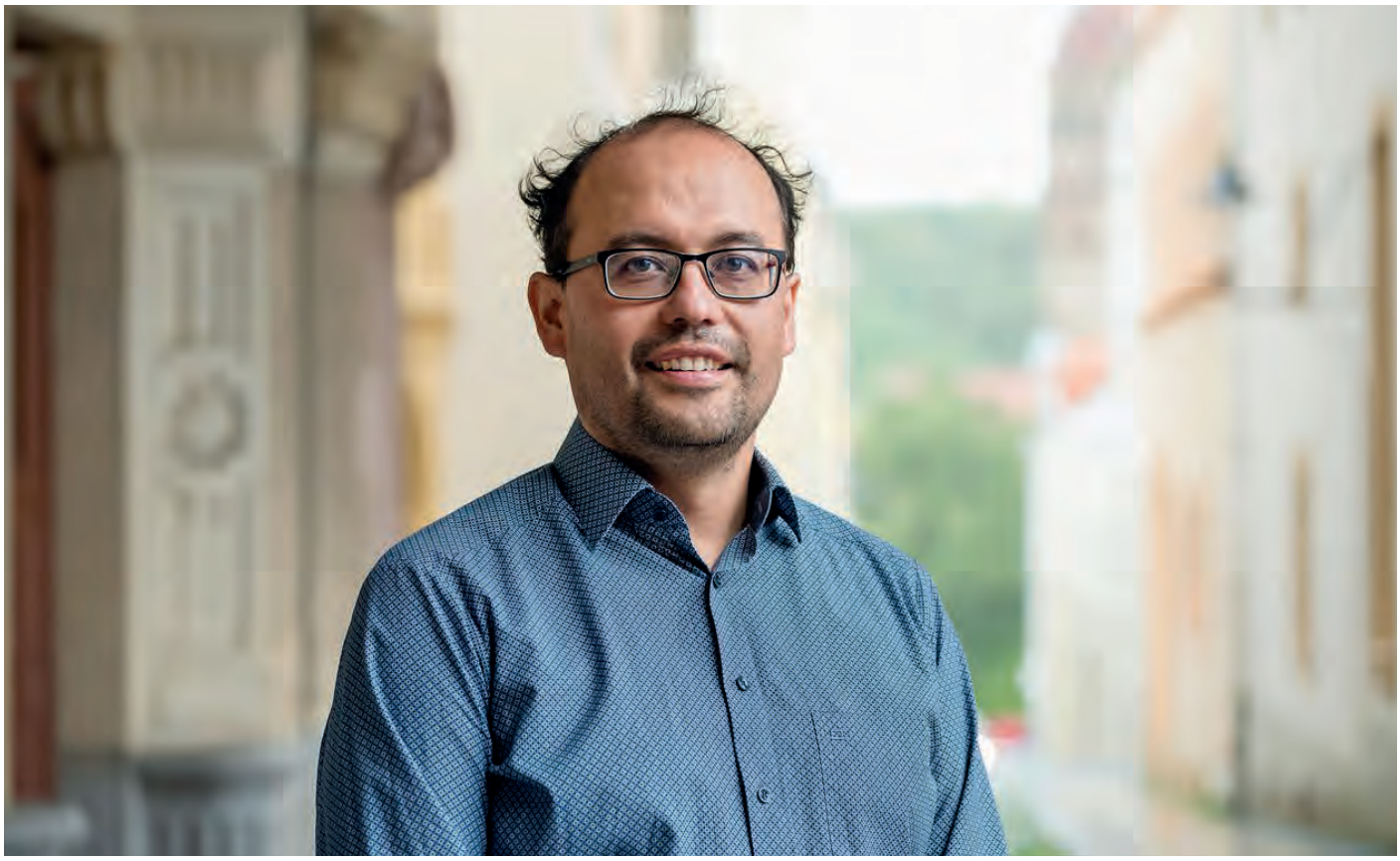


Foto: Antje Kraemer Photography

Vor zwei Jahren wurde der Verein für Nationales Hochleistungsrechnen (NHR) gegründet. Dieser war in der Entstehungsphase im DFN-Verein angesiedelt. Welche Fortschritte bisher erzielt wurden und welche Herausforderungen es derzeit im Hochleistungsrechnen gibt, erzählt Prof. Dr. Thomas Kühne, Gründungsdirektor des Center for Advanced Systems Understanding (CASUS) und Sprecher des NHR-Nutzungsausschusses.

Vor zwei Jahren erst wurde der Verein für Nationales Hochleistungsrechnen aus der Taufe gehoben. Wo steht er heute?

Der NHR-Verein war mit dem Ziel gestartet, allen Forschenden deutschlandweit einen einheitlichen, einfachen und fairen Zugang zu wertvollen Rechenressourcen zu ermöglichen. Da hat sich seit der Gründung sehr viel getan.

Am Anfang der Gründung stand zunächst ein Wettbewerb. Unterschiedliche Rechenzentren bewarben sich für die Aufnahme in den NHR-Verein. Jede Einrichtung hat versucht, sich möglichst gut zu profilieren. Nachdem die Auswahl der Rechenzentren

abgeschlossen war, begann der gegenteilige Prozess, nämlich als Verbund zusammenzuwachsen und gemeinsam eine Kooperationskultur zu etablieren – etwa im Bereich der Ausbildung des wissenschaftlichen Nachwuchses oder großer Infrastrukturprojekte. Das funktioniert bisher sehr gut.

Ein Beispiel für eine erfolgreiche Kollaboration ist das Atomistic Simulation Center (ASC), zu dem sich drei NHR-Zentren – das Paderborn Center for Parallel Computing, das NHR-FAU in Erlangen und das Zuse Institute Berlin (ZIB) – zusammengeschlossen haben, um atomistische Simulationen in den Anwendungsbereichen Physik, Chemie und Life Sciences abzudecken und hier ihre Ressourcen zu bündeln.

Wie funktioniert der Zugang zu den Rechenressourcen nun im Verbund?

Gemeinsam haben wir NHR-weite Vergaberichtlinien mit einheitlichen Qualitätsstandards etabliert. Bis dahin hatte jedes der neun NHR-Zentren – schon aufgrund der spezifischen Fach- und Anwendungsgebiete – eigene, sehr unterschiedliche Antragsverfahren und Vergabeprozedere, mit denen sich Nutzende, aber auch Gutachterinnen und Gutachter auseinandersetzen mussten. Ein Meilenstein für die Beantragung von HPC-Rechenzeit ist darum das elektronische Vergabeportal JARDS (Joint Application Review and Dispatch Service, siehe Kasten S. 10), das wir seit Kurzem im NHR-Verein nutzen. Es ermöglicht Forschenden nicht nur die einfache und zentrale Antragstellung, sondern gewährleistet sowohl ihnen als auch den Begutachtenden einen transparenten Einblick in den Vergabeprozess. Sämtliche Anträge und ihre Begutachtung unterliegen einem wissenschaftsgeleiteten Peer-Review-Verfahren.

Welche Aufgaben hat der NHR-Nutzungsausschuss in diesem Verfahren?

Der Nutzungsausschuss gestaltet die Verfahrensordnung zur Auswahl der Anträge und überwacht deren Durchführung nach einheitlichen Qualitätsstandards. So können Begutachtende nun in JARDS die Historie alter und neu eingereichter Anträge vergleichen und so beispielsweise den Neuheitsgrad beurteilen.

Mit JARDS kann ich also heute beantragen – und wann genau rechnen?

Eine Forderung des Strategieausschusses, der 2019 von der Gemeinsamen Wissenschaftskonferenz (GWK) als selbstständiges und unabhängiges Gremium eingesetzt wurde, war tatsächlich, die Zykluslänge für die Beantragung von Rechenzeit massiv zu verkürzen. Heute sind wir bei quartalsweiten Antragsperioden. Das ist ein großer Erfolg, sehr viel schneller geht es nicht.

> „Ein Meilenstein für die Beantragung von HPC-Rechenzeit ist das elektronische Vergabeportal JARDS.“

Vom Review-Prozess bis zum Start der Rechenzeit ist das für die Rechenzentren bereits ein Rund-um-die-Uhr-Betrieb. Mit der Bewilligung geht es gleich in die Vorbereitungen – ein Dauerstress. Aber mit der zentralen Vergabe haben wir die Möglichkeit, die Lasten zu verteilen. Außerdem ist der Pool der Begutachtenden jetzt größer. Jede Person, die beim NHR-Verein Rechenzeit beantragt, steht auch in der Verantwortung, Gutachten zu schreiben – es ist ein Geben und Nehmen. Aber ja, nach der Beantragung ist quasi vor der Beantragung.

Womit beschäftigt sich der Nutzungsausschuss außerdem?

Eine übergeordnete Aufgabe ist die Beobachtung der Anwendungsgebiete im NHR, denn hier gibt es eine sehr starke Profilierung. In Absprache mit allen Zentren achten wir darauf, dass die Ressourcen für sämtliche HPC-relevanten Anwendungsbereiche ausreichend vorhanden sind. Das beinhaltet auch die dafür notwendige Hardware und vor allem spezielle Rechenarchitekturen. Bei Bedarf greift der Nutzungsausschuss regulierend ein.

Ein wichtiges Kriterium ist außerdem die Verhältnismäßigkeit der eingesetzten Ressourcen. Wenn ein Antrag massiv aufwendiger ist als ein anderer, aber genauso gut, kann es sein, dass die Bewilligung auf Kosten anderer Anträge geht. Im Extremfall könnten dann andere Anträge nicht bewilligt werden. Das gilt es in der Begutachtung auszubalancieren. Dafür haben wir momentan kein besseres Review-System als sehr erfahrene Wissenschaftlerinnen und Wissenschaftler.

Eine weitere Aufgabe ist der Ausgleich der Rechenlast. Wenn es akute Engpässe gibt oder ein Rechenzentrum überlastet ist, haben wir im Interesse des globalen NHR-Systems die Möglichkeit, auf ein anderes NHR-Rechenzentrum umzuschichten. Bisher ist das nicht vorgekommen, weil wir gleich zu Beginn der Gründung sehr leistungsfähige neue Hochleistungsrechner beschafft haben. Wenn aber Rechenzentren an das Ende ihrer Lebenszeit gekommen sind – das ist nach etwa fünf Jahren der Fall – müssen wir künftig mit Umschichtungen rechnen.

Größer, schneller, besser: Sie haben die heutigen Supercomputer mal als Zeitmaschinen bezeichnet.

So wie die Astronomie in der Lage ist, mit immer besseren Teleskopen Milliarden von Lichtjahren in die Vergangenheit zu schauen, so kann die rechnergestützte Wissenschaft mit immer größeren Rechenressourcen de facto in die Zukunft gucken. Normale Arbeitsplatzrechner benötigen für komplexe Simulationen viele Jahre. Gerade in einem hochkompetitiven

Übernahm den Session Chair in der Keynote Lecture Atomistic Simulation: Prof. Dr. Thomas Kühne | *Foto: ALOI.PHOTO*

Prof. Dr. Thomas Kühne, Inhaber der Professur für Rechnergestützte Systemwissenschaften (Computational Systems Science) an der Technischen Universität Dresden (TUD)

Seit 2023 Gründungsdirektor des CASUS – Center for Advanced Systems Understanding in Görlitz
Partner: Helmholtz-Zentrum Dresden Rossendorf (HZDR), Helmholtz-Zentrum für Umweltforschung GmbH (UFZ), Technische Universität Dresden (TUD) und Max-Planck-Institut für molekulare Zellbiologie und Genetik (MPI-CBG), Dresden

Stellvertretender Vorsitzender des Paderborn Center for Parallel Computing (PC^2) und des kürzlich gegründeten Center for Sustainable Systems Design (CSSD)

Vorsitzender des NHR Atomistic Simulation Center und dem NHR Center for Computational Physics, Mitglied des DFG-Fachkollegiums

Mitautor des Open-source-Simulationsprogramms CP2K
Forschungsschwerpunkte: Entwicklung neuer numerischer Methoden und Algorithmen für chemische und physikalische Vorgänge und ihre Implementierung in Form von Computerprogrammen

Umfeld wie der Wissenschaft ist ist die Nutzung von Supercomputern ein entscheidender Fortschritt.

Die gesamte Infrastruktur für Supercomputer ist jedoch hochgradig angepasst und, gelinde gesagt, nicht gerade günstig, was den Energieverbrauch angeht. Da fragen sich nicht wenige, welchen Mehrwert das schafft, und ob wir nicht einfach 20 Jahre warten können. Die Antwort ist: Ja, könnten wir. Aber auf die Lösung dringlicher Probleme wie im Bereich Klimawandel oder nachhaltige Energieversorgung möchten und dürfen wir nicht 20 Jahre warten. Da spielen Computersimulationen und Modellierungen heute eine immer wichtigere Rolle.

Sie haben das Thema Energieverbrauch eben angeschnitten: Welchen Stellenwert hat Green IT im HPC?

Da geht es einerseits um die spannende Frage der Ressourcen und andererseits um ganz elementare monetäre Gesichtspunkte. Green IT ist aus dem einfachen Grund ein riesiges Thema, weil Hochleistungsrechner eine Menge Strom verbrauchen und damit immense Kosten verursachen. Gerade im NHR sehen wir, dass bei der Modernisierung von Rechenzentren durchgehend innovative Kühlkonzepte eingesetzt werden, die den Stromverbrauch senken können. Christian Plessl (Anm. Red. Universität Paderborn) und ich haben 2019 für unser Projekt „Green IT: Exakte Berechnungen mit ungenauen, aber energieeffizienten Rechnern“ den Forschungspreis der Uni Paderborn erhalten. Die Idee dahinter war, mit niedrigerer Präzision und dafür energieeffizient zu rechnen – besser gesagt mit Näherungen zu rechnen – und die Ungenauigkeiten mit neuartigen, fehlertoleranten Algorithmen zu kompensieren.

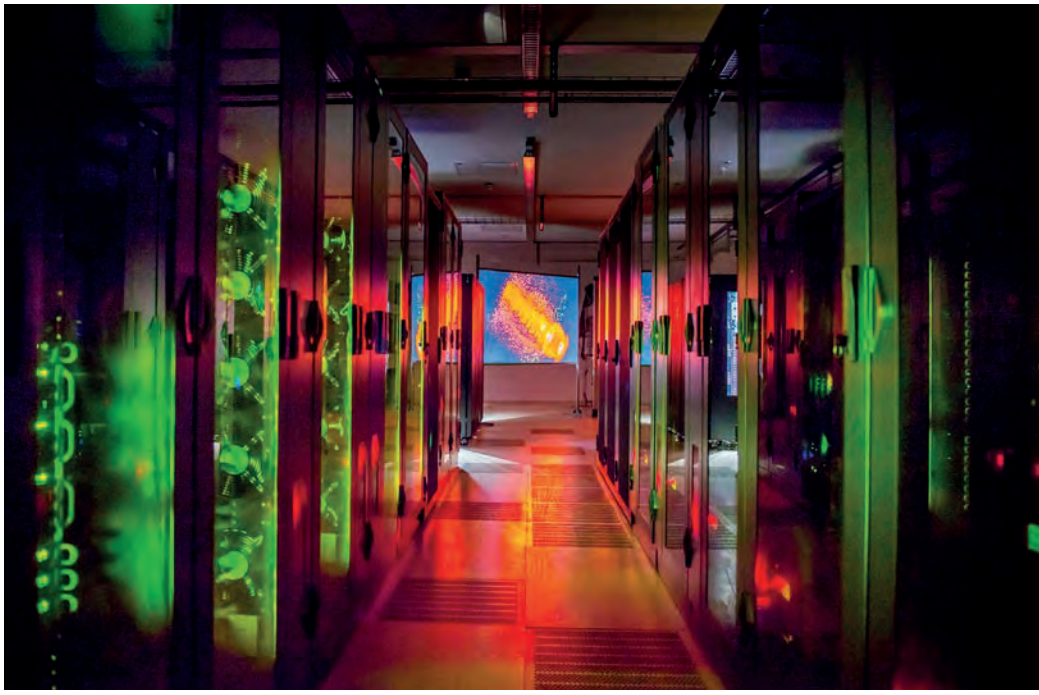
Ein anderer Aspekt von Green IT ist Nachhaltigkeit. Durch den Erfolg des NHR-Vereins ist der Zugang zu Rechenressourcen sehr einfach geworden. Als die Ressourcen noch extrem begrenzt waren, mussten sich Nutzende sehr genau Gedanken darüber machen, wie sie sie einsetzen. Heute müssen wir Nutzende

sensibilisieren, damit die Ressourcen nicht verschwenderisch zum Einsatz kommen für unsinnige oder unnötige Simulationen, die keinen Mehrwert bieten. Ich weiß nicht, ob die Community das so gerne hört. Insbesondere junge Forschende, die nur den NHR-Zugang kennen, sollen ein Gefühl dafür bekommen, was Rechnen kostet. Darum weisen bereits erste HPC-Zentren die Kosten für den Stromverbrauch aus. Das können, was den CO_2-Ausstoß angeht, schon das Äquivalent für mehrere transatlantische Flüge sein. Das führt in der Regel zu einem Aha-Effekt.

Im NHR-Verbund sind HPC-Rechenzentren der Leistungsklasse Tier-2 vereint. Sie selbst haben bereits an Tier-1-Rechenzentren gearbeitet. Ist die Trennung beider Ebenen zeitgemäß?

Wenn die Frage impliziert, ob Tier-1-Systeme sinnvoll sind, bin ich ganz klar der Meinung: ja. Letztendlich ist die maximale Rechenleistung ganz trivial auch eine Frage des Stromverbrauchs. Das ist am Ende des Tages die ultimative Grenze. Damit führt kein Weg an Beschleunigerarchitekturen vorbei. In aktuellen Flaggschiffrechnern sind das in der Regel GPU. Um maximale Rechenleistung zu erzielen und die Grenzen des Höchstleistungsrechnens auszuloten, gibt es nicht viele Möglichkeiten. Dafür brauchen wir Methodenentwicklung, das ist eine wichtige Zukunftsfrage. Wir prüfen beispielsweise, ob neuartige Algorithmen auf Beschleunigerarchitekturen skalieren. Das machen wir heutzutage in den Tier-1-Rechenzentren. Wenn wir aber nur diese hätten, wäre es sehr schwierig, den Großteil der Anwendungsgebiete abzudecken. Zur Wahrheit gehört nämlich auch, dass es nur wenige Anwendungen gibt, die zwingend auf Tier-1-Systemen erfolgen müssen: Gute Beispiele sind die Gitter-Quantenchromodynamik für Berechnungen in der Teilchen- und Kernphysik oder atomistische Simulationen, die in den Materialwissenschaften oder der theoretischen Chemie vorkommen. Absolut gesehen sind beide die größten Verbraucher von Supercomputerressourcen. Beide haben jedoch auch einen hohen Bedarf an Tier-2-Ressourcen – befinden sich also im Überlappungsbereich. Dieser Bereich ist definitiv größer geworden. Tier-2-Rechenzentren übernehmen mittlerweile einen Großteil aller Rechenjobs und können wesentlich flexibler auf Bedarfe in den Anwendungsgebieten eingehen – was die Schulung der Leute betrifft, aber auch was die Anpassung der Rechenressourcen angeht.

> „Letztendlich ist die maximale Rechenleistung ganz trivial auch eine Frage des Stromverbrauchs."



Geballte Rechenressourcen: das Rechenzentrum des Helmholtz-Zentrums Dresden Rossendorf (HZDR) | *Foto: Detlef Müller/HZDR*

Sie selbst nutzen für Ihre Forschung sogar Quantencomputer. Wie werden diese im HPC eingesetzt?

Das ist ein Paradigmenwechsel, eine ganz neue Art des Hochleistungsrechnens, die im Anwendungsbereich noch nicht weitverbreitet ist. In meinem Forschungsbereich, der Quantenmechanik, beschäftigen wir uns mit der Berechnung von Erwartungswerten. Dafür setzen wir Supercomputer mit einer Vielzahl parallel angeordneter Rechenkerne oder eben Quantencomputer ein. Aber nur ein Teil der gesamten Simulation, nämlich die Funktionsevaluierung, findet auf dem Quantencomputer statt. Die variationelle Optimierung läuft auf einem konventionellen Hochleistungsrechensystem. Beide Vorgänge alternieren. Die erfolgreichsten Algorithmen im Bereich des Quantencomputing sind deshalb hybride Algorithmen. Das wirft die Frage auf, wie wir das Hochleistungsrechensystem mit einem möglichen Quantencomputer verbinden können. Naheliegend ist es, diese Technologie an einem Hochleistungsrechenzentrum aufzubauen, weil dort bereits die entsprechenden Hochleistungsrechner für den klassischen Teil dieser hybriden Algorithmen vorliegen.

Sehen Sie mittelfristig Anwendungsmöglichkeiten für Quantencomputer?

Es ist eine sehr interessante Zukunfts-

technologie, die auf jeden Fall in irgendeiner Form bedient werden muss. Damit wir morgen dafür vorbereitet sind, müssen heute Wissenschaftlerinnen und Wissenschaftler darauf ausgebildet werden. Darum brauchen wir heute einen Zugang zu Quantencomputern. Aber dieser Zugang ist weitaus schwieriger als bei konventionellen HPC-Systemen. Der Infrastrukturaufwand und die damit verbundenen Investitionen sind erheblich. Einen Quantencomputer kauft man sich nicht mal eben. Die meisten Architekturen benötigen einen sehr hohen Kühlaufwand mit extrem tiefen Temperaturen.

> „Insbesondere im Bereich der atomistischen Simulationen arbeiten wir bereits sehr viel mit KI."

Das ist definitiv eine Sache für kooperative Forschung. Deswegen geht man heute immer mehr zu Subskriptionsmodellen über, bei denen Quantencomputer vom Hersteller betrieben und pro Rechenzeit abgerechnet werden. Das birgt aber die ganz gefährliche Entwicklung, dass eine normale Universitätsarbeitsgruppe sich das schlicht nicht leisten kann mit ihrem Budget bzw. existierenden Förderinstrumenten. Der Verzicht auf die experimentelle Erprobung von Quantencomputern wäre wiederum ein großer Wettbewerbsnachteil für Deutschland. Deswegen müssen wir einen anderen Zugang zu Quantencomputern finden. Diese an einem HPC-Zentrum aufzubauen, halte ich zumindest für überlegenswert. Auf absehbare Zeit werden Quantencomputer nicht großflächig in HPC-Zentren zum Einsatz kommen. Das ist meine private Meinung. Womit wir aber bereits sehr viel arbeiten – insbesondere im Bereich der atomistischen Simulationen – ist Künstliche Intelligenz (KI).

Welche Rolle spielt KI im HPC?

Das ist ein hochaktuelles Thema, das uns auch im Nutzungsausschuss sehr stark beschäftigt, weil es viele Veränderungen nach sich zieht. In der HPC-Anwendung ist der Anteil der KI-Komponenten rapide gestiegen, ein Ende ist nicht abzusehen. In den aktuellen Beschaffungen tragen wir dem wachsenden KI-Anteil mit dafür notwendiger Hardware, hauptsächlich speziellen Beschleunigerarchitekturen, Rechnung.

Können Sie ein Anwendungsbeispiel nennen?

Bis vor wenigen Jahren haben wir hochgradig aufwendige quantenmechanische Simulationen auf Hochleistungsrechenarchitekturen durchgeführt. Mit diesen Simulationsdaten – einer Vielzahl in Datenbanken abgelegter atomistischer Konfigurationen – werden heute sogenannte Surrogatmodelle trainiert. Diese sind in der Lage, quantenmechanische Lösungen sehr gut vorauszusagen. Das ersetzt letztendlich langwierige komplizierte Simulationsvorgänge und führt zu gänzlich neuen Arten von Simulationen. Die Surrogatmodelle benötigen zwar auch viel HPC-Rechenressourcen und sind damit ein NHR-Thema, aber sie ermöglichen regelrechte Sprünge in der Zeit- oder Größenskala, was die Skalierbarkeit angeht. Das ist über eine direkte Simulation nicht möglich.

Welche Herausforderungen gibt es derzeit im Hochleistungsrechnen?

Ein Aspekt betrifft Big Data: Die Rechenressourcen nehmen exponentiell zu und in den HPC-Simulationen generieren wir Unmengen an Daten, die wiederum analysiert und für weitere Forschung eingesetzt werden.

Bestimmte Simulationen werden über mehrere Rechenzentren hinweg vorgenommen. Die entsprechenden benötigten Hardwareressourcen sind an unterschiedlichen Standorten vorhanden. Darum sind wir auf ein schnelles Netz wie das X-WiN angewiesen, das unsere NHR-Rechenzentren miteinander verbindet.

Aber das ist nur ein Teil der Lösung: Wir müssen darauf achten, dass die Menge der transferierten Daten möglichst klein gehalten wird. Das erreichen wir, indem wir die berechneten Datensätze gleich an Ort und Stelle weiterverarbeiten. Idealerweise analysieren wir die Daten schon während der Simulation oder gleich danach –, erhalten also vorprozessierte Daten. Damit können wir deutlich kleinere Datenmengen übertragen. Besser wäre es natürlich, wenn wir die Daten gar nicht übertragen müssten, sondern sie auch lokal langzeitarchivieren könnten. Was die Langzeitarchivierung angeht, ist das bisher kein klassisches NHR-Thema. Hier treffen wir uns auf der Datenseite mit der Nationalen Forschungsdateninfrastruktur (NFDI).

Was hat der NHR-Verein bisher bewirkt? Ist Deutschland im internationalen Vergleich nun besser aufgestellt?

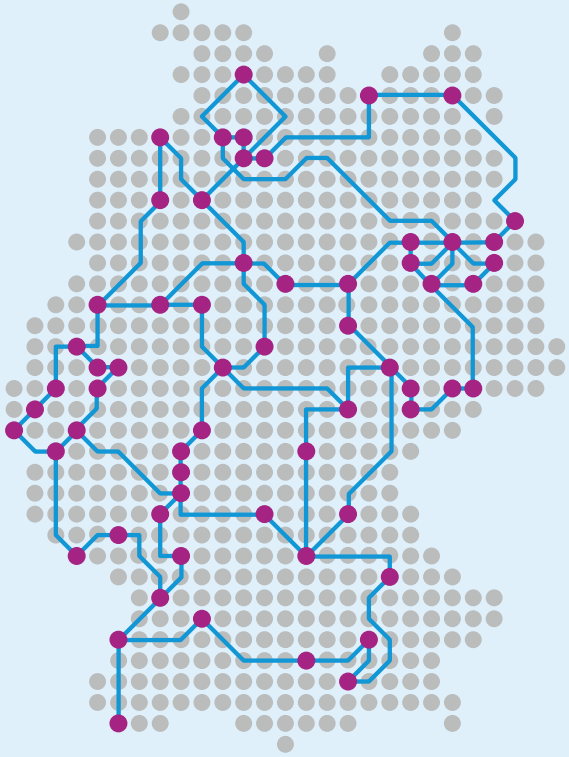
Auf jeden Fall! Damit meine ich aber nicht die medienwirksamen Top-500-Listen im Hochleistungsrechnen. Wenn Sie sich daran orientieren, dann stehen die Tier-1-Rechner ganz vorne. Wenn Sie aber die aggregierte Leistung der HPC-Systeme in Deutschland betrachten, sind die großen NHR-Zentren sehr präsent. Der Großteil der Forschung, die wichtige Fragestellungen etwa im Bereich der Katalysatorentwicklungen, der nachhaltigen Systeme oder der Energiematerialien betrifft, findet verstärkt auf Tier-2-Systemen statt. Mit unserem Beantragungssystem können Sie innerhalb eines Quartals Zugang zu exzellenten Rechenressourcen bekommen und Ihre Forschung auf international höchstem Niveau hier in Deutschland durchführen. Genau das macht unsere Wettbewerbsfähigkeit aus. Da hat der NHR-Verein die Tür weit geöffnet.

Das Gespräch führte
Maimona Id (DFN-Verein).

Leistungsstark und zuverlässig – das Wissenschaftsnetz X-WiN

Datenintensive Forschung mit gewaltigen Rechenressourcen wie im High Performance Computing (HPC), in der Multi-Messenger-Astronomie oder der Hochenergiephysik benötigt heute eine leistungsstarke Kommunikationsinfrastruktur, die in der Lage ist, große Datenmengen nahezu in Echtzeit zwischen disziplin- und länderübergreifenden Kooperationen großer Forschungskonsortien zu transferieren. Für die Wissenschaftscommunity in Deutschland betreibt und entwickelt der DFN-Verein in eigener Funktionsherrschaft das Wissenschaftsnetz X-WiN inklusive eines umfangreichen Portfolios aus netzgestützten IT-Services, die auf die anspruchsvollen Bedarfe in der Forschung zugeschnitten sind.

Mit einer Gesamtlänge von 10 250 km Glasfaser im Backbone und einem Multi-Terabit-Kernnetz, das sich zwischen 65 Kernnetzstandorten aufspannt, zählt das X-WiN zu den größten und leistungsfähigsten Forschungsnetzen weltweit. Es verbindet Hochschulen, außeruniversitäre Forschungseinrichtungen sowie forschungsnahe Wirtschaftsunternehmen an aktuell 849 Standorten bundesweit.



→ Für höchste Anforderungen

Die optische Plattform wird sowohl zum Aufspannen eines Netzes zwischen den IP-Routern des DFN als auch für virtuelle Private Netze (VPN) der Anwender genutzt, insbesondere wenn diese sehr hohe Anforderungen an die Bandbreite haben. Speziell für die Bedarfe des HPC bietet der DFN-Verein die Möglichkeit, dedizierte Kommunikationsinfrastrukturen, VPNs oder OPNs auf der Basis des X-WiN zu nutzen. Diese können national und in Zusammenarbeit mit den Partnernetzen des DFN auch international organisiert werden.

→ Auf Leistungsfähigkeit optimiert

Mit der optischen Übertragungsplattform sind eine Vielzahl von parallelen Verbindungen mit bis zu 400 Gbit/s und eine maximale Bandbreite zwischen zwei benachbarten Standorten des Kernnetzes 23,2 Tbit/s möglich.

Die Aggregations-Router werden aktuell durch eine neue Geräteklasse ersetzt und auf eine höhere Bandbreite umgerüstet. Diese bietet mit einer Gesamtkapazität von 2 400 Gbit/s pro System erhebliche Leistungsreserven für künftige Leistungssteigerungen im X-WiN. Für das nächste Jahr ist der Austausch der acht Core-Router durch wesentlich leistungsfähigere Systeme vorgesehen, die es ermöglichen, die Bandbreitenanforderungen auch jenseits der 400 Gbit/s Schwelle und damit auch zukünftige Bedarfe von Teilnehmern wie den HPC-Zentren zu erfüllen.

→ Internationale Konnektivität

In über 120 Ländern der Erde gibt es Nationale Forschungsnetze (National Research and Education Networks, NRENs) ähnlich dem Deutschen Forschungsnetz (DFN). Sie sind über regionale Backbone-Netze wie das europäische GÉANT auf der ganzen Welt miteinander verbunden. Das X-WiN ist aktuell mit 600 Gbit/s georedundant an GÉANT angeschlossen und verbindet DFN-Teilnehmer nicht nur national, sondern auch mit europäischen sowie weltweiten Wissenschaftsnetzen – über leistungsstarke Austauschpunkte außerdem mit dem allgemeinen Internet.

Kurzmeldungen

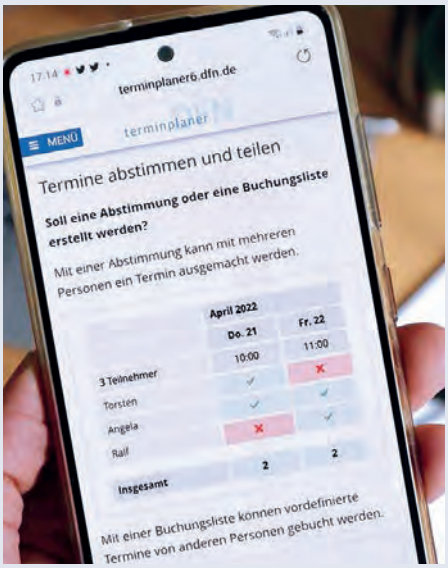
Gut im Plan: Modernisierung der Aggregationsplattform im X-WiN bald abgeschlossen

Die Migrationsphase der insgesamt 58 neuen Router-Systeme an 56 Standorten nähert sich ihrem Ende. Am Montag, 15. Mai 2023, war der DFN-Verein mit dem Deutschen Elektronen-Synchrotron DESY am Standort Zeuthen gestartet und seitdem in allen Himmelsrichtungen in Deutschland unterwegs. Vom Standort Bremen im Norden über Chemnitz im Osten und Dortmund im Westen bis hin zu Erlangen im Süden wurden bereits Stand Mitte Oktober 38 Kernnetzknoten mit den neuen Routern versorgt.

Mit der Modernisierung der Aggregationsplattform wird die verfügbare Switching-Leistung vervielfacht – auf 2,4 Tbit/s. Zum Vergleich: Die bisherige Router-Plattform verfügte über eine Leistung von 400 Gbit/s. Mit der neuen Switching-Leistung können teilnehmende Einrichtungen nun auch lokal mit 100-Gigabit-Ethernet angebunden werden. Das war bisher nur an den acht Core-Routern möglich. Die Migration endet voraussichtlich am 19. Dezember 2023 mit dem Kernnetzknotenstandort in Kaiserslautern. Ein herzlicher Dank geht an alle Kolleginnen und Kollegen der gastgebenden Einrichtungen unserer Kernnetzknoten, die uns beim Umbau tatkräftig unterstützt haben.

Fortsetzung folgt: Für 2024 sind die Aufrüstung der DWDM-Systeme mit 400+-Gbit/s-Transpondern und die Erneuerung der Core-Router geplant. ◆

Gleich ausprobieren! DFNTerminplaner jetzt mit neuem Umfragetool



Mit dem DFNTerminplaner können seit Neuestem nicht nur Termine abgestimmt, sondern auch unkompliziert textbasierte Umfragen beispielsweise für ein Teamevent erstellt werden. Das Ergebnis wird übersichtlich grafisch dargestellt – damit ist der Terminplaner ideal geeignet, um ein Meinungs- oder Stimmungsbild einzuholen.

Mit den unterschiedlichen Anwendungsmöglichkeiten der aktuellen Version lassen sich Termine, Veranstaltungen und Umfragen im Arbeitsalltag schnell und einfach organisieren. Um zu einer Abstimmung einzuladen, kann nicht nur auf die Kontakte des E-Mail-Programms zugegriffen, sondern auch direkt über den Terminplaner eingeladen werden. CSV-Exporte sind vollständig mit Excel kompatibel, die Kommentarfunktion ist deaktivierbar.

Für bestimmte Funktionen wie das neue Umfragetool ist ein Nutzerkonto notwendig. Vorteil: Angemeldete Nutzende können eine Übersicht ihrer eigenen Abstimmungen einsehen sowie alle selbst abgegebenen Stimmen zu Terminabfragen in einer übersichtlichen Kalenderansicht abrufen. Die Termine sind per iCal-Datei oder Webcal-Feed importierbar. Feste Termine wie Seminarplätze oder Raumreservierungen können mit dem Erstellen von Buchungslisten bequem koordiniert werden. Dabei besteht die Option, sowohl die maximale Teilnehmerzahl festzulegen als auch die Anzahl der zu wählenden Termine. Darüber hinaus können Buchungslisten fortgeschrieben und kopiert werden. Datenschutz und Datensparsamkeit stehen neben einer guten Bedienung im Vordergrund.

.

Aktuell liegt der DFNTerminplaner bei 3 274 294 gleichzeitig abgegebenen Stimmen, monatlich werden knapp 50 000 Abstimmungen neu erstellt und vom System etwa 200 000 E-Mails versendet. Einfach einloggen und loslegen! Wir sind gespannt auf das Feedback. ◆

Zum DFNTerminplaner geht es hier:
https://terminplaner6.dfn.de/

Kurzmeldungen

Cloud-Dienste für die Wissenschaft I: Neuausschreibung der Rahmenverträge in GN5-1

Nach erfolgreicher Beendigung des EU-Projekts Open Clouds for Research Environments (OCRE) im Dezember 2022 laufen derzeit die Vorbereitungen für die europäische Neuausschreibung der Cloud-Rahmenverträge im GÉANT-Projekt GN5-1. Als Partner der Wissenschaftscommunity in Deutschland ist der DFN-Verein hier für die Bedarfs- und Anforderungsbestimmung der Folgeausschreibung zuständig.

Die Angebote der aktuellen Rahmenverträge stehen bis zum Ende der Laufzeit November 2024 weiterhin zur Verfügung: Einzelabrufe (mit bis zu 4 Jahren Laufzeit) können bis Laufzeitende abgeschlossen werden. Einzelne Discounts (z. B. Microsoft) bleiben bis Oktober 2025 bestehen. Europaweit nutzen etwa 900 Einrichtungen aus 26 Ländern die aktuellen Rahmenverträge, das Auftragsvolumen beträgt mittlerweile circa 100 Millionen Euro jährlich. In Deutschland gibt es derzeit ein geringes Auftragsvolumen für externe Cloud-Dienste, erst 91 Einrichtungen haben Rahmenverträge beauftragt.

Der Fokus der Neuausschreibung liegt auf Leistungen vom Typ „IaaS+“. Darüber sind Dateninfrastrukturen, Plattformen und Dienste für Künstliche Intelligenz (KI), maschinelles Lernen, Container-Entwicklungsumgebungen bis hin zu Erdbeobachtungsdiensten erreichbar.

Mit einer Informationskampagne zu Beginn dieses Jahres sowie mehreren Cloud-Workshops wurden die unterschiedlichen Anforderungen der DFN-Community zusammengetragen und gemeinsam Möglichkeiten der Optimierung der bisherigen Rahmenverträge diskutiert.

Die dabei gesammelten Informationen wurden mit GÉANT und anderen europäischen Forschungsnetzen geteilt, um in Vorbereitung des Vergabeverfahrens entsprechende Leistungsanforderungen zusammenzustellen. Zuletzt wurde in einer Vorabinformation („Prior Information Notice“) auch möglichen Cloud-Anbietern die Gelegenheit geboten, Feedback auf diese Anforderungen zu geben und auf Umsetzbarkeit zu prüfen. ◆

Informationen zur DFN-Cloud erhalten Sie unter:
https://www.dfn.de/dienste/cloud

Cloud-Dienste für die Wissenschaft II: Föderierte Dienste

Von der Wissenschaft aus der Wissenschaft: In der Community besteht ein hohes Interesse an den Föderierten Diensten in der DFN-Cloud. Dabei handelt es sich um „Sync & Share“-Dienste wie bwSync & Share vom Karlsruher Institut für Technologie (KIT), GWDG ownCloud von der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), TU Berlin Collab Cloud von der Technischen Universität Berlin sowie UNIBW Sync&Share von der Universität der BW München. Einen „Compute & Store“-Dienst bietet mit der heiCLOUD die Universität Heidelberg an. Etwa 50 Einrichtungen nutzen einen oder mehrere dieser Services, am meisten verbreitet ist die TU Berlin Collab Cloud. Ein Neuzugang in der DFN-Cloud ist bwLehrpool von der Universität Freiburg und der Hochschule Offenburg (siehe Artikel S. 38). ◆

Neues zu den DFNconf-Rahmenverträgen für Cloud-basierte Web- und Videokonferenzdienste

Die Rahmenverträge für Cloud-basierte Web- und Videokonferenzdienste gehen in die Verlängerung: Nach intensiven Gesprächen sowohl mit teilnehmenden Einrichtungen als auch mit Anbietern und Vertriebspartnern wurde jetzt vereinbart, die Laufzeit der insgesamt sieben Rahmenverträge ab April 2024 um 24 Monate zu verlängern. Dabei handelt es sich um folgende Produkte: Zoom X (Telekom Deutschland GmbH), Cisco Webex (Deutsche Telekom Business Solutions GmbH), BigBlueButton (infra.run GmbH), Microsoft Teams (DrVis Software GmbH), Adobe Connect (reflact AG), OpenTalk (OpenTalk GmbH) und Class Collaborate (asknet Solutions AG).

Die Entscheidung wurde von allen Beteiligten begrüßt – nicht zuletzt, weil die Verlängerung die Planungssicherheit erhöht und Kostenstabilität garantiert. DFN-Teilnehmer haben nun bis März 2026 die Möglichkeit, Leistungen aus den Rahmenverträgen zu beauftragen. Diese Bestellungen haben eine eigene Laufzeit von bis zu zwei Jahren. ◆

Bei allen Fragen rund um die DFNconf-Rahmenverträge wenden Sie sich bitte per E-Mail an:
vertraege@conf.dfn.de

You are connected! Neuausschreibung für Teilnehmeranbindungen an das DFN-Kernnetz gestartet

Im Rahmen der europaweiten Neuausschreibung aller Carrier-Verbindungen wurde nach intensiver Vorbereitung und Durchführung eines vorgeschalteten Teilnahmewettbewerbs im Sommer 2023 das Angebotsverfahren eröffnet. Das betrifft Teilnehmerstandorte, die nicht über lokale, sondern über angemietete Datenleitungen an die Kernnetzknoten des Wissenschaftsnetzes X-WiN angebunden werden. Diese Teilnehmeranbindungen (TNA) stellt der DFN-Verein regelmäßig in den Wettbewerb, um qualitativ hochwertige und kosteneffiziente Angebote zu ermitteln. Neben aktuellen Datenraten wird den steigenden Anforderungen Rechnung getragen: So werden auch Optionen für Anbindungen mit bis zu 100 Gbit/s abgefragt.

Nach Prüfung und Bewertung der eingereichten Unterlagen wird der Zuschlag für Rahmenverträge und darin enthaltene Angebotsoptionen voraussichtlich zum Jahresanfang 2024 erteilt. Mit den ersten Beauftragungen von Teilnehmeranbindungen aus diesem Verfahren ist nach aktueller Planung in der ersten Jahreshälfte 2024 zu rechnen. ◆

Weitere Informationen zum Wissenschaftsnetz finden Sie unter:
https://www.dfn.de/netz

Die Welt der Qubits kennenlernen: Onlinekurs Quantum Algebra verfügbar

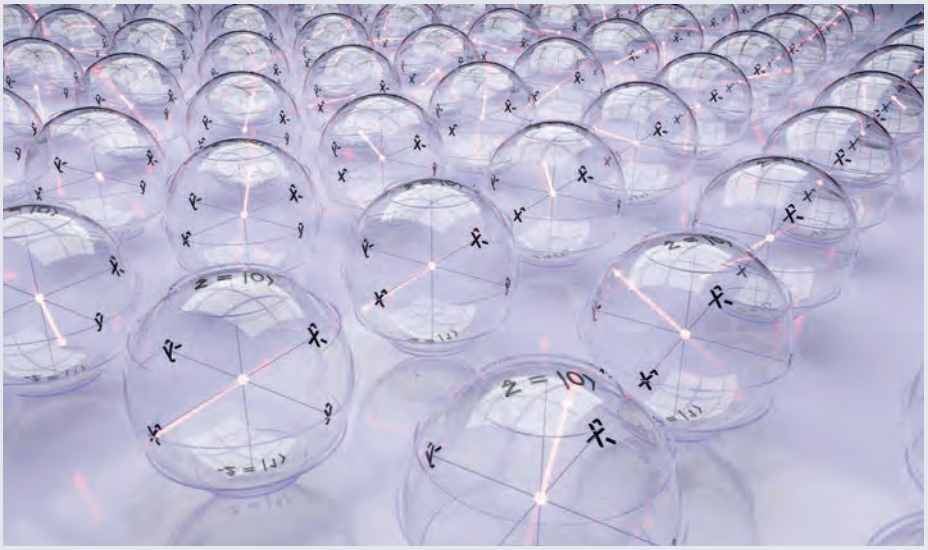


Foto: Peter Hansen/Adobe Stock

„Beam me up, Scotty!“ So heißt es an Bord des Raumschiffs Enterprise in der gleichnamigen, fast 60 Jahre alten Science-Fiction-Serie. Heute sind Verfahren wie Teleportation – zumindest von Lichtteilchen – in den Bereich des Möglichen gerückt. Um Quantentechnologien wie etwa den Aufbau von Quantennetzen besser verstehen zu können, hat Peter Kaufmann (DFN-Verein) im Rahmen der eAcademy des europäischen Forschungsnetzes GÉANT den mehrteiligen Onlinekurs „Quantum Algebra“ konzipiert. Mit Texten, audiounterstützten Erläuterungen und Übungsabschnitten sowie einem Quiz vermittelt der Kurs neben den mathematisch-physikalischen Grundlagen abwechslungsreich Wissen rund um die Themen Quantenverschränkung und Quantenteleportation. ◆

Die ersten beiden Teile „Qubits“ und „Operator Multiplication: Variants“ sind nun verfügbar und können auf der Webseite der GÉANT eAcademy abgerufen werden unter: **https://e-academy.geant.org/moodle/course/view.php?id=372§ion=1**

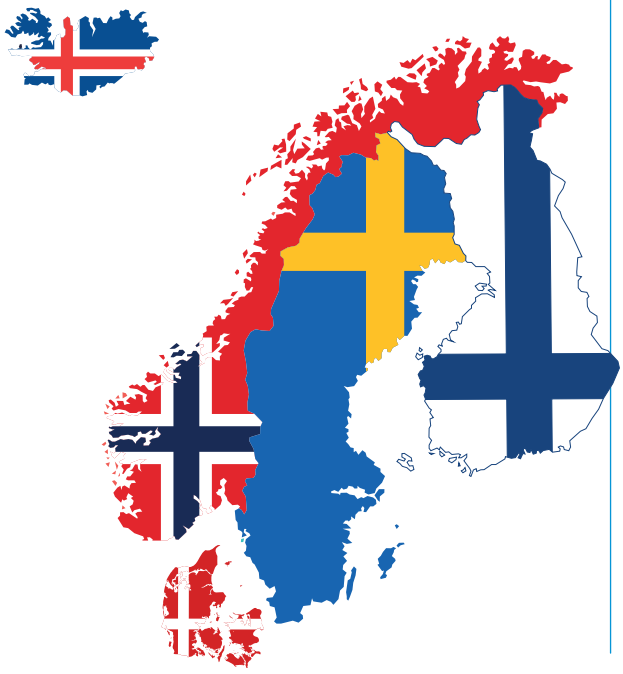
Um auf die GÉANT eAcademy zugreifen zu können, wählen Sie bitte für die Authentifizierung den Identity Provider Ihrer Heimateinrichtung oder den Login über ein Social Network.

Einblicke in das Thema liefert auch der Artikel „II. Quantenrevolution – die Welt der Qubits“ in der Ausgabe 99 der DFN-Mitteilungen, Seite 20 unter:
https://www2.dfn.de/fileadmin/5Presse/DFNMitteilungen/DFN_Mitteilungen_99.pdf

NORDUnet – a regional research and education network

Starke Partner weltweit

Konnektivität fördern, Zukunft gestalten, Herausforderungen gemeinsam meistern: Nationale Forschungsnetze rund um den Globus betreiben leistungsfähige Infrastrukturen für Wissenschaft, Forschung und Lehre. Ein Blick in die Welt der NREN-Community.



More than 400 research & education institutions in the Nordics, with over 1.2 million users, are connected via the Nordic NREN networks, enabling scientists, educators, and students to work and share knowledge globally. Each NREN has a national mandate, while NORDUnet acts to connect the NRENs in the region, and the region to the rest of the world. One milestone: For the benefit of all of Europe they have created the Polar Connect project, seeking to connect Europe and Asia through the Arctic Sea.

Text: **Lars Fischer** (NORDUnet)

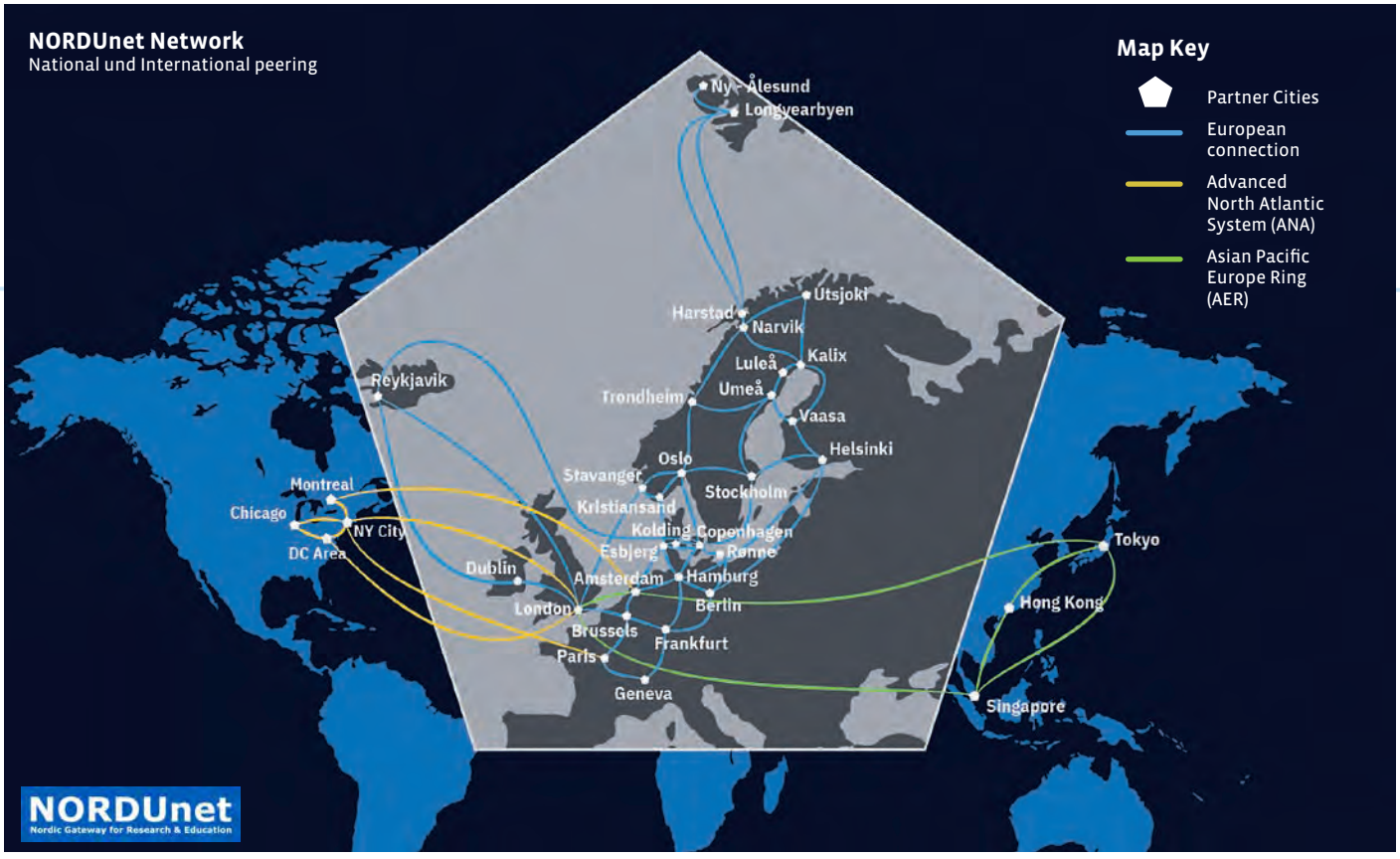
The Nordic Region

The Nordic region consists of five countries north of Germany: Denmark, Norway, Sweden, Finland, and Iceland. The countries cover a large geographic area, roughly three times that of Germany on the European continent plus Greenland, Iceland and the Faroe Islands in the North Atlantic. The region includes temperate farmland in the south and vast arctic tundra in the north. The population is 27 million, and the region has eight official languages.

The Nordic countries share a long history and have similar culture that emphasizes consensus, similar economies, and similar social structures. The countries have worked together in the Nordic Council since 1952 and had a passport union since 1954. The tradition for collaboration, especially in science, education, and culture is strong.

Origins of NORDUnet

In the 1970s, the first research network developments took place in the Nordic countries, notably the UNINETT program in Norway, the



DeiC
Danish e-infrastructure Consortium

Sikt
Norwegian Agency for Shared Services in Education and Research

SUNET
Swedish University Computer Network

RHnet
Icelandic Research and University Network

FUNET
Finnish University and Research Network

first country outside North America connected to ARPAnet. As networking between universities developed, the need for collaboration became clear. This led NordForsk – the research agency of the Nordic Council – to organize a meeting of Nordic experts in 1980: the first NORDUnet conference.

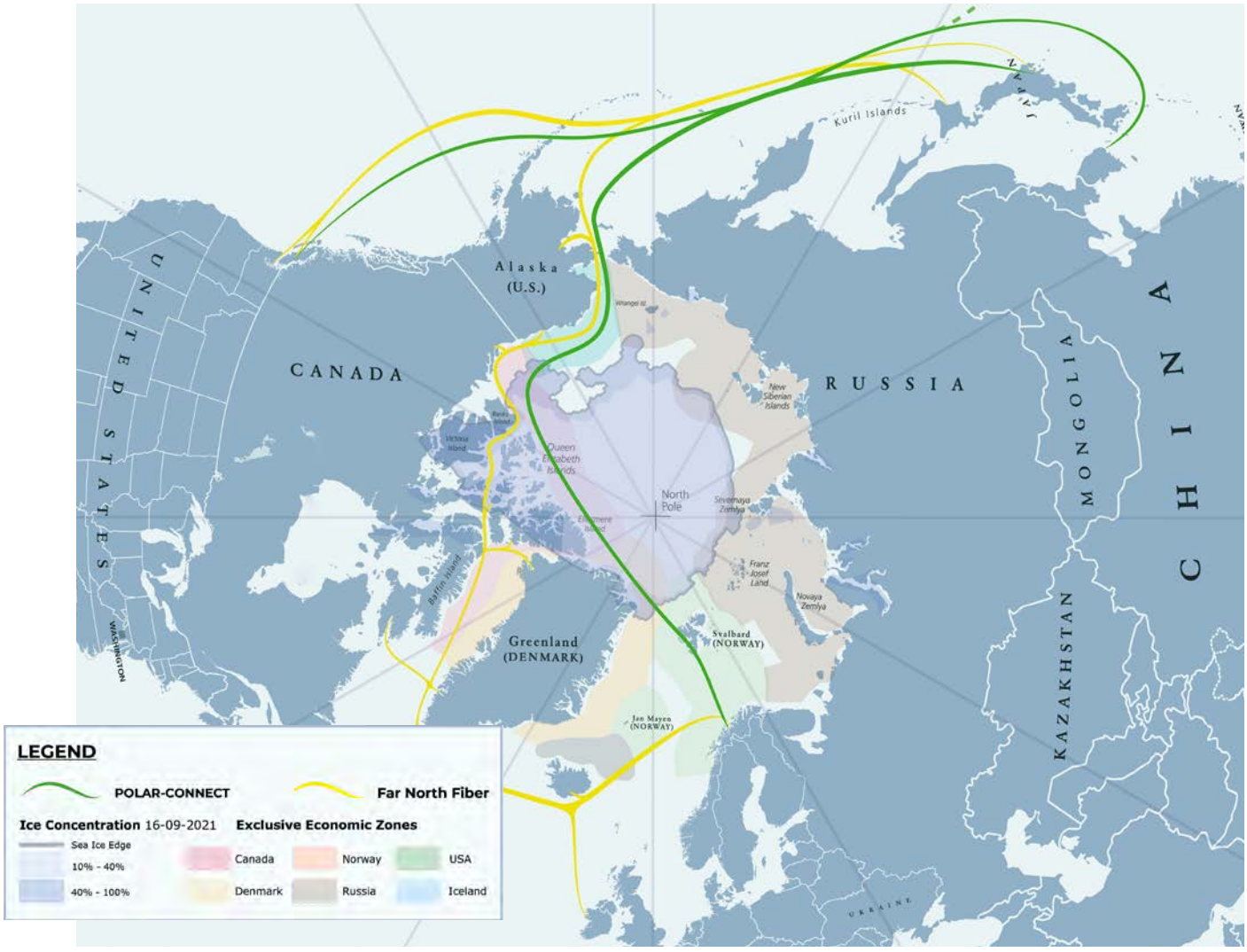
The NORDUnet conferences became an annual event and the focal point of the Nordic networking community. From the start, the community was focused on collaboration, developing national research networks in each country, and working together to connect the countries in the region while also forging stronger connections to the rest of Europe and to North America.

The 1980s saw the emergence of research networking across Europe, with many initiatives and technologies that came with it. From 1985, The Nordic Council of Ministers funded a project to establish a joint Nordic research and education network to connect the national networks that were being developed. Like the conference, this project was called NORDUnet. Eventually, the NORDUnet network deployed the TCP/IP protocols in 1988 and joined the internet developed in the USA, and the rest of Europe soon followed.

A regional network – NORDUnet and the Nordic NRENs

As networking for research and education (R&E) transitioned from experiments to infrastructure that research depends on, NORDUnet was incorporated in Denmark in 1992 as a company tasked with developing and operating a regional network. From the outset the model was clear: each Nordic country has its own national R&E network (NREN)[1], connecting universities and research institutions. Each NREN has a national mandate, while NORDUnet acts to connect the NRENs in the region, and the region to the rest of the world. The activities of NORDUnet are funded by the Nordic NRENs.

1 DeiC in Denmark, Funet in Finland, RHnet in Iceland, Sikt (formerly UNINETT) in Norway, and Sunet in Sweden.



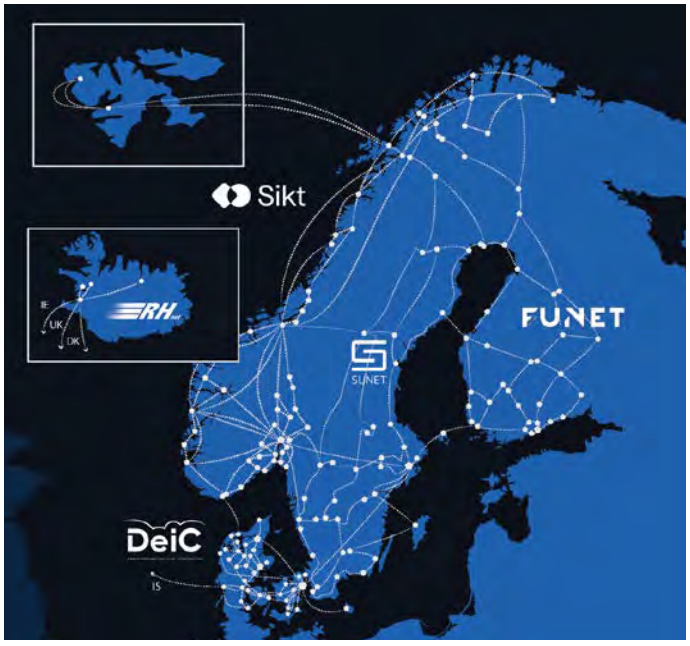
Connecting Europe and Asia through the Arctic Sea: These Routes are way shorter than current routes between Europe and Asia. Thereby latency can be kept at a minimum.

Throughout the 1990s, network connectivity was highly expensive, and with NORDUnet acting as a market aggregator, the organization had more purchasing power and was able to get better prices and more powerful connections.

In the same period, European collaboration in research networking was maturing. Through a series of EU-funded projects the GÉANT network developed, connecting all of Europe. In these projects, NORDUnet was the partner on behalf of all the Nordic NRENs. The Nordic NRENs connect to the GÉANT network through NORDUnet, and they contribute to the GÉANT projects and the evolution of the GÉANT infrastructure as part of NORDUnet.

Through the approach, three pillars emerged for the regional network: joint development, joint procurement, and joint representation. By pooling resources to develop new infrastructures and services together, by procuring expensive resources together, and by jointly representing a joint Nordic voice in European and global collaborations, the relatively small Nordic countries have been able to punch above their weight and have impact on the evolution of research networking.

With collaboration at its heart, NORDUnet has been instrumental ensuring cross-border functionality and sharing. When national identity federations were developed, the Kalmar2 project developed inter-federations between the countries, a development that led to eduGAIN. When NRENs deployed their own optical fibre networks, NORDUnet led initiatives to share optical networks across borders, a technology now known as spectrum sharing and used throughout Europe.



The Nordic Network and Joint Nordic Services

It is important to understand that NORDUnet does not exist as an alternative to or a competitor of European collaboration. The Nordic NRENs are fully part of and committed to European collaboration in GÉANT. Instead, NORDUnet represents a desire to do more than may be possible in the larger European collaboration.

The NORDUnet network is built entirely through sharing national optical networks, a radical approach to building a joint network. This model has enabled a model where each NREN must have more than three connections to the rest of the world, and that no country can be connected to only one other country. By using the approach, the Nordic NRENs have realized a very high level of resilience and redundancy, a quality of growing importance in a time of geopolitical challenges.

NORDUnet has developed a global network footprint, allowing NORDUnet to peer and exchange traffic with cloud providers around the world, with no middleman, ensuring high network quality to all resources. And across their borders, the Nordic NRENs have interconnected their networks, allowing such developments as the recent deployment of a 12 terabit-per-second network in the Arctic for the EISCAT_3D instrument.

NORDUnet has deploying locally hosted versions of key components for the digital transition of education, such as a privately hosted Zoom platform and locally hosted media services. By scaling these local platforms, the Nordic NRENs wer able to serve the Nordic universities with advanced remote education services through the COVID-19 years.

NORDUnet, Europe, and the world

The Nordic countries are part of Europe – and indeed the world. We are small countries, and we appreciate that we can only be effective when we work together for research and education. European and global collaboration is essential for NORDUnet. The GÉANT projects and the GÉANT collaboration of European NRENs is critical for NORDUnet in realizing our mission of connecting the Nordic countries to the world.

It should therefore be no surprise that NORDUnet is an active and enthusiastic partner in European projects and initiatives. We seek to drive the evolution of global network collaborations, of trust and identity infrastructure, support for student mobility, and much more. And we welcome all European partners in collaborations.

In support of Nordic research communities, we are currently part of initiatives to use optical networks, including those using cables that cross the oceans, as well as high-precision scientific sensors – and we are pleased to work with German research partners on some of these projects.

Inspired by the growing need for European – Asian network capacity and the geopolitical challenges for such network connections, we have created the Polar Connect project, seeking to connect Europe and Asia through the Arctic Sea. We are pleased to have formed partnerships with the European Commission and the GÉANT collaboration in aiming to forge such connections for the benefit of all of Europe.

The Nordic NRENs and DFN have a strong history of collaboration, from the early development of eduroam to leading the development of the pan-European Infrastructure-as-a-Service procurement in the GÉANT and OCRE projects. And with NORDUnet as the collaboration hub and facilitator, finding Nordic partners for new collaborations is never further away than contacting NORDUnet. Collaboration is why we are here. ◆

Wer hat an der Uhr gedreht? Zeitsynchronisation mit PTP

Text: **Susanne Naegele-Jackson, Sascha Schweiger, Martin Seidel** (WiN-Labor der Universität Erlangen-Nürnberg)

In der Welt der Computertechnologie ist das Network Time Protocol (NTP) weit verbreitet und aufgrund seiner einfachen Handhabung bei Nutzenden beliebt. Es ermöglicht eine regelmäßige Synchronisierung der Systemzeit, ohne dass sich mit dem manuellem Einstellen von Sommer- und Winterzeit befasst werden muss. Im alltäglichen Einsatz sind Abweichungen von einigen Millisekunden meist ausreichend präzise. Jedoch stößt NTP in Bereichen wie Industrie, Telekommunikation und Wissenschaft, wo Präzision und Genauigkeit von entscheidender Bedeutung sind, an seine Grenzen. Hier kommt das Precision Time Protocol (PTP) – IEEE 1588 Standard – ins Spiel, das im Vergleich zum wesentlich einfacher implementierten NTP eine deutlich genauere Zeitabstimmung zwischen Geräten ermöglicht.

Foto: sergeyparser/freepik

Das Precision Time Protocol (PTP) wurde entwickelt, um anspruchsvollen Anwendungen gerecht zu werden. In der Netzwerküberwachung werden hochpräzise Zeitstempel benötigt, um die Anzahl an gesendeten oder empfangenen Paketen bei hohen Übertragungsraten (Gbit) zu erfassen. Ein weiteres Anwendungsgebiet ist der Hochfrequenzhandel mit Aktien. Hier führen Algorithmen in kürzester Zeit, teilweise im Mikrosekundenbereich, selbstständig Kauf- und Verkaufsoperationen durch, ohne dass ein menschliches Eingreifen erforderlich ist.

PTP ist ein auf Paketen und dem Leader-Follower-Prinzip[1] basierendes Protokoll, das bei Bedarf zur hochgenauen Synchronisation von Geräten in einem Netzwerk dient. Mit dem Standard PTPv1 kann eine Genauigkeit im Mikrosekundenbereich erreicht werden, während die neueste Revision v2.1 sogar eine Genauigkeit bis in den Sub-Nanosekundenbereich ermöglicht.

Die Ursprünge

IEEE 1588-2002, auch PTPv1 genannt, ist die erste Version des Standards und definiert das Basisprotokoll. Im Vergleich zu seinen Nachfolgern bietet PTPv1 eine geringere Genauigkeit und Funktionalität. Dies liegt daran, dass PTPv1 bei der Berechnung der Zeitstempel im Protokoll ausschließlich von einem symmetrischen Delay (Round-Trip-Time/2) ausgeht und asymmetrische oder hardwarebedingte Verzögerungen und andere Effekte nicht berücksichtigt.

… wie v1, nur besser

IEEE 1588-2008 (PTPv2) enthält gegenüber der Version 1 eine Reihe von Verbesserungen, die nun theoretisch Genauigkeiten im Nanosekundenbereich ermöglichen. Neben einer generellen Erhöhung der Genauigkeit der Zeitsynchronisation können nun durch zusätzliche Optionen im Bereich Fehlertoleranz und Redundanz robustere Systeme aufgebaut werden. Aufgrund dieser umfassenden Verbesserungen des Protokolls ist PTPv2 allerdings nicht mehr mit dem Vorgängerstandard kompatibel.

Ein weiterer Fortschritt der zweiten Version ist die Einführung bzw. Unterstützung von transparenten Uhren und höheren Abtastraten. Transparente Uhren sind Netzwerkgeräte, die die Synchronisation der Uhren innerhalb einer PTP-Domäne verbessern, indem sie die durch das Netzwerk verursachte Verzögerung messen. Diese Verzögerung wird in den Zeitstempeln der PTP-Nachrichten berücksichtigt und ermöglicht so eine präzisere Synchronisation zwischen den Uhren.

Zeitsynchronisation mit Profil

Eine weitere wichtige Neuerung ist die offizielle Einführung von Profilen. Ein Profil definiert die Anforderungen und Konfigurationsoptionen für die Anwendung des Standards in einem bestimmten Bereich, wie beispielsweise der Telekommunikation, der industriellen Automatisierung oder bei Test- und Messsystemen. Dadurch kann der Standard besser an Anwendungen angepasst werden. Im besten Fall sind solche Profile bereits in der verwendeten Hardware integriert, sodass Anwendende das Protokoll ohne größere Anpassungen direkt einsetzen können.

Ein solches Profil wurde unter dem Namen High Accuracy Profile als drittes IEEE 1588-2019 Standard-PTP-Profil eingeführt. Dabei handelt es sich um White-Rabbit-Technologie, die ursprünglich als Idee am Schweizer Forschungszentrum CERN entstanden ist. Die Technologie wurde im Rahmen der Erneuerung und Verbesserung des bisher dort eingesetzten Timing-und-Controlling-Systems entwickelt. Das Profil ermöglicht eine präzise Phasendetektion, Kalibrierung und Onlineschätzung von Asymmetrien sowie eine Angleichung der Frequenz der lokalen PTP-Uhr. Die Uhr weist eine Genauigkeit im Sub-Nanosekundenbereich und eine Präzision im Pikosekundenbereich auf.

Das Prinzip PTP

Egal welche Revision wir betrachten, das Grundprinzip bleibt gleich:

Zum Zeitpunkt t1 sendet der Leader eine Sync-Message mit der ihm bekannten Zeit an den Follower. Dieser verfügt beim Empfang der Nachricht zum Zeitpunkt t2 bereits über die Zeitstempel t1 und t2 und kann somit berechnen, inwiefern seine eigene Zeit abgewichen ist. Da jedoch bei Empfang der Nachricht um t2 bereits wieder Zeit vergangen ist, kann diese Zeitreferenz nicht als exakt bezeichnet werden. Um den Netzwerkdelay angemessen zu berücksichtigen, wird vom Follower ein Delay_Req an den Leader versendet, der wiederum mit einem Zeitstempel antwortet, woraus der Follower die Verzögerung errechnen kann, welche durch das Netzwerk entstanden ist.

Wie zu erwarten, können hier nur gute Genauigkeiten erreicht werden, wenn die Kommunikationswege symmetrisch sind.

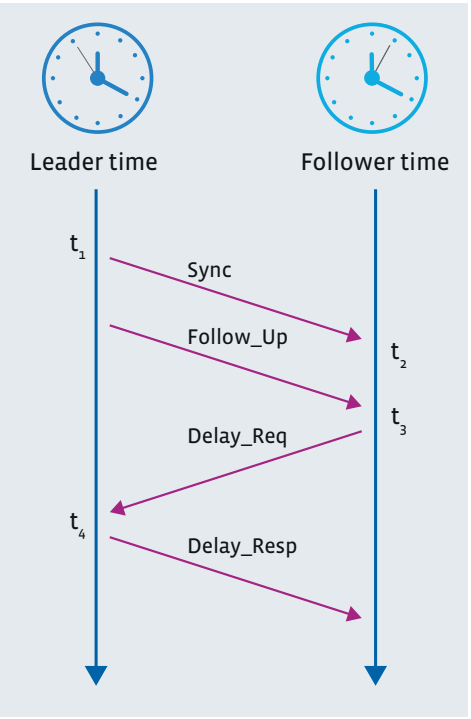


Abbildung 1: Ablauf PTP-Sychronisierung

1 Das Leader/Follower-Prinzip entspricht dem Master/Slave-Prinzip aus IEEE 1588.

Taktsyntonisierung–SyncE

Synchronous Ethernet ist eine Technologie zur Synchronisation mittels eines gemeinsamen Taktsignals, d. h. die Frequenz (125 MHz) wird auf dem physikalischen Kanal mitgeliefert. Die Taktableitung aus dem Nutzsignal ist jederzeit möglich, selbst wenn keine Datenübertragung stattfindet. Die Angleichung der Frequenz zweier Uhren wird als Syntonisierung bezeichnet.

Da White-Rabbit-PTP auf SyncE angewiesen ist, muss gewährleistet werden, dass jedes Gerät im Netzwerk SyncE-fähig ist und damit eine durchgehende SyncE-Verbindung im Netz besteht.

Analog zu PTP wird der Roundtrip Delay anhand von vier Zeitstempeln ermittelt, jedoch werden unterschiedliche Laufzeiten (link asymmetry) für den Hin- bzw. Rückweg mitberücksichtigt. Link-Asymmetrien treten unter anderem auf, wenn für das Senden bzw. Empfangen unterschiedliche Wellenlängen (Glasfaser) verwendet werden.

Phasenmessung

Das Kernstück von White Rabbit sind die Bestimmung der Phase ph_S und der Abgleich der Roundtripphase ph_{MM}. Dadurch wird zusammen mit SyncE und der Bestimmung des asymmetrischen Delays eine Verbesserung der Präzision bei der Zeitsynchronisation gegenüber PTPv2 ermöglicht. Die vollständige Funktionsweise von White Rabbit ist jedoch sehr komplex, sie wird in der White-Rabbit-Spezifikation beschrieben (Link im Quellenkasten).

Die SyncE-Technologie sorgt für eine Kopplung der Frequenzen von Follower- und Leaderclock. Die steigenden oder fallenden Flanken des Taktsignals (Frequenz) werden dafür verwendet, Signale auf der Sender- und Empfängerseite zu detektieren:

In Abbildung 2 werden der Effekt der Frequenzanpassung (Syntonisierung) mit SyncE (Taktsignale 1–3) und des Phasenangleichs

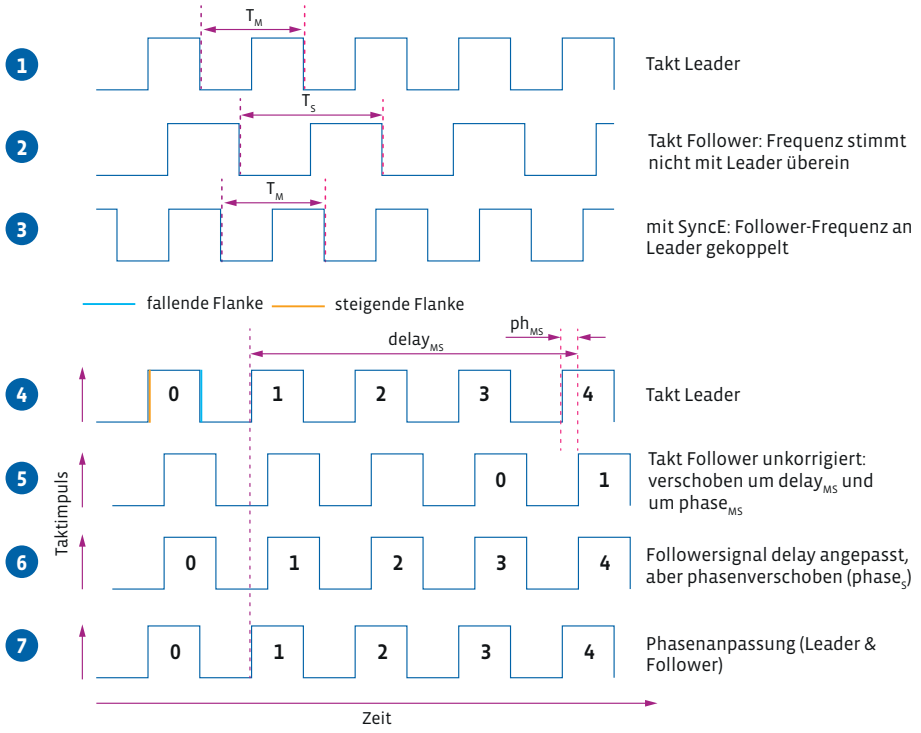


Abbildung 2: Frequenz-, Delay- und Phasenkorrektur

auf das Taktsignal der Follower-Clock dargestellt (Taktsignale 4–7). Wie aus der Abbildung zu entnehmen ist, stimmen die Periode (T_M) der Leader- (Signalform 1) und die Follower-clock (T_S, Signalform 2) nicht überein. Durch Anwendung des SyncE-Verfahrens wird das Taktsignal des Followers an das Leaderclock-Signal gekoppelt und die Periodendauer ist danach bei beiden Takten gleich (TS=TM, Signalform 3).

Die Laufzeit des Leader-Taktsignals – also die Zeit, die das Leader-Taktsignal zum Erreichen der Followerclock benötigt – ist in Signalform 4 durch Ziffern in den Taktperioden gekennzeichnet: Demnach vergehen drei Taktzyklen, bevor das Taktsignal den Follower erreicht. Der Follower kann das Signal des Leaders jedoch nur mit einer steigenden oder fallenden Flanke detektieren. Werden die Signalform 4 und 5 (Taktsignal Follower) übereinandergelegt, so erkennt man, dass der Follower das Signal des Leaders nicht sofort bei Eintreffen des Signals, sondern erst mit der nächsten steigenden Flanke detektiert. Dieser Unterschied wird als Phasenversatz ph_{MS} bezeichnet. Wird zur Laufzeit des Leadersignals der Phasenversatz $phase_{MS}$ addiert, ergibt sich die Gesamtverzögerung $delay_{MS}$. Signalform 6 ist das vom Follower ausgehende Taktsignal an den Leader, das mittels eines Phasenschiebers (siehe Abbildung 3) um die frei einstellbare Phase ph_S verzögert wurde. Dieses Signal wird wiederum vom Leader detektiert, um die sogenannte Roundtripphase ph_{MM}, die den Phasenunterschied zwischen dem vom Leader ausgesendeten und empfangenen Signal angibt, zu erfassen.

Mit den Laufzeiten δ_{MS} und δ_{SM} (siehe Abbildung 3) für den Hin- und Rückweg des Signals zwischen Leader- und Followerclock ergibt sich:

$$phase_{MM} = (\delta_{ms} + \delta_{sm} + ph_s) mod\ T_{ref}$$

Wobei T_{ref} die Frequenzperiode der Leaderclock ist. Bei 125 MHz sind dies 8 Nanosekunden. Damit wird deutlich, dass mit White Rabbit eine Präzision bis in den Sub-Nanosekundenbereich möglich ist. Die Abkürzung mod steht für Modulo Operator, der als Ergebnis den Rest einer Division liefert, zum Beispiel 3 mod 2 = 1.

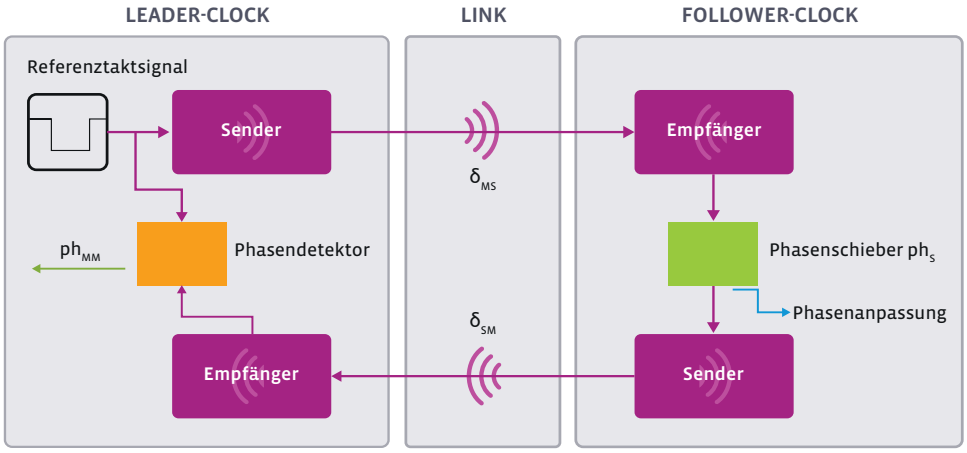


Abbildung 3: White-Rabbit-Link-Modell und Roundtripphase

Ist der Phasenversatz ausgeglichen, lassen sich wiederum präzisere Zeitstempel für den Roundtripdelay ermitteln, und der Offset zwischen der Leader- und der Followerclock wird weiter verringert. Durch einen Vergleich von Signalform 4 und 7 in Abbildung 2 wird deutlich, dass das vom Leader ausgehende Signal jetzt derart phasenverschoben ist, dass das Signal bei Ankunft am Follower eine steigende Flanke hat und das Signal dadurch sofort detektiert wird, d. h. der Phasenversatz $phase_{MS}$ ist jetzt eliminiert.

Zusammenfassend zeigt PTP exemplarisch die rasante Entwicklung in der Zeitmesstechnologie und den wachsenden Bedarf nach immer präziseren und genauer synchronisierten Zeitmessungen in modernen Netzwerken und Anwendungen, sei es in den Bereichen Telekommunikation, Wissenschaft oder Wirtschaft.

Das Network Time Protocol (NTP) bietet eine bewährte und weitverbreitete Methode zur Synchronisation von Uhren über das Internet, während das Precision Time Protocol (PTP) in seinen verschiedenen Versionen und Ausprägungen als präzisere und robustere Option für lokale Netzwerke gilt. Besonders bemerkenswert ist die hochgenaue Zeitverteilung mit dem White-Rabbit-Projekt, welches es mit SyncE und PTPv2 als Grundlage geschafft hat, als Standardprofil in die Revision 2.1 von PTP integriert zu werden. Dadurch wird eine hochpräzise Zeitmessung zugänglicher. ◆

PROTOKOLL	ERZIELBARE PRÄZISION	ANWENDUNGEN
NTP	Millisekundenbereich	Abgleich von Server-systemzeiten
PTPv1, PTPv2	Mikro- bis Nanosekundenbereich	Hochfrequenzhandel, Netzwerkmonitoring
PTPv2.1 / White Rabbit / High Accuracy Profile	bis in den Sub-Nanosekundenbereich	Spezialanwendungen in Wissenschaft und Technik wie der Erfassung von Sensordaten am CERN

QUELLEN UND WEITERFÜHRENDE INFORMATIONEN:

IEEE 1588-2019 : [https://standards.ieee.org/ieee/1588/6825/]

White-Rabbit-Spezifikation: [https://ohwr.org/project/wr-std/wikis/Documents/White-Rabbit-Specification-(Revision-History)](aktuell 2.0) [https://white-rabbit.web.cern.ch]

Das WiN-Labor entwickelt Software und Tools im Auftrag des DFN -Vereins. Seit 1992, mit Beginn des damaligen „2-Mbit-WiN-Labor-Projektes", ist das WiN-Labor am Regionalen Rechenzentrum (RRZE) der Universität Erlangen-Nürnberg angesiedelt.

Es beschäftigt sich derzeit vor allem mit Untersuchungen zu Quantennetzwerken und mit Techniken zur Zeitsynchronisation im Netz.

https://www.win-labor.dfn.de

Den Notfall trainieren

Bei einem Unfall oder Notfall diktiert im Rahmen der Ersten Hilfe die Rettungskette, welche Maßnahmen wann und wie zu ergreifen sind. In der Informationssicherheit ist ein solch strukturiertes Vorgehen weniger bekannt. Jochen Becker, Leiter des Computer Emergency Response Team und stellvertretender Chief Information Security Officer (CISO) der TU Darmstadt, ist ehrenamtlich im Katastrophenschutz tätig. Er plädiert dafür, analog zur Ersten Hilfe, in jeder Hochschuleinrichtung digitale Ersthelfende zu haben.

Text: **Jochen Becker** (TU Darmstadt)

Foto: photoPepp/Adobe Stock

Völlig überraschend, wie aus dem Nichts tritt er ein – der Notfall. Alles muss jetzt schnell gehen. Sofortmaßnahmen werden eingeleitet: Überblick verschaffen, die Unfallstelle absichern und natürlich an den Eigenschutz denken. Als Laie kümmere ich mich um Unterstützung: Ich spreche Umstehende an beziehungsweise setze selbst einen Notruf ab. Ich leite lebensrettende Maßnahmen ein und versorge gegebenenfalls akute Blutungen. Bis zum Eintreffen der Rettungskräfte setze ich die Maßnahmen um, die ich gelernt habe. Ist der Rettungsdienst vor Ort, übergebe ich an die Expertinnen und Experten. Mein Job als Ersthelfer ist damit erst einmal abgeschlossen. Kennen Sie das nicht? Genau, das Einmaleins der Ersten Hilfe.

Wäre es nicht toll, wenn wir dieses „Erste-Hilfe-Konzept“ auch für digitale Notfälle hätten? IT ist heute so komplex wie ein menschlicher Körper. Wie lerne ich vorab, kleine Störungen oder leichte Verletzungen von einer ernsthaften Erkrankung zu unterscheiden? Über Jahre hinweg hat sich in der IT jeder so seine eigenen Zugänge zu dem Thema verschafft. Ein geordnetes Vorgehen ist jedoch noch nicht etabliert.

BSI-Leitfaden für digitale Ersthelfende

Im Rahmen meiner Recherchen bin ich auf den „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“ gestoßen, der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) seit 2021 herausgegeben wird. Neben den verschiedenen Arten von Störungen werden darin das Erkennen eines Notfalls dargestellt und Verhaltensweisen vermittelt. Anhand einer digitalen Rettungskette werden die einzelnen Eskalationsstufen erklärt, um eine Systematik ähnlich zum Erste-Hilfe-Konzept herzustellen (siehe Abbildung 1).

Jetzt gibt es also digitale Ersthelfende. Aber wer hat überhaupt Kenntnis von deren Vorgehensweise? Oder ist es wie beim Erste-Hilfe-Kurs? Jeder hat davon gehört, aber wie das eigentliche, praktische Training im Notfall funktioniert, ist entweder nicht bekannt oder vergessen, weil der letzte Kurs viel zu lange her ist.

In Unternehmen ist in puncto Arbeitsschutz schon viel passiert. Über die Jahre haben die Berufsgenossenschaften über Regularien und Kontrollen eine Verbesserung erreicht. Dadurch passieren weniger Unfälle und Verletzungen in den Betrieben. Auch wird die Ausstattung stetig verbessert: So sind Notruftelefone, Notrufnummern, Feuerlöscher, Erste-Hilfe-Kästen und seit „Neuestem“ auch AED-Geräte (Defibrillatoren) in nahezu jedem Büro zu finden.

Mit dem BSI gibt es eine zentrale Stelle, die sich wie die Berufsgenossenschaften Gedanken über sinnvolle Maßnahmen macht und grundsätzliche Regelungen erlässt. In der BSI-Kritisverordnung (KritisV) wird beispielsweise definiert, welche Einrichtungen als kritische Infrastrukturen für das Versorgen der Bevölkerung oder das Funktionieren des staatlichen Gemeinwesens gelten. Darüber hinaus werden die Pflichten sehr genau aufgezeigt.

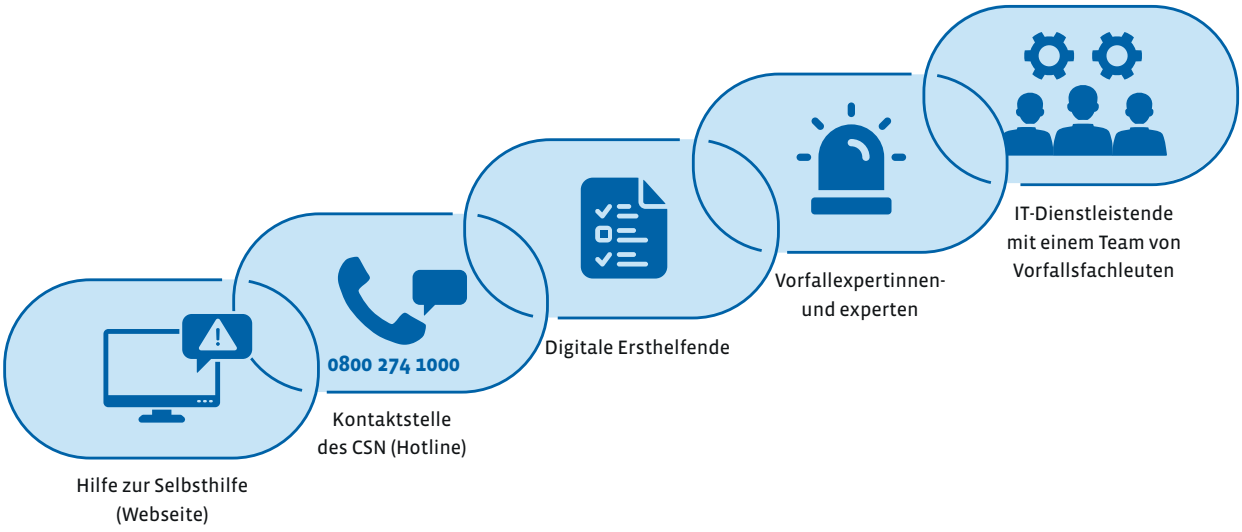


Abbildung 1: Hilft, schwere Schäden einzudämmen – die Rettungskette bei Sicherheitsvorfällen (Quelle: BSI-Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer)

Wie kann ich an dieser Stelle mitwirken oder unterstützen, damit nicht erst durch Unfälle und teure Schäden ein Bewusstsein geschaffen wird? Indem ich in meiner Einrichtung dafür Sorge trage, dass es neben Ersthelfenden auch Digitale Ersthelfende gibt, dass neben Brandschutztüren auch Antivirensoftware flächendeckend vorhanden ist und analog zur 112 die Rufnummer zu einem CERT oder einem Notfallkontakt etabliert wird. Das allein wird weitere Folgen haben: das Beschneiden von vermeintlichen Freiheiten im Umgang mit der IT, das Schaffen und Vorhalten von Reserven an Personal oder anderen Ressourcen für den Notfall, das Schulen von Mitarbeitenden. Das klingt alles sehr zeit- und kostenintensiv. Die Denkweise, bisher ist immer alles gut gegangen und es trifft ja zumeist die anderen, ist leider weit verbreitet – obwohl die Anzahl und Intensität von Cyberangriffen auf Hochschulen extrem zugenommen hat.

In der IT-Sicherheit ist es wichtig, dass sofort gehandelt wird. Unterlassen oder Abwarten ist schädlich. Im Gegensatz zur Ersten Hilfe für Menschen und zum Glück für digitale Ersthelfende gibt es einen entscheidenden Vorteil: In den meisten oder fast allen alltäglichen Fällen ist nicht unmittelbar ein Menschenleben bedroht.

In der IT-Sicherheit ist es häufig so, dass sich zwar nach einem Vorfall intensiv damit auseinandergesetzt wird, jedoch nicht langfristig genug und auch nicht finanziell nachhaltig. Die entsprechenden Reserven aus Menschen und Geräten samt notwendigen Prozessen zur Bewältigung eines Sicherheitsvorfalls können so nicht aufgebaut werden. Es ist eben schwer zu argumentieren, dass diese Reserven dringend notwendig sind, obwohl sie – wenn es gut läuft – die meiste Zeit nicht genutzt werden. Mit Blick auf den Zivil- und Katastrophenschutz während der Coronapandemie oder der Ahrtal-Flut hat sich deutlich gezeigt, dass es sinnvoll ist, Vorbereitungen zu treffen und Reserven zu bilden. So konnte zur Bewältigung dieser Ereignisse auf vorhandene Strukturen wie Krisenstäbe und Führungssysteme zurückgegriffen werden. Obwohl durchaus bewährt, werden diese Strukturen stets aufs Neue infrage gestellt.

Im Krisenfall: die besondere Aufbauorganisation (BAO)

Im IT-Notfallmanagement oder beim Planen des Umgangs mit einem IT-Notfall, der unter Umständen mit einem Cyberan-

Dipl.-Inform. Jochen Becker

Leiter des Computer Emergency Response Team der TU Darmstadt und stellvertretender Chief Information Security Officer (CISO)

Vortragender bei der 79. DFN-Betriebstagung im Forum Sicherheit zum Thema „Notfallmanagement: die ersten 24 Stunden nach (und vor!) einer Kompromittierung“

Foto: DFN

griff (Ransomware) oder dem zentralen Datenverlust einhergeht, ist es wichtig, vorab zu wissen, wo welche Daten liegen und wer wo Ansprechperson ist. Gemäß BSI-Standard 200-4 sollte nicht erst im IT-Notfall festgestellt werden, dass eine gewöhnliche Führungsstruktur und Hierarchie, auch Allgemeine Aufbauorganisation (AAO) genannt, mit der Lage überfordert ist. An dieser Stelle wird eine andere Struktur – die besondere Aufbauorganisation (BAO) – benötigt, in der eben nicht zwingend dieselben Personen wie im Normalbetrieb Leitungsaufgaben übernehmen. Die BAO ist wie ein Krisenstab im Katastrophenschutz, sie plant und übt den Ernstfall am Reißbrett (Stabsrahmenübungen), sie verfügt über ihre eigenen Rettungskräfte und Einheiten auf Abruf, um bei Bedarf unmittelbar tätig werden zu können.

In der Hochschulrealität sieht es anders aus: Welche Einrichtung hat über das IT-Stammpersonal hinaus Kapazitäten für das notwendige zusätzliche Personal für IT-Sicherheit? Denn dabei handelt es sich um Personen und Ressourcen, die im gewöhnlichen Betrieb keinen fühlbaren Mehrwert bringen, sondern vermeintlich einen zusätzlichen Aufwand verursachen. Häufig wird verlangt, dass sich diese Bereiche selbst verargumentieren und ihre Daseinsberechtigung begründen. Dabei sollte sich jede IT-betreibende Einrichtung darum kümmern, diese Bereiche für IT-Sicherheit aufzubauen und zu unterstützen. Falls es dann noch möglich ist, dass sich diese Teams ausschließlich auf den IT-Notfall sowie auf die Prävention konzentrieren und darüber hinaus einrichtungsübergreifend tätig werden dürfen, dann hat man langsam das erreicht, was es im Rettungsdienst, bei der Feuerwehr und dem Katastrophenschutz schon lange gibt – die Rettungskette, das strukturierte Vorbereiten auf Notfälle, die über Betriebsstörungen hinausgehen.

Jede größere Einrichtung benötigt den Zugriff auf ein Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT) oder Security Operations Center (SOC), welchen Begriff man auch gerade aktiv verwenden möchte. Diese Bereiche benötigen ausreichend Mittel und Möglichkeiten, um ihre Aufgabe der proaktiven IT-Sicherheit möglichst gut erfüllen zu können. Sie sind bei einem Sicherheitsvorfall die erste Adresse für ihre digitalen Ersthelfenden. Mit dem DFN-CERT ist für alle am X-WiN teilnehmenden Einrichtungen eine zentrale Stelle mit einem sehr guten Kontakt in den CERT-Bund vorhanden. Dessen Unterstützung stößt aber nur dann auf fruchtbaren Boden, wenn der entsprechende Teil der Rettungskette innerhalb der Einrichtung etabliert worden ist.

Jedes CERT-Team freut sich über gute digitale Ersthelfende. Denken Sie daran, genügend Personen analog zur Ersten Hilfe weiterzubilden, eine Gefahr zu erkennen und zu melden – denn zumindest einen Notruf absetzen zu können, ist bei jeder Person vorauszusetzen. Achten Sie außerdem darauf, dass sich das Team der „digitalen Rettungskette“ parallel zu Ihrer IT weiterentwickelt und geben Sie diesem die Freiheit und die Möglichkeiten zu handeln. ◆

Den BSI-Leitfaden finden Sie unter **https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210712_Leitfaden_Digitaler_Ersthelfer.html**

easyroam: The Next Generation

Seit 2021 befindet sich die Erweiterung des bewährten Dienstes eduroam in der Entwicklung. easyroam verwaltet zurzeit etwa 130 000 Nutzende und deren Endgeräte in eduroam. Bis Ende 2023 wird der große Sprung zur neuen easyroam-Infrastruktur gemacht, die zahlreiche Verbesserungen und Tools mit sich bringt, die es einfacher denn je machen, Nutzende und deren Endgeräte in eduroam zu bringen und zu verwalten.

Text: **Long Yang Paffrath, Ralf Paffrath** (DFN-Verein)

Was ist easyroam?

easyroam ist ein optionales Leistungsmerkmal des Dienstes eduroam, das den Aufwand hinter eduroam reduzieren und für mehr Sicherheit und Kontrolle sorgen kann. Dies erfolgt über einen sogenannten Managed eduroam IdP, der indirekt von der DFN-AAI (Authentifizierungs- und Autorisierungsinfrastruktur) verwaltet wird und ausschließlich die Authentifizierung über EAP-TLS (zertifikatsbasierte Anmeldung) in eduroam unterstützt. Kennungen und Passwörter

> Entwicklung und Evolution sind eng mit den Anforderungen der Einrichtungen verbunden.

werden mithilfe von easyroam in eduroam nicht mehr benötigt. Stattdessen erhält jedes Gerät ein eigenes Profil mit einem Zertifikat. Dadurch wird es sowohl in easyroam als auch in eduroam eindeutig identifizierbar. Die teilnehmenden Personen werden pseudonymisiert verwaltet. Während der Pilotphase und auch nach der offiziellen Einführung in den Regelbetrieb wurde ein agiler Arbeitsstil mit den Einrichtungen gepflegt, die easyroam nutzen. Dadurch konnten viele Vorschläge gesammelt werden, die in die neue Infrastruktur eingeflossen sind.

Monolithischer Aufbau von easyroam

Die Entwicklung und Evolution von easyroam ist eng mit den Anforderungen der verschiedenen Einrichtungen verbunden. Die gegenwärtige Version von easyroam verwendet eine monolithische Architektur. Das bedeutet, dass alle Komponenten und Funktionen des Systems in einem einzigen, massiven Codeblock integriert sind. Für die Kernentwicklung von easyroam war diese Form der Architektur eine praktische Lösung, die es ermöglicht hat, zeitnah und schnell die zertifikatsbasierte Anmeldung (EAP-TLS) für kleine und große Forschungs- und Bildungseinrichtungen im Regelbetrieb anzubieten.

In der aktuellen Architektur sind Funktionen wie der Authentifizierungsdienst eng mit anderen Funktionen wie der Profilverwaltung, der Nutzerverwaltung und der Protokollierung verknüpft. Dadurch entstehen eine gewisse Komplexität und ein Mangel an Flexibilität. Durch die steigenden Anforderungen der Forschungs- und Bildungseinrichtungen stößt die monolithische Architektur an ihre Grenzen.

Besonders deutlich wurden diese Grenzen in den Bereichen Sicherheit und Anpassungsfähigkeit. In einer Zeit, in der Sicherheitsbedenken höchste Priorität haben, führt eine enge Verknüpfung von Authentifizierung und anderen Funktionen zu unnötiger Komplexität im System und verlangsamt geplante Änderungen und Erweiterungen erheb-

lich. Die Entkopplung der Authentifizierung von anderen Diensten ist entscheidend, um ein Höchstmaß an Sicherheit zu gewährleisten und eine schnelle Erweiterung des Authentifizierungssystems zu ermöglichen.

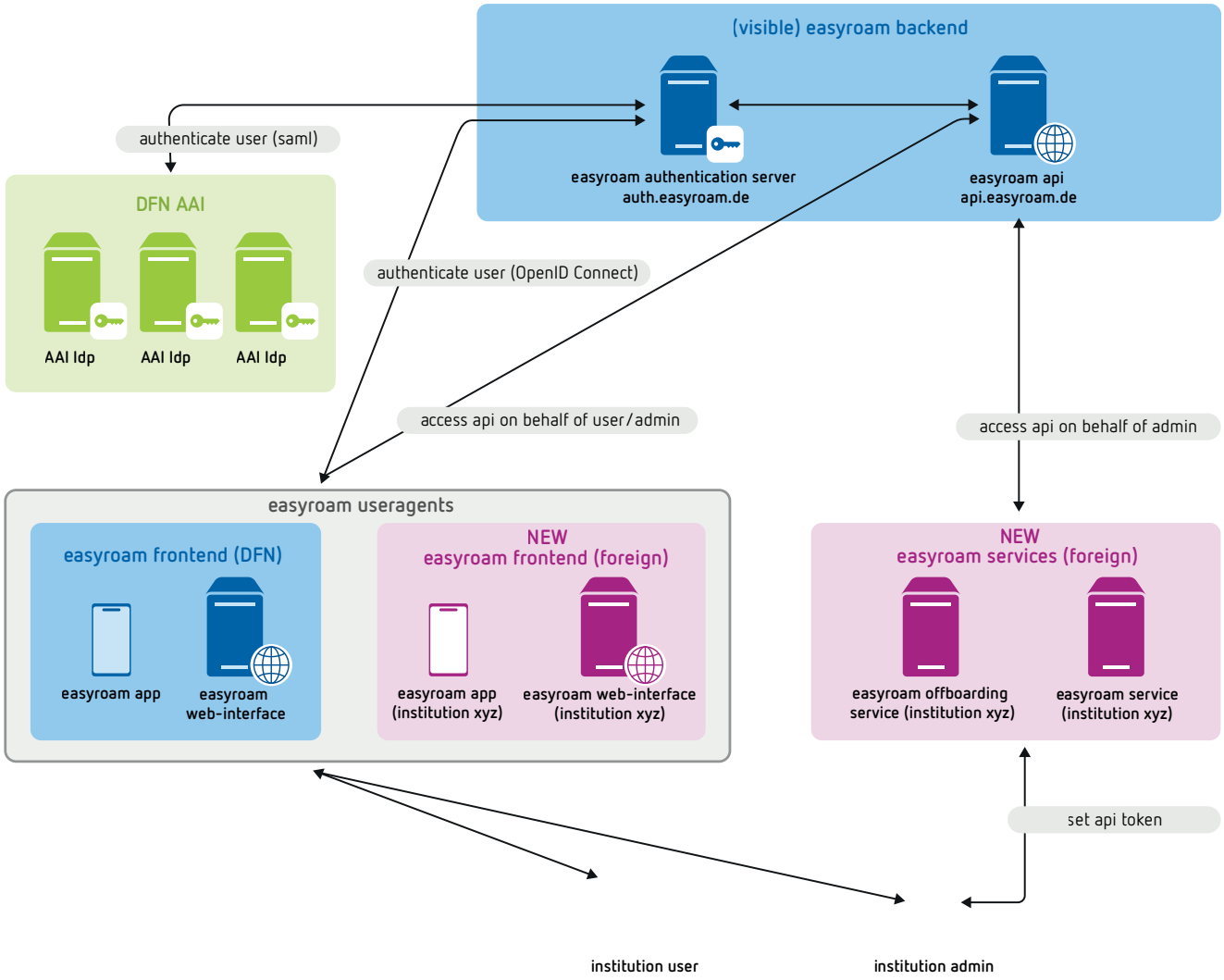
Darüber hinaus ist die monolithische Architektur angesichts der wachsenden Vielfalt an unterstützten Geräten und Betriebssystemen, insbesondere im Bereich Linux, weniger anpassungsfähig an die verschiedenen Anforderungen der unterschiedlichen Systeme. Zudem gestaltet sich auch die effektive Umsetzung neuer Funktionalitäten herausfordernd, wie es zum Beispiel beim easyroam-Offboarding der Fall war.

Angesichts dieser Komplexität und des Bedarfs, easyroam für die Zukunft nachhaltig und flexibel zu gestalten, wurde die Architektur umfassend überarbeitet. Die Veröffentlichung der neuen easyroam-Infrastruktur markiert den Beginn einer vielversprechenden Entwicklung, in der die monolithische Struktur durch eine modernere und flexiblere Architektur ersetzt wird, die besser auf die Bedürfnisse von Bildungs- und Forschungseinrichtungen zugeschnitten ist.

Der Authentifizierungsserver

Eine wichtige Neuerung in der easyroam-Infrastruktur ist die Einführung eines hochmodernen Authentifizierungsservers, der das OpenID-Protokoll in der „easyroam-Welt“ beherrscht und gleichzeitig eine nahtlose Integration in die DFN-AAI-Infrastruktur ermöglicht. Diese Architekturänderung eröffnet neue Möglichkeiten für Einrichtungen, Administrierende und Entwicklerinnen und Entwickler, die durch den neuen Authentifizierungsserver Anwendungen schreiben können, welche direkt auf interne easyroam-Komponenten zugreifen können. Der Authentifizierungsserver unterstützt zwei verschiedene Arten von Anwendungen: die easyroam-Useragents und die easyroam-Services.

ÜBERBLICK ÜBER DIE NEUE EASYROAM-INFRASTRUKTUR



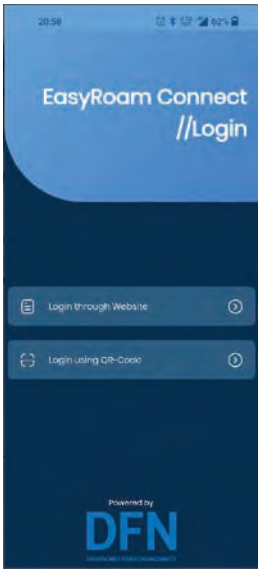
easyroam „Useragents“ sind Anwendungen, die mit Nutzenden interagieren, die easyroam-Komponenten verwenden. Falls eine solche Anwendung genutzt werden soll, müssen Nutzende im Authentifizierungsprozess über das Web-Interface mit dem Authentifizierungsserver interagieren, um sich anzumelden. Auf diese Weise kann die neue API genutzt werden, um eine eigene, kundenorientierte easyroam Web-Plattform zu entwickeln. Diese können Teilnehmer mit einem Versorgeranschluss beispielsweise den Einrichtungen zur Verfügung stellen, die sie versorgen.

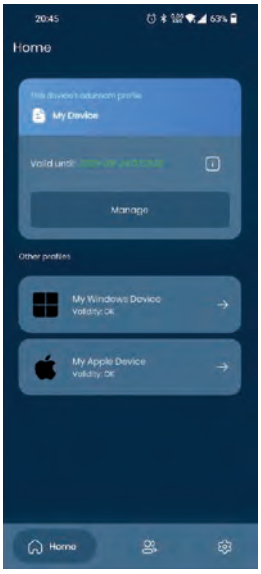
Die easyroam-Services umfassen Anwendungen, die innerhalb einer Einrichtung direkt mit easyroam-Komponenten interagieren. Diese Anwendungen können sich am Authentifizierungsserver ohne direkte Anwesenheit einer Person authentifizieren und verfügen generell über Administrationsrechte. Dies ist insbesondere für Serveranwendungen geeignet, die im Hintergrund auf Ereignisse oder Daten warten und diese an die easyroam-Infrastruktur weiterleiten. Ein klassisches Beispiel ist das einrichtungsbezogene easyroam-Offboarding.

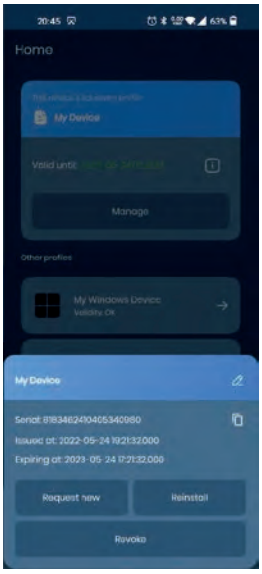
Um Anwendungen beim Authentifizierungsserver zu registrieren, wird eine Kontoverwaltungskonsole bereitgestellt, die es Nutzenden ermöglicht, alle aktiven Sitzungen zu verwalten und Login-Einstellungen zu ändern. Admins können neue Anwendungen am Authentifizierungsserver registrieren und die Berechtigungen der Anwendungen festlegen. Im easyroam-Anwendungstyp „Useragents“, der von Einrichtungen selbst entwickelt werden kann, haben sie die Möglichkeit, eigene Logos und Hintergrundbilder festzulegen, die den easyroam-Nutzenden während des Anmeldevorgangs angezeigt werden können.

Die easyroam-API

Die neue easyroam-API ist ein leistungsstarkes Instrument, welches es Einrichtungen ermöglicht, easyroam in ihre eigenen Anwendungen, Dienste, Tools und Workflows zu integrieren. Alle Funktionalitäten, die bereits im Regelbetrieb vorhanden sind, werden ebenfalls von der neuen easyroam-API unterstützt. Zusätzlich verbessert die API einige Funktionalitäten wie das Offboarding erheblich. Um eine nahtlose Integration von easyroam in bestehende oder neue Anwendungen zu gewährleisten, steht eine umfassende API-Dokumentation zur Verfügung. Diese umfasst detaillierte Informationen zu den verfügbaren Endpunkten sowie zu den Authentifizierungsmethoden des easyroam-Authentifizierungsservers. Zur Verbesserung der Verständlichkeit der API-Dokumentation wurden Beispiele hinzugefügt, die zeigen, wie die API genutzt werden kann.







Die App EasyRoam kann bei Google Play oder im App Store kostenfrei heruntergeladen werden

Mehr Transparenz in easyroam

Die easyroam-Architektur erweitert die neue API und den neuen Authentifizierungsserver um eine wichtige Sicherheitsfunktion in Form eines Audit-Logs. Administrierende und Sicherheitsbeauftragte können mit diesem Tool umfassende Protokolle von Aktivitäten in easyroam einsehen. Der Audit-Log zeichnet wichtige Aktionen und Ereignisse im System auf, einschließlich Anmeldungen von Admins, Konfigurationsänderungen sowie Änderungen an Benutzerkonten und Benutzerprofilen.

Der Audit-Log liefert eine wertvolle Ressource zur Identifizierung von Sicherheitsvorfällen. So können verdächtige Konten und Anwendungen schneller identifiziert und aus dem System entfernt werden. Darüber hinaus trägt er zur Erhöhung der Integrität und Transparenz bei easyroam sowie zur Bereitstellung eines zusätzlichen Maßes an Kontrolle und Sicherheit bei.

> Der Audit-Log liefert eine wertvolle Ressource zur Identifizierung von Sicherheitsvorfällen.

Fazit

Nutzende und Administrierende, die easyroam wie bisher verwenden möchten, können dies weiterhin uneingeschränkt tun. Die neue Infrastruktur schafft jedoch die Möglichkeit für innovative Anwendungen in den Einrichtungen rund um das Thema easyroam. ◆

Kampf gegen Phishing – neue Abwehrkomponente in DFN.Security

Seit diesem Jahr ist der Dienst DFN.Security produktiv im Einsatz. Neue Leistungsmerkmale wie die Logdateneinlieferung werden von immer mehr DFN-Teilnehmern genutzt. Die nächste Erweiterung zur Erhöhung der Informationssicherheit steht bereits in den Startlöchern. Als aktive Abwehrkomponente insbesondere im Kampf gegen Phishing-Angriffe wird das Verfahren DNS-RPZ implementiert. Dabei baut der DFN-Verein auf die zukünftige Kooperation mit der Stiftung SWITCH, dem nationalen Forschungsnetz der Schweiz.

Text: **Christine Kahl** (DFN-CERT)

Foto: brytta/iStock

Cyberangriffe auf Hochschulen und Wissenschaftseinrichtungen im Deutschen Forschungsnetz mit teils schwerwiegenden und langwierigen Schäden haben in den vergangenen zwei Jahren deutlich zugenommen. Mit dem seit Juni 2023 produktiven Dienst DFN.Security reagiert der DFN-Verein auf die stetig wachsenden Herausforderungen im Bereich der Informationssicherheit. Mit dem eigens für heterogene IT-Landschaften im Wissenschaftsbereich optimierten Dienst steht DFN-Teilnehmern ein breites Portfolio an Sicherheitsleistungen zum Schutz der eigenen IT-Infrastrukturen zur Verfügung.

In einer intensiven Umbauphase wurden die Leistungsmerkmale des DFN-CERT-Dienstes und des DoS-Basisschutzes sowie die neu entwickelten Leistungsmerkmale der Security Operations unter dem Dach des Dienstes DFN.Security konsolidiert

> Durch DNS-RPZ werden Zugriffe auf Seiten mit maliziösen Inhalten blockiert.

und ausgebaut. Mit der Option, Logdaten auf sicherheitsrelevante Vorfälle zu analysieren sowie der Möglichkeit, Überwachungsziele im Selfservice zu hinterlegen, erhalten DFN-Teilnehmer einen breiten Überblick zu ihrer eigenen Sicherheitslage.

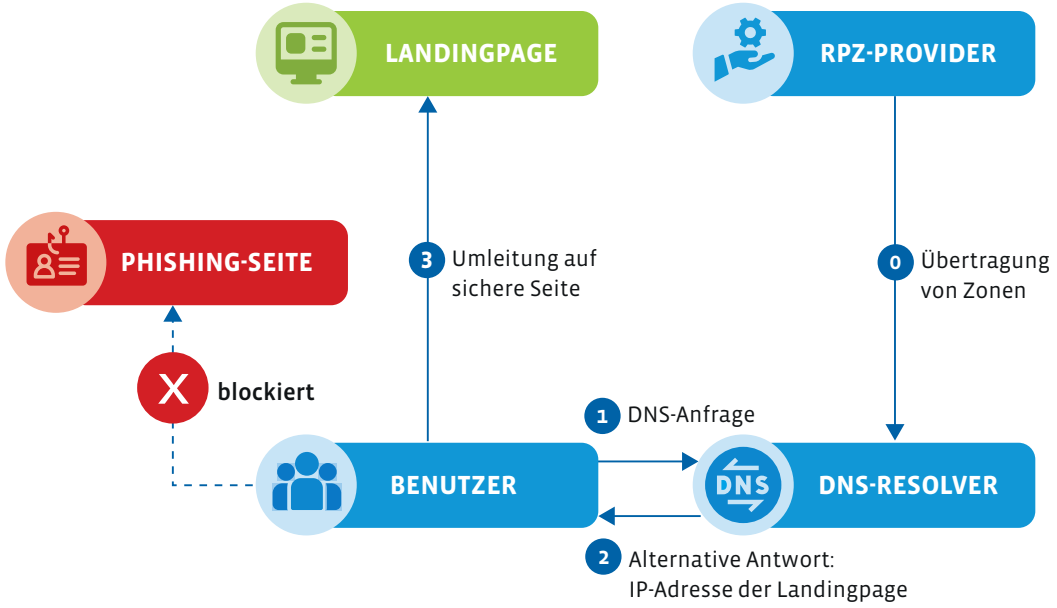
Der Dienst DFN.Security ist, wie sein Vorgängerdienst DFN-CERT, primär ein Informationsdienst: Das beinhaltet die Zustellung von Informationen zu Schwachstellen, potenziellen Sicherheitsvorfällen und offen im Netz erreichbaren Diensten. Die Bewertung der Meldungen als Sicherheitsrisiko und das Ergreifen von (Gegen-)Maßnahmen obliegt allerdings dem Teilnehmer. Mit dem in Vorbereitung befindlichen neuen Leistungsmerkmal DNS-RPZ (Domain Name System Response Policy Zone) bietet DFN.Security nun eine aktive Abwehrkomponente an, die nach Einbindung in die eigene Infrastruktur automatisch auf wechselnde Bedrohungen reagiert. Durch DNS-RPZ werden Zugriffe auf Seiten mit maliziösen Inhalten blockiert, um Nutzende z. B. vor der unbeabsichtigten Eingabe von Zugangsdaten auf Phishing-Webseiten zu schützen. Eine Bewertung durch den Teilnehmer ist nur dann erforderlich, wenn eine Blockierung zu Unrecht erfolgt (also kein Sicherheitsrisiko vorliegt) und damit aufgehoben werden kann.

Aktive Gefahrenabwehr mit DNS-RPZ

DNS-RPZ ist ein Verfahren (siehe Abbildung), um bei der Namensauflösung durch rekursive DNS-Resolver mittels eigener Richtlinien einzugreifen und dadurch letztlich den Zugriff auf bestimmte Domains zu unterbinden.

Stellen Nutzende eine DNS-Anfrage für eine Seite mit maliziösen Inhalten, (1) so erkennt der DNS-Resolver dies durch die Auswertung der eingebundenen Zonen (0). Als Antwort auf die DNS-Anfrage liefert der DNS-Resolver daher nicht die IP-Adresse des eigentlich angefragten bösartigen Ziels, sondern die IP-Adresse einer sogenannten Landingpage (2). Statt auf eine

DNS-RPZ-SCHEMA



Seite mit maliziösen Inhalten greifen Nutzende – sofern sie bei ihrer Anfrage auf den Einsatz von TLS (Transport Layer Security) verzichten oder die üblicherweise angezeigte Zertifikatswarnung akzeptieren – auf eine sichere Landingpage (3) zu, die sie darüber informiert, dass das gewünschte Ziel als bösartig eingestuft und daher umgeleitet wurde.

Neben der Teilnahme am Dienst DFN.Security erfordert die Nutzung dieses Angebotes den Betrieb einer DNS-Server-Software, die RPZ unterstützt. Als Software stehen derzeit BIND, PowerDNS Recursor oder Knot Resolver zur Verfügung. Alternativ ist der Einsatz einer DNS-Appliance notwendig, die das Aktivieren von RPZ erlaubt, wie Infoblox, BlueCat, EfficientIP oder Nokia VitalQIB (Quelle SWITCH).

> Durch den automatischen Abruf werden Nutzende vor dem Ansurfen bösartiger Webseiten geschützt.

Konkret wird über den Dienst DFN.Security ein Feed (genauer: mehrere Response-Policy-Zonen) bereitgestellt, in dem Informationen zu maliziösen Domains gesammelt zur Verfügung stehen. Wird eine Zone aktualisiert, wird der RPZ-fähige Resolver des Teilnehmers informiert. Durch den automatischen Abruf der Zone und die Einbindung in das eigene DNS wird direkt auf neu ermittelte Bedrohungen reagiert – so werden Nutzende vor dem Ansurfen einer bösartigen Webseite geschützt. Die sichere Landingpage kann von der teilnehmenden Einrichtung selbst bereitgestellt werden. Alternativ kann das mit den Einrichtungsinformationen angereicherte Template des Dienstes DFN.Security eingesetzt werden. In jedem Fall sollte die Landingpage über den Vorgang, den Grund für die Blockierung sowie die zur Verfügung stehende Handlungsmöglichkeit informieren.

Es ist trotz aller Sorgfalt beim Erstellen der Zonen möglich, dass eine Domain fälschlicherweise blockiert wird. In diesem Fall können Nutzende das Entfernen der Domain aus der Liste der maliziösen Domains beantragen. Als schnelle Antwort auf eine Anforderung zum Entblocken kann eine Einrichtung die betreffende Domain in eine eigene Whitelist (Ausnahmeliste) auf dem DNS-Server eintragen und dadurch den Zugriff für die eigenen Nutzenden kurzfristig wieder freigeben. Zusätzlich sollte die Information über das ungerechtfertigte Blocken – ein sogenannter „false positive“-Eintrag – an den Feed-Provider weitergeleitet werden, damit dieser die Domain aus der Response-Policy-Zone entfernt und somit den Zugriff auf die fälschlicherweise geblockte Domain für alle Teilnehmer an dem Dienstmerkmal wieder freigibt.

Teilnehmer, die DNS-RPZ einsetzen wollen, haben durch die im Dienst DFN.Security enthaltene Logdatenanalyse die Möglichkeit, sich einen Überblick über die Vorgänge in der eigenen Einrichtung zu verschaffen: Mit dem Übermitteln der betreffenden DNS-Server-Logs werden die geblockten Zugriffsversuche in Form automatischer Warnmeldungen für Administrierende zusammengefasst.

Forschungskooperation mit SWITCH geplant

Die Schweizer Stiftung SWITCH betreibt seit Jahren unter dem Namen DNS Firewall u. a. für die Schweizer Hochschulen einen DNS-RPZ-Dienst. Die Ähnlichkeit des Einsatzgebietes wie auch die bisher vom DFN-CERT durchgeführten Tests sprechen dafür, dass die von SWITCH erstellte Response-Policy-Zone auch für Teilnehmer am Deutschen Forschungsnetz eine hohe Relevanz hat. Um den DFN-Teilnehmern das neue Dienstmerkmal DNS-RPZ zügig bereitzustellen und einen optimalen Austausch vertraulicher Informationen zwischen dem DFN-Verein und SWITCH zu gewährleisten, ist eine Übereinkunft für eine künftige Forschungskooperation getroffen worden.

Im Rahmen der Zusammenarbeit stellt SWITCH dem DFN-Verein in einem ersten Schritt seine Technik und Expertise zu DNS-RPZ zur Verfügung: Das umfasst die Beratung beim Systemdesign sowie die Freigabe der Nutzung der SWITCH-Zone für alle Teilnehmer am Dienst DFN.Security. Der zweite Schritt richtet sich auf den Austausch von Daten zur Verbesserung der Zone und die voraussichtliche Erstellung weiterer Zonen, die sowohl für Nutzende des SWITCH-Dienstes als auch für DFN-Teilnehmer verfügbar sind. Ziel ist es, allen Einrichtungen im Deutschen Forschungsnetz umfassende Angebote zur Informationssicherheit bereitzustellen, die in der Praxis von möglichst vielen Teilnehmern genutzt werden. Denn Cybersecurity bedarf der Anstrengung aller in der Hochschul- und Forschungsgemeinschaft. ◆

Kontaktieren Sie uns! Bei Interesse an der Nutzung von DNS-RPZ oder bei Fragen zum Dienst DFN.Security erreichen Sie uns unter:
dfn.security@dfn.de

Flexibel lehren und lernen – mit bwLehrpool

Die Föderierten Dienste in der DFN-Cloud haben einen Neuzugang: Seit September 2023 ist bwLehrpool bundesweit über den DFN-Verein verfügbar. Die Plattform bietet virtuelle Lehrumgebungen für PC-Poolräume an. Mit bwLehrpool haben Dozierende die Möglichkeit, schnell, einfach und unabhängig von Dritten personalisierte Lehr- und Lernszenarien für Studierende bereitzustellen.

Text: **Steffen Ritter** (Hochschule Offenburg), **Dirk von Suchodoletz** (Universität Freiburg)

Kaum eine Lehrveranstaltung kommt heutzutage ohne irgendeine Form von Computersoftware aus – ob im Fachbereich der Informatik, in dem mit Programmierumgebungen, Datenbanken oder aktuell mit Tools zum Training von Künstlicher Intelligenz gearbeitet wird, oder in den Ingenieurwissenschaften, die zur Planung und Modellierung von Bauteilen sogenannte CAD-Software einsetzen. Geografinnen und Geografen wiederum benötigen Software zur Vermessung, in den Literaturwissenschaften sind es eher Programme zur Text- oder Sentimentanalyse. Diese Liste lässt sich beliebig weiterführen. Dabei fällt auf, dass jeder Fachbereich teils völlig unterschiedliche Anforderungen an die Lehrumgebung und die jeweilige Softwareausstattung stellt. Für Hochschulen ist es damit kaum möglich, einen PC-Poolraum bereitzustellen und zu verwalten, der alle an ihn gestellten Anforderungen erfüllt.

> Am Ende entscheiden überlastete Administrierende.

Bisher kommen an vielen Einrichtungen vermehrt unflexible Softwareumgebungen zum Einsatz, die im Verteilverfahren persistent auf definierte Desktop-Rechner installiert werden. Hierbei bestehen zudem deutliche Einschränkungen auf eine fest vorgegebene Basisumgebung. Zwar können Lehrende bis zu einem bestimmten Grad Vorstellungen einbringen, aber am Ende entscheiden überlastete Administrierende, wie Umgebungen aussehen. Diese Vorgehensweise ist nicht nur unflexibel, sondern geht vielfach mit langen Änderungszyklen einher, da Änderungen und Updates häufig nur einmal pro Semester vorgenommen werden. Falsche Versionen, unvollständige Softwarepakete, aufgeblasene Installationen oder ungünstige Konfigurationen und Voreinstellungen führen letztendlich dazu, dass Lehrende oder Prüfende unzufrieden sind.

Foto: baona/iStock

Hier kommt bwLehrpool ins Spiel: Das Kooperationsprojekt der Universität Freiburg und der Hochschule Offenburg ermöglicht die flexible und effiziente Bereitstellung von virtuellen Lehr- und Laborumgebungen in PC-Poolräumen von Hochschulen. Mittels Desktop-Virtualisierung können auf der Plattform beliebige Softwareumgebungen

„Ich schätze bwLehrpool als flexible und vielseitig einsetzbare Plattform für angewandte und praxisnahe Lehrangebote. Die Basisimages für verschiedene Betriebssysteme (Windows/Linux), die wir selbst modifizieren und um weitere Software ergänzen können, erlauben es, für jeden Kurs eine maßgeschneiderte Umgebung bereitzustellen. Diese lässt sich, was ich sehr gut und sinnvoll finde, in einem besonderen Modus auch zur Durchführung entsprechender Abschlussklausuren nutzen."

Dr. Ernst August Frhr. v. Hammerstein | Akademischer Oberrat
Studienfachberatung Stochastik, insb. zur Profillinie „Finanzmathematik"
Albert-Ludwigs-Universität Freiburg

„Mit bwLehrpool können wir eine große Zahl an IT-Lehrveranstaltungen raumtechnisch sehr flexibel planen und unseren Lehrbeauftragten gleichzeitig auch die entsprechenden Lernumgebungen zur Verfügung stellen. Diese lassen sich zudem sehr einfach verwalten und aktualisieren. Das ist ein großer Supportgewinn für alle Beteiligten."

Katja Fimmen | Fachbereichsleitung IT am Zentrum für Schlüsselqualifikationen
Albert-Ludwigs-Universität Freiburg

für jede Art von Lehr- und Lernszenarien bereitgestellt werden. Dozentinnen und Dozenten haben mit dem Dienst die Möglichkeit, selbstständig Lehrumgebungen zu erstellen und zu verwalten sowie ohne Aufwand jederzeit anzupassen und zu verändern. Auch das kollaborative Erstellen und hochschulübergreifende Teilen von Virtuellen Maschinen (VM) wird erleichtert.

Neben der Nutzung vor Ort können die Softwareumgebungen zusätzlich über Campusgrenzen hinweg im Fernzugriff angeboten werden. Dadurch konnten während des Pandemie-Lockdowns viele praxisorientierte Lehrveranstaltungen auch von zu Hause durchgeführt werden. Inzwischen nutzen Studierende dieses Angebot verstärkt für freies Lernen, ohne an die Hochschule kommen zu müssen. Zusätzlich dient bwLehrpool als flexible Basisplattform für E-Prüfungen – häufig auch im Zusammenhang mit Learning-Management-Systemen (LMS) wie beispielsweise ILIAS oder Moodle.

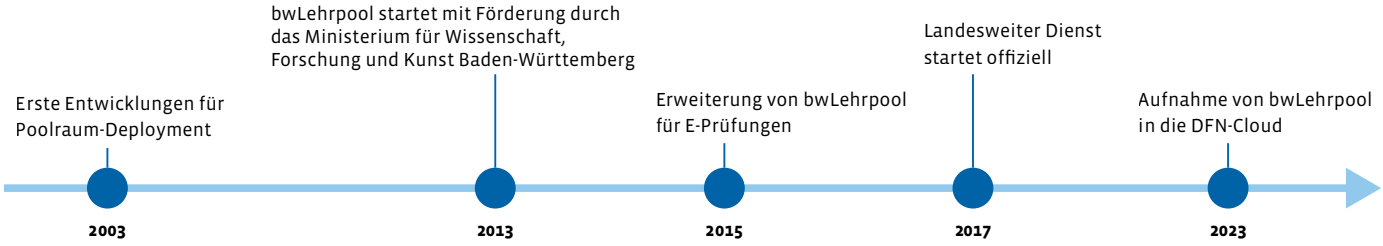
> Zusätzlich dient bwLehrpool als flexible Basisplattform für E-Prüfungen.

Im Ergebnis erlaubt der Dienst eine bessere Auslastung bestehender Ressourcen: IT-Administrierende aus den Rechenzentren oder Verantwortliche für die PC-Pools werden entlastet und können sich auf den Betrieb der Umgebung konzentrieren, ohne sich mit deren Lehrinhalten beschäftigen zu müssen. Damit adressiert bwLehrpool die gestiegenen Aufwände in der bisher oft dezentralen IT-Administration – mit ihren verteilten Zuständigkeiten zwischen dem Rechenzentrum, Fakultäten und Poolverantwortlichen – und gibt Antworten auf den zunehmenden Fachkräftemangel im IT-Bereich sowie gestiegene Sicherheitsanforderungen.

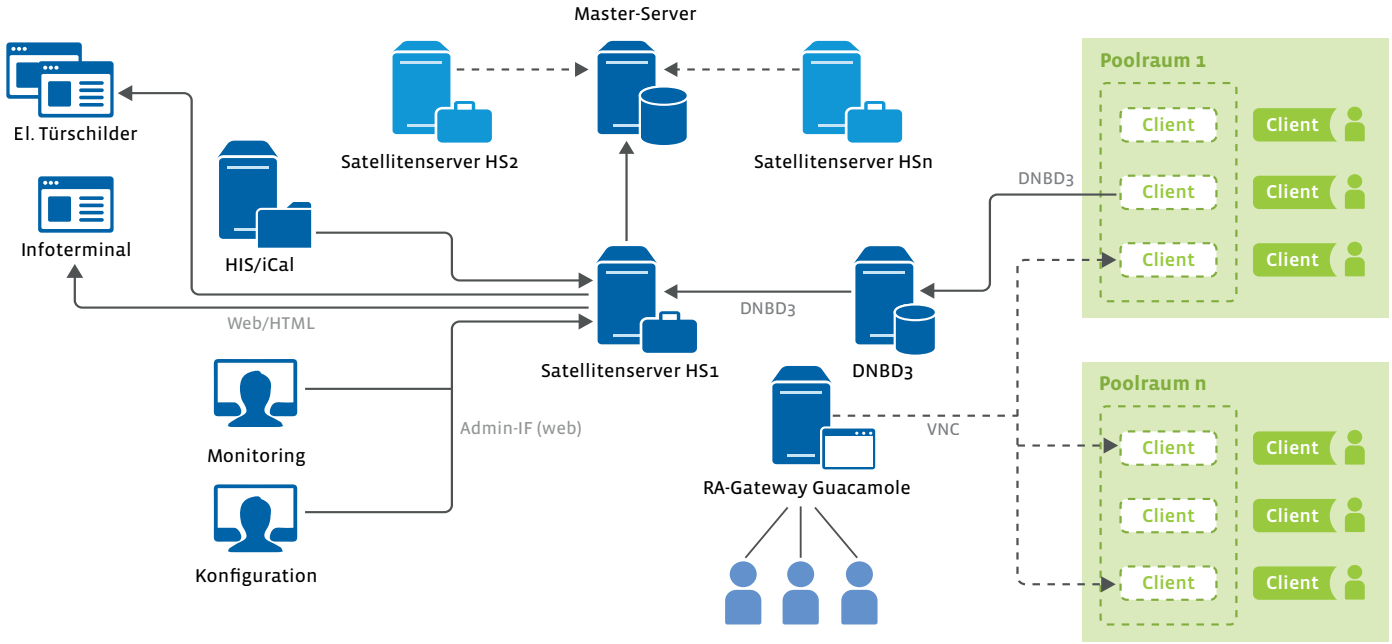
Das technische Konzept von bwLehrpool

bwLehrpool besteht im Wesentlichen aus drei Komponenten: Der erste Baustein ist der sogenannte Satellitenserver, den jede Hochschule für den eigenen Standort betreibt. Dieser ermöglicht die Konfiguration und Verwaltung des Systems über eine einfache Weboberfläche. Poolrechner werden automatisch erfasst und deren Hardwareausstattung übersichtlich dargestellt. Dadurch erhalten Administrierende einen Überblick über die genutzte Hardware sowie über die aktuelle Auslastung und Nutzung der Pool-PCs. Einstellungen wie automatisches Herunterfahren nach Inaktivität oder zu bestimmten Uhrzeiten zur

VOM LANDESDIENST ZUM BUNDESWEITEN DFN-ANGEBOT



DAS TECHNISCHE KONZEPT



Reduzierung des Stromverbrauchs lassen sich global, pro Raum oder individuell pro Rechner vornehmen.

Der zweite zentrale Baustein ist ein angepasstes Linux-Basisbetriebssystem (MaxiLinux), welches per iPXE-Netzwerkboot vom Satellitenserver an die Poolrechner ausgeliefert wird. Dies gewährleistet eine breite Hardwareunterstützung typischer Desktop-PCs und kann parallel zu bestehenden Lokalinstallationen eingesetzt werden. Auf Basis des MaxiLinux können anschließend Container (z. B. Docker) oder VMs (mittels diverser Hypervisoren wie VMware, VirtualBox, QEMU/KVM) ausgeführt werden, die die verschiedenen Lehr-, Prüfungs- und Forschungsumgebungen (Windows- oder Linux-basiert) darstellen. Die Virtualisierung erfolgt dabei im Gegensatz zu klassischen Virtual-Desktop-Infrastructure-Lösungen, lokal auf den Poolrechnern.

Die bwLehrpool-Suite bildet die dritte Komponente in Form einer Java-Desktop-Applikation, mit deren Hilfe Lehrende eigene VMs und Container hoch- oder herunterladen, zugeordnete Veranstaltungen verwalten und diese gegebenenfalls als E-Prüfung definieren können.

Zusätzliche Module ermöglichen beispielsweise

- lokales Caching,
- den Einsatz von Proxy-Servern für einen schnelleren Startvorgang bei Netzwerkengpässen,
- die Steuerung der Bildausgabe von Poolrechnern durch Dozierende mithilfe des Pool-Video-Switch (PVS),
- die Einrichtung von Kiosk-Rechnern als Rechercheterminal in der Bibliothek,
- das Konfigurieren von Clients als Anzeige für Digital Signage oder
- elektronische Türschilder.

Als weitere Nutzungsmöglichkeit lässt sich das System minutenschnell in einen abgesicherten Modus für E-Prüfungen umstellen. Lehrende können dabei selbst Firewall-Regeln definieren oder externe Speichermedien blockieren. Nach einem Neustart der Rechner steht der Raum im Anschluss an die Prüfung sofort für weitere Lehr- oder Prüfungsveranstaltungen zur Verfügung.

Für die Erstellung und Pflege von Softwareumgebungen in VMs – dazu gehören beispielsweise die Konfiguration von Multi-Monitor-Setups, das Anfahren der

„Gerade in den Bereichen Netzwerke und IT-Sicherheit sind praktische Experimente und Versuche hilfreich, um das Erlernte zu vertiefen. Da die Images in einem isolierten Netzwerk verbunden sind und nach Ende des Kurses deaktiviert werden, stellt die Umgebung kein zusätzliches IT-Sicherheitsrisiko für das Hochschulnetzwerk dar. Ein weiterer Vorteil ist, dass unsere Studierenden mit dem erstellten VM-Image mühelos in der eingerichteten Linux-Umgebung loslegen können – ohne sich um Falschkonfigurationen sorgen zu müssen. Im Zweifel wird neu gestartet und mit einer sauberen Installation begonnen."

Prof. Dr. Richard Zahoransky | Professor für Netztechnologien und IT-Sicherheit Hochschule Furtwangen

„Seit 2019 nutzen wir bwLehrpool für unsere Prüfungen zur Einführung in die Programmierung mit etwa 500 bis 600 Teilnehmenden in den Poolräumen des Rechenzentrums. Der Dienst ermöglicht uns die Vorbereitung einer definierten Prüfungsumgebung, die flexibel konfigurierbar ist und den Teilnehmenden zum Testen über das Netz zur Verfügung gestellt werden kann. Auf den Prüfungsrechnern ist die Umgebung jedoch komplett abgeschottet. Zu Beginn der Prüfung müssen Studierende nur den Rechner starten, der dann automatisch unsere Umgebung im Prüfungsmodus bereitstellt."
Prof. Dr. Peter Thiemann | Professor für Programmiersprachen und Softwaretechnik
Albert-Ludwigs-Universität Freiburg

„In der Geografie setzen wir eine Vielzahl IT-basierter Systeme zur Analyse, Modellierung und Visualisierung von Geodaten ein. bwLehrpool gibt uns die Möglichkeit, die unterschiedlichsten Systeme passgenau zu konfigurieren und sie im Handumdrehen in der Lehre zu nutzen."
Rafael Hologa | Wissenschaftlicher Mitarbeiter
Albert-Ludwigs-Universität Freiburg

gewählten VM oder die Einbindung von Beamern und Kalendern – wurden eigens Werkzeuge entwickelt, die für Lehrende einfach zu handhaben sind.

Neben dem MaxiLinux, welches je nach Konfiguration bereits einen umfangreichen grafischen Desktop anbietet, kann das System durch den Einsatz verschiedener Hypervisoren sowie durch Containerisierung sehr flexibel und weitgehend durch Lehrende angepasst werden. Dies setzt eine strikte Trennung von Zuständigkeiten mit starker Delegationskomponente um. Lehrende sind nicht mehr auf die Erreichbarkeit von Pool-Administrierenden angewiesen und können ihre Vorbereitungen zeitlich und örtlich unabhängig in der gewünschten Softwareumgebung treffen. Für Administrierende bietet bwLehrpool ein umfangreiches, webbasiertes Konfigurationsinterface und Monitoring der Poolrechner.

Vom Landesdienst zum bundesweiten DFN-Angebot

bwLehrpool ist ein System mit über zehn Jahren Entwicklungshistorie und hat sich in der Praxis als sehr robust gegenüber Ausfällen gezeigt. Seit sechs Jahren steht das vom Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg geförderte Projekt als Landesdienst – und seit September 2023 bundesweit in der DFN-Cloud – zur Verfügung.

Mittlerweile setzen 22 Hochschulen in Baden-Württemberg, Nordrhein-Westfalen und der Schweiz bwLehrpool im produktiven Lehrbetrieb ein. Der kooperative Ansatz – die Verteilung der Zuständigkeiten auf Lehrende und Administrationspersonal sowie die gemeinsame Nutzung von Lehrumgebungen – hilft Hochschulen, sich auf die Grundversorgung und breit nachgefragte IT-Dienste zu konzentrieren. So können

> Die gemeinsame Nutzung hilft Hochschulen.

neue Möglichkeiten in der IT-gestützten Lehre sowie für die Durchführung elektronischer Prüfungen geschaffen werden. Darüber hinaus werden zentrale Strategien wie Open Source und die Hoheit über eigene Daten (ohne Austausch mit externen Cloud-Dienstleistern) verfolgt.

bwLehrpool versteht sich dabei nicht als Ersatz etablierter Installationen, sondern punktet durch ein modulares Konzept mit einfacher Einbindung in bestehende Services sowie eine übergreifende Steuerung und Überwachung großer Rechnerinstallationen. Die Plattform ist ein weiterer Baustein zeitgemäßer IT-Strategien von Hochschulen, die auf Bildungsgerechtigkeit und digitale Souveränität Wert legen und sich damit auch unabhängiger von kommerziellen IT-Anbietern machen wollen.

Eine Einführung des Dienstes inklusive Basisschulung des lokalen Administrationspersonals benötigt selten mehr als einen Tag. Erfahrungsgemäß braucht es eine gewisse Zeit, das System an Hochschulen bekannt zu machen und Lehrenden die vielen Vorteile zu vermitteln. Nach der Einführungsphase überzeugt der Dienst in der Regel sehr schnell durch unkomplizierte Handhabung und Flexibilität. Bei jährlich stattfindenden Veranstaltungen an wechselnden Standorten haben Nutzende seit 2016 die Möglichkeit, sich mit dem Entwicklungsteam direkt auszutauschen und so Anregungen für die praxisorientierte Weiterentwicklung zu geben. In den kommenden Jahren wird der Fokus unter anderem auf Entwicklungen im Bereich der Verbesserung des Fernzugriffs sowie einer Integration in OpenStack-Clouds liegen, um vollständig virtuelle Poolräume zu ermöglichen und lokale Ressourcen on demand zu erweitern. ◆

Cyberangriff ade mit dem CRA-E?

Die EU-Kommission schlägt zur Verbesserung der IT-Sicherheit den Cyber Resilience Act vor

Im Zuge ihrer Digitalstrategie veröffentlichte die Europäische Kommission im Herbst 2022 einen Entwurf für eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen oder kurz Cyberresilienzverordnung (Cyber Resilience Act [CRA]).[1] Im Juni 2023 haben das Europäische Parlament und der Rat der Europäischen Union eine vorläufige Einigung über den Entwurf erzielt. Der CRA soll die Cybersicherheit von in der EU vertriebenen digitalen Produkten durch eine sektorübergreifende Regulierung verbessern. Wie dies gelingen soll, welche Ansätze verfolgt werden und inwieweit Hochschulen betroffen sein werden, wird im Folgenden erörtert.

Text: **Klaus Palenberg** (Forschungsstelle Recht im DFN)

I. Ziel des Gesetzgebungsverfahrens

Es wird mittlerweile gebetsmühlenartig wiederholt, jedoch mindert dies nicht den Wahrheitsgehalt der Aussage: Die Gefahr von Cyberangriffen ist erheblich. Sowohl Hardware- als auch Softwareprodukte sind zunehmend Gegenstand erfolgreicher Cyberangriffe. Jährlich entstehen so weltweit durch Cyberkriminalität geschätzt Kosten von 5,5 Billionen Euro.[2] Einfallstor für die Angreifer sind dabei meist Produkte mit digitalen Elementen. Diese weisen häufig zu wenige oder unzureichende Maßnahmen der Cybersicherheit auf. Fatalerweise werden regelmäßige Sicherheitsupdates entweder gar nicht angeboten oder nicht durchgeführt oder die technischen Komponenten sind schlicht von vornherein nicht ausreichend gegen Angriffe abgesichert. Digitale Produkte bergen somit erhebliche Gefahren für die IT-Sicherheit und verursachen sowohl für Unternehmen als auch für Verbrauchende einen immensen wirtschaftlichen Schaden.

Als Reaktion auf diese Problematik veröffentlichte die Europäische Kommission im Herbst 2022 einen bereits im Jahr 2021 angekündigten Verordnungsentwurf für einen Cyber Resilience Act. Durch diesen soll die Cybersicherheit von in der EU vertriebenen digitalen Produkten einheitlich und horizontal reguliert werden. Konkret sollen sektorübergreifend alle Produkte mit digitalen Elementen erfasst werden, das heißt, sämtliche Produkte, die bestimmungsgemäß oder vernünftigerweise vorhersehbar dazu benutzt werden können, eine Datenverbindung zu einem Gerät oder einem Netzwerk aufzubauen (Art. 2 I CRA-E). Insofern weist die Verordnung einen sehr weiten Anwendungsbereich auf. Es dürften somit jede Software, jedes Smartphone, jeder PC, aber auch smarte Geräte wie Kühlschränke oder Waschmaschinen, kurz jedes erdenkliche vernetzte digitale Produkt von den Regelungen des Cyber Resilience Act in unterschiedlicher Ausprägung betroffen sein.[3]

1 Abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 (zuletzt abgerufen am 01.08.2023).
2 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (zuletzt abgerufen am 01.08.2023).
3 Rennert, Mehr Cybersicherheit für vernetzte Produkte: Der Vorschlag der EU-Kommission für einen „Cyber Resilience Act“, ZfDR 2023, 206 (209).

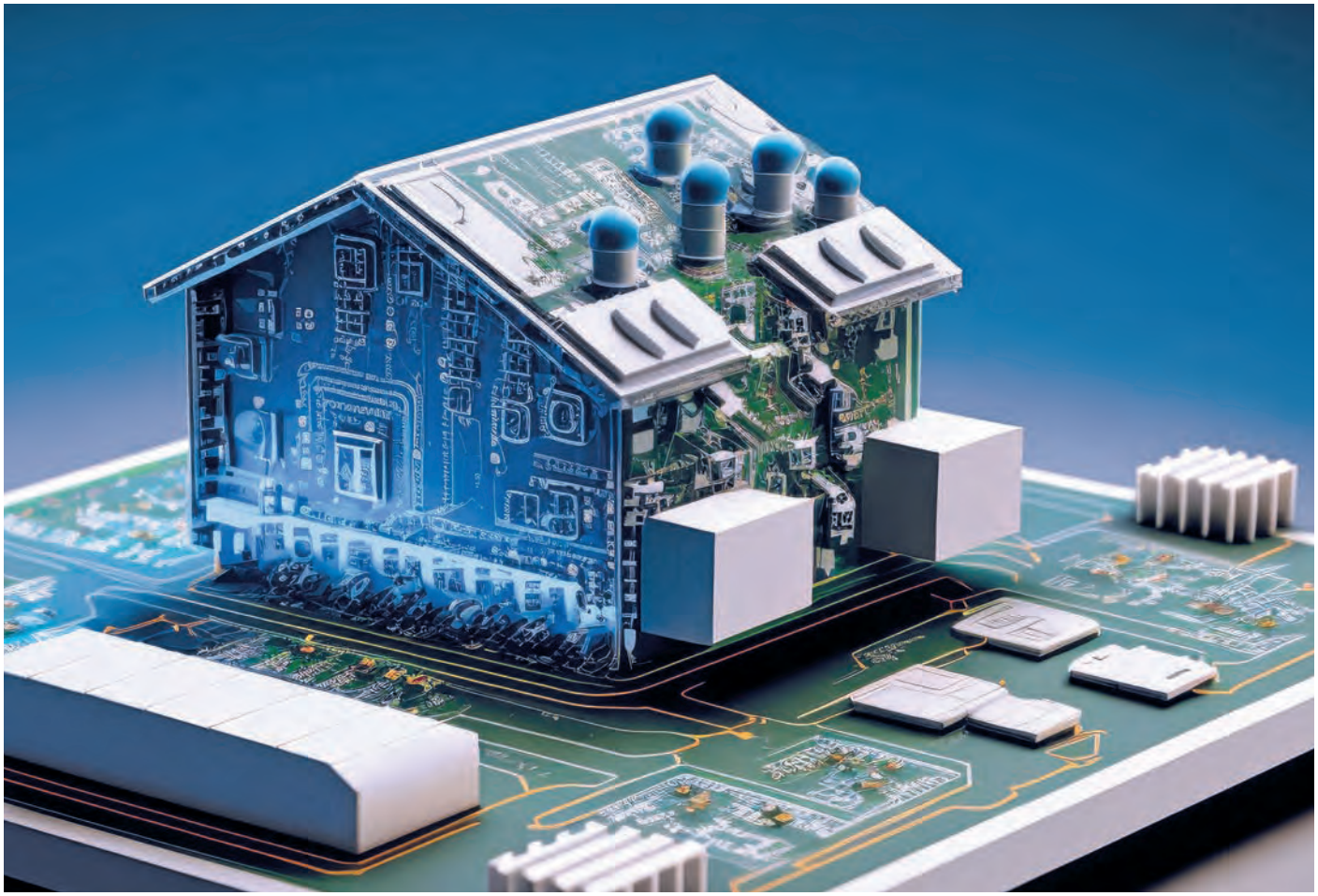


Foto: AstralAngel/Adobe Stock

II. Cyber Resilience Act

1. Bisherige Cybersicherheitsregulierung in der EU

Der Cyber Resilience Act reiht sich dabei in eine ganze Reihe europäischer Gesetzgebungsverfahren ein, die zu einer Stärkung der Cybersicherheit führen sollen. Bislang kamen hier hauptsächlich die NIS-RL[4] zum Schutz für elektronische Kommunikationsnetze und ihre Nachfolgerin, die NIS2-RL[5], zum Tragen.[6] EU-weit wird die Cybersicherheit darüber hinaus durch den Rechtsakt zur Cybersicherheit[7] und die EU-Infrastrukturschutz-RL[8] geregelt. Zwar wurde somit auf europäischer Ebene bereits eine Reihe von harmonisierenden Rechtsakten geschaffen, die das Sicherheitsniveau für digitale Produkte und digitale Kommunikation teilweise erhöhen sollen. Die große Schwäche der vielen verschiedenen Teilregelungen ist jedoch, dass sie ausschließlich punktuell schützen. So schützen die NIS-Richtlinien oder die EU-Infrastrukturschutz-RL beispielsweise ausschließlich den Bereich der kritischen Infrastrukturen. Eine effektive, sektorübergreifende Regulierung fehlt aber bislang. Diesen Missstand soll nun der Cyber Resilience Act beseitigen.

4 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

5 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

6 Hierzu bereits ausführlich: John, „CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?“ in DFN-Infobrief Recht 04/2023.

7 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

8 Richtlinie 2008/114/EG DES RATES vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

2. Anwendungsbereich des Cyber Resilience Act

Durch den Cyber Resilience Act werden deshalb alle vernetzten Produkte mit digitalen Elementen erfasst. Vom Anwendungsbereich der Richtlinie umfasst sind alle Software- oder Hardwarekomponenten, die separat auf den Markt gebracht werden und mit einem Netzwerk oder anderen Geräten verbunden sind. Ausgenommen wird lediglich „freie und quellenoffene Software, die außerhalb einer Geschäftstätigkeit entwickelt oder bereitgestellt wird“ (Erwägungsgrund 10), meist also wohl sog. „Open-Source-Software“. Ebenfalls sollen für solche Produkte keine weiteren Verpflichtungen entstehen, für die bereits spezifische Regelungen auf Grundlage anderer Rechtsakte, wie beispielsweise den oben genannten, vorhanden sind. Dies gilt insbesondere im medizinischen und verkehrstechnischen Sektor.

Doch sollen nicht für alle von der Verordnung erfassten digitalen Produkte dieselben Sicherheitsanforderungen gelten. Vielmehr werden verschiedene Sicherheitsstufen, namentlich kritische Produkte mit digitalen Elementen und hochkritische Produkte mit digitalen Elementen, eingeführt. Für sie gelten zusätzlich erhöhte Sicherheitsanforderungen. Für kritische Produkte mit digitalen Elementen findet sich im Anhang der Verordnung eine Festlegung von typischen, von der Definition erfassten Produktkategorien, aufgeteilt in zwei Klassen. Umfasst sind beispielsweise Passwortmanager, Produkte mit der Funktion eines virtuellen privaten Netzes (VPN), Industrielles-Internet-der Dinge-Geräte (IIoT), aber auch (virtuelle) Betriebssysteme für Desktop-Computer und mobile Endgeräte. Für sie gelten besondere Konformitätsbewertungsverfahren.

Für hochkritische Produkte mit digitalen Elementen fehlt eine solche Auflistung hingegen. Diese sollen, wenn sie ein bestimmtes Cybersicherheitsrisiko bergen, von der Kommission gesondert festgelegt werden. Erfasst werden sollen hier z. B. Produkte, die von wesentlichen Einrichtungen, die in der NIS2-RL aufgezählt sind, genutzt werden oder für die Widerstandsfähigkeit der gesamten Lieferkette von Produkten mit digitalen Elementen gegen Störungen von Bedeutung sind. Bei dieser Kategorie von Produkten wird dann ein Cybersicherheitszertifikat notwendig sein.

Konkret verpflichtet der Cyber Resilience Act auch Importeure und Vertreiber, aber vor allem natürlich Hersteller solcher Produkte. So werden konkrete Sicherheitsanforderungen für digitale Produkte insbesondere im Anhang I festgelegt, die die Hersteller zwingend zu berücksichtigen haben. Außerdem müssen Risikoanalysen durchgeführt werden, um die Cybersicherheit des Produktes sicherzustellen. Ebenso werden die Hersteller verpflichtet, Sicherheitslücken effektiv zu beheben. Konkret wird ihnen beispielsweise hierfür aufgegeben, für die Lebensdauer des Produktes, mindestens aber für fünf Jahre, Sicherheitsupdates für das digitale Produkt bereitzustellen. Außerdem müssen sogenannte Konformitätsbewertungsverfahren (Art. 24 CRA-E) durchgeführt werden. Es werden Informationspflichten (Anhang II) eingeführt und bei entdeckten Sicherheitslücken bestehen Berichtspflichten an die jeweils zuständigen Stellen.

Sollte den Verpflichtungen durch den Hersteller, Importeur oder Vertreiber nicht nachgekommen werden, drohen laut Art. 53 CRA-E Bußgelder in Höhe von 15 Mio. Euro oder alternativ 2,5 Prozent des weltweiten Vorjahresumsatzes. Außerdem besteht eine Rückrufbefugnis der Aufsichtsbehörden für Produkte, die nicht im Einklang mit den Vorschriften des Cyber Resilience Act stehen und daher ein erhebliches Cybersicherheitsrisiko oder eine Gefahr für die Gesundheit oder Sicherheit von Personen darstellen (Art. 45 CRA-E i. V. m. Erwägungsgrund 59).

Wer als Hersteller gilt, ergibt sich nach Art. 3 Nr. 18 CRA-E. Demnach wird ein Hersteller definiert als eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter eigenem Namen oder eigener Marke vermarktet, sei es entgeltlich oder unentgeltlich. Somit tritt neben die eigentliche Herstellung noch eine zweite Variante, nämlich die Vermarktung. Damit sind auch solche Akteure gemeint, die fremde Produkte unter eigenem Namen anbieten.

Bei Herstellern ergeben sich die obengenannten Pflichten, wenn sie das jeweilige Produkt „in Verkehr bringen“. Das ist nach Art. 3 Nr. 22 CRA-E bei der erstmaligen Bereitstellung eines Produkts mit digitalen Elementen auf dem EU-Binnenmarkt der Fall. Diese Bereitstellung wiederum liegt vor, wenn ein Produkt zum ersten Mal an einen Händler oder einen Endverbraucher geliefert wird.[9]

Bei den weiteren Akteuren kann auch eine „Bereitstellung auf dem Markt“ ausreichen, was nach Art. 3 Nr. 23 CRA-E jede entgeltliche oder unentgeltliche Abgabe eines Produkts mit digitalen Elementen zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit sein kann.

9 So der Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide“) – 2022/C 247/01, S. 19 (verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022XC0629(04)&from=EN, zuletzt abgerufen am 01.08.2023).

3. Weiterer Gang des Gesetzgebungsverfahrens

Der Entwurf der Kommission ist zwischenzeitlich vom Europäischen Parlament und dem Rat der Europäischen Union geprüft worden. Am 26. Juni 2023 wurde auch eine vorläufige Einigung[10] zwischen diesen beiden Institutionen erzielt und am 19. Juli 2023 ein gemeinsamer Standpunkt der Mitgliedstaaten[11] veröffentlicht. Hierin finden sich einige Änderungen in den Details, wie eine im Vergleich zum Kommissionsentwurf vereinfachte Konformitätserklärung. Auf Basis dieser Entscheidungen beginnt nun das Trilog-Verfahren über die endgültige Fassung der Verordnung. Nach Inkrafttreten besteht voraussichtlich eine ein- bis zweijährige Übergangsfrist für die betroffenen Akteure.

III. Auswirkungen für Hochschulen

Auch Hochschulen dürften von den Regelungen des Cyber Resilience Act unmittelbar betroffen sein. Dabei kann der Hochschule sogar eine Doppelnatur zukommen, indem sie zugleich als Herstellerin digitaler Produkte als auch als Nutzerin digitaler Produkte fungiert.

Soweit die Hochschulen selbst Produkte mit digitalen Elementen im Rahmen des Hochschulbetriebes oder auch zu Forschungszwecken herstellen bzw. entwickeln, ist zudem noch ein „Inverkehrbringen“ erforderlich. Grundsätzlich können somit auch digitale Produkte aus Hochschulhand unter den Anwendungsbereich des CRA fallen. Im Hinblick auf drohende Bußgelder ist dabei allerdings zu beachten, dass Art. 53 VIII CRA-E festlegt, dass jeder Mitgliedstaat Vorschriften darüber erlässt, ob und in welchem Umfang gegen Behörden und öffentliche Stellen Geldbußen verhängt werden können.

Vom Sinn und Zweck des Regelungsinhalts der Verordnung her erscheint es grundsätzlich richtig, dass auch Hochschulen von den Regelungen des Cyber Resilience Act erfasst werden. Neben Bußgeldern besteht als weitere Sanktionsmöglichkeit nämlich die Befugnis der Aufsichtsbehörden, einen Rückruf anzuordnen. Dieser sollte auch gegenüber Hochschulen durchgesetzt werden können, da sein Schutzzweck auf eine höhere Cybersicherheit abzielt. Die IT-Sicherheit kann auch durch digitale Produkte von Hochschulen gefährdet werden. Es ist daher davon auszugehen, dass auch Hochschulen als Hersteller von digitalen Produkten von den Regelungen des Cyber Resilience Act umfasst sein werden.

Besonders im Rahmen hochschulischer Tätigkeit ist die bereits angesprochene Bereichsausnahme für Open-Source-Software zu beachten. In jedem Fall nicht von dem Entwurf erfasst werden „offen geteilte und frei zugängliche, nutzbare, veränderbare und weiterverteilbare Software, einschließlich ihres Quellcodes und ihrer veränderten Versionen“ (Erwägungsgrund 10). Wie weit diese Ausnahme allerdings genau reicht und ob auch von Unternehmen unterstützte Projekte erfasst sind oder ob Open-Source-Software als fester Bestandteil eines weiteren digitalen Produkts unter die strengen Regelungen des CRA fallen soll, ist derzeit noch unklar. ◆

10 Siehe die Pressemitteilung vom selben Tag, abrufbar unter: https://www.consilium.europa.eu/de/press/press-releases/2023/06/26/cybersecurity-at-the-eu-institutions-bodies-offices-and-agencies-council-and-parliament-reach-provisional-agreement/ (zuletzt abgerufen am 01.08.2023).

11 Abrufbar unter: https://www.consilium.europa.eu/de/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/ (zuletzt abgerufen am 01.08.2023).

Hier werden keine Daten gecloud

DSK stellt Positionspapier zur Nutzung von souveränen Clouds vor

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)[1] hat eine Stellungnahme zur Nutzung von souveränen Clouds veröffentlicht.[2] Hierzu nennt sie eine Vielzahl konkreter Kriterien, anhand derer Cloud-Anbieter und -Anwender überprüfen können, ob ein spezifischer Cloud-Computing-Dienst souverän im Sinne ihrer Stellungnahme ist.

Text: **Johannes Müller** (Forschungsstelle Recht im DFN)

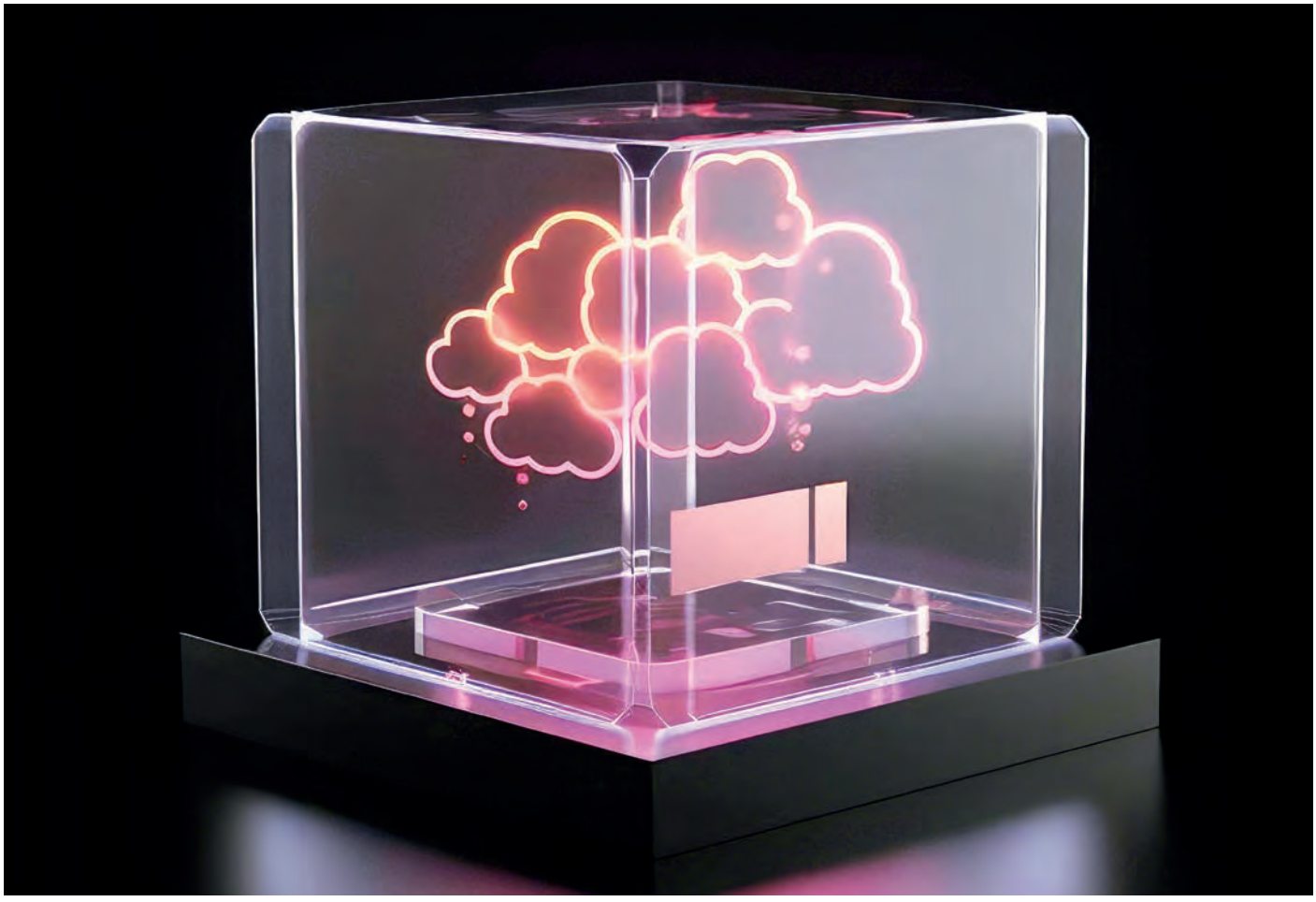


Foto: thongk8326/Freepik

I. Souveräne Clouds als politisches Entwicklungsziel

Die Auslagerung von Computerressourcen, etwa in Form von Datenspeichern oder Softwareanwendungen, auf Cloud-Computing-Dienste über das Internet stellt einen integralen Bestandteil der derzeitigen Digitalisierung dar. Vorteile der Nutzung von Cloud-Computing-Diensten liegen unter anderem darin, dass die verwendete Cloud-Infrastruktur dynamisch an die eigenen Ansprüche angepasst werden kann. Besteht etwa kurzzeitig ein erhöhter Bedarf für zusätzlichen Speicherplatz, lässt sich dieser im benötigten Zeitraum flexibel anmieten, ohne dass dauerhafte Investitionen, beispielsweise in die Erweiterung des eigenen Rechenzentrums, notwendig sind. Ebenso bringen Cloud-Computing-Dienste den Vorteil mit sich, dass ein Zugriff auf die Anwendungen über eine Internetverbindung von nahezu jedem Gerät möglich ist.

Die Auslagerung von Ressourcen auf Cloud-Computing-Dienste birgt allerdings auch Risiken. Die Nutzung fremder IT-Infrastruktur kann mit einer Ungewissheit darüber einhergehen, welche Personen Zugriff auf die gespeicherten Daten oder die genutzte Software haben. Befinden sich die Server der Cloud im EU-Ausland, beispielsweise in den USA, besteht etwa das Risiko, dass ausländische Sicherheitsbehörden Zugriff auf die Daten erhalten. Daneben kommen aber auch zahlreiche Gefahren durch private Akteure in Betracht, etwa in Form eines Datendiebstahls durch einen Hackerangriff. Aufgrund dieser Gefahren gewinnt die Thematik der souveränen Clouds zunehmend an Bedeutung und wird auch auf politischer Ebene kritisch diskutiert. Die Anforderungen an eine souveräne Cloud sind bisher nicht fest definiert. In ihrer Stellungnahme nennt die DSK die Definition des Kompetenzzentrums Öffentliche IT, nach der „Digitale Souveränität" als „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können"[3] definiert wird. Daran anknüpfend beschäftigt sich die DSK in ihrer Stellungnahme mit unterschiedlichen Kriterien, die eine souveräne Cloud erfüllen soll. Diese Kriterien richten sich sowohl an Anbieter von Cloud-Diensten als auch an deren Anwender. Insbesondere Letztere sollen durch die Kriterien bei der Auswahl einer Cloud-Lösung unterstützt werden. Die Bewertung von souveränen Clouds erfolgt durch die DSK primär aus datenschutzrechtlicher Perspektive. So betont die DSK, dass eine souveräne Cloud alle Vorgaben des Datenschutzrechtes, sowohl aus der DSGVO als auch aus den bundes- und landesrechtlichen Regelungen einzuhalten hat. Eine souveräne Cloud soll darüber hinausgehend jedoch nicht lediglich datenschutzkonform sein, sondern auch die zugrunde liegende Problematik grundlegend und nachhaltig lösen.

Im Rahmen ihrer Stellungnahme nennt die DSK einerseits Muss-Kriterien, die eine souveräne Cloud zwingend zu erfüllen hat, und darüber hinaus Soll-Kriterien, die zusätzliche Empfehlungen darstellen.

II. Nachvollziehbarkeit durch Transparenz

Die DSK beschäftigt sich zunächst mit dem Transparenzgrundsatz des Art. 5 Abs. 1 lit. a DSGVO. Diesem zufolge hat eine Verarbeitung personenbezogener Daten in einer für die betroffene Person nachvollziehbaren Weise zu erfolgen. Demnach müssen Anbieter von Cloud-Diensten imstande sein nachzuweisen, dass die Datenverarbeitung nach den Vorgaben der DSGVO erfolgt. Im Rahmen eines transparenten Cloud-Angebots muss der Cloud-Anbieter dem Cloud-Anwender bereits vor Vertragsschluss eine Dokumentation zur Verfügung stellen, die Auskunft darüber gibt, welche externen Komponenten und Dienstleistungen im Rahmen des Cloud-Angebots eingesetzt werden und dass die Verarbeitung hierbei datenschutzkonform erfolgt. Zum Nachweis können etwa Vereinbarungen mit Dritten vorgelegt werden.

Zur Gewährleistung der Interoperabilität mit anderen Cloud-Systemen müssen Cloud-Anbieter die Anwender über die verfügbaren Schnittstellen und Möglichkeiten des Datenexports informieren. Zu den Transparenzanforderungen zählt die DSK auch die Pflicht der Anbieter nachzuweisen, wie sie in Zukunft einen dauerhaften und unabhängigen Betrieb des Angebots gewährleisten wollen. Als Empfehlungen für eine transparente Cloud-Nutzung nennt das Papier darüber hinaus den Einsatz von Open-Source-Software und offenen Standards.

III. Datenhoheit und Kontrollierbarkeit

Essenziell für eine souveräne Cloud ist die Kontrollierbarkeit ihrer Nutzung, sodass betroffene Personen ihre Datenhoheit wahren können.

Um die Anforderungen an die Kontrollierbarkeit einer souveränen Cloud zu erfüllen, ist es erforderlich, dass die Anbieter der Cloud

1 Vgl. zur Arbeit der DSK beispielhaft Müller, Datenschutz auf Rezept, DFN-Infobrief Recht 02/2023.

2 Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023. Kriterien für Souveräne Clouds, https://www.datenschutzzentrum.de/uploads/dsk/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf (zuletzt abgerufen am 15.06.2023).

3 Kompetenzzentrum Öffentliche IT, Digitale Souveränität, 3, https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t (zuletzt abgerufen am 15.06.2023).

personenbezogene Daten ausschließlich im Rahmen von konkreten Weisungen verarbeiten. Innerhalb der Cloud-Nutzung muss zudem eine Trennung der unterschiedlichen Verarbeitungsvorgänge erfolgen. Ist eine physische Trennung nicht möglich, hat diese durch technische und organisatorische Maßnahmen zu erfolgen. Die Stellungnahme empfiehlt zudem, dass bei der Einschaltung von Unterauftragsverarbeitern die Anwender selbst möglichst weitgehend auf diese einwirken und auch einzelne Unterauftragsverarbeiter abwählen können.

Zu dem Kriterium der Datenhoheit zählt die DSK auch die Verhinderung von Zugriffsmöglichkeiten der Behörden von Drittländern. Die Anbieter haben sicherzustellen, dass ausschließlich Datenzugriffe möglich sind, die nach EU-, EWR- bzw. nationalem Recht zulässig sind. Hierfür genügen in der Regel keine vertraglichen Maßnahmen.

Um die Beherrschbarkeit der Daten sicherzustellen, müssen Rechte und Pflichten eindeutig vertraglich festgehalten werden. Es muss festgelegt werden, wie die Verletzung dieser Rechte und Pflichten sanktioniert wird. Die Sanktionen müssen ferner gerichtlich durchsetzbar sein.

Bezüglich des Anbietersitzes und des Verarbeitungsortes geht die Empfehlung über die datenschutzrechtlichen Pflichten hinaus. Die DSGVO sieht die Möglichkeit zur Übertragung personenbezogener Daten in Drittländer vor. Hingegen erfordert eine souveräne Cloud nach Ansicht der DSK eine Datenverarbeitung, die ausschließlich im Europäischen Wirtschaftsraum stattfindet.

IV. Offenheit

Ein weiteres Kriterium, welches der effektiven, nachprüfbaren und dauerhaften Einhaltung der datenschutzrechtlichen Pflichten von Cloud-Anbietern dient, ist das der Offenheit. Zur Ausgestaltung ihrer Verarbeitungstätigkeiten sollen die Anwendenden eine Wahlmöglichkeit zwischen unterschiedlichen Cloud-Angeboten haben, um Abhängigkeiten zu vermeiden. Dazu sollen auch spätere Wechsel des Cloud-Angebots mit möglichst geringem Aufwand möglich sein.

Um diesem Kriterium gerecht zu werden, ist es notwendig, dass die Cloud-Angebote einfach zu ersetzen sind. Sie müssen insbesondere den Export aller betrieblich relevanten Daten und Objekte ermöglichen. Außerdem empfiehlt die DSK, den Anbietern souveräner Clouds ein hohes Maß an Kombinierbarkeit ihrer Lösungen zu ermöglichen und den Anwendern diesbezüglich angemessene Dokumentationen und Hilfsmittel bereitzustellen. Zum einen sollte die Einbindung externer IT-Systeme und -dienste in das Cloud-Angebot möglich sein. Zum anderen sollte das Cloud-Angebot selbst in andere Lösungen einzubinden sein. Hiermit geht die Möglichkeit einher, Teilkomponenten und -funktionen souveräner Cloud-Angebote zu nutzen, die für Anwender bestehen sollte.

Der Offenheit von Cloud-Angeboten kommt zudem zugute, wenn die souveräne Cloud in möglichst allen Bereichen eine Nutzung auf Basis offener Standards erlaubt. Nicht nur Dateiformate, sondern auch etwaige Schnittstellen und Protokollierungen sollten auf offenen Standards basieren. Allerdings sollte die Nutzung einer Cloud auch ohne spezifische Erweiterungen möglich sein. Darüber hinaus sollten souveräne Clouds bestenfalls vollständig auf Open-Source-Software basieren, um Anwendern bei Bedarf Einblick in die Umsetzung der Cloud-Plattform zu verschaffen. So könnten im Falle eines Angebotswechsels hilfreiche Informationen erlangt und – sofern die Plattform unter einer freien Lizenz steht – Teile der Umsetzung übernommen werden.

V. Vorhersehbarkeit und Verlässlichkeit

Um die Souveränität der Cloud-Angebote langfristig zu erhalten, müssen diese vorhersehbar und verlässlich sein. Dazu ist es notwendig, dass die Anbieter die Anwender frühzeitig über Strukturänderungen informieren, die sich negativ auf die Souveränität des Angebotes auswirken könnten. Weiterhin sind die Prinzipien des Art. 25 Abs. 1 und 2 DSGVO einzuhalten: Voreinstellungen von Cloud-Angeboten sind von den Anbietern stets datenschutzfreundlich zu wählen und Wechselwirkungen müssen transparent gemacht werden. Außerdem müssen Weiterentwicklungen möglichst modular erfolgen und – insbesondere im Falle sich ergebender datenschutzrechtlicher Risiken – möglichst auch abwählbar sein. Empfehlenswert ist zudem ein transparentes Geschäfts- und Finanzierungsmodell der Anbieter, damit sich die Seriosität und Rechtmäßigkeit des Modells überprüfen lassen. Um Änderungen nachvollziehen zu können, sollte sich die Transparenz zudem nicht auf das gegenwärtige Finanzierungsmodell beschränken. Damit die Weiterentwicklung, Änderung und Abkündigung von Eigenschaften für die Anwender eines Cloud-Angebots verlässlich und vorhersehbar ist, müssen diese in transparent dargelegten und planbaren Zyklen erfolgen. Außerdem bietet sich die Verwendung von Open-Source-Software wegen der notwendigen Prüffähigkeit von Cloud-Angeboten an, da diese den Anwendern die Überprüfung der Qualität eines Angebots erlaubt. Wenn Anbieter ihre Public Clouds auch in einer souveränen Ausgestaltung anbieten, sollten sie mittelfristig Feature-Parität zwischen beiden Varianten anstreben, um einen schleichenden Druck zum Verzicht auf das souveräne Angebot zu verhindern. Wird Feature-Parität nicht geschaffen, sollte zumindest über die Unterschiede zwischen den Varianten transparent und neutral informiert werden.

VI. Regelmäßige Prüfung der Kriterien

Zum Schluss beschäftigt sich die DSK in ihrer Stellungnahme noch mit der Überprüfung der aufgestellten Kriterien. Ob und welche der genannten Kriterien ein Cloud-Angebot erfüllt, muss für Anwender prüf- und nachvollziehbar sein. Zum einen muss die Software deshalb grundsätzlich überprüfbar sein. Zum anderen muss sie auch tatsächlich regelmäßig – und spätestens bei einer Änderung der mit den Verarbeitungsvorgängen verbundenen Risiken – überprüft werden. Dazu bedarf es der Bereitschaft der Anbieter, an einer solchen Überprüfung aktiv mitzuwirken (vgl. Art. 28 Abs. 3 lit. h DSGVO). Die Anbieter müssen also detaillierte Dokumentationen bereitstellen, auf Nachfragen antworten oder sich auch selbst an Vor-Ort-Überprüfungen beteiligen. Bestenfalls nutzen sie Zertifizierungsverfahren, mit denen die Einhaltung der DSGVO und der Kriterien der DSK nachgewiesen werden kann.

VII. Relevanz für wissenschaftliche Einrichtungen

Die Stellungnahme der DSK weist eine hohe Relevanz für wissenschaftliche Einrichtungen auf. Wie allen Veröffentlichungen der DSK kommt auch der vorliegenden Stellungnahme keine verbindliche Wirkung zu.[4] Aufgrund der Zusammensetzung der DSK aus allen Datenschutzbeauftragten der Länder und dem Bundesdatenschutzbeauftragten ist ihren Empfehlungen jedoch stets ein hohes Gewicht beizumessen. Befinden sich Universitäten oder andere wissenschaftliche Einrichtungen im Auswahlprozess eines Cloud-Computing-Dienstes, bieten die aufgestellten Kriterien eine starke Orientierungshilfe, um festzustellen, ob ein Cloud-Dienst die gängigen Anforderungen an die Souveränität erfüllt. Wissenschaftliche Einrichtungen sollten diese Kriterien berücksichtigen und lediglich souveräne Cloud-Computing-Dienste einsetzen. Einen großen Mehrwert bietet das Positionspapier der DSK insbesondere deshalb, weil eine Vielzahl der Kriterien konkret überprüfbar und umsetzbar ist und sich die Empfehlung damit nicht lediglich auf die Wiedergabe der Rechtslage beschränkt. ◆

4 Vgl. Müller, Datenschutz auf Rezept, DFN-Infobrief Recht 02/2023.

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 hinaus. Wo wir überall unterwegs sind, zeigen wir hier.

Als Koordinatorin für internationale Beziehungen und Projekte im DFN-Verein arbeitet Leonie Schäfer eng mit den Kolleginnen und Kollegen des europäischen Forschungsnetzes GÉANT zusammen. Pflichttermin im Sommer war selbstverständlich das jährliche Klassentreffen der nationalen Forschungsnetze, …

… die TNC23, die vom 5. bis 9. Juni 2023 in Tirana stattfand.

Gibt es für Sie noch weiße Flecken auf der Landkarte? Orte, an denen Sie noch nie waren und von denen Sie kaum etwas wissen? Die gab es für mich – sogar mitten in Europa. Tirana, die Hauptstadt des Balkanstaats Albanien, war nämlich der Veranstaltungsort der diesjährigen Konferenz. Jedes Jahr trifft sich die Community der weltweiten nationalen Forschungsnetze (National Research and Education Networks, NRENs) auf der TNC, einer der größten Netzwerkkonferenzen für Forschung und Bildung. Dieses Mal war ich sehr gespannt, nicht nur auf die TNC selbst, sondern auch auf Land und Leute. Und ich wurde nicht enttäuscht.

Tirana entpuppte sich als quirlige, lebendige Hauptstadt im südländischen Stil mit polyglotter Bevölkerung. Man sprach italienisch, griechisch, deutsch, englisch und natürlich albanisch, eine Sprache komplett unverwandt mit anderen europäischen Sprachen. Die durchschnittlich sehr junge Bevölkerung genießt das Leben draußen, in Restaurants und Cafés. Tirana ist eine moderne Metropole mit gut ausgebauten Fahrradwegen, E-Rollern, einer fortschrittlichen Mülltrennung, großstädtischem Verkehr und modernen, architektonisch spannenden Gebäuden.

Die TNC23 fand im Stadtzentrum im Palace of Congresses statt und wurde mit einer bombastischen Show eröffnet, die Hollywood alle Ehre gemacht hätte. Das polnische Forschungsnetz Poznan Supercomputing and Networking Center (PSNC) stellte in Kooperation mit dem nordischen Regionalnetz NORDUnet das Team für Organisation und Technik.

Erik Huizer, CEO von GÉANT, eröffnete die Veranstaltung gewohnt professionell und showmäßig. Begrüßt wurden die rund 800 Teilnehmenden von Arjan Xhelaj, dem Direktor des albanischen NRENs RASH sowie von Evis Kushi, Ministerin für Erziehung und Sport in Albanien. Einer der Höhepunkte der Eröffnungsveranstaltung war die Überreichung der Ehrenmedaille der Vietsch Foundation an Arjan Xhelaj und Sabine Jaume-Rajaonia. In seiner Würdigung betonte Kuratoriumsmitglied John Dyer die Verdienste des RASH-Direktors, der das albanische Forschungsnetz 2007 gegründet und innerhalb von 16 Jahren zu einer erfolgreichen Institution gemacht hat. Sabine Jaume-Rajaonia, vormalig bei RENATER, erhielt die Ehrenmedaille für ihren langjährigen Einsatz bei dem Aufbau und der Entwicklung von Forschungsnetzen in Europa und Afrika.

Das Publikum der TNC war, wie jedes Jahr, sehr international. Mehr als 120 Länder weltweit haben ein nationales Forschungsnetz. Für mich war dies besonders interessant, da ich im Auftrag des GÉANT-GN5-1-Projekts unterwegs war, genauer, für das Partner Relations International Team. Meine Aufgaben: für das neue Subprojekt „GÉANT Twinning Programme“ Partner zu finden und zudem Kontakt zu Repräsentierenden südamerikanischer NRENs aufzubauen. Beides war von Erfolg gekrönt: Bereits zum 1. Oktober starteten zwei GÉANT Twinning Pilots mit dem norwegischen NREN SIKT (Norwegian Agency for Shared Services in Education and Research), dem armenischen NREN ASNET-AM sowie den NRENs aus Malawi (MAREN) und Uganda (RENU). Die Pilotprojekte dauern sechs Monate und verfügen über ein symbolisches Budget. Die Projektergebnisse werden auf der nächsten TNC vorgestellt. Falls die Pilotprojekte erfolgreich verlaufen, sollen – so die Idee – weitere internationale Twinning-Projekte folgen. Auch die Kontakte mit Südamerika konnten intensiviert werden. Hier wird eine engere Zusammenarbeit zwischen dem europäischen Backbone-Netz GÉANT und RedClara, dem südamerikanischen Gegenstück, anvisiert.

Interessant gestaltete sich auch das Emerging NREN Programme von GÉANT. Das Programm soll die Integration von Vertretenden aufstrebender NRENs aus der ganzen Welt in die TNC-Gemeinschaft ermöglichen, Verbindungen auf verschiedenen organisatorischen Ebenen schaffen und künftig Kooperationen fördern. Dazu gehören eine eigene Session mit Vorträgen, ein Partnerprogramm mit Mitgliedern der GÉANT-Gemeinschaft auf der Grundlage gemeinsamer

Fortschritt und Tradition: Als Gastgeberin der TNC23 bewies die quirlige und junge Metropole Tirana, dass sie beides gekonnt vereint | *Fotos: DFN*

beruflicher Hintergründe und ein Social Event. Ich war in diesem Jahr eine der Teilnehmenden dieses Partnerprogramms. Meine Gesprächspartner kamen aus dem Nahen Osten. Obwohl zu dieser Zeit die Situation noch friedlich war, verlangte das Gespräch durchaus diplomatisches Fingerspitzengefühl. Dank an GÉANT für die Organisation dieses tollen Programms, die interessanten Gespräche und die daraus resultierenden Kontakte.

Insgesamt zeigte sich die TNC vielfältig und präsentierte einen großen Querschnitt an Themen. Genau dies ist für mich auch das Besondere an der TNC – diese bunte und wertvolle Mischung an Themen. Man kann Einblicke gewinnen in den State of the Art in Quantenkommunikation, lernt etwas über Unterseekabel und bringt sich nebenbei noch auf den neuesten Stand in Sachen Projektkommunikation.

Natürlich wurden bei der TNC23 auch die Social Events nicht vernachlässigt. Neben dem großen TNC-Dinner gab es eine Party im Stadtzentrum von Tirana, bei der albanische Bands spielten. Dafür wurde sogar eine Straße gesperrt und zur Partyzone erklärt. Das eigentliche TNC-Dinner fand vor den Toren von Tirana statt, im Farmrestaurant Ferma 100, das mit seinem riesigen Außengelände inmitten des Erzen-Tals nur wenige Kilometer von der Hauptstadt entfernt liegt. Hier gab es zusätzlich die Gelegenheit, Kontakte zu knüpfen und dabei auch die Kultur Albaniens in Form von Musik, Tanz und Kulinarik zu erleben.

Die TNC23 schloss genauso grandios wie sie startete, mit einer Keynote und einem ebenso inspirierenden wie humorigen Grußwort des Bürgermeisters von Tirana, Erion Veliaj, der mit seiner charismatischen Persönlichkeit die energiegeladene Aufbruchsstimmung Albaniens in Richtung EU sehr gut repräsentierte. Mit seiner Anekdote über die Simpsons, die den albanischen Austauschschüler Adil Hoxha aufnehmen, der sich später als Spion entpuppt, hatte er die Lacher auf seiner Seite und bewies eine feine Selbstironie.

Im Anschluss betonte Erik Huizer, wie wichtig Vertrauen innerhalb der NREN-Gemeinschaft ist – gerade in Zeiten zahlreicher Herausforderungen wie dem Klimawandel oder geopolitischen Auseinandersetzungen. Daran schloss John Dyer mit seiner Würdigung der Kolleginnen und Kollegen des ukrainischen NRENs URAN an und erinnerte daran, unter welch harten Bedingungen diese derzeit arbeiten müssen, um die Infrastruktur für Forschung und Bildung im Land aufrechtzuerhalten.

Zum krönenden Abschluss wurde das Geheimnis des nächsten Austragungsorts gelüftet: Zur TNC24 begrüßt uns im kommenden Jahr das französische Forschungsnetz RENATER in der Hauptstadt der Bretagne, Rennes. ◆

Connectivity at its best: Ob beim gemeinsamen TNC-Dinner unter freiem Himmel oder der Eröffnungsparty mit albanischen Bands – um sich auszutauschen, Beziehungen zu stärken und sich besser kennenzulernen, blieb ausreichend Zeit | *Fotos: DFN*

Alle Vorträge der TNC23 gibt es unter
https://tnc23.geant.org/recordings/

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 lebendigen Dialog und Wissenstransfer.

DFN-Betriebstagung

Kaum zu toppen: Bei der 79. DFN-Betriebstagung (BT), die am 17. und 18. Oktober 2023 im Leonardo Royal Hotel Berlin Alexanderplatz stattfand, schien die Lust auf eine Präsenzveranstaltung nicht nur DFN-seitig, sondern auch aufseiten unserer Community groß gewesen zu sein. Das machte sich insbesondere in den erneut gestiegenen Teilnehmendenzahlen bemerkbar – rund 300 Teilnehmende besuchten die BT vor Ort, mehr als 60 Leute schauten sich die Plenumsvorträge im Stream an.

Zum Auftakt der Tagung gaben die DFN-Kolleginnen und -Kollegen aus den Fachbereichen im Plenum ein Update der Themen rund um das Wissenschaftsnetz und seine Dienste: So gab es u. a. eine Wasserstandsmeldung zu den Upgrades im X-WiN, Informationen zu den Neuzugängen in den Föderierten Cloud-Diensten sowie einen Überblick zu neuen sowie geplanten Leistungsmerkmalen im Dienst DFN.Security. Überhaupt war das Thema IT-Sicherheit tagungsübergreifend sehr präsent – auch wegen der jüngsten Angriffswelle gegen Hochschulen. Nicht nur im Forum Sicherheit, sondern auch in den ebenso gut besuchten Foren Wissenschaftsnetz und Mail gab es Beiträge, die sich mit Cybersecurity befassten. Hier zeigte sich erneut der Benefit der DFN-Betriebstagung als geschütztes Forum für den aktuell hohen Diskussionsbedarf und den offenen Erfahrungsaustausch in der Community.

TERMIN

Die 80. DFN-Betriebstagung findet am **Dienstag und Mittwoch, 19. und 20. März 2024,** statt.

Ob im Plenum oder in der Pause, die spannenden Themen und Neuigkeiten sorgen für viel Gesprächsstoff unter den Teilnehmenden | *Fotos: Stella Lenz, DFN*

DFN-Mitgliederversammlung

Am Dienstag, 13. Juni 2023, fand die 86. Mitgliederversammlung (MV) des DFN-Vereins in der Berlin-Brandenburgischen Akademie der Wissenschaften in Berlin statt. Zweimal im Jahr treffen sich Vertretende der mehr als 350 institutionellen Mitglieder aus Forschung und Lehre, darunter die Mehrzahl der deutschen Hochschulen, Forschungseinrichtungen sowie forschungsnahe Wirtschaftsunternehmen, um gemeinsam die Zukunft des DFN-Vereins zu gestalten.

Zu Beginn berichteten der Vorstand und die Geschäftsführung über die Aktivitäten des DFN-Vereins im Jahr 2022 sowie über die aktuellen Entwicklungen bei der Netzinfrastruktur und den DFN-Diensten. Dabei lag der Fokus unter anderem auf dem im Januar 2023 gestarteten Projekt GN5-1. Thema waren außerdem die europaweite Ausschreibung von Teilnehmeranbindungen im Zugangsnetz, die aktuelle Welle von Cyberangriffen auf deutsche Hochschulen sowie die nächsten Schritte bei der Entwicklung von weiteren Leistungsmerkmalen im Dienst DFN.Security.

Beim Vorabendempfang, der traditionell der Kontaktpflege und der Vernetzung gilt, trafen die Mitgliedsvertretenden im Museum für Naturkunde Berlin, das im Übrigen auch Mitgliedseinrichtung des DFN-Vereins ist, auf ganz besondere „Tischnachbarn“: Neben Giraffatitan brancai, der mit seinen rekordträchtigen 13,27 Metern über den Saal des Museums wacht, sorgte auch das originale Berliner Exemplar des Urvogels Archaeopteryx lithographica – die Mona Lisa der Fossilien – dafür, dass der Gesprächsstoff garantiert nicht ausging. Ein Highlight war der Vortrag von Museumsdirektor Prof. Johannes Vogel. Danach hatten die Geladenen Gelegenheit, das Museum auf eigene Faust zu erkunden.

Speisen unter Riesenechsen: Beim Vorabendempfang im Naturkundemuseum gehen die Mitgliedsvertretenden auf Tuchfühlung mit den Exponaten | *Fotos: Christoph Schieder*

TERMIN

Die 87. Mitgliederversammlung und der Vorabendempfang finden am **Dienstag und Mittwoch, 12. und 13. Dezember 2023,** (nach Redaktionsschluss der DFN-Mitteilungen) statt.

Die 88. Mitgliederversammlung und der Vorabendempfang finden am **Montag und Dienstag, 10. und 11. Juni 2024,** statt.

Vorstand und Geschäftsführung: Sie stehen den Mitgliedsvertretenden Rede und Antwort zu den Aktivitäten des DFN-Vereins (v. li. DFN-Geschäftsführer Jochem Pattloch, stellvertretender Vorsitzender Christian Zens, MV-Versammlungsleiter Hartmut Hotzel, Vorstandsvorsitzender Prof. Dr. Odej Kao und DFN-Geschäftsführer Dr. Christian Grimm) | *Foto: Nina Bark*

DFN-Konferenz „Sicherheit in vernetzten Systemen“

Die DFN-Konferenz „Sicherheit in vernetzten Systemen“ wird jedes Jahr von der DFN-CERT Services GmbH im Auftrag des DFN-Vereins veranstaltet. Mit ihrer explizit technischen und wissenschaftlichen Ausrichtung und einer großen Vielfalt an praxisbezogenen Themen hat sich die DFN-Konferenz als eine der größten deutschen Tagungen für Informationssicherheit etabliert.

TERMIN

Die 31. DFN-Konferenz „Sicherheit in vernetzten Systemen“ findet am **Dienstag und Mittwoch, 30. und 31. Januar 2024,** statt.

Forum Hochschulkanzler 2024

Das Diskussionsforum der Kanzlerinnen und Kanzler der Hochschulen im DFN-Verein richtet sich an alle Personen, die auf Ebene der Hochschulleitung eine strategische Verantwortung für Informationsverarbeitung und datentechnische Kommunikation (IuK) tragen.

Im Abstand von zwei Jahren bietet das DFN-Forum die Gelegenheit, sich auf Ebene der Hochschulleitungen über aktuelle Themen rund um die sich schnell wandelnden Herausforderungen der Nutzung von netzbasierten Informations- und Kommunikationsdiensten zu informieren und sich untereinander sowie mit Vertretenden des DFN-Vereins auszutauschen.

TERMIN

Das Diskussionsforum der Kanzlerinnen und Kanzler der Hochschulen im DFN-Verein findet am **Montag und Dienstag, 13. und 14. Mai 2024,** in Berlin statt.

DFN-Konferenz „Datenschutz“

Seit 2012 veranstaltet das DFN-CERT im Auftrag des DFN-Vereins jährlich die DFN-Konferenz „Datenschutz“. Ziele sind 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 Vertretenden der Datenschutzaufsichtsbehörden sowie eingeladenen Expertinnen und Experten aus der Datenschutzpraxis zu diskutieren.

TERMIN

Die 11. DFN-Konferenz „Datenschutz“ findet am **Dienstag und Mittwoch, 26.11. und 27.11.2024,** statt.

Tagung der DFN-Nutzergruppe Hochschulverwaltung in Bamberg

Seit ihrer Gründung 1991 veranstaltet die DFN-Nutzergruppe Hochschulverwaltung alle zwei Jahre eine Tagung. Diese greift aktuelle Themen aus den Bereichen Informations-, Kommunikations- und Medientechnik auf und setzt sie in direkten Bezug zu Themen aus der Hochschulverwaltung.

Die 17. Tagung der DFN-Nutzergruppe fand vom 8. bis 10. Mai 2023 in der Aula der Universität Bamberg, einer ehemaligen Dominikanerkirche, statt. Hieß es im vergangenen Jahr unter dem Blickwinkel der Coronabedingungen noch „Campus transformieren – Surfen auf der Digitalisierungswelle“, so folgte die Nutzergruppe in diesem Jahr dem Motto „Digitalisierung – Einfach? Gemeinsam machen!“ Behandelt wurden dabei unter anderem zentrale Fragen zur Informationssicherheit, Kooperationen im Bereich von Hochschulverwaltungen, Datenhaltung und Softwarebeschaffung. Das hochkarätige Programm war bewusst so geplant, dass ausreichend Zeit für den fachlichen Austausch der Teilnehmenden blieb.

Nachdem der Präsident der Universität Bamberg, Prof. Kai Fischbach, und die Leiterin der DFN-Nutzergruppe, Dr. Inga Scheler, die Anwesenden am Montag begrüßt hatten, berichtete der stellvertretende Vorsitzende des DFN-Vereins, Dr. Rainer Bockholt, über aktuelle Themen rund um das Deutsche Forschungsnetz.

Beschäftigen sich mit den aktuellsten Themen der Community: Die Mitglieder der DFN-Nutzergruppe Hochschulverwaltung: Dr. Beate Firla, Ingrid Bohr, Fabian Heuel, Bärbel Hannak, Silke Heimlicher, Dr. Lars Hinrichs, Dr. Robert Reilein, Prof. Dr. Gerhard Peter, Dr. Claudia Pauli, Uwe Blotevogel, Heike Ausserfeld, Dr. Inga Scheler, Artur Bursy, Peter Kurz, Herbert Röbke (untere Reihe v. li. bis obere Reihe v. li.)

Vergangenheit trifft Gegenwart: In den sakralen Räumlichkeiten der ehemaligen Dominikanerkirche diskutieren die Teilnehmenden zukunftsgewandte Themen aus dem Hochschulbereich. Prof. Dr. Gerhard Peter, Klaus Palenberg, Nicolas John (v. li.) | Alle *Fotos: DFN-Nutzergruppe Hochschulverwaltung*

ersten Impulse zum Themenschwerpunkt der Tagung kamen aus dem Bayerischen Staatsministerium für Digitales. Anschließend erhielten die Teilnehmenden einen Einblick in die gemeinsame IT-Strategie der bayerischen Hochschulen. Die Ergebnisse dieser Vorträge mündeten zum Abschluss des ersten Tages in einer regen Podiumsdiskussion: So wurden die Vor- und Nachteile von Kooperationsformen zur Unterstützung der Digitalisierung an Hochschulen kontrovers diskutiert.

Am zweiten Tag standen zunächst Digitale Souveränität, Informationssicherheit und rechtliche Aspekte der Digitalisierung im Fokus. Hier wurde primär die Problematik adressiert, in Zeiten der Globalisierung und der Cloud-Nutzung die Hoheit über die eigenen Daten zu behalten, den Anforderungen der deutschen Datenschutz-Grundverordnung gerecht zu werden und gleichzeitig zuverlässige, professionelle Dienste anbieten zu können. Das Programm des Tages wurde durch das Themenfeld E-Government und Onlinezugangsgesetz (OZG) abgerundet. Dabei ging es um die Komplexität dieser Vorhaben und die Herausforderungen, die gesetzlichen Vorgaben im heterogenen Hochschulumfeld umzusetzen. Mit Praxisbeispielen aus diesen beiden Bereichen startete der letzte Tag der Veranstaltung. Der Vortrag „European University Networks (EUN) – Digital open campus“ setzte sich mit den unterschiedlichen Herangehensweisen im europäischen Vergleich auseinander. Den Abschluss der Tagung bildeten Vorträge aus dem Bereich des Prozessmanagements und der Messbarkeit des Digitalisierungsgrades von Hochschulverwaltungen mithilfe einer Prozesslandkarte.

Die 17. Tagung der DFN-Nutzergruppe Hochschulverwaltung war ein voller Erfolg. Die breite positive Resonanz der insgesamt 250 Teilnehmerinnen und Teilnehmer zeigte, dass es die Nutzergruppe auch in diesem Jahr mit einem hochaktuellen Programm, spannenden Themen sowie Gelegenheiten zur Diskussion und Vernetzung geschafft hat, die Wünsche der Hochschul-Community zu adressieren. Auch das Rahmenprogramm, mit dem die Besucherinnen und Besucher auf den historischen Spuren des Weltkulturerbes Bamberg wandelnkonnten, trug zum Gelingen der Tagung bei. Die Nutzergruppe dankt allen Unterstützerinnen und Unterstützern, insbesondere der Universität Bamberg als Gastgeberin, und freut sich bereits jetzt auf die nächste Tagung 2025, deren Datum und Ort zu gegebener Zeit bekannt gemacht werden.

Text: **Inga Scheler**, Leiterin der DFN-Nutzergruppe Hochschulverwaltung und Stellvertretende Leitung des Regionalen Hochschulrechenzentrums (RHRZ) Kaiserslautern-Landau der Rheinland-Pfälzischen Technischen Universität Kaiserslautern-Landau, Kontakt: **scheler@rptu.de**
https://www.hochschulverwaltung.de/wir-ueber-uns

Das Tagungsprogramm und die Vortragsfolien sind auf der Homepage (siehe QR-Code) zu finden

Alle Veranstaltungen des DFN-Vereins finden Sie hier:
https://www.dfn.de/news/veranstaltungen/

Überblick DFN-Verein

(Stand: 11/2023)

Foto: 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 insbesondere verwirklicht 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

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

Standort Stuttgart
DFN-Verein e. V.
Lindenspürstraße 32
70176 Stuttgart
Telefon: +49 711 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, Hochschule Heilbronn.

Verwaltungsrat
Der Verwaltungsrat beschließt alle wesentlichen Aktivitäten des Vereins, insbesondere die technisch-wissenschaftlichen Arbeiten, und berät den Jahreswirtschaftsplan. Für die 13. Wahlperiode sind Mitglieder des Verwaltungsrates:

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

Franziska Broer
(Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.)

Prof. Dr. Frank Jenko
(Technische Universität München)

Prof. Dr. Sabina Jeschke
(Arctic Brains AB, Schweden)

Prof. Dr. Odej Kao
(Technische Universität Berlin)

Dr. Holger Marten
(Christian-Albrechts-Universität zu Kiel)

Dr. Karl Molter
(Hochschule Trier)

Prof. Dr.-Ing. Stephan Olbrich
(Universität Hamburg)

Dr. Hartmut Plehn
(Otto-Friedrich-Universität Bamberg)

Prof. Dr.-Ing. Dr. h.c. Stefan Wesner
(Universität zu Köln)

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

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

Prof. Dr. Harald Ziegler
(Ruhr-Universität Bochum)

Der Verwaltungsrat hat als ständige Gäste

eine Vertreterin der Hochschulrektorenkonferenz:
Prof. Dr. rer. nat. Ulrike Tippe
(Technische Hochschule Wildau)

einen Vertreter der Hochschulkanzlerinnen und -kanzler:
Dietmar Smyrek
(Hauptberuflicher Vizepräsident für Personal, Finanzen und Hochschulbau der Technischen Universität Braunschweig)

einen Vertreter der Kultusministerkonferenz:
Jürgen Grothe
(SMWK Dresden)

den Vorsitzenden der jeweils letzten Mitgliederversammlung:
Prof. Dr. Gerhard Peter
(Hochschule Heilbronn)

den Vorsitzenden des ZKI:
Torsten Prill
(Freie Universität Berlin)

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. Odej Kao
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 Mitgliedseinrichtungen

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	Technische Hochschule Augsburg
	Universität Augsburg
Bad Homburg	NTT Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	Berlin-Brandenburgische Akademie der Wissenschaften
	Berliner Institut für Gesundheitsforschung/Berlin Institute of Health
	Berliner Hochschule für Technik (BHT)
	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
	Bundesanstalt für Materialforschung und -prüfung
	Bundesinstitut für Risikobewertung
	Deutsche Telekom AG Laboratories
	Deutsche Telekom IT GmbH
	Deutsches Herzzentrum Berlin
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	European School of Management and Technology GmbH (ESMT)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin (FUB)
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hertie School gGmbH
	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
	Museum für Naturkunde – Leibniz-Institut für Evolutions- und Biodiversitätsforschung
	NOW GmbH Nationale Organisation Wasserstoff- und Brennstoffzellentechnologie
	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)
	Zuse-Institut Berlin (ZIB)
Biberach	Hochschule Biberach
Bielefeld	Hochschule Bielefeld – University of Applied Sciences and Arts (HSBI)
	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, für Bau und Heimat
	BundesminIsterium für Umwelt, Naturschutz und 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 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
Buxtehude	hochschule 21 gemeinnützige GmbH
Chemnitz	Technische Universität Chemnitz
	TUCed – An – Institut für Transfer und 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	Forschungsinstitut 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	Folkwang Universität der Künste
	RWI – Leibniz-Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Europa-Universität Flensburg
	Hochschule Flensburg
Forchheim	Institut für Nanotechnologie und korrelative Mikroskopie gGmbH
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
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH
	Leibniz-Rechenzentrum der 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
	Burg Giebichenstein Kunsthochschule Halle
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
Hameln	Hochschule Weserbergland
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 Heilbronn
Hildesheim	Hochschule für angewandte Wissenschaft und Kunst Fachhochschule Hildesheim/Holzminden/Göttingen
	Stiftung Universität Hildesheim
Hof	Hochschule für angewandte Wissenschaften Hof
Idstein	Hochschule Fresenius gemeinnützige Trägergesellschaft mbH
Ilmenau	Technische Universität Ilmenau
Ingolstadt	BayZiel - Bayerisches Zentrum für Innovative Lehre
	Technische Hochschule 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
	Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau
Karlsruhe	Bundesanstalt für Wasserbau
	FIZ Karlsruhe - Leibnitz-Institut für Informationsinfrastruktur
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe – Technik und Wirtschaft
	Karlshochschule International University
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	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
	IPN Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik
	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	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
	Leibniz-Institut für Neurobiologie Magdeburg
Mainz	Hochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Katholische Hochschule Mainz
Mannheim	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	Hochschule Mannheim
	Universität Mannheim
	ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung GmbH
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Philipps-Universität Marburg
Meißen	Hochschule Meißen (FH) und Fortbildungszentrum
Merseburg	Hochschule Merseburg (FH)
Mittweida	Hochschule Mittweida
Mülheim an der Ruhr	Hochschule Ruhr West
Müncheberg	Leibniz-Zentrum für Agrarlandschaftsforschung (ZALF) 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	FH Münster University of Applied Sciences
	Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neu-Ulm	Hochschule für Angewandte Wissenschaften Neu-Ulm
Nordhausen	Hochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
	Technische Universität Nürnberg
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)
	Hochschule für Gestaltung (HfG)
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
	Filmuniversität Babelsberg KONRAD WOLF
	Potsdam-Institut für Klimafolgenforschung (PIK)
	Universität Potsdam
Regensburg	Ostbayerische Technische Hochschule Regensburg
	Universität Regensburg
Reutlingen	Hochschule Reutlingen
Rosenheim	Technische Hochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	CISPA – Helmholtz-Zentrum für Informationssicherheit gGmbH
	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
Vallendar	Vinzenz Palotti University gGmbH
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 Information Services 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
Würzburg	Julius-Maximilians-Universität Würzburg
	Technische Hochschule Würzburg-Schweinfurt
	Universitätsklinikum 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 Informationsrechts

DFN newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

Podcast Forschungsstelle Recht im DFN
„Weggeforscht“ beschäftigt sich mit aktuellen juristischen Fragestellungen aus dem digitalen Umfeld

DFN auf Mastodon
trötet & teilt spannende News rund um das Deutsche Forschungsnetz

DFN auf X
postet aktuelle Nachrichten zum Deutschen Forschungsnetz

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