DFN mitteilungen

Zuverlässig gesichert

Mit einem starken Konzept
für IT-Sicherheit

Eine Sache der Perspektive

DFN-Vorstandsvorsitzender
Stefan Wesner im Interview

Für Forschung und Lehre

Chat AI, die datenschutzfreundliche KI

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

Fotonachweis
Titel: mariusz szczygieł/Adobe Stock
Rückseite: Elenarts/Adobe Stock

Prof. Dr. Helmut Reiser
Stellvertretender Vorsitzender im DFN-Verein
Stellvertretender Leiter des Leibniz-Rechenzentrums
der Bayerischen Akademie der Wissenschaften
Professor am Lehrstuhl Kommunikationssysteme und
Systemprogrammierung der Ludwig-Maximilians-
Universität (LMU) München

Kommunikation, Kollaboration und Vernetzung auf höchstem Niveau zeichnen uns als Wissenschaftsgemeinschaft aus. Sie machen aber unsere offene Infrastruktur auch angreifbar. Ob große oder kleine Einrichtungen mit unterschiedlichen Bedarfen und Kapazitäten – alle im DFN-Verein haben ein Grundbedürfnis nach Sicherheit. Grundlage unseres gemeinsamen Handelns ist das gegenseitige Vertrauen und das Wissen, dass dem anderen meine Sicherheit genauso am Herzen liegt wie die eigene.

Vertrauen wiederum speist sich aus gemeinsamen Werten und einem gemeinsamen Verständnis, was Sicherheit beinhaltet. Einheitliche Standards für ein wirksames Informationssicherheitsmanagement und definierte Prozesse sind hilfreich und erleichtern das Handeln. Wichtig ist, IT-Sicherheit als Aufgabe anzunehmen, aktiv zu werden und voneinander zu lernen. Im Verein muss nicht jede Einrichtung das Rad neu erfinden. Die Erfahrungen, die wir im LRZ gemacht haben, können wir gerne weitergeben. Frei machen müssen wir uns von dem Gedanken, das Thema IT-Sicherheit vollenden zu können. IT-Sicherheit ist ein permanenter Entwicklungsprozess, der dem rasanten Technologiefortschritt folgt.

Hat sich die Zertifizierung unseres Informationssicherheits-Managementsystems (ISMS) am LRZ gelohnt? In mehr als einer Hinsicht. Nach außen hat sie Vertrauen und Glaubwürdigkeit, die über eine bloße Selbstauskunft hinausgehen und von einer externen objektiven Quelle auditiert wurden, geschaffen. Nach innen hat sie dafür gesorgt, dass wir uns nach wie vor intensiv und kontinuierlich mit dem Thema IT-Sicherheit auseinandersetzen. Wir haben auf diesem Weg Vieles gelernt, und das hat uns als Organisation nicht nur stärker und resilienter gemacht, sondern das Vertrauen in unsere Dienste gefestigt.

Und ja, die Einführung eines ISMS erfordert einiges an Ressourcen und bringt einen Kulturwandel innerhalb einer Organisation mit sich. Ich weiß, wovon ich rede. Ich möchte jedoch allen Mut machen, sich auf diesen Weg zu begeben, der bei uns im LRZ schon vor langer Zeit begonnen hat. Wer nun resigniert und sagt, solche Kapazitäten und Zeithorizonte sind in meiner kleinen Einrichtung nicht zu leisten, dem sei versichert, auch noch der kleinste Einsatz ist gut angelegt. Es muss nicht gleich das Schloss Neuschwanstein sein. Die solide Berghütte bietet Schutz und ist ein angemessener Schritt in Richtung Prävention und Cybersicherheit.

Entscheidend ist, jetzt loszulegen – und nicht erst morgen.
Ihr Helmut Reiser

Inhalt

Eine Sache der Perspektive
Um Supercomputer RAMSES im Besonderen, Perspektivenwechsel im Allgemeinen und viele weitere Themen ging es im Interview mit Prof. Dr.-Ing. Stefan Wesner

Schritt für Schritt zur Zertifizierung
Mit standardisierten Prozessen die IT-Sicherheit erhöhen – und darüber hinaus Vertrauen schaffen

Ordnung muss sein
Bei der Bereitstellung von IT-Services in großen Organisationen ist ein Organisationsverzeichnis für skalierbare Prozesse essenziell

Sicherheit

Wissenschaftsnetz

International

Forschung

Campus

40 Jahre DFN-Verein
Ein Hoch auf die Gemeinschaft im Wissenschaftsnetz – und den runden Geburtstag des DFN-Vereins

Recht

DFN-Verein

Autorinnen und Autoren dieser Ausgabe im Überblick

1 Maimona Id, DFN-Verein (id@dfn.de); **2** Marcel Nellesen, RWTH Aachen (nellesen@itc.rwth-aachen.de); **3** Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **4** Michel Gerdes, DFN-CERT (gerdes@dfn-cert.de); **0. Abb.** Christine Kahl, DFN-CERT (kahl@dfn.de); **5** Stefan Metzger, Leibniz-Rechenzentrum (stefan.metzger@lrz.de); **6** Miran Mizani, Leibniz-Rechenzentrum (miran.mizani@lrz.de); **7** Eda Seval-Munke, Leibniz-Rechenzentrum (eda.seval@lrz.de); **8** Prof. Dr. Helmut Reiser, Leibniz-Rechenzentrum (helmut.reiser@lrz.de); **9** Anne Dubau, BSI (anne.dubau@bsi.bund.de); **10** Dr. Dirk Bei der Kellen, DFN-Verein (beiderkellen@dfn.de); **11** Christian Meyer, DFN-Verein (meyer@dfn.de); **12** Michael Röder, DFN-Verein (roeder@dfn.de); **13** Dr. Jakob Tendel, DFN-Verein (tendel@dfn.de); **0. Abb** Jonathan Decker, Georg-August-Universität Göttingen (jonathan.decker@uni-goettingen.de); Ali Doost Hosseini, Georg-August-Universität Göttingen (ali.doost-hosseini@gwdg.de); Tino Meisel, GWDG (tino.meisel@gwdg.de); Martin Skowronek, GWDG (martin.skowronek@gwdg.de); **14** Nikolaj Kopp, GWDG (nikolaj.kopp@gwdg.de); **15** Johannes Weiß, GWDG (johannes.weiss@gwdg.de); **16** Elis Bertazzon, GARR (elis.bertazzon@garr.it); **17** Eric Gedenk, DFN-Verein (info@impact-scicomm.com); **18** Thomas Eifert, RWTH Aachen (eifert@itc.rwth-aachen.de); **19** Thorsten Kurth, RWTH Aachen (kurth@itc.rwth-aachen.de); **20** Jan Quaing, Deutsche Bundesstiftung Umwelt (j.quaing@dbu.de); **21** Nikolaus von Bernuth, Forschungsstelle Recht im DFN (n.von.bernuth@fu-berlin.de); **22** Philipp Schöbel, Forschungsstelle Recht im DFN (philipp.schoebel@fu-berlin.de)

Eine Sache der Perspektive

Seit Dezember 2023 ist Prof. Dr.-Ing. Stefan Wesner Vorstandsvorsitzender des DFN-Vereins. Als Wissenschaftler, Lehrender und Leiter des IT Center University of Cologne (ITCC) schaut er aus unterschiedlichen Blickwinkeln auf seine Arbeit, aktuelle Herausforderungen und den DFN-Verein. Der Perspektivenwechsel hilft ihm dabei, Situationen zu analysieren, Bedarfe zu erkennen und neue Lösungsansätze zu finden.

Rechnet mit RAMSES: Prof. Dr.-Ing. Stefan Wesner ist mit seinem Team am ITCC für den Betrieb und die Anpassung des neuen High-Performance-Computing-Clusters an der Universität zu Köln verantwortlich | *Alle Fotos: Jürgen ALOIsius Morgenroth*

Im Juli 2022 wurden Sie auf die W3-Professur für Parallele und Verteilte Systeme an der Universität zu Köln (UzK) berufen und übernahmen die Leitung des Regionalen Rechenzentrums (RRZK). Was war Ihre erste Herausforderung?

Eine meiner ersten Aufgaben bestand darin, die bisher verteilten Einheiten des Regionalen Rechenzentrums mit der Stabsstelle Informationstechnologie der Universitätsverwaltung zusammenzuführen und damit die IT-Kräfte der UzK stärker zu bündeln. Mit dem neuen Namen „IT Center University of Cologne (ITCC)“ wollten wir bewusst die IT-Services in den Vordergrund stellen, denn die Bezeichnung Rechenzentrum impliziert eher, dass Rechner, also die Hardware, im Mittelpunkt stehen.

Mit Blick auf die vielen Cyberangriffe, von denen zahlreiche Hochschulen in Deutschland bisher betroffen waren, war bei der Umstrukturierung das Thema IT-Sicherheit eine der Prioritäten – das hieß, die Security Operations zügig aufzubauen und die dafür notwendigen Strukturen zu schaffen. Meine Forderung, diesen Bereich dringend zusätzlich personell zu verstärken, wurde auch von der Hochschulleitung uneingeschränkt unterstützt. Wir haben außerdem eine campusweite Schwachstellenanalyse und eine Multi-Faktor-Authentifizierung eingeführt. Neben unseren eigenen Aktivitäten hilft uns das Dienstangebot von DFN-Security beispielsweise mit Meldungen oder Hinweisen zu erkannten Schwachstellen. Wir planen, künftig auch die erweiterten DFN-Sicherheitsleistungen in Anspruch zu nehmen.

Das hört sich nach umfassenden Änderungen an. Wie schwierig ist eine Umstrukturierung?

Dinge inhaltlich neu aufzustellen und Veränderungsprozesse anzustoßen, ist ein spannender Auftrag. Dafür bin ich nach Köln gekommen. Aber es ist auch eine Herausforderung. Bei solchen Umstrukturierungen greifen wir massiv in das Arbeitsfeld der Beschäftigten ein. Da geht es um die Zusammenführung doppelter Arbeitsbereiche, Abteilungen bekommen eine neue Ausrichtung. Das sorgt natürlich für Unsicherheiten. Diese Art von Change-Prozessen muss gut durchdacht und kommuniziert werden.

In meiner beruflichen Laufbahn habe ich schon große Infrastruktureinrichtungen leiten dürfen. Gelernt habe ich dabei, dass es bei Veränderungen oder Konflikten das Wichtigste ist, auch die Perspektive des Gegenübers einzunehmen und zu verstehen. Die verschiedenen Rollen, die ich als Wissenschaftler, Lehrender

> „Nach rund zwei Jahren der Umstrukturierung sind wir nun auf der Zielgeraden.“

und Leiter einer Dienstleistungseinrichtung einnehme, helfen mir bei diesem Perspektivenwechsel. Im Grunde genommen müsste Kommunikation in allen Fachbereichen ein Teil der Ausbildung sein. Man eignet sich im Laufe der Jahre schon die eine oder andere Fähigkeit an, aber ich lerne immer wieder, dass man es noch besser machen kann.

Nach rund zwei Jahren der Umstrukturierung sind wir nun auf der Zielgeraden. Wir haben kürzlich eine neue Governance-Struktur verabschiedet: Zukünftig wird es ein CIO-Board geben. Und dann wird die neue Benennung ITCC auch formal eingeführt.

Zusätzliches Personal war Teil Ihrer Strategie. Wie haben Sie es geschafft, Leute im Bereich Cybersecurity zu rekrutieren?

Expertinnen oder Experten für IT-Sicherheit zu finden, ist eine echte Herausforderung, insbesondere mit den Gehaltsstrukturen, die wir im öffentlichen Dienst haben. Wir sind den, glaube ich, fortschrittlichen Weg gegangen, eigene Mitarbeitende zu fördern und für die neuen Aufgaben auszubilden. Es war gut, dass wir bereits Leute an Bord hatten, die sich ohnehin mit dem Thema Cybersecurity beschäftigt hatten. In bestehendes Personal zu investieren und dieses weiterzuentwickeln, setzt meiner Meinung nach noch einmal ganz andere Motivationskräfte frei. Zusätzlich konnten wir uns noch weiter verstärken.

Waren Sie schon mal von einem Cyberangriff betroffen?

Bisher sind wir von größeren Angriffen verschont geblieben. Unsere Systeme werden täglich angegriffen, nur zum Glück nicht erfolgreich – das glauben wir zumindest. Das Schlimmste wäre, wenn ein Cyberangriff erfolgreich war und die Einrichtung es nicht bemerkt. Ich finde es gut und besonders wichtig, dass mit den betroffenen Hochschulen ein offener und intensiver Austausch stattfindet. So können wir voneinander lernen.

Haben Sie als Verantwortlicher Angst vor dem Krisenfall?

Angst ist ein schlechter Ratgeber. Aber wir müssen mit dem nötigen Respekt agieren. Wir haben es eben nicht mit Amateuren zu tun, sondern mit hochprofessionellen Gegnern, die mittlerweile alarmierend gut organisiert und mit sehr großen Rechenressourcen ausgestattet sind. Aus meiner Sicht ist es wichtig, dass wir mit anderen Einrichtungen gemeinsam am Thema IT-Sicherheit arbeiten und nicht als Einzelkämpfer unterwegs sind. Absolute Sicherheit gibt es nicht, egal, wie sehr wir uns anstrengen. Mit immer fortschrittlicheren Abwehrtechnologien auf dem Stand der Zeit zu bleiben, gehört jetzt zu unserem Alltag. Mit dem Dienst DFN-Security, der kontinuierlich weiterentwickelt wird,

und der Expertise des DFN-CERT sind wir, denke ich, sehr gut gewappnet.

Der neue Supercomputer an der Uni zu Köln trägt das Wort Sicherheit sogar im Namen.

Ein besonderes Angriffsziel sind zunehmend hochsensible Gesundheitsdaten. Unser neuer High-Performance-Computing-Cluster RAMSES – der Name steht für „Research Accelerator for Modeling and Simulation with Enhanced Security" – ist speziell für solche Daten entwickelt worden. Eine Besonderheit von RAMSES ist seine hoch spezialisierte Sicherheitsarchitektur. So gibt es eine durchgehende Verschlüsselung im gesamten Berechnungsprozess. Das ist derzeit bundesweit einzigartig. RAMSES ist vielleicht nicht der größte Rechner, aber mit seiner Systemarchitektur und dem Betriebsmodell sehr stark auf die Bedarfe in den anwendungsnahen Bereichen der Lebenswissenschaften und Medizin maßgeschneidert. Die Analyse klinischer Genomdaten, die bisher nicht zum klassischen Nutzungsfeld von HPC-Systemen gehörte, kann nun auf RAMSES mit höchsten Sicherheitsansprüchen verarbeitet werden. Aber auch andere rechenintensive Großforschungsbereiche der UzK wie Quantenphysik, Astronomie und Mathematik profitieren von RAMSES.

> „Auch andere rechenintensive Großforschungsbereiche der UzK profitieren von RAMSES."

Steht das Cluster nur der Uni zu Köln zur Verfügung?

Nein, selbstverständlich nicht. Unsere Dienste werden bundesweit nachgefragt. Schon mit ihren Exzellenzclustern ist die UzK deutschlandweit in Kooperationen mit anderen Zentren vernetzt. So sind wir beispielsweise auch mit dem Deutschen Humangenom-Phenomarchiv (GHGA) als eines der Konsortien in der Nationalen Forschungsdateninfrastruktur (NFDI) organisiert. Mit unserem HPC-System RAMSES können wir Forschenden, die mit sensiblen Daten arbeiten, nun besondere Möglichkeiten und Bedingungen für Simulation und Machine Learning anbieten. Darüber hinaus planen wir gerade ein Tier-3-System zur Versorgung mehrerer Standorte in NRW und denken natürlich jetzt schon darüber nach, wie das nächste System aussehen soll.

Prof. Dr. Stefan Wesner
Studium der Elektrotechnik und Informationstechnik an der Universität des Saarlandes | 2008 Promotion zum Dr.-Ing. an der Universität Stuttgart | 2013 Berufung zum Professor für Informationssysteme und zum Direktor des Kommunikations- und Informationszentrums an der Universität Ulm | von 2013 bis 2022 wissenschaftlicher Leiter des Landeshochschulnetzes Baden-Württemberg BelWü | von 2019 bis 2022 CIO der Universität Ulm | seit 2020 Mitglied des DFN-Verwaltungsrates | seit 2022 Professor für Parallele und Verteilte Systeme und Direktor des IT Center an der Universität zu Köln | seit Dezember 2023 Vorstandsvorsitzender des DFN-Vereins

Welche Rolle spielt dabei das fast schon inflationär gehypte Thema Künstliche Intelligenz im HPC?

Ob wir wollen oder nicht, die Hersteller optimieren ihre Hardware für KI und nicht mehr für die klassische HPC-Simulation. Geld wird im Moment mit den großen Rechnern verdient, die für KI eingesetzt werden und weniger im HPC-Umfeld. Das heißt, die schnellsten Prozessoren, die schnellsten Grafikkarten orientieren sich nicht mehr an den Simulationsanforderungen, sondern an den KI-Anforderungen. Das müssen wir auf jeden Fall berücksichtigen.

Macht KI die klassische Simulation überflüssig?

Nein, auf keinen Fall. KI-Methoden sind beispielsweise Teil der klassischen Simulationssoftware. Sie führen eine Koexistenz. Das ist kein Entweder-oder. Insbesondere bei der Skalierbarkeit sind die langjährigen Erfahrungen aus dem klassischen HPC wichtige methodische Grundlagen dafür. Ich glaube aber auch, dass KI zur Veränderung von Betriebsmodellen führen wird. Die interaktive Nutzung der Großrechner spielt eine viel größere Rolle als das noch vor ein paar Jahren der Fall war.

Interessant zu sehen ist, dass wir dadurch neue Kundinnen und Kunden bekommen, für die Simulationen nicht so einen hohen Stellenwert haben, die aber durchaus mit Machine Learning etwas anfangen können. Das sind ganz neue Fachdisziplinen, die sich jetzt für die Nutzung von großen Rechensystemen interessieren. Vor allem die Medizin, die bisher auch schon stark im Simulationsbereich engagiert war, hat noch einmal zugelegt, was das Thema KI-Bilderkennung oder Auswertung von Daten angeht.

> „Das Thema Energieeffizienz wird in der IT immer wichtiger."

Bei KI müssen wir differenzieren. Was sich meiner Meinung nach gerade auf dem „Peak of Inflated Expectations" bewegt, ist generative KI. Spannend ist vielmehr, wie wir damit umgehen, dass Dinge generiert werden, die echt aussehen, aber nicht real sind, oder Texte erstellt werden, die sich toll lesen, nur leider mit den Fakten nichts zu tun haben. Es ist schon eine große Herausforderung, mit solch einer Rechenpower und den entsprechenden Algorithmen umzugehen. Momentan arbeiten wir daran, lokale Large Language Models als Open-Source-Modelle bereitzustellen, um auch lokale Inhalte in die Modelle integrieren zu können.

In diesen Bereich investieren Unternehmen eine Menge an Rechenressourcen, bei denen man schon staunen kann. Ich frage mich da schon, wie das durch Einnahmen refinanziert werden soll. Damit KI nachhaltig in der Breite genutzt werden kann, muss der Energiefußabdruck deutlich reduziert werden. Im täglichen Einsatz ist KI aber definitiv angekommen.

Welche Rolle spielt die Energieeffizienz beim Betrieb eines Supercomputers?

Die Komplexität der benötigten Infrastruktur hat in den vergangenen Jahren extrem zugenommen. Das Thema Energieeffizienz wird allgemein in der IT immer wichtiger und ist beim Betrieb eines Großrechners noch einmal eine größere Herausforderung, was beispielsweise eine hocheffiziente Kühlung angeht. Die Qualität der Infrastruktur entscheidet zunehmend, ob ein System überhaupt aufgestellt werden kann.

Unsere Serverhalle ist zwar relativ neu, aber im Moment arbeiten wir daran, die Energieeffizienz weiter zu optimieren. Früher konnte man eine Infrastruktur in diesem Leistungsbereich über ein paar Jahre stabil betreiben. Diese Zeiten sind vorbei.

Wir müssen in diesem Zusammenhang außerdem über die Regionalisierung von Diensten sprechen. Ich bin der festen Überzeugung, dass wir als Rechenzentrum künftig überlegen müssen, in welchen Bereichen wir uns mit anderen zusammentun. Nicht jedes Rechenzentrum muss oder kann alle Dienste anbieten. Die Regionalisierung von IT-Services ist dann besonders gut, wenn die Nutzenden gar nicht merken, welche Dienste von der eigenen oder einer anderen Hochschule angeboten werden. Das setzt natürlich voraus, dass die Konnektivität bei allen Einrichtungen gleich gut ist. Und hier kommt der DFN-Verein ins Spiel, der mit dem Wissenschaftsnetz X-WiN den Großteil der Hochschulen und außeruniversitären Forschungseinrichtungen in Deutschland verbindet – und darüber hinaus mit Einrichtungen in der ganzen Welt.

Was haben Sie sich vorgenommen als Vorstandsvorsitzender des DFN-Vereins?

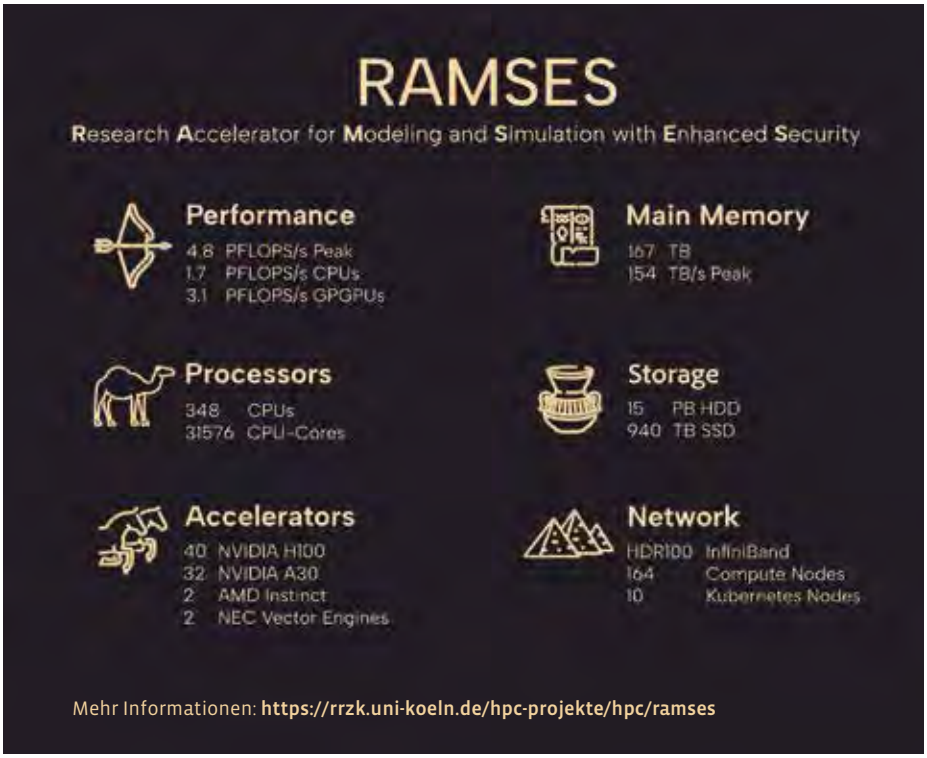
Ich kenne den DFN-Verein seit Langem, sei es aus der Sicht eines Mitgliedsvertreters oder aus dem Verwaltungsrat. Ich betrachte den DFN-Verein als Rechenzentrumsleiter, als „Kunde“ und gleichzeitig auch als Provider. Als Rechenzentrumsleiter tut man übrigens gut daran, auch mal die Kundensicht einzunehmen. Wir haben ja bereits über Perspektivenwechsel gesprochen.

> „Wir müssen sicherstellen, dass wir auch in Zukunft relevante Dienste anbieten.“

Ich glaube, dass es eine ziemlich hohe Zufriedenheit mit den Diensten des DFN-Vereins gibt. Unser Ziel ist es, diese Zufriedenheit zu bewahren. Wir müssen sicherstellen, dass wir auch in Zukunft relevante Dienste anbieten, die die teilnehmenden Einrichtungen mühelos nutzen können. Wenn alles so reibungslos läuft, dass Leute es für selbstverständlich halten, dann haben wir als Service-Dienstleister einen sehr guten Job gemacht.

Welche Themen sehen Sie derzeit im Fokus?

Beim Thema DFN-Security gibt es aktuell die spannendsten Entwicklungen – und auch strategische Fragestellungen. Wir haben eine sehr heterogene Teilnehmerschaft. Was die beiden Dienstmerkmale Basisleistungen und erweiterte Leistungen angeht, gibt es unterschiedliche Erwartungshaltungen an den Verein, aber auch verschiedene Möglichkeiten der Partizipation. Um Letztere effizient nutzen zu können, sind eine gewisse Mitarbeit und Reife des Informationssicherheitsmanagements aufseiten der teilnehmenden Einrichtungen notwendig. Darum müssen wir hier genau hinschauen, ob die Leistungen den richtigen Zuschnitt für alle haben. Aus diesem Grund haben wir einige Einrichtungen gebeten, das gemeinsam mit uns intensiver zu untersuchen.



Feedback einzuholen, ist überhaupt ein wichtiges Thema. Aufgrund der Differenzierung der Rollen, die an manchen Universitäten stattfindet, sollten wir zusammen mit unseren Mitgliedsvertretenden möglicherweise weitere Kommunikationskanäle identifizieren. Die Frage lautet, wie schaffen wir es, unser Diensteportfolio noch besser in die Einrichtungen hineinzutragen?

Zum Schluss: Welcher Bereich Ihrer Tätigkeit gefällt Ihnen am besten? Forschung, Lehre oder der Rechenzentrumsbetrieb?

Das ist eine unfaire Frage. Die Kombination macht es aus. Was mir gut gefällt, ist die Freiheit, die ich in der Forschung habe. Nicht alles muss direkt zum Erfolg führen. Es wird einem nicht permanent das „Return of Investment“ vorgerechnet. Ein Fehlschlag ist eher Erkenntnisgewinn als Versagen. Auf der anderen Seite macht es unfassbar Spaß, in der Forschung etwas zu schaffen, was später für Menschen einen Mehrwert hat. Als IT-Dienstleister wiederum kann ich im Hintergrund anderen helfen – beispielsweise beim Betrieb von RAMSES –, ihre Forschung auf ein neues Level zu bringen. Das muss man mögen, und das muss einem wichtig sein.

Das Gespräch führte Maimona Id (DFN-Verein)

Er wächst und gedeiht – der NFDI-Basisdienst IAM4NFDI

Nachdem der NFDI-Basisdienst Identity & Access Management (IAM4NFDI) Anfang des Jahres die Integrationsphase erreicht hat, lohnt sich ein Blick auf die aktuellen Entwicklungen. Ein guter Indikator für den Fortschritt sind die Inkubator-Projekte.

Text: **Marcel Nellesen** (RWTH Aachen), **Wolfgang Pempe** (DFN-Verein)

Foto: neirfy/Adobe Stock

Im Rahmen der Nationalen Forschungsdateninfrastruktur (NFDI) werden aktuell 26 Fachkonsortien gefördert, die jeweils eine oder mehrere Forschungs-Communitys repräsentieren. Das Projekt IAM4NFDI zielt auf die Implementierung technischer und organisatorischer Lösungen ab, die ein dezentrales und föderiertes Identitätsmanagement für einen Community-gesteuerten, einheitlichen und sicheren Zugriff auf digitale Ressourcen ermöglichen. Durch die Integration in die DFN-AAI können nicht nur die etwa 400 an der DFN-AAI teilnehmenden Heimateinrichtungen partizipieren, sondern über eduGAIN potenziell auch Nutzende aus weiteren rund 5700 Hochschulen und Forschungseinrichtungen weltweit.

Was bisher geschah – IAM4NFDI und das Konzept der NFDI-AAI

Wie alle im Rahmen des NFDI-Basisdienste-Konsortiums Base4NFDI geförderten Projekte durchläuft auch IAM4NFDI drei Projektphasen, die jeweils einzeln beantragt werden müssen: Initialisierung, Integration und Ramping up for operation. Aktuell befindet sich das Projekt in der Integrations-

phase, die von Februar 2024 bis einschließlich Januar 2026 dauert.

Ziel des Projekts ist es, Forschenden im Rahmen einer NFDI-AAI den sicheren Zugang sowohl zu Community-spezifischen als auch zu Community-übergreifenden Ressourcen bzw. Diensten zu ermöglichen. Eine zentrale Rolle hierbei spielt das Konzept der „Community-AAI“. Eine Community-AAI dient insbesondere der Anbindung fachspezifischer Ressourcen und ermöglicht es der jeweiligen Community, ihr eigenes Rechte- und Rollenmanagement für den Zugriff auf diese Ressourcen zu realisieren. Die Anbindung an die DFN-AAI – und damit auch an eduGAIN – erfolgt jeweils über eine Serviceprovider-Proxy-Komponente der jeweiligen Community-AAI-Implementierung. Dienste, die fachübergreifend genutzt werden sollen, werden über einen Infrastruktur-Proxy („Infra Proxy“) integriert (Abb. 1).

Im Rahmen des Basisdienstes IAM werden vier Open-Source-Implementierungen zur Umsetzung einer Community-AAI (CAAI) unterstützt, für die ein langfristiger Support seitens der zuständigen Projektpartner gewährleistet ist. Zum Dienstportfolio gehört daher insbesondere das Hosting besagter Lösungen: Community-AAI-as-a-Service, (CAAIaaS).

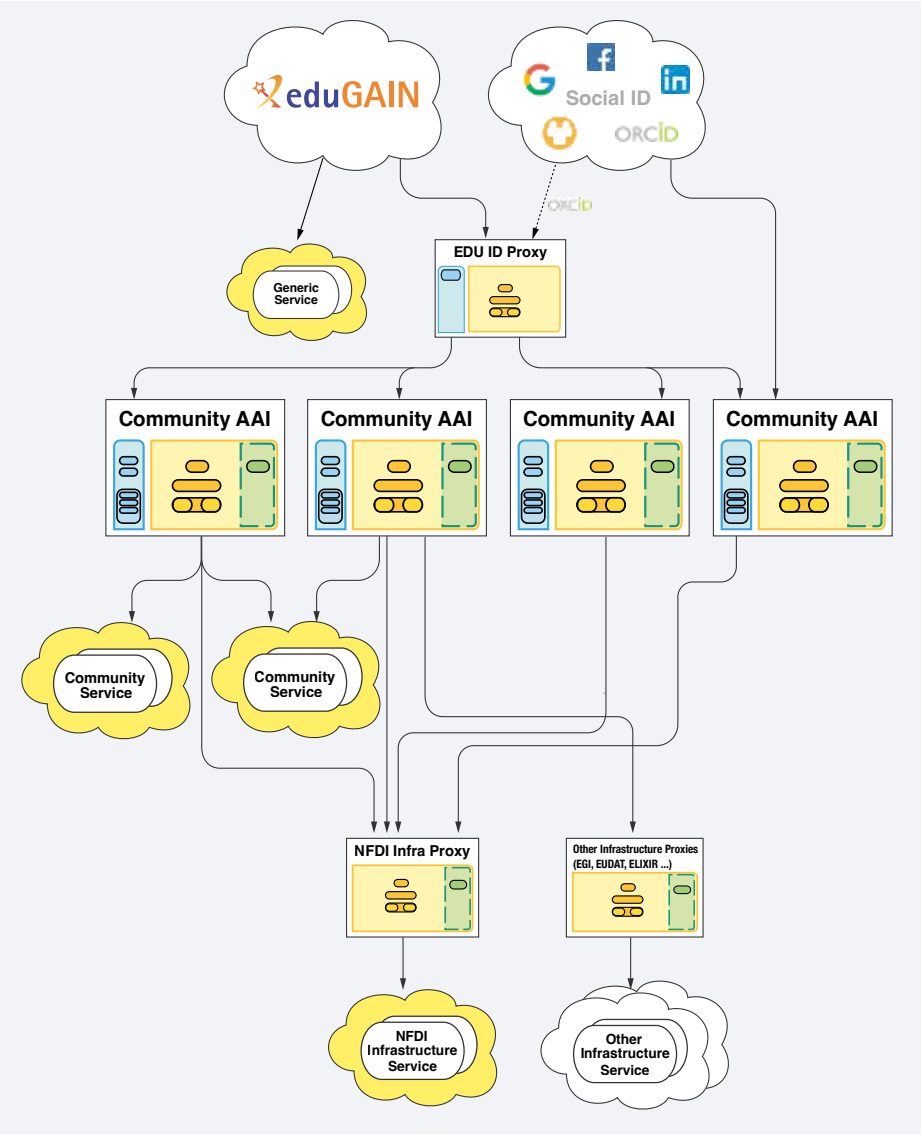


Abbildung 1: Architektur der NFDI-AAI

Das Inkubator-Konzept

Um die Fachkonsortien bestmöglich dabei zu unterstützen, ihre jeweiligen Anwendungsfälle in das Community-AAI-Konzept zu integrieren, bietet das IAM4NFDI-Projektteam hierfür unterstützende und begleitende Maßnahmen an. Als Rahmen dient das Modell des Inkubators, das sich bereits in den GÉANT-Projekten bewährt hat. Hierbei handelt es sich um kleine Projekte, die von Forschenden aus den Fachkonsortien beantragt und im Rahmen von sechs Monate dauernden Zyklen abgearbeitet und dokumentiert werden.

Ein Inkubator-Projekt erlaubt Servicebetreibenden innerhalb der NFDI-Konsortien einen direkten und einfachen Austausch mit den Betreibenden sowie Entwicklerinnen und Entwicklern der jeweiligen Community-AAI-Lösung. Die Antragstellenden haben die Möglichkeit, eigene Ideen einzubringen und Unterstützung in Form von Mentoring, Ressourcen oder Netzwerken zu erhalten. Das Ziel ist, die Antragstellenden bei nicht trivialen Anwendungsfällen zu unterstützen und eine erfolgreiche Anbindung der Services des jeweiligen NFDI-Konsortiums vorzunehmen. Vorteil: Weitere Services können den Communitys nachfolgend unkompliziert zur Verfügung gestellt werden.

Umsetzung im Rahmen von IAM4NFDI

Im Rahmen der Integrationsphase des Projekts IAM4NFDI sind vier Inkubator-Projektzyklen geplant. Dabei ist jeder dieser Zyklen auf eine Dauer von sechs Monaten angelegt. Der allgemeine Ablauf ist in Abb. 2 exemplarisch dargestellt.

Zwei Monate vor Beginn des jeweils nachfolgenden Zyklus wird ein „Call for Incubator Projects“ gestartet. Interessierte Servicebetreibende können sich mithilfe eines Templates bewerben, das neben technischen und organisatorischen Kontaktdaten eine

Beschreibung des Inkubator-Projekts inklusive der adressierten Herausforderungen enthalten soll. Während des Calls werden zusätzliche Workshops angeboten, in denen noch einmal das generelle Konzept einer CAAI sowie die zugrunde liegende Architektur vorgestellt werden. Diese beinhalten eine kurze Präsentation der verschiedenen AAI-Lösungen und bieten interessierten Antragstellenden die Möglichkeit, Fragen zu stellen, um die für sie geeignete Lösung zu identifizieren.

Einen Überblick über die abgeschlossenen und laufenden Inkubator-Projekte finden Sie unter: **https://incubators.nfdi-aai.de**.

Ausführliche Informationen zum Projekt finden Sie auf der Projekt-Homepage unter **https://doc.nfdi-aai.de** sowie in Ausgabe 103 der DFN-Mitteilungen auf Seite 40: **https://dfn.de/wp-content/uploads/2024/01/DFN-Mitteilungen-103.pdf**

Der NFDI-Basisdienst IAM4NFDI wird von der DFG im Rahmen des Projekts „Base4NFDI – Basisdienste für die NFDI“ mit Projektnummer 521453681 gefördert.

Nach Ende der Frist prüft das Projektteam alle eingegangenen Projektanträge. Es klärt offene Fragen und notiert die Herausforderungen. Dies dient als Vorbereitung für ein großes offenes Meeting, bei dem alle Antragstellenden ihre Projekte vorstellen. Anschließend hat das Projektteam die Möglichkeit, letzte Fragen zu erörtern, um die Aufgaben und Herausforderungen besser abschätzen zu können. Die Entscheidung, welche Projekte IAM4NFDI unterstützen wird, trifft das Team im Anschluss gemeinsam mit Expertinnen und Experten von BASE4NFDI. Kriterien können beispielsweise die Komplexität des Projektes, die Kapazitäten der AAI-Lösungen und die den Antragstellenden zur Verfügung stehenden Ressourcen sein.

Nachdem ein Projektantrag akzeptiert wurde, beginnt die eigentliche Arbeit: In einem ersten Treffen werden gemeinsam mit den Antragstellenden Arbeitspakete identifiziert und ein Zeitplan für die Umsetzung erstellt. Dabei werden die Arbeitspakete auf verschiedene Sprints von jeweils etwa einem Monat aufgeteilt. Hierbei ist ein kontinuierlicher Austausch zwischen den Projektteilnehmenden wichtig. Neben dem projektinternen Austausch gibt es außerdem noch regelmäßige Meetings, in denen alle geförderten Projekte ihren aktuellen Arbeitsstand vorstellen.

Ausblick

In der Integrationsphase gilt es, den Basisdienst IAM im Laufe der hierfür vorgesehenen zwei Jahre innerhalb der gesamten NFDI auszurollen. Die Anzahl und die Diversität der Inkubator-Projekte können in diesem Zusammenhang als Indikator für die Integrationstiefe des Basisdienstes betrachtet werden. Sowohl im ersten als auch im kürzlich gestarteten zweiten Zyklus wurden die Inkubator-Projekte sehr positiv angenommen. Dadurch konnten mittlerweile aus der Mehrheit der NFDI-Konsortien Projekte unterstützt und umgesetzt werden. Aktuell befindet sich der Basisdienst Identity & Access Management auf einem guten Weg. ◆

2. INKUBATOR-ZYKLUS

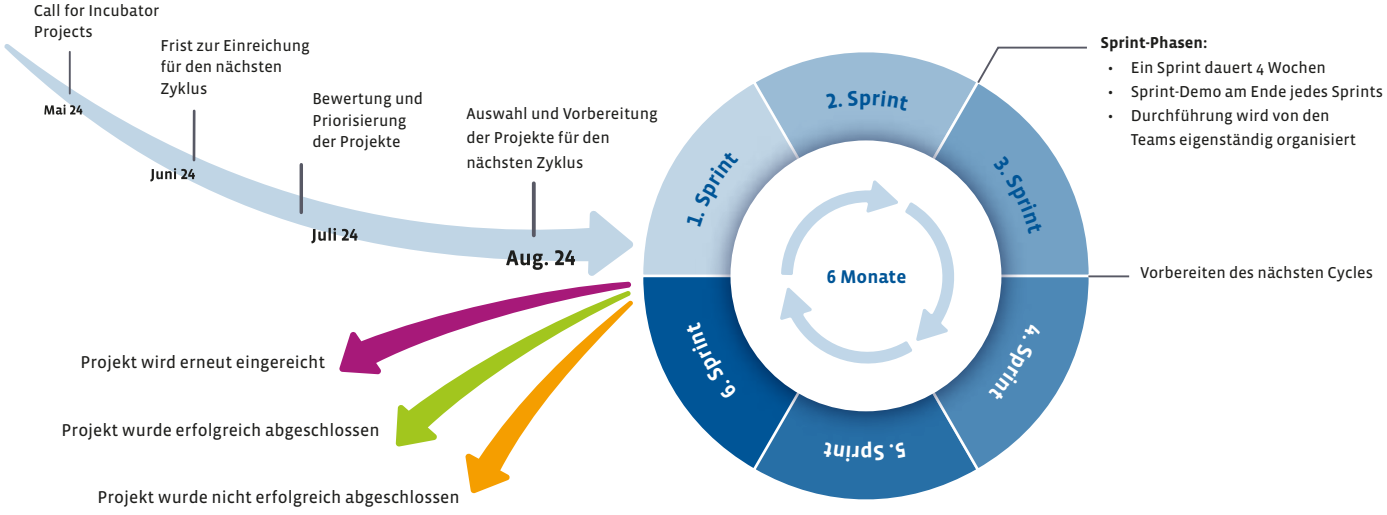


Abbildung 2: Agile Projektentwicklung – im Rahmen der einzelnen Sprints werden die Inkubator-Projekte umgesetzt. Sie unterstützen die Fachkonsortien dabei, ihre Anwendungsfälle in das Community-AAI-Konzept zu integrieren.

Reif für das Security Bootcamp?

In Forschung und Lehre stehen Organisationen in der Pflicht, die Reife der eigenen Informationssicherheit regelmäßig auf den Prüfstand zu stellen und bei Bedarf zu verbessern – zum Schutz der eigenen Institution sowie derjenigen, mit denen Daten und Dienste geteilt werden. Mit dem Security Bootcamp bietet das europäische Verbindungsnetz GÉANT nun ein Hands-on-Training für Informationssicherheitsmanagement (ISM) an.

Text: **Michel Gerdes** (DFN-CERT)

Die Stärke der nationalen Forschungsnetze (NRENs, National Research and Education Networks) beruht auf der weltweiten, zuverlässigen Vernetzung von Forschung und Lehre. Die NRENs stellen die Infrastruktur zur Verfügung, in der beteiligte Institutionen Daten und Dienstleistungen untereinander teilen können. Ein entscheidender Faktor ist dabei Vertrauen: Vertrauen darin, dass die Partnerinstitutionen über einen validen Ansatz für Informationssicherheit verfügen und dadurch das Risiko eines Sicherheitsvorfalls für die eigene Institution minimiert werden kann.

Insbesondere kleine Forschungsnetze und Organisationen stehen oft vor der Frage, wie sie ein Informationssicherheitsmanagement (ISM) aufbauen sollen bzw. wie sie die vorhandenen, meist technischen Sicherheitsmaßnahmen in ein strukturiertes Managementsystem integrieren können. Seit März dieses Jahres bietet das europäische Verbindungsnetz GÉANT darum mit dem Security Bootcamp ein neues Trainingsformat an, das sich genau dieser Frage widmet. Das erste Security Bootcamp fand im Rahmen des EU-Projekts EaPConnect (Eastern Partnership) mit den nationalen Forschungsnetzen RENAM (Moldau), GRENA (Georgien), AzScienceNet (Aserbaidschan) und ASNET-AM (Armenien) und URAN (Ukraine) statt. Bei der TNC24 nahmen die Chief Executive Officers (CEOs) beziehungsweise die GÉANT-Mitgliedsvertretenden der NRENs an einem Mini-Bootcamp teil.

Foto: benzoix/Freepik

Leichtgewichtig und einfach umzusetzen: die GÉANT Security Baseline

Viele Organisationen fokussieren sich auf die Implementierung von technischen Sicherheitsmaßnahmen wie Firewalls oder Intrusion-Detection-Systeme, aber der organisatorische Aspekt wird oft nicht ausreichend beachtet. Aber nur mit einem Konzept, das auf Strategien, Richtlinien, Prozessen, Verantwortlichkeiten und Arbeitsanweisungen basiert, kann die Informationssicherheit ganzheitlich umgesetzt werden. Die Dokumentation aller Maßnahmen ist ein entscheidender Punkt. Es genügt nicht, das Konzept im Kopf zu haben, sondern es muss implementiert, dokumentiert und vor allem gelebt werden. Nur dann entsteht ein nachweislich belastbares ISM. Genau hier setzt das Security Bootcamp an.

Bei den Hands-on-Workshops kommt die GÉANT Security Baseline als gemeinsame Grundlage zum Einsatz. Der Leitfaden wurde im Rahmen des GN4-3-Projekts speziell für NRENs entworfen und in den Folgeprojekten weiterentwickelt. Er unterstützt sie dabei, Schlüsselaspekte von Sicherheitspraktiken zu verstehen und anzuwenden. Die Security Baseline definiert Anforderungen der F&E-spezifischen Herausforderungen auf modulare Weise, wobei jedes Modul ein organisatorisches Thema wie Risiko- oder Lieferantenmanagement abdeckt. Auf diese Art können NRENs ein ISM aufstellen, das so flexibel wie möglich ist, dessen Aspekte und Niveau aber mit denen anderer NRENs vergleichbar sind. Ein Ziel der Security Bootcamps ist, die breite Anwendung der Security Baseline in der Community als Framework für die Strukturierung des ISM zu etablieren. Darüber hinaus bringt der Leitfaden ein einheitliches Bewertungsschema für den Ist-Zustand der Informationssicherheit mit. Dieses liefert den Verantwortlichen bei GÉANT wichtige Indizien, um weitere Dienste im Bereich Security zu gestalten und Schwerpunkte bei Veranstaltungen und Trainings zu setzen. Im Vergleich zu anderen Cyber-Security-Frameworks ist die Baseline leichtgewichtig und einfach umzusetzen.

Hilfe zur Selbsthilfe

Das Konzept des Security Bootcamps sieht drei Module vor: In der Vorbereitungsphase, die ausschließlich online stattfindet, erarbeiten die Teilnehmenden zunächst getrennt voneinander in zwei Sitzungen die Ziele sowie den aktuellen Stand der Informationssicherheit ihrer eigenen Organisation. Die Ergebnisse werden im zweiten Meeting in einem Assessment mit der Security Baseline abgeglichen.

Der Erfolg des Trainings im Security Bootcamp basiert letztendlich auf vertrauensvoller Zusammenarbeit. Zwischenmenschliches Vertrauen kann nicht technisch oder mathematisch hergestellt werden, sondern nur in persönlichem Kontakt. Darum findet die zweite Phase des Trainings ausschließlich in Präsenz und in kleinen Gruppen statt. So kann individuell auf die Teilnehmenden sowie auf die Bedarfe jeder einzelnen Organisation adäquat eingegangen werden. Erst die persönliche Interaktion schafft eine Vertrauensbasis, auf deren Grundlage sich die Teilnehmenden im geschützten Rahmen

> Das Bootcamp ist auch ein Startpunkt für Community Building.

auch über Probleme in der eigenen Organisation austauschen, offen Fragen stellen und Lösungsansätze diskutieren können. Denn häufig stehen diese vor ähnlichen Herausforderungen. Das Bootcamp ist somit auch ein Startpunkt für Community-Building. Insbesondere große und im Bereich der Informationssicherheit bereits reife Organisationen profitieren vom Community-Effekt und können voneinander lernen, wertvolles Feedback erhalten und sich mit ihren schon bewährten Lösungswegen einbringen.

Für das Präsenztraining werden Organisationen gematcht, die entweder vor verwandten Problemen stehen, regional nahe beieinander liegen oder eine ähnliche Größe und Reife im ISM haben. Die praktischen Aufgaben beinhalten die Arbeit an einer fiktiven Organisation sowie die Implementierung eines ISM für die eigene Organisation.

Weitere Informationen zum Security Bootcamp und zur GÉANT Security Baseline finden Sie unter: **https://security.geant.org/security-bootcamp | https://security.geant.org/baseline | https://connect.geant.org/2024/07/24/geant-security-bootcamps-strengthening-cybersecurity-for-re**

Darüber hinaus wird in den theoretischen Einheiten ein Basiswissen hinsichtlich ISM hergestellt.

Da thematisch sehr stark auf Leitungsebene und Steuerung der Informationssicherheit gearbeitet wird, richtet sich das Bootcamp primär an die oberste Leitungsebene wie Chief Executive Officer (CEO) oder Chief Information Security Officer (CISO). Denn diese sind dafür verantwortlich, die Konzepte und Richtlinien in einer Organisation umzusetzen. Die Agenda jedes Bootcamps baut auf den Erkenntnissen des Vorbereitungsmoduls auf. Die Inhalte sind damit sehr stark auf die Bedarfe der teilnehmenden Organisationen zugeschnitten. So ist beispielsweise neben Informationssicherheit auch der Aufbau eines Datenschutzmanagements ein von den NRENs aktiv nachgefragtes Thema. Das Training berücksichtigt, ob die Organisationen der DSGVO oder einer anderen Datenschutzgesetzgebung unterliegen und orientiert sich dann an deren Grundprinzipien.

In der Nachbereitungsphase arbeiten die Teilnehmenden in ihren Einrichtungen eigenständig an der Umsetzung der Informationssicherheit. Die Trainerinnen und Trainer des Bootcamps stehen dabei für Beratungen zur Verfügung. Bei Bedarf werden bis zu zwei Videokonferenzen angesetzt, um den Fortschritt der Organisation bei der Verbesserung ihrer Informationssicherheit zu unterstützen und weitere Fragen zu klären. Die Nachbereitungstermine finden in der Regel drei und sechs Monate nach dem Präsenzmodul statt.

Fazit: Hilfe zur Selbsthilfe lautet die Maxime im Security Bootcamp. Mit dem maßgeschneiderten Training bietet GÉANT NRENs oder Organisationen die Möglichkeit, ihr ISM zu verbessern, sich in puncto Cybersicherheit mit anderen Organisationen zu vernetzen und von deren Erfahrungen zu profitieren. Dieses Jahr finden weitere Security Bootcamps statt: für die regionalen Forschungsnetze UbuntuNet Alliance in Tansania und RedCLARA in Brasilien. ◆

Gemeinsam stark – die DNS-RPZ Community Edition

Die neue Community-Zone, ein Bestandteil des Dienstmerkmals DNS-RPZ, sorgt dafür, dass Erkenntnisse zu Phishingkampagnen geteilt werden und damit allen am Dienst DFN-Security teilnehmenden Einrichtungen zur Verfügung stehen. Neben dem Know-how setzt das Verfahren auf das Verantwortungsbewusstsein der DFN-Teilnehmer – das ermöglicht letztendlich die erforderliche Schnelligkeit und Flexibilität im Prozess.

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

Foto: wildpixel/iStock

Gemeinsam für Sicherheit sorgen – das ist das Prinzip der neuen Community-Zone, die Mitte September 2024 als Bestandteil der Abwehrkomponente DNS-RPZ (Domain Name System Response Policy Zone) aktiviert wurde. Mit DNS-RPZ, das als wichtiges Leistungsmerkmal des Dienstes DFN-Security Anfang des Jahres in Betrieb gegangen ist, werden bösartige Domains identifiziert und der Zugriff auf diese unterbunden. Die Informationen werden nach bestimmten Richtlinien in Response-Policy-Zonen, zu der auch die Community-Zone zählt, gelistet und Nutzenden des Dienstes bereitgestellt.

Als Ergänzung der bereits verfügbaren Dokumente zu DNS-RPZ beschäftigt sich ein neues Dokument ausschließlich mit der Community-Zone. Außerdem steht das auf der Open-Source-Software BIND basierende Konfigurationsbeispiel in einer überarbeiteten Fassung zur Verfügung.

Alle Dokumente und Konfigurationsbeispiele finden Sie unter:
https://www.dfn-cert.de/leistungen/security-operations/

Einen ausführlichen Bericht zu den Funktionen von DNS-RPZ finden Sie in Ausgabe 104 der DFN-Mitteilungen ab S. 35 unter:
https://www.dfn.de/wp-content/uploads/2024/01/DFN-Mitteilungen-104.pdf

Bei Interesse an oder Fragen zu den Angeboten in DFN-Security können Sie uns gern kontaktieren unter: **dfn-security@dfn.de**

„With great power comes great responsibility“

Das Konzept der Community-Zone beruht darauf, dass die Erkenntnisse der an DNS-RPZ teilnehmenden Einrichtungen geteilt und anderen Einrichtungen zur Absicherung der eigenen Umgebung zur Verfügung gestellt werden. So können Nutzende, die eine Phishingkampagne erkennen, dem DFN-CERT über ein genau geregeltes Prozedere Domains melden, die über die vorhandenen Zonen noch nicht blockiert werden. Anschließend erfolgen eine Syntaxprüfung und ein Abgleich mit einer Liste häufig genutzter Domains (aktuell Cloudflare Top 10 000). Auf eine zeitintensive manuelle Prüfung vor Eintrag der Domain in die Community-Zone wird jedoch verzichtet. An dieser Stelle wird zum einen auf Schnelligkeit und zum anderen auf das Know-how sowie das Verantwortungsbewusstsein der Teilnehmer gesetzt – denn wie schon Marvel wusste: „With great power comes great responsibility“.

Mit dem Eintrag in die Community-Zone ist ein zügiger Schutz gegen eine schädliche Domain möglich. Die Empfehlung ist, den Zugriff auf die Einträge zu blockieren, damit neue Phishingkampagnen schnell gestört werden. Wenn im Falle eines Fehlers eine Domain eingetragen wird, über die keine maliziösen Inhalte verteilt werden, kann allerdings auch einiges Ungemach ausgelöst werden. Darum ist es wie so häufig in diesem Bereich eine Herausforderung, die richtige Balance zu finden zwischen „viele Daten sammeln“ und „besonders gute Daten sammeln“. Für die erste Erprobung der Community-Zone werden deshalb nur Domaindaten von explizit benannten Kontakten einer Einrichtung akzeptiert, die das Dienstmerkmal DNS-RPZ selbst einsetzt. Abhängig von zukünftigen Erfahrungen und Rückmeldungen der Teilnehmer sind hier Anpassungen möglich.

Mit der Aktivierung der Community-Zone wurde auch die Empfehlung zum Umgang geändert: Statt „Logging“ wird jetzt „Blocking“ empfohlen. Außerdem wurde die Zone in der Sortierreihenfolge weiter nach unten gesetzt. Im Zuge dieser Änderungen wurden zusätzliche Anpassungen in der empfohlenen Konfiguration vorgenommen. Um DNS-RPZ zügig von der Pilotphase in den Produktivbetrieb überführen zu können, wurden verschiedene DFN-Zonen zunächst initial angelegt. Die Fertigstellung der erforderlichen Erweiterungen für die Nutzung erfolgte parallel zum produktiven Betrieb. Aufgrund der Erkenntnisse aus diesem Betrieb wurde eine misc-Zone implementiert, die jetzt zusätzlich bezogen werden kann.

DFN-Zonen auf einen Blick

Neben der Community-Zone können teilnehmende Einrichtungen nun weitere sechs DFN-Zonen nutzen: Die DFN-Allow-List (al) umfasst Domains, die stets erreichbar sein und nicht versehentlich durch einen falschen Eintrag blockiert werden sollen. In diese Liste werden automatisch alle im Sicherheitsportal hinterlegten sowie verifizierten Domains eingetragen und entsprechend bei Ablauf einer Verifikation aus dieser wieder entfernt. Zwei DFN-Zonen (eval-f und eval-l) dienen der Evaluierung von neuen Daten, weshalb eine Blockierung hier nicht empfehlenswert ist. Die restlichen Zonen (ph = phishing, mw = malware, misc = sonstiges) beinhalten als maliziös eingestufte Domains, die entsprechend nicht aufgelöst werden sollten.

Fazit

Das Konzept der Community-Zone verdeutlicht einmal mehr, dass es sinnvoll ist, Sicherheit als eine gemeinsame Aufgabe aller teilnehmenden Einrichtungen am Wissenschaftsnetz zu verstehen. Dementsprechend wird die Community-Zone nur dann erfolgreich sein und einen großen Mehrwert entfalten, wenn viele an ihr mitarbeiten. ◆

Schritt für Schritt zur Zertifizierung

Hochschulen und außeruniversitäre Forschungseinrichtungen geraten aufgrund ihrer teils dezentralen Strukturen immer häufiger ins Visier von Cyberkriminellen. Zur Bekämpfung und Prävention von Sicherheitsvorfällen ist es notwendig, rechtzeitig ein solides Fundament für IT-Sicherheit aufzubauen. Welche Schritte dafür erforderlich sind und warum sich der mitunter beschwerliche und lange Weg lohnt, zeigt als Vorreiter das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ).

Text: **Stefan Metzger, Miran Mizani, Eda Seval-Munke, Helmut Reiser** (Leibniz-Rechenzentrum, LRZ)

Foto: Fineblick/Adobe Stock

Als wissenschaftliche Einrichtung ist das Leibniz-Rechenzentrum IT-Service Provider für die Universitäten und Hochschulen in München. Sehr früh, bereits im Jahr 2009, trieb das LRZ den Aufbau eines Service- sowie Informationssicherheitsmanagementsystems (ISMS) in Anlehnung an internationale Standards ISO/IEC 20000 und ISO/IEC 27001 massiv voran. Die Motivation bestand darin, Daten, die in wissenschaftlichen Kooperations- und Forschungsprojekten am LRZ gespeichert und verarbeitet werden, zu schützen und darüber hinaus als vertrauenswürdiger Partner aufzutreten.

Heute, 15 Jahre später, ist das Thema IT-Sicherheit dringlicher als je zuvor. Immer häufiger werden unter anderem Hochschulen und Forschungseinrichtungen Opfer von Cyberangriffen, die bei Erfolg den Betrieb massiv beeinträchtigen und für Kosten in Millionenhöhe sorgen können. Das bestätigt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI). In seinem aktuellen Lagebild schätzt das BSI die Sicherheitslage als „angespannt bis kritisch" ein. Zu den häufigsten Angriffsaktivitäten cyberkrimineller Akteure zählen Ransomware und verteilte Denial-of-Service-Angriffe, aber auch Hacktivism.

Regulatorische Vorschriften wie das IT-Sicherheitsgesetz oder die NIS2-Richtlinie sollen Abhilfe schaffen. Stand heute fällt der Hochschulbereich jedoch nicht zwingend in deren Geltungsbereiche. In Bayern legte deshalb das Staatsministerium für Wissenschaft und Kunst (StMWK) fest, dass jede bayerische Hochschule bis 2027 ein wirksames Informationssicherheitsmanagementsystem aufgebaut haben muss.

Der Weg zur Zertifizierung

Gestartet ist das LRZ mit der Etablierung einer definierten Vorgehensweise zur Behandlung von Sicherheitsvorfällen. Nach und nach kamen weitere Sicherheitsrichtlinien hinzu, die beispielsweise den Umgang mit Passwörtern oder mit Logdaten regelten. Im Laufe der Zeit wurde aber deutlich, dass diese auf Einzelmaßnahmen fokussierte Herangehensweise langfristig nicht zum erhofften Erfolg führen würde, da hierzu die Einbettung in einen organisatorischen und risikobasierten Rahmen fehlte.

Im Jahr 2017 beschloss daher die LRZ-Leitung, ein integriertes Service- (SMS) und Informationssicherheitsmanagementsystem (ISMS) aufzubauen und dieses nach den internationalen Normen ISO/IEC 20000 und ISO/IEC 27001 zertifizieren zu lassen. Folgende übergeordnete Zielsetzungen wurden dabei beachtet:

- Erhöhung der Kundenzufriedenheit durch mehr Professionalität, Transparenz und Kommunikation
- Einhaltung rechtlicher Rahmenbedingungen und Compliance-Anforderungen
- Verbesserung der Informationssicherheit durch festgelegte Prozesse
- Verbesserung des Reifegrades der Organisation
- Erfahrungsaufbau zur Wegbereitung anderer Organisationen im Hochschulumfeld

Im Fokus: Anwenderinnen und Anwender sollen darauf vertrauen können, dass mit ihren am LRZ verarbeiteten Daten sorgsam umgegangen wird und dies auch nachgewiesen werden kann. Aber hätte dann nicht auch eine Orientierung an der ISO-Norm ausgereicht? Nein, denn erst mit einer Zertifizierung kann die Einhaltung von Best-Practice-Sicherheitsvorgaben gegenüber Außenstehenden nachgewiesen werden. Zudem wird eine kontinuierliche Weiterentwicklung des ISMS sichergestellt.

47k – das Einführungsprojekt

Mit einer geplanten Laufzeit von 15 Monaten und dem definierten Ziel der Zertifizierung fiel im Januar 2018 der Startschuss für das Einführungsprojekt „47k". Die Projektbezeichnung ergab sich aus der Addition der zugrunde gelegten Normenreihen ISO/IEC 20k und 27k zu „47k". Als Geltungsbereich des integrierten Managementsystems wurden die vier Betriebsabteilungen des LRZ und damit alle angebotenen IT-Dienste festgelegt.

> Die Einführung eines Managementsystems erfordert einiges an Ressourcen.

Wichtig: Die LRZ-Leitung stand von Anfang an hinter dem Vorhaben. Die Projektleitung erhielt Unterstützung durch einen erfahrenen externen Berater und ein etwa 30-köpfiges Projektteam aus motivierten Kolleginnen und Kollegen aus allen Abteilungen. Die Einführung eines Managementsystems erfordert einiges an Ressourcen und stellt einen organisatorischen Umbruch dar, der nicht nur Prozesse und Technik betrifft, sondern insbesondere auch alle Mitarbeitenden. Erst ein gut austariertes magisches Dreieck aus „People, Process und Technology" ermöglicht ein funktionierendes Managementsystem. Keiner dieser Bereiche darf vernachlässigt werden.

Eine initiale Gap-Analyse zeigte, wo noch Abweichungen zu den Normvorgaben bestanden. Aus den identifizierten Defiziten wurden nachfolgend konkrete Maßnahmen abgeleitet. Oberste Prämisse war es, diese so umzusetzen, dass die angestrebte Zertifizierung realisiert werden kann und es gleichzeitig möglich ist, sich an der gelebten betrieblichen Praxis zu orientieren und ausreichend Spielraum für Verbesserungen zu lassen. Zur Veranschaulichung wurden hier die „Holzhütte vs. Schloss Neuschwanstein" gegenübergestellt. Die schlichte Holzhütte unterscheidet sich doch deutlich vom verspielt wirkenden Schloss, welches von Türmen und Erkern geprägt ist. Analog dazu neigen Forschende und Technikleute oft dazu, eine Lösung erst dann als fertig zu akzeptieren, wenn diese 100 Prozent der Anforderungen erfüllt. Zu akzeptieren, dass

zunächst auch 80 Prozent oder sogar weniger ein durchaus gutes und ausreichendes Ergebnis sind, war nicht für alle ganz einfach.

Prof. Dr. Dieter Kranzlmüller
Vorsitzender des Direktoriums des LRZ

Die Zertifizierung war ein Großprojekt, an dem das ganze LRZ, jede Mitarbeiterin und jeder Mitarbeiter beteiligt waren. Es war ein gemeinsamer Kraftakt, der sich aber auf ganzer Linie ausgezahlt hat. Wir haben intern Prozesse und Dokumentationen, die unsere Arbeit unterstützen, und extern ein Qualitätsmerkmal, das für unsere Kunden in der Wissenschaft einen wichtigen Mehrwert darstellt.

Die prozessuale Vorgabe für den ISMS-Kernprozess, das Risikomanagement, war relativ schnell erstellt. Die Anwendung in der Praxis, zumal ohne dediziertes Tool, gestaltete sich jedoch zunächst schwierig. Betriebsrelevante Dokumentationen zu Server- und Netzkomponenten waren vorhanden. Jedoch mangelte es an Aussagen zu dort verarbeiteten und im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit zu schützenden Informationswerten. Diese Informations-„Assets“ wurden daher zunächst eher allgemein, beispielsweise als „Konfigurationsdaten“, erfasst und mit den technischen „Assets“ in Beziehung gesetzt. Nicht nur die physische Netzkomponente, sondern vor allem deren Konfiguration ist vor Offenlegung oder unerlaubten Änderungen zu schützen. Wichtig war, loszulegen und die definierten Verfahren zu testen, inwieweit sie die gewünschten Ergebnisse bereits liefern konnten oder ob sie bei Bedarf nachjustiert werden mussten.

> Das Risikomanagement war relativ schnell erstellt.

Gemeinsam mit der LRZ-Leitung wurden geforderte Richtlinien und Prozessbeschreibungen erstellt, die das Arbeiten am LRZ und den Umgang mit Informationswerten „regelten“ und den Mitarbeitenden Handlungssicherheit gaben (Governance). Daneben wurden Pläne für die interne und externe Kommunikation definiert, ein Schulungs- und Awareness-Programm zum Thema Informationssicherheit aufgebaut und alle Beschäftigten geschult. Ein Kennzahlensystem überprüfte anhand einfacher Ja- oder Nein-Fragen die Normkonformität und gab der Leitung ein hilfreiches Steuerungsinstrument an die Hand.

Ein definierter Prozess regelt bis heute die Lenkung der Vorgabedokumentation, während die Nachweisdokumente (Records) als Freitext oder mit anderen Werkzeugen erfasst werden. Das LRZ nutzt kein dediziertes ISMS-Tool, sondern die allgemein zu Dokumentationszwecken eingesetzte und damit allen Beschäftigten vertraute Software Confluence. Die Erstellung und das Management der Dokumente funktionieren mit dieser nach wie vor sehr gut. In Verbindung mit einem Ticket-Tool und einer selbst entwickelten CMDB (Configuration Management Database) konnte ein dezidiertes ISMS-Tool bislang sehr gut ersetzt werden.

Foto: photoPepp/Adobe Stock

Nach nur knapp einem Jahr Projektlaufzeit waren die Gaps größtenteils geschlossen. Die Vorbereitung auf die angestrebte Zertifizierung konnte damit in Angriff genommen werden. Das vorgeschaltete interne Audit bewertete die erarbeiteten Ergebnisse anhand der Normvorgaben kritisch, größere Defizite fanden sich zum Glück keine mehr. Etwa ein halbes Jahr später, im Juli 2019, wurde die Erstzertifizierung erfolgreich bestanden. Ein sehr schöner Erfolg für das Projektteam und das gesamte LRZ.

Die Aufteilung in themenspezifische Teilprojekte hat sich bewährt. Diese erlaubte, mehrere Themenfelder parallel zu bearbeiten. Das verschaffte der Projektleitung ausreichend Zeit, sich sowohl auf die Koordination des Projekts und die Abstimmung mit

den Fachabteilungen zu konzentrieren als auch sicherzustellen, dass die erarbeiteten Ergebnisse im Einklang mit den festgelegten Anforderungen stehen. Das Hinzuziehen eines erfahrenen Beraters erwies sich ebenfalls als äußerst hilfreich. Ein großes Stück Pragmatismus, Orientierung an bestehenden Abläufen und die Vermeidung unnötigen Beiwerks waren wichtige Schritte zum Erfolg.

Herausforderungen im Betrieb des ISMS

Der Betrieb des Managementsystems endet keinesfalls zum Termin der erfolgreich abgeschlossenen Zertifizierung. Eine kontinuierliche Auseinandersetzung mit diesem, die Verbesserung des Gesamtsystems sowie insbesondere das tagtägliche „Leben" dokumentierter Vorgaben rücken in den Vordergrund.

> Das Hinzuziehen eines erfahrenen Beraters erwies sich ebenfalls als äußerst hilfreich.

Ein Managementsystem versucht Abläufe nicht nur zu strukturieren, sondern auch organisationsweit zu standardisieren. Dienstspezifische Vorgehensweisen, die hiervon abweichen, sind grundsätzlich erlaubt. Am LRZ wurden diese durch Ergänzungen in der Dokumentation abgebildet, infolgedessen litt deren Lesbarkeit und Verständlichkeit. In den jährlichen Reviews wird nun versucht, die Ergänzungen Stück für Stück zu vereinfachen und Richtlinien, Prozesse sowie Verfahren von unnötigem Ballast und aufwendigen Dokumentationspflichten zu befreien.

Häufig wird ein ISMS mit extrem hohem Dokumentationsaufwand verbunden. Aber nicht die Dokumentation, sondern die Umsetzung der Prozesse und Verfahren in der täglichen Praxis und die Integration des ISMS in den betrieblichen Alltag sind das, was zählt. Verlangt wird daher von allen Beteiligten, nur das Notwendigste so ausführlich zu dokumentieren, dass die mit dem ISMS gesteckten Ziele erreicht werden. Statt Dokumentation lediglich als lästige Pflicht zu betrachten, sollte sie als sinnvoll erachtet und nachvollziehbar und zweckdienlich verfasst werden.

Mitarbeitende sehen sich durch das ISMS oft mit Einschränkungen konfrontiert. Dies rührt nicht zwingend aus dem Konzept eines Managementsystems selbst, sondern aus den Regelungen, die eine Organisation erlässt. Für einige zuvor ungeregelte Zustände bzw. Verfahrensweisen, die den Mitarbeitenden viel Freiraum gaben, werden nun explizite Entscheidungen getroffen und so der Wille der Leitung kundgetan. Dies führt oft zu Konflikten aus Präferenz, Gewohnheit oder auch Bequemlichkeit. Eine völlige Freiheit in der Ausgestaltung sicherheitsrelevanter Vorgänge existiert heute nicht mehr. Übliche Beispiele sind die Installation von Software auf dem Arbeitslaptop oder die Nutzung privater Endgeräte für die Erledigung dienstlicher Aufgaben. Eine große Bedeutung kommt hier der Kommunikation und dem Schaffen von Awareness zu. Dabei sollten weniger die Fragen „was" oder „wie" etwas gemacht wird, beantwortet werden, sondern vor allem das „warum" im Mittelpunkt stehen.

Eine weitere und gerade auch im Hochschulumfeld nicht zu vernachlässigende Herausforderung entsteht durch personelle Abgänge und Wechsel sowie damit verbundene Änderungen im Aufgabenspektrum. Das führte am LRZ dazu, dass das ehemals sehr große Projektteam nach und nach schrumpfte. Die Verantwortlichkeiten für die stattliche Anzahl an Richtlinien und Prozessen waren auf einige wenige Schultern zu verteilen, was die Geschwindigkeit der Verbesserung des ISMS und seiner Bestandteile nach und nach bremste. Für das „Leben" des ISMS im Alltag ist es notwendig, dass die Verantwortung hierfür mehr und mehr in die Linienorganisation, also an das zuständige Führungspersonal, übergeht.

Die Pflicht zur kontinuierlichen Verbesserung des Managementsystems birgt die Herausforderung, die gelebte Praxis in Form regelmäßig stattfindender Überwachungsaudits und interner Audits zu überprüfen. Audits werden insbesondere von Mitarbeitenden nicht selten als unnötig und zeitaufwendig erachtet, sind aber durch ihren unabhängigen und objektiven Blick von außen entscheidend dafür, Schwachpunkte im Managementsystem zu identifizieren und ausräumen zu können.

Dr. Oliver Diekamp
Leitung Dezernat Informations- und Kommunikationstechnik der LMU München

Dank der Sicherheitszertifizierung können Forscherinnen und Forscher der LMU, aber auch Drittmittelgeber und andere Partner sich nun auch nachweislich darauf verlassen, dass Daten in der Infrastruktur des LRZ stets nach dem Stand der Technik geschützt werden können. Angesichts der Bedrohung durch Cyberangriffe, aber auch der damit verbundenen zunehmenden Regulierung leistet die Sicherheitszertifizierung des LRZ damit einen wichtigen Beitrag für exzellente Forschungsbedingungen an der LMU.

HOCHSCHULÜBERGREIFENDE IT-SERVICES FÜR INFORMATIONSSICHERHEIT (HITS-IS)

Mit HITS-IS fördert die bayerische Staatsregierung den Aufbau hochschulübergreifender IT-Services für Informationssicherheit. Die Strategie dahinter: Know-how und Dienste im Digitalverbund Bayern zentral aufzubauen und allen Hochschulen in Bayern zur Verfügung zu stellen, um so gezielt Synergien zu schaffen.

Das Angebot umfasst u. a. Unterstützung bei schwerwiegenden IT-Sicherheitsvorfällen und beim Aufbau eines Information Security Management System (ISMS) oder Business Continuity Management (BCM), die Durchführung von Schwachstellenscans, Security-Awareness-Maßnahmen sowie technisches Consulting.

Weitere Informationen finden Sie unter:
https://digitalverbund.bayern/hits/informationssicherheit/

LITERATUR

Aufbau eines Managementsystems – Tools vs. Prozesse, Ausgabe 101:
https://www.dfn.de/wp-content/uploads/2024/01/DFN-Mitteilungen-101.pdf

Praxisbuch ISO/IEC 27001 – Management der Informationssicherheit und Vorbereitung auf die Zertifizierung (Michael Brenner, Nils Gentschen Felde, Wolfgang Hommel, Stefan Metzger, Helmut Reiser, Thomas Schaaf):
Erschienen im Carl Hanser Verlag GmbH & Co. KG

Hat es sich gelohnt?

Nach fünf Jahren Betrieb des integrierten Managementsystems und damit einigen erfolgreichen Voll- und Überwachungsaudits stellt sich die Frage, ob sich der Schritt tatsächlich gelohnt hat.

Von Beginn an wurde der konkrete individuelle Mehrwert für die eigene Arbeit von den Mitarbeitenden kritisch hinterfragt. Für die einzelne Kollegin oder den einzelnen Kollegen kann dieser überschaubar sein, für die Organisation insgesamt ist er jedoch enorm.

Dokumentierte, wiederholbare Prozesse und Verfahren helfen, die eigene Arbeit besser zu strukturieren oder die Arbeitslast teamintern auf mehrere Schultern zu verteilen. Die Behandlung von Sicherheitsvorfällen oder der Umgang mit technischen Schwachstellen erfolgen, wie im ISMS-Kontext genannt, gesteuert. Entscheidungen, etwa eine Schwachstelle zu patchen, werden nicht ad hoc oder nach Bauchgefühl getroffen, sondern nachvollziehbar und nach Abwägen damit verbundener Risiken. Wo früher Einzelmaßnahmen isoliert umgesetzt wurden, existiert nun ein gesamtheitlicher Ansatz, wodurch der Reifegrad der Dienstbringung am LRZ gesteigert werden konnte. Auch die Zufriedenheit der Kunden, die das LRZ jetzt noch stärker als vertrauensvollen Partner und IT-Dienstleister wahrnehmen, erhöhte sich messbar. So genügt in Forschungsprojekten von LRZ-Kunden mit externen Partnern nicht selten der einfache Hinweis auf das bestehende ISO/IEC 27001-Zertifikat oder reduziert zumindest die Anzahl der zu beantwortenden Fragen hinsichtlich umgesetzter Sicherheitsmaßnahmen deutlich. Das ISMS bildet somit ein solides Fundament, auf dem weitergehende Sicherheitsmechanismen, etwa zum Schutz besonders sensibler Daten wie etwa in der Medizin aufbauen.

Es soll aber keinesfalls verschwiegen werden, dass der Aufbau eines ISMS einen organisatorischen Wandel, nicht selten einen Kulturwandel, erfordert. Der Betrieb eines ISMS und die Aufrechterhaltung der Zertifizierung bedeutet täglichen Aufwand, der nicht nur für das zuständige ISMS-Personal, sondern auch in nicht zu unterschätzendem Umfang für die gesamte Belegschaft entsteht. Dieser Aufwand aber lohnt sich! ◆

Vertrauen auf einen Blick – das IT-Sicherheitskennzeichen

Das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene IT-Sicherheitskennzeichen für smarte Produkte und Dienste gibt es nun auch für Videokonferenzdienste. Als erster Anbieter erhielt im Juli 2024 die OpenTalk GmbH die Kennzeichnung für ihre Open-Source-Videokonferenzlösung, gefolgt von Zoom im September. Damit haben sich beide DFN-Conf-Rahmenvertragspartner dazu verpflichtet, die Sicherheitsanforderungen der neuen DIN SPEC 27008 zu erfüllen.

Text: **Anne Dubau** (Bundesamt für Sicherheit in der Informationstechnik, BSI)

Spätestens seit der Coronapandemie sind Videokonferenzen im beruflichen wie auch privaten Alltag etabliert. Oft ist für Nutzerinnen und Nutzer jedoch nicht transparent, welche Sicherheitseigenschaften ihnen von Videokonferenzanbietern versprochen werden. Je mehr vernetzte Geräte und Software auf den Markt kommen und im Einsatz sind, desto schwieriger sind deren Sicherheitseigenschaften zu beurteilen. Für den Einkauf smarter Elektronikprodukte, Mobilgeräte oder Dienste bietet das IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik (BSI) einen wertvollen Kompass.

Foto: Vader Stocker/Freepik

Der Wille zum IT-Sicherheitscheck ist da – die Möglichkeiten auch?

Eine repräsentative Befragung der Verbraucherzentralen (siehe Infokasten S. 25) im Jahr 2023 ergab, dass bei nahezu jedem Dritten mindestens ein persönlicher Onlineaccount schon einmal Ziel eines Hackingangriffs wurde. Gleichzeitig wächst in der Bevölkerung das Bewusstsein für die Cybersicherheit, wie eine in diesem Jahr durch das BSI in Auftrag gegebene Verbraucherumfrage (siehe Infokasten S. 25) belegt: Demnach ist für 76,5 Prozent der Teilnehmenden IT-Sicherheit das zweitwichtigste Kriterium bei der Kaufentscheidung – noch vor dem Preis. Lediglich die Benutzerfreundlichkeit wird höher priorisiert. Drei von vier Befragten sehen es als wichtig bis sehr wichtig an, dass smarte Geräte grundlegende IT-Sicherheitsanforderungen erfüllen. Und zwei von drei Personen wünschen sich ein unabhängiges Kennzeichen, welches über die IT-Sicherheit smarter Geräte informiert.

Diese Zahlen zeigen: Die Cybersicherheit rückt zunehmend in den Fokus von Nutzerinnen und Nutzern. Allerdings hatten diese es in der Vergangenheit schwer, an transparente und verständliche Informationen zur IT-Sicherheit von Produkten zu kommen. Die Vielen bereits bekannte „CE"-Kennzeichnung gibt zwar Auskunft zu physischen Produkteigenschaften, verrät jedoch nichts über die Cybersicherheit. Um diese Informationslücke zu schließen und für mehr Transparenz zu sorgen, vergibt das BSI seit Dezember 2021 das IT-Sicherheitskennzeichen für digitale Produkte und Dienste.

Worauf basiert die Kennzeichnung und wie wird sie vergeben?

Mit dem IT-Sicherheitsgesetz 2.0 hat das BSI im Jahr 2021 den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen einzuführen. Dieses basiert je nach Produktkategorie auf unterschiedlichen, vom BSI entwickelten oder anerkannten Standards. Für die Produktkategorie „Videokonferenzdienste" hat das BSI von der Branche entwickelte IT-Sicherheitsvorgaben anerkannt. Um das Kennzeichen zu erhalten, prüfen Hersteller und Anbieter zunächst selbst oder mit Unterstützung einer Konformitätsbewertungsstelle, ob ihr Produkt oder Dienst die Sicherheitsanforderungen des BSI erfüllt. Dazu gehört auch die Verpflichtung, Schwachstellen an das BSI zu melden, diese unverzüglich zu schließen und das Produkt während der gesamten Laufzeit des Kennzeichens mit Sicherheitsupdates zu versorgen. Nach der positiven Eigenprüfung kann das IT-Sicherheitskennzeichen beantragt werden. Im Anschluss prüft das BSI die Unterlagen auf Plausibilität, Nachvollziehbarkeit und bekannte Schwachstellen. Dann erhalten Hersteller oder Anbieter das Kennzeichen zur Verwendung. Während der Laufzeit überprüft das BSI stichprobenartig anlasslos und anlassbezogen, zum Beispiel bei Bekanntwerden von Schwachstellen, ob die Sicherheitsanforderungen des IT-Sicherheitskennzeichens eingehalten werden.

Der Erteilung des IT-Sicherheitskennzeichens für die Produktkategorie Videokonferenzdienste liegt die technische Spezifikation DIN SPEC 27008 zugrunde. Diese adressiert mögliche Risiken für die Informationssicherheit und Privatsphäre von Nutzerinnen und Nutzern und beinhaltet technische Vorgaben, wie diese Risiken minimiert werden können. Darunter fallen die Aspekte Accountschutz, ein angemessenes Update- und Schwachstellenmanagement, zeitgemäße Authentisierungsmechanismen, ein sicherer Rechenzentrumsbetrieb und weitere Sicherheitsfunktionen. Dazu zählen aktuelle Verschlüsselungstechnologien sowie Transparenz und Kontrolle während der Videokonferenz darüber, wer auf welche Weise zugeschaltet ist. So müssen die vorkonfigurierten Standardeinstellungen neuer Meetings beinhalten, dass diese privat (nicht öffentlich) erstellt werden und über schwer zu erratende Zugangsdaten abgesichert werden. Sie müssen zudem mit einer Warteraumfunktionalität ausgestattet sein, sodass Moderatoren neu beigetretenen Teilnehmenden den Zugang zum Meeting manuell gewähren müssen. Videokonferenzdienste müssen überdies ermöglichen, alle Teilnehmenden der Konferenz anzeigen zu lassen; der Beitritt neuer Teilnehmerinnen oder Teilnehmer muss per Audio- oder Videosignal klar erkennbar gemacht werden. Auftretende Schwachstellen müssen unverzüglich Nutzenden sowie dem BSI gemeldet und sogleich behoben werden. Die DIN SPEC 27008 fordert zudem eine Transportverschlüsselung nach Stand der Technik (aktuelle Transportverschlüsselung nach BSI-TR-02102).

Tue Gutes und kennzeichne es!

Gemäß diesem Motto können Hersteller und Anbieter von E-Mail-Diensten, Routern, smarten Verbraucherprodukten, Videokonferenzdiensten sowie mobilen Endgeräten das IT-Sicherheitskennzeichen für ihre Produkte beantragen. Sie zeigen damit: Wir sorgen aktiv für die Einhaltung der IT-Sicherheitsvorgaben des BSI. Und das freiwillig – denn weder auf Bundes- noch auf EU-Ebene gibt es derzeit verpflichtende IT-Sicherheitsanforderungen für vernetzte Consumer-Geräte und -Dienste. Diese werden frühestens mit der Umsetzung des Cyber Resilience Acts der EU zu erwarten sein. Bereits heute können sich Hersteller mit dem IT-Sicherheitskennzeichen darauf vorbereiten.

Produkte kaufen, die es „drauf haben" – so geht's!

Produkte, die das IT-Sicherheitskennzeichen besitzen, können dies z. B. im Onlineshop oder bei Tarifübersichten sichtbar machen. Alternativ kann das Kennzeichen am Produkt selbst oder an dessen Verpackung angebracht werden.

Beispielhafte Abbildung des IT-Sicherheitskennzeichens

Das Label lässt auf einen Blick das Versprechen von Herstellern und Diensteanbietern erkennen, dass ein Produkt nach den Sicherheitsanforderungen des BSI gestaltet wurde und diese über die Laufzeit aufrechterhalten werden. Das schafft Vertrauen und gibt Orientierung bei der Kaufentscheidung. Per QR-Code auf dem Kennzeichen gelangen interessierte Kundinnen und Kunden auf eine Produktinformationsseite des BSI. Dort werden das gekennzeichnete Produkt sowie die wichtigsten Informationen zur Cybersicherheit leicht verständlich dargestellt. Dazu gehören z. B. die Sicherheitseigenschaften, dem BSI bekannte Schwachstellen und zugehörige Updates sowie die Laufzeit und Gültigkeit des jeweiligen Kennzeichens. Die Produktinformationsseite des jeweiligen Kennzeichens kann dynamisch angepasst werden und z. B. kenntlich machen, wenn zugehörige Sicherheitsupdates bereitstehen.

Fazit: Ein Win-win für Hersteller und Nutzende – auch in Forschung und Lehre

Das IT-Sicherheitskennzeichen bietet Nutzerinnen und Nutzern für den Einsatz smarter Technik sowie Videokonferenzdiensten Orientierung und erleichtert die Kaufentscheidung zugunsten von Herstellern, die sich zur Einhaltung von grundlegenden Sicherheitsanforderungen verpflichtet haben. Es fasst wichtige Fakten und aktuelle Informationen über die Sicherheitseigenschaften eines vernetzten Produkts oder Dienstes verständlich zusammen, dokumentiert die vom Hersteller zugesicherten Sicherheitseigenschaften eines Produkts und regt nicht zuletzt dazu an, das Sicherheitsniveau von Produkten ganz allgemein zu erhöhen und dies auch zu kennzeichnen.

Das IT-Sicherheitskennzeichen wird durch das BSI kontinuierlich weiterentwickelt. Derzeit findet eine Evaluierung statt, welche die Sichtweisen von Herstellern, Verbänden und Verbraucherinnen und Verbrauchern auf das Kennzeichen beinhaltet und auswertet. Die Veröffentlichung der Ergebnisse wird für Anfang 2025 erwartet. ◆

Befragung der Verbraucherzentralen zur Sicherheit von Online-Accounts: **www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/umfrage-account-gehackt-das-erwarten-betroffene-von-den-unternehmen-89064**

BSI-Verbraucherumfrage 2024 zur Priorisierung von Cybersicherheit: **www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240906_BSI-Umfrage_IT-Sicherheit_Kaufkriterium**

Mehr Informationen unter: **www.bsi.bund.de/it-sik**

Nachgefragt bei Frank Schulze, Kompetenzzentrum für Videokonferenzdienste (VCC) an der TU Dresden

Welchen Mehrwert bietet das IT-Sicherheitskennzeichen des BSI den teilnehmenden Einrichtungen am Wissenschaftsnetz X-WiN?

Alle Produkte, die das IT-Sicherheitskennzeichen tragen, sichern dadurch ein Basislevel von Schutzeigenschaften zu. Die teilnehmende Einrichtung muss diese nicht mehr aufwendig selbst prüfen. Durch eine transparente Beschreibung aller durchgeführten Sicherheitstests und die Visualisierung der erzielten Ergebnisse können sich Nutzende schnell und umfassend über die Eigenschaften des Produktes oder auch des IT-Dienstes informieren. Die Sicherheitsanforderungen werden leicht verständlich auf der Produktinformationsseite des BSI ganz ohne „Fachchinesisch“ erklärt. Damit sparen Hochschulen und Forschungseinrichtungen Zeit und haben trotzdem ein verlässliches Level an Sicherheit jenseits von Hersteller- und Marketingaussagen erreicht. Die Vergleichbarkeit der Tests in verschiedenen Produktkategorien des BSI hilft des Weiteren, einen schnellen Marktüberblick bei anstehenden Sondierungen zu gewinnen. Die Verantwortlichen in den Institutionen müssen nicht mehr alles selbst aus verschiedenen Informationsquellen zusammensuchen, sondern finden die notwendigen Angaben kompakt für jedes gekennzeichnete Produkt beim BSI auf einer eigenen Webseite.

Was sichert der Hersteller den Nutzenden zu – und was nicht?

Mit dem IT-Sicherheitskennzeichen sichert der Hersteller zu, dass er die Anforderungen des BSI selbst geprüft oder hat prüfen lassen. Er verspricht nicht, dass es nunmehr keinerlei Schwachstellen im System gibt, die nicht doch durch Angriffe ausgenutzt werden können. Der Hersteller verpflichtet sich aber verbindlich für die gesamte Laufzeit des IT-Sicherheitskennzeichens, bei Bekanntwerden solcher (bisher unbekannter) Schwachstellen in seinen Produkten diese unverzüglich an das BSI zu melden und schnellstmöglich durch Updates zu beseitigen.

Frank Schulze, CIDS – Center for Interdisciplinary Digital Sciences, Department Informationsdienste und Hochleistungsrechnen (ZIH), Kompetenzzentrum für Videokonferenzdienste (VCC) - Dresden | Tel. +49 (0)351 46335438, E-Mail: vcc@tu-dresden.de
https://tu-dresden.de/zih/vcc

Eine für alle, alle für eine – 10 Jahre DFN-Cloud

Fast unbemerkt, still und leise feiert die DFN-Cloud in diesem Jahr ihr 10-jähriges Jubiläum. Unter dem Eindruck der Feierlichkeiten zum 40-jährigen Bestehen des DFN-Vereins kam dieses Ereignis eindeutig zu kurz. Ein Rückblick erinnert an die Anfänge der heute fast selbstverständlichen Dienstleistungen.

Text: **Dirk Bei der Kellen, Christian Meyer, Michael Röder, Jakob Tendel** (DFN-Verein)

Foto: Alizay|Freepik

Eines der ältesten Dokumente zur DFN-Cloud ist ein Gesprächsprotokoll zur „Gewünschten Unterstützung des DFN-Vereins bei der Veranstaltung Cloud-Speicher im Hochschuleinsatz“, datiert auf den 27. Januar 2014. Es markiert den produktiven Beginn der DFN-Cloud-Dienste – wenngleich die Ursprünge des Dienstes noch weiter zurückliegen. Bereits im November 2012 veranstaltete der DFN-Verein in der Geschäftsstelle am Alexanderplatz den Workshop „Onlinespeicher als föderierter DFN-Dienst“. Die Initiative dazu geht auf das ehemalige Verwaltungsratsmitglied Wolfgang Slaby († 2024) von der Katholischen Universität Eichstätt-Ingolstadt zurück, der in der 63. DFN-Mitgliederversammlung unter TOP 9a „Vermischtes“ darum bittet, sich mit der Frage zu befassen, welche Alternativen es für einen Speicherdienst ähnlich dem Dienst Dropbox gibt. Das brachte den Stein ins Rollen. Schnell war klar, dass der DFN-Verein die Rolle des „Wegbereiters“ übernehmen würde, der den am Wissenschaftsnetz teilnehmenden Einrichtungen eine Plattform bietet, um föderierte Leistungen aus eigener Hand untereinander anbieten zu können.

Föderation als Inspiration

Erste Workshops skizzierten die Idee für einen Cloud-Dienst und widmeten sich den organisatorischen, technischen und rechtlichen Aspekten. Ein Blick in die Liste der Teilnehmenden zeigt ein Who's who der Fachleute im Verein, die sich für das „neue“ Thema engagierten. Genannt seien stellvertretend die Namen des langjährigen Vorstandsmitglieds Dr. Rainer Bockholt (Universität Bonn), des DFN-CERT-Geschäftsführers Prof. Dr. Klaus Peter Kossakowski und von Prof. Dr. Ramin Yahyapour, dem Geschäftsführer der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG). Alle Mitstreitenden, die sich mit Elan engagiert haben, dürfen sich heute zu Recht als Wegbereiterinnen und Wegbereiter der DFN-Cloud bezeichnen.

In den folgenden Jahren boten die Föderierten Dienste hauptsächlich Sync-and-Share-Services an. Im September 2014 konnte bei der ZKI-Herbsttagung vermeldet werden, dass bereits drei Forschungsrahmenverträge zu den Diensten GWDG CloudShare, UniBW Sync&Share und TU Berlin ownCloud – „bedarfsgerecht, interoperabel und ohne Vendor Lock-in“ – erfolgreich abgeschlossen werden konnten. Noch ein Jahr zuvor hatte DFN-Geschäftsführer Jochem Pattloch bei der Tagung berichtet, dass mit Zustimmung der DFN-Mitglieder ein formaler Rahmen geschaffen werde, um verlässlich auf Föderierte DFN-Dienste zugreifen zu können.

Es gehe darum, die Vielfalt der deutschen Forschungslandschaft zu managen, außerdem biete der Wettbewerb von Konzepten einige Vorteile. Mit den Sync-and-Share-Diensten erhielt die X-WiN-Community eine Alternative zu den damals wenig auf die Bedarfe von Wissenschaft und Forschung angepassten kommerziellen Cloud-Services.

Durchbruch für die Cloud-Dienste – europaweites Vergabeverfahren mit OCRE

Nur wenige Jahre später hatte sich der öffentliche Markt weiterentwickelt und konnte nun mit Cloud-Services aufwarten, die einen zentral koordinierten Einsatz in öffentlichen Einrichtungen ermöglichten. Das neue Anwendungsszenario hieß „Infrastructure as a Service“ und wurde vorrangig von den großen amerikanischen Hyperscalern angeboten. Gemeinsam mit anderen europäischen nationalen Forschungsnetzen (National Research and Education Networks, NRENs) führte der DFN-Verein 2016 ein EU-weites Vergabeverfahren für Dienste kommerzieller Cloud-Anbieter durch. Die Ausschreibung fand unter der Leitung von GÉANT statt, der Dachorganisation der europäischen Forschungsnetze. Damit konnten DFN-Teilnehmereinrichtungen mithilfe von Direktabrufen auf diverse Rahmenverträge zu guten Konditionen zugreifen. Bereits bei den ersten Rahmenverträgen „GÉANT IaaS“ von 2017 bis 2020 war das Ziel, die Beschaffung kommerzieller Services durch öffentliche Einrichtungen leichter, schneller, und rechtssicherer zu machen. Im Kern waren damals bereits fast alle der heute bekannten zentralen Vorteile für die DFN-Teilnehmer und deren Forschungscommunitys vorhanden. Dazu gehörten in erster Linie die Ausschreibung nach EU-Recht und verbindliche Zusagen der Anbieter zur Datenspeicherung entsprechend der Datenschutz-Grundverordnung (DSGVO). Darüber hinaus hatten die NRENs die Möglichkeit, ihre teilnehmenden Einrichtungen als beratende und koordinierende Instanz im Umgang mit den kommerziellen Anbietern zu unterstützen. Vor allem der europaweit kollektive Ansatz der Forschungsnetze, als beschaffungsrechtlich legitime Vertreter der beinahe 10 000 Einrichtungen in Europa geschlossen aufzutreten, hat bei vielen globalen Anbietern eine echte Verhandlungsbereitschaft eröffnet, die bis heute wertvolle Zugeständnisse liefert.

> Das neue Anwendungsszenario hieß „Infrastructure as a Service“ und wurde vorrangig von den großen amerikanischen Hyperscalern angeboten.

Richtig Fahrt aufgenommen haben die Cloud-Dienste jedoch erst in der zweiten Ausschreibungsrunde von 2021 bis Ende 2024. Das Vergabeverfahren fand erstmalig im Rahmen des EU-Projekts OCRE


Auf dem Weg in die DFN-Cloud

„Auf dem Weg in die Cloud“ hieß es vor zehn Jahren in den DFN-Mitteilungen: Von KI bis Virtualisierung – heute profitieren die DFN-Teilnehmer von den vielfältigen Angeboten in der DFN-Cloud | *Foto: Stella Lenz/DFN*

(Open Clouds for Research Environments) statt. Seitdem hat sich die Abkürzung OCRE für Cloud-Rahmenverträge etabliert. Dem voran ging ein regelrechter Erklärmarathon für die Cloud-Verantwortlichen in der DFN-Geschäftsstelle. Durch die hohen Investitionskosten zum Beispiel in der Netzwerktechnik waren europaweite Ausschreibungen zwar geläufig, aber einen Wettbewerb für ein Infrastrukturformat durchzuführen, das den teilnehmenden Einrichtungen bis dato wenig bekannt war – und ohne selbst im Dienstbetrieb tätig zu sein –, stellte eine besondere Herausforderung dar. Nur wenige Einrichtungen konnten 2019, als das Vergabeverfahren mit ersten Bedarfs- und Anforderungsanalysen bei GÉANT startete, etwas mit dem Begriff IaaS anfangen. Viele Einrichtungen standen einem „Outsourcing“ von Rechenleistungen mindestens skeptisch, wenn nicht sogar ablehnend gegenüber. Ebenso wurde klar, dass nicht jedes Rechenzentrum optimal über die Bedarfe der Forschenden in den Einrichtungen im Bilde war. Keine Frage also, dass die DFN-Kollegen neben der technischen Herausforderung auch als Organisationsentwickler kulturwandlerisches Geschick zeigen mussten. Heute werden Cloud-Dienste viel mehr akzeptiert als noch vor zehn Jahren. Mit den neuen Cloud-Rahmenverträgen „OCRE 2024“ haben Nutzerinnen und Nutzer voraussichtlich ab Februar 2025 die Gelegenheit, auf ein vielfältiges Angebot an Services zuzugreifen.

DFN-Fernsprechen – von ISDN bis Cloud-Telefonie

Der Übergang von ISDN zur Cloud-Telefonie hatte eine wichtige Funktion als Türöffner und führte dazu, dass Cloud-Technologien besser akzeptiert wurden. Begonnen hat die Geschichte des DFN-Fernsprechens im Jahr 1998, als die entsprechenden Provider erste Schritte zur Organisation von Telekommunikationsnetzen wagten. Von Anfang an war das langfristige Ziel die „Konvergenz der Netze“, das heißt die Integration verschiedener Kommunikationsdienste in ein einziges Netzwerk, das Wissenschaftsnetz.

Ein wichtiger Meilenstein auf diesem Weg wurde 2006 erreicht, als der produktive Einsatz von Voice over Internet Protocol (VoIP) via Wissenschaftsnetz gelang. Dieser Schritt ermöglichte es, Telefonie unabhängig von Providernetzen zu betreiben und die eigentlich noch nicht veraltete ISDN-Telefonie zu substituieren. Zwar blieb die notwendige Infrastruktur zunächst lokal – On-Premises – und wurde von den jeweiligen Einrichtungen selbst betrieben, aber dies markierte den Beginn einer neuen Ära in der Telekommunikation (TK). In den folgenden Jahren fanden umfassende Planungen für ein „Portmodell“ statt, das die Auslagerung der lokalen TK-Infrastruktur zu einem zentralen Betreiber vorsah. Dieses Modell, heute als Cloud-Telefonie bekannt, sollte die Effizienz und Skalierbarkeit der Telekommunikationsdienste verbessern.

Im Jahr 2012 wurde ein Konzept für eine über das Wissenschaftsnetz vermittelte Cloud-Telefonie erarbeitet, das in die Vorbereitung eines entsprechenden Vergabeverfahrens einfließen sollte – ein weiterer Meilenstein auf dem Weg zur Realisierung der Konvergenz der Netze.

Schließlich wurde 2014 „VoIP-Centrex“ als cloudbasierte Telefonielösung im DFN-Fernsprechen eingeführt. Damit konnten Einrichtungen auf eine eigene Telefonanlage verzichten und stattdessen auf eine zentrale, cloudbasierte Infrastruktur zurückgreifen. In den zehn Jahren seit der Einführung von VoIP-Centrex sind viele DFN-Teilnehmer umgestiegen und profitieren nun von den Vorteilen einer skalierten, effizienten Telekommunikationslösung.

Dieser Erfolg zeigt die Bedeutung der Konvergenz der Netze und die Zukunftsfähigkeit der Cloud-Telefonie im DFN-Fernsprechen. Dazu konnte die Betreuung der Nutzenden sukzessive ausgebaut und professionalisiert werden.

DFN-Conf-Rahmenverträge für cloudbasierte Web- und Videokonferenzdienste

Der Dienst, der im Deutschen Forschungsnetz (DFN) infolge der Covid-19-Pandemie am härtesten auf die Probe gestellt wurde, war DFN-Conf. Universitäten, Hochschulen und Forschungsinstitutionen gingen deutschlandweit ad hoc in den Notbetrieb und schickten einen Großteil ihrer Beschäftigten zeitgleich ins Homeoffice. Dadurch gingen die Meeting- und Teilnehmerzahlen von DFN-Conf über Nacht durch die Decke und ein funktionierendes System stieß an seine Grenzen. Der massive Zugriff zeigte, dass Cloud nicht nur zentral betriebene, gemeinsam genutzte Ressourcen adressiert, sondern sehr stark auch auf Skalierbarkeit abzielt. Die teilnehmenden Einrichtungen wurden plötzlich mit der Situation konfrontiert, selbst Videokonferenzdienste beschaffen zu müssen.

Es waren die Kanzlerinnen und Kanzler der Hochschulen, die schnell bemerkten, dass die dezentrale Beschaffung durch die einzelnen Einrichtungen Unmengen an Ressourcen benötigt und dass der DFN-Verein von allen Organisationen am ehesten in der Lage wäre, eine zentrale Ausschreibung von

> Die Meeting- und Teilnehmerzahlen von DFN-Conf gingen über Nacht durch die Decke und ein funktionierendes System stieß an seine Grenzen.

Rahmenverträgen für cloudbasierte Web- und Videokonferenzdienste durchzuführen, denn mit dem deutschen und europäischen Ausschreibungsrecht kannte man sich bereits bestens aus. Nach umfangreichen Auswertungen und Verhandlungen waren die Rahmenverträge im März 2022 für die teilnehmenden Einrichtungen verfügbar.

Wenn heute im DFN-Kontext über Cloud-Technologien gesprochen wird, geht es in erster Linie um zentrale Ausschreibungen. Diese bieten nicht nur unschlagbare Vorteile beim Beschaffungsaufwand, sondern auch bei Verhandlungen mit potenziellen Anbietern, hinsichtlich Preisgestaltung, IT-Sicherheit und Datenschutz.

Föderierte Dienste als innovative Inkubatoren

Ein besonderer Fokus im DFN-Verein liegt damals wie heute auf den Föderierten Diensten, denn mit ihnen schließt sich der Kreis. 2014 war der Betrieb gemeinsam genutzter zentraler Cloud-Speicherlösungen noch Neuland. Heute verfügt der DFN-Verein über ein ausgedehntes Ökosystem an Cloud-Services und mit den teilnehmenden Einrichtungen im Wissenschaftsnetz über eine geballte Expertise auf dem Gebiet. Die Technische Universität Berlin beispielsweise nahm damals eine Vorreiterrolle ein und ist bis heute mit Diensten wie der Nextcloud ein starke Partnerin, die mit Thomas Hildmann zudem einen langjährigen Sprecher des Cloud-Forums bei den DFN-Betriebstagungen stellt. Für den DFN-Verein ist diese Form der Partizipation überaus wichtig in Hinblick auf die Entwicklung einer geteilten Wissenskultur – neudeutsch „Community-Building“.

Neue Dienste stehen nun im Mittelpunkt: Server- und Poolraum-Virtualisierung ermöglicht Einrichtungen den Einsatz von Cloud-Infrastrukturen, ohne selbst Hardware betreiben zu müssen. Mit Open Xchange ist eine Open-Source-Alternative für E-Mail-Verarbeitung möglich. Und seit Kurzem können interessierte Einrichtungen auf diesem Weg auch auf Großsprachmodelle zugreifen. Nach dem Motto „von teilnehmenden Einrichtungen für teilnehmende Einrichtungen“ sind bei den Föderierten Diensten der Fantasie fast keine Grenzen gesetzt. Insbesondere Cloud-Angebote, die noch nicht weit verbreitet sind, können zur realistischen Erprobung mithilfe der Föderierung einer breiten Nutzerschaft angeboten werden.

Und ab hier richtet sich der Blick nicht länger in die Vergangenheit, sondern in die Gegenwart und die Zukunft der DFN-Cloud, in der das kreative Potenzial der am Wissenschaftsnetz teilnehmenden Einrichtungen ein fruchtbares Umfeld findet. ◆

Chat AI – die datenschutzfreundliche KI für Forschung und Lehre

Am Wissenschaftsnetz teilnehmende Einrichtungen können über die föderierten Dienste in der DFN-Cloud seit September 2024 den Dienst Chat AI beziehen. Der KI-basierte Chatbot wird von der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) betrieben. Ihr Ziel ist es, den Zugang zu KI-Services für die akademische Landschaft einfach und kostengünstig herzustellen sowie einen Beitrag zur Erforschung von KI zu leisten.

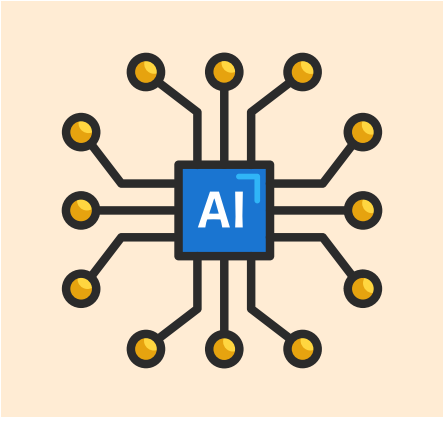
Text: **Jonathan Decker, Ali Doost Hosseini** (Georg-August-Universität Göttingen), **Tino Meisel, Martin Skowronek** (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen, GWDG)

Seit dem massiven Anstieg der Popularität von KI-gestützten Chatdiensten, beginnend mit ChatGPT 3 Ende 2022, sind viele konkurrierende Angebote für KI-basierte Chatdienste entstanden. Die Kerntechnologie hinter diesen KIs sind Large Language Models (LLMs). Trainiert mit einer großen Menge von Textdaten werden sie eingesetzt, um textbasierte Anfragen mit Informationen aus ihren Trainingsdaten zu beantworten. Während einige Unternehmen ihre Modelle proprietär halten, gibt es auch viele Bemühungen der Open-Source- und Forschungsgemeinschaft, um LLMs zu erstellen und zu verbessern. Der Internetkonzern Meta hat diese Entwicklung weiter beschleunigt, indem er seine Llama-Modelle öffentlich zugänglich gemacht hat.

Als Alternative zu bestehenden Angeboten hat die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) in Zusammenarbeit mit dem KI-Servicezentrum für sensible und kritische Infrastrukturen (KISSKI) einen LLM-basierten Chatdienst mit Open-Weight-Modellen entwickelt und hostet ihn auf der eigenen HPC-Infrastruktur. Zusätzlich zum Dienst ist der Zugang zu proprietären Modellen verfügbar. Beabsichtigt ist es, den Dienst stetig weiterzuentwickeln, komplexere und leistungsfähigere offene Modelle hinzuzufügen und die Integration mit anderen Plattformen auszuweiten. Insbesondere für Anwendungsfälle mit strengsten Datenschutzanforderungen ist Chat AI geeignet.

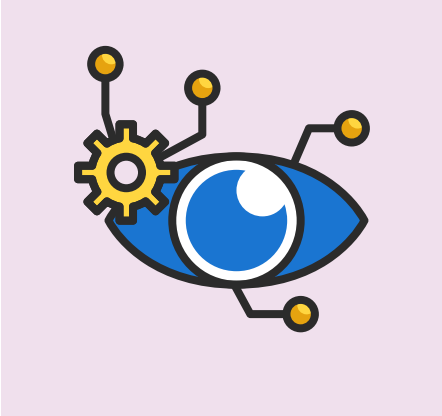
Der Einsatz von KI in der Lehre wird derzeit intensiv diskutiert und neue Ansätze an den Universitäten werden erforscht. Zum Beispiel können Studierende ihr Lernen durch LLM-Services verbessern. Gleichzeitig

müssen sie – aber auch Lehrende – wissen, wie solche Dienste verantwortungsbewusst genutzt werden. Es geht nicht nur um Textgenerierung – KI kann bei der Recherche, der Text- und Bildanalyse, bei der Strukturierung von Daten und vielen anderen Aufgaben eingesetzt werden. Ziel der Einrichtung von LLM-Diensten bei der GWDG ist es, den Zugang zu KI-Services für die akademische Landschaft einfach und kostengünstig zu ermöglichen – und darüber hinaus einen Beitrag zur verantwortungsvollen Erforschung des Potenzials von KI für Lehre, Lernen und Forschung zu leisten. Das erfordert ein gemeinsames Unterfangen von Serviceprovidern, Nutzenden und Forschenden.



Wie funktioniert Chat AI?

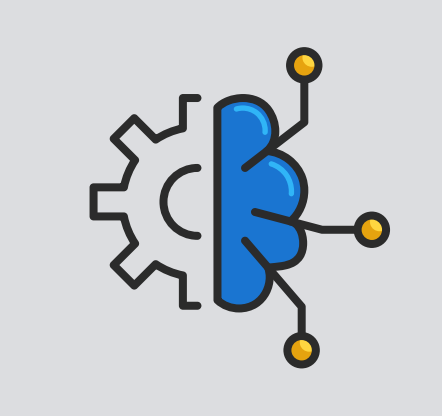
Die Privatsphäre der Nutzeranfragen ist von grundlegender Bedeutung, weshalb die GWDG garantiert, dass der Dienst zu keinem Zeitpunkt Prompts oder Antworten



serverseitig persistent speichert. Lediglich die Anzahl der Anfragen pro Nutzerin oder Nutzer, die Anzahl der I/O-Tokens und die jeweiligen Zeitstempel werden aufgezeichnet, um die Verwendung des Systems zu überwachen und Abrechnungen vornehmen zu können. Nutzende können ihre im Browser lokal gespeicherten Anfragen und Antworten ebenfalls per Knopfdruck löschen. Um zu einem späteren Zeitpunkt auf einen Chatverlauf zurückzugreifen, gibt es die Option, den Verlauf in eine Datei zu exportieren und später in einem neuen Chat wieder hinzuzufügen.

Chat AI beherbergt eine Auswahl an hochwertigen Open-Source-Modellen (Meta Llama 3.1, Mistral Large Instruct, Codestral, Qwen) sowie die Anbindung an verschiedene OpenAI-Modelle (ChatGPT-3.5, 4, 4o-mini). Neben der Auswahl eines passenden KI-Modells bietet Chat AI über den System-Prompt weitere Optionen, um die Bearbeitung der Aufgabenstellung anzupassen. Für die KI kann eine Rolle mit detaillierten Antwortbedingungen definiert werden. Damit lassen sich zum Beispiel verschiedene Perspektiven auf eine Fragestellung simulieren oder spezifisch strukturierte Antworten generieren. Über Schieberegler können zudem Parameter für die kreative Freiheit bei der Generierung der Antwort angepasst werden.

Über Chat AI hinaus bietet die GWDG auch Voice AI, einen KI-basierten Transkriptions- und Untertitelungsdienst auf der Basis des Whisper-Modells an sowie CoCo AI, einen Codevervollständigungsdienst mit Einbindung in Visual Studio Code über das Continue Plugin. Weitere Services stehen kurz vor dem Launch in den produktiven Dienst: Dazu gehören Image AI zur Generierung hochauflösender Bilder in diversen Stilen sowie das RAG-System (Retrieval Augmented Generation), welches erlaubt, eigene Daten und Dokumente sicher in die Arbeit mit LLM-Diensten einzubeziehen.



Das System wird auf der im KISSKI entwickelten Infrastrukturplattform SAIA (Scalable Artificial Intelligence Accelerator) gehostet. Diese erlaubt den Zugriff auf die KI-Dienste über das Interface der Academic Cloud als Web-User oder über die Integration in ein eigenes Frontend per API-Zugriff. SAIA besteht im Wesentlichen aus drei Teilen: Cloud-Server, HPC-Anmeldeknoten und HPC-Cluster. Auf dem Cloud-Server läuft die Frontend-App. Es erfolgt eine Anmeldung über die Academic Cloud SSO, wenn die Webanwendung zum ersten Mal geöffnet wird. Die Frontend-Applikation kommuniziert die Eingabe lokal an die Mediator-App, die ebenfalls auf dem Cloud-Server läuft und für die Kommunikation mit dem Backend „HPC“ zuständig ist.

In einer typischen HPC-Cluster-Umgebung sind die Rechenknoten, auf denen die Modelle laufen, nicht direkt über das Internet zugänglich. Daher leitet der Mediator über eine sichere Verbindung zum HPC-Anmeldeknoten des Clusters auf das Backend weiter. Über die Verbindung werden eingehende Anfragen auf die LLM verteilt. Leistungsstarke LLMs benötigen große Mengen an Grafikkartenspeicher, um effizient zu laufen. Bei größerer Nutzerauslastung kann es dazu kommen, dass eine Instanz eines Modells nicht ausreicht, um Anfragen zeitnah zu beantworten. Als Teil von SAIA wurde daher ein Scheduler entwickelt, welcher stets sicherstellt, dass genügend Instanzen für jedes Model verfügbar sind. Gleichzeitig versucht der Scheduler auch, die Grafikkarten zeitnah freizugeben sobald die Nutzerauslastung wieder sinkt, sodass die Grafikkarten für andere Aufgaben genutzt werden können. In zukünftigen Versionen von SAIA sollen Nutzende selbst in der Lage sein, Modelle einzustellen, welche dann vom Scheduler ausgeführt werden. ◆

Den Open-Source-Code von Chat AI sowie das Paper zur Architektur finden Sie unter folgenden Links:
https://github.com/gwdg/chat-ai
https://github.com/gwdg/saia-hub
https://arxiv.org/abs/2407.00110

Aktuelle Informationen zu den vorhandenen Open-Source- sowie Open-AI-Modellen und ihren Anwendungsbereichen finden Sie in der Dokumentation der GWDG:
https://docs.hpc.gwdg.de/services/chat-ai/models/index.html

Weitere Informationen finden Sie hier:
https://kisski.gwdg.de
https://chat-ai.academiccloud.de

E-Mail mit Open-Xchange

Open-Source-Alternative zu Microsoft Exchange: Seit dem 1. August 2024 können am Wissenschaftsnetz teilnehmende Einrichtungen den E-Mail-Service Open-Xchange (OX) über die Föderierten Cloud-Dienste des DFN-Vereins beziehen. Damit steht ein Dienst zur Verfügung, der nicht nur auf die Forschungscommunity zugeschnitten ist, sondern der sich auch durch hohe Flexibilität und sehr gute Skalierbarkeit auszeichnet.

Text: **Nikolaj Kopp, Johannes Weiß** (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen, GWDG)

Offizieller Startschuss für die produktive Nutzung des neuen E-Mail-Dienstes Open-Xchange: Seit Anfang August 2024 haben DFN-Teilnehmer die Möglichkeit, den Dienst der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) über die Föderierten Cloud-Angebote des DFN-Vereins zu beziehen. Vorteil der Open-Source-Alternative: Open-Xchange ist ein zentral bereitgestellter, wissenschaftlicher und föderierter E-Mail-Dienst, der unabhängig von großen, marktbeherrschenden Anbietern wie Microsoft ist.

Die Roll-out- und Migrationsprozesse haben begonnen. Eine Universität aus Süddeutschland und zwei Max-Planck-Institute haben das neue Angebot bereits für sich entdeckt, erste Postfächer- und Groupware-Funktionalitäten wurden kürzlich in Betrieb genommen.

Was ist Open-Xchange?

Mit den DFN-Teilnehmern richtet sich das Open-Xchange-Angebot an ein breites Spektrum an Nutzenden aus Wissenschaft und Forschung, die aufgrund des zunehmenden Preisdrucks der Marktführenden und deren forciertem Marketing ihrer Cloud-Dienste nach einer sinnvollen und soliden Alternative suchen.

Foto: fujiwara/Adobe Stock

Die Initiative startete im Jahr 2020 mit einer intensiven Marktbeobachtungsphase und zahlreichen Testszenarien, bei denen neben dem Funktionsumfang insbesondere auf Betriebssicherheit und Verfügbarkeit geachtet wurde. Open-Xchange ist eine modulare und open-source-basierte Softwarelösung, die sich durch eine hohe Flexibilität und sehr gute Skalierbarkeit für große E-Mail-Umgebungen auszeichnet. Mandantenfähigkeit zur getrennten Verwaltung unterschiedlicher Benutzergruppen ist ebenso gegeben wie die Unterstützung gängiger Standards aus der E-Mail- und Groupware-Welt.

Technisch überzeugt auch die ausgereifte Sicherheitsarchitektur. So ist bereits zum Start des Produktivbetriebs eine Single-Sign-on-Anbindung mit Multifaktorauthentifizierung implementiert. Der Zugriff von E-Mail-Clients wird durch anwendungsspezifische Zugangsdaten abgesichert, die für jedes Gerät individuell generiert werden. Die GWDG bindet dabei auch gern Authentifizierungsdienste von DFN-Teilnehmern für Open-Xchange ein, die bereits betrieben werden. Mit diesen und weiteren Sicherheitsfunktionen wird ein nachhaltiger Betrieb des E-Mail-Dienstes angestrebt.

Wie bietet die GWDG Open-Xchange an?

Schon in der Konzeptionsphase des neuen Dienstes war klar, dass die GWDG den neuen E-Mail-Dienst für eine breite Nutzerschaft auslegen möchte. Sie nutzte die Erfahrungen der vergangenen 20 Jahre im Betrieb von Microsoft Exchange und griff dabei auf viele bereits vorhandene Strukturen in der Mail-Infrastruktur zurück. Die technischen Dimensionen sind so gewählt, dass ein hoher Zuwachs an Postfächern durch interessierte Institutionen in den kommenden Jahren problemlos möglich ist.

Um allen E-Mail- und Groupware-Anforderungen gerecht zu werden, wurde bereits zu Beginn darauf geachtet, dass ein paralleler E-Mail-Betrieb von Microsoft Exchange und Open-Xchange auch innerhalb einer Einrichtung möglich ist. Gleichermaßen umsetzbar ist es, mit bereits existierenden Postfächern in die Open-Xchange-Installation der GWDG zu migrieren oder Postfächer für Nutzende anzulegen, die noch nie ein E-Mail-Postfach hatten.

Hochschulen und außeruniversitäre wissenschaftliche Einrichtungen haben über ihre Teilnahme am Wissenschaftsnetz des DFN-Vereins die Möglichkeit, Open-Xchange als Portfoliobestandteil der Föderierten Cloud-Dienste anzufragen. Teilnahmeberechtigt sind alle Einrichtungen, die ihre Nutzungsabsicht gemeinsam mit dem DFN-Verein vereinbaren. Die Abrechnung erfolgt über den DFN-Verein. Es fallen keine Vermittlungsgebühren oder Provisionen an.

Wie sieht der Onboarding-Prozess aus?

Bei Interesse können sich DFN-Teilnehmer über die E-Mail-Adresse cloud@dfn.de melden. Im weiteren Verlauf wird dann ein erstes Abstimmungsgespräch mit der GWDG vereinbart. Darin werden das konkrete Leistungsangebot von Open-Xchange vorgestellt und alle technischen und organisatorischen Fragen ausführlich geklärt. Nach dem ersten Kennenlernen begleitet die GWDG Interessierte bei allen Fragen und stellt Testkonten zur Verfügung. Mit diesen können alle Funktionen des Dienstes ausprobiert und näher betrachtet werden. Mit der weiteren Interessenbekundung beginnt die Vorbereitungsphase, in der die Themen Anbindung und Migration an das zentrale Identity-Management-System der GWDG (GWDG-IdM) geplant und durchgeführt werden. Die Anbindung an das IdM-System ist ein essenzieller Bestandteil des Dienstangebotes und eröffnet die Möglichkeit einer vollumfassenden Verwaltung der Nutzerkonten und aller Postfachfunktionen. Anschließend wird eine mögliche Migration der Bestandsdaten organisatorisch und technisch vorbereitet, damit zum Stichtag eine begleitete Datenübernahme durchgeführt werden kann.

Das zentrale Identity-Management-System der GWDG und die Software Open-Xchange sind technisch so angelegt, dass Einrichtungen zentral, aber getrennt voneinander verwaltet werden können. Somit bestimmen die Einrichtungen selbst über die Einstellungen und Funktionalitäten, ohne dabei von anderen Einrichtungen und deren technischen Anforderungen beeinflusst zu werden. Durch diese technische Flexibilität ist es der GWDG möglich, für nahezu alle heterogenen Anforderungen passende individuelle Lösungen zu finden.

Fazit

Das große Interesse und die bereits gestarteten Onboarding-Prozesse mit ersten Einrichtungen zeigen, dass das neue E-Mail-Angebot der GWDG Open-Xchange als Alternative zum weitverbreiteten Microsoft-Exchange-Dienst sehr gut angenommen wird. Die wachsende Nachfrage nach Föderierten Cloud-Angeboten sichert die Servicebereitstellung zentral in Deutschland betriebener Dienste und stärkt damit die digitale Souveränität von Hochschulen und Forschungseinrichtungen. ◆

Weitere Angebote im Rahmen der Föderierten Cloud-Dienste finden Sie unter: **https://www.dfn.de/dienste/cloud/foerderierte-cloud-dienste/**

Bei Interesse oder weiteren Fragen sprechen Sie uns gerne an unter: **cloud@dfn.de**

Kurzmeldungen

Auf der Zielgeraden: Cloud-Rahmenverträge in OCRE 2024

Die im Rahmen des GÉANT-Projekts GN5-1 gestartete EU-weite Neuvergabe von kommerziellen Cloud-Diensten „OCRE 2024“ (Open Clouds for Research Environments) nähert sich erfolgreich dem Ende. Die neuen Rahmenverträge werden voraussichtlich ab dem 3. Februar 2025 für die teilnehmenden Einrichtungen am Wissenschaftsnetz abrufbar sein. Sie gelten für einen Zeitraum von fünf Jahren.

Nach einer intensiven Phase der Evaluierung der eingegangenen Angebote konnte das internationale Ausschreibungsteam, an dem der DFN-Verein beteiligt ist, sehr gute Konditionen für die neuen Rahmenverträge erzielen: Der Leistungsumfang von IaaS+ (Infrastructure as a Service) inkl. PaaS (Platform as a Service) und SaaS (Software-as-a-Service) bleibt erhalten. Neben einer verbesserten Compliance mit Schwerpunkt u. a. auf Datenschutz und Sicherheit gibt es zusätzliche Discounts wie den Erlass der Egress-Kosten, garantierten Exit-Support und Split-Billing sowie viele weitere Verbesserungen. In die Bewertungen floss außerdem ein, ob die Anbieter zusätzlichen Support, Beratung, Trainings und Mehrwertdienste wie plattformspezifische Bildungsangebote für Lehre und Weiterbildung („Cloud in the Classroom“) im Portfolio hatten. Auch die Themen Inklusion und Nachhaltigkeit spielten bei der Auswahl der Angebote eine wichtige Rolle.

Über das Vorgehen beim Abruf der neuen Verträge informieren wir sie in Kürze über die üblichen Kanäle.

Bei allen Fragen zu den neuen Rahmenverträgen wenden Sie sich gerne an cloud@dfn.de ◆

Neue X-WiN-Core-Router erfolgreich installiert und in Betrieb

Nach dem Start des Roll-outs der neuen Core-Router im Mai dieses Jahres am Kernnetzknoten Hannover wurden im August die letzten beiden von zehn Nokia-Geräten an den Kernnetzknoten Duisburg/Essen und Düsseldorf eingebaut. Die Hardware-Installation der Router ist damit erfolgreich abgeschlossen.

Derzeit arbeiten die Kolleginnen und Kollegen vom DFN-NOC und DFN-CERT mit Hochdruck an der Migration der mehr als 1000 Teilnehmeranschlüsse und der DFN-Internet- sowie DFN-VPN-Dienste auf die neue Plattform. Voraussichtlich bis Ende des Jahres ist mit einem Abschluss dieser Arbeiten zu rechnen.

Parallel zur Installation der Hardware erfolgte bereits die Anbindung der Router an das Echtzeitmonitoring-Tool DMon – eine Voraussetzung, damit das Core-Router-Netz vollständig in den Produktivbetrieb übernommen werden kann.

DMon überwacht die komplexe X-WiN-Infrastruktur und liefert Analysen zum aktuellen Betriebszustand und zu Störungssituationen. Aufgrund des Herstellerwechsels waren hier umfangreiche Neuentwicklungen und Anpassungen notwendig. Für die neue Messtechnologie „Streaming Telemetry“ waren die Implementierung neuer Monitoring-Protokolle und Verfahren erforderlich. Die erste Version des deutlich optimierten Echtzeitmonitorings ist nun erfolgreich im Einsatz. Neben einer Erhöhung der zeitlichen Messpunkte um den Faktor 5 ist auch eine schnellere Alarmierung mit einer Verzögerung von maximal einer Minute möglich.

Mit dem Plattformwechsel geht eine deutliche Erhöhung der Übertragungskapazität pro Standort einher. Die Gesamtkapazität der neuen Geräte vom Typ Nokia 7750 Servicerouter beträgt im Endausbau 108 000 Gbit/s je Chassis, unterstützt werden Schnittstellen bis zu 800 Gbit/s. Damit wird noch einmal eine deutliche Erhöhung der Leistungsfähigkeit für zukünftige Anforderungen der Teilnehmer am Wissenschaftsnetz erreicht.

Foto: Jacqueline Struyken/DFN

Bereits im vergangenen Jahr wurde die „kleine“ Geräteklasse der IP-Plattform modernisiert, die Aggregationsrouter. Die auf dieser Plattform eingesetzten 58 IP-Router bieten eine Gesamtkapazität von 2 400 Gbit/s pro System. Im Zusammenspiel beider Geräteklassen wird die runderneuerte IP-Plattform ausreichend Leistungsreserven bereitstellen, um auch künftige Anforderungen der Teilnehmer verlässlich bedienen zu können. ◆

Informationen zum Aufbau des Wissenschaftsnetzes finden Sie unter: **https://www.dfn.de/netz/aufbau/**

Auf Wachstumskurs: easyroam registriert knapp 250 000 Nutzende

The easy way to eduroam: Aktuell verzeichnet easyroam rund eine Viertelmillion Nutzende, die den einfachen und sicheren Zugang zum WLAN-Dienst eduroam über die DFN-AAI wählen. Sowohl für die Nutzenden als auch für die teilnehmenden Einrichtungen am Wissenschaftsnetz bedeutet die Diensterweiterung weniger Aufwand bei der Nutzung von eduroam. Davon profitieren insbesondere kleine Einrichtungen.

Bei einer passwortgestützten Authentifizierung ist es leider immer noch möglich, dass Passwörter kompromittiert werden. easyroam verwendet hingegen ausschließlich die zertifikatsbasierte Authentifizierung über die DFN-AAI und bietet so mehr Sicherheit.

Die easyroam-App gibt es für alle gängigen Betriebssysteme wie Android, iOS, Linux, macOS und Windows. Sie erleichtert Nutzenden die Konfiguration der easyroam-Profile auf den Endgeräten, die für die Anmeldung in eduroam erforderlich sind. Für ältere oder proprietäre Geräte besteht die Möglichkeit der manuellen Konfiguration, damit auch bei diesen Geräten eine passwortgestützte Anmeldung in eduroam nicht mehr notwendig ist. ◆

Mehr zum Thema easyroam gibt es in unserer Dokumentation: **https://doku.tid.dfn.de/de:eduroam:easyroam**

Bei Fragen zu easyroam wenden Sie sich gern an: **easyroam@dfn.de**

DFN-Terminplaner 6 jetzt per DFN-AAI erreichbar

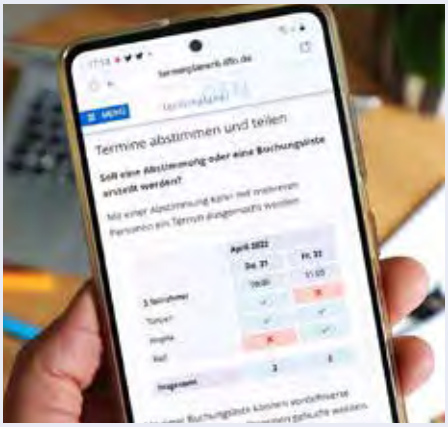


Foto: DFN

Teilnehmende Einrichtungen am Wissenschaftsnetz können sich freuen: Ab sofort ist die DFN-AAI-Anbindung für den DFN-Terminplaner Version 6 verfügbar. Diese Erweiterung ermöglicht es Nutzenden, die über die DFN-AAI authentifiziert werden, die bereits existierenden Anmeldedaten der Heimateinrichtung für die Anmeldung auf dem Terminplaner zu verwenden. Dafür ist die Konfiguration des Shibboleth Identity Provider (IdP) im zuständigen Rechenzentrum notwendig.

Bei der Anmeldung über die DFN-AAI wird ein neues Nutzerkonto für den Terminplaner generiert – unabhängig davon, ob Nutzende bereits mit einem Konto auf dem Terminplaner registriert sind. Dabei ist eine wichtige Einschränkung zu beachten: Bereits vorhandene Abstimmungen, die auf dem „alten“ Nutzerkonto durchgeführt wurden, werden nicht automatisch auf das über die DFN-AAI neu erstellte Konto übertragen.

Die DFN-AAI-Integration in den Terminplaner 6 stellt eine bedeutende Verbesserung für die Benutzerfreundlichkeit dar, da keine Notwendigkeit besteht, ein separates Nutzerkonto mit eigenem Passwort anzulegen. Dies reduziert den Verwaltungsaufwand sowohl für die Nutzenden als auch für Administrierende und verbessert gleichzeitig die User Experience (UX).

Wichtig für Administrierende: Die Informationen zur Implementierung der DFN-AAI sind in den FAQs des Terminplaners (aktuell vorletzte Frage) hinterlegt. Neben den dafür erforderlichen Attributen ist dort auch ein Konfigurationsbeispiel für die Einrichtung eines Shibboleth-IdP verlinkt, um Administrierende bei der Implementierung zu unterstützen. ◆

Zum DFN-Terminplaner geht es hier: **https://terminplaner6.dfn.de/**

Starke Partner weltweit

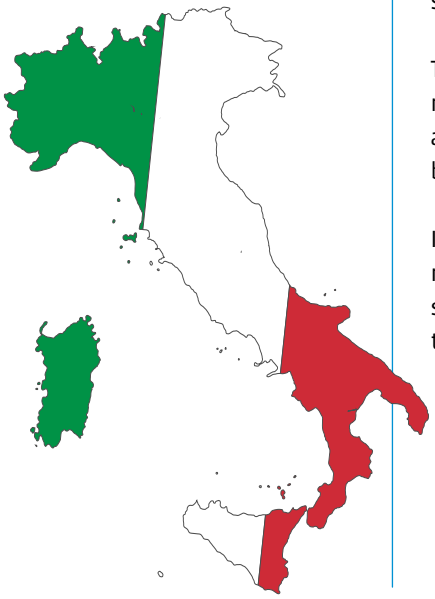
Konnektivität fördern, Zukunft gestalten, Herausforderungen gemeinsam meistern: Nationale Forschungsnetze rund um den Globus betreiben leistungsfähige Infrastrukturen für Wissenschaft, Forschung und Lehre. Ein Blick in die Welt der NREN-Community.

What IT Takes to be a Community

A glimpse of GARR, the network powering research and education in Italy

In an era where digital connectivity is fundamental to scientific and cultural progress, national research and education networks (NRENs) are a powerful resource for continuous innovation and, in turn, opportunities for all. Each country organises its own NREN to better respond to the needs of researchers, professors, and students. In Italy, such infrastructure is called GARR, and, as we will see shortly, it is much more than an ultra-broadband infrastructure, but rather a vibrant community shaping the future of digital innovation in the country. Let's take a look.

Text: **Elis Bertazzon** (Consortium GARR)



GARR connects a community nationwide and beyond

GARR, which stands for, "Group for the Harmonisation of Research Networks," is firstly an extensive digital infrastructure with about 20,000 km of optical fibre covering the entire national territory. It reaches about 3 million users and connects more than 1,000 sites, mostly public institutions.

This network has an extremely high transmission capacity (up to 200 Gbps for single access) in both download and upload, with a backbone capacity of 23 terabits per second.

In addition to connectivity and network management, GARR also offers a suite of services ranging from security solutions to mobility and digital identity management, cloud and storage services, and applications for web conferencing and live streaming.

An infrastructure powered by its community

The GARR user community is diverse, covering different domains from scientific and biomedical research to universities, cultural institutes (like libraries and museums), schools and the performing arts (music conservatories). This vibrant user base has particular requirements, and part of GARR's mission is to design custom network solutions and services. But how can we ensure that GARR hears and understands these different voices? The association's strength relies on its community-driven approach. GARR isn't simply a service provider; it's a network of people collaborating to advance research and innovation in Italy, and this is reflected in its governance model: the network's users are also its main actors. They play a significant role shaping the institution.

This novel approach is reflected in GARR's organisational structure, which promotes inclusiveness and involves users in decision-making regarding the future evolution of the network and digital infrastructures.

Map of the GARR-T network

Indeed, the association was founded in the 1990s by the major Italian research bodies. All state universities and research hospitals later joined as partners with representatives in the assembly. This model ensures that the user community needs directly guide strategic decisions about the network. But there is more: Each connected organisation appoints a local technical manager, a so-called access point manager (APM), who plays a crucial role. The APM ensures the smooth day-to-day operation of the local network and acts as a direct liaison with GARR network experts. Thanks to this constant line of communication, GARR can address specific needs or challenges that may arise, ensuring that each organisation receives tailored solutions in terms of network and services.

From specific requests to broader solutions

Over the years, the collaboration with users led to the development of solutions that were later extended to the whole community and beyond. One example is LOLA, which is short for LOw LAtency audio visual streaming system. This pioneering technology was born from the cooperation between GARR and the Music Conservatory of Trieste. Such a system, now widespread worldwide, has revolutionised long-distance music education by allowing real-time live musical performances with artists located even thousands of kilometres away.

Another example is the IDP in the Cloud service, which GARR initially created to ease access to federated services for the biomedical research community and later employed in similar use cases. The service offers a quick and secure way for organisations without in-house expertise to join the Italy's IDEM federation for identity management and access national and international federated services (through eduGAIN).

Another service that GARR developed for its community is eduid.it, which was set up in collaboration with the Italian Ministry of University and Research and the Italian Erasmus+ agency, INDIRE. An identity provider dedicated to student mobility, eduid.it, enables access to Erasmus+ digital services published in eduGAIN through the MyAcademicID platform, which is managed by GÉANT. It also provides digital credentials to performing arts students, even if their institutions are outside the GARR network.

GARR-T: going beyond the network

When it comes to innovation, GARR has recently launched GARR-T, the latest evolution of its network backbone. GARR-T has been fully operational since late 2023 and it expanded the backbone capacity from three to over 23 Tbps and increased the minimum capacity for backbone connections at 100 Gbps.

The novelty of GARR-T lies in its architecture, which features a dual-layer design with a packet layer using a data centre model and an optical layer based on a disaggregated structure that separates fibres and equipment. This design ensures flexibility, scalability, and sustainability by avoiding technological lock-ins and optimising resource use. The adoption of an open line system (OLS) allows dynamic optical spectrum management, enabling advanced services like spectrum sharing and distributed computing. Automation further enhances reliability by streamlining network management, enabling real-time fault detection and rapid service reconfiguration.

One example of GARR-T's impact on Italian research is the spectrum-sharing project between Bologna and Geneva. In September 2023, GARR and the European collaboration of NRENs – GÉANT – connected the national computing centre, INFN-CNAF in Bologna, with CERN in Geneva. The two organisations are over 1,000 km apart. This data centre interconnection, using a multi-domain shared spectrum, achieved a capacity of 1.6 Tbps and a latency of 9.5 milliseconds, allowing researchers at the two centres in Italy and Switzerland to collaborate as if they were right next door.

But this is just the first step. The GARR team continues to enhance and expand its network to other areas of the national territory. While this initial phase of GARR-T was built using GARR funds, its expansion relies on EU Next Generation Funds (NRRP) resources with the TeRABIT and ICSC projects. After its expected completion

At a glance: The Italian Education & Research Network

in 2025, the GARR-T network will span 25,000 km and reach a total capacity of about 40 Tbps throughout Italy.

Beyond terrestrial boundaries: subsea connections and sensing

GARR innovation efforts continue beyond the shoreline. A recent development in this area is the acquisition of optical spectrum in a underwater cable to Sardinia, funded by the EU project TeRABIT. This expansion will exploit the Sparkle BlueMed submarine cable system's spectrum to create a virtual fibre optic bridge between GARR-T optical infrastructure in the Italian mainland and the one on Sardinia, integrating Sardinia's university and research network into the larger GARR national backbone.

Besides an improved connectivity that will benefit the entire island's scientific community, this link will also support the candidature of the Sardinian Sos Enattos area to host the Einstein Telescope project, the European third-generation gravitational-wave detector. But there is more. This subsea cable opens new possibilities in terms of environmental sensing, giving the possibility for researchers to use the optical fibre as a sensor of undersea seismic and volcanic activities, as well as for detecting and studying marine life.

Who will build the network of the future?

A network is not only composed of cables and technology; the human factor is also essential. Like many other NRENs, GARR also faces significant challenges in attracting and retaining young talent, which is mainly due to competition with large corporations and the dynamic nature of careers in information and communication technology. To address this difficulty and to maintain GARR infrastructure at the top of innovative technology, GARR has introduced the GARR Academy, an initiative offering intensive training courses for young students in relevant technical fields, with the possibility of employment at the end of the programme. The idea is not only to provide participants with practical skills and industry insights, but also to allow them to continue their education while gaining valuable experience, ultimately bolstering the ranks of the next generation of network professionals. In its first edition, the campaign attracted 50 applicants, from which 10 participants were selected and trained, leading to five of them being hired on fixed-term contracts, with four later transitioning to permanent positions.

This initiative goes hand-in-hand with GARR's decade-long effort to fund young students' innovative projects, which has led GARR to award 10 scholarships every year.

In Italy and Europe: an international community

GARR has been instrumental in founding and continually supporting GÉANT, the network of European NRENs. GARR collaborates with GÉANT to provide high-capacity connectivity across Europe and beyond, supporting cutting-edge research projects, including the Large Hadron Collider (LHC) and high-performance computing centres. Within GÉANT, GARR actively participates in EU-funded network projects that underpin its infrastructure development and in the steering committee and user groups, where different European networks bring their expertise and perspectives across various areas.

Recently, GARR upgraded its link to GÉANT to a total international capacity of 600 Gbps, supporting the high data exchange needs of international collaborations. Following the new connection, peaks of over 200 Gbps were recorded during the LHC Data Challenge, highlighting the increased capability to support major scientific experiments.

Thanks to such collaborations, GÉANT and all European NRENs can support the progress of the most advanced user communities, such as those in high-energy physics, radio astronomy, and supercomputing, in Europe and worldwide. ◆

International Newsflashes

GÉANT Announces Lise Fuhr as Organization's Next CEO

The GÉANT Association recently announced Lise Fuhr as its next Chief Executive Officer (CEO). She is set to succeed current CEO Erik Huizer on 21 November 2024. Before becoming GÉANT's CEO, Fuhr served as Director General of ETNO, the Brussels-based association representing Europe's leading telecom operators, for nine years. She is Chair of the Danish cyber security organisation "Security Tech Space."

Her experiences in these roles led to her being nominated in August 2022 as a member of the United Nations Internet Governance Forum Leadership Panel, where she is serving a three-year term. Between 2017 and 2024, she was also a board member of European Cyber Security Organisation (ECSO). From 2016-2022 she served as Chairwoman of the Boards of both the Public Interest Registry (.org domain name registry) and the Public Technical Identifiers (PTI), formerly IANA, and affiliate of ICANN.

From 2009 to 2016, Fuhr was Chief Operating Officer of DK Hostmaster and DIFO, the company managing .dk domain names. From September 2014 to October 2016, she also chaired the Cross Community Working Group for the IANA Stewardship Transition, building on her strong network within the internet community. Fuhr has over 20 years of experience within the internet, technology, and telecoms industries and is a lifelong member of ATV – the Danish Academy of Technical Sciences – an independent think tank. ◆

More information: **https://connect.geant.org/2024/09/03/geant-proudly-announces-lise-fuhr-as-next-ceo**

GÉANT Begins GN5-2, A Large Project Dedicated to Increasing Europe's Research Infrastructure

The largest association of research and education networks (NRENs) in Europe, GÉANT, received funding approval for a new large project, GN5-2. The project, funded by the European Commission to the tune of €80 million, will further expand Europe's digital infrastructure for research and education. The project officially begins on Jan. 1, 2025 and is a key component for the strategic framework agreement GN5-FPA.

The project primarily focuses on further expansion and modernization of European research networks, with a particular focus on:

- Improved data transfer rates: In order to better address the increasing challenges associated with large volumes of data movements, the project aims to improve data transfer to terabit speed. This improvement allows researchers to send larger data volumes more efficiently, particularly in the realms of artificial intelligence, high-performance computing, and big data.
- Improved security: Innovative security solutions are aimed at protecting confidential data and allowing for more secure collaborations. The project has a special focus on further improving security against cyber attacks.
- Flexible services: New services and applications should make it easier for researchers and research institutions to collaborate globally. Funding will be used to further improve innovations in the realm of digital research spaces, cloud-based services, and other collaborative tools.

Further, the project is also heavily focused on further expanding European NRENs' identity and access management infrastructure. This will enable a secure, standardized access platform to access research data and services across all of Europe. The DFN Association, which operates the German Research Network (DFN), plays an active role in implementing the GN5-2 project. Together with third-party partners at DFN-CERT, the Karlsruhe Institute of Technology (KIT), the Leibniz Supercomputing Centre (LRZ), and the Regional Computing Centre Erlangen (RRZE), DFN is involved in all of the project's different work packages. The German involvement secures not only Europe's strong position in the realm of research networks, but also contributes to better connecting the German research landscape to partners and collaborators internationally. ◆

GÉANT Community Welcomes New Special Interest Group on AI for NRENs

The GÉANT community is excited to announce the establishment of a new Special Interest Group (SIG) focused on "AI for NRENs." This marks the inaugural year of operation for the SIG-AI, which was formally founded at TNC2 – the premier research and education networking conference – in June 2024.

The SIG-AI for national research and education networks (NRENs) is dedicated to exploring the transformative potential of artificial intelligence (AI) within the context of NRENs. The group will investigate how AI can enhance cybersecurity, above-the-net services, network management, and other network services currently offered by GÉANT and its member NRENs. Additionally, the SIG will closely examine new European Commission regulations concerning AI and their implications for GÉANT and the broader NREN community. Participation in the SIG is also open to universities and research institutes working on AI, meaning that institutions participating in the DFN Association are welcome to participate in the SIG.

A series of meetings are planned for the SIG-AI, with the first gathering scheduled for early December in Poznań, Poland. This initial meeting will provide a comprehensive overview of how AI is currently being utilised by NRENs. A subsequent meeting, coinciding with the GÉANT Security Conference, will delve deeper into the intersection of cybersecurity and AI. A Call for Participation for the December meeting will be released shortly.

The Steering Committee of the new SIG is comprised of seven members, including Leonie Schäfer (DFN) as the initiator and coordinator of the group, and Jan Kohlrausch (DFN-CERT) as an AI expert.

This exciting new SIG represents a significant step forward in leveraging AI to drive innovation and improve the services offered by GÉANT and its member NRENs. ◆

More information:
https://community.geant.org/sig-ai

EU Project EaPConnect Enters Final Phase with ROM-Interviews and International Conference

The European Union (EU) project EaPConnect is nearing its conclusion and is undergoing a comprehensive evaluation to assess its impact and sustainability. The European Commission's Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR) is launching a final evaluation to measure the project's relevance, effectiveness, efficiency, impact, sustainability, coherence, and added value.

The project focuses on increasing high-speed connectivity within and between the national research and education networks (NRENs) in five Eastern Partnership nations – Armenia, Azerbaijan, Georgia, Moldova, and Ukraine – to other NRENs in Europe and beyond. DFN has served as an associate partner in the second round of the project.

As part of this evaluation, DG NEAR is conducting ROM-Interviews (Results -Oriented Monitoring Interviews) on October 7th in Chisinau, Moldova that will involve key project partners and stakeholders, including representatives from the Moldovan National Research and Education Network (RENAM). Advisors to the project, such as Leonie Schäfer from the German National Research Network (DFN), will also participate.

The EaPConnect project has played a crucial role in strengthening the digital connectivity and research infrastructure of countries in the Eastern Partnership region. The final evaluation will provide valuable insights into the project's achievements and lessons learned and will inform future initiatives in this area. ◆

Collaboration on this Newsflash:
Leonie Schäfer, Eric Gedenk

You can find more international community news under:
https://connect.geant.org/community-news

Radiation-Free Breast Cancer Screenings Come Closer to Reality

An international research consortium, as part of the European-Union-funded QUSTom Project, is focused on using computer modelling and ultrasound technology to make a less intrusive way to screen for breast cancer. The project collaborators use high-speed networks to share large amounts of ultrasound and simulation data.

Text: **Eric Gedenk** (DFN-Verein)

THE FIELD

National research & education networks (NRENs) all over the world working together. With our powerful communication infrastructures we enable access to knowledge & resources, connect people, foster collaboration.
In this series our participating institutions share their inspiring stories and achievements.

Since the 1980s, most nations have experienced a steady decline in breast cancer mortality. While treatments have undoubtedly improved, medical professionals have focused on early detection as a key component in raising the survival rate. Germany, for instance, encourages women over 50 to get a free screening every two years.

Most women are screened using mammograms, which compress the breast and then take x-ray images from several angles. While mammograms are safe and effective for many women, they do have downsides. While modest, x-ray imaging delivers a dose of radiation, meaning that following health guidance will expose a healthy woman to many doses of radiation over the course of her later years. Further, for roughly 40 percent of women who have so-called dense breasts, mammogram imaging is not always as clear. For these women, mammograms can occasionally miss the beginnings of cancer, but more often, might flag something as "suspicious" that ultimately is not cancerous but leads to days of worry and anxiety for the patient.

At the Karlsruhe Institute for Technology, researchers are developing a 3D ultrasound computer tomography instrument to use for radiation-free breast cancer screen. This measuring aperture (above) is outfitted with many individual ultrasound transducers. | *Foto: KIT*

Piezoelectric elements generate mechanical movements (ultrasonic waves) through electrical voltage and are used in ultrasonic transducers. They enable precise measurements and imaging in ultrasound devices. | *Foto: Qustom-pacient*

"This is where we come in with ultrasound tomography to help," said Dr. Nicole Ruiter, Department Head at the Karlsruhe Institute of Technology's (KIT's) Institute for Data Processing and Electronics. "With ultrasound imaging, we can avoid using radiation, meaning we could safely run scans on pregnant women and younger women. Further, our methods can screen at a higher frequency, and might deal better with accurately scanning women with dense breasts."

Ruiter and her KIT colleagues are a part of a large European research project called QUSTom, which aims to revolutionize breast cancer screening. The two-and-a-half-year project aims to develop a workflow for fully 3D ultrasound tomography (USCT) breast cancer screenings. Headquartered at the Barcelona Supercomputing Centre (BSC) in Spain, QUSTom uses ultrasound imaging in concert with high-performance computing (HPC) in pursuit of its goals. For Ruiter and her KIT collaborators, access to a world-class research and education network – such as the Deutsches Forschungsnetz's (DFN's) X-WiN network – is an essential piece of the technological puzzle needed to improve breast cancer screening accuracy and safety.

Imaging and simulation work together to advance the state-of-the-art

In the 1970s, researchers had begun experimenting with using ultrasound tomography technology to scan for breast cancer. While the lab experiments showed promise, mammography became the preferred method for screening. Traditional ultrasound methods are primarily used only in situations where doctors are scanning soft tissue in the body, which in theory would work well for breast cancer screening. However, standard ultrasound imaging by itself can struggle to catch early warning signs for breast cancer – such as small calcium deposits forming – and are more prone to false positives or negatives in women with dense or fattier breasts.

In the last decade, technology became available to start designing methods to combine ultrasound technology with computed tomography for clinical application – a method that normally uses x-rays that takes many images from different angles. Ruiter and other researchers in the field started focusing on USCT. Unlike traditional CT scans, USCT does not use x-rays for imaging, substituting ultrasound – albeit a different type. Traditional ultrasound sonography – commonly used in prenatal exams, identifying kidney stones, and a host of other applications – focuses waves via a transducer array. While effective in certain contexts, these arrays can leave blind spots when scanning for breast cancer. USCT devices address traditional ultrasound's shortcomings by creating "spherical" waves, and reconstruct images by collecting many two-dimensional slices of a 3D image or building full 3D devices that create images from ultrasound transducers that are positioned at many different angles then combining that data.

Ruiter noted that the availability of fast data acquisition and management made USCT possible. "USCT is possible due to the availability of many parallel channels, doing fast data acquisition due to how many distributed ultrasound transducers we need, and then, of course, powerful computing and networking resources so that we can accurately reconstruct these images at high resolution," she said.

Stronger networks support advancements in medical technology

The QUSTom project involves six partners from Germany, Slovenia, Spain, and the

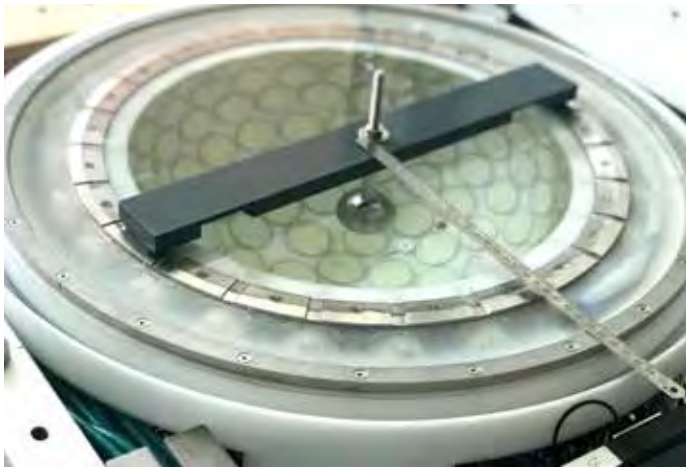
United Kingdom. Further, patient ultrasound data falls underprotected medical data, meaning the project participants need to anonymize data before working with it.

"On the one hand, we must keep this information safe, and on the other hand, we are dealing with huge amounts of data that needs to be transported," Ruiter said. "Our group is checking the data that is coming in and are creating starting models, so we are downloading it, checking for errors and accuracy, doing initial reconstructions, then reuploading analysis and the models. Another group does data preprocessing, and then that data is sent to a supercomputer in Barcelona. There is a huge need for high bandwidth, stable data movement and storage—we are collecting roughly 500 gigabytes of data per patient."

The KIT team relies heavily on DFN's X-WiN network to efficiently download and upload these massive datasets and transmit them to partners across Europe. DFN's connections within Germany ensure that Ruiter can move data across German efficiently, and she is hopeful that connections forged through the GÉANT collaboration of Europe's collection of national research and education networks (NRENs) continue raise speed and efficiency of moving data between institutions supported by different NRENs. Spain's NREN, RedIRIS, connects BSC's supercomputing resources to research organizations in Spain and internationally through the greater GÉANT collaboration, including Ruiter and her colleagues at KIT.

The QUSTom project has already successfully performed a feasibility study and continued work on improving prototype USCT devices. Moving forward, the project will continue to rely on high-resolution simulations supporting imaging being done at medical facilities. Project partners are also continuing to find ways to integrate their workflow into the computing cloud, ultimately striving for a "black box" technology that allows doctors to scan a patient, process the data quickly and securely, and give the patient accurate results as efficiently as possible.

"Doctors appreciate being able to put a patient on a device, get the images directly, and transfer these data to their own internal systems" Ruiter said. "That is ultimately the way to go, but to get there, we have a lot of research to go to scale down calculations, reduce data movement, and help medical professionals create quality images that are just a couple of gigabytes." ◆



As part of the EU-funded QUSTom project, Karlsruhe Institute of Technology Dr. Nicole Ruiter works with researchers across Europe to develop next-generation breast cancer screening devices. The team is actively creating prototypes for radiation-free breast cancer screening devices.
Foto: KIT

For more information on the QUSTom project, visit the project's website at: **https://www.qustom-project.eu/**

For more information about the Ruiter group at KIT, please visit **https://www.ipe.kit.edu/english/2596.php**

For more information about Barcelona Supercomputing Center, visit **https://www.bsc.es/discover-bsc**

IN THE FIELD

Find more exciting research stories from all over the world on In The Field blog:
www.inthefieldstories.net

Ordnung muss sein

Einrichtungsübergreifende Prozesse sind an Hochschulen allgegenwärtig. Insbesondere in der IT-Versorgung sind die Grenzen einer großen Organisation selten klar umrissen. So werden unterschiedliche Klassen von Organisationen und Einrichtungen mit einem differenzierten Angebot an IT-Services versorgt. Für konsistente und skalierbare Prozesse ist darum ein Organisationsverzeichnis essenziell, das alle Organisationen und Einrichtungen erfasst – und darüber hinaus deren Unterschiede und Merkmale widerspiegelt.

Text: **Thomas Eifert, Thorsten Kurth** (RWTH Aachen)

Foto: BohumilB/iStock

In großen Organisationen wie Hochschulen greifen unterschiedliche Einrichtungen innerhalb dieser Organisation auf zentrale IT-Services zu. Dabei ist es häufig so, dass einzelne Mitarbeitende aus der jeweiligen Einrichtung als Ansprechperson für solche Services autorisiert werden, idealerweise für die Nutzung entsprechender Selbstbedienungsfunktionalitäten. Einer der ersten so nutzbaren Services an der Rheinisch-Westfälischen Technischen Hochschule Aachen (RWTH Aachen) war beispielsweise der Software-Shop. Über diesen (bzw. dessen Nachfolger) können Einrichtungen bis heute Zugang zu zentral lizenzierter Software erhalten. Ein weiterer Dienst bietet lokal Verantwortlichen die Möglichkeit, selbstständig clientbezogene Back-up- und Restore-Aufgaben wahrnehmen zu können. Neuere Beispiele, bei denen Nutzende verwaltet werden müssen, sind Kollaborationsplattformen oder aber die Pflege dezentraler Informationen in einem zentralen Personenverzeichnis.

Alle Beispiele stellen Geschäftsprozesse dar, die mehrere Einrichtungen umfassen und bei denen die Notwendigkeit besteht, Personen eine Handlungsvollmacht zu erteilen. Diese

Vollmacht kann über die Grenzen der einzelnen an dem Prozess beteiligten Einrichtungen hinweg genutzt und interpretiert werden. Anders ausgedrückt: Ohne eine IT-taugliche, mit Identitäten verknüpfte Bearbeitung der Fragestellung, wer im Auftrag welchen Lehrstuhls oder welcher Einrichtung welche Aufgaben wahrnehmen darf oder soll, ist die Skalierbarkeit von IT-Services sehr eingeschränkt. Ein unverzichtbarer Baustein bei der Beantwortung ist ein Organisationsverzeichnis.

Motivation, ein Organisationsverzeichnis zu etablieren

Die Skalierbarkeit der IT-Versorgung hängt in hohem Maße von der Skalierbarkeit der Prozesse ab, mit denen Informationen schnell und sicher über lokale Zuständigkeiten und Vollmachten transportiert werden. Diese

> Die Skalierbarkeit der IT-Versorgung hängt in hohem Maße von der Skalierbarkeit der Prozesse ab.

Informationen gelangen von der Entscheidungsinstanz einer Einrichtung – meist der Leitung der jeweiligen Einrichtung oder Organisationseinheit – zu der Einrichtung, die die Informationen verarbeitet, beispielsweise zur IT-Einrichtung der Hochschule. Diese ist auf die Informationen angewiesen, um mit den benannten Ansprechpersonen zu einzelnen IT-Diensten Kontakt aufnehmen zu können oder – noch wesentlich häufiger – zu wissen, welche Person für die jeweilige Einrichtung verbindlich Aussagen treffen kann. Da der Zugriff auf Daten und Informationen gesteuert wird und darüber hinaus entlang dieser Geschäftsprozesse Kosten entstehen können, sind hier Authentizität, Integrität und Aktualität unverzichtbare Anforderungen an Pflege und Transport von Informationen.

Organisationseinheiten definieren

Damit IT-Prozesse – oder aber Geschäftsprozesse, die mittels IT-Services realisiert werden – geeignet unterstützt werden können, bedarf es eines weiter gefassten Organisationsbegriffs. Auf der Hand liegt, typische Einheiten wie Institute, Lehrstühle, Fachbereiche oder aber zentrale Einrichtungen wie die Universitätsbibliothek und die Abteilungen der Verwaltung als Organisationseinheiten einer Hochschule zu begreifen. Tatsächlich aber ist eine Hochschule kein geschlossener Organismus. Vielmehr involvieren zahlreiche Prozesse auch Einrichtungen in der unmittelbaren Umgebung einer Hochschule. Beispiele hierfür sind An-Institute (rechtlich selbstständige Einrichtungen innerhalb einer Hochschule), Forschungs-Campi oder auch Einrichtungen der akademischen Selbstverwaltung wie Fachschaften, studentische Initiativen und Gruppen, die mit der jeweiligen Hochschule interagieren. Auch Einrichtungen von Wissenschaftskooperationen wie der Max-Planck-Gesellschaft, Helmholtz-Gemeinschaft, Fraunhofer-Gesellschaft oder Leibniz-Gemeinschaft, die mit Lehrstühlen verbunden sind, gehören in diese Liste.

Prozesse vereinheitlichen

Sollen IT-gestützte Prozesse möglichst effizient funktionieren, so müssen sie für alle partizipierenden Einrichtungen einheitlich gestaltet werden. Demgegenüber führen Unterschiede in der Prozessgestaltung für die oben genannten hochschulinternen Einrichtungen, gegenüber den sonstigen Einrichtungen, zu einem hohem Maß an manuellem Betrieb und erheblichen Einschränkungen in der Skalierbarkeit der betroffenen IT-Services und Geschäftsprozesse. Der Grund ist, dass für Pflege und Transport von prinzipiell gleichartigen Informationen unterschiedliche Prozesse und Wege etabliert sind.

Eine Voraussetzung für eine homogene Prozessgestaltung ist ein Verzeichnis von Organisationseinheiten, das alle Organisationsformen sowie externe, in Geschäftsprozessen interagierende Einrichtungen einheitlich und konsistent erfasst. An diesem Punkt ist bei der Umsetzung erfahrungsgemäß eine Menge Überzeugungsarbeit zu leisten, denn es ist wenig sinnvoll, ein Verzeichnis für die „richtigen“ Einrichtungen und eines für die „anderen“ zu pflegen. Notwendig ist ein einheitliches, alle Einrichtungen umfassendes Verzeichnis.

Ein zentrales Verzeichnis für alle Prozesse

Fortschrittlich und wegweisend wird das Ganze nicht durch die dahinterliegende Technik, sondern durch eine alle Eventualitäten berücksichtigende Konzeption und Handhabung. Gemeint ist ein eigenständiges Verzeichnis, das offen für alle möglichen Arten von Organisationen ist, beispielsweise auch für temporäre Organisationen wie etwa Sonderforschungsbereiche.

Wichtig ist, dass dieses Verzeichnis für alle relevanten Prozesse der Hochschule zwingend vorgeschrieben, allgemein akzeptiert und von allen Einrichtungen verwendet wird. Dies impliziert auch abgestimmte Pflegeprozesse, um an möglichst zentraler Stelle zum Beispiel kooperierende Organisationen bereits im Rahmen der Kooperationsvereinbarung in das Organisationsverzeichnis aufzunehmen – und nicht erst dann, wenn IT-Services nachgefragt werden. In einer solchen Konstellation entsteht Mehrwert für die Gesamtorganisation und aus einer undifferenzierten Liste wird ein wertvolles Steuerungsinstrument für Prozesse. Eine Kategorisierung der Organisationen erlaubt es, lizenzierte Software oder die Teilnahme an hochschulinternen Buchungsprozessen nur bestimmten Organisationsformen zur Verfügung zu stellen.

Im Sinne der Unterstützung von IT-basierten Prozessen und der Bereitstellung von Services sollte dieses Organisationsverzeichnis als vorrangig betrachtet werden und sämtliche Organisationen umfassen,

Abbildung 1: Das Organisationsverzeichnis als Baustein für einrichtungsbezogene Prozesse

unabhängig davon, ob sie für einzelne Stakeholder wie Finanzwesen, Lehre oder Serviceerbringer relevant sind. Alle diese Stakeholder werden bereits in der einen oder anderen Form eine für sie relevante Liste von Organisationen haben, wie etwa eine Liste der Kostenstellen. Insofern sollte jede Hochschule bereits eine gute Basis für den Aufbau eines Organisationsverzeichnisses vorliegen haben.

Eindeutige Referenzen mittels Organisations-ID

Die Herausforderung liegt nun darin, mit einem zentralen Organisationsverzeichnis eine Gesamtschau zu ermöglichen und eine eindeutige Referenz zu erzeugen, die über die Zeit stabil und für jedwede Zuordnung von Daten oder Personen in Prozessen geeignet ist: eine Organisations-ID. Diese überlebt idealerweise Umbenennungen, Änderungen von Kostenstellen oder andere in Verwendung befindliche Referenzen der Organisationen in verschiedensten Systemen der Hochschule.

Die über eine unveränderliche ID hergestellte Zuordnung von Prozessen und Leistungen zu Organisationseinheiten kann von großem Nutzen sein: So ist auch bei hoher Personalfluktuation die Ermittlung einer aktuellen Ansprechperson möglich, wenn eine Maildomäne einer Organisation zugeordnet ist und nicht einer oder mehreren einzelnen Ansprechpersonen.

> Eine Organisationseinheit hat auch dann Zugriff auf einen Service, wenn alle Ansprechpersonen abhandengekommen sind.

Kombiniert man nun Organisationsverzeichnis und Rollenverwaltung in der Weise, dass eine Organisation als Kontext begriffen wird, in der Personen ihre Rollen wahrnehmen, kann sich in unserem Beispiel eine Organisationseinheit auch dann Zugriff auf einen Service verschaffen, wenn alle Ansprechpersonen (womöglich sukzessive) nicht mehr verfügbar sind. In dem Zusammenhang gibt man die Pflege der Ansprechpersonen direkt in die Hand derjenigen, die über die nötigen Informationen verfügen: die Leitung bzw. die Mitarbeitenden in der Organisationseinheit selbst. Diese Wege der Selbstverwaltung kommen erst an ihre Grenzen, wenn auch der letzte Rollenverwaltende einer Einrichtung nicht mehr zugegen ist. In diesem Fall kann die (möglicherweise neue) Leitung einer Organisationseinheit über einen organisatorischen Prozess mit den rollenverwaltenden Berechtigungen ausgestattet werden.

Am Beispiel wird deutlich, dass alle Service- und Supportprozesse, die sich aus der Bereitstellung von IT-Services in einer großen Organisation wie einer Hochschule ergeben, enorm von einem Organisationsverzeichnis profitieren können. Aber auch andersherum können nun Organisationseinheiten selbst Support für ihre eigenen „Kunden“ leisten wie die Pflege der eigenen Mitarbeiterinnen und Mitarbeiter in zentralen Diensten wie E-Mail.

Das Argument Sicherheit

Nicht zuletzt stellt ein Organisationsverzeichnis einen Sicherheitsgewinn dar. Wird eine Organisation an zentraler Stelle als nicht mehr existent markiert, bekommt sie einen Lifecycle, auf dessen Basis Dienste, die für diese Organisationseinheit erbracht wurden, strukturiert abgebaut werden können. Damit werden Systeme oder Accounts, die nicht mehr gepflegt werden, sowie sonstige Angriffsvektoren wesentlich reduziert. ◆

Innovationen zur Nachhaltigkeit in der IT

Wir leben in einer Zeit, in der scheinbar pausenlos um uns herum Innovationen entstehen. Doch wird oft übersehen, dass „innovativ“ nicht einfach „neu“ bedeutet, sondern eine Verbesserung darstellt. Ein digitaler Prozess ist nur dann innovativ, wenn er dem analogen überlegen ist. Heutzutage haben Verbesserungen oft auch einen nachhaltigen Effekt: Ressourcen werden geschont oder weniger Energie wird verbraucht. Besonders im IT-Bereich sind diese ökologischen Aspekte von Bedeutung. Damit sind Rechenzentren das Rückgrat der digitalen Transformation und der Treibstoff von Innovationen.

Text: **Jan Quaing** (Deutsche Bundesstiftung Umwelt, DBU)

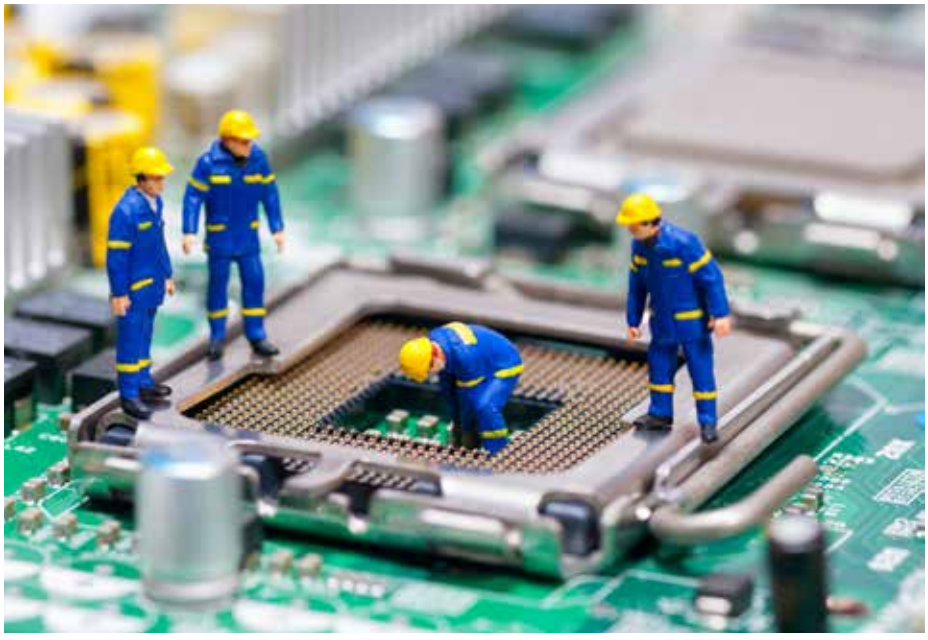


Foto: kirill_makarov/Adobe Stock

Bereits vor einigen Jahren, während des Booms der Kryptowährungen, rückte der hohe Energiebedarf von Rechenzentren stärker in den Fokus. Mit dem Aufkommen der Künstlichen Intelligenz (KI) hat der Energieverbrauch ein neues Niveau erreicht. So verbrauchte allein das Training des ersten ChatGPT-Modells (Version 3.5) so viel Strom wie 400 durchschnittliche deutsche Haushalte in einem Jahr (Albrecht 2023, 30). Und dies ist nur der Anfang: Der Bedarf wächst exponentiell.

Allein Microsoft plant, seine Kapazitäten bis Mitte 2025 zu verdreifachen. Der dafür notwendige Strom entspricht der Leistung von drei Atomkraftwerken oder dem gesamten Stromverbrauch Portugals in einem Jahr – private Haushalte und Industrie. Doch der immense Stromverbrauch, der Abbau seltener Erden für die Chipproduktion und die damit verbundenen Emissionen sind nur die Spitze des Eisbergs.

Ein weiteres Problem stellt die Kühlung der Server dar. Google verbrauchte im Jahr 2021 rund 13 Milliarden Liter Wasser – 90 Prozent davon Trinkwasser (Li et al. 2023, 1). Das entspricht dem jährlichen Wasserverbrauch aller privaten Haushalte einer Stadt wie Mönchengladbach. Die ökologischen Herausforderungen durch KI sind also erheblich – und sie nehmen weiter zu.

Im Hinblick auf die ökologische Nachhaltigkeit müssen die Auswirkungen von KI und Rechenzentren in größere Zusammenhänge eingeordnet und bewertet werden. Für innovative Ideen ist es nicht notwendig,

Foto: alan/Adobe Stock

Rechenzentren radikal neu zu gestalten. Es gibt jedoch konkrete Maßnahmen, um Rechenzentren nachhaltiger zu betreiben, sei es im eigenen Unternehmen oder in angemieteten Rechenzentren. Bereits kleinere Prozessinnovationen steigern den Nutzen für Kunden und Mitarbeitende und machen einzelne Prozessschritte effizienter. Solche Verbesserungen können zudem positiv für die Außenkommunikation genutzt werden.

Rechenzentren nachhaltig gestalten – mit Abwärme zur Beheizung

Die Kühlsysteme von Rechenzentren verbrauchen einen Großteil der Energie. Es gibt zwei Ansätze, um diesen Energieverbrauch zu senken: zum einen durch das Erhöhen der Toleranz bei der Betriebstemperatur der Server, zum anderen durch die Nutzung von Abwärme. Beide Ansätze haben jedoch Schwachstellen.

Der erste Weg ist kaum erforscht und erste Studien kommen zu dem Schluss, dass eine höhere Betriebstemperatur zwar die Kühlenergie reduziert, dies jedoch durch den steigenden Energieverbrauch wieder zunichtegemacht wird. Die Verfassenden einer der wenigen Studien betonen jedoch, dass eine individuelle Bewertung stets notwendig ist und netto auch zu einem positiven Ergebnis führen kann (Clement et al. 2022). Der zweite Ansatz stößt auf Umsetzungsprobleme, da die nötige Infrastruktur in Deutschland derzeit fehlt. Dennoch gibt es erste Vorreiter, wie das Dresdner Unternehmen Cloud & Heat Technologies GmbH, das durch eine intelligente Integration von Servern in Gebäuden die Abwärme zur Beheizung nutzt – etwa in einem der Finanztürme in Frankfurt/Main. Bei der Errichtung neuer Server sollte daher die Frage gestellt werden: Welche Bereiche können von der Abwärme profitieren? Müssen die Server vor Ort im Unternehmen stehen oder kann mit lokalen öffentlichen Einrichtungen kooperiert werden? Eine Erweiterung des Horizonts kann nicht nur ökologische, sondern auch ökonomische Vorteile bringen, da Heizenergie eingespart wird.

Während für die Abwärmenutzung derzeit noch flächendeckende Infrastrukturen fehlen, kann sie beim Bau neuer Zentren berücksichtigt werden – beispielsweise im eigenen Gebäude oder aber in Gebäuden der öffentlichen Nahversorgung wie Schwimmbädern oder Schulen, die damit beheizt werden.

Rechenzentren neu denken – mit innovativer Energienutzung

Auch im Bereich der Energienutzung gibt es erste Pilotprojekte, die alternative Ansätze verfolgen. Das Unternehmen windCORES (WestfalenWIND IT GmbH & Co. KG) hat sich beispielsweise entschieden, Rechenzentren im Sockel von Windrädern zu bauen. Dies hat zwei zentrale Vorteile: Zum einen wird bereits versiegelte Fläche sinnvoll genutzt, da Windräder innen hohl sind und abgesehen von einem kleinen Schaltschrank und einer Treppe leer stehen. Zum anderen profitieren diese Rechenzentren direkt von der Energieerzeugung, da Windräder von Zeit zu Zeit trotz vorhandenen Winds stillstehen, wenn das Netz überlastet ist. Bei windCORES bleiben die Windräder im Wind und versorgen die Rechenzentren, wodurch „überflüssiger" Strom effizient genutzt und die Energiekosten langfristig gesenkt werden. So können jährlich etwa 14 Tonnen CO_2 eingespart werden.

Ressourcennutzung – mit refurbished Hardware

Die Verwendung von refurbished Hardware schont nicht nur Ressourcen, sondern ist nachweislich auch zuverlässiger als neue Hardware. Die aufbereitete Hardware hat bereits gezeigt, dass sie zuverlässig läuft, was sogenannte Montagsmodelle und Fehler in der Produktion weitestgehend ausschließt.

Hinzu kommt, dass das Mooresche Gesetz zunehmend außer Kraft gesetzt wird. Die 1965 von Gordon Moore formulierte Prognose besagt, dass sich in regelmäßigem Zeitraum (je nach Quelle 12

Foto: Nuthawut/Adobe Stock

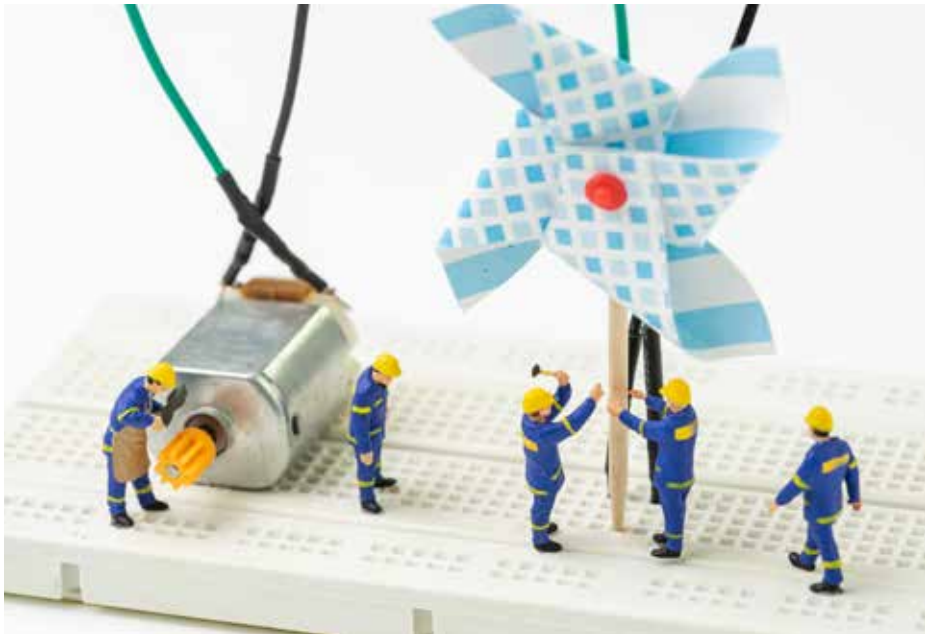


Foto: Nuthawut/Adobe Stock

oder 24 Monate) die Leistungsfähigkeit von Schaltkreisen verdoppelt und der Energiebedarf im gleichen Zeitraum halbiert. Kurzum: Technologie wird immer leistungsfähiger. Aufgrund physikalischer Grenzen hat sich diese Gesetzmäßigkeit immer weiter verlangsamt, bis zum aktuellen Zeitpunkt, zu dem es de facto außer Kraft gesetzt ist. Dies hat zur Folge, dass der Einsatz von bereits genutzter Hardware keinen elementaren Wettbewerbsnachteil gegenüber neuer Hardware darstellt – insbesondere nicht für Hardwarekomponenten ab 2016 (Wynne et al. 2022).

Experimente mit verschiedenen Serverkonfigurationen haben gezeigt, dass es nur minimale Leistungsunterschiede zwischen neuen und wiederaufbereiteten Servern gibt. Häufig reichen Speicher- und Prozessoraufrüstungen aus, um die Energieeffizienz zu steigern, ohne komplette Server austauschen zu müssen (Bashroush et al. 2022). Die Ergebnisse legen nahe, dass Strategien zur Servererneuerung Prinzipien der Circular Economy einbeziehen sollten, um Elektroschrott zu reduzieren und Energie zu sparen. Dies ist besonders bei Servern, die älter als fünf Jahre sind, ökologisch und wirtschaftlich von Vorteil. Interact, eine Anwendung für maschinelles Lernen, kann bei der Analyse unterstützen, indem sie einen 12-stufigen Prozess zur Bewertung des gesamten Lebenszyklus eines Servers durchläuft. Dabei werden Umwelt- und Kostenfaktoren wie der Energieverbrauch über die Zeit berücksichtigt, um fundierte Entscheidungen zu ermöglichen.

Für Interessierte von refurbished Hardware gibt es eine Vielzahl von Anbietern, die sowohl für Unternehmen als auch für Privathaushalte entsprechende Geräte aufbereiten – stets mit Garantieanspruch. Zwei Unternehmen, die zudem viel Herzblut in dieses Geschäft stecken, sind AfB social & green IT und Techbuyer. Während AfB die ökologische Komponente um eine soziale erweitert, indem sie verschiedenen Menschen eine Chance auf Arbeit gibt, unterstreicht Techbuyer sein Geschäftsmodell durch kontinuierliche Forschung und Aufklärung über Sekundärhardware. So wird der klare Mehrwert von refurbished Hardware aufgezeigt.

Für eine konsequente nachhaltige Serverinfrastruktur ist das regulatorische Rahmenwerk unerlässlich. Akteure brauchen eine verbindliche Richtschnur, an der Aktivitäten ausgerichtet werden können. Dennoch lohnt es sich bereits heute, Rechenzentren nachhaltiger zu gestalten, wie die genannten Beispiele zeigen. Ebenfalls darf die kollektive Macht nicht unterschätzt werden. Möchten Sie etwas ändern, suchen Sie sich Gleichgesinnte und versuchen Sie, Ihre Interessen in die Politik zu tragen. Gemeinsam kann so Zukunft gestaltet werden. ◆

QUELLEN

Bashroush, Rabih; Rteil, Nour; Kenny, Richard und Wynne, Astrid (2022)
Optimizing Server Refresh Cycles: The Case for Circular Economy With an Aging Moore's Law. In IEEE Transactions on sustainable computing, VOL. 7, No. 1. 2022

Clement, Stephen; Burdett, Kat; Rteil, Nour; Wynne, Astrid und Kenny, Richard (2022)
Is Hot IT a False Economy? An Analysis of Server and Data Center Energy Efficiency as Temperatures Rise. In IEEE Transactions on sustainable computing, VOL. 9, NO. 3. 2022

Wynne, Astrid; Rteil, Nour und Kenny, Richard (2022)
Das technische Argument für Server in der Circular Economy. Über die Vorteile von refurbished Hardware. In Böckel, Alexa; Quaing, Jan; Weissbrod, Ilka und Böhm, Julia (2022) Mythen der Circular Economy. Seite 67–74

Interact: CEDaCI-Projekt
Unique european reasearch project uses Interact's energy efficiency metrics and cost projections: **https://interactdc.com/static/images/documents/Interact_Case_Study_CEDaCI.pdf** (zuletzt abgerufen 18.09.2024)

Systemische Risiken riesiger Systeme

Sehr große Onlineplattformen müssen unter dem DSA systemische Risiken erkennen und bekämpfen

Seit einem Jahr gelten die spezifischen Regelungen des Digital Services Act (DSA) für sehr große Onlineplattformen und Suchmaschinen. Das Herzstück bilden Pflichten zum Umgang mit systemischen Risiken wie etwa Suchtpotenzial oder der Verbreitung von Hetze und Desinformation. Allerdings besteht ein erhebliches Risiko, dass die Plattformen ihre neuen Pflichten nur unzureichend umsetzen, um ihre lukrativen Geschäftsmodelle zu schützen.

Text: **Nikolaus von Bernuth** (Forschungsstelle Recht im DFN)

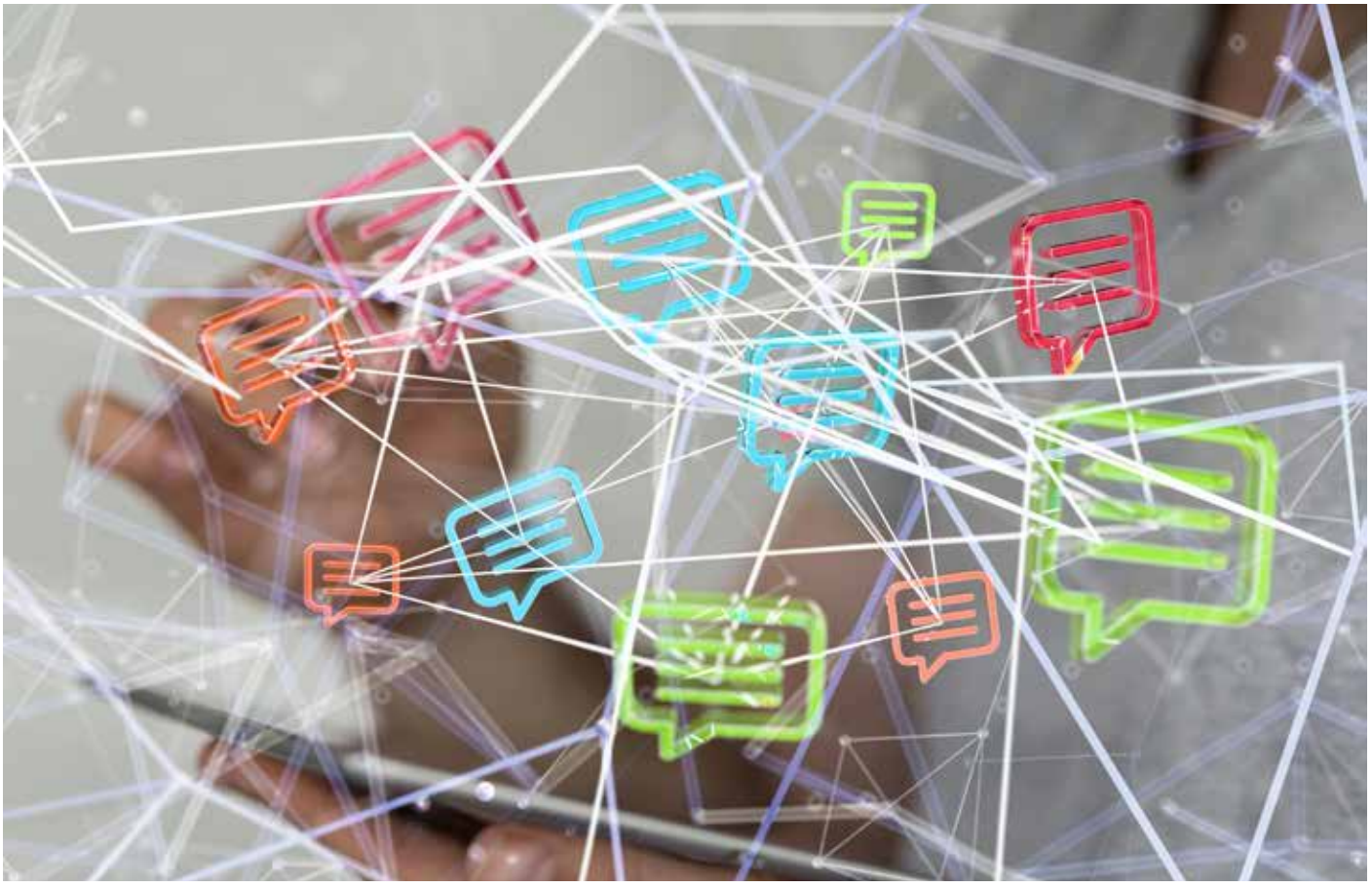


Foto: Wirestock

I. Die Macht der sehr großen Onlineplattformen

Es gehört mittlerweile zu den Binsenweisheiten der netzpolitischen Debatte, auf die Macht der sehr großen Onlineplattformen und Suchmaschinen hinzuweisen. Sie sind nicht nur Dienste, mithilfe derer Menschen individuell miteinander kommunizieren und Inhalte teilen. Das Internet und Onlineplattformen im Speziellen sind zu einer der meistgenutzten Quellen für Nachrichten geworden. Im Jahr 2024 verwendet jede/-r Dritte in Deutschland zum Empfang von Nachrichten im Internet neben Onlineauftritten klassischer Medien auch soziale Netzwerke.[1] In der Altersgruppe bis 35 Jahre ist es sogar die Hälfte.

Welche Inhalte diese Menschen zu sehen bekommen, richtet sich nicht nur danach, wem sie selbst und ihr eigenes Netzwerk folgen. Maßgeblich werden die Inhalte auf den Onlineplattformen durch Algorithmen und Empfehlungssysteme zusammengestellt. Diese wiederum sind darauf ausgerichtet, das werbegestützte Geschäftsmodell zu optimieren. Der DSA will diese Algorithmen und Empfehlungssysteme transparenter machen.[2] Die zentralen Parameter müssen in den Allgemeinen Geschäftsbedingungen (AGB) bekannt gemacht werden (Art. 27 Abs. 1 DSA). Bei sehr großen Plattformen muss eine Option ohne Profiling wählbar sein (Art. 38 DSA). Dennoch: Für einzelne Nutzende bleibt der Einfluss begrenzt. Dies gilt umso mehr für Plattformen bzw. Funktionen wie TikTok, Instagram Reels oder YouTube Shorts, die ihre Inhalte fast ausschließlich aufgrund von Algorithmen zusammenstellen.

Die sehr großen Onlineplattformen und Suchmaschinen haben eine kaum zu überschätzende Bedeutung für die öffentliche Meinungsbildung und Debatte – und durch ihre Algorithmen entsprechende Macht darüber. Mit dem DSA ist es der EU nun erstmals gelungen, spezifische Regelungen einzuführen, die diese Machtverhältnisse und die hiervon ausgehenden gesellschaftlichen Gefahren in den Blick nehmen. Dieser Beitrag wird die Pflichten zur Ermittlung, Analyse, Bewertung und anschließenden Minderung systemischer Risiken auf Onlineplattformen und Suchmaschinen in Art. 34, 35 DSA näher erläutern. Zunächst bietet sich in diesem Zusammenhang aber die Gelegenheit zu erläutern, wen genau die neuen Regelungen betreffen.

II. Was genau sind sehr große Onlineplattformen?

Der DSA verfolgt einen risikobasierten Ansatz. Das intensivste Pflichtenprogramm trifft also nur wenige Adressaten, von denen nach Ansicht des Gesetzgebers eine besonders hohe Gefahr ausgeht. Dies sind Onlineplattformen und Onlinesuchmaschinen mit mehr als 45 Mio. aktiven monatlichen Nutzenden in der EU (Art. 33 Abs. 1 DSA).[3]

Onlineplattformen sind solche Vermittlungsdienste, die Informationen im Auftrag ihrer Nutzenden speichern und öffentlich verbreiten und bei denen dies keine unwesentliche Nebenfunktion darstellt (Art. 3 lit. i DSA).[4] Dazu gehören etwa soziale Netzwerke, Videosharing-Plattformen oder Onlinemarktplätze. Aber auch Wikipedia als Onlineenzyklopädie oder Google Maps als Kartendienstleister fallen in die Kategorie Online-Plattform. Messengerdienste wie WhatsApp oder Signal hingegen verbreiten die Informationen (bspw. eine Chatnachricht) nicht öffentlich, jedenfalls nicht an eine beliebige Öffentlichkeit. Sie sind also nur Dienste der reinen Durchleitung von Informationen und keine Onlineplattformen. Ein Spezialfall ist Telegram: Anfangs stand die Individualkommunikation hier ebenfalls im Fokus. Doch seit einiger Zeit werden die Kanäle, auf denen Inhalte an eine beliebige Öffentlichkeit verbreitet werden können, immer bedeutsamer und prägender für den Dienst. Sie sind (nicht nur, aber auch) zentrale Sprachrohre für rechte Hetze, Verschwörungstheorien oder Desinformationskampagnen.[5] Daher ist die öffentliche Verbreitung keine unwesentliche Nebenfunktion mehr – Telegram ist eine Onlineplattform. Streitig ist bislang aber, ob Telegram genug Nutzende hat, um sich auch an die strengsten Pflichten des DSA halten zu müssen, unter anderem also die Pflichten zur Risikobewertung und Risikominderung.[6]

Suchmaschinen sind keine Onlineplattformen, denn ihr Service besteht nicht in der

1 Reuters Institute Digital News Report 2024: Ergebnisse für Deutschland, S. 16f, https://www.ssoar.info/ssoar/handle/document/94461 (zuletzt abgerufen am 14.08.2024).

2 Grundlegend zum DSA: Gielen, Digital Services Act: Das Plattformgrundgesetz?, DFN-Infobrief Recht 03/2021; Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 06/2022; John, Geschenke verpacken leicht gemacht: Transparenz ist in!, DFN-Infobrief Recht 12/2023; siehe auch von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

3 Zur Anwendbarkeit ist eine Benennung durch die Europäische Kommission erforderlich. Die Liste aller 25 bisher benannten Onlineplattformen und Suchmaschinen findet sich hier: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (zuletzt abgerufen am 15.08.2024).

4 Eine unwesentliche Nebenfunktion sind etwa die Kommentarspalten in Onlineauftritten einer Zeitung, so explizit Erwägungsgrund 13 DSA.

5 Telegram ist etwa zentrales Medium der rechtsextremen „Freien Sachsen“, ebenfalls für russische Propaganda: https://correctiv.org/faktencheck/hintergrund/2024/04/10/telegram-analyse-desinformation-russland-vernetzt-sich-um-alina-lipp-in-deutschland-mit-propaganda-fakes-zum-ukraine-krieg/ (zuletzt abgerufen am 15.08.2024).

6 Telegram meldete „nur“ 41 Mio. aktive Nutzerinnen und Nutzer„ die EU-Kommission zweifelt aber an diesen Zahlen, https://www.inside-it.ch/eu-nimmt-sich-wohl-telegram-an-20240529# (zuletzt abgerufen am 15.08.2024).

öffentlichen Verbreitung von Informationen, sondern in der Such- und Auflistungsfunktion.[7] Für Suchmaschinen mit über 45 Mio. aktiven Nutzenden (zurzeit: Google Search und Bing) gelten die besonders strengen Pflichten der Art. 33–48 DSA aber ebenfalls.

III. Haftungsbefreiung für Freiheit im Netz

Über viele Jahre konnten sich die großen Onlineplattformen in einem ausgesprochen innovationsfreundlichen Rechtsrahmen entwickeln und waren kaum Haftungsrisiken und Sorgfaltspflichten ausgesetzt. Die E-Commerce-Richtlinie von 2001 sah eine weitgehende Haftungsbefreiung vor: Onlineplattformen waren für Inhalte, die Nutzende hochgeladen hatten, regelmäßig nicht verantwortlich.

Der DSA hält an diesem Grundkonzept fest. Eine grundsätzliche Haftungsprivilegierung ist erforderlich, damit die Kommunikationsfreiheiten so ausgeübt werden können, wie es mittlerweile selbstverständlich ist. Würden Onlineplattformen unmittelbar für alle Inhalte haften, wäre ein freier, ungefilterter Austausch von Inhalten undenkbar.

Dennoch hat sich gezeigt, dass die Plattformen mehr Verantwortung tragen müssen. Die Gefahren, die die Freiheit im Netz zwangsläufig mit sich bringt, zeigten sich in den vergangenen Jahren immer deutlicher. Hassrede, systematische Rechtsverletzungen und Desinformation haben spürbar zugenommen – ihre Auswirkungen zeigen sich etwa in sensiblen demokratischen Momenten wie Wahlen oder gesellschaftlichen Krisen.[8] Verschärft werden diese Gefahren durch die spezifische Funktions- und Wirkweise der sehr großen Onlineplattformen. An genau dieser Stelle setzen die Pflichten zur Risikobewertung und Risikominderung in Art. 34, 35 DSA an.

IV. Systemische Risiken

Nach Art. 34 Abs. 1 DSA müssen die benannten sehr großen Onlineplattformen ermitteln, welche systemischen Risiken von dem Betrieb ihrer Dienste ausgehen und diese anschließend analysieren und bewerten. Mindestens einmal jährlich muss die Risikobewertung erfolgen sowie stets dann, wenn die Plattform eine neue Funktion mit Risikopotenzial einführt.[9]

Der Begriff „systemische Risiken“ ist aus der Bankenregulierung bekannt.[10] Systemische Risiken sind mehr als nur die Summe der einzelnen Beschwerden und Rechtsverstöße, die an die Plattformen herangetragen werden. Das Ziel ist insbesondere die Ermittlung struktureller Risiken, die mit dem Betrieb sehr großer digitaler Dienste einhergehen und die sich aus der Analyse des eigenen Dienstes und den – ohnehin gesammelten – Nutzungsdaten ergeben: Welche Gefahren oder negativen Auswirkungen treten immer wieder auf und lassen sich auf die Funktionsweise des eigenen Dienstes zurückführen? „Systemisch“ stellt zudem einen Bezug zur europäischen Grundordnung her, die in ihrer Funktionsfähigkeit oder Stabilität durch diese Risiken gefährdet sein muss. Der DSA gibt vier Kategorien von systemischen Risiken auf Onlineplattformen vor (Art. 34 Abs. 1 DSA).

Erstens ist dies die Verbreitung rechtswidriger Inhalte über den Dienst. Rechtswidrig sind alle Inhalte, die gegen das Unionsrecht oder das Recht eines Mitgliedstaats verstoßen. Typischerweise wird es etwa um die Verbreitung von strafbarer Hassrede, Missbrauchsdarstellungen auf Videosharing-Plattformen oder den massenhaften Verkauf gefälschter Güter gehen.[11] Plattformen müssen also prüfen, ob ihre Funktionsweise gerade solche Praktiken besonders begünstigt bzw. systematisch zulässt.

Zweitens sind dies die tatsächlichen oder absehbaren Auswirkungen auf die Ausübung der Grundrechte. Hier soll ausweislich der Erwägungsgründe der Fokus insbesondere auf der Meinungsfreiheit, dem Recht auf Nichtdiskriminierung sowie dem Jugendschutz liegen. Aber auch die Auswirkungen auf andere Grundrechte durch die Funktionen und Algorithmen der Plattformen sollen beobachtet werden.

Drittens werden als systemische Risiken die Auswirkungen auf die gesellschaftliche Debatte, auf Wahlprozesse und die öffentliche Sicherheit definiert. Hierunter wird in der rechtswissenschaftlichen Literatur insbesondere Desinformation eingeordnet, außerdem Phänomene wie Filterblasen und Echokammern.[12] An dieser Stelle findet sich also eine der wenigen gesetzlichen Regelungen zu Desinformation, die in den

7 Im Einzelnen ist die Kategorisierung von Suchmaschinen sehr streitig. Definiert werden Onlinesuchmaschinen in Art. 3 lit. j DSA. Der Übersichtlichkeit halber wird im weiteren Beitrag hinsichtlich der Adressaten der Art. 34, 35 DSA von (Online-)Plattformen gesprochen, wobei Suchmaschinen mit eingeschlossen sind.

8 Dem Brexit-Referendum sowie der Wahl Donald Trumps 2016 wird nachgesagt, durch Desinformation erheblich beeinflusst worden zu sein. Exemplarisch sind auch die jüngsten Ausschreitungen in Großbritannien.

9 Gegen die Prüfpflicht bei Einführung verstieß aus Sicht der Kommission TikTok Lite, zum Hintergrund siehe https://ec.europa.eu/commission/presscorner/detail/de/IP_24_2227 (zuletzt abgerufen am 15.08.2024).

10 Einen Vergleich zu diesem Sektor ziehend: Broughton Micova/Calef, Elements for Effective Risk Assessment under the DSA, 2023, https://www.ssrn.com/abstract=4512640 (zuletzt abgerufen am 15.08.2024).

11 Aufschlussreich für die Auslegung der systemischen Risiken sind die Erwägungsgründe 80–84 zum DSA.

12 *Kaesling*, in: Hofmann/Raue, Digital Services Act, 1. Auflage, 2023, Art. 34 DSA, Rn. 102ff; siehe auch das erste förmliche Verfahren gegen X: https://ec.europa.eu/commission/presscorner/detail/de/ip_23_6709 (zuletzt abgerufen am 15.08.2024).

Erwägungsgründen des DSA als eine der zentralen Gefahren auf Onlineplattformen ausgemacht wird.[13]

Zuletzt fallen unter die vierte Kategorie systemischer Risiken die nachteiligen Auswirkungen auf geschlechtsspezifische Gewalt, öffentliche Gesundheit, Jugendschutz oder das körperliche und geistige Wohlbefinden einer Person. In diese Kategorie fällt etwa das Suchtpotenzial (gerade für Jugendliche), das von der Gestaltung vieler Onlineplattformen ausgeht. Außerdem kann auch hier laut den Erwägungsgründen Desinformation ein Risikofaktor sein – etwa für die öffentliche Gesundheit, wie es sich während der Coronapandemie eindrücklich gezeigt hat.

Die Auflistung systemischer Risiken ist nicht abschließend. Weil die benannten Risiken aber sehr weit formuliert sind (etwa „Auswirkungen auf die Grundrechte"), werden sie einen erheblichen Teil der systemischen Risiken der sehr großen Onlineplattformen erfassen.

V. Ermitteln, Analysieren und Bewerten

Zur Ermittlung systemischer Risiken gibt der DSA außerdem besonders relevante Parameter zur Hand, die die Plattformen analysieren müssen. Dies sind (Art. 34 Abs. 2 DSA):

a. die Gestaltung ihrer Empfehlungssysteme und anderer relevanter algorithmischer Systeme,
b. ihre Systeme zur Moderation von Inhalten,
c. ihre anwendbaren allgemeinen Geschäftsbedingungen und ihre Durchsetzung,
d. Systeme zur Auswahl und Anzeige von Werbung,
e. ihre datenbezogene Praxis.

In ihren jährlichen Berichten müssen die Plattformen jedenfalls hinsichtlich dieser explizit benannten Parameter für die Risikobewertung Rechenschaft ablegen. Sie müssen also beispielsweise darlegen, inwieweit ihre Empfehlungssysteme zur Verbreitung von Desinformation beitragen oder zu Sucht- und Abhängigkeitsverhalten führen. Dies wurde TikTok Lite zum Verhängnis: Aus Sicht der Kommission hat TikTok die Suchtrisiken der Funktion, die mit Belohnungssystemen arbeitet, nicht ausreichend untersucht – inzwischen hat TikTok die Funktion auf dem europäischen Markt gänzlich zurückgezogen.[14] Auch gegen Facebook und Instagram läuft ein Verfahren, weil diese das Suchtpotenzial der Dienste nicht ausreichend analysiert haben.[15]

Im Übrigen gibt es mangels Erfahrungen mit den neuen Sorgfaltspflichten erst wenig Beispielsfälle, aus denen sich ableiten lässt, wie Risikoermittlung, Analyse und Bewertung durch die Plattformen im Detail auszusehen haben. In der Zivilgesellschaft finden sich schon einige Vorschläge,[16] entscheidend wird aber der von den Plattformen beschrittene Weg sein. Die Pflichten folgen dem Prinzip überwachter Selbstregulierung. Die Plattformen ermitteln und bewerten ihre systemischen Risiken eigenständig. Insbesondere ist es ihnen überlassen, welche Konsequenzen sie aus den ermittelten systemischen Risiken ableiten. Diese Selbstregulierung ist aber überwacht: Sie müssen sich unabhängigen Prüfungen unterziehen (Art. 37 DSA) und unterliegen der Aufsicht durch die Kommission.

VI. Eigenständige Risikominderung

Art. 35 DSA verpflichtet die Onlineplattformen dazu, wirksame und angemessene Maßnahmen zu ergreifen, um die ermittelten systemischen Risiken zu reduzieren. Welche dies sind, kann die Plattform selbst entscheiden – dies ist auch Ausdruck ihrer unternehmerischen Freiheit. Die Maßnahmen müssen aber auf die ermittelten Risiken zugeschnitten sein. Art. 35 Abs. 1 DSA schlägt eine ausführliche Liste von möglichen Maßnahmen vor. Er umfasst unter anderem die Anpassung von Onlineschnittstellen, Empfehlungssystemen und Algorithmen, der Werbesysteme sowie eine Kennzeichnung für manipulierte Inhalte.

Wenn die Plattform also beispielsweise feststellt, dass die automatisierte Inhaltemoderation durch Nutzung algorithmischer Filtersysteme[17] zu einem fortdauernden Overblocking eigentlich rechtmäßiger Inhalte führt, muss sie hierin ein systemisches Risiko für die Meinungsfreiheit der Nutzenden erkennen. Sie muss dann etwa das algorithmische System verbessern oder verstärkt Entscheidungen durch Mitarbeitende überprüfen lassen. Sollte hingegen ein Underblocking (rechtswidrige Inhalte werden nicht erkannt) Ergebnis der Risikoanalyse sein, müsste auch darauf gerichtet der Algorithmus verbessert werden.

Bei allen Minderungsmaßnahmen haben die Plattformen die Auswirkungen auf die Grundrechte besonders zu berücksichtigen. Daher gilt es, unnötige Beschränkungen für die Nutzung der Dienste zu vermeiden.[18] Die Minderungsmaßnahmen müssen zum Ziel haben, nicht einzelne Nutzende von der Plattform auszuschließen oder den

13 Erwähnung findet Desinformation in den Erwägungsgründen 2, 9, 68, 83, 84, 95, 104, 106, 108.
14 https://ec.europa.eu/commission/presscorner/detail/en/IP_24_4161 (zuletzt abgerufen am 15.08.2024).
15 https://ec.europa.eu/commission/presscorner/detail/de/ip_24_2664 (zuletzt abgerufen am 15.08.2024).
16 AlgorithmWatch: https://algorithmwatch.org/en/wp-content/uploads/2023/08/AlgorithmWatch_Risk_Assessment-DSA.pdf; cerre: https://cerre.eu/wp-content/uploads/2023/07/CERRE-DSA-Systemic-Risk-Report.pdf (zuletzt abgerufen am 15.08.2024).
17 Zur Zulässigkeit nach Urteil des EuGH vom 26.04.2022 (Az. C 401/19) siehe Schaller, Alea iacta est: Uploadfilter bleiben, DFN-Infobrief Recht 08/2022.
18 Erwägungsgrund 86 S. 3 DSA.

Dienst insgesamt auszusetzen, sondern die Plattform so zu gestalten, dass es möglichst wenig Anlass für Sperrmaßnahmen gibt.

Aufschlussreich ist auch, dass der Gesetzgeber den Terminus Risikominderung und nicht etwa Beseitigung gewählt hat. Eine vollständige Beseitigung eines Risikos geht regelmäßig mit ungewollten grundrechtlichen Einschnitten einher. So könnte eine vollständige Filterung von Nachrichtenbeiträgen nicht verifizierter Accounts vor Desinformation schützen – der Eingriff in die Presse- und Meinungsfreiheit wäre aber enorm. Für eine gute Balance soll eine Maßnahme die identifizierten Risiken also nicht zwangsläufig beseitigen, sondern in grundrechtssensibler Weise mindern.

VII. Aufsicht

Wirksam ist der Pflichtenkatalog nur dann, wenn die Aufsicht effektiv und kompetent ist. Das Risikomanagement des DSA schlägt viel vor, verpflichtet aber zu wenig Konkretem. Die Plattformen können nicht nur über die Maßnahmen eigenständig befinden, sie sind auch diejenigen, die die Bewertungsgrundlage dafür schaffen, indem sie ihre systemischen Risiken eigenständig analysieren. Das macht die Beaufsichtigung höchst komplex. Es wird wohl einige Jahre brauchen, bis die Aufsichtsbehörden aus einer vergleichenden Analyse der Praxis verschiedener Plattformen ableiten können, welche Plattform ihr Risikomanagement ernst nimmt und welche nicht.

Zuständig für die Aufsicht über die Pflichten gem. Art. 34, 35 DSA ist die Europäische Kommission. Sie kann Bußgelder von bis zu sechs Prozent des Jahresumsatzes verhängen, je nach Plattform also zweistellige Milliardenbeträge. In den ersten Monaten zeigte sie sich als äußerst engagierte Aufsichtsbehörde, die bereits eine Vielzahl an Verfahren gegen die sehr großen Plattformen einleitete. Manche von ihnen hatten auch die Pflichten zum Risikomanagement zum Gegenstand, unter anderem in den genannten Verfahren gegen TikTok, Meta und X.[19] Das Gremium für digitale Dienste[20] wird mit der Kommission in Kürze auch den ersten Bericht veröffentlichen, der die wesentlichen Erkenntnisse nach einem Jahr Aufsicht über das Risikomanagement der Plattformen enthält.

VIII. Bedeutung für die Wissenschaft und Fazit

Onlineplattformen sind für die moderne Informationsgesellschaft zentral. Insofern profitiert auch die Wissenschaft von sicheren Onlineplattformen, auf denen sich Menschen frei austauschen können und die nicht von Desinformation, Verschwörungstheorien und Hetze geprägt sind. Viele Studierende beziehen auch Studieninhalte über sehr große Onlineplattformen. Spezifische Rechte oder Pflichten in Bezug auf die Wissenschaft enthalten Art. 34, 35 DSA nicht. Allerdings könnte die Forschung von den Informationen profitieren, die aus den Berichten über das Risikomanagement hervorgehen werden. Sie dürften wertvolle Einblicke in den Maschinenraum der Plattformen geben.

Daneben bleibt der Datenzugang für Forschende nach Art. 40 DSA die wichtigste DSA-Regelung für die Wissenschaft.[21] Er ermöglicht es, die systemischen Risiken der Plattformen genauer zu erforschen. Zu diesem Zweck können Forschende bei der Bundesnetzagentur eine Zulassung für einen solchen Datenzugang beantragen. Bei Erfüllung aller Kriterien (Art. 40 Abs. 8 DSA) vermittelt sie dann den Zugang.[22]

Der DSA hat für die sehr großen Onlineplattformen und Suchmaschinen anspruchsvolle Pflichten etabliert, deren Herzstück die Pflichten zur Risikobewertung und Risikominderung sind. Nehmen die Plattformen ihre Verantwortung ernst, ist das Potenzial beachtlich. Es scheint möglich, durch die gezielte Verbesserung von Funktionen, Algorithmen und Empfehlungssystemen die Risiken, die von den Plattformen ausgehen, maßgeblich zu reduzieren. Fraglich ist allein, ob die Plattformen eigenständig ausreichende Maßnahmen ergreifen werden. Sie haben nicht zufällig die heutige Form angenommen, sondern wurden konsequent zur Optimierung ihres werbegestützten Geschäftsmodells gestaltet. Systemische Risiken wie Suchtverhalten sind aus plattformökonomischer Perspektive Chancen, den eigenen Gewinn zu steigern. Daher wird der Erfolg der neuen Pflichten ganz entscheidend von der Qualität der Aufsicht abhängen. Das Handeln der Kommission weckt hier nach der ersten Jahresbilanz durchaus Hoffnung. ◆

19 Auch AliExpress und diverse Plattformen mit pornografischen Inhalten sind von Verfahren betroffen, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (zuletzt abgerufen am 15.08.2024).

20 Das Gremium für digitale Dienste setzt sich aus Vertreterinnen und Vertretern der Koordinatoren für digitale Dienste der einzelnen Mitgliedstaaten sowie der Kommission zusammen, vgl. von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

21 Genauer nachzulesen bei John, Geschenke verpacken leicht gemacht: Transparenz ist in!, DFN-Infobrief Recht 12/2023.

22 Siehe von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

Europäische Sandkästen für KI

Mit der KI-Verordnung regelt die EU erstmals die Erprobung und Entwicklung von KI unter realen Bedingungen

Die KI-Verordnung enthält neben einer Reihe von Regelungen zur Risikominimierung auch gesetzgeberische Instrumente zur Innovationsförderung. Die wichtigsten dieser Instrumente sind die sogenannten „regulatory sandboxes“ – im Deutschen auch „KI-Reallabore“ genannt.

Text: **Philipp Schöbel** (Forschungsstelle Recht im DFN)

Foto: AI-generated Sandcastel/Freepik

I. Die KI-Verordnung und die Wissenschaftsfreiheit

Die KI-Verordnung (KI-VO) ist am 1. August 2024 in Kraft getreten und soll ab 2026 weitestgehend gelten. Sie soll Innovation fördern, die Freiheit der Wissenschaft respektieren und die Forschungs- und Entwicklungstätigkeit fördern. Von ihrem Anwendungsbereich ausgenommen sind sowohl Forschung mit KI als auch Forschung an KI: Erstens erfasst die Verordnung nicht KI-Systeme oder KI-Modelle, die allein zum Zweck der wissenschaftlichen Forschung entwickelt und eingesetzt werden. Das Gleiche gilt zweitens für Forschungs-, Test- und Entwicklungstätigkeiten, die stattfinden, bevor ein KI-System auf den Markt gebracht oder eingesetzt wird – es sei denn, sie werden unter realen Bedingungen durchgeführt, also „in der echten Welt". Die Ausnahmen für die Forschung mit und an KI gelten nur für die Vorschriften der KI-VO und nicht für andere europäische Rechtsakte.

Die Verordnung ermöglicht es, KI-Systeme unter realen Bedingungen in sogenannten „regulatory sandboxes" (KI-Reallaboren) zu testen und zu entwickeln. Damit wirkt sich die KI-VO direkt auf die Arbeit von Wissenschaftlerinnen und Wissenschaftlern aus. Der europäische Gesetzgeber betont, dass jede Forschungstätigkeit im Einklang mit anerkannten ethischen und professionellen Standards für wissenschaftliche Forschung und im Einklang mit sonstigem geltenden EU-Recht durchgeführt werden sollte.[1]

II. „Regulatory Sandboxes": Was sind KI-Reallabore?

Reallabore sind keine Eigenart der KI-VO. Sie sind aus der Regulierung von Finanzwesen, Luftfahrt, Verkehr und Energiewirtschaft bekannt.[2] In Deutschland hat das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ein Konzept für ein Reallaboregesetz vorgestellt.[3] Der Konsultationsprozess ist inzwischen beendet.[4] Ein offizieller Gesetzesentwurf wurde bisher nicht veröffentlicht.

Obwohl der Gesetzgeber das regulatorische Instrument breit einsetzt, fehlt bislang eine einheitliche Definition. Ähnliche Konzepte sind etwa Living Labs, Innovationslabore und Realexperimente.[5] Der Rat der Europäischen Union versteht unter Reallaboren einen zeitlich und räumlich begrenzten Testraum, in dem strukturierte Bedingungen für Experimente und Entwicklung unter regulatorischer Aufsicht geschaffen werden.[6]

Die KI-VO orientiert sich an diesem Verständnis und definiert ein KI-Reallabor als einen von der zuständigen nationalen Behörde eingerichteten kontrollierten Rahmen. Dieser Versuchsrahmen soll es Anbietenden[7] ermöglichen, ein innovatives KI-System gemäß einem vorher vereinbarten Plan für eine begrenzte Zeit unter behördlicher Aufsicht zu entwickeln, zu trainieren, zu validieren und gegebenenfalls unter realen Bedingungen zu testen. In einem solchen vereinbarten Plan müssen die Anbietenden in Zusammenarbeit mit der zuständigen Behörde Folgendes gemeinsam festlegen:

- Ziele,
- Bedingungen,
- Zeitrahmen,
- Methode und
- Anforderungen an die im Reallabor durchgeführten Tätigkeiten.

Für die konkrete Umsetzung von KI-Reallaboren belässt die KI-VO den Akteuren einen weiten Gestaltungsspielraum: KI-Reallabore können unterschiedlich konzipiert sein; die KI-VO gibt keine „one-size-fits-all"-Lösung vor. Das KI-Reallabor sowie die zu entwickelnden Anwendungen und Produkte können physischer, digitaler oder hybrider Natur sein.

---

1 Vgl. Erwägungsgrund 25 KI-VO.

2 Rat der Europäischen Union, Schlussfolgerungen des Rates zu Reallaboren und Experimentierklauseln als Instrumente für einen innovationsfreundlichen, zukunftssicheren und resilienten Rechtsrahmen zur Bewältigung disruptiver Herausforderungen im digitalen Zeitalter, 16. November 2020, S. 3, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/de/pdf (zuletzt abgerufen am 10.07.2024).

3 BMWK, Neue Räume, um Innovationen zu erproben – Konzept für ein Reallabore-Gesetz, 2021, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/konzept-fur-ein-reallabore-gesetz.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 10.07.2024).

4 BMWK, Pressemitteilung vom 10. Juli 2023, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Textsammlungen/Digitale-Welt/reallabore-konsultation.html (zuletzt abgerufen am 10.07.2024).

5 BMWK, BMWi-Strategie - Reallabore als Testräume für Innovation und Regulierung, 2018, S. 4, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-reallabore.pdf?__blob=publicationFile&v=10 (zuletzt abgerufen am 10.07.2024).

6 Rat der Europäischen Union, Schlussfolgerungen des Rates zu Reallaboren und Experimentierklauseln als Instrumente für einen innovationsfreundlichen, zukunftssicheren und resilienten Rechtsrahmen zur Bewältigung disruptiver Herausforderungen im digitalen Zeitalter, 16. November 2020, S. 4, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/de/pdf (zuletzt abgerufen am 10.07.2024).

7 Zum Begriff „Anbietende" siehe Seite 57.

III. Ziele der KI-Reallabore

Der Gesetzgeber geht von der Prämisse aus, dass KI eine sich rasch entwickelnde Technologiefamilie ist, die eine regulatorische Aufsicht erfordert. Die Verordnung adressiert bei der Einrichtung von KI-Reallaboren Anbietende von KI. Anbieter oder Anbieterinnen sind die Personen, die ein KI-System entwickeln oder entwickeln lassen und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen.

KI-Reallabore sollen Innovation und Wettbewerbsfähigkeit fördern. Zugleich soll die kontrollierte Versuchs- und Testumgebung für die Entwicklungsphase sicherstellen, dass die entwickelte KI die rechtlichen Anforderungen der KI-VO und anderer einschlägiger Rechtsvorschriften erfüllt. Für die Anbietenden soll der Prozess die Rechtssicherheit erhöhen. Die zuständigen Behörden sollen die Wirkungsweise von KI besser verstehen, um den Rechtsrahmen im Idealfall besser auf die praktischen Gegebenheiten zuzuschneiden. Zudem sollen Zusammenarbeit und Austausch bewährter Praktiken zwischen Behörden gefördert werden. Werden bei der Entwicklung und Erprobung von KI-Systemen erhebliche Risiken festgestellt, müssen Anbietende angemessene Maßnahmen zur Risikominderung implementieren. Ist eine Risikominderung nicht möglich, muss der Entwicklungs- und Erprobungsprozess ausgesetzt werden.

IV. Aufbau und Struktur von KI-Reallaboren

Während der Entwicklung im Reallabor sind die Anbietenden verpflichtet, mit der zuständigen Behörde zusammenzuarbeiten und ihren Anweisungen zu folgen. Die Behörde bietet Anleitung, Aufsicht und Unterstützung, insbesondere zu Fragen, die für die Anbietenden noch mit Rechtsunsicherheiten verbunden sind. Sie erstellt Leitfäden zu regulatorischen Erwartungen und zur Erfüllung der in der KI-VO festgelegten Anforderungen und Pflichten. Bereits vor der Einrichtung eines KI-Reallabors kann die Behörde Anbietende an beratende Dienste verweisen. Zweck der Zusammenarbeit von Behörden und Anbietenden ist es, die rechtliche Konformität der KI sicherzustellen – nicht die technische Entwicklung. Die Behörde darf die forschende Tätigkeit der Anbietenden nicht übernehmen oder ersetzen.

Auf Anfrage der Anbietenden stellt die Behörde ihnen einen schriftlichen Nachweis für die im Reallabor erfolgreich durchgeführten Tätigkeiten aus. Außerdem verfasst die Behörde einen Abschlussbericht. Darin beschreibt sie die im Reallabor durchgeführten Tätigkeiten, deren Ergebnisse und die gewonnenen Erkenntnisse im Detail. Dieser Bericht soll es den Anbietenden erleichtern, bestimmte nachgelagerte Verfahren der Produktsicherheit durchzuführen (dazu unten mehr).

Die KI-VO sieht vor, dass die Mitgliedstaaten den zuständigen Behörden ausreichende Mittel zur Verfügung stellen, damit diese wirksam und zeitnah Reallabore einrichten können. Die Europäische Kommission kann den nationalen Behörden technische Unterstützung, Beratung und andere Instrumente für die Einrichtung und den Betrieb von KI-Reallaboren bereitstellen. Zudem wird sie eine eigene Schnittstelle einrichten, die alle relevanten Informationen zu KI-Reallaboren enthält. Interessenträger können so mit den KI-Reallaboren interagieren und Anfragen an die zuständigen Behörden richten.

Reallabore müssen nicht auf einen Mitgliedstaat begrenzt sein. Behörden unterschiedlicher EU-Mitgliedstaaten können auch gemeinsam ein KI-Reallabor einrichten. Auch ansonsten können nationale Behörden zusammenarbeiten und dabei nationale oder europäische Akteure in ihre Arbeit einbeziehen. Zu diesen Akteuren zählen: Normungsorganisationen, notifizierte Stellen, Test- und Versuchseinrichtungen, Forschungs- und Versuchslabore, europäische digitale Innovationszentren sowie einschlägige Interessenträger und Organisationen der Zivilgesellschaft.

V. Vorteile der Entwicklung in einem KI-Reallabor

Der Zugang zu einem KI-Reallabor ist grundsätzlich kostenlos.[8] Für Anbietende erhöht die Teilnahme die Rechtssicherheit. Sie dürfen davon ausgehen, dass ihr in Absprache mit der Behörde entwickeltes KI-System gesetzeskonform ist, und sie können die von der Behörde erstellten Unterlagen auch für andere Verfahren nutzen, um nachzuweisen, dass sie die Vorschriften der KI-VO einhalten. So müssen etwa Marktüberwachungsbehörden die Unterlagen bei einer Prüfung positiv berücksichtigen.

Hinzu kommt: Soweit die Anbietenden den spezifischen Plan und die Bedingungen für die Beteiligung am KI-Reallabor beachten und Anweisungen der zuständigen nationalen Behörden in gutem Glauben folgen, dürfen die Behörden keine Geldbußen wegen Verstößen gegen Vorgaben der KI-VO verhängen. Auch vor Bußgeldern wegen eines Verstoßes gegen andere europäische Vorschriften (zum Beispiel die DSGVO) sind sie geschützt, wenn die für die Überwachung des jeweiligen Rechtsakts zuständige Behörde aktiv an der Beaufsichtigung des KI-Systems im Reallabor beteiligt war und eine Anleitung für die Einhaltung der entsprechenden Vorschriften

8 Behörden können lediglich die Erstattung außergewöhnlicher Kosten verlangen. Was konkret unter diesem Begriff zu verstehen ist, ist nicht geregelt.

bereitgestellt hat, die die Anbietenden in gutem Glauben befolgt haben.

Zu beachten ist aber: Die Einhaltung dieser Vorgaben führt nicht zu einer Haftungsprivilegierung, wenn Dritte, die Schäden erlitten haben, die Anbietenden verklagen. Geschädigte können ihre Ansprüche nach dem Zivilrecht der Mitgliedstaaten (in Deutschland etwa nach den Vorschriften des Bürgerlichen Gesetzbuchs (BGB)) geltend machen.

VI. Anforderungen an KI-Reallabore

Nach der KI-VO ist die Kommission dafür zuständig, Durchführungsrechtsakte zu erlassen, um die Anforderungen an KI-Reallabore weiter zu konkretisieren. Sie sollen detaillierte Regelungen für Einrichtung, Entwicklung, Umsetzung, Betrieb und Beaufsichtigung der KI-Reallabore enthalten. Ziel ist es, Forschungs- und Versuchslabore, einzelne Forschende sowie andere wissenschaftliche Akteure in die KI-Reallabore einzubeziehen und bei ihrer Arbeit zu unterstützen.

Für die Verarbeitung personenbezogener Daten sieht die KI-VO Spezialregelungen vor. Für die Verwendung personenbezogener Daten, die für einen anderen Zweck als die Entwicklung des KI-Systems erhoben wurden, enthält die KI-VO einen neuen Erlaubnistatbestand. Dies ist notwendig, damit die Datenverarbeitung nicht gegen den Zweckbindungsgrundsatz der DSGVO verstößt und dadurch rechtswidrig ist. Damit der Erlaubnistatbestand greift, muss das KI-System einem der nachfolgenden Ziele dienen: der öffentlichen Sicherheit, der öffentlichen Gesundheit, dem Umweltschutz, der nachhaltigen Energie, der Sicherheit und Widerstandsfähigkeit von Verkehrssystemen und kritischen Infrastrukturen sowie der Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste.

Die Datenverarbeitung muss zudem erforderlich sein, um die Einhaltung der Anforderungen der KI-VO an Hochrisiko-KI-Systemen[9] sicherzustellen. Dazu gehören zum Beispiel die Einrichtung eines Risikomanagementsystems, die Einrichtung eines Qualitätsmanagementsystems, die vorgeschriebene technische Dokumentation, Transparenzvorkehrungen, Vorkehrungen für Robustheit und Cybersicherheit. Erforderlich ist die Verarbeitung dann, wenn sich die Einhaltung der rechtlichen Anforderungen nicht durch eine Verarbeitung anonymisierter, synthetischer oder sonstiger nicht personenbezogener Daten wirksam erfüllen lässt.

Anbietende müssen wirksame Überwachungsmechanismen schaffen und einhalten, um zu beobachten, ob hohe Risiken für die Rechte und Freiheiten betroffener Personen bei Reallaborversuchen bestehen. Die verwendeten Daten müssen in einer funktional getrennten, isolierten und geschützten Datenverarbeitungsumgebung unter der Kontrolle der Anbietenden aufbewahrt werden. Sie sind durch technische und organisatorische Maßnahmen zu schützen; nur befugte Personen dürfen Zugriff haben. Personenbezogene Daten, die im Reallabor entstanden sind, dürfen nicht außerhalb des Reallabors weitergegeben werden. Sobald die Beteiligung an dem Reallabor endet, sind die Daten zu löschen.

VII. Behördliche Zuständigkeit in Deutschland

In Deutschland wird voraussichtlich die Bundesnetzagentur (BNetzA) die zentrale Aufsichtsbehörde für die KI-VO werden. Die Datenschutzkonferenz, also das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, hat sich dafür ausgesprochen, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) sowie die Landesdatenschutzbehörden als nationale Marktüberwachungsbehörden zu benennen.[10] Die Bündelung von Datenschutz- und KI-Aufsicht würde dazu führen, dass die Bürgerinnen und Bürger „es mit nur einer Aufsichtsbehörde“ zu tun hätten. Auch verfügen die Datenschutzaufsichtsbehörden über die einschlägige Fachkunde und die notwendige Unabhängigkeit und sind mit funktionierenden Kooperations- und Kohärenzmechanismen ausgestattet. Zudem sind sie für KI-Systeme, die personenbezogene Daten verwenden, ohnehin zuständig. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit fügt hinzu, dass sich Doppelstrukturen und Rechtsunsicherheiten vermeiden ließen.[11]

---

9 Zur Erklärung der unterschiedlichen Risikokategorien bereits Rennert, One KIss is all it takes in DFN-Infobrief Recht 01/2023; Europäisches Parlament, KI-Gesetz: erste Regulierung der künstlichen Intelligenz, abrufbar unter: https://www.europarl.europa.eu/topics/de/article/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz (zuletzt abgerufen am 10.07.2024).

10 DSK, Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 3. Mai 2024, Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO), abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf (zuletzt abgerufen am 10.07.2024).

11 Berliner Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung vom 8. Mai 2024, abrufbar unter: https://www.datenschutz-berlin.de/pressemitteilung/datenschutzkonferenz-bezieht-position-nationale-zustaendigkeiten-fuer-die-verordnung-zur-kuenstlichen-intelligenz/ (zuletzt abgerufen am 10.07.2024).

VIII. Alternative zu KI-Reallaboren nach der KI-VO

KI-Systeme können grundsätzlich auch außerhalb von KI-Reallaboren getestet werden. Für Tests von Hochrisiko-KI-Systemen unter realen Bedingungen gelten dafür aber bestimmte Regelungen. KI-Systeme mit einem geringeren Risiko müssen diese Anforderungen hingegen nicht erfüllen. Die Vorgaben für Tests von Hochrisiko-KI-Systemen unter realen Bedingungen ähneln denen von KI-Reallaboren. So müssen Anbietende etwa einen Plan für den Test erstellen und bei der zuständigen Marktüberwachungsbehörde einreichen. Die Behörde hat den Test anhand des eingereichten Plans zu genehmigen. Der Test muss in einer dafür einzurichtenden EU-Datenbank registriert werden. Er darf nicht länger dauern, als zur Erfüllung seiner Zielsetzung notwendig ist. Regelmäßig ist die Dauer auf sechs Monate begrenzt und kann einmalig um sechs Monate verlängert werden. Die Personen, die am Test teilnehmen, müssen vor Testbeginn ihre informierte Zustimmung erteilen. Zudem ist eine qualifizierte Person mit der wirksamen Überwachung des Tests zu beauftragen.

Wenn im Testverlauf ein schwerwiegender Vorfall eintritt, müssen Anbietende ihn den nationalen Marktüberwachungsbehörden melden und Sofortmaßnahmen zur Schadensbegrenzung einleiten. Andernfalls müssen sie den Test abbrechen oder jedenfalls die Entwicklung aussetzen, bis eine Schadensbegrenzung stattgefunden hat. Für Schäden, die während der Tests unter realen Bedingungen entstehen, sind die Anbietenden grundsätzlich nach den zivilrechtlichen Gesetzen der Mitgliedstaaten (in Deutschland beispielsweise nach dem BGB) haftbar. ◆

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 stellvertretender Leiter des Bereichs Collaboration Services in der DFN-Geschäftsstelle beschäftigt sich Dirk Bei der Kellen mit den Schwerpunkten Cloud, Videokonferenzen und Telefonie. Zu seinen Veranstaltungshighlights gehörte …

… die TNC24, die vom 10. bis 14. Juni 2024 in Rennes, Frankreich, stattfand. Bei der Netzwerkkonferenz trifft sich jedes Jahr die Community der weltweiten nationalen Forschungsnetze zum Austausch und gemeinsamen Arbeiten.

Bereits im Mittelalter ein Ort des Lernens: Der Le Couvent des Jacobins eignete sich mit seinem Innenhof und den Kapellen hervorragend als Treffpunkt der NREN-Community | *Fotos: Dirk Bei der Kellen/DFN*

Als im vorherigen Jahr der Veranstaltungsort für die TNC24 enthüllt wird, bin ich sofort geflasht. Frankreich, das Land meiner Urahnen, wie man mit viel Fantasie am Namen erkennt: Bei der = Pays de, Kellen = Calais. Die Anreise zu meinem Rendezvous mit der Hauptstadt der sagenumwobenen Bretagne dauert per Flieger dreieinhalb Stunden ab Hamburg. Nach dem Umstieg in Frankfurt sehe ich bereits viele bekannte Gesichter im „Nerd-Bird“ nach Rennes. Jemand scherzt, ob es denn Leute an Bord gibt, die nicht zur TNC wollen: einvernehmliches Gekicher. Bei der Landung in Rennes zieht es alle in die Sicherheitsgurte. Die Landebahn auf dem Miniflughafen ist so kurz, dass selbst ein kleines Flugzeug heftig in die Eisen gehen muss. Vom DFN bin ich einer der Ersten vor Ort. Viele Kolleginnen und Kollegen sind noch bei der 40-Jahr-Feier des Vereins.

Rennes ist eine mir bislang völlig unbekannte Stadt. Erster Eindruck am Sonntagabend: nett, aber etwas verschlafen. Ich kenne die nahe gelegenen Städte Nantes und vor allem Angers, in denen wir als Kinder der deutsch-französischen Versöhnung in den 80er-Jahren mehrfach zum Schüleraustausch bei der Familie Baudrier waren. Und ich bin erstaunt, wie gut es mir noch gelingt, in einem Bistro auf Französisch zu bestellen. Na gut, „Moules et Frites“ ist jetzt nichts, wofür man ein Sprachgenie sein muss.

Pflichtprogramm: Gleich Montag startet das Cloud-Forum, für das ich schweren Herzens unsere schöne Jubiläumsfeier hab sausen lassen. Neben einem Update zu OCRE 2024 gibt es viel Input vom niederländischen NREN SURF. Ich freue mich, die Leute aus den monatlichen VC-Meetings persönlich zu treffen.

Der Veranstaltungsort der TNC24 ist ein ehemaliges Dominikanerkloster mitten im Zentrum an der Place Sainte-Anne, direkt neben der dem heiligen Albin von Angers gewidmeten Basilika. Der Konvent ist ein beeindruckender Ort, dessen Geschichte bis ins Mittelalter zurückreicht und die Bedeutung Rennes als kulturelles und politisches

Gemeinsam bei der TNC24: Für viele Mitarbeitende der DFN-Geschäftsstelle ist die TNC jedes Jahr ein Highlight: v. li. Dirk Bei der Kellen, Christian Meyer und Peter Kaufmann
Foto: Maël Gonnet/TNC24

Zentrum der Bretagne unterstreicht. Vor dem Umbau zu einem Kongresszentrum wurde das „Couvent des Jacobins" als Militärdepot genutzt und in den 2010er-Jahren schließlich mutig, aber behutsam umgebaut.

Vor dem Hintergrund, dass wir uns im Bereich des Cloud-Servicemanagements möglicherweise personell verstärken wollen, liegt mein Augenmerk unter anderem auf dem Future Talent Programme. Das Format eignet sich hervorragend dazu, die Teilnehmerinnen und Teilnehmer des Programms persönlich kennenzulernen. Ich habe Kontakt zu einer Kollegin aufgenommen, die gerade ihren Master beim finnischen Forschungsnetz FUNET macht und sich mit einem Lightning Talk präsentiert. Wir verständigen uns darauf, dass ich mich mit einer eventuellen Stellenbeschreibung an sie wenden darf. So funktioniert das bei der TNC: Lächeln, ein paar Brocken Englisch hervorkramen und die Leute einfach ansprechen. In dieser freundlichen und wohlwollenden Atmosphäre gelingt der Austausch zur Not mit Händen und Füßen.

Beim gemeinsamen Abendessen lerne ich Gül kennen, die sich bei SURF um Fragen der Zukunft kümmert, und die wie ich – so klein ist die Welt – in der Vorwoche beim University: Future Festival des Hochschulforums Digitalisierung vortrug. Bei der Eröffnungsparty treffe ich liebe Kollegen vom KIT und den total sympathischen Weltenbummler Sean von Internet2 – unserem US-amerikanischen Pendant. Wir stellen bei belgischem Bier fest, dass er wahrscheinlich der einzige Amerikaner auf der Social-Media-Plattform Mastodon ist. Und dass Zoom die Preise erhöht, erfahre ich auch von ihm. Das Fazit von meinem Kollegen Ralf Paffrath und mir nach dem tollen Event: Belgisches Erdbeerbier sieht schöner aus, als es schmeckt!

Programmhöhepunkte? Einer ist die Panel-Diskussion mit Madara Ogot, CEO der UbuntuNet Alliance, der mich mit seiner Klarheit, seinem Fachwissen und ganz besonders mit seinem Optimismus inspiriert, trotz politisch komplizierter Bedingungen den Mut nicht zu verlieren. Auch Paul Iskes (Universität Maastricht) Keynote über grandiose Fehlleistungen ist sehr geistreich. Der emotionalste Programmpunkt ist für mich aber die Verleihung der Ehrenmedaille der Vietsch Foundation an Christian Grimm, einen unserer Geschäftsführer. Selten habe ich ein 1000-Zuschauer-Auditorium derart leise erlebt, dass sogar das Surren der Klimaanlagenlüftung zu hören war – insbesondere als er von seiner letzten Begegnung mit Karel Vietsch (1952-2014), dem Gründer der niederländischen Stiftung, spricht. Das hat mich, wie ich zugeben muss, richtig angefasst.

Den letzten Abend der TNC lassen wir mit einigen CERTies im Abri du Marché ausklingen, begleitet von einem lieben Kollegen des norwegischen Forschungsnetzes SIKT. Kein einziges Wort fällt an diesem Abend zu eduMEET – trotzdem haben wir jede Menge Gesprächsstoff. In der Mitte des Tisches sitzt Christian Grimm, unser frischgebackener Vietsch-Preisträger. Ein wunderbarer Abend beendet die diesjährige TNC, für mich fast so etwas wie eine verspätete 40-Jahr-Feier. Es gibt wieder Muscheln mit Pommes, dazu Steaks und Bier. Vegetarier bitte nicht weiterlesen: In Rennes habe ich meine Vorliebe für Boeuf Tartare, rohes Rindfleisch, entdeckt.

Nomen est omen: Wer bei den TNC-Eröffnungspartys nicht dem Freudenrausch verfällt, ist selbst schuld

Am nächsten Morgen trennen sich unsere Wege. Für mich steht noch ein Side-Meeting von EUMETSAT auf dem Programm. Einige bekannte Gesichter laufen mir über den Weg: mein Kollege Stefan Piger und noch ein lieber Kollege von BelWue. Auch die KIT-Kollegen sind noch da, ich plaudere noch ein wenig mit einem kenianischen Kollegen von KENET, der eduroam in Kenia eingeführt hat. Ich soll doch schöne Grüße an Ralf Paffrath ausrichten. Das war es nun, um mich herum wird schon aufgeräumt. Zum Abschied werden noch ein paar Karamellbonbons verteilt. Sie versüßen mir die Zeit bis zur TNC25. Und dann lautet das Motto: „Brighter together" in Brighton. ◆

Alle Vorträge der TNC24 gibt es unter:
https://tnc24.geant.org/recordings/

Im Dienst der Wissenschaft – 40 Jahre DFN-Verein

„Ein Leben ohne DFN? Möglich, aber sinnlos“ – so lautete frei nach Loriot der Titel der Festrede, die der ehemalige DFN-Vorstandsvorsitzende Prof. Dr. Hans-Joachim Bungartz zum 40-jährigen Bestehen des DFN-Vereins hielt. Dass der DFN einem verständlicherweise mindestens so ans Herz wachsen kann wie ein Mops (Originalzitat von Loriot), davon zeugten die zahlreichen Gäste, die am 10. Juni 2024 am Vorabend der Mitgliederversammlung in die European School of Management and Technology Berlin (ESMT Berlin) gekommen waren, um den runden Geburtstag gemeinsam zu zelebrieren.

Text: **Maimona Id** (DFN-Verein)

Das Festprogramm

Zum Auftakt der Veranstaltung begrüßte Prof. Dr.-Ing. Stefan Wesner, der Vorstandsvorsitzende des DFN-Vereins und Direktor des IT Center University of Cologne (ITCC), die Anwesenden im Foyer des ehemaligen Staatsratsgebäudes der DDR, in dem die ESMT seit 2006 beheimatet ist. Das unter Denkmalschutz stehende Gebäude wurde von 1962 bis 1964 erbaut. Anschließend startete das abwechslungsreiche Festprogramm mit Führungen ins benachbarte Humboldt Forum. Hier konnten die Gäste unter anderem die ethnologischen Sammlungen bewundern und hatten die Gelegenheit, von der Dachterrasse in rund 30 Metern Höhe einen exklusiven Ausblick auf Berlin zu genießen. Bei dem anschließenden Sektempfang mit Imbiss konnten sich die Gäste mit regionalen Spezialitäten aus ganz Deutschland stärken. Am späten Nachmittag versammelte sich die Festgesellschaft im Konferenzraum Tower View zur Rede von Prof. Bungartz. Dem voraus gingen einleitende Worte von Prof. Wesner und ein Vortrag von Georg Garlichs, Chief Financial Officer and Managing Director der ESMT Berlin, zur Gründung der Hochschule sowie zur Historie des Gebäudes.

Der Festvortrag

In seiner kurzweiligen Rede – durch die sich Loriot als roter Faden zog – betonte Prof. Bungartz, dass der DFN-Verein quasi als Blaupause für „Selbsthilfe der Wissenschaft“ in der deutschen Wissenschaftslandschaft Schule gemacht habe. In einem kurzen Überblick ging er auf die Höhepunkte und Erfolge, aber auch die Herausforderungen der 40 Vereinsjahre von 1984 bis 2024 ein. Zu nennen sind hier die Gründungszeit, das erste eigene Wissenschaftsnetz und

als großer Meilenstein der Schritt von einem geförderten Projekt in die wirtschaftliche Eigenverantwortung einer Organisation der Wissenschaft.

Als Grund für den Erfolg des DFN-Vereins bezeichnete der Dekan der TUM School of Computation, Information and Technology der TU München das „verantwortungsvolle Agieren aller Akteure im Verein“ und meinte unter anderem die Mitgliedsvertretenden, die zwar den Interessen ihrer Einrichtung verpflichtet sind, aber eben auch dem Gesamtwohl: „Mein eigenes Gärtchen wird nicht auf Dauer blühen und gedeihen können, wenn meine Nachbarn unter Wassermangel leiden.“ Als weiteren Erfolgsgaranten nannte er die DFN-Geschäftsstelle, die „durch unglaublich viel Fachkompetenz, Einsatzbereitschaft, Verantwortungsbewusstsein, ja Hingabe für den Verein, für ihren Verein“ das operative Geschäft übernehmen und damit den Vorstand entlasten. Er selbst leitete den Vorstand von 2011 bis 2020. Als ein Highlight seiner Amtszeit nannte er unter anderem die Entgeltordnung, die nach drei Jahren der Vorbereitung 2020 verabschiedet und ab 2022 fair, solidarisch und bedarfsgerecht umgesetzt wurde. Mit einem „Herzlichen Glückwunsch, lieber DFN-Verein, zum Geburtstag! Weiter so, und ad multos annos!“ dankte Prof. Bungartz und gab den Startschuss zum gemütlichen Ausklang des Abends. Dieser endete mit einem feierlichen Abendessen im Auditorium Maximum mit seinem 35 Meter langen Bildfries aus Meissener Porzellan. Nicht zu vergessen: der Anschnitt der DFN-Geburtstagstorte, den der stellvertretende Vorstandsvorsitzende und stellvertretende Leiter des Leibniz-Rechenzentrums (LRZ) Prof. Dr. Helmut Reiser zu fortgeschrittener Stunde tatkräftig übernahm.

Lesen Sie auch das Interview zum 40-jährigen Bestehen mit Prof. Dr. Bernhard Neumair, dem ehemaligen stellvertretenden Vorstandsvorsitzenden des DFN-Vereins, in Ausgabe 105 der DFN-Mitteilungen.

So jung kommen wir nicht mehr zusammen: Aus ganz Deutschland waren die Gäste angereist, um den 40. Geburtstag des DFN-Vereins im historischen Ambiente des ehemaligen Staatsratsgebäudes der DDR, in dem die ESMT seit 2006 ihren Sitz hat, zu feiern | *Fotos: Jürgen ALOIsius Morgenroth*

Kurzmeldungen DFN-Verein

DFN-Geschäftsführer Christian Grimm erhält die Ehrenmedaille der Vietsch Foundation

Für seine Verdienste bei der Gründung und Entwicklung der europäischen Forschungsnetzorganisation GÉANT Association wurde Dr. Christian Grimm (Geschäftsführer im DFN-Verein, gemeinsam mit Jochem Pattloch) am 13. Juni 2024 mit der renommierten Ehrenmedaille der niederländischen Vietsch Foundation ausgezeichnet. Die Preisverleihung fand im Rahmen der Netzkonferenz TNC24 in Rennes statt.

Als Mitglied des Vorstandes von DANTE Limited (Delivery of Advanced Network Technology to Europe) in Cambridge war Christian Grimm ab 2013 mitverantwortlich für den mehrjährigen Prozess der Fusion mit TERENA (Trans-European Research and Education Networking Association), der Ende 2014 zur Gründung der GÉANT Association führte. Das machte den Weg frei für den Beitritt weiterer europäischer Forschungsnetze als stimmberechtigte Mitglieder. In seiner Zeit als Vorstandsvorsitzender der GÉANT Association (2015 bis 2020) erfolgte die Konsolidierung der beiden Geschäftsstellen in Amsterdam und Cambridge mit heute 160 Mitarbeitenden.

In seiner Laudatio betonte Valentino Cavalli, der Vorsitzende des Kuratoriums der Vietsch Foundation, die Rolle, die Christian Grimm in der Gründungsphase der

GÉANT Association einnahm: „Als Vorstandsvorsitzender von GÉANT hat er mit viel Engagement, Hingabe und Empathie die Organisation mitgestaltet. Davon wird die gesamte F&E-Gemeinschaft noch sehr lange profitieren". ◆

Große Ehre: DFN-Geschäftsführer Christian Grimm erhält die Vietsch Medal of Honour – überreicht von Valentino Cavalli, dem Vorsitzenden des Kuratoriums der Vietsch Foundation (von links)
Fotos: GÉANT

Gemeinsam Zukunft gestalten – das DFN-Diskussionsforum der Kanzlerinnen und Kanzler

Am Montag und Dienstag, 13. und 14. Mai 2024, trafen sich die Führungskräfte von Hochschulleitungen aus ganz Deutschland beim DFN-Diskussionsforum der Kanzlerinnen und Kanzler in Berlin, um gemeinsam Innovationen, Entwicklungen und aktuelle Herausforderungen der Digitalisierung in Bildung und Forschung zu diskutieren. Dabei lag der Fokus auf den Themen Künstliche Intelligenz und IT-Sicherheit.

Alle zwei Jahre lädt der DFN-Verein die Verwaltungschefinnen und -chefs der am Wissenschaftsnetz teilnehmenden Hochschulen ein. Ziel ist es, den Erfahrungsaustausch zwischen Hochschulleitungen und Vereinsführung zu fördern sowie den Teilnehmenden ein Forum zu bieten, bei dem sie sich zu aktuellen Themen rund um das Wissenschaftsnetz und seine Dienste informieren können.

Nach der Begrüßung und einem Überblick zum Stand des DFN-Vereins von Prof. Dr. Helmut Reiser, dem stellvertretenden Vorstandsvorsitzenden des DFN-Vereins, startete das Diskussionsforum am ersten Tag mit der Keynote „Rechtliche Anforderungen beim Einsatz von ChatGPT und anderen KI-Systemen“ von Dr. Carsten Ulbricht. Darin sprach der Rechtsanwalt über die rechtlichen Risiken des ungesteuerten Einsatzes von ChatGPT und anderen generativen KI-Systemen. Er empfahl, geeignete Richtlinien für den Einsatz von KI an Institutionen und Unternehmen einzuführen. Nur so könnten Chancen und Einsatzszenarien abgesichert „ausgetestet“ werden, um hieraus zu lernen und mit den weiteren Entwicklungen Schritt zu halten. Das tolle warme Wetter und das schöne Ambiente des am Ufer der Dahme gelegenen Veranstaltungsortes sorgten beim Konferenzdinner am Abend für entspannte Gespräche und die Möglichkeit zum Kennenlernen und Netzwerken unter den Teilnehmenden.

Gut vernetzt: Schwerpunkt des diesjährigen Forums war das Zukunftsthema KI. Am Stehpult: Prof. Dr. Helmut Reiser, stellvertretender DFN-Vorstandsvorsitzender | *Foto: Nina Bark/DFN*

Im Rahmen der Sessions „Einsatz von KI“, „Aktuelles zum Thema Sicherheit“ und „Rechtsforschung im DFN – Aktuelles aus Gesetzgebung und Rechtsprechung“ boten unter anderem die Vorträge von Prof. Dr. Moreen Heine von der Universität zu Lübeck und Prof. Dr. Thomas Schreck von der Hochschule München am zweiten Tag der Veranstaltung viel Stoff für angeregte Diskussionen. ◆

Erfolgreiches All Hands 2024 der DFN-Geschäftsstelle

Alle Hände an Bord: 63 Mitarbeitende des DFN-Vereins und Thorsten Visbal als Moderator trafen sich am Montag und Dienstag, 16. und 17. September 2024, im Hotel Müggelseeperle im Südosten Berlins. Die Veranstaltung fernab des gewohnten Alltags im Grünen bot Gelegenheit, neue Kolleginnen und Kollegen der letzten zwei Jahre noch besser kennenzulernen und erfolgreich als Team zusammenzuwachsen.

Neben intensiven Gesprächen fand sich genügend Raum für Gruppenarbeiten und kreative Diskussionen zur weiteren Entwicklung der Geschäftsstelle. In verschiedenen Formaten konnten Mitarbeitende ihre Anregungen vorstellen, bewerten und gemeinsam nächste Schritte erarbeiten. Aber was wäre ein Teamevent ohne den Austausch nach der Arbeit? Gemeinsame Spaziergänge, Joggen, Bogenschießen und der Klassiker Bowling sorgten für den Spaß am Abend. Mit vielen frischen Eindrücken und jeder Menge Input versorgt, freuen sich die Mitarbeitenden in der Geschäftsstelle auf zukünftige spannende Herausforderungen. ◆

Für Forschung und Lehre: Die Mitarbeitenden des DFN-Vereins sorgen seit 40 Jahren dafür, dass teilnehmende Einrichtungen am Wissenschaftsnetz sicher und schnell miteinander kommunizieren können | *Foto: Christoph Schieder*

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.

88. DFN-Mitgliederversammlung

Am Dienstag, 11. Juni 2024, fand die 88. Mitgliederversammlung (MV) des DFN-Vereins in der 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 2023: Bei den Projektbeteiligungen sind u. a. der mit der RWTH Aachen gemeinsam entwickelte Basisdienst Identity & Access Management (IAM4NFDI) im Rahmen der Nationalen Forschungsdateninfrastruktur (NFDI) und das GÉANT-Projekt GN5 Phase 2, das offiziell am 1. Januar 2025 startet, zu nennen.

Hinsichtlich der Netzinfrastruktur wurde über die Entwicklung und den Stand des X-WiN berichtet. Außerdem genehmigte die Mitgliederversammlung die Leistungssteigerung des Dienstes DFN-Internet. Zu erwähnen ist weiter das im März 2024 in den Regelbetrieb gegangene Leistungsmerkmal DNS-RPZ (Domain Name Service – Response Policy Zone) von DFN-Security, das den Zugriff auf Phishingseiten verhindern soll. Das Leistungsmerkmal wird durch eine „Community-Zone“ ergänzt, in der sich Teilnehmer über Bedrohungslagen austauschen können. Über die Verabschiedung von Prof. Dr. Gerhard Peter als langjährigem Vorsitzenden der Mitgliederversammlungen und die Begrüßung von Dr. Rainer Bockholt als seinem designierten Nachfolger wird hier gesondert berichtet.

Geballte Kompetenz und Erfahrung: Mitgliedsvertretende der über 350 institutionellen Mitglieder treffen sich zweimal im Jahr, um über die Geschicke des DFN-Vereins abzustimmen | *Foto: Jürgen ALOIsius Morgenroth*

Wir danken Prof. Dr. Gerhard Peter!
Im Rahmen der 88. Mitgliederversammlung am 11. Juni 2024 in der Berlin-Brandenburgischen Akademie der Wissenschaften wurde Prof. Dr. Gerhard Peter als langjähriger Vorsitzender der Mitgliederversammlungen verabschiedet.

In seiner Rede bedankte sich DFN-Vorstandsvorsitzender Prof. Dr.-Ing. Stefan Wesner im Namen der Mitglieder für die wertvolle Arbeit und würdigte das außerordentliche Engagement, mit dem der ehemalige Rektor der Hochschule Heilbronn

Mit Engagement und Herzblut: Für seine Verdienste als langjähriger Leiter der Mitgliederversammlungen erhielt Prof. Dr. Gerhard Peter (3. v. li.) stehenden Applaus.

Von links:
Geschäftsführer Jochem Pattloch, Vorstandsvorsitzender Prof. Dr.-Ing. Stefan Wesner, stellvertretender Vorstandsvorsitzender Christian Zens, Geschäftsführer Dr. Christian Grimm und stellvertretender Vorstandsvorsitzender Prof. Dr. Helmut Reiser
Foto: Jürgen ALOIsius Morgenroth

seine Aufgabe versah. Ihm sei es maßgeblich zu verdanken, dass die Mitgliederversammlungen auch bei kontroversen Diskussionen stets konstruktiv verlaufen sind und letztendlich immer zu sehr guten und gemeinsam getragenen Ergebnissen geführt haben. Abschließend schlug er den Mitgliedsvertretenden vor, Prof. Peter zum Ehrenvorsitzenden zukünftiger Mitgliederversammlungen zu ernennen. Der Vorschlag wurde per Akklamation und unter stehendem Applaus angenommen. „Ich habe es gerne gemacht", sagte Prof. Peter und verriet, dass er bereits vor 40 Jahren bei der Gründungsversammlung des DFN-Vereins dabei war. Den Führungsstab übergab er an Dr. Rainer Bockholt, den Direktor des Hochschulrechenzentrums der Rheinischen Friedrich-Wilhelms-Universität Bonn, der sich für die Rolle als Vorsitzender der Mitgliederversammlung künftig zur Verfügung stellt.

TERMIN

Die 89. Mitgliederversammlung findet am **Dienstag und Mittwoch, 3. und 4. Dezember 2024**, statt.

Die 90. Mitgliederversammlung findet am **Montag und Dienstag, 2. und 3. Juni 2025,** statt.

DFN-Konferenz „Sicherheit in vernetzten Systemen"

Diese im Sicherheitsbereich etablierte Veranstaltung beinhaltet Beiträge und Diskussionen zu vielfältigen Aspekten der Informationssicherheit. Mit ihrer explizit technischen und wissenschaftlichen Ausrichtung hat sich die DFN-Konferenz als eine der größten deutschen Tagungen für Informationssicherheit etabliert.

TERMIN

Die 32. DFN-Konferenz „Sicherheit in vernetzten Systemen" findet am **Dienstag und Mittwoch, 18. und 19. Februar 2025,** statt.

DFN-Betriebstagung

Die 81. DFN-Betriebstagung (BT), die am 8. und 9. Oktober 2024 im Leonardo Royal Hotel Berlin Alexanderplatz stattfand, ging mit vielen spannenden Diskussionen, Themen am Puls der Zeit, frischen Eindrücken und neuen Kontakten zu Ende. Mehr als 300 Teilnehmende verzeichnete die Präsenzveranstaltung. 130 Leute schauten sich die Plenumsvorträge im Stream an. Der erste Tag ging mit den Vorträgen im Plenum und den darauffolgenden Foren Sicherheit, Rechtsfragen, AAI und Mail erfolgreich zu Ende. Ein Highlight war das Get-together am Abend, das anlässlich des 40-jährigen Jubiläums in einem bayerisch angehauchten Bierzelt stattfand und den Teilnehmenden ausgiebig Gelegenheit zum Netzwerken bot.

Auch der 2. Tag bot in den Foren Wissenschaftsnetz, Multimedia, Mobile IT, VoIP und Cloud viele Themen, die das Fachpublikum tagtäglich beschäftigt – u. a. „IT-Sicherheit im Wandel: Cloud-Dienste als Schutzschild für Bildung und Forschung“, „Die Bedeutung von Open-Source-Lösungen für Bildungsinstitutionen“ und „GWDG Chat AI – ein neuer föderierter Zugang zu Großsprachmodellen künstlicher Intelligenz“.

Gut besucht: die 81. DFN-Betriebstagung im 40. Jahr des DFN-Vereins war mit mehr als 300 Teilnehmenden bis auf den letzten Stuhl ausgebucht | *Foto: Maimona Id/DFN*

TERMIN

Die 82. Betriebstagung findet am **Dienstag und Mittwoch, 25. und 26. März 2025,** statt.

TERMIN

Die 18. Tagung der DFN-Nutzergruppe „Hochschulverwaltung“ findet von **Montag bis Mittwoch, 5. bis 7. Mai 2025,** in Bonn statt.

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

18. Tagung der DFN-Nutzergruppe „Hochschulverwaltung“

Im kommenden Jahr findet die Tagung der DFN-Nutzergruppe Hochschulverwaltung unter dem Motto „(R)evolution der Hochschulverwaltung – KI und Souveränität“ in Bonn statt. Organisiert wird sie vom DFN-Verein in Zusammenarbeit mit der Universität Bonn. Vortragende aus Rechenzentren, Forschung, Verwaltung und Wirtschaft beschäftigen sich mit hochaktuellen Fragen zur Informationssicherheit, zur Digitalen Souveränität und zum Onlinezugangsgesetz aus den Blickwinkeln Rechtliches, Kollaboration und Umsetzung.

Weitere Informationen zur Arbeit der Nutzergruppe und zu ihren Tagungen finden Sie unter: https://www.hochschulverwaltung.de

Überblick DFN-Verein

(Stand: 12/2024)

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:

Kerstin Bein
(Universität Mannheim)

PD Dr. Wolfgang zu Castell
(Helmholtz-Zentrum Potsdam, Deutsches GeoForschungsZentrum GFZ)

Peter Gietz
(DAASI International GmbH)

Ilona Glaser
(Deutscher Wetterdienst)

Prof. Dr. Frank Jenko
(Technische Universität München)

Dr. Lars Köller
(Technische Hochschule Ostwestfalen-Lippe)

Dieter Lehmann
(Universität Leipzig)

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

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

Prof. Dr. Helmut Reiser
(LRZ der Bayerischen Akademie der Wissenschaften)

Prof. Dr.-Ing. Günter Schäfer
(Technische Universität Ilmenau)

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

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

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.-Ing. Stefan Wesner
Vorsitz

Prof. Dr. Helmut Reiser
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 - Technik und Wirtschaft
	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 Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung e. V. (DIW)
	European School of Management and Technology GmbH (ESMT)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hertie School gGmbH
	Hochschule für Technik und Wirtschaft Berlin
	Hochschule für Wirtschaft und Recht Berlin
	Humboldt-Universität zu Berlin
	International Psychoanalytic University Berlin gGmbH
	IT-Dienstleistungszentrum Berlin
	Leibniz-Gemeinschaft e. V.
	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
	Zuse-Institut Berlin (ZIB)
Biberach	Hochschule Biberach
Bielefeld	Hochschule Bielefeld
	Universität Bielefeld
Bingen	Technische Hochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Hochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Hochschule Georg Agricola
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern und für Heimat
	Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz
	Deutsche Forschungsgemeinschaft
	Deutscher Akademischer Austauschdienst e. V.
	Deutsches Zentrum für Luft- und Raumfahrt e. V.
	Deutsches Zentrum für Neurodegenerative Erkrankungen e. V.
	Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.
	Rheinische Friedrich-Wilhelms-Universität Bonn
Borstel	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
	Technische Universität Braunschweig
Bremen	Constructor University Bremen gGmbH
	Hochschule Bremen
	Hochschule für Künste Bremen
	Universität Bremen
Bremerhaven	Alfred-Wegener-Institut, Helmholtz-Zentrum für Polar- und Meeresforschung
	Hochschule Bremerhaven
Buxtehude	hochschule 21 gemeinnützige GmbH
Chemnitz	Technische Universität Chemnitz
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
	Technische Universität Darmstadt
Deggendorf	Technische Hochschule Deggendorf
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 Dresden
	Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden e. V.
	Leibniz-Institut für Polymerforschung Dresden e. V.
	Sächsische Landesbibliothek – Staats- und Universitätsbibliothek
	Technische Universität Dresden
Dummerstorf	Forschungsinstitut für Nutztierbiologie (FBN)
Düsseldorf	Hochschule Düsseldorf
	Heinrich-Heine-Universität Düsseldorf
	Information und Technik Nordrhein-Westfalen (IT.NRW)
	Kunstakademie Düsseldorf
	Robert Schumann Hochschule Düsseldorf
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
	DIPF | Leibniz-Institut für Bildungsforschung und Bildungsinformation
	Frankfurt University of Applied Sciences
	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-Triesdorf
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 hereon 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
	FernUniversität in Hagen
Halle/Saale	Leibniz-Institut für Wirtschaftsforschung Halle e. V.
	Martin-Luther-Universität Halle-Wittenberg
	Burg Giebichenstein Kunsthochschule Halle
Hamburg	Berufliche Hochschule Hamburg (BHH)
	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 Hamburg
	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 Hannover
	Landesamt für Bergbau, Energie und Geologie
	Medizinische Hochschule Hannover
	Technische Informationsbibliothek
	Stiftung Tierärztliche Hochschule Hannover
Heide	Fachhochschule Westküste
Heidelberg	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	NEC Laboratories Europe GmbH

	Universität Heidelberg
Heilbronn	Hochschule Heilbronn
Hildesheim	Hochschule für angewandte Wissenschaft und Kunst 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 - Leibniz-Institut für Informationsinfrastruktur GmbH
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe
	Karlshochschule International University
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	Staatliche Akademie der Bildenden Künste Karlsruhe
Kassel	Universität Kassel
Kehl	Hochschule für öffentliche Verwaltung Kehl
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 Hochschule 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 GmbH – UFZ
	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.	Deutsche Schillergesellschaft e. V. Deutsches Literaturarchiv Marbach
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 zur Förderung der Wissenschaften e. V.
	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
	Hochschule für Gestaltung Offenbach
Offenburg	Hochschule Offenburg
Oldenburg	Carl von Ossietzky Universität Oldenburg
	IBS IT & Business School 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 Potsdam Deutsches GeoForschungs Zentrum – GFZ
	Filmuniversität Babelsberg KONRAD WOLF
	Potsdam-Institut für Klimafolgenforschung (PIK) e. V.
	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	Landesamt für Kultur und Denkmalpflege 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
	Stiftung "Medien in der Bildung" – 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
Weimar	Bauhaus-Universität Weimar
	Hochschule für Musik FRANZ LISZT Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz
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 LinkedIn
postet aktuelle Nachrichten zum Deutschen Forschungsnetz

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