DFN mitteilungen

Gute Aussichten
mit der DFN-Cloud

Fit für die Zukunft
Technik-Upgrade im X-WiN

Blick nach vorn
die Forschungsstelle Recht im DFN

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: ARNOLDprint service GmbH

Fotonachweis
Titel: Labor3, Foto: Günter Albers/Adobe Stock
Rückseite: Pixel-Shot/Adobe Stock

Dr. Oliver Schumacher
Bereichsleiter für Informations- und Wissensmanagement der Fraunhofer-Gesellschaft

Flexibilität, Skalierbarkeit und Elastizität, aber auch Verfügbarkeit gehören heute zu den Grundvoraussetzungen für agile Arbeitsweisen und moderne IT-Infrastrukturen. Verschiedenste Cloud-Provider bieten hierfür seit Jahren Lösungen auf unterschiedlichen Ebenen. Das Angebot von Leistungen ist mittlerweile so mannigfaltig und auch so selbstverständlich geworden, dass Vorbehalte zunehmend in den Hintergrund rücken. Die Vorteile in Sachen Effizienz und Geschwindigkeit liegen geradezu auf der Hand.

Für besonders sensible Anwendungen, bei denen Datenschutz eine wichtige Rolle spielt, implementierte die Fraunhofer-Gesellschaft eine „Private Cloud“. Diese bietet zwar ein hohes Maß an Sicherheit, bringt jedoch auch einen beträchtlichen investiven und personellen Aufwand mit sich. Außerdem weist sie durchaus Limits in der Skalierbarkeit auf.

Der Zugang zu Public-Cloud-Angeboten war für Wissenschaftsorganisationen bisher eher mit administrativen Hürden als mit technischen Herausforderungen behaftet. Unterschiedliche Angebotsmodelle und Kostenstrukturen der Provider sind in Projekten mitunter schlecht zu budgetieren, die Abrechnungsprozesse für Einrichtungen teils schwer handhabbar. Darüber hinaus ist der Aufwand einer eigenen Ausschreibung enorm.

Durch die OCRE-Rahmenverträge für kommerzielle Cloud-Dienste haben sich viele dieser Hürden deutlich reduziert. Wir sehen seither einen deutlichen Zuwachs an Buchungen – ausgelöst zum einen durch den Anreiz der generativen KI-Services und zum anderen durch den wachsenden Bedarf an Angeboten nationaler Cloud-Provider.

Kernpunkt für die effiziente Nutzung der über OCRE angebotenen Cloud-Services sind bei der Fraunhofer-Gesellschaft umfangreiche Beratungsleistungen. Damit erhalten Forschende Hilfestellung bei der Auswahl der Angebote. Dies betrifft neben dem reinen Zugang auch viele technische Belange sowie Anforderungen an die Vertraulichkeit der Daten, sodass eine gute Balance zwischen Kosten, Funktionalität und Datenschutz gewährleistet ist.

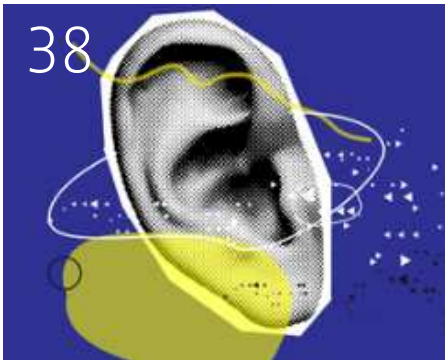
Die technische Entwicklung und Infrastrukturen in Form von Codes zu definieren und auszurollen, erlangt für uns in der Fraunhofer-Gesellschaft zunehmend eine enorme Bedeutung. Cloudagnostische Lösungen zu entwickeln ist damit sicherlich der Königsweg, um das eigene Angebot kontinuierlich an sich stetig verändernde Rahmenbedingungen anpassen zu können.

Ihr Oliver Schumacher

Inhalt

Mit Rückenwind in die Cloud
Die neuen Rahmenverträge von OCRE 2024 machen es möglich

Auf Socken zur Mondbasis
IT-Sicherheit spielerisch gedacht – mit der DFN-Security Challenge



The Power of Music
Marriage between Music and Technology

Wissenschaftsnetz

Sicherheit

Forschung

International

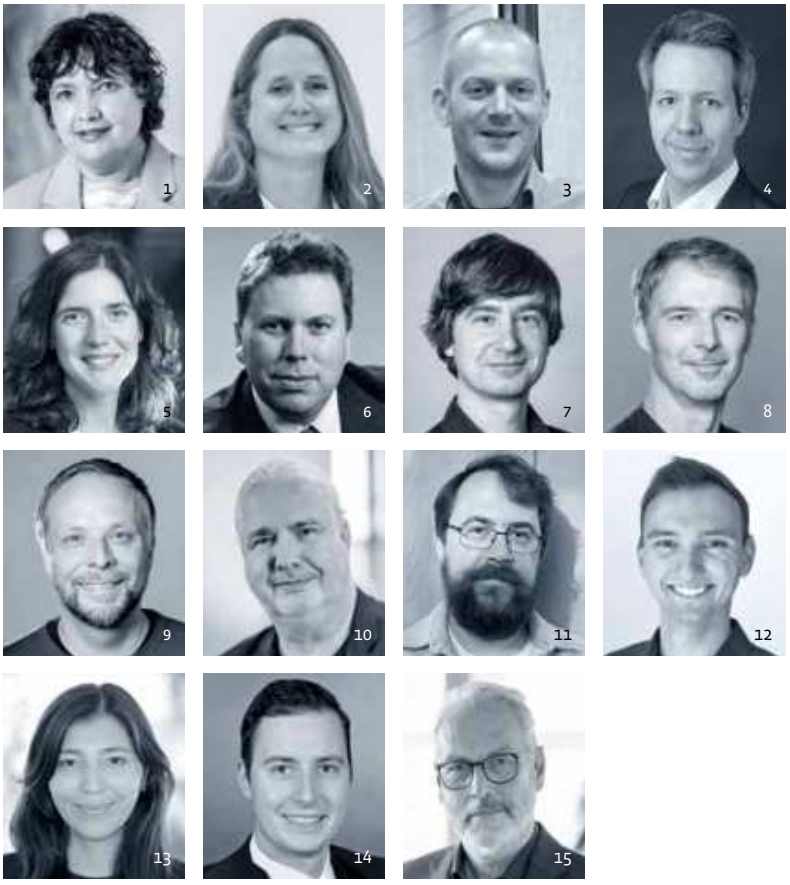
Campus

Recht

Blick nach vorn – Recht im DFN
Zwei Standorte, ein Ziel: Professorin Dr. Katharina de la Durantaye von der Forschungsstelle Recht im Interview

DFN-Verein

Autorinnen und Autoren dieser Ausgabe im Überblick



1 Maimona Id, DFN-Verein (id@dfn.de); **2** Sarah Grzemski, RWTH Aachen (grzemski@itc.rwth-aachen.de); **3** Ingo Hengstebeck, RWTH Aachen (hengstebeck@itc.rwth-aachen.de); **4** Marcel Nohl, RWTH Aachen (nohl@itc.rwth-aachen.de); **5** Prof. Dr. Fatma Deniz, Technische Universität Berlin (vp-dn@tu-berlin.de); **6** Dr. Thomas Hildmann, Technische Universität Berlin (thomas.hildmann@tu-berlin.de); **7** Christian Meyer, DFN-Verein (cmeyer@dfn.de); **8** Henry Kluge, DFN-Verein (kluge@dfn.de); **0. Abb.** Christine Kahl, DFN-CERT (kahl@dfn.de); **9** Dr. Ralf Gröper, DFN-Verein (groeper@dfn.de); **10** Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **11** Eric Gedenk, DFN-Verein (info@impact-scicomm.com); **12** Julian Kropp, Hochschule Darmstadt (julian.kropp@stud.h-da.de); **0. Abb.** Annette Rülke, DFN-Verein (ruelke@dfn.de); **13** Anna Maria Yang-Jacobi, Forschungsstelle Recht im DFN (a.yang-jacobi@fu-berlin.de); **14** Marc-Philipp Geiselmann, Forschungsstelle Recht im DFN (marc-philipp.geiselmann@uni-muenster.de); **15** Jochem Pattloch, DFN-Verein (pat@dfn.de)

Auf Wolke sieben? Cloud in Forschung und Lehre

Fotos: Maimona Id/DFN-Verein

Herausforderung Cloud: Seit 2019 engagiert sich Denise Dittrich von der RWTH Aachen University für den breiten Erfahrungsaustausch in Fragen der Cloud-Nutzung. Was es zu beachten gilt und welche Vorteile die OCRE-Rahmenverträge bieten, erzählt die Sprecherin des ZKI-Arbeitskreises Cloud Management im Interview.

Wie sind Sie zum Thema Cloud gekommen?
Ich war an der RWTH lange für zentrale Dienste auf Basis von Microsoft-Produkten wie Exchange oder SharePoint zuständig – alles On-Premises. Es hat sich schnell herausgestellt, dass Microsoft zunehmend eine klare Cloud-Strategie verfolgt. Wir mussten uns früh damit auseinandersetzen und sind dabei auf einige Herausforderungen gestoßen. Naheliegend war, dass wir nicht die Einzigen sind, die sich mit dem Thema befassen müssen. Der Wunsch nach einer Community, mit der gemeinsam diskutiert und Lösungen gefunden werden können, war groß. Ich bin ein Mensch, der gerne eigene Erfahrungen weitergeben und den gegenseitigen Erfahrungsaustausch fördern möchte.

Das Thema Cloud ist mein absolutes Herzensthema. Mein Engagement im ZKI (Verein der „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V.“) war darum ein logischer Schluss – zunächst in der temporären ZKI-Kommission Cloud, in der wir den konkreten Auftrag umgesetzt haben, einen Leitfaden zur Einführung von Cloud-Produkten an Hochschulen zu schreiben. Seit Frühjahr 2024 hat sich das Thema im Arbeitskreis Cloud Management (CLM) verstetigt. Ich freue mich, dass ich von Anfang an dabei sein konnte.

Was sind aus Ihrer Sicht die großen Katalysatoren bei der Nutzung von Cloud-Diensten?

Da sind zunächst einmal die starken Eigeninteressen der Public-Cloud-Hersteller. Das macht sich dadurch bemerkbar, dass immer mehr Produkte nur noch in der Cloud angeboten werden. Wir merken außerdem, dass der Funktionsumfang On-Premises stark eingeschränkt wird, was die Nutzung zunehmend unattraktiv macht. Zudem sind

> „Hochschulen können nicht mehr alles On-Premises bereitstellen.“

viele Dienste nur noch über ein Cloud-Konto beim Hersteller erreichbar, früher ging das noch über Lizenzschlüssel. Letztendlich müssen wir uns an diese neue Welt anpassen. Hochschulen können nicht mehr alles On-Premises bereitstellen. Eine Lösung ist, sich zusammenzutun. Community Clouds sind zum Beispiel eine gute Möglichkeit, die Souveränität zu wahren und Ressourcen zu bündeln.

Was bedeutet Souveränität im Zusammenhang mit Cloud-Leistungen?

Digitale Souveränität ist ein Wort, was gerade in aller Munde ist. Wenn ich zum Beispiel ein großes SAP-Produkt On-Premises hoste, von dem sämtliche Prozesse in der Verwaltung abhängen, bin ich dann souverän? Weiß ich nicht. Deswegen finde ich die Diskussion rein auf Cloud-Produkte bezogen zu kurz gedacht. Natürlich begebe ich mich mit der Nutzung von Cloud-Leistungen in Abhängigkeit zu einem Hersteller und gebe auch ein Stück weit die Hoheit über meine Daten ab. Darum kann Souveränität auch bedeuten, dass Hochschulen Alternativen anbieten, um Abhängigkeiten zu verringern und den Mitarbeitenden oder Studierenden eine Wahl zu lassen, wo sie ihre Daten ablegen oder welches Produkt sie für ein Szenario verwenden.

Das nennt sich Multi-Vendor-Strategie und ist eine Empfehlung, die wir den Hochschulen geben. Natürlich gibt es Grenzen: Keine Hochschule schafft sich beispielsweise noch eine zweite ERP-Software an. Darüber hinaus gilt: Für Produkte, die gut mit anderen interagieren oder fest in bestimmte Prozesse integriert sind, ist es oft schwierig, Alternativen zu finden.

Welche Treiber für Cloud-Nutzung gibt es intern?

Das sind in gewisser Weise die Nutzenden selbst, Stichwort verteiltes Arbeiten und Verfügbarkeit: Ob im Homeoffice in Düsseldorf oder im Büro in Berlin, seit Corona arbeiten wir wesentlich mobiler und von Standorten unabhängiger. Daraus ergeben sich natürlich ganz andere Anforderungen an die Produkte, die wir nutzen – und damit sind diese ebenfalls indirekte Treiber für die Cloud-Nutzung.

Forschende benötigen für weltweite Kollaborationen mit Projektpartnern außerhalb der eigenen Einrichtung Tools, mit denen sie unkompliziert kommunizieren und kollaborieren können. Das sind in der Regel Cloud-Lösungen. Die Anforderungen der Nutzenden werden immer heterogener. Sie wollen nicht mehr nur einen Datenbanktyp oder einen Storage-Typ, sie wollen ALLES.

Das ist ganz schön ehrgeizig.

Aber realistisch. Was zu beachten ist: Mit zunehmendem Einsatz von Cloud-Leistungen steigt auch die Eigenverantwortung der Nutzenden stark an. Das ist eine große Herausforderung für Einrichtungen. Wir wissen genau, was passiert, wenn wir keine Cloud-Dienstleistungen anbieten: Die Leute nutzen sie trotzdem. Sie suchen nach Möglichkeiten, ihren Bedarf einfach und schnell zu realisieren. Ich will gar nicht wissen, wie viele Hochschulangehörige ein Google-Konto mit ihrer Hochschul-Mail-Adresse haben. Das ist doch gang und gäbe.

Was ist das Problem?

Im schlimmsten Fall hat man als Hochschule keine Zugriffsmöglichkeiten auf solche Konten – damit auch nicht mehr auf die Daten, die im persönlichen Ablageort des Mitarbeitenden liegen. Das kann ein vertraulicher Projektantrag sein, an dem vielleicht Geld hängt. Wenn dann der Mitarbeitende nicht mehr in dem Projekt oder an der Hochschule arbeitet, kann die Einrichtung nicht mehr darauf zugreifen. Das ist ein nicht zu unterschätzender Kontrollverlust. Und um diese Dunkelziffer zu verringern, müssen wir gute Alternativen für die Nutzenden anbieten. Außerdem müssen wir die Nutzenden im Umgang mit Cloud-Services schulen und sensibilisieren. Dazu gehört auch die Klassifikation von Daten: Ist etwas streng vertraulich und welche Möglichkeiten der Ablage gibt es dafür? Das macht die Arbeitswelt natürlich um einiges komplexer. Letztendlich gilt das nicht nur für Cloud-Dienste. Datenschutz und Informationssicherheit sind ein grundsätzliches Thema.

Zur Wahrheit in puncto Sicherheit gehört aber auch: Was kritische Infrastrukturmaßnahmen angeht, sind die meisten Cloud-Anbieter im Gegensatz zu uns Hochschulen komplett zertifiziert – vorsichtig ausgedrückt. Manchmal hat es durchaus Vorteile, Cloud-Dienste zu nutzen.

Denise Dittrich
Studium der Künstlichen Intelligenz an der Maastricht University | 2010 bis 2012 stellv. Abteilungsleiterin IT-Servicedesk des IT Centers der RWTH Aachen University | 2012 bis 2015 Gruppenleitung Beratung und stellv. Abteilungsleiterin IT-Prozessunterstützung | seit 2015 stellv. Abteilungsleiterin der Abteilung Systeme und Betrieb | seit 2020 Leiterin der EUNIS Special Interest Group Cloud Management | seit 2024 Leitung der Cloud-Koordination der RWTH Aachen University | seit 2024 Sprecherin des ZKI Arbeitskreises Cloud Management

Welche Vorteile für Hochschulen sehen Sie noch?
Das sind ganz klar schnelle Verfügbarkeit, aber auch schneller Abbau, was zum Beispiel das Forschungs- und Projektgeschäft an Hochschulen unterstützt. Erreichbarkeit unabhängig vom Standort ist für mobiles Arbeiten ausschlaggebend. Kollaborationen sind wesentlich einfacher, weil es gemeinsame Standards und organisationsübergreifende Plattformen gibt. Ein weiterer Vorteil entsteht durch flexible Skalierungsmöglichkeiten. Nehmen wir das Semestergeschäft zu Beginn des Studiums, das viele Ressourcen benötigt, wenn alle Studierenden sich auf einmal einloggen. Entweder ich entscheide mich dafür, Hardware vorzuhalten, um den Semesterstart abzufangen, oder ich verlagere das in die Cloud. Dann kann ich zu Semesterstart für vier Wochen kurz hochskalieren und danach wieder runter. Das sind Effekte, die On-Premises nicht gehen. Ich stelle mir ja nicht für vier Wochen Hardware in die Maschinenhalle und reiße sie raus, um sie dann in sechs Monaten wieder anzuschaffen.

Aber um zu beantworten, welches die richtige Cloud-Lösung für eine Hochschule ist, braucht es ganz klar eine Strategie. Das kann dann Cloud first heißen, aber auch On-Premises first. Auch das ist eine Cloud-Strategie.

Was ist der allererste Schritt, wenn ich eine Cloud-Strategie aufbauen möchte?
Zunächst einmal ist es wichtig, Gremien und Interessensvertretungen frühzeitig mit ins Boot zu holen und nicht vor vollendete Tatsachen zu stellen. Es geht darum, alle Beteiligten auf einen Wissensstand zu bringen, um das Thema gut und neutral besprechen zu können. Das ist beim ersten Aufschlag aufwendig und bindet Ressourcen. Nur wenn ich verantwortungsbewusst mit dem Thema Cloud umgehe, baue ich intern Vertrauen auf – und das erleichtert das weitere Vorgehen ungemein.

Die größte Hürde ist, sich erst mal zu sortieren: Wo stehen wir, was wollen wir? Wie sind die Zuständigkeiten? Im ZKI-Kommissionsbericht empfehlen wir, sich einen Cloud-Anbieter herauszupicken und an diesem exemplarisch den gesamten Prozess abzubilden. Wir merken dabei – das betrifft generell das Thema Digitalisierung –, dass Sonderlocken schlecht funktionieren. Darum sind standardisierte Prozesse so wichtig, sowohl für Digitalisierungs- als auch für Cloud-Prozesse.

Natürlich gibt es intern auch Bedenken nach dem Motto „Cloud kommt von Datenklau“ und Fragen wie: Was bedeutet das für die Ressourcen? Werden wegen Cloud-Diensten Stellen abgebaut? Beim Thema Cloud geht es um Entscheidungsprozesse und die Diskussionen dazu können sehr emotional geführt werden.

Besteht denn die Gefahr, dass Stellen abgebaut werden?
Ich sehe keinen Abbau, sondern eher einen Umbau. Ich glaube, dass langfristig nicht weniger Personal, sondern anderes und vielleicht sogar mehr gebraucht wird. Je nach Strategie fallen vielleicht bestimmte Aufgaben in den Rechenzentren weg, weil zum Beispiel nicht mehr so viel Hardware benötigt wird. Es gibt tatsächlich Hochschulen, die eine Cloud-First-Strategie verfolgen

und bei neuen Hardware-Anschaffungen entscheiden, die Services direkt aus der Cloud zu beziehen. Aber ganz ehrlich, diese Veränderungsprozesse brauchen Zeit. Niemand baut von heute auf morgen seine Maschinen ab.

Brauche ich weniger oder mehr Ressourcen, wenn ich auf Cloud setze?
Ich brauche andere Ressourcen und anderes Know-how, zum Beispiel Personal mit anderen Fähigkeiten. Die Herausforderung bei der Cloud-Nutzung ist, diese in die Prozesse der Hochschule zu integrieren. Das heißt, ich brauche Leute, die Ahnung von Schnittstellen und Integration haben und weniger von Betrieb. Je nachdem, welche Cloud-Strategie man fährt, bleibt vielleicht nicht mehr

> „Ein Trend ist ganz klar die Bereitstellung von KI-Modellen als Community-Cloud-Lösung."

viel Betrieb übrig. Ich brauche Leute, die organisatorisch begabt sind wie etwa Cloud Service Broker. Diese kümmern sich nicht nur um die Auswahl und Vermittlung von Cloud-Diensten, sondern auch um das Management wie Bereitstellung, Skalierung und Interoperabilität. Darüber hinaus sind Menschen notwendig, die sich mit IT-Recht und Datenschutz auskennen, da sich in diesem Bereich Gesetzesgrundlagen häufig ändern, siehe Schrems I und Schrems II.

Inwieweit profitieren die Einrichtungen von den OCRE-Rahmenverträgen?
Wenn ich in den Infrastrukturbereich mit Cloud-Diensten gehen möchte, dann ganz klar über die OCRE-Verträge. Diese sind ein probates Mittel, wenn ich auf eine Multi-Vendor-Strategie setze. Aus dem großen Portfolio kann ich mir maßgeschneidert Cloud-Lösungen zusammenstellen. Außerdem ist gewährleistet, dass alle Rahmenbedingungen und Kriterien erfüllt sind – sei es in puncto Datenschutz, Authentifizierung, beschaffungsrechtlicher Vorgaben oder Rechnungsstellung. Ich habe Standards, auf die ich mich verlassen kann. Das ist ein riesiger Vorteil und eine Erleichterung für die Hochschul-Community.

Durch OCRE haben wir außerdem eine breite Basis zum Austausch und Vergleich, da alle anderen teilnehmenden Einrichtungen dieselben Verträge zu denselben Bedingungen nutzen.

Welche Trends beobachten Sie bei der Cloud-Nutzung momentan?
Ein Trend ist ganz klar die Bereitstellung von KI-Modellen als Community-Cloud-Lösung. Dabei werden zum Beispiel Open-Source-basierte KI-Modelle lokal aufgesetzt oder die API-Schnittstelle zu Public-Cloud-Modellen so verwendet, dass personenbezogene Daten anonymisiert werden. Das macht die GWDG (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen) beispielsweise mit ihrem Dienst Chat AI, der über die föderierten Cloud-Dienste des DFN-Vereins angeboten wird.

In NRW haben wir das Projekt KI:connect.nrw, das die Hochschulen des Landes bei der Bereitstellung kommerzieller generativer KI-Dienste unterstützt. Das nutzen gerade viele Einrichtungen, damit Hochschulangehörige ChatGPT nicht einfach unkontrolliert über den Browser nutzen. Außerdem gibt es einige Initiativen, KI-Dienste in die Lernmanagementsysteme der Hochschulen wie Moodle oder Ilias zu integrieren.

Was ist Ihre Prognose, was Cloud-Nutzung an Hochschulen angeht?
Meine Einschätzung ist, dass die Cloud-Nutzung noch ein Stück weit steigen und irgendwann stagnieren wird. Es wird wahrscheinlich auf ein hybrides Cloud-Modell aus Public Cloud und Community Cloud hinauslaufen, zu dem es immer noch Leistungen On-Premises gibt. Ich könnte mir vorstellen, dass gerade kleinere Hochschulen sehr viel in den Communitybereich investieren und Dienstleistungen anderer Einrichtungen bevorzugen– beispielsweise Rechenleistungen, wie sie der Verein für Nationales Hochleistungsrechnen (NHR-Verein) bereitstellt. Da geht es auch um Vertrauen, denn Hochschulen sind nicht kommerziell und unter Umständen kennen sich die Verantwortlichen untereinander sogar persönlich.

Ob Cloud first oder On-Premises first kann von unterschiedlichen Faktoren abhängen, unter anderem von den Ressourcen im Rechenzentrum oder sogar von der Cloud-Strategie meines Bundeslandes. In einigen Ländern gibt es klare Vorgaben. Wir nehmen derzeit im ZKI wahr, dass gemeinsame Lösungen von Hochschulen anstelle von „jede für sich allein" von den Ministerien der Bundesländer politisch stark gefördert werden.

Das Gespräch führte Maimona Id (DFN-Verein)

WEITERE INFORMATIONEN

Informationen zum Arbeitskreis Cloud Management gibt es unter:
https://www.zki.de/ueber-den-zki/arbeitskreise/arbeitskreis-cloud-management/

Die Publikation „Cloud Management" finden Sie unter:
https://www.zki.de/fileadmin/user_upload/Cloud_Management-Aenderung-in-Verwaltung-und-Bereitstellung.pdf

Unermüdlich im Einsatz – IT-Support mit KI

Teilnehmende Einrichtungen des DFN-Vereins können mithilfe der OCRE-Rahmenverträge für kommerzielle Cloud-Dienste unkompliziert Sprachmodelle für verschiedene Anwendungsfälle über die Plattform Azure OpenAI nutzen. Das Team der Abteilung Service & Kommunikation des IT Centers der RWTH Aachen University hat dieses Angebot verwendet, um zwei KI-gestützte Chatbot-Prototypen zu entwickeln. Diese setzen Sprachmodelle und Retrieval Augmented Generation ein, um den IT-Support zu unterstützen.

Text: **Sarah Grzemski, Ingo Hengstebeck**, **Marcel Nohl** (RWTH Aachen)

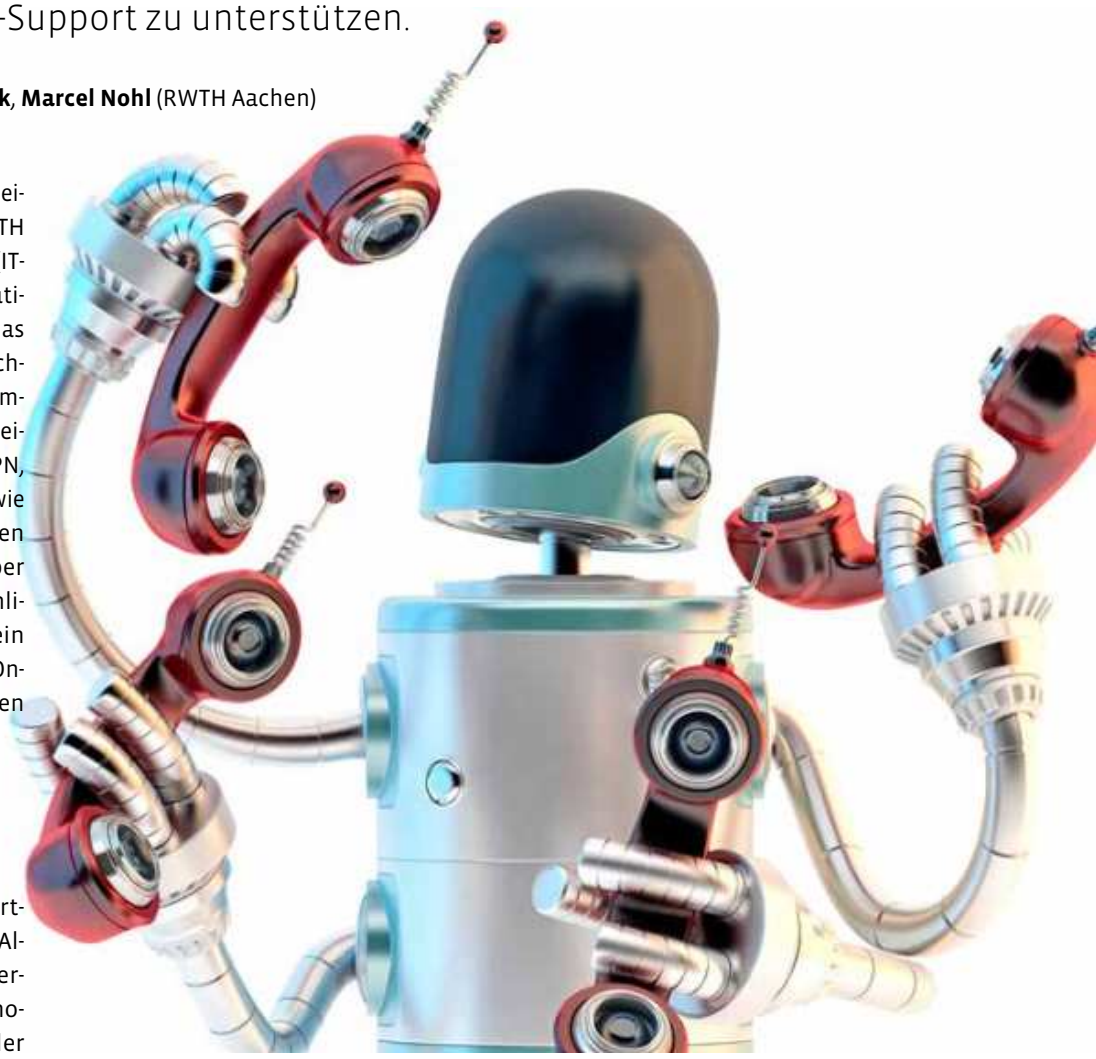


Foto: kirill_makarov/Adobe Stock

Für rund 55 300 Studierende und Mitarbeitende sowie externe Partner der RWTH Aachen University ist das IT-ServiceDesk (IT-SD) der Abteilung „Service & Kommunikation“ (SeKo) die zentrale Anlaufstelle, was das breit gefächerte Serviceangebot des hochschuleigenen IT Centers angeht. Dieses umfasst unter anderem unterschiedliche Bereiche wie Identity Management, WLAN, VPN, Forschungsdatenmanagement, E-Mail sowie viele weitere Services. Seit über 15 Jahren bietet das IT-SD breite Unterstützung per Telefon, E-Mail, Ticketportal und persönlichem Vor-Ort-Support an. 2015 wurde ein Support-Chat etabliert, der eine direkte Onlinekommunikation zwischen Nutzenden und Mitarbeitenden ermöglicht.

Im Dauereinsatz – die Anforderungen nehmen zu

Im vergangenen Jahr kam der Supportchat in rund 5 000 Fällen zum Einsatz. Allein im Jahr 2024 bearbeitete das IT-ServiceDesk circa 65 000 Anfragen. Diese hohe Zahl resultierte aus dem Anstieg der

Anzahl der Studierenden von 32 240 im Wintersemester 2010/11 auf 44 892 im Wintersemester 2024/25. Zusätzlich stieg das Angebot an IT-Services, insbesondere während der Coronapandemie, stark an. Zudem führte die erheblich wachsende Anzahl internationaler Studierender zu mehr Anfragen in englischer Sprache. Insgesamt entspricht das durchschnittlich über 250 teils komplexen Anfragen pro Arbeitstag – eine enorme Herausforderung für das Team des IT-SD.

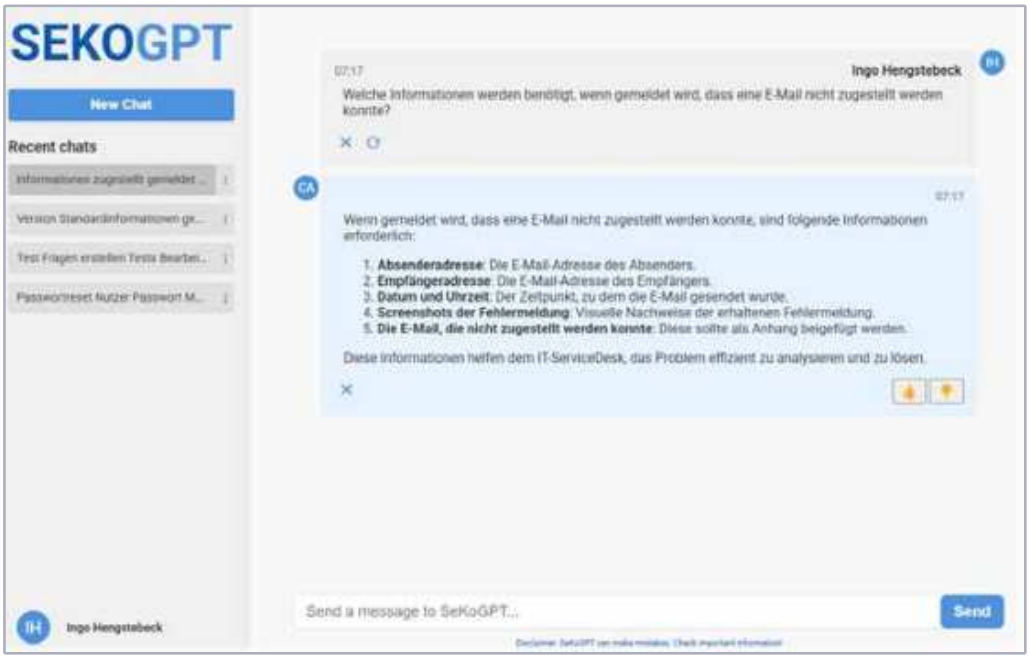


Abb. 1: Entlastung für das Team des IT-ServiceDesks – SeKoGPT für Mitarbeitende unterstützt bei Supportanfragen

Außerhalb der regulären Öffnungszeiten sind die Mitarbeitenden des IT-ServiceDesks nicht erreichbar. Das führt dazu, dass Anfragen, die am Wochenende gestellt werden, erst am Montag beantwortet werden. Darüber hinaus gibt es Stoßzeiten, in denen das IT-SD mit einem weit höheren Anfrageaufkommen konfrontiert ist. Diese Fälle treten nicht nur nach den Wochenenden, sondern auch zu Semesterbeginn oder bei Störungen von Services auf. Dabei kann es aufgrund des erhöhten Volumens für die Nutzenden zu längeren Wartezeiten kommen. Angesichts dieser Belastungen stellt sich die Frage: Wie kann das IT-SD auf der einen Seite den Bedürfnissen und Anforderungen der Nutzenden noch besser gerecht werden und gleichzeitig die Mitarbeitenden entlasten? Der Ansatz: ein KI-gestützter Chatbot mit Zugriff auf die interne Dokumentation des IT-ServiceDesks sowie die externe Supportdokumentation des IT Centers. Damit war die Idee zu SeKoGPT geboren.

Eine Idee und zwei Prototypen

Im August 2023 begannen die Tests einer über Microsoft Azure bereitgestellten OpenAI-Instanz. Diese konnte innerhalb der Rahmenverträge für kommerzielle Cloud-Dienste im Projekt Open Clouds for Research Environments (OCRE) über den DFN-Verein bezogen werden. Ziel war es zunächst herauszufinden, ob der Support durch den Einsatz von KI unterstützt werden kann. Letztendlich fiel die Wahl auf Microsoft Azure, da dort alle benötigten Komponenten wie LLM, Speicher und Suchdienst schnell und unkompliziert bereitgestellt werden. Dies ersparte den aufwendigen und teuren Aufbau einer eigenen Infrastruktur. Mit Unterstützung des Projekts KI:connect.nrw startete das ehrgeizige Projekt.

Im Dezember 2023 wurde ein erster Prototyp entwickelt, der neben der Funktionalität der bereitgestellten LLM zusätzlich auf Exporte der Wissensdatenbank des IT-ServiceDesk mittels Retrieval Augmented Generation (RAG) zugreifen kann, um Anfragen zu den Services des IT Centers zu beantworten. Die Erfahrungen aus dieser Phase führten 2024 zu der Fragestellung, wie Azure OpenAI in das IT-SD integriert werden kann. Ab Februar 2024 konnten zwei Prototypen unter dem Namen SeKoGPT getestet werden:

- **SeKoGPT** für Mitarbeitende sowie
- **SeKoGPT** für Nutzende des IT Centers

Die Instanz für Mitarbeitende ist ausschließlich Teammitgliedern der Abteilung SeKo vorbehalten. Der KI-Chatbot unterstützt sie bei der Beantwortung von Supportanfragen. Da ihm zusätzliche Inhalte aus der internen Wissensdatenbank zur Verfügung stehen, können Handlungsempfehlungen und Kurzanleitungen für Nutzende „on the fly“ erstellt werden. Auch das Zusammenfassen komplexer Supportanfragen und

KI:CONNECT.NRW

Seit der Einführung von ChatGPT ist der Bedarf an leistungsstarken, insbesondere generativen KI-Lösungen stark gestiegen. Hochschulen stehen dabei vor zusätzlichen Herausforderungen, etwa in Bezug auf Datenschutz und Beschaffung. Das Projekt KI:connect.nrw unterstützt die Hochschulen in Nordrhein-Westfalen bei der Bereitstellung und Nutzung generativer KI-Modelle, indem es einen zentralen, skalierbaren und kosteneffizienten Zugang zu KI-Diensten ermöglicht. Weitere Informationen und Ergebnisse finden Sie auf der Projektwebsite unter: **https://kiconnect.pages.rwth-aachen.de/pages/**

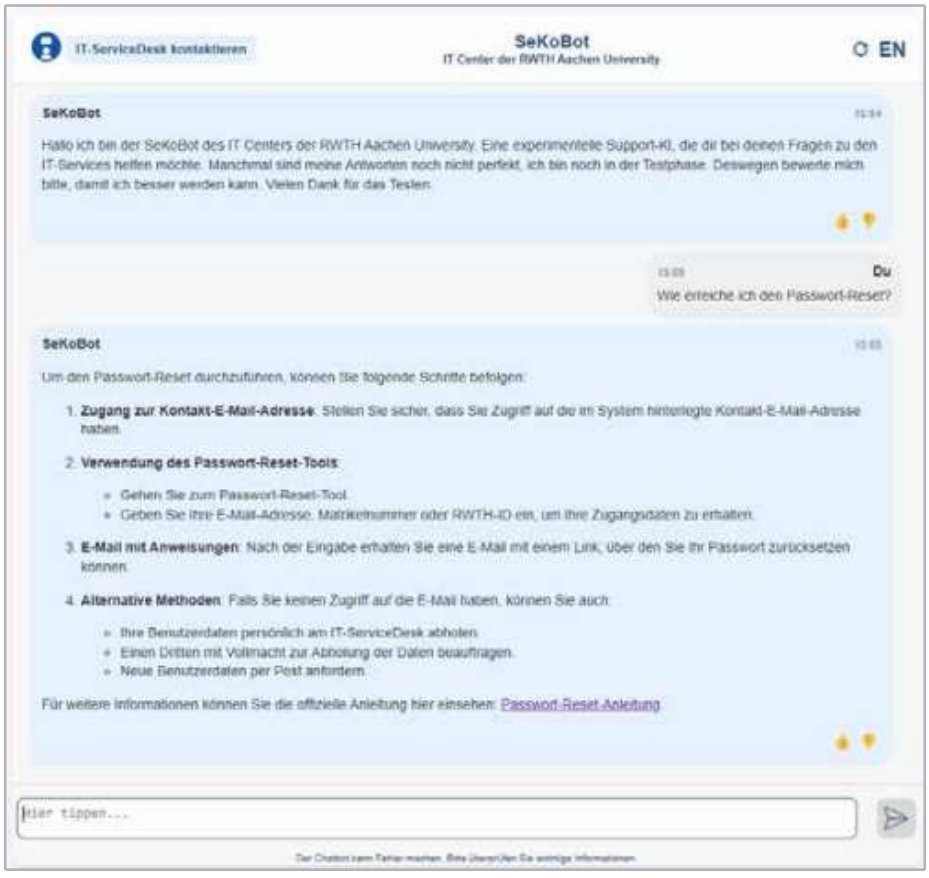


Abbildung 2: Echte Alternative zum Supportchat – SeKoGPT für Nutzende ist auch außerhalb der Öffnungszeiten im Einsatz

RAG: SO WIRD KÜNSTLICHE INTELLIGENZ NOCH TREFFSICHERER

Retrieval Augmented Generation (RAG) ist ein Verfahren, bei dem ein Sprachmodell nicht nur auf sein internes, vortrainiertes Wissen zurückgreift, sondern zusätzlich in Echtzeit relevante externe Informationen aus einer definierten Wissensbasis abruft:

1. Zunächst wird ein „Retrieval"-Schritt durchgeführt, bei dem das System gezielt nach Dokumenten oder Daten sucht, die inhaltlich zur gestellten Frage passen.
2. Diese abgerufenen Informationen werden anschließend dem Sprachmodell als Kontext bereitgestellt.
3. Auf Basis dieser zusätzlichen Daten generiert das Modell daraufhin eine Antwort, die sowohl die intern gespeicherten Informationen als auch die aktuellen, externen Fakten berücksichtigt.

Der Hauptvorteil von RAG liegt darin, dass das Modell so stets auf aktuelle und spezifische Informationen zugreifen kann – das ist insbesondere dann eine Hilfe, wenn das vortrainierte Wissen des Modells bereits veraltet oder unvollständig ist.

Formulierungshilfen für multilinguale Anfragen ist möglich. Dadurch können Effizienz, Konsistenz und Qualität des Supports erheblich gesteigert und die Mitarbeitenden entlastet werden.

Die Instanz für Nutzende steht allen Personen zur Verfügung, die Fragen zu den Services des IT Centers haben oder Hilfestellung benötigen. Damit bietet SeKoGPT eine Alternative zum bestehenden Support-Chat, da er auch außerhalb der regulären Öffnungszeiten im Einsatz ist. Die Beantwortung von häufig wiederkehrenden Standardfragen und -informationen können automatisiert werden. Sollte SeKoGPT einmal an seine Grenzen kommen, können Nutzende über das Frontend ein Ticket für die weitere Bearbeitung erstellen, das den gesamten vorherigen Chatverlauf beinhaltet. Alternativ haben sie künftig die Möglichkeit, sich von SeKoGPT aus an den bereits etablierten Chat-Support weiterleiten zu lassen. Der offizielle Start von SeKoGPT ist für die erste Jahreshälfte 2025 geplant. Ein neuer Name für den Chatbot soll diesen Meilenstein krönen.

Aktuell und faktenbasiert mit Retrieval Augmented Generation (RAG)

Im Laufe der Jahre haben das IT Center und das IT-SD eine umfangreiche externe und interne Wissensdatenbank zu sämtlichen Diensten entwickelt. Um dem KI-Chatbot dieses spezifische Wissen bereitzustellen, wird die KI-Technik „Retrieval Augmented Generation" eingesetzt, die Informationsabruf (Retrieval) mit Textgenerierung (Generation) kombiniert. Diese erlaubt es, eigene Wissensdatenbanken und/oder Dokumente als Informationsquellen bei der Beantwortung von Anfragen durch den KI-Chatbot zu nutzen. Verschiedene Exporte der Wissensdatenbank des IT-SD dienen als Grundlage für beide Prototypen. Im Falle der Instanz für Nutzende wird auf die umfangreiche externe Wissensdatenbank zurückgegriffen, bei der Instanz für Mitarbeitende kommt

noch die detaillierte interne hinzu. Über die API-Schnittstelle von Azure OpenAI wurden die verwendeten KI-Instanzen so konfiguriert, dass sie ausschließlich auf die genannten Datenbanken zugreifen. Dies sorgt zum einen für eine hohe Konsistenz bei der Beantwortung, zum anderen stellt es sicher, dass ähnliche oder gleichlautende Dienste anderer Anbieter von Informationen im Internet nicht mit den Services des IT Centers verwechselt werden.

Ein eingebautes Feedbacksystem sichert die Qualitätskontrolle

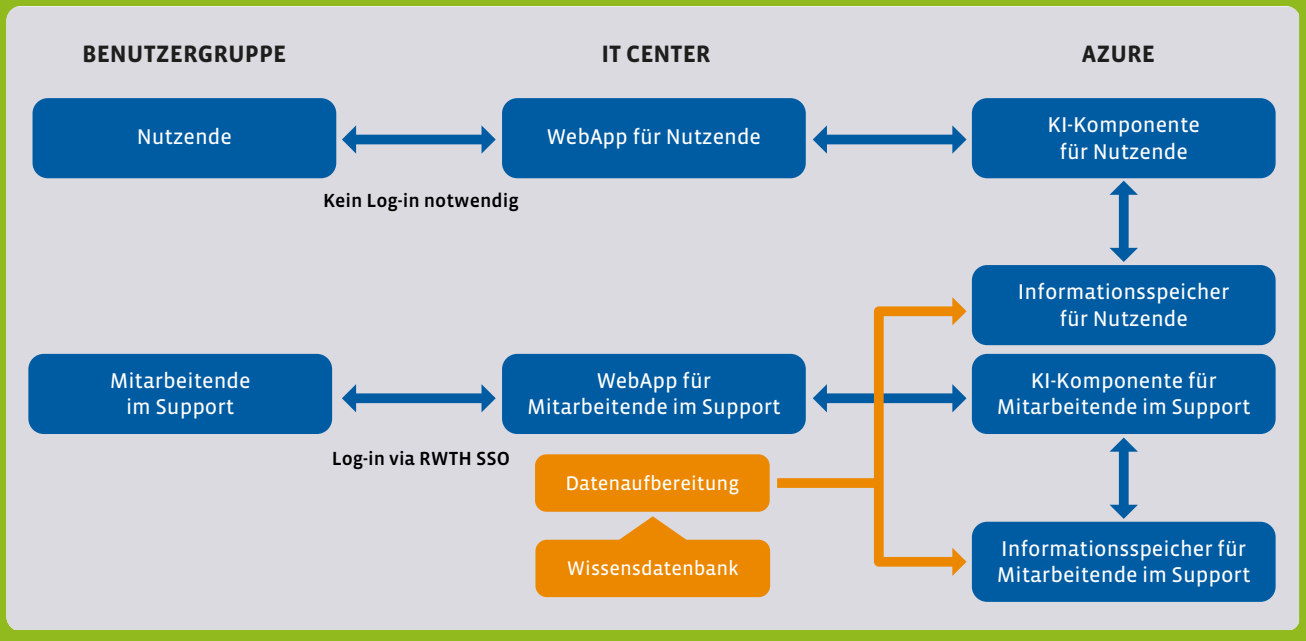
Um Rückmeldungen darüber zu bekommen, wie verständlich und zielführend die Antworten des KI-Chatbots jeweils sind, wurde ein einfaches Feedback-System implementiert, das auf „Daumen hoch“ und „Daumen runter“ basiert. So haben sowohl Mitarbeitende als auch Nutzende jederzeit die Möglichkeit, die Antworten des KI-Chatbots zu bewerten. Im Backend wird das eingegangene Feedback anonymisiert und in chronologischer Reihenfolge dargestellt. Anschließend können die Administrierenden diese Bewertung analysieren und die Dokumentation entsprechend anpassen. Bei einem negativen Feedback wird erstens geprüft, ob die Antwort des Systems fehlerhaft ist, zweitens, ob sie zu knapp oder übermäßig ausführlich ausfiel und drittens, ob die KI Begriffe durcheinandergebracht hat. Das Feedback-System dient so der kontinuierlichen Weiterentwicklung und Qualitätssicherung der Wissensdatenbank sowie von SeKoGPT selbst. Als zentrale Komponente von SeKoGPT wurde es so implementiert, dass das Geben eines Feedbacks so einfach wie möglich und außerdem universell verständlich ist. Dadurch wird der Anreiz, eine Meinung abzugeben, zusätzlich erhöht.

Integration in die bisherige Infrastruktur

Selbst die beste Dokumentation kann Lücken haben und eine KI schon mal „auf dem falschen Dampfer“ sein. Aus diesen Gründen ist es geplant, den KI-Chat in Zukunft tiefer in die bestehende OmniChannel-Anlage zu integrieren. Damit haben Nutzende die Möglichkeit, sich entweder direkt mit einem Support-Mitarbeitenden telefonisch verbinden zu lassen oder per Chat in Kontakt zu treten – zusätzlich zur Ticketerstellung über das Frontend des Chatbots. ◆

TECHNISCHE UMSETZUNG

Die Abbildung zeigt den schematischen Aufbau der technischen Umsetzung. Für die beiden Benutzergruppen wird auf Servern des IT Centers je eine Webapplikation bereitgestellt. Diese Webapplikationen greifen über eine API-Schnittstelle auf OpenAI-Instanzen (KI-Instanzen) zu, die über Microsoft Azure bereitgestellt werden. Innerhalb des IT Centers erfolgt zudem noch die Bereitstellung und Aufbereitung zusätzlicher Informationen für die beiden genutzten OpenAI-Instanzen. Nachdem die Daten innerhalb des IT Centers aufbereitet wurden, werden sie täglich automatisiert in eine Speicherkomponente übertragen, die ebenfalls über Microsoft Azure bereitgestellt wird. Die Datenaufbereitung muss zwingend erfolgen: Tests mit den reinen Exporten aus der Wissensdatenbank haben gezeigt, dass die Antworten nicht immer korrekt sind. Eine bessere Strukturierung der Daten schafft hier Abhilfe.



Der Cloud-Werkzeugkasten – eine Lösung für viele Szenarien

Wachsende Anforderungen in Forschung und Lehre bringen Hochschulrechenzentren zunehmend an ihre Grenzen. Neben leistungsstarken Netzen sind flexible Cloud-Lösungen gefragt, die Engpässe schnell überbrücken können. Die TU Berlin setzt dabei auf ein Baukastensystem.

Text: **Fatma Deniz, Thomas Hildmann** (Technische Universität Berlin)

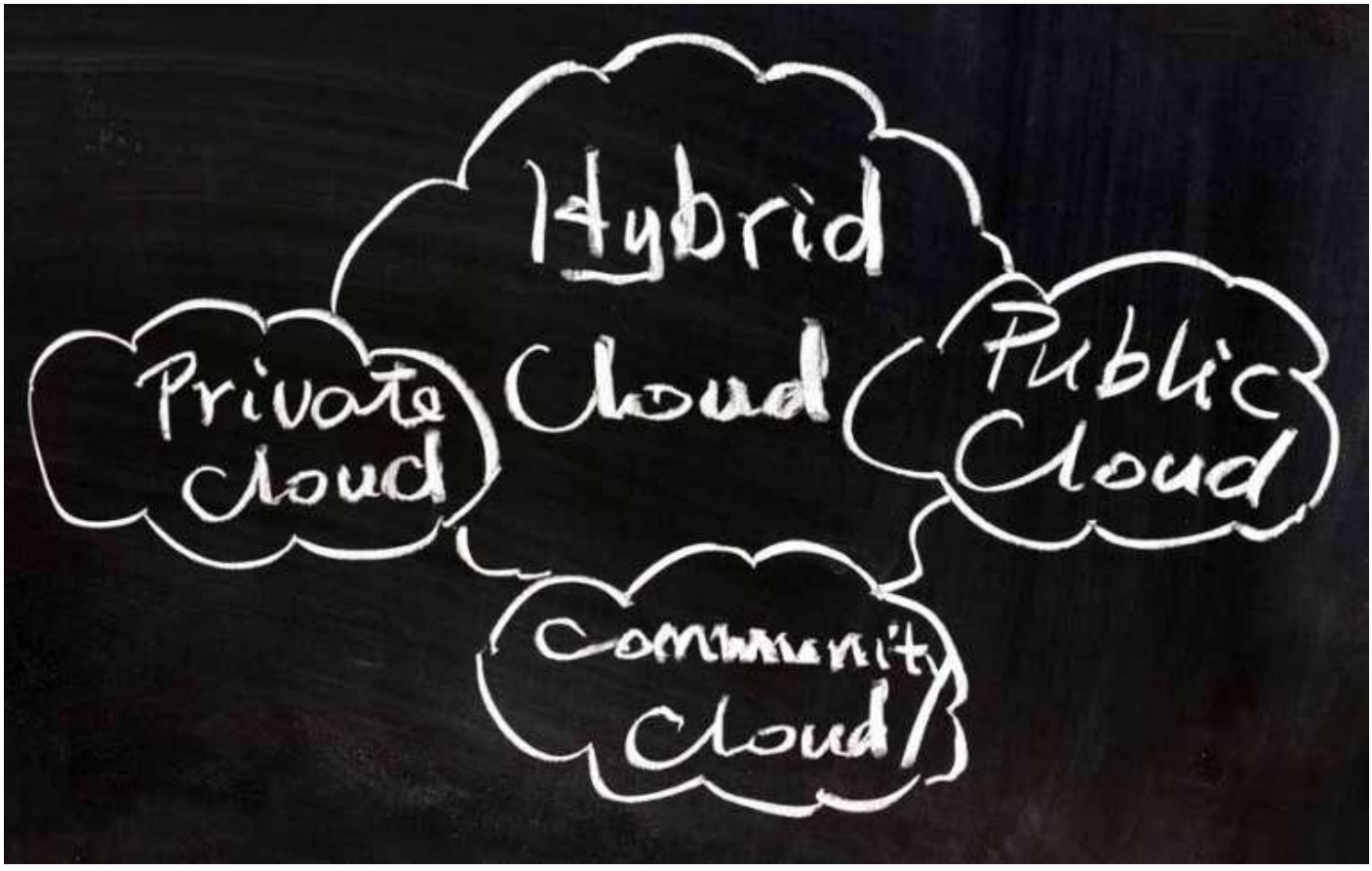


Foto: raywoo/Adobe Stock

Was für ein Monat! Oder war es nur eine Woche? Angesichts der sich überschlagenden Ereignisse in der Welt, im Land oder auch nur auf dem Uni-Campus verliert man langsam jedes Gefühl für die Zeit. Und das, obwohl wir doch im Kontext von Forschung und Lehre galoppierende Entwicklungen gewohnt sind. Sind wir doch selbst diejenigen, die mit neuen Erkenntnissen das Rad der Zeit immer schneller antreiben.

Nun stehen wir vor der Herausforderung, eine sich immer dynamischer entwickelnde Wissenschaft mit IT-Diensten versorgen zu müssen, während sich der Rest der Welt ebenfalls immer schneller ändert. Förderanträge und Haushaltsplanungen sind im Nu veraltet und die Anforderungen, die nicht zuletzt mit dem Einzug neuer KI-Anwendungen aus allen Richtungen erfolgen, treffen auf Grenzen in Bezug auf Zeit, Personal, Gebäude und Infrastruktur sowie Klimatisierung und Stromversorgung.

Der DFN-Verein ist Anbieter eines zeitgemäßen Netzwerks und unterschiedlicher Dienste sowie Vermittler und Halter von Rahmenverträgen. Er ist aber auch Broker und Unterstützer von kooperativen, föderierten Diensten zwischen den Hochschulen in ganz Deutschland. Damit steht uns ein zuverlässiger Werkzeugkasten zur Verfügung, aus dem wir uns für alle Eventualitäten bedienen können – sei es, um Engpässe zu überbrücken oder die Abhängigkeiten von Projekten zu entkoppeln, wie das Beispiel E-Kreide zeigt.

Schnell und unkompliziert – mit den OCRE-Rahmenverträgen

Seit vergangenem Jahr bietet die Zentraleinrichtung Campusmanagement (ZECM) der TU Berlin einen Hostingdienst auf Basis von OpenStack für ihre Einrichtungen an. Dieser löste den VMware-basierten Dienst ab. Leider gelang das nicht ganz lückenlos. Eine Zwischenlösung war gefragt, um beispielsweise das Programm E-Kreide zu hosten. Das Tool ersetzt die traditionelle Tafel und Kreide und ermöglicht es Lehrenden, Aufzeichnungen mit elektronischer Stifteingabe über ein interaktives Whiteboard zu übertragen und sogar online zur Verfügung zu stellen.

Da für den E-Kreide-Dienst dringend virtuelle Maschinen gebraucht wurden, entschieden wir uns, mithilfe der OCRE-Rahmenverträge übergangsweise das OpenStack der Telekom (Open Telekom Cloud) zu nutzen – so lange, bis unser eigener Hostingdienst zur Verfügung steht.

Die ZECM übernahm die Beschaffung („Call-Off“) des Cloud-Services für die gesamte TU Berlin. Der Vorteil: Interessieren sich künftig weitere Einrichtungen innerhalb der Universität für den Dienst, können jederzeit zusätzliche „Mandanten“ unterhalb der TU Berlin angelegt werden und die Rechnung kann gesplittet werden.

Cloud-Power gegen Engpässe

Die rapide steigenden Anforderungen an KI-Leistung bringen nicht nur unser Rechenzentrum an der TU Berlin an seine Leistungsgrenzen. Neben berlinweiten Lösungen – zum Beispiel einer Zusammenarbeit mit dem Zuse-Institut Berlin (ZIB) im Housing-Bereich für KI-Infrastrukturen – stehen auch andere Lösungen zur Diskussion: Um Platz, Kühlung und Strom zu schaffen, lassen sich insbesondere alte Server aus dem Housingbereich auf OCRE-IaaS-Dienste migrieren. Das bietet sich vor allem an, wenn Server-Erneuerungen oder aber umfangreiche Betriebssystemupdates anstehen. Gleiches gilt für große Mengen an Speicherplatz, der ebenfalls über die Rahmenverträge angemietet werden kann, wohingegen die Back-ups problemlos im eigenen Rechenzentrum Platz finden. Die schnelle Internetleitung des X-WiN und entsprechende Garantien der ausgewählten OCRE-Anbieter machen es möglich.

Der Cloud-Werkzeugkasten: Föderation Next Generation

Nicht nur die kommerziellen Cloud-Dienste stehen hoch im Kurs, auch die föderierten Cloud-Dienste des DFN-Vereins haben ein beachtliches Portfolio: Chat AI, der datenschutzfreundliche Dienst der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), bietet von der kostenlosen Nutzung über einen Account der Academic Cloud bis hin zur pseudonymisierten Nutzung von AI-Drittanbietern verschiedene Modelle an. So lag der integrative Schritt nahe, die föderierten Dienste „TU Berlin Collab Cloud” und „GWDG Chat AI” zusammenzuführen und damit einen neuen kombinierten Dienst zu schaffen, der allen am Wissenschaftsnetz teilnehmenden Einrichtungen zur Verfügung steht.

> So lag der integrative Schritt nahe, die föderierten Dienste zusammenzuführen.

Die „TU Berlin Collab Cloud” basiert auf der Software Nextcloud sowie Collabora online und bietet unter anderem Kollaborationstools zur Dateiablage und -synchronisation über verschiedene Endgeräte hinweg an. Mittlerweile besitzt die Nextcloud eine sehr gute KI-Integration (AI Assistant). Dabei ist es möglich, sowohl Open-Source-Modelle lokal auszuführen und abzufragen als auch Remote-Dienste aufzurufen.

Durch die Integration des KI-Modells in die Nextcloud stehen verschiedene Funktionen zur Verfügung:

- Chatten mit dem KI-Modell direkt in der Nextcloud-Web-GUI
- Generieren von Texten mithilfe der KI
- Zusammenfassen von Dokumenten, die in der Nextcloud gespeichert sind

Bereits vor der letzten Betriebstagung im März 2025 haben wir gemeinsam mit der

GWDG erfolgreich getestet, eine unserer Nextcloud-Instanzen über die API von Chat AI anzubinden und als Ergebnis einen integrierten Dienst aus zwei föderierten Diensten zu ermöglichen. Weitere Kombinationen aus den Nextcloud-Mailfrontends und der „GWDG-Open-Xchange“ oder der „HU-Mailbox“ wären beispielsweise denkbar.

Föderierte DFN-Cloud vs. OCRE IaaS

Mit Ausnahme der „heiCLOUD“ der Universität Heidelberg, die eine echte Alternative zu kommerziellen IaaS-Anbietern darstellt, handelt es sich bei den föderierten Diensten um komplette Anwendungen oder wie bei unserer „Collab Cloud“ sogar um eine Plattform zur Kombination von höherwertigen Diensten für Endanwenderinnen und -anwender.

Die föderierten Dienste stammen aus dem Hochschulkontext. Sie werden in der Regel für die eigene Einrichtung entwickelt und auch anderen Einrichtungen in Forschung und Lehre zur Verfügung gestellt. Darum sind sie sehr passgenau auf die Anforderungen von Hochschulen und Wissenschaftseinrichtungen zugeschnitten.

Die Entscheidung zwischen föderierten Cloud- oder OCRE-Angeboten kann unter anderem davon abhängen, ob Zertifizierungen oder beispielsweise Service Level Agreements (SLAs), wie bei kommerziellen Anbietern üblich, ein K.-o.-Kriterium sind oder ob es eher auf die Flexibilität und ein gemeinsames Serviceverständnis unter Hochschulrechenzentren ankommt. Denn erfahrungsgemäß ist ein Erprobungspartner (Terminologie aus den Verträgen der föderierten DFN-Cloud) in erster Linie ein Partner mit sehr ähnlichem Lehr- und Forschungsalltag und damit komplett nachvollziehbaren Problemen und Anliegen. Sehr selten vorkommende Differenzen werden in aller Regel zwischen den Partnern gelöst – mit der Option, den DFN-Verein zur Schlichtung einschalten zu können. In aller Regel handelt es sich um einen für beide Seiten geräuschlos laufenden Dienst. Anderenfalls könnten wir als TU Berlin den Dienst nicht über 30 anderen Institutionen anbieten.

Unser größter Kunde sind wir selbst. Aber gemeinsam können wir als Föderation gegenüber Hersteller- oder Entwicklerfirmen viel mehr erreichen, als es jede Einrichtung von uns alleine könnte. So geht es weiter in schnellem Tempo durch die unbeständigen Zeiten – aber wir können uns gegenseitig stärken, indem wir zuverlässige Kooperationen zwischen den Hochschulen aufbauen. ◆

ZECM: ZENTRALEINRICHTUNG CAMPUSMANAGEMENT

Die ZECM ist der zentrale IT-Dienstleister der TU Berlin. Neben der Bereitstellung des Netzwerks versorgen wir die zentrale Universitätsverwaltung vollumfänglich, betreiben die Verwaltungs-IT und stellen zahlreiche Infrastruktur- und Anwendungsangebote für alle Mitglieder der Universität zur Verfügung. Zu den Angeboten gehören auch die zentrale Beschaffung einiger universitätsweiter Lizenzen und Angebote Dritter.

TU BERLIN COLLAB CLOUD

Als eine der ersten großen Universitäten in Deutschland bot die TU Berlin schon 2013 einen Sync’n’Share-Dienst basierend auf der Software ownCloud für alle Hochschulangehörigen an. Seit 2017 basiert der Dienst auf der Software Nextcloud mit einigen Plug-ins, inklusive der auf Collabora basierenden Online-Office-Lösung.

Ist die Skalierung eines solchen Dienstes einmal für 30 000 Nutzende geschafft, so ist es ein kleiner Schritt, zusätzlich Instanzen für 2 500 oder 11 000 Nutzende von Nachbaruniversitäten aufzubauen und zu betreiben.

Heute stellen wir für über 30 Einrichtungen Nextcloud-Instanzen bereit und profitieren so von besseren Preisen für Compute- und Storage-Hardware und der Option, aufgrund der Größenordnungen höhere Flexibilität zu genießen und auch anbieten zu können. Bei einem halben Petabyte DFN-Cloud-Speicher in Summe ist die Anforderung „Wir bräuchten mal kurz 15 TB mehr” schnell umzusetzen.

Aktuell finanzieren wir auf Umlagebasis des föderierten Dienstes eine Stelle, sodass wir auch den 2nd-Level-Support anbieten können, den wir uns für unsere Partnereinrichtungen vorstellen.

Mehr Informationen zur „TU Berlin Collab Cloud“ gibt es unter: https://www.tu.berlin/go59747/.

Mit Rückenwind in die Cloud – OCRE 2024

Foto: Sergei Ginak/iStock

Seit Februar 2025 steht wissenschaftlichen Einrichtungen im DFN-Verein mit OCRE 2024 die dritte Generation an Rahmenverträgen für kommerzielle Cloud-Dienste zur Verfügung. Diese bieten nicht nur ein beeindruckendes Portfolio an innovativen Cloud-Diensten, sondern überzeugen auch mit zahlreichen Neuerungen.

Text: **Christian Meyer** (DFN-Verein)

Die Digitalisierung im Forschungs- und Hochschulbereich erfordert hocheffiziente Infrastrukturen, um den stetig wachsenden Anforderungen an Rechenleistung, Speicherplatz und Datenverarbeitung gerecht zu werden. Cloudbasierte Infrastrukturen ermöglichen, was Skalierbarkeit, Flexibilität und bedarfsgerechte Steuerung von Kosten angeht, vielversprechende Lösungen, die traditionelle On-Premises-Leistungen oft nicht bieten können.

Mit der Neuauflage der Rahmenverträge für kommerzielle Cloud-Dienste in „OCRE 2024“ (Open Clouds for Research Environments) haben teilnehmende Einrichtungen des DFN-Vereins auch künftig die Möglichkeit, aus einem breiten Portfolio Cloud-Infrastrukturangebote auszuwählen, die ihre spezifischen Anforderungen in Forschung und Lehre berücksichtigen. Die Rahmenverträge, die innerhalb des GÉANT-Projekts GN5-1 europaweit ausgeschriebenen wurden, stehen nun europäischen Forschungs- und

Abbildung 1: Verfügbare Plattformen in OCRE 2024. Die obere Reihe enthält die Plattformen mit den bewerteten Lieferanten, die untere Reihe zeigt Plattformen, die direkt vom Hersteller bezogen werden.

Bildungseinrichtungen in 39 Ländern zur Verfügung – in Deutschland über den DFN-Verein. Die Versorgung der am Wissenschaftsnetz teilnehmenden Einrichtungen mit Cloud-Services ist damit für die nächsten fünf Jahre sichergestellt.

Die Leistungen im Überblick

Mehr als 50 Unternehmen haben sich im Ausschreibungsverfahren beworben, auf dem deutschen Markt wurden dabei zehn verschiedene Plattformen angeboten. Der generelle Leistungsumfang ist unverändert umfangreich, die zentrale Leistung bleibt „Infrastructure-as-a-Service (IaaS)“, und auch dieses Mal hatten die Plattformbetreiber die Möglichkeit, weiterführende Dienste in Form von PaaS und SaaS einzubringen.

Unter den verfügbaren Cloud-Plattformen sind neben den bekannten US-amerikanischen Großanbietern, den „Hyper-Scalern“, auch deutsche beziehungsweise europäische Firmen. Diese decken teils sehr spezifische Anforderungen ab und erbringen forschungsnahe Leistungen wie die Bereitstellung und Prozessierung von Erdbeobachtungsdaten aus dem Copernicus-Programm. In dieser dritten Generation von Rahmenverträgen wurden – anders als bei den Vorgängerverträgen – bis zu drei Provider je Plattform zugelassen. Dies sorgt, neben mehr Flexibilität in der Leistungsbereitstellung, auch für eine Absicherung im Bestellvorgang der Produkte, sollten Lieferanten wegfallen.

Alle Angebote wurden vom GÉANT-Vergabeteam, an dem der DFN-Verein maßgeblich beteiligt war, in einem gemeinsamen Bewertungsprozess gewichtet. Daraus ergab sich für jede Cloud-Plattform eine Platzierungsliste der Anbieter.

Transparenz, Sicherheit und Nachhaltigkeit – die Mindestanforderungen

Die Mindestanforderungen der OCRE-Verträge setzen hohe Maßstäbe für Cloud-Dienste in Forschung und Lehre. Sie sorgen nicht nur für wirtschaftliche Transparenz und Datensicherheit, sondern tragen auch zu einer leistungsfähigen, nachhaltigen und zukunftsfähigen IT-Infrastruktur für wissenschaftliche Einrichtungen bei. Damit schaffen sie die Grundlage für eine effiziente und verantwortungsbewusste Nutzung von Cloud-Technologien in der Wissenschaft.

Transparente Preisgestaltung und flexible Lizenzmodelle

Ein wesentliches Kriterium der Verträge ist eine faire und transparente Preisgestaltung. Provider müssen einen Mindestnachlass von acht Prozent auf Listenpreise gewähren und eine klar definierte Währungsumrechnung sicherstellen. Zudem ist die Rechnungsstellung in lokaler Währung erforderlich, um den Einrichtungen eine einfache Abwicklung zu ermöglichen.

Ein weiterer wichtiger Punkt ist die Konfiguration der Cloud-Plattform. Identitätsmanagement über die bewährten AAI-Mechanismen muss gewährleistet sein, ebenso spezifischer Admin-Zugang für Superuser beziehungsweise Root-Zugriff.

Eine mandantenfähige Struktur, die es unterschiedlichen Einrichtungen ermöglicht, gemeinsam eine Cloud-Plattform zu nutzen, ist essenziell – ebenso wie das „Bring Your Own License“-Prinzip (BYOL), das den Einsatz schon vorhandener Softwarelizenzen ermöglicht. Lokaler Vor-Ort-Support sowie reichhaltige Schulungsangebote runden dieses Anforderungsprofil ab.

Unverändert hohe Standards bei Datenschutz und Sicherheit

Der Schutz der über die Cloud-Dienste verarbeiteten Daten hat oberste Priorität. Um teilnehmenden Einrichtungen die dafür notwendige Datenschutzbewertung zu ermöglichen, müssen Provider ein hohes Maß an Transparenz gewährleisten und dafür ein Datenschutzanalyseformular „GDPR Privacy Analysis Form“ vorweisen. Änderungen in der Datenverarbeitung, etwa durch den Wechsel von Unterauftragnehmern, sind aktiv mitzuteilen. Zudem sind Berichtsmechanismen für Sicherheitsvorfälle verpflichtend. Eine strikte Vorgabe ist, dass Dienstleister für das Training von Künstlicher Intelligenz keine Einrichtungsdaten verwenden dürfen.

Optimierte Konnektivität ohne versteckte Kosten

Für die Anbindung wissenschaftlicher Einrichtungen an die verfügbaren Cloud-Dienste ist eine leistungsfähige Netzwerkinfrastruktur erforderlich. Alle Anbieter müssen deswegen direkte Peerings mit GÉANT oder den nationalen Forschungsnetzen gewährleisten. Dadurch ist eine stabile und schnelle Datenkonnektivität sichergestellt. Die Kosten für die Datenübertragung entfallen in den meisten Fällen oder sind gedeckelt – insbesondere dürfen keine Ingress-Kosten (Kosten für Upload und Initialisierung von Daten) anfallen. Egress-Kosten (Kosten für Download und Schlussentnahme von Daten) müssen mindestens zu 15 Prozent des Umsatzes gedeckelt sein, um unerwartete Zusatzkosten für Forschungseinrichtungen zu vermeiden.

Detaillierte Abrechnung und übersichtliches Berichtswesen

Eine präzise und nachvollziehbare Kostenkontrolle ist für wissenschaftliche Einrichtungen wichtig. Daher schreiben die OCRE-Verträge eine Split-Billing-Funktion vor, die eine getrennte Rechnungsstellung für verschiedene Projekte, Institute oder Kostenstellen ermöglicht. Rechnungen müssen zudem elektronisch bereitgestellt werden. Ergänzend dazu gibt es ein detailliertes Berichtswesen, das eine monatlich zusammengefasste transparente Übersicht über die Nutzung und Abrechnung der Dienste bietet. In den Abrechnungen der Leistungen ist auch der Kostendeckungsbeitrag des DFN-Vereins, die sogenannte Cost Recovery Fee, enthalten. Für die Aufwände in der Bereitstellung und Vermittlung der unterschiedlichen Cloud-Leistungen erhält der DFN-Verein vier Prozent des angefallenen Umsatzes.

Nachhaltigkeit als zentrales Kriterium

Ein besonderes Augenmerk liegt auf der ökologischen Verantwortung der Cloud-Anbieter. Die Energieeffizienz in europäischen Rechenzentren muss mit einem Power Usage Effectiveness (PUE)-Wert unter 1,4 gewährleistet sein. Zudem wird ein steigender Anteil erneuerbarer Energien gefordert: Beginnend bei mindestens 70 Prozent soll dieser Wert bis 2030 auf 100 Prozent ansteigen. In die Wertung wurden auch Angaben zur CO_2-Bilanz einbezogen. Ergänzend zu diesen Kriterien sind individuelle Workshops und Nachhaltigkeitsanalysen vorgesehen, um den ökologischen Fußabdruck von Cloud-Diensten weiter zu optimieren. Darüber hinaus mussten die Bieter in der Angebotslegung ihre gesellschaftliche Unternehmensverantwortung offenlegen. Anbieter, die im Bereich der Nachhaltigkeit besonders hohe Standards erfüllen, konnten sich so als zukunftsfähige und verantwortungsbewusste Partner für teilnehmende Einrichtungen positionieren.

Das „Extra“ macht den Unterschied - die Mehrwertleistungen

Neben den Mindestanforderungen spielen bei OCRE auch eine Reihe zusätzlicher Bewertungskriterien eine Rolle. Mit Mehrwertleistungen, Barrierefreiheit, Nachhaltigkeit und Bildungsangeboten können sich Cloud-Provider positiv abheben. Diejenigen, die besonders gut abschnitten, konnten sich im Wettbewerb besser positionieren. Der Pluspunkt für teilnehmende Einrichtungen? Sie profitieren von besseren Serviceangeboten, finanziellen Vorteilen und zukunftsorientierten Cloud-Lösungen.

Umfassender Service und Exit Support

Zentrale Aspekte sind Service und Support. Provider müssen eine detaillierte Beschreibung ihrer Leistungen, ihres Organisationsprozesses sowie ihres Serviceangebotes vorlegen. Dazu gehört auch der Exit Support. Er stellt sicher, dass Einrichtungen ihre Daten

ENTWICKLUNG IN OCRE

2016 GÉANT schreibt die erste Generation von Cloud-Rahmenverträgen für „Infrastructure-as-a-Service (IaaS)“ aus. Obwohl Europa zu den weltweit größten Produzenten von Forschungsdaten gehört, bestehen nach wie vor administrative Hürden beim Zugang zu kommerziellen Cloud-Diensten. Ziel ist es, den Zugang für Forschende zu erleichtern.

2020 Aufgrund der starken Nachfrage wird eine Folgeausschreibung initiiert, neue Rahmenverträge folgen. Der Name dieser zweiten Generation von Verträgen lautet ursprünglich „IaaS+“ – mit einer großen Betonung auf dem Plus-Zeichen. Erstmals werden neben IaaS zusätzlich PaaS- (Platform-as-a-Service) und SaaS-Dienste (Software-as-a-Service) aufgenommen. Das Angebot weitet sich nun auf eine größere Anzahl von Ländern aus, um die Services über Initiativen wie die European Open Science Cloud (EOSC) zugänglich zu machen. Während dieser vierjährigen Vertragsphase startet in der EOSC ein Projekt namens OCRE, das die Etablierung und Nutzung kommerzieller Cloud-Infrastrukturen fördert.

2024 Das Projekt in OCRE ist längst Vergangenheit, der Name OCRE ist geblieben: Unter der Bezeichnung OCRE 2024 entsteht in einem neuen Vergabeverfahren die dritte Generation an kommerziellen Cloud-Diensten.

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

Mehr Informationen zu OCRE gibt es unter: **https://www.ocre-project.eu**

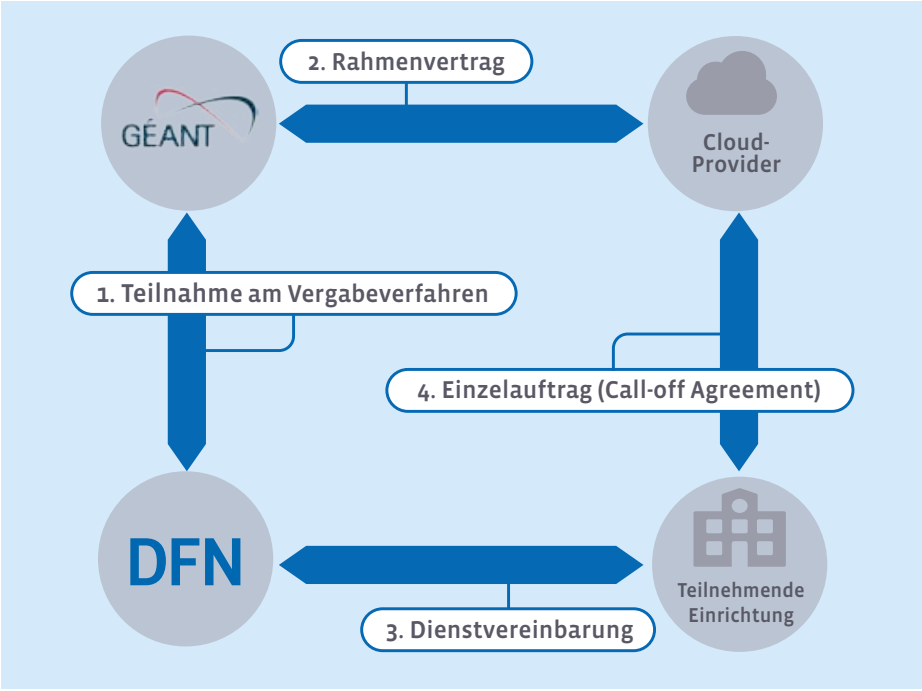


Abbildung 2: Beziehungsdiagramm für die neuen Rahmenverträge

problemlos exportieren und in andere Systeme übertragen können. Wichtige Punkte sind hier die Datenportabilität, die Extraktion von Metadaten und der Export großer Datensätze.

Unterstützung durch Informationsveranstaltungen
Damit Einrichtungen ihre Cloud-Dienste optimal nutzen können, ist Unterstützung in Form von umfassenden Informationsangeboten und Produktkommunikation erforderlich. Dazu zählen Workshops und Webinare für Anwenderinnen und Anwender.

Mehrwertleistungen und Bildung im Fokus
Anbieter können sich durch zusätzliche Mehrwertleistungen hervorheben. Dazu gehören beispielsweise Beratung oder Vor-Ort-Services, die eine zielgerichtete Unterstützung bei der Umsetzung von speziellen Anwendungsfällen ermöglichen.

Ein weiterer wichtiger Punkt ist „Cloud in the Classroom" – das sind spezielle, plattformorientierte Angebote mit Bildungscharakter. Diese sind einerseits für den Einsatz in der Lehre gedacht, um Studierenden aktuelle Cloud-Technologien näherzubringen. Andererseits sollen die Weiterbildungsangebote die eigene Belegschaft zur Nutzung dieser Cloud-Technologien befähigen.

Bestellprozess, Vertrags- und Leistungslieferwege

Dank des strukturierten und rechtskonformen Vergabeverfahrens in OCRE 2024 wurden Rahmenverträge abgeschlossen, auf die Einrichtungen bequem ohne weitere Ausschreibungsmaßnahmen zugreifen können. Dafür müssen sich diese lediglich an das Cloud-Team der DFN-Geschäftsstelle wenden.

Für den Bestellprozess wird – sofern noch nicht vorhanden – die (unentgeltliche) Dienstvereinbarung Cloud mit dem DFN-Verein abgeschlossen (Punkt 3 in Abb. 2). Daraufhin erhält die Einrichtung alle vergaberechtlich relevanten Unterlagen. Dazu gehört auch der Bestellvertrag für den Einzelauftrag („Call-Off Contract"), mit dem die Einrichtung direkt bei den Cloud-Providern die Leistungen abruft (Punkt 4 in Abb. 2). Bei dem Bestellvertrag handelt es sich um ein für IT-Beschaffungen standardisiertes Dokument. Um den Einrichtungen einen niederschwelligen Abruf zu ermöglichen, muss nur noch an den entsprechenden Stellen die zu bestellende Leistung ausgefüllt werden.

Bei der Auswahl der Provider für die gewünschten Leistungen gibt es je nach Ausgangslage unterschiedliche Vorgehensweisen: Anwendungsfälle, die auf einer spezifischen Cloud-Umgebung abgebildet sind, werden durch Direktvergabe via Kaskade beauftragt. Dabei werden Erstplatzierte der entsprechenden Plattformen direkt beauftragt. Falls diese die geforderte Leistung nicht liefern können (beispielsweise bei Lieferfristüberschreitung oder Ausscheiden vom Markt), wird auf zweitplatzierte Anbieter kaskadiert.

In Fällen, in denen die Plattform zur Umsetzung der Anforderungen noch nicht feststeht oder in denen spezifische Anforderungen erfüllt werden sollen, die über den im Vergabeverfahren beschriebenen Leistungsumfang hinausgehen, können Einrichtungen einen Miniwettbewerb veranstalten. Dazu wird der Wettbewerb zwischen den Erstplatzierten der verschiedenen Plattformen oder zwischen allen Anbietern einer spezifischen Plattform gestartet und diese zur Abgabe eines auf die individuellen Anforderungen bezogenen Angebotes eingeladen.

Mit OCRE 2024 ist es den nationalen Forschungsnetzen erneut gelungen, ihre geballte Verhandlungsmacht mit großem Erfolg zum Vorteil von zehntausenden wissenschaftlichen Einrichtungen in Europa einzusetzen und den Zugang zu innovativen und leistungsfähigen Cloud-Infrastrukturen in den kommenden Jahren zu decken. Die neue Vertragsgeneration erhöht zudem die Flexibilität, indem sie mehrere Provider pro Plattform zulässt und ermöglicht dadurch eine breite Auswahl an Cloud-Diensten. Durch transparente Preisgestaltung, hohe Datenschutzstandards, optimierte Netzwerkanbindung und nachhaltige Betriebsanforderungen bieten die Rahmenverträge für kommerzielle Cloud-Services eine zukunftsfähige Grundlage für Forschung und Lehre. ◆

Fit für die Zukunft – Technik-Upgrade im X-WiN

Das X-WiN, Rückgrat der Wissenschaft in Deutschland, hat ein Technik-Upgrade bekommen. Neue Core-Router mit 800 Gbit/s-Schnittstellen, eine leistungsfähige Optische Plattform und ein innovatives Echtzeitmonitoring sorgen für noch mehr Bandbreite, Ausfallsicherheit und Effizienz – insbesondere mit Blick auf die aktuelle Umsetzung der Leistungssteigerung des Dienstes DFN-Internet.

Text: **Maimona Id, Henry Kluge** (DFN-Verein)

Ob bahnbrechende Erkenntnisse in der Astrophysik wie die Entdeckung der Kilonova, Erkenntnisse in der Teilchenphysik wie der Nachweis des Higgs-Bosons oder die Analyse kompletter Genome – große wissenschaftliche Durchbrüche entstehen heute meist in disziplinübergreifenden internationalen Kooperationen. Forschungsverbünde mit mehreren Tausend Wissenschaftlerinnen und Wissenschaftlern sind längst Alltag. Dabei werden enorme Mengen an Forschungsdaten erzeugt, die nahezu in Echtzeit weltweit übertragen werden müssen.

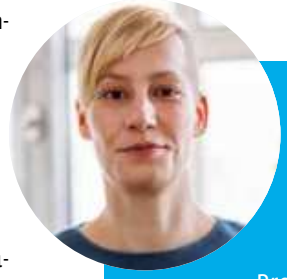
Um die Bandbreiten für solche Datenmengen verlässlich zur Verfügung stellen zu können, entwickelt der DFN-Verein sein Netz stetig weiter. In den vergangenen vier Jahren wurden darum die Optische Plattform umfassend modernisiert und die IP-Plattform vollständig erneuert – und damit optimal auf die kommende Leistungssteigerung vorbereitet.

Auf Leistungsfähigkeit ausgelegt

Mit dem X-WiN verfügt die Wissenschaft in Deutschland über ein eigenes Hochleistungsnetz, das sie selbst gestaltet und kontrolliert. Es verbindet über 850 Standorte im ganzen Land und öffnet den Zugang zu Tausenden Forschungseinrichtungen weltweit – über das europäische Wissenschaftsnetz GÉANT.

Das X-WiN zeichnet sich durch eine maßgeschneiderte, skalierbare Netzarchitektur aus, die höchste Flexibilität bei der Bandbreitennutzung ermöglicht. Die Kapazitäten lassen sich präzise an die individuellen Anforderungen der teilnehmenden Institutionen anpassen.

Im Zentrum der Weiterentwicklung der Netzinfrastruktur stehen drei zentrale Ziele: maximale Verfügbarkeit, hohe Fehlertoleranz und eine standardisierte, zukunftsfähige Servicearchitektur. Sämtliche aktiven Netzelemente sind redundant ausgelegt – so lassen sich Wartungen und Systemwechsel im laufenden Betrieb durchführen, ohne den Datenfluss zu unterbrechen. Auch die durchgehende Redundanz der Leitungswege leistet einen wesentlichen Beitrag zur Stabilität und Zuverlässigkeit des Netzes.



Jacqueline Struyken, DFN-Standortverwaltung: „Zu Beginn war vieles neu – vom Konzept bis zur Hardware. Mit kontinuierlicher Abstimmung und auch Flexibilität in der Zusammenarbeit ließen sich fast alle Probleme lösen. Das Schönste: Wenn neue Infrastruktur in Betrieb ging, leuchteten nicht nur die LEDs – sondern vor allem unsere Augen."

Frisch getuned – das wurde modernisiert

Eine Infrastruktur wie das X-WiN fit für die Zukunft zu machen, ist kein Projekt von der Stange. Es braucht kluge Planung, verlässliche Partner und viele exakt aufeinander abgestimmte Schritte – über Jahre hinweg.

Robert Stoy, DFN-NOC: „Die Koordination der vielen parallel stattfindenden Arbeiten war sehr komplex. Neben dem Umzug von Teilnehmern und Services musste die automatisierte Konfigurationserstellung weiterentwickelt und Datenbanken angepasst werden. Herausfordernd war die Inbetriebnahme der 400 Gbit/s-Schnittstellen zwischen dem Optischen Netz und den Routern. Der Kraftakt hat sich gelohnt. Zu wissen, welche Unterstützung wir für Forschung und Lehre leisten, ist nach wie vor eine große Befriedigung."

Die nachfolgenden Beispiele geben einen kleinen Einblick in die vielen Puzzlestücke, die es braucht, um ein Netz für die Wissenschaft von morgen zu bauen.

Konfigurierbare Bandbreite dank Flex-Grid

Bereits 2021 hat der DFN-Verein begonnen, an den Kernnetzknoten Flex-Grid-fähige ROADMs (Rekonfigurierbare Optische Add-Drop-Multiplexer) zu installieren. Die Flex-Grid-Technologie bietet den entscheidenden Vorteil, dass die Bandbreite einzelner Wellenlängenkanäle im optischen Netz flexibel angepasst werden kann. Während früher eine feste Kanalbreite von 50 GHz vorgegeben war, erlaubt Flex-Grid die Zuweisung von Bandbreite in feinen 6,25 GHz-Schritten. Dadurch können Kanäle bedarfsgerecht mit 50, 100 oder 150 GHz betrieben werden. Durch diese flexible Nutzung des Frequenzspektrums lassen sich Bandbreiten von über 100 Gbps pro Wellenlänge realisieren – eine wichtige Voraussetzung für die Skalierbarkeit der optischen Infrastruktur. Zusätzlich zum Hardwareeinbau waren umfangreiche Upgrades der Soft- und Firmware erforderlich.

Neue Router für die Aggregationsplattform

Im Jahr 2023 wurden sämtliche Router der Aggregationsplattform

Thomas Schmid, DFN-NOC: „Die größte Herausforderung war die Integration eines neuen Herstellers und die Migration unserer Servicearchitektur – während des laufenden Betriebes. Spannend war, ob am Ende alles wie geplant funktioniert. Nach harten und intensiven Monaten konnten wir die Umbauten schließlich termingerecht und erfolgreich abschließen."

WAS DIE PLATTFORMEN IM X-WIN LEISTEN

Die Faserplattform bildet das Fundament des X-WiN: Rund 10 250 Kilometer Glasfaserpaare verbinden bundesweit insgesamt 66 Kernnetzstandorte miteinander. Sie dienen als Transportmedium und leiten die Daten – buchstäblich mit Lichtgeschwindigkeit (in Glas 200 Tkm/s). Jeder Standort ist dabei über mindestens zwei unabhängige Strecken erreichbar – ein wichtiger Beitrag zur Ausfallsicherheit.

Die Optische Plattform wandelt elektrische Signale mithilfe von optischen Transpondern und Muxpondern in Lichtsignale um. Sie sind die Schnittstelle zur IP-Plattform. Muxponder ermöglichen zusätzlich die Bündelung mehrerer Signale auf einem einzigen Wellenlängenkanal.

Die Lichtsignale werden anschließend über das sogenannte DWDM-System (Dense Wavelength Division Multiplexing) übertragen. An jedem Kernnetzstandort sorgt diese Technik dafür, dass mehrere Datenströme gleichzeitig – auf unterschiedlichen Wellenlängen – durch eine Glasfaser geschickt werden können. Mithilfe dieser Technologie werden auf der Glasfaserplattform Punkt-zu-Punkt-Verbindungen zwischen den Kernnetzknoten hergestellt. Für die Weiterleitung der Lichtsignale sorgen Flex-Grid-fähige ROADMs (Reconfigurable Optical Adddrop Multiplexer).

Die IP-Plattform sorgt mit ihren Routern und Switches für die richtige „Weichenstellung" im Netz und damit für den schnellen und sicheren Datentransport zwischen den Einrichtungen – auch bei hohem Datenaufkommen oder Ausfällen einzelner Komponenten.

Konkret setzt sich die IP-Plattform aus zwei Ebenen zusammen: dem IP-Core mit acht leistungsstarken Routern an zentralen Netzpunkten sowie der Aggregationsplattform mit 58 weiteren Routern. Diese beiden Ebenen bilden gemeinsam ein hochverfügbares, redundantes Routing-Netz, das auf den Verbindungen der Optischen Plattform aufsetzt.

gegen leistungsfähigere Geräte ausgetauscht. Insgesamt wurden 58 neue Systeme an 56 Standorten erfolgreich migriert. Die neue Plattform bietet mit 2,4 Tbit/s die sechsfache Routingkapazität der bisherigen Lösung (400 Gbit/s). Damit ist es nun möglich, auch an den Aggregationsstandorten Anbindungen mit 100-Gigabit-Ethernet bereitzustellen – was zuvor nur an den acht Core-Routern realisiert werden konnte.

Upgrade-Vorbereitung: 800-Gigabit-Backbone für den IP-Core

Im Zuge der Vorbereitung künftiger Leistungssteigerungen wurde ein neuer optischer Backbone mit 800 Gbit/s Kapazität für den IP-Core aufgebaut. Dafür kam eine neue Generation DWDM-Systeme mit leistungsstarken Transpondern zum Einsatz. Diese bieten zwei unabhängige Verbindungen mit 400 Gbit/s bzw. 800 Gbit/s. und können als Regeneratoren für lange Distanzen genutzt werden – bei einer maximalen Leistungsaufnahme von nur 210 Watt. Die Schnittstellen in Richtung der Router sind derzeit für 400 Gigabit Ethernet ausgelegt. 800 GE-Schnittstellen werden dann voraussichtlich Ende 2026 verfügbar sein.

Erneuerung der Core-Router im Kernnetz

Im Jahr 2024 wurde das Herzstück des Wissenschaftsnetzes modernisiert: die Core-Router im Kernnetz. Dabei ging es nicht nur um neue Hardware, sondern auch um einen kompletten Herstellerwechsel – von Cisco zu Nokia. Zum Einsatz kommen nun

Jochen Schönfelder, DFN-CERT Projekt- und Entwicklungsteam: Wir mussten eine Messplattform auf Basis von Telemetry entwickeln, die DDoS-Erkennung und -Abwehr komplett umbauen und wegen des Herstellerwechsels Zusammenhänge neu erlernen – vieles auf der Grundlage von Dokumentationen. Spannend war, ob die Theorie der Realität standhält. Es war ein großartiger Moment, als die neuen Router produktiv gingen.

Servicerouter vom Typ Nokia 7750 SR, leistungsstarke Chassis-Systeme mit einer Gesamtkapazität von bis zu 108 Tbit/s im Endausbau. Unterstützt werden Schnittstellen mit Übertragungsraten von bis zu 800 Gbit/s. Die Line-Cards der neuen Router bieten 36 QSFP-DD-Schnittstellen und eine Routing-Performance von 12 Tbit/s – ideal für datenintensive Anwendungen und wachsende Anforderungen. Neben der gestiegenen Bandbreite bringt die neue IP-Technik auch ökologische Vorteile: Dank moderner Netzprozessoren konnte der Energieverbrauch deutlich gesenkt werden. Die Modernisierung zahlt sich also nicht nur technisch, sondern auch energetisch aus.

Karsten Kuschel, DFN-Standortverwaltung: „Von der Bestellung der Router-Schränke über die Stromversorgung bis hin zum Einbau der Nokia-Router – die Koordination aller Gewerke vor Ort an den einzelnen Standorten war eine echte Herausforderung. Umso beeindruckender war die reibungslose Zusammenarbeit mit Nokia und allen Partnern: präzise abgestimmt bis ins Detail, hochprofessionell und mit vollem Einsatz."

Analyse in Echtzeit – durch modernes Monitoring

Parallel zur Installation der Hardware wurden die neuen Router in das Echtzeitmonitoring-System DMon integriert. Es liefert Analysen zum aktuellen Betriebszustand, erkennt Störungen frühzeitig und unterstützt eine stabile Netzverfügbarkeit. Der Herstellerwechsel erforderte dabei eine Reihe technischer Anpassungen – insbesondere bei Schnittstellen und Protokollen – um die Einführung der Streaming-Telemetrie zu ermöglichen. Das Ergebnis: ein deutlich leistungsfähigeres Monitoring mit fünfmal mehr Messpunkten und Alarmierungen in unter einer Minute.

Sanfte Migration – im laufenden Betrieb

Insgesamt wurden über 1 000 Teilnehmeranschlüsse für die Dienste DFN-Internet und DFN-VPN auf die neue Plattform migriert – ohne längere Unterbrechungen. Ein echter Kraftakt, der nur durch präzise Planung und abgestimmte Zusammenarbeit aller Beteiligten möglich war. Mit der Inbetriebnahme der neuen Core-Router ist die seit 2021 laufende Modernisierung des X-WiN erfolgreich abgeschlossen. Auch das Vergabeverfahren für die Teilnehmeranschlüsse im Zugangsnetz wurde in diesem Zeitraum beendet und bildet ein weiteres Puzzlestück zur Umsetzung der Leistungssteigerung des Dienstes DFN-Internet.

Resümee der Modernisierung

Viele Köpfe, ein Ziel: Die Rundumerneuerung des X-WiN war ein Kraftakt, getragen von den Expertinnen und Experten der DFN-Geschäftsstelle und des DFN-CERT. Ihr Einsatz verdient große Anerkennung.

Das Ergebnis kann sich sehen lassen: Mit moderner Technik, leistungsfähiger Infrastruktur und höchster Verfügbarkeit gehört das X-WiN heute zu den leistungsstärksten Wissenschaftsnetzen weltweit – bereit für die Herausforderungen von morgen. ◆

Das X-WiN auf einen Blick

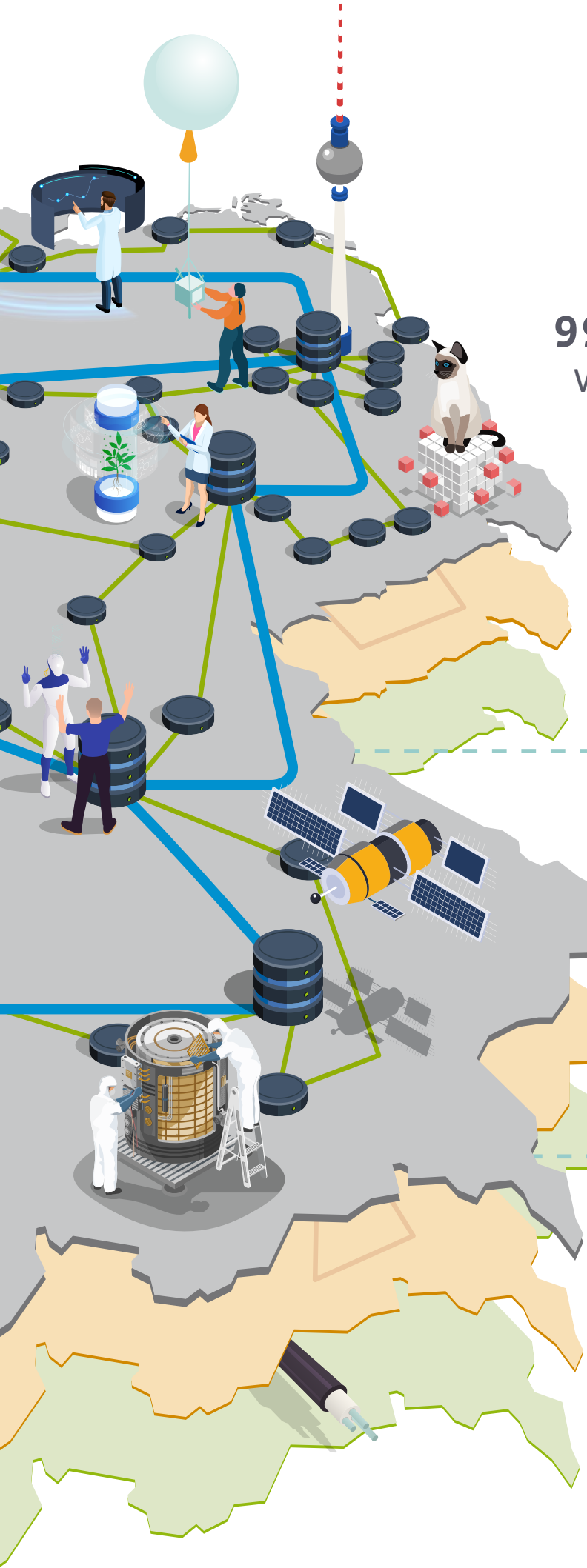
8
Core-Router

58
Aggregationsrouter

66
Kernnetzknoten

1 088
Teilnehmer

10 250 km
Glasfaserkabel



99,993 %
Verfügbarkeit Dienst DFN-Internet

400 Gbit/s
Anschlusskapazitäten

800 Gbit/s
max. Übertragungskapazitäten

146 233,370 TByte
Transf. Datenvolumen/März 25

Kurzmeldungen

Mehr Kapazität an den X-WiN-Außenanbindungen

Erfolgreiches Upgrade der X-WiN-Außenanbindungen: Mitte März 2025 hat der DFN-Verein die Übertragungskapazität der Übergänge zum europäischen Verbindungsnetz der GÉANT Association in Frankfurt/Main und Hamburg von je 300 Gbit/s auf je 400 Gbit/s erhöht. Mit einer Gesamtkapazität von 800 Gbit/s wurde die Konnektivität zu den europäischen und internationalen Forschungsnetzen noch einmal deutlich gesteigert. Darüber hinaus schafft der Technologiewechsel auf 400-Gigabit-Ethernet (400 GE) Optionen für den weiteren Ausbau der Übergänge in den Bereich von Terabit pro Sekunde. ◆

DFN-MailSupport: Neuer Virenscanner in Betrieb

Anfang 2025 hat ein Wechsel der Virenscanner in DFN-MailSupport stattgefunden. Die Ergebnisse von drei verschiedenen Virenscannern fließen in der Regel in die Bewertung von potenziell schädlichen E-Mails ein. Bisher waren das die Produkte von Clam-AV, F-Secure und Sophos. Seit Januar 2025 ist außerdem „Avast Business Antivirus for Linux“ im Einsatz und löst damit „Central Intercept X Advanced for Server“ aus dem Hause Sophos ab. Das DFN-MailSupport-Team überprüft regelmäßig die Erkennungsraten der eingesetzten Scanner, um auch in Zukunft für maximale Sicherheit in den Postfächern der X-WiN-Community zu sorgen. ◆

Neuer Rekord für den DFN-Terminplaner

Anfang April 2025 wurden zum ersten Mal mehr als eine Million aktive Abstimmungen gleichzeitig auf dem DFN-Terminplaner betrieben. Zu den Abstimmungen zählen Terminabstimmungen (946 796), Buchungslisten (36 462) und Umfragen (18 129). Und als wäre das nicht genug, wurde auch noch die Marke von acht Millionen gleichzeitig abgegebenen Stimmen geknackt. Was bedeutet „gleichzeitig abgegebene Stimmen“? Ganz einfach: So viele Stimmen wurden in den aktuellen, noch offenen Umfragen abgegeben und warten darauf, ausgewertet zu werden. Auf dem System befinden sich zudem rund 150 000 aktive Nutzerkonten, versendet werden monatlich etwa 200 000 E-Mails.

Der DFN-Terminplaner bietet außerdem die Möglichkeit, alle Abstimmungen mit einem Passwortschutz zu versehen. Mit der neuen Funktion können Nutzende sicherstellen, dass ihre Eintragungen nur von den vorgesehenen Teilnehmenden eingesehen werden können.

Seit vergangenem Jahr ist der DFN-Terminplaner in die DFN-AAI integriert und mit föderiertem Log-in nutzbar. Damit können Nutzerinnen und Nutzer der angeschlossenen Einrichtungen komfortabel und sicher auf den Dienst zugreifen. Die Integration ermöglicht eine nahtlose Authentifizierung und trägt zur weiteren Vereinfachung der Zusammenarbeit innerhalb der Wissenschafts- und Forschungsgemeinschaft bei. ◆

DFN-Cloud: Start des Mailbox-Dienstes der Humboldt-Universität zu Berlin

Der Mailbox-Dienst der Humboldt-Universität zu Berlin (HU) stellt seit März 2025 den am Wissenschaftsnetz teilnehmenden Einrichtungen des DFN-Vereins virtualisierte Mailboxen in einer hochverfügbaren Cloud-Infrastruktur bereit. Der Zugriff erfolgt TLS-verschlüsselt über IMAP auf Grundlage von Dovecot bzw. dem Webmailer Roundcube, beides freie Software. Der Speicherbedarf pro Mailbox wird mit durchschnittlichen 1 GB kalkuliert. Bei Mehrbedarf wird der Preis pro Mailbox entsprechend jährlich angepasst.

Die Verwaltung der E-Mail-Accounts, der First-Level-Support sowie der Transport und SPAM- und Virenschutz liegen bei der nutzenden Einrichtung. Die HU sorgt für Betrieb, Sicherheit und regelmäßige Back-ups mit Desaster-Recovery.

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

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

„Alte Abkürzung mit neuem Inhalt“ – VCC erweitert Themenspektrum

Das Kompetenzzentrum für Videokonferenzdienste im DFN-Verein wurde Anfang des Jahres umbenannt und heißt nun „Videoconference & Collaboration Center“. Die Abkürzung VCC bleibt – schließlich ist sie in der Wissenschaftscommunity schon lange als Markenzeichen etabliert. Mit dem neuen Namen soll die inhaltliche Erweiterung zum Ausdruck gebracht werden. Ab Januar 2025 geht das VCC über reine Videokonferenzdienste hinaus und widmet sich auch anderen spannenden Technologien der soft- und hardwarebasierten Kommunikation und Kooperation im Bereich Collaboration Services. Außerdem konnten die Verträge für die Fortsetzung des Projekts zu Beginn des Jahres erfolgreich verlängert werden. Das VCC ist an der TU Dresden angesiedelt. Als Projekt des DFN-Vereins war es maßgeblich am Aufbau der audiovisuellen Dienste für die Wissenschaft in Deutschland beteiligt. ◆

Alle Informationen zum VCC unter:
https://tu-dresden.de/zih/vcc

Auf in die nächste Runde: Rahmenverträge für cloudbasierte Videokonferenzdienste

Die Vorbereitungen für die Neuausschreibung der Rahmenverträge für cloudbasierte Videokonferenzdienste laufen seit März 2025 auf Hochtouren. Das Vergabeverfahren startet voraussichtlich in der zweiten Jahreshälfte 2025. Dafür erarbeitet das DFN-Conf-Team derzeit – gemeinsam mit der Arbeitsgruppe VIKTAS (Videokonferenztechnologien und ihre Anwendungsszenarien) der Deutschen Initiative für Netzwerkinformation e. V., DINI, sowie dem Arbeitskreis Medienkonzepte und Technologien des Vereins der „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V.“, ZKI – die aktuellen Anforderungen für Web- und Videokonferenzen. Das ist notwendig, weil in den vergangenen vier Jahren eine Vielzahl neuer Funktionen bei den Cloud-Videosystemen – beispielsweise im Bereich Barrierefreiheit – hinzugekommen sind. Relevant für die Ausschreibung sind außerdem gesetzliche Entwicklungen hinsichtlich künstlicher Intelligenz.

Die aktuellen Rahmenverträge enden im März 2026. Bis dahin sind Einzelaufträge mit einem Jahr Laufzeit plus optionaler zwölfmonatiger Verlängerung möglich. Das ergibt eine potenzielle Handlungsfähigkeit bis März 2028. ◆

Bei allen Fragen rund um die Rahmenverträge für cloudbasierte Videokonferenzen erreichen Sie uns unter:
conf@dfn.de

Auf Socken zur Mondbasis – IT-Sicherheit spielerisch gedacht

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

Illustration: Nina Bark/DFN-Verein

Cybersicherheit ist in einer digitalisierten Welt mehr als nur ein Schlagwort – sie ist eine ständige Herausforderung. Um dem Thema mehr Sichtbarkeit zu verleihen und konkrete Verbesserungen anzustoßen, wurde im November 2024 die DFN-Security Challenge ins Leben gerufen. Über einen Zeitraum von vier Monaten standen spielerischer Wettbewerb und gemeinschaftliches Lernen im Mittelpunkt. Ziel war es, das Bewusstsein für IT-Sicherheit zu stärken – und gleichzeitig praktische Maßnahmen im Rahmen des Dienstes DFN-Security gezielt in den Arbeitsalltag der teilnehmenden Einrichtungen zu integrieren.

Cybersicherheit als Party-Crasher

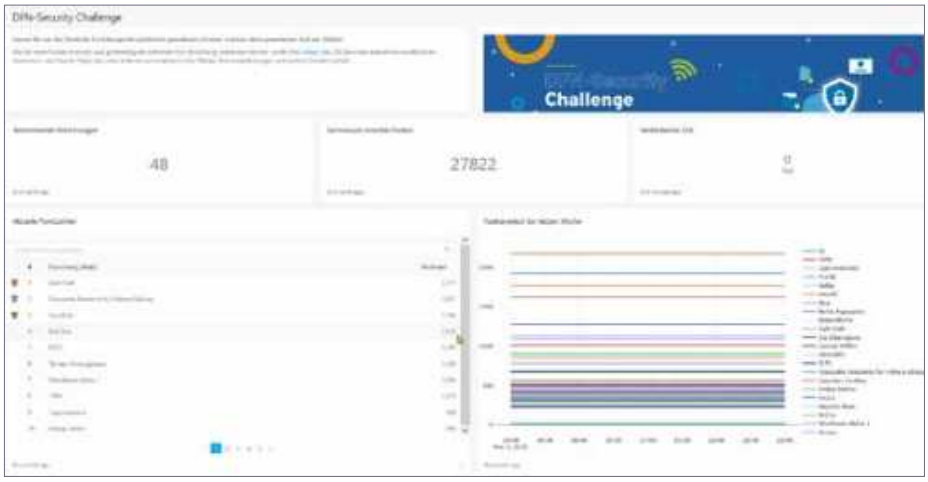
Vernetzung und Digitalisierung ohne Anstrengungen in der IT-Sicherheit ist für Cyberkriminelle vermutlich mit einer Einladung zu einer Party vergleichbar. Angriffe auf unter anderem Krankenhäuser, karitative Einrichtungen und Schulen machen zudem deutlich, dass es für Cyberkriminalität keine Tabus gibt. Alles, was angreifbar und lukrativ erscheint, kann zum Opfer werden. Jeder, der sich in der digitalen Welt bewegt, muss sich daher Gedanken über eine sinnvolle Absicherung dieser Welt machen.

Diese Erkenntnis ist nicht neu – und wird in der Regel auch nicht bestritten. Dennoch ziehen Projekte zur Sicherheitsverbesserung bei der Priorisierung oft den Kürzeren. Neben fehlenden Ressourcen und Expertise spielt hier sicherlich auch eine Rolle, dass Sicherheitsmaßnahmen nicht direkt sichtbare Neuerungen oder Vorteile bringen. Sie werden häufig als aufwendig, störend oder belastend empfunden – und das manchmal zu Recht. Schlechte Startbedingungen also für ein Sicherheitsprojekt – genau hier setzte die DFN-Security Challenge an.

Gamification trifft Sicherheit

Die DFN-Security Challenge versuchte, über das Hinzufügen eines spielerischen Elements die Nutzung der verschiedenen Merkmale des Dienstes DFN-Security attraktiver zu machen. Der Wettbewerb zwischen verschiedenen Einrichtungen sollte dabei nicht nur den Ehrgeiz wecken, sondern auch verdeutlichen, dass letztlich alle „im gleichen Boot“ sitzen. Aktivitäten, die nicht nur lokal Wirkung zeigen, sondern die Community stärken, wurden dabei besonders positiv bewertet.

Ein Blick auf das Challenge-Dashboard mit den teils herrlich kreativen Aliasnamen verriet schnell: Ernsthaftes Engagement schließt Humor nicht aus. Ob das Zentrum für Existenzielles Sockensortieren Ordnung ins digitale Durcheinander brachte, die Guardian Gorillas in Sachen Cybersicherheit auf Bananenjagd gingen oder Mondbasis Alpha 1 mit Weitblick operierte – der Wettbewerb war lebendig und bunt.



Screenshot der DFN-Security Challenge-Webseite

Siegerehrung im Plenum der DFN-Betriebstagung (von links Ralf Gröper vom DFN, Tanja Rolinger und Ralf Becker von der Hochschule Trier sowie Jochem Pattloch vom DFN) | *Foto: Jürgen ALOIsius Morgenroth*

Punkte für Sicherheit – so lief die Challenge ab

Zur Challenge angemeldete Teilnehmer konnten vier Monate lang Punkte für die eigene Einrichtung durch die Nutzung und Verbesserung des Dienstes DFN-Security sammeln. Die Latte für den Einstieg lag bewusst niedrig: Punkte gab es bereits für die Anmeldung, das Unterzeichnen der Dienstvereinbarung oder die Benennung handlungsberechtigter Personen.

Wer sich anschließend über das Security-Portal an die im Selfservice verfügbaren Dienste wagte – etwa Schwachstellenmeldungen, Überwachungsziele oder den Netzwerkprüfer –, konnte weitere Punkte sammeln. Richtig viele Punkte gab es dann für die Nutzung von DNS-RPZ und der Logdatenanalyse, da diese etwas mehr Aufwand erfordern. Und wer darüber hinaus eigene Daten in die DNS-RPZ-Community-Zone einlieferte, neue Use Cases entwickelte oder eine Integrationsmaßnahme zur Anbindung an die Logdatenanalyse erfolgreich umsetzte und der Community zur Verfügung stellte, konnte sich über besonders hohe Punktzahlen freuen.

Technische Beiträge aus der Community

Eine besondere Leistung war die Entwicklung einer Anbindung an die Logdatenanalyse für Wazuh, eine Open-Source-Sicherheitsplattform. Zudem wurden mehrere

Vorschläge für neue Use Cases eingereicht – teils Erweiterungen bestehender Anwendungsfälle, teils ganz neue Ideen. Dreimal konnte dafür die volle Punktzahl vergeben werden. Auch die DNS-RPZ-Community-Zone wächst: Mittlerweile liefern sieben Einrichtungen aktiv Daten ein.

Und der Gewinner ist …

Die Siegerehrung der DFN-Security Challenge fand im Rahmen der 82. DFN-Betriebstagung statt und gehörte zu den Highlights des ersten Tages. Insgesamt haben 48 Einrichtungen teilgenommen und dabei beeindruckende 27 822 Punkte erzielt – ein deutliches Zeichen für das große Engagement.

Mit 2 175 Punkten sicherte sich die Hochschule Trier den ersten Platz. Der verdiente Lohn: Die ersten fünf Plätze gewannen ein Security-Awareness-Paket, das nicht nur die Anerkennung für die erbrachte Leistung darstellt, sondern auch weitere Motivation für künftige Sicherheitsmaßnahmen liefert.

Fazit: Gemeinschaft stärken, Sicherheit leben

Uns (DFN & DFN-CERT) hat die Challenge richtig Spaß gemacht – besonders das Engagement der Teilnehmer war beeindruckend. Natürlich hoffen wir, dass dieses Engagement auch über das Ende der Challenge hinaus anhält, die IT-Security-Community im DFN gestärkt daraus hervorgeht und eventuell sogar lokale Nachahmer findet. Vielleicht inspiriert die Challenge auch zu weiteren Maßnahmen, die wir gemeinsam angehen können, um das Thema IT-Sicherheit im DFN noch weiter voranzubringen. ◆

MOTIVATION UND WIRKUNG – EIN BLICK HINTER DIE KULISSEN DES GEWINNERTEAMS

Hinter der beeindruckenden Punktzahl des Wettbewerbs stehen reale Erfahrungen und konkrete Veränderungen im Arbeitsalltag. Besonders anschaulich zeigt sich dies beim Gewinnerteam der Hochschule Trier, das mit 2 175 Punkten den ersten Platz belegte. In einem kurzen Erfahrungsbericht gab das Team Einblick in seine Motivation, die Umsetzung und die Auswirkungen der Teilnahme an der DFN-Security Challenge.

Was war Ihre persönliche Motivation, an der DFN-Security Challenge teilzunehmen? Und wie viele Kolleginnen und Kollegen waren bei Ihnen involviert?
„Wir verwenden das DFN-Security Portal schon seit Längerem, mit dem Fokus auf Schwachstellen- und Warnmeldungen. Die Challenge hat uns dazu gebracht, auch Funktionen in die tägliche Arbeit zu integrieren, die wir bis zu diesem Zeitpunkt nicht genutzt haben. Maßgeblich zwei Kollegen haben die Umsetzung der von der Challenge abgedeckten Dienste vorangetrieben und die jeweils zuständigen Personen aktiviert. Der Wettbewerbscharakter hat uns veranlasst, uns konzentriert mit dem Portal DNS-RPZ und dem SOC-Connector auseinanderzusetzen und diesbezügliche Änderungen intern zu kommunizieren. So sind auch Kolleginnen und Kollegen mit DFN-Security in Kontakt gekommen, die dieses zuvor nicht auf dem Schirm hatten. Schnell wurden aus anfänglich zwei Personen dann auch neun."

Gab es während des Wettbewerbs einen Punkt, an dem Sie dachten: Jetzt könnten wir tatsächlich gewinnen?
„Dass wir uns schon früh in der Platzierung ganz oben sahen, hat uns natürlich veranlasst, dort bleiben zu wollen und möglicherweise sogar zu gewinnen. In die Karten spielte uns sicherlich, dass wir im Hinblick auf DNS-RPZ und SOC-Connector Ideen einbringen wollten und konnten, von denen die Community profitiert."

Was nehmen Sie aus der Challenge mit? Gibt es etwas, das Sie künftig anders machen oder weiterführen möchten?
„Die Nutzung des DFN-Portals ist über die Challenge zur Routine geworden. DFN DNS-RPZ hat unser existierendes DNS-RPZ abgelöst, und wir arbeiten nun aktiv bei der DFN DNS-RPZ-Community-Zone mit. Dass die Log-Daten, die wir per SOC-Connector weitergeben, allen helfen, Angriffe und Schwachstellen zu erkennen, ist ein gutes Gefühl. Letztendlich haben wir die Hoffnung, dass wir von Empfängern einer Dienstleistung zu einem Teil der Community geworden sind, der Inhalte und Kompetenzen beiträgt."

To sign, or not to sign – that is the question!

Im Rahmen der Vertrauensdienste des DFN-Vereins begegnet uns häufiger die Frage, ob man mit Zertifikaten aus der DFN-PKI neben E-Mails auch Dokumente – in der Regel PDF-Dateien – signieren kann. Die Antwort auf diese vermeintlich einfache Frage ist erstaunlich komplex.

Text: **Ralf Gröper** (DFN-Verein)

Foto: agrobacter / Adobe Stock, pixel-shot/Freepik

Was steckt eigentlich hinter der Idee einer digitalen Signatur – und was genau leistet sie? Digitale Signaturen erfüllen zentrale Sicherheitsanforderungen: Sie gewährleisten die Authentizität und Integrität einer Nachricht. Das bedeutet, dass die Nachricht tatsächlich vom angegebenen Absender stammt und auf dem Übertragungsweg nicht verändert wurde. Genau das ist der Zweck beim Signieren von E-Mails mit S/MIME. Darüber hinaus verleiht eine Signatur einem Dokument unter bestimmten Umständen rechtliches Gewicht – vergleichbar mit einer Unterschrift auf einem Vertrag. Besonders bei PDF-Dokumenten geht es oft genau darum: eine verbindliche Aussage mit digitalem Nachdruck zu schaffen.

Von einfach bis qualifiziert – das regelt die eIDAS

Die „Rechtssaussage" von elektronischen Signaturen ist, wenig verwunderlich, in einem

Gesetz geregelt. In diesem Fall ist das die eIDAS-Verordnung der Europäischen Union. Diese definiert drei Signaturarten:

1. *die einfache elektronische Signatur*
2. *die fortgeschrittene elektronische Signatur*
3. *die qualifizierte elektronische Signatur*

Punkt 1, die *einfache elektronische Signatur* wird an dieser Stelle nicht thematisiert, da sie in den meisten Fällen nicht genügend rechtliche Sicherheit bietet. Der Hauptunterschied zwischen Punkt 2, einer *fortgeschrittenen,* und Punkt 3, einer *qualifizierten elektronischen Signatur,* liegt im Sicherheitsniveau und der rechtlichen Anerkennung. Letztere bietet die höchste Sicherheitsstufe. Sie ist der handschriftlichen Unterschrift rechtlich gleichgestellt, genügt dem Schriftformerfordernis und wird EU-weit von Gerichten anerkannt. Die *fortgeschrittene elektronische Signatur* hingegen ist für viele geschäftliche Anwendungen völlig ausreichend: Etwa, wenn es keine gesetzliche Formvorgabe gibt oder das Haftungsrisiko gering ist. Sie ist eine gute Wahl für viele geschäftliche Anwendungen.

> Die fortgeschrittene elektronische Signatur ist für viele geschäftliche Anwendungen völlig ausreichend.

Die *qualifizierte elektronische Signatur* erfüllt alle Anforderungen einer *fortgeschrittenen elektronischen Signatur* – geht aber in einigen Punkten darüber hinaus: Sie wird mit einem besonders gesicherten Gerät erstellt, das vor Manipulation schützt (einer sogenannten „qualifizierten elektronischen Signaturerstellungseinheit"). Außerdem basiert sie auf einem qualifizierten Zertifikat.

Fortgeschritten oder qualifiziert? Das kann die DFN-PKI

Die aktuell in der DFN-PKI angebotenen Zertifikate, egal auf welchem Vertrauensniveau, erfüllen auf keinen Fall die Anforderungen an die *qualifizierte Signatur*. Hierfür gibt es spezielle „qualifizierte Zertifikate" – die Anforderungen an diesen Zertifikattyp sind besonders definiert und reguliert. Somit ist eine Signatur erst dann im rechtlichen Sinne qualifiziert, wenn sie auch mit einem qualifizierten Zertifikat erstellt wurde. Dieser Zertifikattyp und damit auch entsprechende Signaturen sind derzeit in der DFN-PKI nicht enthalten – das kann sich jedoch bei entsprechenden Bedarfen seitens der teilnehmenden Einrichtungen des DFN-Vereins künftig ändern.

Noch einmal zurück zu den *fortgeschrittenen elektronischen Signaturen*, hier lohnt ein genauerer Blick: Obwohl es qualifizierte Signaturen und analog dazu auch spezielle qualifizierte Zertifikate gibt, trifft das auf die *fortgeschrittenen Signaturen* nicht zu. Hier gibt es keine Entsprechung aufseiten des Signaturzertifikats. Der Begriff des *fortgeschrittenen Zertifikats* ist in der eIDAS (und auch in den entsprechenden Standards des European Telecommunications Standards Institute, ETSI) gar nicht erst definiert. Das mag etwas haarspalterisch klingen, ist aber tatsächlich ein fundamentaler Unterschied zum qualifizierten Bereich.

Da in der DFN-PKI Zertifikate ausgestellt werden – und eben keine Signaturen –, stellt sich die Frage, unter welchen Voraussetzungen diese verwendet werden können, um rechtssichere *fortgeschrittene elektronische Signaturen* zu erzeugen.

Die Anforderungen an eine *fortgeschrittene Signatur* sind in der eIDAS-Verordnung in Artikel 26 definiert.

Eine fortgeschrittene elektronische Signatur erfüllt folgende Anforderungen:

a. *Sie ist eindeutig dem Unterzeichner zugeordnet.*
b. *Sie ermöglicht die Identifizierung des Unterzeichners.*
c. *Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.*
d. *Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.*

Es gibt in der DFN-PKI Zertifikattypen, die diese Anforderungen nicht erfüllen. Beispielsweise bei den Zertifikaten vom Typ „E-Mail-Only" ist bereits Punkt a nicht erfüllt, da Vorname und Nachname des Unterzeichners nicht Bestandteil des Zertifikats sind. Die enthaltene E-Mail-Adresse kann problemlos eine Funktionsadresse mit potenziell mehreren Absendern sein.

Andere Zertifikattypen aus der DFN-PKI können hingegen *fortgeschrittene Signaturen* erzeugen, sofern sie eindeutig einer Person zugeordnet sind. Damit wäre Punkt a erfüllt. So sind grundsätzlich alle Zertifikattypen, die den Vor- und Nachnamen des Unterzeichners enthalten, geeignet. Das trifft beispielsweise auf die Userzertifikate aus der *DFN-Verein Community PKI* zu, aber auch auf die E-Mail-Zertifikate von HARICA im Profil IV+OV. Ob die weiteren Anforderungen erfüllt sind, hängt vom konkreten Einzelfall und den notwendigen Vorarbeiten bei den teilnehmenden Einrichtungen ab. Nicht alle Signaturen, die mit diesen Zertifikattypen erstellt wurden, sind automatisch fortgeschritten.

Alle Anforderungen erfüllen – ist das möglich?

Für die *fortgeschrittene* Signierung gilt, alle vier obigen Anforderungen aus Artikel 26 der eIDAS-Verordnung einzuhalten. Im Streitfall sind Einrichtungen in der Verantwortung, dies anhand eigener Unterlagen nachzuweisen. Darüber hinaus ist es ausschlaggebend, ob das Zertifikat mit der gewählten Software kompatibel ist. Das erfordert unter Umständen einiges an Vorarbeiten, wie etwa das Einspielen der vertrauenswürdigen Root-CA (Certificate Authority) des Vertrauensdiensteanbieters in den Zertifikat-Stores der verwendeten Software.

Um die Einhaltung von Anforderung b belegen zu können, sind Nachweise notwendig, die bei der Identitätsprüfung bei Ausstellung des Zertifikats anfallen. Die anfallenden Artefakte müssen idealerweise an zentraler Stelle vorgehalten werden, um den Nachweis auf Nachfrage erbringen zu können. Notwendig hierfür ist ein ausreichendes Vertrauensniveau der Archivierung, beispielsweise durch ein Vieraugenprinzip und eine Archivierung, die vor nachträglichen Veränderungen schützt. Wichtig ist: Aktuell liegen diese Artefakte im Kontext der DFN-PKI nicht beim Vertrauensdiensteanbieter (DFN-Verein oder HARICA) vor.

Die Anforderungen c und d entziehen sich vollständig dem Einflussbereich des Vertrauensdiensteanbieters. Dieser kann in seinen Bedingungen zur Zertifikatnutzung zwar gewisse Maßnahmen einfordern, ob der private Schlüssel aber geheim gehalten und adäquat geschützt wird (Anforderung c), kann er keinesfalls überprüfen oder gar sicherstellen. Hier bieten sich lokal geeignete Maßnahmen wie die Verwendung von Krypto-Token zum Schutz des privaten Signaturschlüssels an. Anforderung d wiederum hängt davon ab, ob das gewählte Datenformat (z. B. PDF) korrekt erstellt wurde – damit beispielsweise von der verwendeten Software. Auch hierauf hat der Vertrauensdiensteanbieter keinen Einfluss.

Zusammenfassend lässt sich festhalten, dass alle Beteiligten an einem Geschäftsprozess selbst prüfen müssen, ob die vier Anforderungen erfüllt werden. Wenn das sichergestellt und nachgewiesen werden kann, ist eine *Signatur fortgeschritten*.

So gehts auch

Im Übrigen können *fortgeschrittene Signaturen* gemäß den Anforderungen der eIDAS (theoretisch) ganz ohne Vertrauensdiensteanbieter erzeugt werden. Das ist mit Schlüsselmaterial möglich, das gar nicht erst von einem Vertrauensdiensteanbieter geprüft oder zertifiziert wurde. Im Zweifel ist es dann aber noch aufwendiger, die vier obigen Bedingungen nachzuweisen.

> Durch die Bereitstellung von Policies ist das Vertrauensniveau der PKI für alle Parteien dokumentiert.

Zertifikate von einem Vertrauensdiensteanbieter haben den Vorteil, dass die Root-CA technisch geschützt betrieben wird. Durch die Bereitstellung von Policies ist das Vertrauensniveau der PKI für alle Parteien transparent dokumentiert. Sie stellen somit einen wichtigen Baustein dar, um die Bedingungen zu erfüllen, sind für sich genommen aber nicht hinreichend. Darüber hinaus gibt es bei einigen kommerziellen Vertrauensdiensteanbietern spezielle Produkte für *fortgeschrittene Signaturen*. Das sind in der Regel sogenannte Fernsignaturen, bei denen das Dokument im Namen des Kunden vom Anbieter signiert wird – nach einer erfolgten Identifizierung beispielsweise über die eID-Funktion des Personalausweises. In diesem Fall hat der Vertrauensdiensteanbieter die Kontrolle über alle vier Anforderungen der eIDAS und kann so garantieren, dass die Signatur im Sinne der EU-Verordnung *fortgeschritten* ist. Hierbei hat der Unterzeichnende aber keinen Zugriff auf den privaten Signaturschlüssel. Dieser wird vom Vertrauensdiensteanbieter erzeugt und verwaltet.

Dem EU-Gesetzgeber ist im Übrigen auch aufgefallen, dass die vier Anforderungen (zu) wenige Vorgaben machen, um den europäischen Bürgerinnen und Bürgern den breiten Einsatz von gerichtsfesten *fortgeschrittenen Signaturen* zu ermöglichen. Daher enthält die Novellierung des eIDAS-Verordnung von 2024 in Artikel 26 neben den bekannten Anforderungen zusätzlich den Auftrag an die Europäische Kommission, bis Mai 2026 zu prüfen, ob Referenzstandards mit Spezifikationen und Verfahren für *fortgeschrittene elektronische Signaturen* festgelegt werden müssen.

Das Resümee: Mit ein wenig Vorarbeit und einigen lokal umgesetzten Prozessen lassen sich mit Zertifikaten aus der DFN-PKI auch *fortgeschrittene Signaturen* erzeugen. Die umzusetzenden Prozesse umfassen die Archivierung von Nachweisen zur Identifizierung (Anforderung b), den Schutz des privaten Schlüssels (Anforderung c) sowie die sorgfältige Auswahl der Software, die zur Signaturerstellung eingesetzt wird (Anforderung d). Anforderung a ist die leichteste Übung: Es wird einfach ein Zertifikattyp gewählt, der Vor- und Nachname enthält. ◆

eIDAS steht für „electronic IDentification, Authentication and Trust Services". Es ist eine EU-Verordnung, die einen einheitlichen Rechtsrahmen für elektronische Identitäten, elektronische Signaturen und Vertrauensdienste innerhalb der Europäischen Union schafft. Ziel ist es, sichere und grenzüberschreitende digitale Kommunikation zwischen Bürgerinnen und Bürgern, Unternehmen und Behörden zu ermöglichen. Kurz gesagt: eIDAS regelt, wie man digital vertrauenswürdig unterschreibt, sich identifiziert oder Daten versiegelt – und dies mit EU-weiter Gültigkeit.

Ein Dienst wird flügge: DFN edu-ID startet in die Pilotphase

Wichtiger Meilenstein im edu-ID-Projekt des DFN-Vereins: Nachdem das von einer ZKI-Arbeitsgruppe entwickelte Konzept einer edu-ID für die deutsche Forschungs- und Bildungslandschaft im Rahmen eines Proof-of-Concept auf Herz und Nieren überprüft wurde, startet das System nun in einer gründlich überarbeiteten Version in den Pilotbetrieb – den zukünftigen produktiven Einsatz fest im Blick.

Text: **Wolfgang Pempe** (DFN-Verein)

Foto: GlobalP/iStock

Das DFN-edu-ID-Projekt verfolgt das Ziel, eine selbstverwaltete, einrichtungsunabhängige und lebenslang gültige digitale Identität für den Bereich Forschung und Bildung in Deutschland bereitzustellen. Die edu-ID soll es Nutzerinnen und Nutzern ermöglichen, unabhängig von ihrer aktuellen Zugehörigkeit zu einer bestimmten Hochschule oder Forschungseinrichtung auf digitale Dienste und Ressourcen zuzugreifen, deren Zugriffsberechtigungen nicht an die Zugehörigkeit zu einer bestimmten Einrichtung gebunden sind. Das Design des edu-ID-Systems ist auf eine nahtlose Integration in die DFN-AAI ausgerichtet. Der technische Betrieb erfolgt durch das DFN-CERT.

Im Rahmen einer Proof-of-Concept-Implementierung wurde eine erste Version des edu-ID-Systems über die letzten anderthalb Jahre anhand ausgewählter Use Cases – insbesondere aus dem Bibliotheksbereich – gründlich erprobt und ein erster Penetrationstest durchgeführt. Dabei wurden die im technischen Konzept beschriebenen User Journeys durchgespielt, parallel erfolgten Umfragen zur User Experience. Darüber hinaus wurde das edu-ID-System prototypisch als Schnittstelle der DFN-AAI zur Schulföderation VIDIS und zu der im Aufbau befindlichen Vernetzungsinfrastruktur Digitale Bildung „Mein Bildungsraum“ konfiguriert. Die im Rahmen dieser Validierungstätigkeiten gesammelten Erfahrungen

und Ergebnisse stellen die Basis für die weitere technische Projektentwicklung dar.

Für den Pilotbetrieb steht nun eine neue, entsprechend überarbeitete Version des edu-ID-Systems zur Verfügung, deren Single-Sign-on- und Datenbankkomponenten bereits standortredundant betrieben werden. Gemeinsam mit ausgewählten Einrichtungen und Dienstanbietern aus der DFN-AAI-Community werden weitere Use Cases erprobt.

Eine besonders wichtige Rolle spielt hierbei die Integration des edu-ID-Systems in die NFDI-AAI, die Authentifizierungs- und Autorisierungsinfrastruktur, die im Rahmen des NFDI-Basisdienstprojekts IAM4NFDI aktuell aufgebaut wird. Das edu-ID-System erfüllt in diesem Kontext drei wichtige Rollen: Zunächst bietet es Nutzenden die besagte lebenslang gültige, einrichtungsunabhängige digitale Identität, adressiert somit das Problem der Researcher Mobility und ermöglicht auf diese Weise die nahtlose Nutzung der über die NFDI-AAI verfügbaren Ressourcen. Zugleich dient es als zentraler Homeless-/Gast-IdP. Darüber hinaus bietet das edu-ID-System die Möglichkeit, die eigene digitale edu-ID-Identität mit weiteren Accounts zu verknüpfen, die damit verbundenen Daten wie die ORCID iD zu aggregieren und diese bei Bedarf an NFDI- oder sonstige Dienste zu übertragen.

Auch in der Pilotphase wird es wieder darum gehen, das bestehende Konzept und die Architektur des Systems zu validieren und bei Bedarf entsprechende Anpassungen vorzunehmen. Eine wichtige Rolle wird dabei die Frage der Skalierbarkeit spielen, sowohl auf technischer als auch auf betrieblich-organisatorischer Ebene – insbesondere, wenn es darum geht, den Support für die Endnutzenden zu organisieren. Bis dahin müssen ein tragfähiges Betriebskonzept erarbeitet sowie alle datenschutzrechtlichen und vertraglichen Fragen geklärt werden. Erst dann kann sinnvollerweise die Aufnahme des Regelbetriebs in Angriff genommen werden. Weiterhin ist für das kommende Jahr ein Security-Audit geplant.

Die Pilotphase des DFN-edu-ID-Projekts markiert einen wichtigen Schritt hin zu einer einheitlichen, lebenslangen digitalen Identität für den Bildungs- und Forschungsbereich in Deutschland. Sie dient der technischen und organisatorischen Erprobung, der datenschutzrechtlichen Absicherung und der Vorbereitung auf eine breite Einführung in den kommenden Jahren. ◆

Weitere Informationen zur DFN edu-ID sowie zum NFDI-Basisdienst IAM bieten die Beiträge „Eine für alle – die edu-ID“, „Sicher FAIR – der NFDI-Basisdienst IAM“ aus Ausgabe 103 auf den Seiten 40 und 44 sowie „Er wächst und gedeiht – der NFDI-Basisdienst IAM4NFDI“ aus Ausgabe 106, Seite 11, der DFN-Mitteilungen.
https://www.dfn.de/news/publikationen/

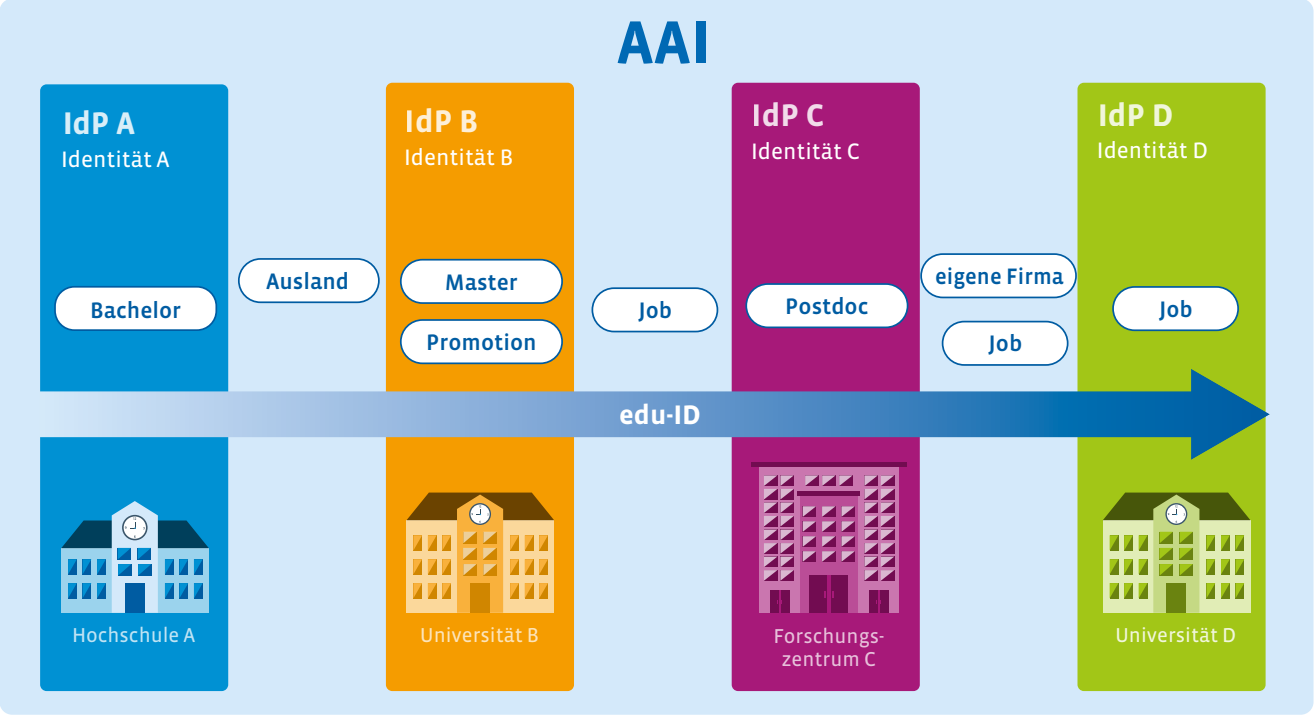


Abbildung 1: Schema einer lebenslangen digitalen Identität

Sicherheit aktuell

GÉANT TCS: Wechsel des Anbieters

Ende vergangenen Jahres fand ein Anbieterwechsel für die Bereitstellung von browserverankerten Zertifikaten statt. Der bisherige Anbieter hatte den Vertrag mit GÉANT über TCS (Trusted Certificate Service) kurzfristig gekündigt und die Leistungserbringung am 10. Januar 2025 eingestellt. Um die Kontinuität des Dienstes sicherzustellen, beauftragte der DFN-Verein den Vertrauensdiensteanbieter HARICA mit der Dienstleistung. Dieser ist Teil des griechischen Universitätsnetzwerks GUnet und seit vielen Jahren in relevanten Standardisierungsgremien sehr gut vernetzt.

Innerhalb weniger Wochen konnte allen teilnehmenden Einrichtungen ein Zugang zu den Diensten des neuen Anbieters HARICA zur Verfügung gestellt werden. Inzwischen hat auch GÉANT eine Vereinbarung mit HARICA geschlossen, sodass der Anbieter im Rahmen von TCS langfristig zur Verfügung stehen wird.

Im Rahmen der DFN-PKI wird der Dienst GÉANT TCS seit 2021 angeboten. Damit können teilnehmende Einrichtungen am Wissenschaftsnetz digitale Zertifikate für Serverdienste und User beziehen, die in Webbrowsern und Betriebssystemen ohne weitere Konfiguration akzeptiert werden. ◆

PKI: Weitere Verringerung der Laufzeit von Serverzertifikaten steht bevor

Die erlaubte Laufzeit von browserverankerten Serverzertifikaten wird seit vielen Jahren immer kürzer. Sowohl die Regelungen des CA/Browserforums als auch spezielle Anforderungen von einzelnen Webbrowsern wie Google Chrome oder Apple werden regelmäßig verschärft. Das Ziel: Nach Ansicht der Webbrowser können sehr kurze Laufzeiten die Gefahren reduzieren, die durch Domain-Besitzerwechsel oder kompromittierte Schlüssel entstehen.

In den vergangenen Monaten konkretisierte sich nun eine weitere Verkürzung. Nachdem Google bereits im Frühjahr 2023 einen Vorschlag unterbreitet hatte, brachte Apple Mitte 2024 eigene Vorstellungen über Zeitpläne und mögliche erlaubte Laufzeiten in das CA/Browserforum ein. Nach mehrmonatigen Diskussionen wurde im April 2025 die folgende Fassung verabschiedet:

Laufzeit von Serverzertifikaten

Ab März 2026	200 Tage
Ab März 2027	100 Tage
Ab März 2029	47 Tage

Zusammen mit der erlaubten Gültigkeit der Zertifikate wird auch die mögliche Wiederverwendbarkeit von Domain-Validierungen beschränkt.

Wiederverwendbarkeit von Domain-Validierungen

Ab März 2026	200 Tage
Ab März 2027	100 Tage
Ab März 2029	10 Tage

Zu beachten ist hierbei insbesondere der Endzustand ab 2029: nur noch zehn Tage mögliche Wiederverwendung!

Domain-Validierungen werden zurzeit noch häufig mit Mail-Challenges beantwortet, die manuell ausgelöst und manuell beantwortet werden. Es ist in keiner Weise sinnvoll, diesen Prozess alle zehn Tage manuell durchzuführen. Damit muss auch die Domain-Validierung automatisiert werden. Hierfür stehen DNS- oder HTTP-gestützte Mechanismen zur Verfügung.

Folgende Handlungsempfehlungen können gegeben werden:

1. Automatisierung der Ausstellung und Erneuerung von Serverzertifikaten, wo immer es möglich ist. Dafür können beispielsweise das ACME-Protokoll oder herstellerspezifische APIs genutzt werden.

2. Prüfen von Anwendungsfällen der Serverzertifikate: Schwer oder nicht automatisierbare geeignete Szenarien können auf Spezial-PKIs mit länger gültigen Zertifikaten migriert werden. Hierfür bieten sich intern betriebene PKIs oder die DFN-Verein Community-PKI an. ◆

Nadel oder Heu

Welcher Systemverantwortliche wünscht sich das nicht: User, die Passworte für genau ein System verwenden, Phishing-Angriffe sicher als solche erkennen und freudig jede Empfehlung umsetzen, um die eigenen Accounts vor Fremdzugriffen zu schützen?

Auch wenn es sich oft nicht so anfühlt, aber in der Realität meistert ein Großteil der Nutzenden diese Aufgabe, aber eben nicht alle. Um Schaden von der eigenen Einrichtung abzuwenden, muss dieser kleine Anteil kompromittierter Accounts möglichst zügig und möglichst sicher erkannt und unschädlich gemacht werden.

Eine wichtige Erkennung erfolgt über E-Mail-Server und anhand der Auswertung der zugehörigen Log-Daten, da erbeutete Accounts oft für den Versand von Spam-, Phishing- und Viren-E-Mails eingesetzt werden.

Um den Missbrauch zu begrenzen, empfiehlt sich eine Beschränkung der versendbaren E-Mail-Menge in einem bestimmten Zeitfenster (Rate Limiting). Da die normale Nutzung durch das Rate Limit aber nicht behindert werden soll, greift diese Maßnahme verhältnismäßig spät. Eine nicht unerhebliche Anzahl E-Mails wurde bereits versendet. Um im nächsten Fall schon früher einzugreifen, sollten die mit einem erkannten Angriff in Verbindung stehenden Daten, wie z. B. die IP-Adresse, von der die E-Mails versendet wurden, genutzte Absenderadressen und Betreffzeilen, für zukünftige Analysen genutzt werden. Über die Erkennung von Ähnlichkeiten bezüglich dieser Daten lassen sich häufig weitere missbräuchlich genutzte Accounts erkennen und deaktivieren.

Mehr Informationen gibt es im EDUCV-Artikel „Nadeln im Heuhaufen finden“ unter:
https://www.educv.de/blog/post-2025-02-25-nadeln-im-heuhaufen/ ◆

BESSER IM VERBUND

Der EDUCV ist eine Arbeitsgruppe von operativen Informationssicherheitsteams, insbesondere Computer Emergency Response Teams (CERTs) und Computer Security Incident Response Teams (CSIRTs), deutscher Hochschulen sowie Lehr- und Forschungseinrichtungen. Er dient dem Informations- und Erfahrungsaustausch sowie der Weiterbildung der teilnehmenden Sicherheitsteams und ermöglicht durch die einrichtungsübergreifende Kooperation und Kollaboration einen effektiven Umgang mit Informationssicherheitsrisiken und -vorfällen im spezifischen Umfeld von Forschung, Lehre und Studium.

Weitere Informationen zum EDUCV finden Sie unter: **https://www.educv.de/**

Sind Sie selbst Teil eines operativen Teams und möchten sich vernetzen? Kontaktieren Sie uns gerne unter: **info@educv.de**.

KONTAKT

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

Mitarbeit an dieser Ausgabe Sicherheit aktuell:
Jürgen Brauckmann, Christine Kahl, Heike Ausserfeld

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.

The Power of Music: Ligeti Center Researchers Marry Music and Technology

A BMBF-funded collaboration in Hamburg fuses music, healthcare, and IT. Hosted at and led by one of DFN's participating institutions, the Hamburg University of Music and Drama, the ligeti center brings together science and art as part of its mandate to transfer academic research into societal benefits. Recent projects investigate topics from how music supports healing to how networked music performance enables collaboration in new digital and physical spaces.

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

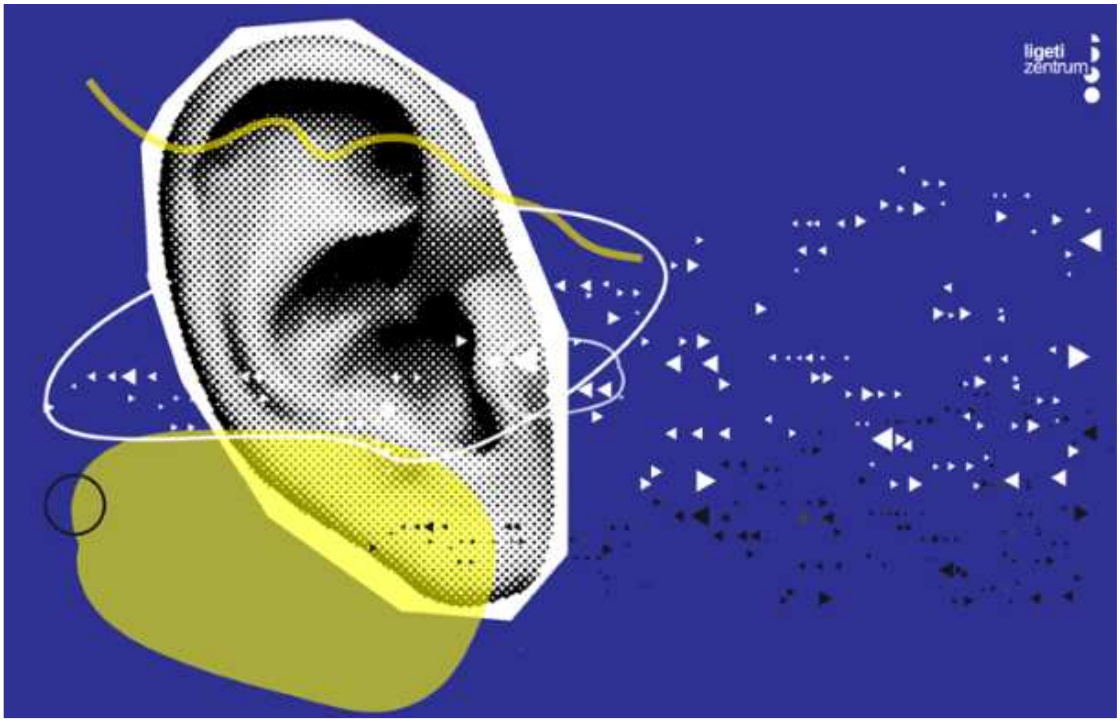


Illustration: Janina Luckow/ligeti center

Composer György Ligeti brought his passion for avant-garde music to the Hamburg University of Music and Drama (Hochschule für Musik und Theater Hamburg, or HfMT) in 1973. As one of the world's earliest computer music enthusiasts, Ligeti served as an HfMT professor until 1989, using teaching and composing as platforms to advocate for understanding and integrating ways to use computer technology for music composition and performance.

In 2023, HfMT joined forces with the Universitätsklinikum Hamburg-Eppendorf (UKE), the Technical University of Hamburg, and the Hamburg University of Applied Sciences to honor Ligeti, starting the *ligeti center* as part of the German Federal Ministry of Education and Research's (BMBF's) "Innovative Hochschule" funding program. The center's mission is to foster interdisciplinary research that brings together the arts, science, culture, and technology, and to provide "laboratories for innovation and general-audience edification through the translation of ideas," according to the center's website.

"When the BMBF established this initiative, it really enabled small universities to take their research and translate that knowledge to society and culture, and that is what the *ligeti center* is all about," said Prof. Georg Hajdu, HfMT professor and head of the *ligeti center*. "The original idea for this project was very much focused on research, and while we are still focused on research, we are also emphasizing how to translate that research into society more broadly."

Since its inception, the center has been busy doing just that. In recent years, the *ligeti center* evolved and extended the ambitious Healing Soundscapes project, which aims to develop methods for creating generative music and evaluating how to create "neutral" music that can positively impact the health and stress levels of patients, medical practitioners, and visitors in hospitals. Collaborators with the *ligeti center* have also developed new methods for networked music performances that allow musicians to play together in networked environments. As a participating institution in the German Research Network (DFN), HfMT offers the center the infrastructural backing to bring music into new spaces – digital and physical alike.

Healing Soundscapes project uses sounds to improve well-being

Before Healing Soundscapes became a formal project, it was a small initiative that started based on conversations between HfMT and UKE professors. The desire for sounds in the operating room was first introduced to the disciplines of multimedia composition and music therapy by a surgeon's clinical practice – an idea that soon grew to include hospital waiting areas. The goal was to create musical soundscape interventions (MSI), or site-specific, generative sound installations that improve the atmosphere of a room and, in turn, the well-being of the people present in the room.

"As a music therapist, part of my professional background is being trained in seeking out empathy with people I interact with," said

Test listening to a composition in the UKE's waiting area, together with patients and staff | *Photo: UKE, Anja Meyer*

Dr. Pia Preißler, research fellow at UKE, lecturer at HfMT, and coordinator of the Healing Soundscapes project. “We are trying to understand how people emotionally perceive the atmosphere and sounds that we are creating.”

To formalize the project, the interdisciplinary researchers had to develop a common vocabulary for describing musical and emotional qualities and how to evaluate them. “We needed time to start to learn from one another and learn to understand one another,” Preißler said. “If you want to describe sounds of a performance, music therapists might start with metaphors that connect to imagination and feelings. Composers might want to start by describing the sounds, scales, or other musical qualities.”

Additionally, they needed to have the infrastructure and technology to produce unique musical performances that meaningfully improved the experiences of patients and staff alike. For this, Hajdu returned to software developed years earlier by a former colleague and mentor, Clarence Barlow. He was enamored with Barlow’s AUTOBUSK software that was written for use on old Atari computers. Hajdu ported Barlow’s software to run in the Max programming language, or the “Lingua Franca of computer music,” as he described it. Integrated into contemporary digital music production platforms – and renamed DJster – the software became the basis for the first Healing Soundscapes experiments. DJster allows composers to use a wide range of sound parameters, scales, and meters in concert with a probability-based event generator to produce music capable of expanding the common rules one might hear in a symphony hall or concert venue.

Photo on top and centre
Performance in the Old Elbe Tunnel, a 426-meter tunnel that connects predestrian and non-vehicle traffic between the center of Hamburg with its docks south of the Elbe river | *Photos: Janina Luckow*

Photo below
The project’s steering committee (from left to right): Prof. Jan Sontag, Prof. Georg Hajdu, Prof. Sebastian Debus, Dr. Pia Preißler, Prof. Eckhard Weymann, Goran Lazarevic | *Photo: UKE, Eva Hecht*

During an exploratory pilot phase that started in 2017, Preißler, Hajdu, and their collaborators began Healing Soundscapes in the UKE Heart Center waiting room. It began with eight student-composed pieces. "Initially, we let the students use whatever sonic materials they wanted to, play with whatever scales they wanted to, and let them create," Hajdu said. As the project collaborators received feedback through surveying staff, guests, and patients, it was able to codify what it meant to create "neutral" music that could promote emotional and physical well-being while remaining so unobtrusive people could actively choose to "tune out." They came up with a core list of features for Healing Soundscapes contributions: the pieces should demonstrate disjunction (wider spacings between notes in a scale), be aperiodic, contain sonic "richness" of individual sounds, progress at slow to medium tempos, and have low to moderate volume dynamics.

With this additional data in hand, Healing Soundscapes developed a finer rubric to use in creating peaceful, soothing music for hospitals, and the project has since branched out into more complex environments, such as the waiting area of the UKE's emergency department and the department of radiotherapy. As the collaborators continue to refine this approach through research in mixed methods designs, the Healing Soundscapes team hopes to deliver on one of the *ligeti center's* core missions in the coming years after the funding from "Innovative Hochschule" expires – forming a company and translating their innovations to society more broadly.

Strong connections: networked music performance enables new ways of collaborating across digital space

HfMT offers the *ligeti center* access to DFN's X-WiN network. As Germany's national research and education network (NREN), DFN offers participating institutions access to high-speed networks that can transfer large data sets, host virtual conferences, enable VR collaboration, and, it turns out, facilitate rehearsals for musicians playing together from a distance.

Hajdu has been involved in networked music performance – musical collaboration happening in real time over a digital network – for more than 25 years. Since his first experiments sending music data between continents in 1999, Hajdu has developed multiple software solutions for sharing scores and sounds in a networked environment. According to Hajdu, the growth of network speed and access to DFN's X-WiN network at HfMT has been a major catalyst for networked music performance innovation at the university. "Network technology has gone far beyond what our typical demands are for music performance and collaboration," he said.

In 2007, he developed the quintet.net multimedia performance environment to facilitate musicians playing together using networks rather than a conductor. He also built out MaxScore as a way of sharing notation with networked musicians. Hajdu still needed to refine software that could distribute accurate scores to musicians in real time. He worked with former HfMT researcher Rama Gottfried, now Professor of Contemporary Computer Music Practice at the Zurich University of the Arts in Switzerland, who developed Drawsocket to share scores accurately in networked environments. "Rama designed this conducting system based on an earlier idea of mine we had discussed, but he went far beyond what I had imagined" Hajdu said. "Drawsocket allows us to generate and disseminate scores in real time."

These tools allow Hajdu's students, colleagues, and collaborators to effectively play music through the internet, but it also allows musicians to perform in unorthodox places. Using these technologies and over a kilometer of fiber-optic cables, the researchers organized a performance in Hamburg's Old Elbe Tunnel – a 426-meter tunnel that connects pedestrian and non-vehicle traffic between the center of the city with its docks south of the Elbe River. Musicians lined up on both sides of the tunnel and read off iPads using the team's software innovations to play scores that would resonate – literally and figurately – with visitors.

Through strong interdisciplinary collaborations between Hamburg's academic institutions and a strong network connection through DFN's X-WiN network, *ligeti center* staff continue to find new ways to bring the power of music – be it for healing, collaboration, or entertainment – to society. ◆

For more information on the *Ligeti Center*, visit the website at:
www.ligeti-zentrum.de

IN THE FIELD

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

International Newsflashes

Expansive GN5-1 Project Goes Through Successful Review with European Commission

At the end of March, 2025, GÉANT's GN5-1 project went through its Period 2 review by the European Commission (EC), focusing on work done during 2024. The 24-month project was part of a long-running series of funded projects that is aimed at bolstering national research and education networks (NRENs) across the European Union in their collaboration and community-building on networking, security, digital identities, and services. The next phase of the project family, GN5-2, started at the beginning of 2025 with an €80 million budget spread across 30 months.

DFN staffer Jakob Tendel, who serves as one of two group leads for the project's 'Above the Net Services' work package during GN5-1 and now for GN5-2, presented to the EC Review. The project efforts were ranked as "excellent" during the review process. In all, the EC review team confirmed the successful work of the whole project and commended the partners' performance, technical achievements, and commitment to innovation and sustainability.

The DFN Association, together with its subcontractors Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities (LRZ), Karlsruhe Institute of Technology (KIT), and DFN-CERT Services GmbH (DFN-CERT), are successfully involved in all nine work packages.

For more information on the GN5-1 review, please visit: https://connect.geant.org/2025/04/15/geants-gn5-1-project-completes-another-successful-ec-review ◆

NRENs Participate in First Cross-Border Crisis Exercise

In March, 2026, European national research and education networks (NRENs) will launch TALON, a simulation-based crisis exercise for NRENs on the continent. The project, started by Europe's NREN collaboration, GÉANT, aims to allow NRENs to test their abilities to respond to a crisis and offer chances to practice collaboration between various NRENs during a cross-border crisis.

TALON will be a one-day, live simulation where each NREN will apply its own established crisis procedure. TALON is not just simulating a single cyber attack on a specific NREN's network, though; the exercise will also simulate an international crisis unfolding to challenge the NREN's abilities to coordinate their responses in real-time, including a media simulator to mimic the public and political responses in such an event.

Registration for the event concludes in the fall or once GÉANT has 10 NRENs signed up to participate in the exercise.

For more information on TALON, please visit: https://connect.geant.org/2025/04/11/introducing-talon-europes-first-cross-border-crisis-exercise-for-nrens ◆

SIG-MSP Meeting Brings Together Representatives to Shape the Future of NREN Service Portfolios

On March 24–25, 2025, The Special Interest Group on Management of Service Portfolios (SIG-MSP) met in Paris. The event, hosted by French NREN Renater, brought roughly 50 participants together to focus on the group's main mission: namely, sharing best practices at the border between business management and technical service management.

The meeting offered opportunities for the various European NRENs to give detailed presentations of their organizations' strategy developments. During the meeting's second day, national NREN's presented their strategies as part of a "lightning talks" session. DFN's Leonie Schäfer presented the German strategy.

For more information about the SIG-MSP meeting, please visit: https://connect.geant.org/2025/04/04/aligning-strategies-shaping-the-future-of-nren-service-portfolios-sig-msp-meets-in-paris ◆

AI Revolution Touches NRENs at Second SIG-AI Meeting in Prague

During the TNC24 conference, a group of representatives from various global national education and research networks (NRENs) started the Special Interest Group for AI (SIG-AI) to share best practices surrounding artificial intelligence and cyber security.

Recently, the group had its second meeting. Taking place in Prague, Czechia, the group focused on both using AI for security and developing a more robust security framework around AI. Officials from the Czech NREN, CESNET, hosted the event, and showcased examples of how to use machine learning methods to mitigate DDoS attacks and identify covert cryptomining operations, among other examples. Many of the other 54 participants also presented during the event, including GÉANT's Magdalena Rzaca, Mary Grammatikou from the Unimversity of Athens, and Maarten Meijer from the University of Twente. DFN's Leonie Schäfer serves as a member of SIG-AI's steering committee and represented DFN during the event.

Participants of the second SIG-AI meeting in Prague, where NREN experts discussed AI applications in cybersecurity and shared best practices | *Photo: CESNET*

For more information on the SIG-AI, please visit: https://community.geant.org/sig-ai/ ◆

SoBigData Academy and GÉANT's Network eAcademy Work Together to Improve Learning Initiatives

This spring, GÉANT announced a new initiative between the organization's Network eAcademy and the SoBigData Academy aimed to share and improve educational resources for work with Big Data and social mining. By combining the expertise and experiences at both organizations, the initiative aims to improve and optimize their shared stable of learning tools and share them with one another.

Through the collaboration, SoBigData is integrating nine learning units from the eAcademy into their program. Participants in SoBigData's program will now have further resources surrounding data modelling, data formats and protocols, and specific formats like XML, YAML, JSON. There is also increased emphasis on Big Data storage with Docker, Kubernetes, Elasticsearch, and GitHub. Inversely, GÉANT Network Automation eAcademy is using SoBigData's training units focused on databases, data analysis, the ethics of data science, data mining and machine learning, and complex network analysis, among several other topics.

For more information on the collaboration and training offerings, please visit: https://connect.geant.org/2025/04/08/geant-network-eacademy-and-sobigdata-academy-join-forces-to-strengthen-their-learning-initiatives ◆

Collaboration on this Newsflash:
Leonie Schäfer, Eric Gedenk, Jakob Tendel

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

Digitale Inklusion fördern – Live-Untertitel als open source

Zahlreiche Vorlesungen finden online statt, sind jedoch nicht für alle gleichermaßen zugänglich. Hörbeeinträchtigte und fremdsprachige Teilnehmende haben oft Schwierigkeiten, dem Unterricht zu folgen. In seiner Bachelorarbeit befasste sich Julian Kropp mit der Entwicklung einer Live-Untertitelfunktion auf Basis von Open-Source-KI. Damit möchte der Stipendiat des diesjährigen Future Talent Programme (FTP) Sprachbarrieren in der Lehre abbauen und den Zugang zu Wissen erleichtern.

Text: **Julian Kropp** (Hochschule Darmstadt)

März 2020: In Deutschland wurde das öffentliche Leben komplett heruntergefahren, Schulen und Universitäten mussten schließen, und plötzlich verlagerte sich alles ins Internet. Die IT von Bildungseinrichtungen stand vor einer gigantischen Aufgabe: Der gesamte Unterricht musste so schnell wie möglich digital stattfinden. Plattformen wie Zoom oder Microsoft Teams wurden hastig eingerichtet. Datenschutz, Stabilität, Inklusion? Davon blieb leider vieles auf der Strecke.

Julian Kropp setzt sich mit seiner Arbeit für mehr Inklusion in der Lehre ein | *Foto: Julian Kropp*

Die Hochschule Darmstadt setzte mit BigBlueButton (BBB) eine eigens gehostete Open-Source-Videokonferenzlösung für Studierende auf. Obwohl BBB in Sachen Datenschutz bereits damals sehr weit war, fehlte etwas Entscheidendes: eine automatische Möglichkeit, Live-Untertitel zu wählen, um zum Beispiel hörbeeinträchtigte Menschen oder Teilnehmende aus verschiedenen Sprachräumen besser einzubinden. Zwar gibt es in BBB schon lange die Möglichkeit, Untertitel einzufügen, aber dafür muss jedes Wort mühsam eingetippt werden – und das ist alles andere als alltagstauglich. Eine Automatisierung durch Künstliche Intelligenz (KI) war hier der nächste logische Schritt. Doch die sensiblen Audiodaten an Drittanbieter wie Google oder Microsoft zu schicken, kam nicht infrage – insbesondere nicht

für öffentliche Einrichtungen, die besonders auf Datenschutz achten müssen.

Der Durchbruch kam mit Whisper, einer frei verfügbaren Open-Source-KI, die Audiodateien in guter Qualität in Text umwandeln kann. Sie unterstützt 57 Sprachen und ist unter der MIT-Lizenz veröffentlicht. Das bedeutet, jeder kann sie einfach herunterladen und verwenden. Allerdings ist sie nur für fertige Audiodateien konzipiert, nicht für einen fortlaufenden Audiostream, wie er in einem Onlinemeeting benötigt wird. Trotzdem war klar: Dieses Werkzeug könnte endlich das fehlende Puzzleteil für eine gute open source Live-Untertitel-Funktion sein.

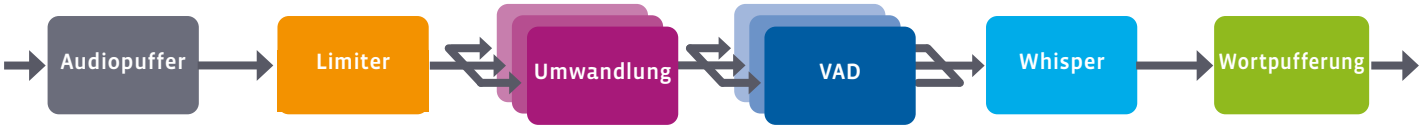
Die Idee nimmt Gestalt an

Zur Verbesserung der Inklusion bei Onlinemeetings wurde ein Projekt gestartet, um einen Bot für BigBlueButton zu entwickeln, der automatisch und in Echtzeit Untertitel generiert – und dabei vollständig auf eigenen Servern betrieben wird – ohne Änderungen am BBB-Code und ohne externe Datenübertragung. Das Ziel: Live-Untertitel, die so schnell wie möglich erscheinen und trotzdem eine hohe Qualität bieten. Dabei sollte alles open source bleiben und selbst gehostet werden. Wichtig war es auch, dass die Live-Transkription und der Bot voneinander getrennt bleiben. Dadurch kann das System zur Untertitelgenerierung auch in anderen Softwarelösungen außerhalb von BigBlueButton eingesetzt werden.

Innerhalb eines halben Jahres wurde eine erste funktionsfähige Version entwickelt. Der Bot trat einem BBB-Meeting bei, nahm den Audiostream auf, zerlegte diesen in 10-sekündige Abschnitte und übergab diese an Whisper. Schon dieser frühe Prototyp war in der Lage, Live-Untertitel in mehreren Sprachen einzublenden. Doch es kam auch schnell ans Licht, dass das System noch weit davon entfernt war, perfekt zu sein:

- **Verzögerungen und Instabilität:** Zwischen der gesprochenen Sprache und den angezeigten Untertiteln lagen etwa drei Sekunden. Außerdem verschwanden alle Wörter, die älter als zehn Sekunden waren.
- **Halluzinationen:** Die KI erfand hin und wieder Sätze, die niemand gesagt hatte. Manchmal tauchten sogar Phrasen wie „Thank you for watching“ auf, obwohl längst Stille herrschte.
- **Hohe Auslastung:** Selbst wenn niemand sprach, lief die Grafikkarte auf Hochtouren und war zu 100 Prozent ausgelastet.

Besonders die feine Balance zwischen Geschwindigkeit und Genauigkeit stellte sich als Herausforderung dar: Je schneller die Untertitel erschienen, desto eher konnte es zu Fehlern kommen, weil ein Wort womöglich noch nicht ganz ausgesprochen worden war. Zusätzlich litt die Qualität, wenn zu früh Text angezeigt wurde und später anhand des Kontextes korrigiert werden musste. Dennoch musste der Untertitel so schnell wie möglich erscheinen, damit man dem Meeting noch folgen konnte.



Empfangen des Audiostreams
Ein Audiopuffer speichert kontinuierlich die letzten 30 Sekunden Ton. Diese 30 Sekunden werden dann weiterverarbeitet.

Limiter
Der eingehende Audiostream besteht aus 50 Paketen pro Sekunde. Da jedoch nicht 50 Verarbeitungen pro Sekunde durchgeführt werden können, wird dies auf zwei Verarbeitungen pro Sekunde reduziert.

Formatumwandlung
Der Audiostream wird im OGG-OPUS-Format empfangen und in das WAV-Format konvertiert, welches Whisper versteht und verarbeiten kann.

VAD (Voice Activity Detection)
Das System erkennt, ob jemand spricht. Hört es drei Sekunden lang nichts, pausiert es die rechenintensive Verarbeitung – das spart eine Menge Ressourcen.

Transkription
Das eigentliche Herzstück Whisper (oder besser gesagt Faster Whisper) wandelt die Sprachsegmente in Text um. Dabei erhält es auch Informationen von VAD darüber, wann in den letzten 30 Sekunden gesprochen wurde. Dies verringert nebenbei „Halluzinationen“ und erhöht die Qualität der Ausgabe.

Wortpufferung
Ein Puffer merkt sich die letzten 50 erkannten Wörter, sodass sie nicht sofort vom Bildschirm verschwinden oder hektisch hin- und herspringen, falls die KI einzelne Wörter im Nachhinein unnötigerweise korrigiert.

Verarbeitung in der Pipeline: In sechs Schritten wird der eingehende Audiostream kontinuierlich und teils parallel verarbeitet und als Textstream mit Live-Untertiteln generiert.

Optimieren, bis es funktioniert

Im Rahmen der Bachelorarbeit standen diese Schwachstellen gezielt im Fokus. Zeitgleich machte auch die Open-Source-Community riesige Sprünge: Projekte wie Faster Whisper, WhisperX und Whisper Streaming verbesserten die Leistung von Whisper stetig – die KI wurde schneller, stabiler und ressourcenschonender. Der Ansatz war, das Beste aus all diesen Projekten zu kombinieren. Das Ergebnis ist eine aus sechs Schritten bestehende Pipeline, welche den einkommenden Audiostream kontinuierlich und teils parallel verarbeitet und am Ende einen Text-Stream als Live-Untertitel generiert.

Begleitend wurden kontinuierlich Messungen durchgeführt, um herauszufinden, wie lange jeder Verarbeitungsschritt dauert und wo es Optimierungspotenzial gibt. Die Ergebnisse waren verblüffend: Bereits etwa 2,15 Sekunden, nachdem ein Wort fertig ausgesprochen worden war, konnte es als Untertitel auf dem Bildschirm angezeigt werden – ein guter Kompromiss zwischen Schnelligkeit und Genauigkeit. In einer experimentellen Variante war sogar eine Anzeige nach nur 0,7 Sekunden möglich – allerdings mit der Einschränkung, dass die KI manche Wörter erst im Nachhinein korrigieren konnte und sich somit Wörter kurzzeitig mehrfach veränderten, bis sie nach circa 2,67 Sekunden stabil blieben.

Mit dem erzielten Ergebnis ist es nun möglich, die digitale Lehre wesentlich inklusiver zu gestalten als bisher.

Chancen in der Lehre – mit KI-Echtzeitübersetzung

Live-Untertitel sind weit mehr als nur eine technische Spielerei. Sie bedeuten einen echten Fortschritt. Sie gestalten Onlineveranstaltungen barriereärmer, verringern Sprachhürden und schaffen mehr Chancengleichheit in der digitalen Bildung. Diese Lösung ist nicht nur auf BBB beschränkt, sondern lässt sich auch in andere Anwendungen integrieren – und das, ohne die Privatsphäre aus den Augen zu verlieren. Anders als bei vielen externen Diensten verlassen dabei keine Daten das eigene System.

Live-Untertitel sind jedoch erst der Anfang: Mit künftigen Verbesserungen könnten KI-gestützte Echtzeitübersetzungen oder automatisch erstellte Zusammenfassungen die Onlineveranstaltungen weltweit noch effektiver machen. Auch ein interaktiver KI-Tutor, der sich wie ein menschliches Gegenüber anfühlt, ist denkbar. Er könnte Lernende unterstützen, komplexe Themen besser zu verstehen, ohne dabei einfach nur Antworten vorzusagen. Das Beste daran: Alles bleibt open source, läuft auf eigenen Servern und gehört niemandem allein. Wer mitmachen möchte, kann direkt loslegen. Gemeinsam die digitale Bildung offener, freier und besser machen, das ist das Ziel. Let's work together. Let's go open source. ◆

Bereit für eine Demo?
QR-Code zum Video:

Julian Kropp

2020 – 2024 Studium der Informatik an der Hochschule Darmstadt | Abschluss des dualen Bachelorstudiums mit der Arbeit: Entwicklung einer Open-Source Live-Untertitel-Funktion für Online-Veranstaltungen | 2020 – 2024 Dualer Student im IT-Lab von COUNT+CARE (entega).

FUTURE TALENT PROGRAMME
FOR STUDENTS & YOUNG PROFESSIONALS

Das Future Talent Programme (FTP) von GÉANT und seinen NREN-Partnern vernetzt Studierende und junge Berufstätige mit der internationalen GÉANT-Community und bietet ihnen eine Plattform für ihre innovativen Ideen und Forschungsarbeiten. Teilnehmende erhalten professionelles Präsentationstraining, um ihre Projekte vor Expertinnen und Experten überzeugend vorzustellen. Das Highlight: Ein junges Talent bekommt die Möglichkeit, seine Arbeit mit einem „Lightning Talk" bei der Netzwerkkonferenz TNC vor einem großen internationalen Publikum zu präsentieren – Reisekosten inklusive.

Informationen zum Future Talent Programme gibt es unter:
https://community.geant.org/learning/future-talent-programme/

Blick nach vorn – Recht im DFN

Foto: Arne Radeisen

Seit April 2024 verstärkt Prof. Dr. Katharina de la Durantaye, Lehrstuhl für Bürgerliches Recht und Recht der Digitalisierung der Humboldt-Universität zu Berlin, die Forschungsstelle Recht im DFN. Gemeinsam mit Prof. Dr. Thomas Hoeren vom Institut für Informations-, Telekommunikations- und Medienrecht (ITM) der Universität Münster leitet sie das Projekt „Unterstützung von Wissenschaft und Forschung in rechtlichen Fragen bei der sicheren Nutzung des Deutschen Forschungsnetzes“ an den Standorten Berlin und Münster. Im Interview erzählt die Rechtswissenschaftlerin über die Arbeit der Forschungsstelle Recht.

Seit fast einem Jahr leiten Sie gemeinsam mit Professor Hoeren das Projekt in der Forschungsstelle Recht im DFN. Welche Überlegungen sind Ihnen durch den Kopf gegangen, als er auf Sie zukam?

Das Projekt finde ich sehr wichtig, es hat mich gleich gereizt. Und: Thomas Hoeren und sein Team haben das Projekt hervorragend aufgestellt. Durch die Begeisterung und Motivation, die ich dort wahrgenommen habe, ist die Zusammenarbeit schnell zu einer Herzensangelegenheit für mich geworden. Ich musste nicht lange überlegen.

Was hat Sie an der Aufgabe gereizt?

Ich kenne Thomas Hoeren schon lange und wusste, dass er die Forschungsstelle Recht im DFN mit aufgebaut hat. Den DFN-Verein wiederum schätzen wir an den Hochschulen sehr, weil wir täglich mit seinen Diensten zu tun haben. Sie sind für unsere Forschung und Lehre essenziell. Ich mochte die Aussicht, die Erkenntnisse und Themen aus unserem Fachgebiet in die Wissenschaftscommunity tragen zu können. Gleichzeitig ist es für unsere Arbeit wertvoll, dass uns die Mitgliedseinrichtungen des Vereins spiegeln, welche Rechtsfragen sie in der Praxis umtreiben, wo es Unsicherheiten gibt und inwiefern rechtliche Vorgaben ihre Arbeit erschweren. Spannend finde ich den Austausch auch deshalb, weil wir es im

DFN-Verein nicht nur mit Juristen und Juristinnen zu tun haben, sondern auch mit Forschenden und Mitarbeitenden aus den Rechenzentren oder aus dem Datenschutz. Davon profitieren auch die wissenschaftlichen Mitarbeitenden in der Forschungsstelle Recht sehr. Zum einen hilft uns diese Information dabei, die Mitglieder des DFN-Vereins passgenau zu informieren. Zum anderen gilt: Rechtliche Regeln allgemeinverständlich zu kommunizieren, ist eine hohe Kunst.

Ein Projekt mit einer Doppelspitze zu leiten ist gar nicht so einfach. Wie funktioniert die Zusammenarbeit an unterschiedlichen Standorten?

Wir sind im April 2024 in Berlin gestartet und es war ein Segen, Herrn Hoeren und die Kolleginnen und

> Wir wurden sehr warm aufgenommen und haben viel Unterstützung erfahren.

Kollegen aus Münster an unserer Seite zu wissen. Wir wurden sehr warm aufgenommen und haben viel Unterstützung erfahren. Die Münsteraner waren in jeder Hinsicht großzügig. Vor allem profitieren wir von dem immensen Wissensschatz, der über Jahrzehnte in der Forschungsstelle Recht aufgebaut wurde.

Wenn Sie das vergangene Jahr Revue passieren lassen, wie hat sich das Projekt entwickelt?

Ein thematischer Dauerbrenner ist sicherlich das Datenschutzrecht – oft in Verbindung mit dem Telekommunikationsrecht. Hier gibt es viele aktuelle Entwicklungen und entsprechend viele Anfragen von DFN-Mitgliedern. Ein weiterer Bereich, den wir immer wieder behandeln, ist das Urheberrecht. Zudem haben wir uns intensiv mit der europäischen Digitalregulierung beschäftigt. Ein zentraler Rechtsakt ist der Digital Services Act (DSA). Wir haben etwa die darin enthaltenen Regelungen zu systemischen Risiken und die Datenzugangsrechte für Forschende vorgestellt. Hinzu kommt ein Thema, das für Hochschulverwaltungen, Forschende und Lehrende zunehmend Relevanz erhält: die Regulierung von KI. Die europäische KI-VO zum Beispiel wirft viele spannende Fragen auf, die für die Mitglieder des DFN-Vereins von Interesse sind. So enthält sie etwa Sonderregelungen für Hochschulen.

Prof. Dr. Katharina de la Durantaye
Studium der Rechtswissenschaften an der Humboldt-Universität zu Berlin | Studiengang „Master of Laws“ an der Yale University | 2005 bis 2010 (Gast-)Professorin an der Boston University School of Law, der Columbia Law School und der St. Johns University School of Law | 2010 bis 2018 Juniorprofessorin für Bürgerliches Recht, Internationales Privatrecht und Rechtsvergleichung an der Humboldt-Universität zu Berlin | 2018 bis 2021 Lehrstuhl für Bürgerliches Recht und Privates Medienrecht, Europa-Universität Viadrina, Frankfurt (Oder) | 2021 bis 2024 Lehrstuhl für Bürgerliches Recht, Wirtschafts-, Wettbewerbs- und Immaterialgüterrecht an der Freien Universität Berlin | Seit 2024 Leitung des Projekts „Unterstützung von Wissenschaft und Forschung in rechtlichen Fragen bei der sicheren Nutzung des Deutschen Forschungsnetzes“ | Seit 2024 Lehrstuhl für Bürgerliches Recht und Recht der Digitalisierung an der Humboldt-Universität zu Berlin

Im vergangenen Jahr haben uns außerdem rechtliche Aspekte wissenschaftspolitischer Fragen beschäftigt. Hochschulen sind wichtige gesellschaftspolitische Akteure. Sie müssen sich über ihr Handeln in diesen politisch aufgeladenen Zeiten sorgsam Gedanken machen. Neuralgische Punkte sind etwa die Forschungsfreiheit an Hochschulen oder Vorgaben zur Verfassungstreue von Beamtinnen und Beamten. Texte dazu hätten wir vor zehn Jahren im Infobrief Recht vielleicht noch nicht gelesen. Wir hoffen, dass eine differenzierte juristische Betrachtung gerade bei polarisierenden Diskussionen einen Mehrwert hat.

Mir fällt auf, dass die genannten Themen auch Ihre persönlichen Forschungsschwerpunkte widerspiegeln.

Ja, durchaus. Ich forsche schon lange zum Wissenschaftsurheberrecht. Deshalb freue ich mich so sehr, über den DFN-Verein nun stärker mit der Wissenschaftscommunity in Kontakt zu stehen und mein Wissen um Inputs aus der Praxis bereichern zu können.

Auch mit KI-Regulierung beschäftige ich mich aktuell viel. Ich untersuche insbesondere, wie sich die EU im Vergleich zu den USA und China aufstellen kann, um an der Wertschöpfung, die KI mit sich bringt, zu partizipieren, ohne unsere Werte aus dem Blick zu verlieren.

> „Gerade generative KI stellt natürlich auch für die Lehre eine Herausforderung dar."

Gerade generative KI stellt natürlich auch für die Lehre eine Herausforderung dar. Meines Erachtens sollten wir den Studierenden vermitteln, wofür sie sich eignet, aber auch, wo die Limitationen sind. Dafür müssen wir die technischen Hintergründe verstehen und erklären können. Ich biete in meiner Veranstaltung zu wissenschaftlichem Arbeiten eine Einheit zu generativer KI an. Die Studierenden lassen dort Rechtsfragen durch KI beantworten und untersuchen dann die Ergebnisse. Dabei erkennen sie, wie schlecht ihre Studienarbeiten wären, wenn sie sie durch generative KI schreiben lassen würden. Aber sie erfahren auch, wie gut bestimmte Dinge funktionieren. Generative KI wird Forschung, aber auch Lehre und Verwaltung auf absehbare Zeit stark verändern. Meines Erachtens sollten wir ihre Existenz nicht leugnen, sondern uns aktiv damit auseinandersetzen, wie sie unsere Forschung verändern wird und welche Kompetenzen wir den Studierenden vermitteln müssen, damit sie sie sinnvoll einsetzen und die Ergebnisse, die sie erhalten, kritisch überprüfen können.

Wo sehen Sie künftige Themenschwerpunkte?

KI-Regulierung, Datenschutz- und Urheberrecht bleiben uns ganz sicher erhalten. Ich sehe aber noch einen weiteren, verwandten Schwerpunkt für die Zukunft: Durch die wachsende Menge an Daten und die Entwicklung von Datenräumen wird das Datenwirtschaftsrecht immer wichtiger. Hier stellt sich insbesondere die Frage, wie der Zugang zu und der Austausch von Daten gelingen können. Überdies plant die EU nach wie vor eine ganze Reihe weiterer Digitalrechtsakte. In der Wissenschaft wird etwa der angekündigte Digital Networks Act schon hitzig diskutiert. Daneben werden durch technologische, wirtschaftliche oder politische Entwicklungen regelmäßig aktuelle Themen hinzukommen. Ein Beispiel sind nationale und europäische Vorgaben für die Digitalisierung der Verwaltung, die natürlich auch Hochschulen und Forschungseinrichtungen betreffen.

Welchen Benefit hat die Forschungsstelle Recht für die DFN-Mitglieder?

Mit dem Infobrief Recht, dem Podcast „Weggeforscht" sowie unseren Vorträgen und Handreichungen bieten wir einen Überblick über aktuelle rechtliche Themen, die wichtig sind für Hochschulen und Forschungseinrichtungen. Unser Angebot bietet hoffentlich eine gute Basis, um sich allgemein über relevante Fragen zu informieren. Mitglieder können aber auch Rückfragen stellen und niedrigschwellig um Unterstützung bitten. Auf Basis unserer Erklärungen können sie einfacher entscheiden, inwieweit sie rechtliche Vorgaben umsetzen und/oder eine individuelle Rechtsberatung in Anspruch nehmen müssen. Ich glaube, für die DFN-Community ist es gut zu wissen, dass sie mit ihren rechtlichen Fragestellungen nicht alleine dastehen. Auch für uns ist es hilfreich, in den Austausch zu gehen und zu erfahren, wo Informationsbedarf besteht. Dann können wir diese Themen verstärkt behandeln. Deshalb freuen wir uns, wenn Mitglieder auf uns zukommen und die Behandlung von Themen anregen, die in den Wissenschaftseinrichtungen virulent sind.

Das Gespräch führte Annette Rülke (DFN-Verein).

Föderal. Digital. Gut.

Die deutsche Verwaltung soll digitalisierter arbeiten

Der Planungsrat für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (IT-Planungsrat) beschloss am 13. November 2024 den ersten Teil der föderalen Digitalstrategie für die Verwaltung, die sogenannte Dachstrategie, bestehend aus einem Zukunftsbild und Leitlinien. Die Strategie ermöglicht einen ersten Einblick, wie sich das Gremium die Verwaltung von morgen vorstellt.

Text: **Anna Maria Yang-Jacobi** (Forschungsstelle Recht im DFN)

Foto: mh.desing/Adobe Stock

I. Der IT-Staatsvertrag als rechtliche Grundlage

Die Verwaltungszuständigkeiten von Bund und Ländern sind prinzipiell getrennt. Für eine kontinuierliche Digitalisierung von Verwaltungsverfahren braucht es allerdings Interoperabilität und gemeinsame Standards. So veränderten Bundestag und Bundesrat 2009 im Zuge der Föderalismusreform II[1] das Grundgesetz und beschlossen Art. 91c Grundgesetz (GG). Über Art. 91c GG sind der Bund und die Länder ermächtigt, bei IT-Systemen im Rahmen der staatlichen Aufgabenerfüllung zusammenzuwirken, Standards und Sicherheitsanforderungen festzulegen und den gemeinschaftlichen Betrieb sowie die Errichtung von IT-Systemen zu vereinbaren.

Folglich entstand ein Staatsvertrag (IT-Staatsvertrag).[2] Der IT-Staatsvertrag ist ein Länderstaatsvertrag. Mithilfe von Länderstaatsverträgen vereinbaren die Länder untereinander und/oder mit dem Bund einheitliche Maßstäbe in bestimmten öffentlich-rechtlichen Bereichen. Sie bedürfen eines gesetzgeberischen Akts, sodass die Landesparlamente zustimmen müssen. Ziel des IT-Staatsvertrags ist, die Zusammenarbeit von Bund und Ländern bei der Digitalisierung von Verwaltungsleistungen zu regeln und zu koordinieren. Auf Grundlage des IT-Staatsvertrags etablierte sich ein gemeinsames Bund-Länder-Gremium, der IT-Planungsrat.

2019 wurde der IT-Staatsvertrag erstmals verändert und die Föderale IT-Kooperation (FITKO) sowie ein gemeinsames Digitalisierungsbudget eingeführt.[3] Eine zweite Modifikation des IT-Staatsvertrags erfolgte über ein entsprechendes Gesetz im Herbst 2024[4] und trat am 1.12.2024 in Kraft.[5]

II. Der IT-Planungsrat und die FITKO

Der IT-Planungsrat besteht seit 2010. Die Mitglieder sind nach § 1 Abs. 2 IT-Staatsvertrag der IT-Beauftragte der Bundesregierung (CIO Bund) sowie 16 für Informationstechnik zuständige Vertreter:innen der Bundesländer. Zusätzlich können drei Vertreter:innen der Gemeinden und Gemeindeverbände sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) beratend an den Sitzungen teilnehmen. Sofern Fachministerkonferenzen von den Entscheidungen des IT-Planungsrats betroffen sind, beteiligen sich diese auch an den Sitzungen. Der Vorsitz wechselt jährlich von Bund zu Ländern. So löst die Vertreterin aus Mecklenburg-Vorpommern, Ina-Maria Ulbrich, den CIO Bund 2025 als neue Vorsitzende des IT-Planungsrats ab.

Die Aufgaben des IT-Planungsrats sind vielfältig. Nach § 1 Abs. 1 IT-Staatsvertrag übernimmt das Gremium die IT-Koordination zwischen Bund und Ländern, legt IT-Standards im Bereich der Interoperabilität und Sicherheit fest, treibt die Digitalisierung der Verwaltung voran, lenkt Projekte des sogenannten E-Governments und ist für das Verbindungsnetz zwischen Bund und Ländern nach Art. 91c Abs. 4 GG zuständig. Um diesen zahlreichen Aufgaben nachzukommen, tagt der IT-Planungsrat in der Regel jeweils im Frühjahr, Sommer und Herbst eines Jahres. Auf Antrag des Bundes oder von drei Ländern können zusätzliche Sitzungen stattfinden. In den Zusammentreffen tauscht sich der IT-Planungsrat aus und fasst Beschlüsse. Im Bereich der Standardisierung von Datenobjekten, Datenformaten, Verfahren zur Datenübertragung und zur IT-Sicherheit können Beschlüsse, die für den Datenaustausch von Bund und Ländern sowie mit Bürger:innen und der Wirtschaft notwendig sind, nach § 2 Abs. 2 IT-Staatsvertrag Bindungswirkung entfalten. Dadurch können Veränderungen allgemeingültig in die öffentliche Verwaltung getragen werden.

Seit dem 1.1.2020 existiert auf Grundlage des § 5 IT-Staatsvertrag die FITKO neben dem IT-Planungsrat. Ziel war es, eine zusätzliche Beratungs- und Umsetzungsorganisation für den IT-Planungsrat zu schaffen. Die FITKO arbeitet eng mit den Kommunen zusammen und unterstützt den IT-Planungsrat organisatorisch und fachlich. So bündeln sich die föderalen Aktivitäten zur Digitalisierung der Verwaltung. Vor allem konzipiert und entwickelt die FITKO eine föderale IT-Architektur und begleitet die Finanzierung und Umsetzung von Digitalisierungsprojekten. Die Arbeit der FITKO ergänzt und erleichtert demnach die Tätigkeiten des IT-Planungsrats.

Jüngst passte das Gesetz zum zweiten IT-Änderungsstaatsvertrag die Aufgaben des IT-Planungsrats an. Die Verwaltungsdigitalisierung ist nun als Daueraufgabe von Bund und Ländern definiert. Außerdem kann der oder die FITKO-Präsident:in künftig beratend an den Sitzungen des IT-Planungsrats teilnehmen und das Finanzierungsmodell der FITKO wurde neu ausgerichtet.

---

1 Föderalismusreform II von 2009, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl109s2248.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl109s2248.pdf%27%5D__1733741825275 (alle Links dieses Beitrags zuletzt abgerufen am 7.1.2025).

2 Der Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern, Vertrag zur Ausführung von Artikel 91c GG (IT-Staatsvertrag) trat am 1.4.2010 in Kraft. In der Zwischenzeit wurde er zweimal verändert und ist in seiner aktuellen Fassung hier zu finden, https://www.buzer.de/IT-Staatsvertrag.htm.

3 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/12/foederale-it-kooperation.html.

4 https://www.recht.bund.de/bgbl/1/2024/326/VO.html.

5 Eine Bekanntmachung im Bundesgesetzblatt steht bislang noch aus. Beispielsweise in Bayern erfolgte sie bereits, https://www.verkuendung-bayern.de/gvbl/2024-642/.

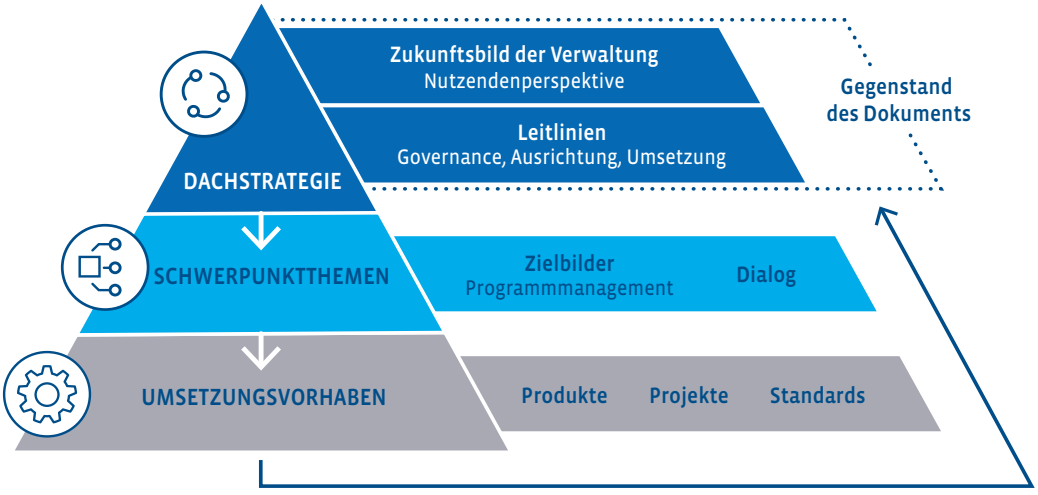


Abbildung 1: Schaubild Zukunftsbild der Verwaltung, Quelle: https://www.it-planungsrat.de/der-it-planungsrat/foederale-digitalstrategie

III. Die föderale Digitalstrategie für die Verwaltung

Die föderale Digitalstrategie des IT-Planungsrats geht auf einen Beschluss des IT-Planungsrats von November 2023 zurück.[6] Die Verwaltung soll zukunftsfähig werden und die Zusammenarbeit von Bund, Ländern und Kommunen bei der Digitalisierung der Verwaltung effizienter erfolgen. Die Digitalstrategie soll zudem Dienstleistenden und Verbänden zur Orientierung dienen, um die Vorteile der Digitalisierung zu nutzen und bestehende Hürden abzubauen. Mithin soll die Digitalstrategie die Verwaltung darin unterstützen, den Vorgaben des EU-Rechts und des nationalen Rechts nachzukommen.

Die Digitalstrategie umfasst drei Komponenten: Erstens soll eine Dachstrategie die gesamtstrategische Ausrichtung festlegen. Die Dachstrategie besteht aus einem Zukunftsbild der Verwaltung und Leitlinien für die Verwaltung. Zweitens gibt es seit 2022 fünf Schwerpunktthemen, die bestimmten Bundesländern oder dem Bund in Patenschaft zugeordnet sind. Für die Umsetzung der Themen sind eigene Zielbilder und Ableitungsvorhaben erforderlich. Drittens ergeben sich aus den ersten beiden Komponenten Umsetzungsvorhaben. Diese sind teilweise schon umgesetzt, müssen aber neu miteinander verknüpft werden oder sind erst noch anzustoßen.

IV. Die Dachstrategie

Der IT-Planungsrat verabschiedete im November 2024 den ersten Teil der föderalen Digitalstrategie. Die Dachstrategie sei laut Markus Richter, dem CIO Bund, der „größte Schritt der vergangenen Jahre“.[7] Im Rahmen der Strategie ermittelte der IT-Planungsrat die Probleme der deutschen Verwaltung wie beispielsweise sinkende personelle und finanzielle Mittel, zunehmende Krisensituationen und ein abnehmendes Vertrauen der Bürger:innen in die staatliche Handlungsfähigkeit.[8] Das Zukunftsbild widmet sich der Lösung dieser Herausforderungen. Oberstes Gebot stellt das gemeinsame Handeln in der Verwaltung der Zukunft dar. Durch Arbeitsteilung, Nutzung bestehender Synergien, Automatisierung und Cloud-Anwendungen kann die Effizienz der Verwaltung als Antwort auf knappere Ressourcen gesteigert werden.[9] Eine weitere Säule des Zukunftsbilds ist ein vorausschauendes Handeln der Verwaltung. Die Verwaltung muss auf Krisen und Angriffe vorbereitet sein und Daten für (politische) Entscheidungen bereitstellen. Zuletzt kann die Verwaltung das Vertrauen in den Staat und die Demokratie durch transparente Strukturen stärken, was auch im Zukunftsbild festgelegt wird.

Die Leitlinien bieten den Rahmen für bestehende und geplante Umsetzungsvorhaben.[10] Aus ihnen können anschließend konkrete Beschlüsse folgen, die das gemeinsame Vorgehen untermauern.[11] Sie sind in die Gruppen Governance-Leitlinien, fachliche Leitlinien und Umsetzungsprinzipien aufgeteilt.

6 IT-Planungsrat, Beschluss 2023/42, 3.11.2023, https://www.it-planungsrat.de/beschluss/beschluss-2023-42#:~:text=Der%20IT%2DPlanungsrat%20beschließt%2C%20dass,Arbeiten%20in%20den%20Schwerpunktthemen%20beinhaltet.
7 https://www.heise.de/news/Digitalisierung-der-Verwaltung-Revolution-im-IT-Planungsrat-gescheitert-10032117.html.
8 IT-Planungsrat, Beschluss 2024/40, 13.11.2024, https://www.it-planungsrat.de/beschluss/beschluss-2024-40, S. 8f.
9 IT-Planungsrat, Beschluss 2024/40, 13.11.2024, https://www.it-planungsrat.de/beschluss/beschluss-2024-40, S. 11.
10 IT-Planungsrat, Beschluss 2024/40, 13.11.2024, https://www.it-planungsrat.de/beschluss/beschluss-2024-40, S. 13.
11 IT-Planungsrat, Beschluss 2024/40, 13.11.2024, https://www.it-planungsrat.de/beschluss/beschluss-2024-40, S. 14–18.

Die Governance-Leitlinien gelten vor allem für den IT-Planungsrat selbst. Darunter fallen Arbeitsschritte wie beispielsweise Aufgaben zu ermitteln, die Kommunen bisher dezentral erledigen oder die schon zentralisiert auf Bundesebene oder über länderübergreifende Kooperationen abgewickelt werden können. Andere Beispiele sind: das „Einer-für-Alle-Prinzip“ zu einem „Einer prüft für Alle“ und „Einer betreibt für Alle“ auszubauen,[12] das zentrale Digitalbudget für gemeinsam benötigte Basiskomponenten und IT-Komponenten zu nutzen, die Zusammenarbeit von öffentlichen IT-Dienstleistern und privaten Anbietern zu verbessern sowie mit den Verfahrensverantwortlichen eng zusammenzuarbeiten, um neue Technologien und Prozesse transparent zu identifizieren.

Die fachlichen Leitlinien[13] legen die übergreifende Ausrichtung der fünf Schwerpunktthemen (Digitale Transformation, Digitale Infrastruktur, Digitale Anwendungen, Datennutzung und Informationssicherheit) fest. Wichtige Rollen spielen die Automatisierung von Prozessen, die Schaffung eines Referenzmodells für eine „Deutschland-Architektur“, um die gemeinsame Nutzung von IT-Lösungen interoperabel zu machen, und die Umsetzung des Once-Only-Prinzips[14] über Technikentwicklung. Bei allen Anwendungen sind hohe Qualitätsstandards einzuhalten, sodass Datenschutz, IT-Sicherheit, Barrierefreiheit, Datenmanagement und Nutzerfreundlichkeit bereits bei der Entwicklung der Angebote mitgedacht werden sollen. Eine enge Vernetzung zwischen Hochschulen und Verwaltung ist gerade im Bereich der Nachwuchsgewinnung vorgesehen.

Die Umsetzungsprinzipien[15] dienen dazu, die Umsetzung des Zukunftsbilds in der Realität zu gewährleisten. Dafür schafft man (auch mithilfe der FITKO) verbindliche und arbeitsfähige Strukturen zur Verantwortungsübernahme. Zusätzlich sollen bisher bestehende (umständliche) Nachweispflichten durch Belehrung, Eigenerklärung, Stichprobenprüfungen und ggf. Sanktionen ersetzt werden. Der Dialog mit den Nutzenden ist dabei stetig zu suchen. Die konkreten Umsetzungsvorhaben sollen regelmäßig anhand der Wirkung beurteilt werden.

Alles in allem sind sowohl das Zukunftsbild als auch die Leitlinien einem dynamischen Prozess ausgesetzt und begleiten die Pläne für die digitale Verwaltung langfristig. Die föderale Digitalstrategie ist auch für öffentliche Hochschulen und wissenschaftliche Einrichtungen von Bedeutung. Als Körperschaften oder Anstalten des öffentlichen Rechts sind sie regelmäßig Adressaten der Verwaltungsdigitalisierungsgesetze.[16] ◆

12 Das Bundesministerium des Innern und für Heimat (BMI) hat das „Einer-für-Alle-Prinzip“ bei der Umsetzung des Onlinezugangsgesetzes von 2017 eingeführt. Danach soll jedes Bundesland Leistungen so digitalisieren, dass andere Bundesländer diese im Nachhinein auch nutzen können und eine eigene Entwicklung von Anwendungen überflüssig ist. Genaueres zu diesem Prinzip: https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/efa/efa-node.html.

13 IT-Planungsrat, Beschluss 2024/40, 13.11.2024, https://www.it-planungsrat.de/beschluss/beschluss-2024-40, S. 18–24.

14 Das Once-Only-Prinzip besagt, dass eine Information von Bürger:innen und Unternehmen nur ein einziges Mal bereitgestellt werden muss. Die Behörden tauschen die Informationen sodann digital aus. Für weitere Informationen: https://www.bundesfinanzministerium.de/Monatsberichte/2023/06/Inhalte/Kapitel-3-Analysen/3-3-once-only-prinzip.html.

15 IT-Planungsrat, Beschluss 2024/40, 13.11.2024, https://www.it-planungsrat.de/beschluss/beschluss-2024-40, S. 24–26.

16 Den konkreten Folgen von nationalen (Digitalisierungs-)Gesetzen für Hochschulen und Forschungseinrichtungen, die Teil der öffentlichen Verwaltung sind, wird in Yang-Jacobi, Von Papierbergen zur e-Verwaltung?, DFN-Infobrief Recht 4/2025 nachgegangen, https://recht.dfn.de/wp-content/uploads/2025/04/Infobrief_Recht_4-2025.pdf.

Heute schon geNISt?

Die Umsetzung der NIS-2-Richtlinie durch die Bundesregierung lässt weiter auf sich warten

Die Network and Information Security (NIS)-2-Richtlinie (NIS-2-RL) der Europäischen Union muss nach wie vor vom deutschen Gesetzgeber umgesetzt werden, obwohl die Umsetzungsfrist seit dem 18. Oktober 2024 abgelaufen ist. Ein umfangreicher Gesetzentwurf der Bundesregierung liegt vor, der insbesondere den Anwendungsbereich des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) stark erweitert.

Text: **Marc-Philipp Geiselmann** (Forschungsstelle Recht im DFN)

I. Hintergrund der NIS-2-RL

Cyberangriffe gefährden die Funktionsfähigkeit von Unternehmen wie Behörden. Der Gesamtschaden durch Datendiebstahl, Industriespionage oder Sabotage betrug in Deutschland im Jahr 2024 266,6 Milliarden EUR.[1] Demgegenüber stehen Ausgaben für die IT-Sicherheit in Höhe von 11,2 Milliarden EUR.[2] Die NIS-Richtlinie sollte 2016 als erste europäische Regulierung Mindestanforderungen bezüglich der Sicherheit der Netze und Informationssysteme harmonisieren und EU-weit die Zusammenarbeit der Mitgliedstaaten in Bereich der Informationssicherheit verbessern. Allerdings wurde die NIS-RL in den Mitgliedstaaten sehr unterschiedlich umgesetzt. Insbesondere der Begriff der „wesentlichen Dienste“ wurde unterschiedlich definiert, was zu einem uneinheitlichen Anwendungsbereich innerhalb der EU führte. Zudem stellte sich das Schutzniveau der NIS-RL angesichts der zunehmenden Cyberangriffe als zu niedrig heraus.[3] Anfang 2022 trat die zweite Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-RL) anstelle der bisherigen Vorgaben in Kraft.[4]

Bis 17. Oktober 2024 sollten die EU-Mitgliedstaaten die NIS-2-Richtlinie in nationales Recht umsetzen.[5] Bislang hat die Bundesrepublik Deutschland allerdings kein Umsetzungsgesetz erlassen. Am 2. Oktober 2024 wurde der Entwurf der Bundesregierung für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) dem Bundestag zugeleitet.[6] Angesichts der im Februar durchgeführten Neuwahl wurde der Entwurf in der abgelaufenen Legislaturperiode nicht mehr verabschiedet. Dabei leitete die EU-Kommission schon Ende November gegen 23 der 27 EU-Mitgliedstaaten, darunter Deutschland, ein Vertragsverletzungsverfahren wegen der Nichteinhaltung der Umsetzungsfrist ein.[7] Jedoch wird der aktuelle Gesetzentwurf auch in der neuen Legislatur wegen des Grundsatzes der materiellen Diskontinuität nicht sofort, sondern erst nach neuerlichen Beratungen verabschiedet werden können.[8] Damit steigt die Wahrscheinlichkeit einer Klage der EU-Kommission vor dem Europäischen Gerichtshof (EuGH) wegen der fehlenden Umsetzung der NIS-2-RL.

1 Schäden durch Datendiebstahl, Industriespionage oder Sabotage in Deutschland im Jahr 2024, abrufbar unter https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen, zuletzt abgerufen am 28.02.2025.

2 Ausgaben für IT-Sicherheit in Deutschland in den Jahren 2017 bis 2023 und Prognose bis 2024, abrufbar unter https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/, zuletzt abgerufen am 28.02.2025.

3 Ausführlich dazu John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?, DFN-Infobrief Recht 4/2023.

4 Gitter, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. 2024, § 15 Rn. 13.

5 Vgl. Art. 41 Abs. 1 NIS-2-RL.

6 BT-Drs. 20/13184 vom 02.10.2024, abrufbar unter https://dserver.bundestag.de/btd/20/131/2013184.pdf, zuletzt abgerufen am 28.02.2025.

7 Pressemitteilung, EU-Kommission, Die Kommission fordert 23 Mitgliedstaaten auf, die NIS-2-Richtlinie vollständig umzusetzen, https://digital-strategy.ec.europa.eu/de/news/commission-calls-23-member-states-fully-transpose-nis2-directive, zuletzt abgerufen am 28.02.2025.

8 Magiera, in: Sachs, 10. Aufl. 2024, GG, Art. 39 Rn. 15.

II. NIS-2-RL

Die NIS-2-Richtlinie erweitert und konkretisiert die Regelungen der NIS-Richtlinie, die im August 2016 in Kraft trat. Sie nimmt einen Wechsel vom vorherigen sektoralen Ansatz hin zu einem risikobasierten vor.[9] Insbesondere wurde der Anwendungsbereich der Richtlinie deutlich erweitert und harmonisierte Sicherheitsanforderungen wurden konkretisiert. Während der Sektor der öffentlichen Verwaltung vom Anwendungsbereich der NIS-Richtlinie noch nicht umfasst war (vgl. Art. 1 NIS-RL), erstreckt sich der erweiterte Anwendungsbereich der NIS-2-Richtlinie nun auch auf Einrichtungen der öffentlichen Verwaltung i. S. d. Art. 2 Abs. 2 lit. f Ziffer ii NIS-2-RL, Art. 6 Nr. 35 NIS-2-RL.

1. Gegenstand und Anwendungsbereich

Mit der NIS-2-RL soll ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden, Art. 1 Abs. 1 NIS-2-RL. Dazu werden alle Mitgliedstaaten verpflichtet, nationale Cybersicherheitsstrategien zu verabschieden sowie Behörden für das Cyberkrisenmanagement und Computernotfallteams zu benennen oder einzurichten, Art. 1 Abs. 2 lit. a NIS-2-RL. Einrichtungen, die von der NIS-2-RL erfasst sind, werden zudem Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Berichtspflichten auferlegt, Art. 1 Abs. 2 lit. b NIS-2-RL. Außerdem werden Vorschriften zum Austausch von Cybersicherheitsinformationen sowie Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten implementiert.

Für die Bestimmung der von der Richtlinie erfassten Einrichtungen verweist Art. 2 Abs. 1 NIS-2-RL auf den Anhang I und II der Richtlinie. Im Anhang I sind elf Sektoren mit hoher Kritikalität aufgeführt, die sich wiederum in Teilsektoren und verschiedene Arten der jeweiligen Einrichtungen untergliedern. Dabei handelt es sich um Energie (Nr. 1), Verkehr (Nr. 2), Bankwesen (Nr. 3), Finanzmarktinfrastrukturen (Nr. 4), Gesundheitswesen (Nr. 5), Trinkwasser (Nr. 6), Abwasser (Nr. 7), digitale Infrastruktur (Nr. 8), Verwaltung von IKT-Diensten (Business-to-Business) (Nr. 9), öffentliche Verwaltung (Nr. 10) und Weltraum (Nr. 11). Im Anhang II sind sieben sonstige kritische Sektoren aufgelistet. Das sind Post- und Kurierdienste (Nr. 1), Abfallbewirtschaftung (Nr. 2), Produktion, Herstellung und Handel mit chemischen Stoffen (Nr. 3), Produktion, Verarbeitung und Vertrieb von Lebensmitteln (Nr. 4), Verarbeitendes Gewerbe / Herstellung von Waren (Nr. 5), Anbieter digitaler Dienste (Nr. 6) und Forschung (Nr. 7). Der Begriff der Forschungseinrichtung ist nach Art. 6 Nr. 41 NIS-2-RL als Einrichtung definiert, deren primäres Ziel es ist, die angewandte Forschung oder die experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschließt. Die Einrichtungen sind jedoch nur betroffen, sofern sie nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten. Das bedeutet, dass die Einrichtung 50 oder mehr Personen beschäftigen oder der Jahresumsatz der Einrichtung 10 Mio. EUR oder mehr betragen muss. Der Art. 2 Abs. 2 bis 4 NIS-2-RL listet Einrichtungen auf, die unabhängig von ihrer Größe erfasst sind. Die Mitgliedstaaten können zudem kommunale Einrichtungen und Bildungseinrichtungen miteinbeziehen, Art. 2 Abs. 5 NIS-2-RL.[10]

Art. 3 NIS-2-RL unterteilt die Einrichtungen anschließend nochmals in wesentliche und wichtige Einrichtungen. Wesentlich sind die Einrichtungen der in Anhang I aufgeführten Art, die die in Art. 2 Abs. 1 des Anhangs der Empfehlung 2003/361/EG genannten Schwellenwerte für mittlere Unternehmen überschreiten. Das bedeutet, dass die Einrichtungen 250 oder mehr Personen beschäftigen oder einen Jahresumsatz von mehr als 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf mehr als 43 Mio. EUR belaufen muss. In Art. 3 Abs. 1 lit. b bis g NIS-2-RL sind weitere Einrichtungen unabhängig von ihrer Größe aufgelistet. Alle weiteren in Anhang I und II aufgeführten Unternehmen, die nicht als wesentliche Einrichtungen gelten, gelten als wichtige Einrichtungen.

2. Cybersicherheitsstrategie

Gemäß Art. 7 obliegt es jedem Mitgliedstaat, eine nationale Cybersicherheitsstrategie zu erlassen, welche die strategischen Ziele definiert und die zur Erreichung dieser Ziele notwendigen Ressourcen sowie angemessene politische und regulatorische Maßnahmen umfasst. Diese Strategie muss insbesondere die Ziele und Prioritäten im Bereich der Cybersicherheit abbilden, die in den Anhängen genannten Sektoren berücksichtigen und einen Steuerungsrahmen zur Erreichung dieser Ziele festlegen, Art. 7 Abs. 1 lit. a und b NIS-2-RL. Der Steuerungsrahmen soll die Aufgaben und Zuständigkeiten der nationalen Interessenträger klarstellen und die Koordination sowohl auf nationaler Ebene als auch mit den sektorspezifisch zuständigen Behörden der Union sicherstellen, Art. 7 Abs. 1 lit. c NIS-2-RL. Weiterhin sieht die Strategie Mechanismen zur Risikoermittlung und -bewertung vor, um Vorsorge, Reaktionsfähigkeit und Wiederherstellung im Falle von Sicherheitsvorfällen zu gewährleisten, Art. 7 Abs. 1 lit. d und e NIS-2-RL. Eine Liste der beteiligten Behörden und Interessenträger ist zu erstellen, und es sind Maßnahmen zur Förderung der Cybersicher-

9 Bostelmann, in: Hornung/Schallbruch, IT-Sicherheitsrecht, §25 Rn. 17.
10 Gitter, in: Hornung/Schallbruch, IT-Sicherheitsrecht, §15 Rn. 13 ff.

heitssensibilisierung der Bürger zu ergreifen, Art. 7 Abs. 1 lit. f und h NIS-2-RL.

Im Rahmen der nationalen Cybersicherheitsstrategie müssen Mitgliedstaaten Konzepte entwickeln, die insbesondere die Sicherheit in der Lieferkette von IKT-Produkten und -Diensten betreffen, Art. 7 Abs. 2 lit. a NIS-2-RL. Dies schließt die Spezifikation von Cybersicherheitsanforderungen bei öffentlichen Aufträgen ein, etwa zur Zertifizierung, Verschlüsselung und Nutzung quelloffener Produkte, Art. 7 Abs. 2 lit. b NIS-2-RL. Zudem sind Maßnahmen zur koordinierten Offenlegung von Schwachstellen und zur Sicherstellung der Integrität und Vertraulichkeit des öffentlichen Internets, einschließlich Unterseekabel, erforderlich, Art. 7 Abs. 2 lit. c und d NIS-2-RL. Die Strategie fördert den Einsatz fortschrittlicher Technologien, die Bildung und Sensibilisierung im Bereich Cybersicherheit sowie die Unterstützung von Hochschulen bei der Verbesserung der Cybersicherheitsinstrumente und -infrastruktur, Art. 7 Abs. 2 lit. e bis g NIS-2-RL. Ein effektiver Informationsaustausch zwischen Einrichtungen soll gewährleistet werden und die Cyberresilienz von kleinen und mittleren Unternehmen ist zu stärken, insbesondere von solchen außerhalb des Anwendungsbereichs der Richtlinie, Art. 7 Abs. 2 lit. h und i NIS-2-RL. Abschließend wird die Förderung eines aktiven Cyberschutzes angestrebt, Art. 7 Abs. 2 lit. j NIS-2-RL.

Die Mitgliedstaaten sind verpflichtet, ihre Cybersicherheitsstrategien innerhalb von drei Monaten nach deren Erlass der Europäischen Kommission zu notifizieren, wobei auf nationale Sicherheitsbelange bezogene Informationen ausgenommen werden können, Art. 7 Abs. 3 NIS-2-RL. Eine regelmäßige, mindestens alle fünf Jahre durchzuführende Bewertung und gegebenenfalls Aktualisierung der Strategien anhand wesentlicher Leistungsindikatoren wird vorgeschrieben. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) steht den Mitgliedstaaten auf Anfrage beratend zur Seite, um die Strategie konform mit den Richtlinienanforderungen anzupassen oder zu aktualisieren, Art. 7 Abs. 4 NIS-2-RL.

3. Behörden für das Cyberkrisenmanagement

Gemäß Art. 9 NIS-2-RL muss jeder Mitgliedstaat eine oder mehrere Behörden ernennen oder einrichten, die für das Management von Cybersicherheitsvorfällen großen Ausmaßes zuständig sind. Diese Behörden sind mit angemessenen Ressourcen auszustatten und sollen im Einklang mit bestehenden nationalen Krisenmanagementsystemen arbeiten. Sollte es mehrere solche Behörden geben, muss eine als Koordinator benannt werden, Art. 9 Abs. 1 f. NIS-2-RL.

Zudem hat jeder Mitgliedstaat die notwendigen Kapazitäten, Mittel und Verfahren zu identifizieren und einen nationalen Reaktionsplan zu entwickeln, Art. 9 Abs. 3 NIS-2-RL. Darüber hinaus ist ein nationaler Plan zu verabschieden, der die Ziele und Verfahren des Cyberkrisenmanagements festlegt, die Verantwortlichkeiten der zuständigen Behörden klärt, die Verfahren in den nationalen Krisenmanagementrahmen integriert und relevante Interessenträger sowie Infrastrukturen berücksichtigt, Art. 9 Abs. 4 NIS-2-RL.

Die Mitgliedstaaten sind verpflichtet, der Europäischen Kommission innerhalb von drei Monaten die Identität der zuständigen Behörde zu melden und relevante Informationen über ihre Reaktionspläne bereitzustellen. Informationen können ausgeschlossen werden, wenn dies für die nationale Sicherheit erforderlich ist, Art. 9 Abs. 5 NIS-2-RL.

4. Computernotfallteams (CSIRTs)

Jeder Mitgliedstaat muss nach Art. 10 NIS-2-RL ein oder mehrere Computer-Notfallteams (CSIRTs) benennen oder einrichten, die die Anforderungen der Richtlinie erfüllen und für bestimmte Sektoren zuständig sind, Art. 10 Abs. 1 NIS-2-RL. Diese CSIRTs erhalten ausreichende Ressourcen und eine sichere Kommunikationsinfrastruktur für den Informationsaustausch mit wichtigen Einrichtungen und anderen Akteuren, Art. 10 Abs. 2 f. NIS-2-RL. Sie arbeiten mit sektorenübergreifenden Einrichtungen zusammen, nehmen an Peer Reviews teil und kooperieren innerhalb des CSIRTs-Netzwerks, Art. 10 Abs. 4 bis 6 NIS-2-RL. Auch Beziehungen zu nationalen Computer-Notfallteams von Drittländern können aufgenommen werden, um einen effektiven Informationsaustausch zu ermöglichen, Art. 10 Abs. 7 f. NIS-2-RL. Die Mitgliedstaaten müssen der Europäischen Kommission die Identität und Aufgaben der CSIRTs mitteilen und haben die Möglichkeit, bei der Einrichtung der CSIRTs Unterstützung von der ENISA zu erhalten, Art. 10 Abs. 9 f. NIS-2-RL.

III. Gesetzentwurf der Bundesregierung

Um die NIS-2-RL umzusetzen, sieht der Entwurf des NIS2UmsuCG insbesondere umfangreiche Änderungen am BSIG vor.

Änderungen des BSIG

Der Entwurf der von der Ampelkoalition getragenen Bundesregierung sieht wesentliche Änderungen des BSIG vor. Statt der bisherigen 14 Paragrafen beinhaltet das BSIG-E der Bundesregierung 65 Paragrafen.

Kernstück des Gesetzentwurfs ist Teil 3, der die Sicherheit in der Informationstechnik von Einrichtungen regelt. In diesem wird zunächst der Anwendungsbereich des BSIG deutlich erweitert. War dieser bisher auf Betreiber kritischer Infrastrukturen, Anbieter

digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkt, so führt der Entwurf der Bundesregierung für das NIS2UmsuCG die durch die NIS-2-RL vorgegebenen Einrichtungskategorien „besonders wichtige Einrichtungen und wichtige Einrichtungen“ ein. Dies schließt in Summe deutlich mehr Unternehmen ein.[11] Zudem führt § 28 Abs. 7 BSIG-E die neue Kategorie der Betreiber kritischer Anlagen ein. Der Begriff der kritischen Anlage wird in § 2 Nr. 22 BSIG-E legaldefiniert und meint demnach Anlagen, die für die Erbringung einer kritischen Dienstleistung erheblich sind. Gem. § 29 Abs. 1, 2 BSIG-E sind auf Einrichtungen der Bundesverwaltung, mit wenigen Ausnahmen, die Regelungen für besonders wichtige Einrichtungen anzuwenden.

In § 30 BSIG-E finden sich die Mindestsicherheitsanforderungen des Art. 21 Abs. 2 NIS-2-Richtlinie als Risikomanagementmaßnahmen für besonders wichtige Einrichtungen und wichtige Einrichtungen. Diese sind gem. § 30 Abs. 1 BSIG-E dazu verpflichtet, „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen […] zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden […].“ § 30 Abs. 2 BSIG-E konkretisiert die Mindestanforderungen an die zu ergreifenden technischen und organisatorischen Maßnahmen.

Mit der Klassifizierung als besonders wichtige oder wichtige Einrichtung gem. § 28 BSIG-E gehen außerdem auch Melde-, Registrierungs- und Unterrichtungspflichten einher, welche die §§ 32 ff. BSIG-E umsetzen. Darüber hinaus kommen den Geschäftsleitungen entsprechender Einrichtungen Umsetzungs-, Überwachungs- und Schulungspflichten zu, § 38 BSIG-E. Statt wie bisher alle zwei Jahre sollen Betreiber kritischer Anlagen gem. § 39 BSIG-E nur noch alle drei Jahre die Umsetzung der technischen und organisatorischen Maßnahmen i. S. d. § 30 BSIG-E nachweisen müssen.

IV. Relevanz für Hochschulen

Die Umsetzung der NIS-2-Richtlinie wird sich in Deutschland aufgrund der vorgezogenen Bundestagswahl im Februar noch verzögern. Jedoch hat die EU-Kommission bereits ein Vertragsverletzungsverfahren initiiert, sodass die Umsetzung eilt. Dass sich der neue Bundestag den Gesetzentwurf der von der Ampelkoalition getragenen Bundesregierung von Oktober 2024 in weiten Teilen zu eigen machen wird, ist deshalb nicht unwahrscheinlich. Dieser allerdings sieht keine Übergangsfristen vor, sodass sich bereits jetzt die Prüfung lohnt, ob eine Einrichtung von dem Anwendungsbereich der NIS-2-RL betroffen ist.[12]

Die NIS-2-RL erfasst Forschungseinrichtungen in Anhang II Nr. 7 als sonstige kritische Einrichtungen. In der Definition der Forschungseinrichtungen in Art. 6 Nr. 41 NIS-2-RL werden Bildungseinrichtungen allerdings ausgeschlossen. Dennoch können die Mitgliedstaaten nach Art. 2 Abs. 5 lit. b NIS-2-RL vorsehen, dass die Richtlinie auf Bildungseinrichtungen Anwendung findet, insbesondere, wenn sie kritische Forschungstätigkeiten durchführen.

Auch § 2 Nr. 12 BSIG-E übernimmt diese Definition, welche Bildungseinrichtungen von der Definition der Forschungseinrichtungen ausnimmt. In der Stellungnahme des Nationalen Normenkontrollrates, der dem Gesetzentwurf als Anlage 2 beigefügt ist, ist aufgeführt, dass der Gesetzentwurf einem Beschluss des IT-Planungsrates (2023/39) folgt, der den Bund auffordert, Bildungseinrichtungen aus dem Anwendungsbereich des nationalen Umsetzungsgesetzes auszunehmen.

Dementsprechend kann davon ausgegangen werden, dass Hochschulen wohl nicht vom Anwendungsbereich der NIS-2-RL umfasst sind.

Universitätskliniken hingegen fallen in den Anwendungsbereich der NIS-2-RL. Sie sind im Anhang I Sektor 5 Gesundheitswesen aufgeführt. Dieser nennt als Art der Einrichtung Gesundheitsdienstleister im Sinne des Art. 3 lit. g der RL 2011/24/EU des Europäischen Parlaments und des Rates. Dieser wiederum definiert als „Gesundheitsdienstleister“ jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt.

V. Fazit

Die NIS-2-RL entwickelt das IT-Sicherheitsniveau in der Europäischen Union weiter und erhöht die Mindestanforderungen für die IT-Sicherheit. Auch wenn Unternehmen oder Einrichtungen nicht von der NIS-2-RL umfasst sind, ist es empfehlenswert, sich mit der IT-Sicherheit zu befassen und in sie zu investieren. Eine Möglichkeit, wie dies geschehen kann, zeigt der Entwurf des Landes Nordrhein-Westfalen für ein Hochschulstärkungsgesetz: Nach § 8b Hochschulgesetz-NRW-E haben Hochschulen einen Chief Information Officer (CIO) und einen Chief Information Security Officer (CISO) zu bestellen.[13] Diese haben ihre Ämter hauptamtlich zu führen, die IT-Strategie der Hochschule fortzuentwickeln und Regelungen zur Informationssicherheit zu erlassen. Dazu werden ihnen über den Landeshaushalt entsprechende Mittel bereitgestellt. Sie haben schließlich über eine angemessene Qualifikation und Berufserfahrung zu verfügen. ◆

11 Schmidt, RDi 2024, 550, 550 f.
12 Schmidt, RDi 2024, 550 (556).
13 Entwurf eines Gesetzes betreffend die Stärkung der Hochschullandschaft (Hochschulstärkungsgesetz), Vorlage 18/3086, abrufbar unter https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV18-3086.pdf, zuletzt abgerufen am 28.02.2025.

Ein paar Gedanken zum Abschied

Mehr als 20 Jahre Verantwortung in der Geschäftsführung des DFN-Vereins, rund 30 Jahre nachhaltiges Engagement für Forschung und Lehre in Deutschland – und nicht zuletzt herausragende Verdienste um den Aufbau und die Entwicklung des Wissenschaftsnetzes und seiner Services. Mit dieser beachtlichen Bilanz geht Jochem Pattloch Ende des Jahres in den Ruhestand. In seinen persönlichen Gedanken zum Abschied benennt er Bausteine, die aus seiner Sicht das Fundament für die Erfolgsgeschichte des DFN-Vereins bilden.

Jochem Pattloch: 1989 Diplom der Physik an der Freien Universität Berlin | 1990 bis 1996 Lufthansa Systems | 1996 bis 2004 wissenschaftlicher Mitarbeiter im DFN-Verein | 2004 bis 2025 Geschäftsführer im DFN-Verein | *Foto: Christoph Schieder*

Es war ermunternd, im vergangenen Jahr die verschiedenen Stimmen zum 40-jährigen Jubiläum zu hören, die dem DFN-Verein jeweils aus ihren Blickwinkeln eine erfolgreiche Geschichte attestierten. Mit meinem Blickwinkel von innen auf die Organisation habe ich mich gefragt, ob ich dem noch etwas hinzufügen sollte. Sicherlich nicht wertend, denn das steht mir nicht zu. Stattdessen will ich mich an einer kleinen Analyse versuchen: Gibt es Bausteine in der Architektur des DFN-Vereins, von denen ich denke, dass sie für den genannten Erfolg besonders wichtig waren? Einige seien hier genannt, ohne Anspruch auf Vollständigkeit. Es ist meine persönliche Sicht.

Fertigungstiefe und Funktionsherrschaft

Diese beiden Bausteine wurden in der Phase geformt, als der DFN-Verein in den Jahren 2004 bis 2006 den Schritt von

einem geförderten Projekt zu einer nachhaltig finanzierten Organisation machte. Das damalige Netz G-WiN stand bei den teilnehmenden Einrichtungen zu Recht in der Kritik und es fehlten angesichts der beendeten Förderung seitens des Bundes circa 15 Prozent der Mittel. Oha, das klingt nach Disruption. War es auch. Die Antwort seinerzeit war, die Fertigungstiefe beim Netz soweit auszubauen, dass es kostengünstiger und leistungsfähiger wurde und darüber hinaus eine erweiterte Funktionsherrschaft entstand, die dem DFN-Verein eine selbstbestimmte Weiterentwicklung erlaubte.

Das Prinzip ist bis heute handlungsleitend: Wir streben stets eine Fertigungstiefe an, die sowohl eine gute Funktionsherrschaft als auch eine günstige Kostenstruktur bietet. Für das Netz und die verschiedenen Dienste entstehen so jeweils passgenaue Antworten, die über die Jahre regelmäßig auf den Prüfstand gestellt werden.

Bedarfsgerecht und nachvollziehbar

Funktionsherrschaft ist notwendig, aber nicht hinreichend. Denn woher kommen das Wissen und der Wille, um diese klug einzusetzen? Die Gründungsgeneration des DFN-Vereins hatte das offenbar klar im Blick. Sie gestaltete eine einfache und auch deswegen sehr wirksame Governance. Im Mittelpunkt steht, dass die teilnehmenden Einrichtungen sich als Vereinsmitglieder unmittelbar an der fortlaufenden Diskussion zu den Anforderungen an Netz und Dienste beteiligen können. Ergänzt wird dies durch den Sachverstand in den Ausschüssen des Vorstands, in die auch Sichtweisen von außerhalb des DFN-Vereins eingebunden werden. So entsteht fortlaufend ein gemeinsam getragener Wille, wie sich Netz und Dienste weiterentwickeln sollen.

Akzeptanz und Vertrauen

Eine breit angelegte Willensbildung mag gelegentlich anstrengend sein, aber ein gemeinsam verabredetes Vorgehen darf anschließend mit einer hohen Akzeptanz rechnen. Daraus resultiert ein starkes Mandat, das es enorm erleichtert, die von den Vereinsorganen benannten Aufgaben umzusetzen. Als ein Beispiel sei die Gestaltung der aktuellen Kostenumlage zur Finanzierung der DFN-Dienste genannt. So hatten sich die Vereinsmitglieder im ersten Schritt zunächst auf Prinzipien geeinigt und anschließend eine Kostenumlage geformt und beschlossen, die diesen Prinzipien so gut wie möglich entspricht. Die dadurch entstandene Akzeptanz hat bei der nachfolgenden Umsetzung sehr geholfen.

Die im DFN-Verein gelebte Willensbildung trägt zudem sehr zu einem Asset bei, das ich für besonders wichtig halte: Vertrauen in die verantwortlichen Personen im Verein, die Funktionen oder Mandate tragen. Auch ich meine es über die Jahre zunehmend verspürt zu haben und bin sehr dankbar dafür. Gepaart mit dem konstruktiv kritischen Blick aus den Vereinsorganen und Ausschüssen habe ich das als einen wuchtigen Antrieb wahrgenommen, der den DFN-Verein im besten Sinne vorangebracht hat.

Zuversichtliches Selbstverständnis

Der DFN-Verein hat in seiner nunmehr 41-jährigen Geschichte nach meiner Wahrnehmung zunehmend mehr positive Erlebnisse von Selbstwirksamkeit gehabt. Der Übergang vom G-WiN zum X-WiN im Jahr 2006 ist sicherlich ein solcher Moment gewesen, viele ähnliche Erlebnisse sind danach gefolgt. Daraus ist im DFN-Verein ein Selbstverständnis erwachsen, das auf der Zuversicht aufbaut, den wandelnden Herausforderungen gewachsen zu sein. Gerade als eine Organisation, die sich mit ihren Leistungen behaupten muss und nicht auf eine schützende Hand vertrauen darf, ist ein zuversichtliches Selbstverständnis jenseits aller Selbstgefälligkeit ein wichtiges Signal – nach innen und auch an das Umfeld.

Vieles mehr

Vieles mehr könnte zu Recht den Anspruch erheben, hier erwähnt zu werden: Die Einbindung in das nationale und internationale Umfeld, die Beteiligung an innovativen Projekten, die besondere Motivation der Mitarbeitenden der Geschäftsstelle, der gewichtige Beitrag durch unser DFN-CERT, die Kompetenz, die aus den teilnehmenden Einrichtungen auf vielen Ebenen in den DFN-Verein getragen wird, die Kultur eines freundlichen und gelegentlich gar herzlichen Umgangs – das alles darf nicht unerwähnt bleiben. Ein tieferes Beleuchten würde den Rahmen dieses kleinen Abschieds jedoch sprengen.

Danksagung und Abschied

Alles Gute, lieber DFN-Verein. Danke an alle, die den DFN-Verein in meiner Zeit als Geschäftsführer im obigen Sinne geprägt und gelebt haben.

Ich wünsche mir, dass auch die kommenden Jahre und Jahrzehnte eine Erfolgsgeschichte bleiben werden – und bin sehr zuversichtlich, dass das gelingen kann.

Ihr Jochem Pattloch

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 Referentin für Kommunikation in der DFN-Geschäftsstelle ist die Zusammenarbeit mit internationalen Kolleginnen und Kollegen für Maimona Id ein wichtiger Aspekt ihrer Arbeit …

… Ein Highlight war darum das Frühjahrstreffen der Special Interest Group Marketing Communications (SIG-Marcomms), das am 18. und 19. Februar 2025 in Dublin stattfand.

Großartige Gespräche, inspirierende Sessions und viele tolle Ideen für die eigene Kommunikationsarbeit – das Frühjahrstreffen der SIG-Marcomms beim irischen Forschungsnetz HEAnet in Dublin hatte so einiges zu bieten. Insgesamt 17 Kommunikations- und Marketingprofis von NRENs weltweit waren vor Ort, um sich über aktuelle Trends, Strategien und gemeinsame Herausforderungen auszutauschen.

Der erste Tag startete mit einem fantastischen Blick auf die Liffey und die Skyline der Docklands – ein urbaner Mix aus moderner Architektur und alten Hafengebäuden. Auf dem Hafengelände direkt am Fluss hat HEAnet vor Kurzem neue Büroräume bezogen. Zum Auftakt des Meetings begrüßten uns auf das herzlichste Ronan Byrne, der CEO von HEAnet, sowie Barbara Carroll und Sharon Moylan, zuständig für PR und Marketing bei HEAnet. Gleich zu Beginn überreichte Lonneke Walk (SURF), die die SIG-Marcomms über beeindruckende neun Jahre geleitet hat, den Staffelstab an Barbara Carroll.

Blick auf die Liffey und die Docklands in Dublin – toller Rahmen für zwei Tage intensiven Austauschs: Das Frühjahrstreffen der SIG-Marcomms versammelte Kommunikationsprofis aus aller Welt | *Fotos: HEAnet*

In Session 1 ging es um das spannende Thema Employer Branding. Diskutiert wurde, wie NRENs als attraktive Arbeitgeber sichtbarer werden können. Wertvolle Einblicke in die Rekrutierungskampagnen ihrer Organisationen lieferten Salomé Branco

Zwischen Pints und Pfeifen: Das Social Event führte in den stimmungsvollen Pub The Church – mit Livemusik, echter Orgel und jeder Menge Gesprächsstoff | *Foto: HEAnet*

vom portugiesischen NREN FCCN und Grace Cooper von GÉANT. Besonders hilfreich: Tipps zur Zusammenarbeit mit HR-Abteilungen und Erfahrungsberichte.

In der zweiten Session, die Laetitia Lagneau (Belnet) moderierte, stand die Kommunikation rund um Meilensteine im Fokus. Hier zeigten Damian Niemir (PSNC), Olga Popcova (RENAM) und Åshild Berg-Tesdal (Sikt), wie sie Jubiläen, Führungswechsel und andere wichtige Ereignisse kommunikativ begleitet haben. Ich hatte die Ehre, die Veranstaltung zum 40-jährigen Jubiläum des DFN-Vereins vorzustellen. Der Vortrag zum Programm, der Location und den Highlights der Feier in Berlin kam gut an – insbesondere unsere Give-aways, Untersetzer in Form von alten Disketten, auf denen Klassiker der 80er-Jahre wie Pac-Man, Ghostbusters oder Commodore 64, aber auch die DFN-Netze ERWiN oder X.25-WiN verzeichnet waren.

Ein Highlight war definitiv auch der interaktive Brand Workshop mit Owen Barry von der Agentur Create. In verschiedenen Übungen hinterfragten wir unsere Markenidentität, schärften Mission und Vision und diskutierten, wie Werte nach innen und außen erlebbar werden.

Am zweiten Tag lud Silvia Fiore (GÉANT), die Mitorganisatorin des Meetings, zur Session Learning Circles ein. In kleinen Gruppen tauschten wir uns zu Themen wie der Kommunikationsplanung 2025 und dem Verhältnis von Paid vs. Organic Campaigns aus. Besonders wertvoll war hier der offene Erfahrungsaustausch zu Tools, Budgets und Erfolgsmessung.

Zum Abschluss rief Elis Bertazzon (GARR) zur Session „Raise Your Challenge“ auf – eine Art kommunikativer Kummerkasten mit Lösungsansätzen. Hier ging es um ganz konkrete Projekte: etwa die OCRE-2024-Kommunikation oder die Weiterentwicklung des Tools FileSender.

Was bleibt? Zwei intensive Tage mit großartigen Menschen, viel Expertise, ehrlichem Austausch, gegenseitiger Wertschätzung und einem klaren Ziel: unsere Kommunikation gemeinsam weiterzuentwickeln – kreativ und vor allem vernetzt. ◆

Kurzmeldungen DFN-Verein

Tapetenwechsel: Die Geschäftsstelle am Standort Stuttgart ist umgezogen

Nach über zwei Jahrzehnten hat unsere Geschäftsstelle am Standort Stuttgart neue Räumlichkeiten bezogen. Seit 1998 war sie an der bisherigen Adresse in der Lindenspürstraße zu Hause – nun hieß es: Kisten packen, Kabel sortieren, Technik ab- und wieder aufbauen. Der Umzug war alles andere als simpel, denn zentraler Bestandteil des Standorts ist auch unser Network Operations Center (NOC), das Herzstück der technischen Betriebsführung im Wissenschaftsnetz.

Dank des großartigen Einsatzes unserer Kolleginnen und Kollegen vor Ort und am Standort Berlin ist der komplexe Ortswechsel nach Monaten der Planung und Vorbereitung reibungslos gelungen. Mit viel Engagement, organisatorischem Geschick und technischem Know-how haben sie den Umzug gestemmt – und damit den Grundstein für einen erfolgreichen Start am neuen Standort gelegt. Wir freuen uns über schöne Räume, eine moderne Infrastruktur und darauf, von hier aus weiterhin mit vollem Einsatz für den DFN-Verein zu wirken.

Die neue Adresse:
DFN-Verein e. V.
Schloßstraße 70
70176 Stuttgart
Telefon: 0711 633 14-0

Geschafft! Nach Monaten der harten Arbeit freuen sich Janette Hofer und das ganze Team über die neuen Räume | *Fotos: Andrea Wardzichowski, Robert Stoy/DFN*

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.

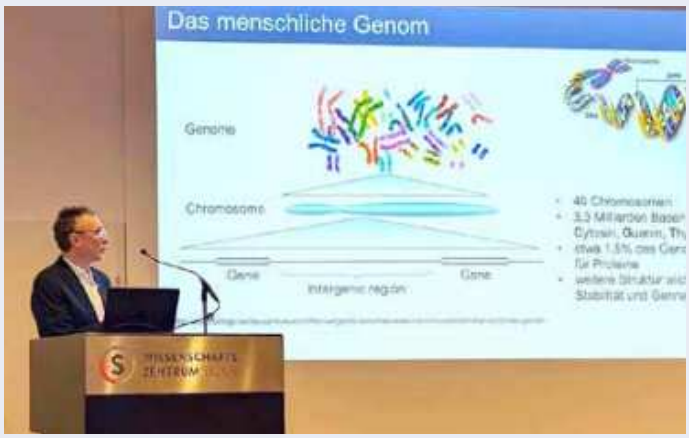
89. DFN-Mitgliederversammlung

Es brummt im Deutschen Forschungsnetz – davon konnten sich die Mitgliedsvertreterinnen und -vertreter überzeugen, die sich am Mittwoch, 4. Dezember 2024, zur 89. DFN-Mitgliederversammlung (MV) im Wissenschaftszentrum Bonn einfanden. Zweimal im Jahr treffen sich die Delegierten der mehr als 350 DFN-Mitgliedseinrichtungen aus Forschung und Lehre, um gemeinsam die Zukunft des DFN-Vereins zu gestalten.

Zum Vorsitzenden der 89. Mitgliederversammlung wurde Dr. Rainer Bockholt, der Direktor des Hochschulrechenzentrums der Rheinischen Friedrich-Wilhelms-Universität Bonn, gewählt. Er folgt auf Prof. Dr. Gerhard Peter. Der ehemalige Rektor der Hochschule Heilbronn leitete die Mitgliederversammlung 20 Jahre lang.

Auf der Tagesordnung standen neben den Berichten über die Aktivitäten des DFN-Vereins im ersten Halbjahr 2024 verschiedene Vorträge zum Stand des Wissenschaftsnetzes, zum Dienst DFN-Security und zu weiteren aktuellen Themen – darunter Erfolgsnachrichten, aber auch Herausforderungen, die den Verein momentan beschäftigen.

Ein Highlight der Vorabendveranstaltung am Dienstag, 3. Dezember 2024, war der Vortrag „High-Performance Computing in der Krebsgenomforschung“ von Prof. Dr. Martin Peifer. Der Wissenschaftler forscht mit seiner Arbeitsgruppe an der Universität zu Köln im Bereich „Computational Cancer Genomics“ und entwickelt computergestützte Methoden zur Analyse groß angelegter Krebsgenom-Sequenzierungsdaten. Ein Schwerpunkt ist der seltene Tumor Neuroblastom, der insbesondere bei Kindern vorkommt. Mit der Risikoklassifizierung des Tumors konnte Martin Peifer dazu beitragen, dass schwere Chemotherapien bei Kindern mit dieser Erkrankung weitaus gezielter und damit schonender eingesetzt werden können.



Mit seiner Forschung trägt Prof. Dr. Martin Peifer dazu bei, dass Chemotherapien gezielter eingesetzt werden können | *Fotos: Maimona Id/DFN*

TERMIN

Die 90. Mitgliederversammlung findet am **Dienstag, 3. Juni 2025**, in Berlin statt.

In Aktion: Im BT-Plenum geben DFN-Kolleginnen und -Kollegen einen Überblick zu den aktuellen Themen im Forschungsnetz (v. li.: Ralf Paffrath und Michael Röder vom DFN-Verein) | *Foto: Jürgen ALOIsius Morgenroth*

TERMIN

Die 83. DFN-Betriebstagung findet am **Dienstag und Mittwoch, 7. und 8. Oktober 2025,** statt.

82. DFN-Betriebstagung

Austausch und gemeinsames Gestalten der digitalen Zukunft in Forschung und Lehre – das stand bei der 82. DFN-Betriebstagung, die am 25. und 26. März 2025 in Berlin stattfand, im Mittelpunkt. Zwei Tage lang diskutierten rund 320 Teilnehmende in neun Foren über die aktuellen Herausforderungen und Innovationen rund um Kommunikationsinfrastrukturen, IT-Sicherheit und kollaborative Dienste im Wissenschaftsbereich. Zusätzlich verfolgten etwa 140 Teilnehmende das Plenum im Livestream.

Zu den Highlights gehörte die Siegerehrung der DFN-Security-Challenge. Der Wettbewerb, der im November 2024 startete, sollte den Einsatz von IT-Sicherheitsmaßnahmen im Rahmen des Dienstes DFN-Security spielerisch fördern und so das Bewusstsein in den teilnehmenden Einrichtungen schärfen (siehe Artikel S. 28).

Auch der zweite Tag bot in den Foren Wissenschaftsnetz, Multimedia, Mobile IT, VoIP und Cloud jede Menge hochaktuelle Themen: u. a. „Barrierefreiheit und Inklusion in der Medientechnik“, „OCRE & Co. – Neues aus der DFN-Cloud“ oder „Flexible Skalierung und Segmentierung mittels eduVPN/OpenVPN“.

27. Workshop Videokonferenzen im Wissenschaftsnetz

Am Dienstag und Mittwoch, 10. und 11. Dezember 2024, veranstaltete das Kompetenzzentrum für Videokonferenzdienste (VCC) den 27. Workshop Videokonferenzen im Wissenschaftsnetz in Dresden. Einen ausführlichen Bericht zu den aktuellen Themen rund um den Dienst DFN-Conf, Neuigkeiten zu den Rahmenverträgen für cloudbasierte Videokonferenzdienste sowie zu den Vorbereitungen eines Vergabeverfahrens für Folgeverträge hielt Christian Meyer vom DFN-Verein.

Weitere Programmhighlights waren ein geschichtlicher Abriss über 100 Jahre Lautsprechertechnologien von Matthias Heß (MR Datentechnik) und Oliver Merz (Fohhn), ein Bericht über den Neubau von Videostudios im Gebäude InformatiKOM am Karlsruher Institut für Technologie (KIT) von Andreas Reichert sowie ein Vortrag zum Einsatz einfacher Hilfsmittel für die Aufzeichnung und Übertragung von Vorlesungen und Seminaren von Mathias Magdowski (Otto-von-Guericke-Universität Magdeburg). Spannend war auch der Vortrag von Julian Kropp (Hochschule Darmstadt), der in seiner Bachelorarbeit einen prototypischen Live-Übersetzungs- und Untertitelungs-Bot auf Grundlage von ChatGPT und BigBlueButton entwickelt hat (siehe Artikel S. 44).

Der VCC-Workshop findet jedes Jahr im Klemperer-Saal der Sächsischen Landesbibliothek – Staats- und Universitätsbibliothek Dresden (SLUB) statt | *Foto: Dirk Bei der Kellen/DFN*

TERMIN

Der 28. Workshop Videokonferenzen im Wissenschaftsnetz findet am **Dienstag und Mittwoch, 4. und 5. November 2025,** statt.

11. DFN-Konferenz „Datenschutz“

Die 11. DFN-Konferenz „Datenschutz“ fand am 26. und 27. November 2024 im Hotel Hafen Hamburg an den Landungsbrücken statt. Die Konferenz thematisierte das komplexe Verhältnis von Datenschutz und Künstlicher Intelligenz. In sechs Vorträgen berichteten verschiedene Persönlichkeiten aus Wirtschaft, Wissenschaft und Verwaltung von technischen Neuerungen sowie Chancen und Herausforderungen beim Einsatz von KI mit Bezug zum Datenschutz.

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

Schwerpunkt KI: Bei der 11. DFN-Konferenz „Datenschutz“ wurde der Einsatz von Künstlicher Intelligenz vor dem Hintergrund Datenschutz diskutiert | *Foto: DFN-CERT*

TERMIN

Die 12. DFN-Konferenz „Datenschutz“ findet am **Dienstag und Mittwoch, 9. und 10. Dezember 2025,** statt.

Cybersicherheit im Blick: Bei der 32. DFN-Konferenz „Sicherheit in vernetzten Systemen“ war auch KI ein wichtiges Thema | *Foto: Nina Bark/DFN*

TERMIN

Die 33. DFN-Konferenz „Sicherheit in vernetzten Systemen“ findet am **Dienstag und Mittwoch, 27. und 28. Januar 2026,** statt.

32. DFN-Konferenz „Sicherheit in vernetzten Systemen“

Die 32. DFN-Konferenz „Sicherheit in vernetzten Systemen“ fand am Dienstag und Mittwoch, 11. und 12. Februar 2025, im Grand Elysée Hotel Hamburg statt und wurde vom DFN-CERT im Auftrag des DFN-Vereins veranstaltet. Das Programmkomitee hatte ein hochkarätiges Programm aus Themen rund um Informationssicherheit auf die Beine gestellt – von der quantenresistenten PKI bis zur Resilienz durch Diversität. Die Keynote „Gekommen, um zu bleiben: Cyberangriffe durch KI und die Vorbereitung darauf“ hielt Prof. Dr. Maria Leitner von der Universität Regensburg.

Mit ihrer explizit technischen und wissenschaftlichen Ausrichtung sowie einer großen Vielfalt an Beiträgen und Diskussionen hat sich die DFN-Konferenz als eine der größten deutschen Tagungen für Informationssicherheit etabliert.

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

Überblick DFN-Verein

(Stand: 06/2025)

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.
Schloßstraße 70
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 Dr. Rainer Bockholt, Universität Bonn.

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:
Dr. Rainer Bockholt
(Universität Bonn)

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
	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
	Niedersächsische Landesmuseen Braunschweig
	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
	Medizinische Universität Lausitz – Carl Thiem

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
	Helmholtz-Zentrum für Ozeanforschung Kiel (GEOMAR)
	IPN Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik
	Kiel Institut für Weltwirtschaft
	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.
	Technische 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
	Filmuniversität Babelsberg KONRAD WOLF
	GFZ Helmholtz-Zentrum für Geoforschung
	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

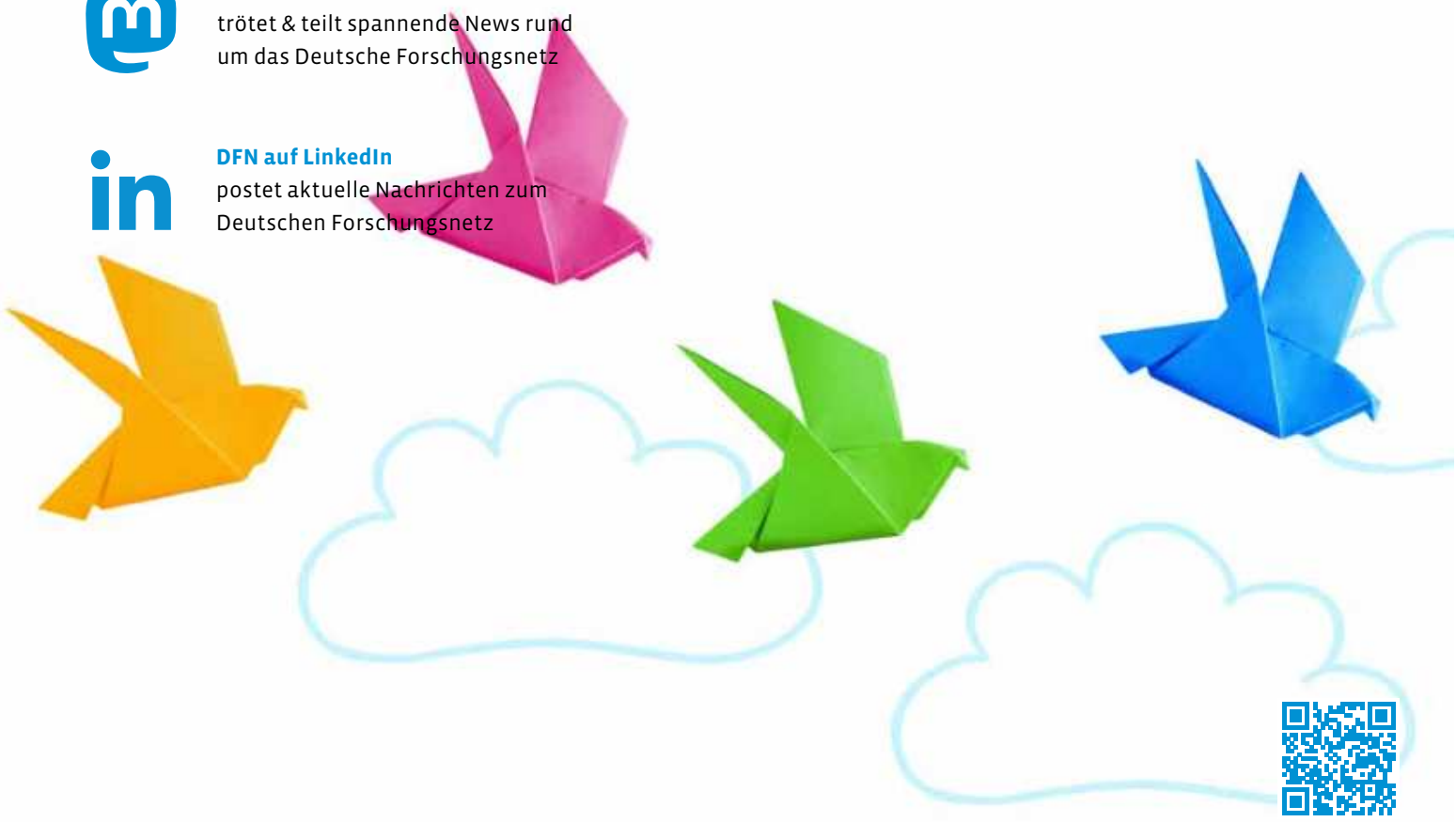
DFN-Infobrief Recht
informiert über aktuelle Entwicklungen und Fragen des Medien- und Informationsrechts

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/