DFN mitteilungen

Harte Nuss?

Herausforderung Security Awareness

Willkommen Alina Hain!

Die neue DFN-Geschäftsführerin im Interview

Digitale Barrierefreiheit praxisnah

Das SHUFFLE-Reifegradmodell

9 770177 689001

Nachruf

Der Verein zur Förderung eines Deutschen Forschungsnetzes e. V. trauert um seinen langjährigen Vorsitzenden der Mitgliederversammlung.

Wir gedenken
Professor Gerhard Peter,
der am 13. Mai 2025 im Alter
von 77 Jahren verstarb.

Lieber Gerhard, als eine treibende Kraft und als langjähriger Vorsitzender der Mitgliederversammlung des DFN-Vereins hast Du Dich herausragend um das Deutsche Forschungsnetz verdient gemacht.

Du hast mit einem außerordentlichen Geschick unsere Mitgliederversammlungen ab dem Sommer 2004 für 20 Jahre geleitet. Dir war es maßgeblich zu verdanken, dass auch kontroverse Diskussionen stets konstruktiv verliefen und letztendlich immer zu sehr guten und gemeinsam getragenen Ergebnissen führten.
Das daraus resultierende starke Mandat der Mitgliederversammlung war eine wesentliche Grundlage für den großen Erfolg des DFN-Vereins in diesen zwei Jahrzehnten.

Auch darüber hinaus warst Du ein Motor für die gemeinsame Weiterentwicklung des DFN-Vereins. So hat Dein Engagement für die DFN-Nutzergruppe Hochschulverwaltung dafür gesorgt, dass die Themen rund um das Deutsche Forschungsnetz eine größere Sichtbarkeit bekamen und uns vielfach wertvolles Feedback bescherten.

Lieber Gerhard, herzlichen Dank für alles – Du wirst uns fehlen, als Mitstreiter, als kluger Kopf, als ausgleichender Vermittler und vor allem als Mensch.

Unser tief empfundenes Mitgefühl gilt Deiner Familie, Deinen Freunden und Wegbegleitern.

Professor Stefan Wesner
im Namen der Mitglieder des DFN-Vereins und der Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle

Foto: Jürgen Aloisius Morgenroth

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: ueuaphoto / Adobe Stock
Rückseite: tsekhmister / Freepik, studyoritim / iStock

Kerstin Bein
Leiterin der Universitäts-IT (UNIT)
Mannheim, Mitglied im
Verwaltungsrat des DFN-Vereins

Wissenschaftliche Erkenntnis lebt vom gemeinsamen Austausch, vielfältigem Dialog und von Kooperation, die diese zusammenführt und erst möglich macht. In Forschung und Lehre zählen Offenheit und kreative Freiheit seit jeher zu den zentralen Werten. Diese Werte haben sich in einer zunehmend digitalen Forschungsumgebung weiterentwickelt und werden heute von hochkomplexen IT-Infrastrukturen und Services unterstützt, die jeden Tag unzählige Prozesse steuern und riesige Mengen an Forschungsdaten bewegen. Doch gerade dort, wo Wissen geteilt und Zusammenarbeit gefördert werden, entstehen auch Angriffsflächen und damit gerät Offenheit leicht zum Einfallstor für Cyberangriffe.

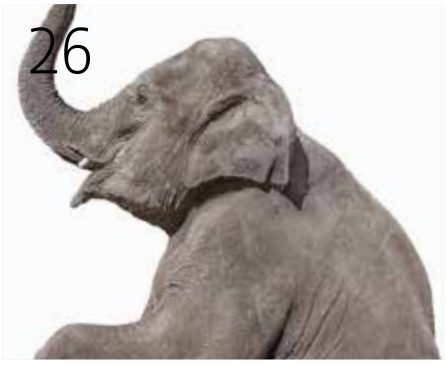
An der Universität Mannheim fördern wir im Rahmen der Informationssicherheit und mit unseren IT-Projekten auf unterschiedlichen Ebenen den Schutz von Daten und den sicheren Umgang mit Informationen, wie beispielsweise der eigenen elektronischen Identität. Neben der Entwicklung effektiver Prozesse für das Vorfalls- und Schwachstellenmanagement ist die Security-Awareness-Kampagne zentraler Bestandteil unserer Informationssicherheit. Denn diese baut nicht allein auf technischen Maßnahmen auf, sondern sie steht und fällt mit den Menschen, die an unserer Einrichtung arbeiten, forschen, lernen und lehren.

Security-Awareness ist darum weitaus mehr als Phishing-Mails zu erkennen und Passwörter zu schützen. Ihr Anliegen ist es, Risiken frühzeitig zu erkennen, reflektiert zu handeln und so deutlich mehr Sicherheit in den Arbeitsalltag zu integrieren – ohne die wissenschaftliche Freiheit einzuschränken. Am Ende geht es um nicht weniger, als ein nachhaltiges Bewusstsein für Informationssicherheit zu schaffen und Verantwortung im digitalen wie analogen Raum gewissenhaft zu übernehmen. Angesichts neuer Herausforderungen, insbesondere im Bereich von Cloud-Diensten und KI-Systemen, gilt es, unsere Sicherheitsanforderungen konsequent weiterzuentwickeln, um auch hier unserer Verantwortung gerecht zu werden. Wenn uns das gelingt, schaffen wir eine vertrauensvolle Kultur, in der Sicherheit selbstverständlich wird – und Forschung und Lehre sich frei und sicher entfalten können.

Ihre Kerstin Bein

Inhalt

Firewall Mensch
Prof. Dr.-Ing. Sebastian Schinzel spricht über Cybervorfälle & Security Awareness



Auf dem Weg ins Fediverse
Das KIT baut eine eigene Mastodon-Instanz auf

Clever Sparen
Stromkauf mit Machine Learning

Sicherheit

Wissenschaftsnetzt

Campus

International

Forschung

Die Kunst des steten Wandels
Die neue DFN-Geschäftsführerin Alina Hain im Interview

Recht

DFN-Verein

Autorinnen und Autoren dieser Ausgabe im Überblick

1 Maimona Id, DFN-Verein (id@dfn.de); **2** Mirko Giese, DFN-Verein (giese@dfn.de); **3** Lukas Härter, Philipps-Universität Marburg (lukas.haerter@uni-marburg.de); **4** Long Yang Paffrath, DFN-Verein (lypaffrath@dfn.de); **o. Abb.** Christine Kahl, DFN-CERT (kahl@dfn.de); **5** Dr. Dirk Bei der Kellen, DFN-Verein (beiderkellen@dfn.de); **6** Jan Kröger, Karlsruher Institut für Technologie (jan.kroeger@kit.edu); **7** David Lohner, Karlsruher Institut für Technologie (david.lohner@partner.kit.edu); **8** Ulrich Weiß, Karlsruher Institut für Technologie (uli.weiss@kit.edu); **9** Max Scheid, Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (mscheid@gwdg.de); **o. Abb.** Nadine Auer, Hochschule der Medien, Stuttgart (auer@hdm-stuttgart.de); **o. Abb.** Prof. Dr. Gottfried Zimmermann, Hochschule der Medien, Stuttgart (zimmermanng@hdm-stuttgart.de); **o. Abb.** Ann-Katrin Böhm, Pädagogische Hochschulen Heidelberg und Freiburg (boehm3@ph-heidelberg.de); **o. Abb.** Hakan Ali Cetin, Pädagogische Hochschule Freiburg (hakan.cetin@ph-freiburg.de); **o. Abb.** Dr. Anja Gutjahr, Pädagogische Hochschule Heidelberg (gutjahr@ph-heidelberg.de); **10** Michael Eichelbeck, Technische Universität München (michael.eichelbeck@tum.de); **o. Abb.** Prof. Dr. Helmut Reiser, Leibniz-Rechenzentrum, Ludwig-Maximilians-Universität München (helmut.reiser@lrz.dee); **o. Abb.** Dr. Jürgen Seidl, Leibniz-Rechenzentrum (Juergen.Seidl@lrz.de); **o. Abb.** Fatjon Tushe, Leibniz-Rechenzentrum, Ludwig-Maximilians-Universität München (tushe.fatjon@campus.lmu.de); **o. Abb.** Prof. Dr. rer. nat. Frank Kargl, Universität Ulm (frank.kargl@uni-ulm.de); **o. Abb.** Prof. Dr. Michael Menth, Eberhard Karls Universität Tübingen (menth@uni-tuebingen.de); **11** Prof. Dr. rer. nat. Oliver P. Waldhorst, Hochschule Karlsruhe (auer@hdm-stuttgart.de); **o. Abb.** Prof. Dr. Steffen Wendzel, Universität Ulm (steffen.wendzel@uni-ulm.de); **o. Abb.** Prof. Dr. Martina Zitterbart, Karlsruher Institut für Technologie, KIT (zitterbart@kit.edu); **12** Maja Vreca, Arnes (maja.vreca@arnes.si); **13** Christopher Williams, High-Performance Computing Center Stuttgart, HLRS (hpccwill@hlrs.de); **14** Eric Gedenk, DFN-Verein (info@impact-scicomm.com); **15** Johannes Müller-Westphal, Forschungsstelle Recht im DFN (johannes.mueller@uni-muenster.de); **16** Anna Maria Yang-Jacobi, Forschungsstelle Recht im DFN (a.yang-jacobi@fu-berlin.de); **o. Abb.** Dr.-Ing. Inga Scheler, Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau (scheler@rptu.de)

Firewall Mensch

Foto: Wilfried Gerharz

Seit 2013 engagiert sich Prof. Dr.-Ing. Sebastian Schinzel an der FH Münster für IT-Sicherheit, seit 2023 zusätzlich am Fraunhofer-Institut für Sichere Informationstechnologie SIT. Welche zentrale Rolle der Mensch bei einem Cyberangriff spielt und warum Awareness-Maßnahmen manchmal überschätzt werden, erzählt der Forscher im Interview.

Seit Ihrem Studium beschäftigen Sie sich durchgehend mit IT-Sicherheit. Worst-Case-Szenarien gehören zu Ihrer täglichen Arbeit. Sind Sie ein Pessimist?
Nein, das bin ich nicht. Aber es belastet mich auch nicht, negative Gedanken zuzulassen. Es ist einfach Teil meiner DNA, Risiken abzuschätzen und mir vor Augen zu führen, was alles schiefgehen kann. Ich habe Informatik studiert und habe daher einen eher technischen Hintergrund. Aber mit zunehmender Erfahrung kam die Erkenntnis, dass IT-Sicherheit kein rein technisches Problem ist, sondern ein soziotechnisches.

Ich habe mich jahrelang akademisch mit dem Thema IT-Sicherheit beschäftigt, zig Vorlesungen dazu gehalten – und dann erlebt man in einer Krisensituation, die die eigene Einrichtung betrifft, hautnah, wie Menschen sich verhalten, welche Fehler passieren und wie sie dann wiederum auf Fehler reagieren. Das war neu für mich und hat mir die Augen geöffnet, wie zentral der Faktor Mensch bei einem Cybervorfall ist.

Was macht ein Cybervorfall mit den Menschen?
Ein Cyberangriff ist eine enorme physische und psychische Belastung. Wir reden hier von Wochen und Monaten, in denen die Mitarbeitenden bei der Bewältigung des Angriffs und dem Neuaufbau der IT auf Anschlag laufen. Die eigentliche Arbeit bleibt liegen und muss nach erfolgtem Wiederaufbau nachgearbeitet werden, was nochmals Monate dauern kann. Manche Menschen reagieren in so einer traumatischen Situation emotional, suchen Schuldige. Das sind dann Diskussionen, die in Meetings eingefangen werden müssen, weil sie in einer akuten Krise einfach nicht weiterhelfen.

Seit dem Cyberangriff auf die FH Münster vor ein paar Jahren wurde ich einige Male zu Krisenstäben anderer gehackter Hochschulen hinzugezogen. Was ich erlebt habe, ist, dass die interne Kommunikation teils schiefläuft, dass der Cybervorfall alte Wunden aufreißt und bereits bestehende Konflikte offenlegt. Da werden zentrale Personalien infrage gestellt und teils neu

besetzt. Das sind Dinge, die bei uns glücklicherweise nicht passiert sind, weil wir ein besonnenes Präsidium haben, das es verstanden hat, die Menschen wieder einzufangen, auf ein Ziel einzuschwören und sie zu motivieren – damit möglichst alle an einem Strang ziehen.

Was uns, glaube ich, von anderen betroffenen Hochschulen unterscheidet, ist, dass wir von Anfang an sehr offen und transparent mit dem Vorfall umgegangen sind. In einem YouTube-Video haben wir unsere Lessons Learned veröffentlicht, damit andere Hochschulen, denen dasselbe passiert, aus unseren Erfahrungen lernen können.

Inwiefern spielt der Faktor Mensch eine entscheidende Rolle?
Viele Cyberangriffe starten mit Aktionen, die direkt auf den Menschen abzielen. Ein Beispiel ist CEO Fraud, auch „Whaling" genannt. Das ist eine Betrugsmasche, bei der sich Kriminelle als Führungskräfte ausgeben. Ihr Ziel ist es, Mitarbeitende – meist in der Buchhaltung oder Verwaltung – dazu zu bringen, hohe Geldbeträge zu überweisen oder vertrauliche Informationen preiszugeben. Das sind teils Schäden in Millionenhöhe. Dabei nutzen die Angreifer täuschend echt wirkende E-Mails, gefakte Telefonanrufe mit teils KI-generierten Stimmen oder gefälschte Identitäten, um Druck und Dringlichkeit zu erzeugen. Angreifer versuchen so, Vertrauen oder aber Stresssituationen auszunutzen.

Aber auch die heutzutage gängigen Cyberangriffe, bei denen Daten gestohlen, dann verschlüsselt und mit Veröffentlichung gedroht wird, sogenannte Ransomware, starten oft mit Phishing-E-Mails, über die die Angreifer einen ersten Fuß in das Organisationsnetz bekommen.

Ist es wirklich so banal? Der Mensch ist fehlbar und nachlässig in puncto IT-Sicherheit – und damit selbst Schuld an der Misere?
In Organisationen arbeiten ja ganz unterschiedliche Menschen, von denen die meisten keinen technischen IT-Hintergrund haben. IT ist ja auch kein Selbstzweck. Sie dient dazu, Arbeitsprozesse aus ganz unterschiedlichen Fachrichtungen zu unterstützen. Um solche Systeme erfolgreich betreiben zu können, brauche ich Menschen, die empathisch sind, die verstehen, dass wir IT-Systeme so aufbauen müssen, dass sie sicher von Menschen bedient werden können. Das ist eine große Herausforderung.

Wir müssen als ITler weg vom Victim Blaming und wieder mehr die Verantwortung übernehmen. Damit meine ich zu akzeptieren, dass Leute nun mal auf Links klicken, wenn sie per E-Mail zugestellt werden. Und es ist eben nicht einfach zu erkennen, ob ein Link Teil eines Cyberangriffs ist oder nicht. Wäre es einfach, könnten wir die „bösen" Links ja einfach automatisiert auf dem Mailserver herausfiltern.

Sicherheit funktioniert nur, wenn sie den Menschen mitdenkt. Der Forschungsansatz der Human-Centered Security beschäftigt sich genau damit: Er verbindet Aspekte aus IT-Sicherheit, Psychologie, Usability und Organisationsverhalten, um Sicherheitskonzepte so zu gestalten, dass sie mit dem Verhalten, den Fähigkeiten und den Bedürfnissen der Menschen harmonieren – statt sie zu überfordern oder zu umgehen.

Was lässt sich daraus für die Praxis ableiten?
Mithilfe von Benutzerstudien erhält man erst einmal ein direktes Feedback darauf, wie Menschen tatsächlich mit Sicherheitssystemen umgehen. Nehmen Sie zum Beispiel Security Awareness-Kampagnen, bei denen innerhalb einer Einrichtung simulierte Phishing-E-Mails an zwei Gruppen von Mitarbeitenden versendet werden. Eine Gruppe hatte bereits eine Awareness-Schulung, die andere nicht. Anschließend wird gemessen, welche Menschen auf die Phishing-E-Mails hereinfallen. Überraschung: Der Unterschied zwischen beiden Gruppen ist zwar messbar, aber insgesamt so gering, dass immer noch viele Menschen hereinfallen, trotz Schulung.

> „Sicherheit funktioniert nur, wenn sie den Menschen mitdenkt."

Die wissenschaftliche Evidenz zeigt, dass viele Security-Awareness-Maßnahmen unterm Strich nur einen sehr geringen Effekt haben. Das belegen verschiedene Studien. Trotzdem bekomme ich immer wieder mit, dass Awareness-Schulungen bei Verantwortlichen nach wie vor einen hohen Stellenwert haben. Nach dem Motto, ich bringe meinen Usern einfach bei, nicht mehr auf Phishing-Mails zu klicken, und dann ist alles fein – sozusagen als menschliche Firewall. Das ist aber ein Trugschluss, so funktionieren Menschen nicht.

Ich habe drei Kinder, ich kann Ihnen genau sagen, wie man sich fühlt, wenn man mehrere Nächte schlecht geschlafen hat, völlig unkonzentriert und gestresst ist. Wenn dann noch die richtige Masche kommt, man wartet auf ein wichtiges Paket und dann kommt die DHL-Phishing-Mail – da klickt man schnell mal, ohne nachzudenken. Da können Sie noch so geschult sein, das aktuelle Mindset überdeckt das.

Was schlagen Sie vor?
Ein Lösungsansatz kann sein, an der Fehlerkultur innerhalb einer Einrichtung zu arbeiten. Diese kann den Ausschlag geben, ob ein Cyberangriff erfolgreich ist oder bereits in einer frühen Phase erkannt und gestoppt werden kann. Es ist ja nicht so, dass User auf einen Link klicken, und zack ist alles verschlüsselt. Sondern da müssen noch viele Schritte erfolgreich geschehen,

Prof. Dr.-Ing. Sebastian Schinzel | 2005 Bachelor B. Sc. Informatik an der Hochschule Darmstadt mit Auslandssemester an der Reykjavik University in Island | 2005–2012 Senior Security Consultant bei der Virtual Forge GmbH | 2007 Master M.Sc. Informatik an der Hochschule Darmstadt mit Auslandssemester an der James Cook University in Australien | 2009–2012 wissenschaftlicher Mitarbeiter am Lehrstuhl für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg im DFG-Projekt „Reliably Secure Software Systems“ (SPP 1496) | 2012 Dr.-Ing. in Informatik an der Friedrich-Alexander-Universität Erlangen-Nürnberg | seit 2013 Professor für IT-Sicherheit an der FH Münster | seit 2023 Abteilungsleiter Fraunhofer-Institut für Sichere Informationstechnologie SIT

die Tage, Wochen und teilweise auch Monate dauern können, bis der eigentliche Angriff erfolgreich ist, große Teile der Daten gestohlen und verschlüsselt werden.

An der FH Münster haben wir neben einer präsenten Webseite der Stabsstelle Informationssicherheit ein Meldeformular und Kontaktadressen eingerichtet. Dort können sich Mitarbeitende melden, wenn sie die Befürchtung haben, dass sie auf Malware geklickt haben. Dann kümmern wir uns darum und – ganz wichtig – bedanken uns für deren Offenheit. Denn das ist keine Selbstverständlichkeit. Wenn wir mit Security-Awareness-Schulungen erreichen können, dass User reflektieren, wenn etwas schiefgelaufen ist und sich im Zweifel melden, dann haben wir gewonnen.

> „Da wurden Finger gehauen und Schienbeine getreten.“

Dann ergeben Cyber-Awareness-Schulungen also doch Sinn?
In gewisser Weise schon. Wir müssen den Leuten ja erklären, warum wir auf einmal Mehr-Faktor-Authentifizierungen einführen. IT-Sicherheitsmaßnahmen können nur kollaborativ funktionieren. Wenn wir in einer Organisation etwas vorgeben oder verbieten, was den Arbeitsalltag behindert, dann suchen sich die Leute unter Umständen einen anderen – vielleicht noch ungünstigeren – Weg. Wir müssen überzeugen und Mitsprache ermöglichen, damit Maßnahmen gelebt werden.

Also ist ein IT-Sicherheitsbeauftragter im Rahmen der Awareness-Maßnahmen so etwas wie ein Vermittler?
Das ist aus meiner Sicht das Hauptverständnis eines IT-Sicherheitsbeauftragten. Historisch gesehen haben sich viele IT-Sicherheitsbeauftragte in den vergangenen Jahrzehnten leider eher als Neinsager etabliert. Da wurden Finger gehauen und Schienbeine getreten. Aber es geht nicht darum, den Leuten Steine in den Weg zu legen, sondern ihnen dabei zu helfen, die IT-Sicherheitsziele zu erreichen.

Darum ist Kommunikation ein wichtiger Faktor. Die Sicherheitslücken, die Angreifer heute ausnutzen, sind oft seit Jahren bekannt und technisch längst gelöst. Die Herausforderung besteht eher darin, aktuelle Erkenntnisse in den Einrichtungen zu vermitteln. Die IT-Strukturen vieler Organisationen sind seit vielen Jahren organisch gewachsen und sehr komplex geworden. Genau diese komplexen und gewachsenen Systeme sind heute das Einfallstor für Angriffe. Sie zu modernisieren bedeutet tiefgreifende Veränderungen – nicht nur technisch, sondern vor allem organisatorisch auf Ebene von Arbeitsprozessen. Das tut manchmal weh – und sollte darum kommunikativ gut vermittelt werden.

Wie nachhaltig sind die Erfahrungen aus dem Cybervorfall heute? Hat sich das Mindset geändert?
Wenn man gezwungen wird, in kurzer Zeit IT-Systeme neu aufzubauen, hat man eine Chance, diese Systeme anders zu bauen. Das macht es leichter, Akzeptanz für durchaus einschneidende Maßnahmen wie zum Beispiel die Einführung von Mehr-Faktor-Authentifizierung zu erhalten. Natürlich sind auch solche Systeme nie perfekt und wir arbeiten weiter kontinuierlich an der Verbesserung der Systeme.

Heute haben wir mit der vor drei Jahren neu geschaffenen Stabsstelle Informationssicherheit ein starkes Team an der FH Münster und fühlen uns gemeinsam mit unserer Datenverarbeitungszentrale gut aufgestellt.

Das Gespräch führte Maimona Id (DFN-Verein).

Das YouTube-Video zum Cybervorfall an der FH Münster finden Sie unter:
https://www.youtube.com/watch?v=l_UzKlbLY-Q

Fehlerkultur als Schlüssel zur IT-Resilienz

Oft liegt der Fokus bei IT-Resilienz auf Technik – doch mindestens genauso wichtig sind die menschlichen und organisatorischen Faktoren. Studien zeigen: Der Großteil von Sicherheitsvorfällen geht auf menschliches Fehlverhalten zurück. Wer das Thema Resilienz ernst nimmt, muss beides im Blick haben, weiß Mirko Giese, der seine Erfahrungen aus früheren beruflichen Tätigkeiten teilt.

Text: **Mirko Giese** (DFN-Verein)

„Chef, ich habe Mist gebaut." Dieses unverhohlene Fehlereingeständnis eines Kollegen hat sich mir eingeprägt. Was zunächst nach einem ernsten Problem klang, war bei näherer Betrachtung ein Geschenk. Denn so wusste ich unmittelbar, worum es ging, konnte das Risiko einschätzen und die weitere Kommunikation zur Fehlerbehebung steuern. Noch wichtiger: Das ganze Team lernte aus dem Vorfall. Diese Erfahrung hat mir gezeigt, wie wertvoll eine offene Fehlerkultur ist – gerade in der IT.

Fehler als Chance

Wenn es um Resilienz in der IT geht, denken viele zuerst an technische Maßnahmen wie Firewalls, Back-ups oder Redundanzen. Menschliche und organisatorische Aspekte werden darüber vernachlässigt. Aber Hand aufs Herz: Sind Ihre IT-Ausfälle eher durch Maschinen oder durch Menschen entstanden? Studien belegen, dass menschliches Fehlverhalten eine der Hauptursachen für die meisten Ausfälle und Sicherheitsvorfälle ist – etwa 60 bis 70 Prozent aller Datenpannen. Laut einer Untersuchung von IBM Security sind es sogar 95 Prozent aller Cybersecurity-Vorfälle, die von Menschen verursacht werden. Dazu zählen Fehlkonfigurationen, unachtsames Klicken auf Phishingmails oder das Verwenden unsicherer Passwörter. Eine Untersuchung der Allianz Global Corporate & Specialty (AGCS) zeigt: „Der Mensch bleibt das größte Risiko in der IT-Sicherheit – aber auch die größte Chance, wenn Fehler offen kommuniziert und gemeinsam Lösungen entwickelt werden."

Fehler sind unvermeidlich. Entscheidend ist, wie wir mit ihnen umgehen. In der IT ist die Fehlerkultur von zentraler Bedeutung. Eine negative Fehlerkultur führt dazu, dass Fehler aus Angst vor Sanktionen vertuscht oder gar wiederholt werden. In der IT kann das fatale Folgen haben – von Datenverlusten über Sicherheitslücken bis hin zu Imageschäden. Eine positive Fehlerkultur hingegen ermöglicht es, Schwachstellen frühzeitig zu erkennen und zu beheben – bevor sie zu echten Krisen werden. Sie erkennt Fehler als unvermeidlichen Bestandteil komplexer Systeme an und nutzt sie als Chance zur Verbesserung. Das

gibt Organisationen die Möglichkeit, daraus zu lernen und sich weiterzuentwickeln.

In Unternehmen mit einer offenen Fehlerkultur melden Mitarbeitende Probleme frühzeitig. So können Risiken rechtzeitig bewertet und Gegenmaßnahmen eingeleitet werden. Ein Beispiel aus der Praxis: In einem internationalen IT-Unternehmen wurde nach der Einführung eines anonymen Meldesystems die Zahl der gemeldeten Vorfälle deutlich erhöht – dadurch sank die Zahl der schwerwiegenden Ausfälle signifikant. Umgekehrt zeigt die Erfahrung: Wo Fehler mit Schuldzuweisungen beantwortet werden, werden sie verschwiegen. Das erhöht das Risiko für die gesamte Organisation.

Ich erinnere mich an eine Situation vor einigen Jahren. Nach einem größeren IT-Ausfall wollte die Führungskraft sofort wissen, „wer schuld ist" und rechnete vor, wie viel Geld jede Minute Ausfall kostet. Die Konsequenz: Niemand in diesem Unternehmen wagte mehr, Verantwortung zu übernehmen – und ausgerechnet die Führungskraft war fortan die letzte Person, die von Problemen erfuhr. Mitarbeitende handelten nach dem Motto „Lieber nichts tun als etwas falsch machen". Das lähmte die Organisation. Sie wurde träge und Innovation fand praktisch nicht mehr statt.

Führung und Vorbildfunktion

Führungskräfte spielen eine zentrale Rolle bei der Fehlerkultur. Sie prägen sie durch ihr eigenes Verhalten. Wer als Chefin oder Chef offen über eigene Fehler spricht und Mitarbeitende ermutigt, Probleme frühzeitig zu melden, schafft Vertrauen und fördert die Resilienz im Unternehmen. Amy Edmondson, Professorin an der Harvard Business School, bringt es auf den Punkt: „Eine gute Fehlerkultur beginnt an der Spitze. Führungskräfte müssen zeigen, dass Fehler zum Lernen dazugehören."

Ich habe einmal – weil es schnell gehen sollte – ein Update von Daten direkt in der Konsole gemacht und das WHERE vergessen. Alle Kunden hatten plötzlich die gleiche E-Mail-Adresse. Sprechen Sie in so einem Fall ruhig offen über eigene Fehler und bitten Sie Ihr Team um Ideen, wie diese künftig vermieden werden können. So schaffen Sie eine Atmosphäre, in der Offenheit und Lernen erst möglich sind.

Praktische Maßnahmen

Wie kann eine Organisation eine offene Fehlerkultur fördern? Hier einige bewährte Maßnahmen:

- Offene Kommunikation fördern: Schaffen Sie regelmäßige Gelegenheiten, in denen Fehler und Lessons Learned besprochen werden – etwa in Retrospektiven oder Teammeetings.
- Anonyme Meldestellen einrichten: Für Mitarbeitende, die Hemmungen haben, Fehler offen anzusprechen, können anonyme Meldesysteme eine wichtige Brücke sein. Wichtig ist, dass die Anonymität wirklich gewährleistet ist.
- Keine Sanktionen bei Fehlern: Statt Schuldzuweisungen sollte der Fokus auf Ursachenanalyse und Prävention liegen. Fehler sind kein Makel, sondern eine Chance zur Verbesserung.
- Nachbesprechungen nach Vorfällen: Analysieren Sie nach jeder Krise gemeinsam, was genau passiert ist und wie dieser Fehler in Zukunft vermieden werden kann. Setzen Sie die Erkenntnisse konsequent um.
- Persönliches Handbuch schreiben: Darin können Mitarbeitende und Führungskräfte ihre Stärken und Schwächen, ihre bevorzugte Art der Kommunikation sowie den Umgang, den sie sich bei Rückmeldungen zu Fehlern wünschen, zusammenfassen. Das Handbuch hilft, die Zusammenarbeit zu verbessern und ein Umfeld zu schaffen, in dem Rückmeldungen konstruktiv und wertschätzend gegeben werden.

Trainieren Sie Kommunikation, wenn es keine akuten Krisen gibt, damit Sie sie im Krisenfall bereits beherrschen. Erwartungsmanagement ist dabei ein wichtiger Baustein: Machen Sie deutlich, dass Veränderungen immer mit Risiken verbunden sind und Fehler dazugehören. Wichtig ist, sich gut vorzubereiten, sich auszutauschen und im Fehlerfall gemeinsam schnell zu reagieren. Das öffnet die Chance für neue Lösungswege.

Fazit

Jeder offen angesprochene Fehler macht Ihr Team ein Stück souveräner im Umgang mit Ausfällen und das Unternehmen widerstandsfähiger. Das fördert Innovation und schützt vor größeren Schäden. Wer heute in eine Fehlerkultur investiert, stärkt die Resilienz von morgen. Sprechen Sie im nächsten Teammeeting offen über einen eigenen Fehler – und laden Sie Ihr Team ein, es Ihnen gleichzutun. Sie werden überrascht sein, wie viel Vertrauen und Lernbereitschaft dadurch entstehen. ◆

QUELLEN

https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Amy C. Edmondson „The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth" (John Wiley & Sons, 2018), ISBN 978-1-11-947724-2

Aus dem Escape-Room in den digitalen Märchenwald – IT-Security-Awareness an der Universität Marburg

Illustration: freepik.com

Schulungen zur IT- und Informationssicherheit gehören mittlerweile zum Standardrepertoire vieler Hochschulen. Hierbei zählt längst nicht nur der Inhalt, sondern vor allem der Unterhaltungswert. Die Universität Marburg möchte ihre Beschäftigten und Studierenden für ein Thema begeistern, das für einige Menschen so interessant sein dürfte wie die jährliche Steuererklärung. Darum hat die Stabsstelle Informationssicherheit ein Schulungskonzept entwickelt, das nun Stück für Stück umgesetzt wird.

Text: **Lukas Härter** (Philipps-Universität Marburg)

An der Universität Marburg gibt es seit 2019 eine Stabsstelle, die sich das Thema IT- und Informationssicherheit auf die Fahnen geschrieben hat. Getreu den Anforderungen aus dem BSI-Standard 200-1 fördert und koordiniert sie den Informationssicherheitsprozess der Universität und ist direkt der Universitätsleitung unterstellt. Konkret bedeutet das, dass sie Managementstrukturen aufbaut, Administratorinnen und Administratoren über verwundbare Server informiert und versucht, Mitglieder und Angehörige der Universität für das Thema Informationssicherheit zu begeistern. Zum Beispiel arbeitet die Stabsstelle täglich daran, die Universität vor Angriffen zu schützen und

Unterhalten und aufklären: mit der Märchenkampagne IT-Security-Awareness fördern | *Foto: Universität Marburg*

Beschäftigte dafür zu sensibilisieren, Phishingmails zu melden. Gerade für Letzteres sind in den vergangenen Jahren zahlreiche Schulungsangebote entstanden. Mit dem kürzlich zur Verfügung gestellten Schulungskonzept wird versucht, dieses Sammelsurium zielgruppengerecht zu strukturieren.

Ohne Pflicht geht es nicht

Der berufliche Alltag in der Informationssicherheit ist selten langweilig. Es gibt täglich neue Angriffe und Schwachstellen, auf die schnell und richtig reagiert werden muss. Dabei rücken konzeptionelle Arbeiten häufig in den Hintergrund. Da ist es manchmal hilfreich, wenn Fortbildungen Prioritäten verschieben. Denn im Rahmen einer Fortbildung entstand das Schulungskonzept zur Informationssicherheit für die Universität. Das Konzept orientiert sich an den Anforderungen aus dem IT-Grundschutz-Baustein ORP.3 des BSI und ergänzt den Regelkatalog der Universität zur Informationssicherheit.[1]

Damit eine Schulung erfolgreich und nachhaltig ist, muss sie Menschen in ihrer individuellen Situation inhaltlich abholen. Deshalb wurden als Ausgangspunkt für das Konzept vier Zielgruppen an der Universität identifiziert. Sie umfassen Studierende, Beschäftigte, die keine IT-Systeme administrieren, Beschäftigte des zentralen IT-Dienstleisters der Universität (Hochschulrechenzentrum) und dezentral verortetes IT-Personal. Auch wenn es Personen mit vergleichbaren Tätigkeiten und Lebenssituationen innerhalb einer Zielgruppe gibt, sind diese trotzdem sehr heterogen und unübersichtlich groß. Daher braucht es Schulungsangebote, die möglichst viele Menschen ansprechen: Vorträge online oder offline, Videos, Texte, Poster, Podcasts, Quiz und vieles mehr – möglichst bunt und glitzernd. Das im Konzept selbst auferlegte Ziel ist, dass sich alle Angehörigen der Universität mindestens einmal im Jahr in einer Schulung mit dem Thema Informationssicherheit auseinandersetzen. Das scheint auf den ersten Blick machbar zu sein, aber die Erfahrung hat gezeigt, dass sich im verdichteten Alltag vieler Menschen selbst ein noch so kleiner Moment für dieses Thema kaum unterbringen lässt. Um hier etwas nachzuhelfen, verpflichtet das Schulungskonzept Universitätsangehörige in bestimmten Situationen zu einer Schulung. Zum Beispiel, wenn Beschäftigte im Homeoffice arbeiten wollen, jemand ein Passwort auf einer Phishingseite eingegeben hat oder mit Daten arbeiten möchte, die einen besonders hohen Schutzbedarf haben. Untermauert wird dies in Dienstanweisungen und Nutzungsordnungen der Universität. Eine pauschale Schulungspflicht wird gewiss niemanden für das Thema begeistern oder inhaltlich abholen. Jedenfalls sind die Fälle, in denen Beschäftigte nach einer verpflichtenden Brandschutzschulung Feuer und Flamme für das Thema waren, eher selten. Damit sich Menschen aus eigenem Antrieb für das Thema begeistern, führt kein Weg an spannenden und vielfältigen Schulungsangeboten vorbei. Textwüsten und endlose Präsentationen sind nicht mehr zeitgemäß.

> Textwüsten und endlose Präsentationen sind nicht mehr zeitgemäß.

Informationssicherheit in vielen Facetten

Die Vor-Ort- und die Onlineschulung zum Thema Informationssicherheit sind die Dauerbrenner der Stabsstelle Informationssicherheit. Seitdem es die Stabsstelle gibt, gibt es diese Schulungen. Jedoch haben Auswertungen dieser Angebote erbarmungslos vor Augen geführt, dass solche Schulungen sehr

1 https://www.uni-marburg.de/de/universitaet/administration/verwaltung/stabsstellen/sis/sicherheitsleitlinien

unattraktiv sind. Als Reaktion hat die Stabsstelle bereits 2020 Schulungsinhalte von einer externen Firma hinzugekauft. Diese hatte zum Beispiel kurze Videoclips, Spiele und Serien im Format großer Streaminganbieter im Portfolio, die anfangs vor allem die eigene Onlineschulung aufwerteten. Seitdem sind externe Schulungsinhalte ein wichtiger Teil des universitären

> Die Schulungskampagne nimmt Teilnehmende thematisch in einen digitalen Märchenwald mit.

Schulungsangebots. Mit diesen Erkenntnissen wurde kürzlich ein neuer Vertrag mit einem anderen Anbieter geschlossen, dessen Portfolio weitere spannende Möglichkeiten bietet. Auf Basis der Schulungsplattform des externen Anbieters startete Anfang August dieses Jahres eine Schulungskampagne, die die Teilnehmenden thematisch in einen digitalen Märchenwald mitnimmt. Die Kampagne bettet wichtige Themen der Informationssicherheit in die Geschichten bekannter Märchen ein. Bis Anfang Oktober wurden die Teilnehmenden jede Woche dazu eingeladen, an interaktiven Schulungsmodulen zu Märchen wie Rotkäppchen oder Hänsel und Gretel teilzunehmen. Durch die Funktionen der externen Plattform wird die Kampagne weitestgehend automatisiert. Es ist der erste Versuch, Angehörige der Universität durch eine Kampagne mit regelmäßigen und möglichst kreativen Informationshäppchen für das Thema nachhaltig zu begeistern. Für die Kampagne haben sich rund 60 Personen angemeldet. Weitere Kampagnen sind geplant.

In den vergangenen Jahren entstanden Seminare für Studierende, mit denen sie für das Studium relevante ECTS-Punkte sammeln können. Außerdem wurden Blockveranstaltungen für Beschäftigte, Workshops zum Einrichten von digitalen Zertifikaten oder einem Passwortmanager, ein Erste-Hilfe-Set, Sticker, Poster und allerhand Infomaterial erstellt. Inspiriert von der Universität Osnabrück bot die Stabsstelle einen digitalen Escape-Room an. In diesen konnten sich Studierende und Beschäftigte einsperren lassen und dabei herausfinden, welche Risiken für die Informationssicherheit an jedem Arbeitsplatz lauern. Aufgrund der heterogenen Zielgruppen an einer Universität, der Schnelllebigkeit einiger Angebote und des Bedarfs an neuen, innovativen Ideen ist es manchmal wie bei einem Freizeitpark, der jedes Jahr eine neue, aufregende Attraktion bauen muss, um die Kundschaft bei der Stange zu halten. Dank all dieser Angebote ist das Thema Informationssicherheit an der Universität Marburg deutlich sichtbarer geworden.

Für mehr IT- und Informationssicherheit: Zielgruppengerecht aufgearbeitete Materialien wie Erste-Hilfe-Kit und Cheat Sheet helfen | *Foto: Universität Marburg*

Erfolgsmessung von Schulungen: mehr als nur Zahlen

Letztlich misst sich Erfolg in Zahlen und es ist entscheidend, wie viele Personen mit Schulungen erreicht werden. Darum erfasst die Stabsstelle Informationssicherheit seit 2022 systematisch, wie viele Personen an Schulungen teilnehmen. Zu den Kursen in den Onlineselbstlernschulungen haben sich bis Ende August 2025 etwa 950 Personen angemeldet. An den anderen Angeboten haben insgesamt 230 Universitätsmitglieder teilgenommen. Das entspricht insgesamt knapp fünf Prozent der Mitglieder und Angehörigen der Universität. Diese Zahlen verdeutlichen einmal mehr, dass es schwierig ist, mit freiwilligen Schulungen eine wirklich große Personenzahl zu erreichen. Andererseits ist ein ausschließlich quantitativer Blick auf den Erfolg von Schulungen auch nur die halbe Wahrheit. Jede Person, die sich mit dem Thema auseinandersetzt, ist ein Gewinn für die Informationssicherheit. Wenn Menschen aufgrund der Schulungen anfangen, einen Passwortmanager zu nutzen oder vorsichtiger im Umgang mit E-Mails sind, hat das einen direkten positiven Einfluss auf die Informationssicherheit – und vielleicht auch auf Kolleginnen und Kollegen, die das Thema IT-Security-Awareness weitertragen. Insofern ist es wichtig, Menschen auch weiterhin mit interessanten Schulungen für das Thema Informationssicherheit zu begeistern. ◆

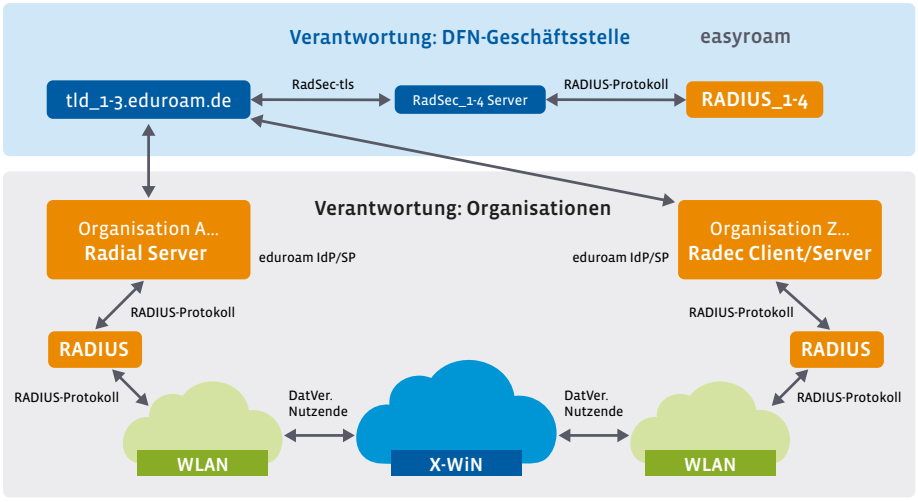
radsecproxy² – automatisiertes Zertifikatsmanagement mit Radial Server

Das RADIUS-Protokoll ist seit Jahrzehnten im Einsatz, weist jedoch inzwischen erhebliche Sicherheitslücken auf. RadSec als TLS-basierte Weiterentwicklung schließt diese Lücken, bringt jedoch neue Anforderungen mit sich – insbesondere beim Zertifikatsmanagement. Im Rahmen der Bachelorarbeit „Design and Implementation of a RADIUS over TLS Proxy with Automated Certificate Management via ACME“ an der Freien Universität Berlin entstand mit Radial Server ein Werkzeug, das diese Herausforderungen adressiert und den Betrieb von RadSec-Infrastrukturen vereinfacht.

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

Mit nun knapp 35 Jahren ist das RADIUS-Protokoll (Remote Authentication Dial-In User Service) eines der älteren Protokolle, die heute noch im Einsatz sind. Das Alter ist dem Protokoll auch anzusehen, denn eine schwache MD5-basierte Integritätsüberprüfung und fehlende Verschlüsselung machen RADIUS zu einem möglichen Sicherheitsrisiko.

Um das Sicherheitsproblem von RADIUS zu lösen, wurde das RadSec-Protokoll entwickelt. RadSec transportiert RADIUS-Pakete ausschließlich über TLS (Transport Layer Security) und ermöglicht so Vertraulichkeit, Integrität sowie gegenseitige Authentifizierung. Der DFN-Verein betreibt bereits seit 2018 als einziges NREN (National Research and Education Network) eine rein auf RadSec basierende Infrastruktur für den Dienst eduroam und vermeidet so die bekannten Schwachstellen des klassischen RADIUS-Protokolls.



Infrastruktur des eduroam/easyroam RadSec Client/Servers

Digitale Zertifikate als kritischer Faktor

Das RadSec-Protokoll basiert auf TLS, einem kryptografischen Protokoll, das auch Anwendung in HTTPS findet. TLS nutzt unter anderem digitale Zertifikate, um die Authentizität beim Aufbau eines verschlüsselten Kommunikationskanals sicherzustellen. Weiterhin stellen digitale Zertifikate einen wichtigen Bestandteil bei der eigentlichen Verschlüsselung dar. Um die Sicherheit von digitalen Zertifikaten zu gewährleisten und um sicherzustellen, dass sie stets den aktuellen Sicherheitsstandards entsprechen, haben sie ein Ablaufdatum.

Sollten Zertifikate nicht rechtzeitig verlängert werden, kann dies zu Ausfällen führen. Bei eduroam Identity-Providern führt dies üblicherweise dazu, dass sich einrichtungsfremde Nutzende nicht mehr in eduroam anmelden können. Das betrifft – je nachdem, wie die interne Infrastruktur aufgebaut ist – auch Nutzende aus der eigenen Einrichtung. Bei Serviceprovidern führt ein abgelaufenes Zertifikat üblicherweise zu einem Komplettausfall von eduroam.

Entwicklung des Radial Servers

Im Rahmen der Bachelorarbeit „Design and Implementation of a RADIUS over TLS Proxy with Automated Certificate Management via ACME“ an der Freien Universität Berlin ist ein Werkzeug entstanden, das das Zertifikatsproblem und auch weitere übergeordnete Probleme wie beispielsweise die Speichersicherheit löst. Radial Server ist ein neu entwickelter „RADIUS over TLS Proxy“, der die Verwaltung eines RadSec Client/Servers enorm vereinfacht. Dabei nutzt Radial Server modernste Technologien wie ACME (Automated Certificate Management Environment) und Rust, um ein hohes Maß an Sicherheit und Robustheit zu erreichen. Durch die Nutzung von ACME werden TLS-Zertifikate nach einmaliger Konfiguration automatisiert ausgestellt und verlängert, sodass Ausfälle durch abgelaufene Zertifikate der Vergangenheit angehören.

Außerdem ist es durch die Automatisierung möglich, die Laufzeit der Zertifikate zu verkürzen, um die Angriffsfläche durch kompromittierte Zertifikate noch weiter zu minimieren. Erweiterungen des ACME-Protokolls wie ARI (ACME Renewal Information), das im Juni 2025 offiziell standardisiert wurde, erhöhen die Robustheit von ACME noch weiter. ARI sorgt dafür, dass Clients darüber informiert werden, wenn Zertifikate noch vor Ablauf widerrufen werden müssen. Die Clients können dann entsprechend reagieren und ein neues Zertifikat anfordern.

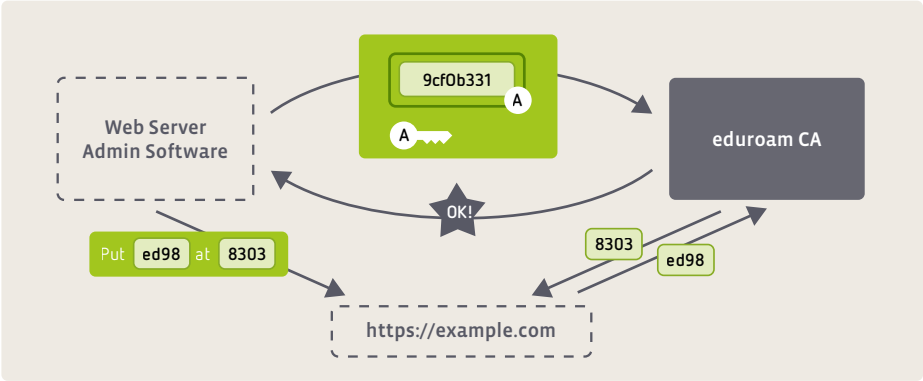
Kreativ Lösungen finden: Mit seinem neu entwickelten Radial Server hat Long Yang Paffrath die Verwaltung des RadSec Client/Servers enorm vereinfacht | *Foto: Christoph Schieder*

Ein weiterer zentraler Sicherheitsfaktor ist die Wahl der Programmiersprache. Während klassische Systeme wie der radsecproxy in C entwickelt wurden, basiert Radial Server vollständig auf Rust. Dadurch werden viele typische Speicherzugriffsfehler wie Use-after-Free oder Buffer Overflows verhindert, die für etwa 70 Prozent der bekannten Schwachstellen in moderner Software verantwortlich sind. Bereits beim Kompilieren stellt Rust sicher, dass Speicher nur auf sichere Weise genutzt werden. Das bedeutet, dass ein Großteil potenzieller Sicherheitslücken bereits auf Code-Ebene verhindert wird, was Radial Server zu einer besonders robusten Lösung macht.

Zusätzlich unterstützt Radial Server „Post-Quantum“-sichere TLS-Verschlüsselung durch ML-KEM, wodurch die Kommunikation in Radsec-Infrastrukturen auch im Zeitalter der Quantencomputer zukunftssicher gewährleistet ist.

Fazit

Radial Server bietet einen signifikanten Mehrwert für Einrichtungen, die ihre RADIUS- oder RadSec-Infrastruktur modernisieren möchten. Durch die vollständige Automatisierung von bisher manuellen, fehleranfälligen Prozessen gewinnen IT-Teams wertvolle Ressourcen zurück und können sich auf strategische Kernaufgaben konzentrieren. Die moderne Struktur ermöglicht zudem die einfachere Integration weiterer Features wie beispielsweise eine Konfiguration über ein Webinterface mit Live-Reload-Funktionalität. Dadurch wird das Administrieren mehrerer Radial Server immens vereinfacht. Auch die Integration von RADIUS-Authentifizierung direkt in Radial Server ist damit möglich. Die Integration in Logging Frameworks wie Grafana oder GrayLog macht es für Organisationen einfacher, Logdaten auszuwerten. Radial Server lässt sich überall dort einsetzen, wo RADIUS/RadSec genutzt wird. ◆



Möglicher schematischer Ablauf einer ACME-Zertifikatsanfrage

Sicherheit im Visier – die Lageberichte des DFN-CERT

Cyberbedrohungen entwickeln sich rasant: Neue Schwachstellen, raffinierte Malware und unbekannte Angreifergruppen machen IT-Sicherheit zunehmend zu einer Herausforderung. Um effektiv reagieren zu können, braucht es aktuelles, kompaktes Wissen. Die Lageberichte der DFN-CERT Services GmbH geben teilnehmenden Einrichtungen im DFN-Verein einen wertvollen Überblick über die spezifische Sicherheitslage.

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

Die Dynamik im Bereich der Cyberbedrohungen ist enorm: täglich neue Schwachstellenmeldungen, eine Vielzahl optimierter Malware und modifizierter Angriffsmethoden sowie noch unbekannte Angreifergruppen. Dazu kommt erfolgreiche Datenexfiltration bei Großunternehmen, die wieder für Angriffe eingesetzt werden, und vieles mehr. Für eine erfolgreiche Gefahrenabwehr ist das Wissen über die aktuellen Entwicklungen unerlässlich. Das kontinuierliche Beobachten des Geschehens und die Ermittlung besonders relevanter Vorgänge ist mit einem erheblichen Ressourceneinsatz verbunden. Erschwert wird diese Aufgabe zudem dadurch, dass viele Betroffene Details zu Vorfällen zurückhalten oder Informationen nur eingeschränkt weitergeben.

Illustration: beast01/iStock

Mit der Einführung des Dienstes DFN-Security 2023 begann das DFN-CERT damit, halbjährliche Lageberichte zu erstellen, die den Dienstverantwortlichen aufseiten der teilnehmenden Einrichtungen im DFN-Verein dabei helfen, einen Überblick über die spezifische Sicherheitslage zu erhalten. Nach zwei Jahren Erfahrung mit den Lageberichten haben sich zwei Dinge herauskristallisiert: Erstens ist die einrichtungsinterne Verteilung der Lageberichte an alle Interessierten suboptimal. Zweitens wird die halbjährliche Erstellung der Dynamik des Geschehens nicht mehr gerecht.

Als Ergebnis wurde im Juni eine spezifische Mailingliste für den Bezug der DFN-CERT-Lageberichte erstellt. Diese sind nicht öffentlich. Sie werden ausschließlich an die Sicherheitskontakte der Einrichtungen verteilt, die am Dienst DFN-Security teilnehmen, wie zum Beispiel Chief Information Security Officer (CISO) oder Administrierende von Netzbereichen. Bevor eine Aufnahmeanfrage für die Mailingliste akzeptiert wird, erfolgt darum zunächst eine manuelle Prüfung, ob der Kontakt berechtigt ist, die Lageberichte zu erhalten. Damit die Sicherheitskontakte noch schneller zu sicherheitsrelevanten Vorfällen informiert werden, erstellt und versendet das DFN-CERT die Lageberichte statt wie bisher alle sechs Monate nun jeden Monat. Das entspricht damit der derzeit maximal möglichen Ausbaustufe.

Die Lageberichte umfassen aktuell drei Informationsblöcke. Der erste Block beinhaltet Informationen zu besonders erwähnenswerten Schwachstellen, die sich zum Beispiel durch eine hohe Kritikalität, eine bekannte oder sehr wahrscheinliche Ausnutzung oder eine besondere Relevanz auszeichnen. Die Schwachstellen werden kurz beschrieben und mit weiterführenden Informationen bereitgestellt – in der Regel erfolgt auch ein Verweis auf eine entsprechende Schwachstellenmeldung des DFN-CERT.

Im zweiten Block geht es um Informationen zur Vorfallsbearbeitung bezüglich automatischer Warnmeldungen und Erkenntnissen, die aus manuellen Anfragen und Meldungen an das DFN-CERT gewonnen werden können und keiner Beschränkung zur Weitergabe unterliegen.

Den derzeit letzten Block des Lageberichts bilden Kennzahlen zu Ereignissen, die über externe Zulieferer wie etwa Shadowserver oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingehen, durch eigene Sensorik erfasst oder von Teilnehmern an der Logdatenanalyse in diese eingeliefert werden. Die Ereignisse werden im Zuge der internen Verarbeitung bestimmten Kategorien zugeordnet: zum Beispiel „Access/Domains: C2/Malware“. Diese beschreibt einen Zugriffsversuch auf eine als maliziös eingestufte Domain, der bei Nutzung von DNS-RPZ (Domain Name System Response Policy Zone) unterbunden wird. Die Datenbasis für diese Kategorie bilden Logdaten, die von teilnehmenden Einrichtungen eingeliefert werden. Für jede Kategorie werden die Ereignisse im Verlauf der vergangenen sechs Monate dargestellt.

Wie alle Dienstbestandteile des Dienstes DFN-Security unterliegt auch der DFN-CERT-Lagebericht einem kontinuierlichen Review und einer entsprechenden Anpassung. Indem neue Datenquellen erschlossen und ausgewertet werden, können weitere Informationen dauerhaft in den Lagebericht aufgenommen werden. Aber auch temporäre Änderungen sind vorfallsbezogen möglich, wobei das Ziel bleibt, mit dem DFN-CERT-Lagebericht weiterhin eine kompakte Informationsquelle bereitzustellen.

Zusammen mit den werktäglich veröffentlichen Schwachstellenmeldungen sowie den nun monatlich erscheinenden Lageberichten stellt das DFN-CERT Sicherheitsverantwortlichen zwei wichtige Informationsquellen zur Beurteilung der aktuellen Sicherheitslage zur Verfügung. Trotz dieser umfangreichen Informationen können nicht alle sicherheitsrelevanten Vorgänge vollständig abgedeckt werden. Kritische Schwachstellen in Software oder Systemen, die derzeit nicht vom Schwachstellendienst unterstützt werden, sowie Vorfälle außerhalb des DFN-Vereins werden nicht betrachtet, können aber eine Auswirkung auf teilnehmende Einrichtungen im DFN-Verein haben. Aus diesem Grund ergänzt das DFN-CERT die eigenen Lageberichte um Inhalte, die vom BSI als nationalem IT-Lagezentrum für Kooperationspartner und Betreiber kritischer Infrastrukturen werktäglich bereitgestellt werden. Diese dienen dazu, das Bild zur Sicherheitslage zu komplettieren. Auch diese Lageberichte sind nicht öffentlich, sondern werden nur innerhalb einer definierten Benutzergruppe geteilt.

Das DFN-CERT als Sicherheitsdienstleister des DFN-Vereins, Mitglied im CERT-Verbund und der Allianz für Cybersicherheit hat als Multiplikator der Allianz für Cybersicherheit die Erlaubnis erhalten, deren Tageslageberichte weiter zu verteilen. Da nur Informationen, die nach dem Traffic Light Protokoll (TLP) als TLP:GREEN für eine organisationsübergreifende Weitergabe vorgesehen sind – nicht aber Informationen, die als TLP:AMBER oder höher eingestuft sind –, werden aus den Tageslageberichten lediglich Auszüge verteilt. Weitergegeben werden Informationen zu Vorfällen sowie Schwachstellen und Exploits. Die CERT-Bund-Kurzinformationen, die einen BSI-Schwachstellenfeed mit eingeschränktem Informationsgehalt darstellen, sowie Informationen der Kategorie Politik und Öffentlichkeit werden entfernt.

Für die Weitergabe der BSI-Tageslageberichte (TLB) wird ebenfalls eine Mailingliste bereitgestellt. Diese Mailingliste steht prinzipiell Mitarbeitenden von DFN-Teilnehmern offen. Die Weitergabe erfordert die Einhaltung des Traffic Light Protokolls. Eine Nichtbeachtung der Vorgaben – beispielsweise das Veröffentlichen der Informationen auf einer frei zugänglichen Webseite – kann zum Verlust der Multiplikatorprivilegien des DFN-CERT führen. Darum ist bei Vorliegen entsprechender Hinweise auf eine Verletzung der Anforderungen ein Ausschluss von der Mailingliste durch das DFN-CERT möglich. Gleiches gilt bei Nichtbeachtung der Weitergaberestriktionen

des DFN-CERT-Lageberichts, wobei hierbei der Schutz der teilnehmenden Einrichtungen im DFN-Verein die Anforderung an die Vertraulichkeit bestimmt. ◆

INFORMATIONSKASTEN ZUM TRAFFIC LIGHT PROTOCOL (TLP)

Das DFN-CERT verwendet für die Einstufung von Informationen das Traffic Light Protocol (TLP) basierend auf der Definition des „Forum of Incident Response and Security Teams“ (FIRST) in der Version 2.0. Das TLP dient der Erhöhung der Sicherheit beim Austausch sensitiver Informationen. Das Recht, Daten zu klassifizieren, obliegt allein seinem Bereitsteller.

Folgende Einstufungen existieren:

TLP:CLEAR:
Unbegrenzte Weitergabe

TLP:GREEN:
Organisationsübergreifende Weitergabe

TLP:AMBER:
Eingeschränkte interne und organisationsübergreifende Weitergabe

TLP:AMBER+STRICT:
Eingeschränkte interne Weitergabe

TLP:RED:
Persönlich, nur für benannte Empfänger

Weitere Informationen gibt es unter:
https://www.first.org/tlp/

MAILINGLISTEN

Mailingliste für den Bezug der Lageberichte des DFN-CERT: **https://www.listserv.dfn.de/sympa/info/dfn-cert-lageberichte**

Die Mailingliste für den Bezug der BSI-Tageslageberichte gibt das DFN-CERT nach Redaktionsschluss bekannt.

Sicherheit aktuell

Hinweise zu MSCHAPv2-basierten Authentifizierungsverfahren in eduroam

Auf neueren Windows-Betriebssystemen wie Windows 11 Enterprise, Education oder Pro, auf denen die Sicherheitsfunktion Credential Guard standardmäßig aktiviert ist, können Einschränkungen bei der Verwendung von MSCHAPv2-basierten Authentifizierungsverfahren auftreten. Bei der Anmeldung in eduroam mit PEAP-MSCHAPv2 und EAP-TTLS-MSCHAPv2 kann es darum zu Problemen kommen.

Credential Guard schützt Anmeldeinformationen wie NTLM-Hashes und Kerberos-Tickets mithilfe der Virtualization-based Security (VBS). Diese Technologie speichert sensible Daten in einer isolierten Umgebung getrennt vom eigentlichen Betriebssystem und verhindert so den unbefugten Zugriff durch Schadsoftware oder Angreifende.

Aufgrund der Einschränkung durch Credential Guard bei der Nutzung von MSCHAPv2-basierten Authentifizierungsverfahren wird unter anderem für WLAN- und VPN-Verbindungen empfohlen, von MSCHAPv2-basierten Verbindungen (z. B. PEAP-MSCHAPv2 und EAP-MSCHAPv2) zur zertifikatbasierten Authentifizierung (z. B. PEAP-TLS oder EAP-TLS) zu wechseln

Im Rahmen von eduroam bietet der DFN-Verein seit etwa vier Jahren ein zentral verwaltetes, auf Pseudonymen basierendes Zertifikatsmanagement für EAP-TLS an. Um die Nutzendenverwaltung für eduroam zu realisieren, nutzt die Diensterweiterung easyroam hierfür die dezentral verwalteten, föderierten DFN-AAI-Identity-Provider, die in jeder an easyroam teilnehmenden Einrichtung vorhanden sind. ◆

Quelle: **https://learn.microsoft.com/de-de/windows/security/identity-protection/credential-guard/considerations-known-issues**

Weitere Informationen zu easyroam sowie Anleitungen für verschiedene Betriebssysteme finden Sie unter:
https://doku.tid.dfn.de/de:eduroam:easyroam

GÉANT TCS: HARICA automatisiert Zertifikatsprozesse

Nach dem Anbieterwechsel im GÉANT Trusted Certificate Service (TCS) weitet der neue Anbieter HARICA (Hellenic Academic and Research Institutions Certification Authority) das Angebot für browserverankerte Zertifikate sukzessive aus. Seit Ende Juni unterstützt HARICA das ACME-Protokoll zur Ausstellung von Serverzertifikaten. ACME (Automatic Certificate Management Environment) ist ein offener Standard, mit dem sich Zertifikate direkt aus der eigenen Serverumgebung heraus automatisch anfordern, erneuern und verwalten lassen. Damit kann der manuelle Verwaltungsaufwand erheblich reduziert werden. Dies ist besonders relevant, um mit der Verringerung der Laufzeit von Serverzertifikaten Schritt halten zu können: Ab März 2026 sind Serverzertifikate aus der Web-PKI nur noch 200 Tage gültig. Die nächsten Abstufungen beinhalten dann im März 2027 eine weitere Verringerung auf 100 Tage und im März 2029 auf 47 Tage. Ohne eine tiefgreifende Automatisierung ist die Versorgung von Servern mit Zertifikaten absehbar nicht mehr möglich. ◆

Erfolgreiches Audit der DFN-PKI „Global“

Die DFN-PKI im Sicherheitsniveau „Global“ wurde mit Erfolg von der TÜV Nord Cert GmbH (bisher TÜVIT) geprüft. Seit 2012 wird sie jährlich auditiert und zertifiziert, um sicherzustellen, dass die strengen Anforderungen von Web-Browsern, Root-Programmen und dem CA/Browserforum eingehalten werden.

Derzeit befindet sich die DFN-PKI „Global“ im Erhaltungsbetrieb, da die Ausstellung browserverankerter Zertifikate der DFN-PKI komplett zum Dienst GÉANT Trusted Certificate Services (TCS) migriert wurde. Aus diesem Grund werden in der DFN-PKI „Global“ seit dem 30. August 2023 keine neuen Zertifikate mehr ausgestellt. Weshalb findet nach wie vor eine Prüfung statt? Die Lösung ist einfach: In der DFN-PKI „Global“ gibt es noch mehr als 100 000 gültige User-Zertifikate. Damit diese, wie vorgesehen, bis zu ihrem Ablaufdatum verwendet werden können, muss die DFN-PKI „Global“ das Vertrauen der Root-Programme erhalten und dafür unter anderem Sperrinformationen bereitstellen – und sich dafür wie in den vergangenen Jahren prüfen lassen. Die letzten Zertifikate werden im Frühjahr 2027 ablaufen. Anschließend sind keine Audits mehr notwendig. ◆

Start des neuen eduroam-Metadatenportals

Seit Anfang Oktober 2025 haben DFN-Teilnehmer die Möglichkeit, das neue eduroam-Metadatenportal zu nutzen. Darin können Administrierende von Einrichtungen, die an der DFN-AAI teilnehmen und einen DFN-AAI-Identity-Provider stellen, verschiedene Parameter flexibel selbst konfigurieren. Das Portal bietet die Grundlage für ein hocheffizientes Management der Föderationsserver.

Bisher wurden die Föderationsserver mit den erforderlichen Betriebsparametern ausschließlich von Mitarbeitenden der DFN-Geschäftsstelle in Berlin manuell konfiguriert. Durch die Integration des eduroam-Metadatenportals in die DFN-AAI können nun alle eduroam Identity- Provider (IdP) und edurom Serviceprovider (SP), die an der DFN-AAI teilnehmen, ihre Daten – beispielsweise die IP-Adressen der Clients und Server sowie die Anmeldeinformationen (Realms) ihrer Einrichtung – im Portal bearbeiten und verwalten.

Das Portal wurde vom DFN-Verein und der DFN-CERT Services GmbH innerhalb von zwei Jahren gemeinsam entwickelt und als DFN-AAI Serviceprovider bereitgestellt. Es ermöglicht unter anderem die gleichzeitige Konfiguration aller drei ortsunabhängigen Föderationsserver beim weltweiten WLAN-Zugangsdienst eduroam. Diese sind zu einem hierarchisch strukturierten Netzwerk mit zahlreichen RADIUS Security (RadSec) Servern verknüpft und gewährleisten den fehlerfreien Betrieb. Das Netzwerk ist Teil der internationalen eduroam-Infrastruktur und wird von den an eduroam teilnehmenden Einrichtungen in Koordination mit dem DFN-Verein betrieben und verwaltet. ◆

Weitere Informationen sowie den Zugang zum eduroam-Metadatenportal finden Sie unter:
https://doku.tid.dfn.de/de:eduroam:emp

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:
Heike Ausserfeld, Jürgen Brauckmann, Ralf Paffrath

Vielfalt gefragt – Videokommunikation im DFN

Die Rahmenverträge des DFN-Vereins für cloudbasierte Videokonferenzsysteme laufen 2026 aus. Mit einer Neuausschreibung stellt der Verein die Weichen für die Zukunft: Gefragt sind nicht nur stabile und bezahlbare Lösungen, sondern auch Vielfalt, digitale Souveränität und Resilienz.

Text: **Dirk Bei der Kellen** (DFN-Verein)

Der DFN-Verein schreibt derzeit die Rahmenverträge für cloudbasierte Videokonferenzsysteme neu aus. Die bestehenden Verträge, die 2021 während der Pandemie initiiert wurden und 2022 in Kraft traten, laufen nach einer Verlängerung im März 2026 aus. Sie hatten den Zweck, den stark gestiegenen Bedarf an Videokonferenzlösungen zu decken. Da sich die Rahmenverträge bewährt haben, wird nun ein neues Vergabeverfahren gestartet. Dabei geht es nicht allein um Kostenoptimierung, sondern vor allem um Vielfalt: Einrichtungen sollen aus verschiedenen Videokonferenzsystemen wählen können, anstatt sich auf nur wenige Anbieter festlegen zu müssen.

Dafür wurden seit Anfang des Jahres teilnehmende Einrichtungen zu ihren aktuellen Bedarfen an Videokonferenztechnologie sowie den Anforderungen an die Systeme befragt. Zu Beginn waren acht Anbieter beteiligt, aktuell sind es noch sieben. Ein Anbieter ist ausgeschieden, da er seine Erfolgschancen im Wettbewerb als zu gering einschätzte, denn die meisten Lizenzen werden derzeit über den Hersteller Zoom und den Vertriebspartner Telekom Deutschland GmbH abgewickelt.

Markt in Bewegung

Auch wenn der Service Zoom X im Wissenschaftsnetz die Marktführerschaft übernommen hat, unterscheiden sich die verschiedenen Systeme technologisch nur noch wenig. Sie setzen aber verschiedene Schwerpunkte, etwa bei der Weiterentwicklung von KI-Werkzeugen. Auffallend ist, dass sich die Bedienung der diversen Systeme immer mehr annähert, sodass Nutzende mittlerweile auch mit Systemen unterschiedlicher Anbieter umgehen können.

Illustration: aelitta /iStock

Auch die Tatsache, dass aus den Schulen heraus Lernende eher mit BigBlueButton groß geworden sind als mit Zoom X, wird sich möglicherweise auch im zukünftigen Nutzungsverhalten an Universitäten und Hochschulen widerspiegeln. In diesem Zusammenhang ist auch die Software Cisco Webex zu nennen. Für diese gibt es etablierte Videokonferenzhardware, die in vielen Einrichtungen noch in Betrieb ist und hinsichtlich des Trends zu hybrider Lehre eine nicht zu unterschätzende Rolle spielen dürfte.

Zunehmend rücken unter dem Schlagwort „Unified Communication“ integrierte Plattformen in den Fokus, die über reine Videokommunikation hinausgehen. Dabei handelt es sich um Gesamtlösungen mit Chat, Kalender, Dokumentenbearbeitung und

-ablage, Telefonie und vielem mehr. Hochintegrierte Systeme – beispielsweise das weitverbreitete Microsoft 365, das ohnehin in vielen Einrichtungen verfügbar ist – bringen die Kommunikations- und Kollaborationsplattform gleich mit und könnten den alleinstehenden Services den Rang ablaufen. Allerdings stehen derart marktbeherrschende Softwareanbieter unter Beobachtung der Europäischen Kommission, deren Ziel es ist, die Interoperabilität zwischen Produkten verschiedener Anbieter zu erhöhen – insbesondere durch Vorgaben des Digital Markets Act (DMA).

Digitale Souveränität im Blick

Ein weiterer Grund, warum auch in der aktuellen Ausschreibung eine Vielfalt an Videodiensten angestrebt wird, ist das Thema digitale Souveränität. Zwar bietet Zoom mit „Zoom X“ eine Lösung mit Serverstandorten in Deutschland und in den Niederlanden, doch bleibt unklar, wie sich das Produkt in Zukunft weiterentwickeln könnte – ohne dass es zu Lock-in-Effekten beispielsweise durch die sehr leistungsfähigen KI-Funktionen kommt, insbesondere bei der Live-Untertitelung. Auf der anderen Seite wird die monatliche Zoom-Open-Hour von Nutzenden sehr positiv wahrgenommen. Der Hersteller zeigt sich hier offen und bietet systematisch Feedback-Möglichkeiten an. So kann die Weiterentwicklung der Software zumindest indirekt von den am Wissenschaftsnetz teilnehmenden Einrichtungen mitgestaltet werden.

Die konkurrierenden quelloffenen Systeme (der Einsatz von Open-Source-Software gilt als ein wichtiger Aspekt bei dem Bestreben, digital souveräner zu werden) haben qualitativ deutlich aufgeholt und im Laufe der letzten Rahmenvertragslaufzeit auch gravierende technische Neuerungen erfahren. So kann BigBlueButton mittlerweile auf die Video-Engine „LiveKit“ aufsetzen, was deutlich spürbare Verbesserungen in der Bild- und Tonqualität mit sich bringt. OpenTalk wurde einem intensiven Refactoring unterzogen, was die Betriebsstabilität spürbar verbessert hat. Zu den bekannteren Open-Source-Anwendungen gehört auch Jitsi. Eine Videokonferenzsoftware, die im französischen Forschungsnetz RENATER bereits als Dienst „Rendez-Vous“ betrieben wird. In Deutschland ist Jitsi zwar über die OCRE-2024-Cloud-Rahmenverträge verfügbar, nicht aber über die DFN-Rahmenverträge.

Im Rahmen der Ausschreibung wurde bei den erweiterten Leistungsbeschreibungen beispielsweise Wert darauf gelegt, dass Open-Source-Anbieter die enge Zusammenarbeit zu den Softwareherstellern belegen können, um eine nachhaltige Entwicklung und einen zuverlässigen Betrieb der Services zu gewährleisten.

> Ein vielfältiges Angebot erhöht nicht nur die Auswahlmöglichkeiten, sondern auch die Ausfallsicherheit.

Im Zuge der Marktrecherche signalisierten alle bisherigen Anbieter innerhalb der aktuellen Rahmenverträge ihr Interesse, erneut teilzunehmen. Dies gilt auch für Unternehmen, die bislang wenig nachgefragt wurden – etwa die reflact AG mit Adobe Connect oder asknet mit Class Collaborate. Auch die DrVis Software GmbH wird erneut Microsoft Teams in die Ausschreibung einbringen. Für Einrichtungen, die Teams bisher kaum genutzt haben, könnte dies den Einstieg erleichtern, auch wenn nicht die gesamte Microsoft-Produktpalette zum Einsatz kommen soll.

Resilienz und Wettbewerb

Ein vielfältiges Angebot erhöht nicht nur die Auswahlmöglichkeiten, sondern auch die Ausfallsicherheit. Videokonferenzlösungen sind mittlerweile so essenziell, dass ein längerer Ausfall weitreichende Folgen für die Kommunikationsfähigkeit einer Einrichtung hat. Es gab bereits Fälle, in denen Einrichtungen mithilfe der DFN-Rahmenverträge kurzfristig auf alternative Systeme umsteigen konnten, etwa nach Cyberangriffen. Manche Organisationen haben sich inzwischen sogar bewusst ein „Zweitsystem“ gesichert. Zugleich wird diskutiert, ob Cloud-Strategien dauerhaft Bestand haben oder ob durch den Fortschritt bei Containertechnologien und wachsendes Know-how im IT-Nachwuchs On-Premises-Lösungen wieder attraktiver werden.

Perspektiven und Ausblick

Im Mittelpunkt der aktuellen Ausschreibung steht die Etablierung eines nachhaltigen Dienstangebots. Das übergeordnete Ziel ist es, Vielfalt und Wettbewerb zu gewährleisten, die digitale Souveränität zu fördern und dabei sowohl wirtschaftliche Rahmenbedingungen als auch die technologische Weiterentwicklung zu berücksichtigen. Noch stärker als vor vier Jahren erwarten Hochschulverwaltungen, dass Anbieterwechsel möglich sind und dass der größer werdende Funktionsumfang der Dienste die verfügbaren finanziellen Budgets der Einrichtungen nicht überlastet. Ab März 2026 werden die neuen DFN-Rahmenverträge für Cloud-Videodienste voraussichtlich zur Verfügung stehen – als Grundlage für eine vielfältige, souveräne und widerstandsfähige Videokommunikation. ◆

Kurzmeldungen

Neue X-WiN-Außenanbindung: direktes Peering mit dem polnischen Forschungsnetz PCSS

Die Außenanbindungen des Wissenschaftsnetzes X-WiN werden kontinuierlich auf Auslastung und Verkehrsflüsse überwacht sowie im Austausch mit Netzbetreibern strategisch weiterentwickelt. Im September 2025 konnte der DFN-Verein gemeinsam mit dem benachbarten polnischen Forschungsnetz PCSS (Poznańskie Centrum Superkomputerowo-Sieciowe) eine direkte Peering-Verbindung mit einer Anschlussbandbreite von 100 Gbit/s zwischen beiden Wissenschaftsnetzen erfolgreich in Betrieb nehmen.

Die Glasfaserstrecke führt über die Cross-Border-Verbindung zwischen Frankfurt (Oder) und Słubice. Die Europa-Universität Viadrina Frankfurt (Oder) stellt einen Teil dieser Trasse bereit.

Ziel der sogenannten Private Network Interconnections (PNIs) – damit ist die direkte Kopplung von Routern zweier Peering-Partner gemeint – ist unter anderem eine sichere und performante Verbindung, die Latenz und Paketverluste reduziert. Mittels direkter Peerings lassen sich die Verfügbarkeit und Antwortzeiten noch einmal erheblich verbessern. In erster Linie geht es jedoch vor allem um eine Erhöhung der Resilienz und Ausfallsicherheit. Bei einer Störung oder einem Ausfall einzelner Verbindungen entstehen so weniger und im Idealfall gar keine Einschränkungen für die Teilnehmer am X-WiN.

Die neue Anbindung an das polnische Forschungsnetz PCSS ergänzt den bestehenden Übergang zum europäischen Forschungsnetz GÉANT. Dieses verbindet die nationalen Forschungsnetze (National Research and Education Networks, NRENs) in Europa miteinander und schafft die Anbindung an weltweite Forschungsnetze. Neben den bestehenden GÉANT-Anschlüssen des X-WiN mit einer Gesamtkapazität von 800 Gbit/s steht nun ein zusätzlicher Übertragungsweg bereit.

Der DFN-Verein optimiert die Außenanbindungen des X-WiN stetig mit zusätzlichen direkten Peerings. In diesem Rahmen sind weitere Peerings mit anderen nationalen Forschungsnetzen bereits in Vorbereitung. ◆

Verbindung über Grenzen hinweg: Stadtbrücke zwischen Frankfurt (Oder) und Słubice | *Foto: Winfried Mausolf*

DFN-Fernsprechen: Neues Dienstportal verfügbar

Nach einer erfolgreichen Pilotphase ist das neue Dienstportal für DFN-Fernsprechen jetzt für alle teilnehmenden Einrichtungen am Dienst verfügbar. Der Roll-out erfolgt in zwei Phasen: Einrichtungen mit Abruf von Einzelverbindungsnachweisen (EVN) oder PDF-Rechnungen wurden zentral aktiviert. Die jeweiligen Ansprechpersonen erhielten hierzu eine E-Mail mit der Erläuterung der notwendigen Schritte. Alle weiteren Einrichtungen werden nun nach Bedarf sukzessive freigeschaltet.

Das neue Portal bietet eine übersichtliche Struktur und ermöglicht die bequeme Verwaltung dienstrelevanter Daten im Selfservice. Dazu gehören:

- die Darstellung des Anschlussbestands inklusive der Anschlussdetails
- Zugriff auf aktuelle und archivierte Rechnungen
- die Verwaltung der Stammdaten (Adressen, Rechnungsinformationen, betriebliche Ansprechpersonen, Missbrauchskontakte)
- Anzeige von Einzelverbindungsnachweisen (EVN)

Darüber hinaus ist eine Reihe neuer Funktionen geplant, von denen einige bereits getestet werden und in Kürze zur Verfügung stehen –, darunter die Abbildung des Auftragsmanagements im Portal und die Bestellung und Nachverfolgung der verschiedenen Leistungsarten von DFN-Fernsprechen.

Der Dienst DFN-Fernsprechen bietet Voice-over-IP (VoIP)-basierte Anschlussarten, die speziell auf die Anforderungen von Wissenschaft und Forschung zugeschnitten sind und auf dem Wissenschaftsnetz X-WiN aufbauen. Neben dem klassischen VoIP-Anschluss für lokal betriebene Telefonanlagen stehen auch die Cloud-Telefonanlage VoIP-Centrex, Mobilfunk und SMS-Gateway zur Verfügung. ◆

Vergabeverfahren für neue Mobilfunk-Rahmenverträge gestartet

Nach einer intensiven Markterkundung wurde im September 2025 das Vergabeverfahren für neue Mobilfunk-Rahmenverträge veröffentlicht. Diese werden voraussichtlich ab März 2026 zur Verfügung stehen. Ziel der Neuausschreibung ist es, bis zu drei Rahmenverträge mit unterschiedlichen Netzbetreibern anzubieten. So haben teilnehmende Einrichtungen im Wissenschaftsnetz die Möglichkeit, nach individuellem Bedarf auszuwählen. Der derzeit gültige Rahmenvertrag mit Vodafone zur Beschaffung von Mobilfunkanschlüssen endet im Februar 2026.

Der Dienst DFN-Fernsprechen schafft Voraussetzungen, um perspektivisch auch den Mobilfunkdienst in die Konvergenz unterschiedlicher Kommunikationssysteme und -netze (Datennetze, Fernsprechnetze, Mobilfunknetze etc.) einzubeziehen. Mit entsprechenden Rahmenverträgen, die auf Forschung und Lehre abgestimmt sind, können DFN-Teilnehmer komfortabel und sicher Sprach-, Nachrichten- und Datenübertragung nutzen. ◆

Kontakt: Haben Sie Fragen zum neuen Dienstportal oder zum DFN-Dienst Fernsprechen? Wir helfen gerne weiter: **fernsprechen@dfn.de**

Auf dem Weg ins Fediverse

Infrastruktur für die Wissenschaft: Mit seinem Pilotprojekt, eine eigene Mastodon-Instanz aufzubauen und zu betreiben, zeigt das Karlsruher Institut für Technologie (KIT), welche Chancen das Fediverse für Forschung und Lehre bietet – und warum andere Hochschulen diesem Beispiel folgen sollten.

Text: **Jan Kröger, David Lohner, Ulrich Weiß**
(Karlsruher Institut für Technologie, KIT)

Von der Idee zum erfolgreichen Gemeinschaftsprojekt: Vor dem Aufbau der eigenen Mastodon-Instanz war das Karlsruher Institut für Technologie (KIT) bereits seit mehreren Jahren mit einem – im Vergleich zu anderen Universitäten recht reichweitenstarken – Profil auf der Instanz mastodon.social vertreten. Auch einzelne Institutionen des KIT waren mit eigenen Accounts auf verschiedenen Instanzen aktiv. Heute, mehr als zwei Jahre später, bietet der Dienst social.kit.edu diesen Institutionen ein eigenes digitales Zuhause im Fediverse. Betreut wird die KIT-Instanz von einem engagierten Moderationsteam, mit tatkräftiger technischer Unterstützung des Scientific Computing Center (SCC).

Foto: f16-iso100/freepik

Starke Infrastruktur für die Wissenschaft

Als Gegenangebot zu den etablierten, zentralisierten und algorithmen-getriebenen Social-Media-Plattformen – deren Intransparenz und einseitige Kontrolle über Kommunikationsräume inzwischen deutlich demokratiefeindliche Tendenzen schüren – ist das Fediverse, insbesondere der Microblogging-Dienst Mastodon, ein geeignetes Netzwerk für Wissenschaftskommunikation. Wissenschaft braucht für den globalen Austausch eine Infrastruktur jenseits der Aufmerksamkeitsökonomie, die offen, interoperabel und nutzerzentriert ist.

Jennifer Heck, Zentrum für Mediales Lernen (ZML): „Wir sind auf Mastodon, weil wir es großartig finden, dass das KIT mit social.kit.edu eine eigene, offene Plattform bereitstellt. So können wir uns in einem datenschutzfreundlichen Umfeld über digitale Lehre austauschen und gleichzeitig die Idee des föderierten, werbefreien Austauschs unterstützen."
@zml_kit@social.kit.edu

Ein Netz ist nur mit vielen Knoten (Instanzen) stabil. Darum war es dem Moderationsteam wichtig, eine eigene Mastodon-Instanz zu betreiben, die mit vielen anderen Instanzen (auch aus dem akademischen Umfeld) vernetzt ist. Dank der Rückendeckung von Prof. Dr. Kora Kristof, KIT-Vizepräsidentin für Digitalisierung und Nachhaltigkeit, kann das KIT seinen Angehörigen mit dieser Instanz heute einen Service anbieten, dem sie vertrauen können: Mastodon ist wegen des Inhouse-Hostings datenschutzfreundlich. Durch einen internen Freigabeprozess bzw. die künftige Anbindung an das Identity-Management-System (IDM) sind außerdem alle Profile verifiziert.

Als ersten praktischen Schritt konsultierte das Moderationsteam, ganz im Sinne des Fediverse, die Admin-Teams anderer Mastodon-Instanzen – speziell im akademischen Bereich. Mit großer Offenheit gewährten diese Einblicke in ihren Maschinenraum. Die dort eingesetzten Ressourcen und Infrastrukturen ließen erkennen, dass der nötige Software-Stack und die Hardwareanforderungen für ein universitäres Rechenzentrum kein Problem sind. Auch der eigentliche Moderationsaufwand wurde als gering eingeschätzt. Die anschließende Machbarkeitsanfrage beim SCC stieß daher auf offene Ohren. Ideelle Unterstützung erhielt das Mastodon-Team zudem von Prof. Dr. Annette Leßmöllmann, einer renommierten Kommunikationswissenschaftlerin des KIT, die das Vorhaben auch aus wissenschaftlicher Sicht befürwortete. Dass es überhaupt ein Interesse an der Idee gibt, zeigte sich ganz deutlich bei der Vorstellung des Projekts in der internen KIT-Arbeitsgruppe Kommunikation. Viele Mitglieder signalisierten, ihre bestehenden Mastodon-Profile auf die neue hauseigene Instanz umzuziehen oder sogar neue Profile anzulegen. Mit diesem Rückenwind und einem Umsetzungsplan in der Tasche holte sich das Projektteam beim Präsidium des KIT den Auftrag für die Realisierung.

Start des Pilotbetriebs

Nachdem erste Versuche mit einer internen Testinstanz recht vielversprechend waren, machte sich das Team an die nötigen Anpassungen. Spätestens jetzt zeigte sich, wie wichtig die Übernahme konkreter Verantwortung ist: Wer kümmert sich um das Verfassen und Abstimmen von Serverregeln, Nutzungsbestimmungen und die Datenschutzerklärung? Wer publiziert die Anleitungen? Auch wenn das Moderationsteam dabei auf den Schultern von Riesen stand, sind es am Ende die vielen kleinen Aufgaben und Entscheidungen, die einen langen Atem erfordern. Für viele dieser (juristisch erforderlichen) Texte gibt es zur Unterstützung offen lizenzierte Textbausteine im Netz, beispielsweise von der Stiftung Datenschutz.

Der offizielle Startschuss für die neue Instanz fiel schließlich am 1. Juli 2025 mit einem Launch-Event. Recht großes Interesse an der Instanz erzeugte ein Beitrag im internen Newsletter. Innerhalb weniger Tage erkundigten sich zahlreiche Mitarbeitende, wie sie einen Account auf der neuen Plattform erstellen können.

WAS IST MASTODON?

Mastodon ist eine gemeinnützige und datenschutzfreundliche Social-Media-Plattform zur Verbreitung von kurzen Nachrichten. Der Microblogging-Dienst ist Teil des sogenannten Fediverse, einem Zusammenschluss quelloffener, dezentraler, nicht kommerzieller und datenschutzfreundlicher Dienste, die über das freie und standardisierte Protokoll ActivityPub miteinander kommunizieren. Personen oder Einrichtungen haben die Möglichkeit, in Mastodon einen Server anzulegen, eine sogenannte Instanz.

Seit September 2025 bietet der Hersteller Mastodon gGmbH für Organisationen einen Hostingservice für Mastodon-Instanzen an.
https://joinmastodon.org/de/hosting

mastodon

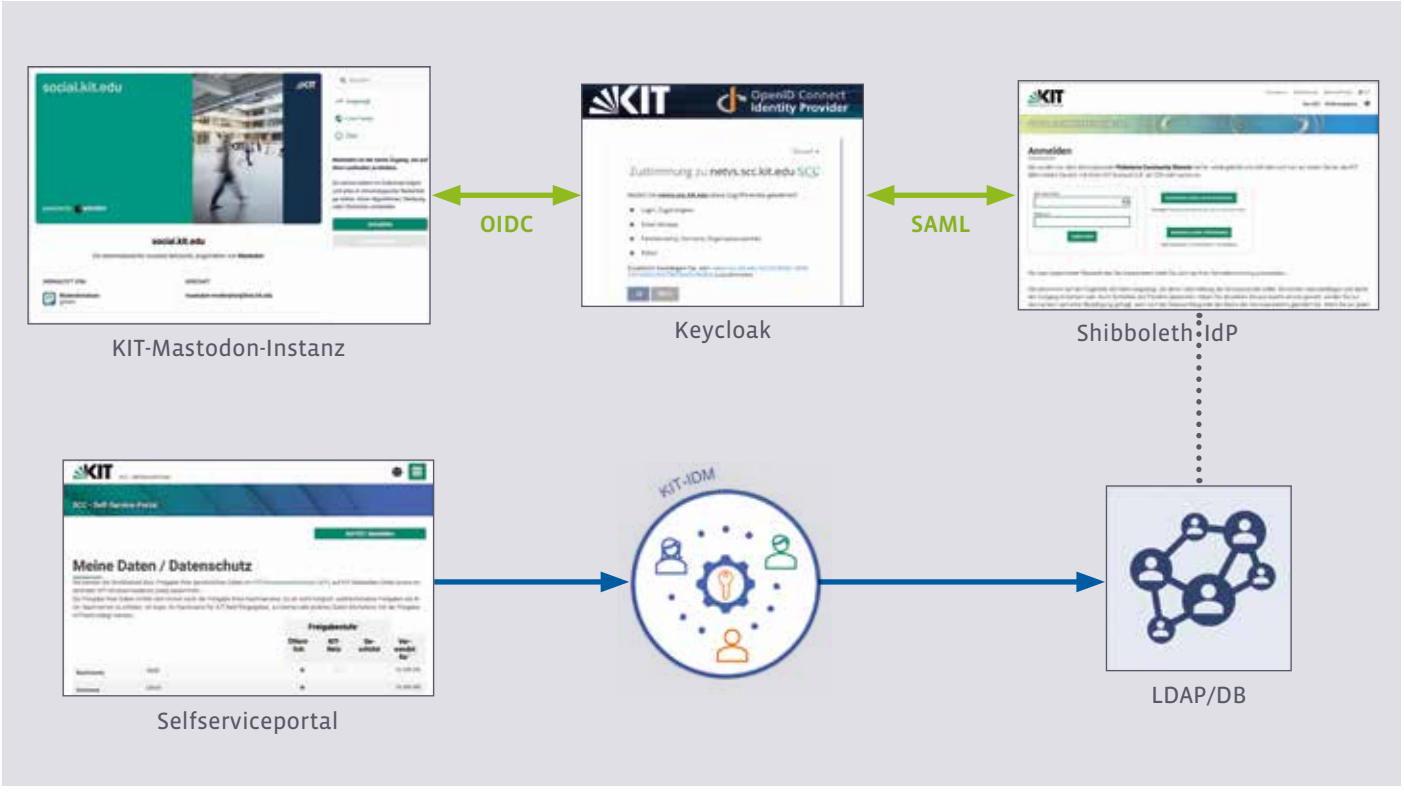
Die Mastodon-Instanz läuft zunächst in einem einjährigen Pilotbetrieb, damit das Team – dem Beispiel der Universität Innsbruck folgend – erst einmal Erfahrungen mit einer geringeren Anzahl an Profilen sammeln kann. Diese Profile können derzeit ausschließlich Institutionen und Projekte des KIT anlegen. In einem nächsten Schritt soll die Instanz für alle Mitarbeitenden geöffnet werden.

Andrea Gappel, KIT-Bibliothek: „Wir möchten unsere Services, Angebote und Neuigkeiten Forschenden, Studierenden sowie allen, die sich für Wissenschaft begeistern, zugänglich machen. Im Fediverse finden wir genau diese Vielfalt und Offenheit. Mit dem Umzug auf die KIT-Instanz unterstreichen wir unsere Zugehörigkeit zum KIT und stärken den direkten Austausch innerhalb der KIT-Community."
@KIT_Bibliothek@social.kit.edu

Herausforderungen und Fragen

Mit dem Anbieten einer öffentlichen Kommunikationsplattform gehen die Betreibenden einer Instanz Verpflichtungen ein. Der Personalrat gab zu bedenken, dass es möglicherweise arbeitsrechtliche Konsequenzen haben könnte, wenn auf einer Instanz für vorrangig dienstliche Kommunikation (so die Regel) jemand mehrheitlich private Inhalte postet. So könne es, selbst wenn die Betreibenden keine diesbezüglichen Sanktionen vorsehen, in Einzelfällen dennoch zu rechtlichen Auseinandersetzungen kommen. Solche und andere Regelverstöße muss das Moderationsteam prüfen – und dabei sicherstellen, dass die Serverregeln zeitnah durchgesetzt werden können. Dazu gehört es auch, schnell auf Meldungen von Nutzenden sowie behördliche Anfragen reagieren zu können. Denn die gesetzlich per Digital Services Act (DSA) der EU festgelegte Moderationsaufgabe des „notice and takedown" muss umgehend erfüllt werden. Die Erfahrungen anderer Instanzen zeigen jedoch, dass Eingriffe bei Rechts- und Regelverstößen in der Praxis äußerst selten sind. Bevor die Instanz für individuelle Nutzende geöffnet wird, klärt das Moderationsteam derzeit weitergehende Haftungsfragen im Fall von Rechtsverstößen und die damit verbundenen

Ressourcen der Instanz social.kit.edu Native Installation auf VM mit Ubuntu, 4 CPU, 8 GB RAM, 150 GB SSD, Anbindung S3-Speicher für Daten und Dokumente



Konfiguration/Festlegung eines persönlichen Mastodon Handles im Selfservice. Provisionierung des Handles und weiterer Attribute via IDM zum Shibboleth IdP. Beim SSO autorisiert der Keycloak dann nur Nutzende, die ein Mastodon-Handle gesetzt haben

Prozesse und Verantwortlichkeiten. Weil solche Abstimmungen Zeit benötigen, ist es sinnvoll, Personalrat und Justiziariat von Anfang an einzubinden.

Anmeldung mit bekannten Zugangsdaten

Die für das Single Sign-On nötige Anbindung an das IDM realisiert routiniert das SCC-Team, das dafür aber eine eindeutige User-Kennung braucht. Für einen Mastodon-Profilnamen ist der im KIT gängige Account (Buchstaben-Zahlen-Kürzel) viel zu unpersönlich, Namen wiederum für das IDM zu fluide. Dafür fand das SCC-Team eine gute Lösung: Es programmierte kurzerhand eine Erweiterung für das hiesige Nutzerportal. Diese erlaubt es Interessierten künftig, sich ein selbst gewähltes, dauerhaftes und regelkonformes Handle zu geben, das bei Anmeldung durch das IDM an Mastodon übergeben wird. So werden sich Nutzende mit ihren bekannten Zugangsdaten auf der Mastodon-Instanz des KIT anmelden können – wie auch bei allen anderen zentralen Diensten.

Thomas Griesbaum, Sebastian Schäfer, Isabel Häuser, Kommunikationsteam der KIT-Fakultät für Informatik: „Die Idee einer dezentralen, werbefreien und datenschutzfreundlichen Plattform, die offenen Austausch ermöglicht und unabhängig von Konzerninteressen ist, überzeugte uns im Grundsatz bereits von Anfang an. Der Besitzerwechsel bei Twitter/X im Jahr 2022 gab den Ausschlag, einen eigenen Mastodon-Account einzurichten – zunächst auf bawü.social. Mit dem Start von social.kit.edu war der Wechsel zur eigenen Heiminstanz für uns dann der logische nächste Schritt."
@KITInformatik@social.kit.edu

Das Fediverse und seine Möglichkeiten für die Wissenschaft

Nach der Freischaltung der Instanz für alle Mitarbeitenden möchte das Moderationsteam in einem nächsten Schritt die Möglichkeiten des ActivityPub-Protokolls im Kontext der Wissenschaftskommunikation weiter ausloten. So ließe sich beispielsweise der persistente Personenidentifikator ORCID mit dem eigenen Mastodon-Profil verknüpfen, um Follower automatisiert auf eigene Publikationen hinzuweisen. Der Dienst Encyclia (https://encyclia.pub/) und andere Dienste im Fediverse wie Pixelfed für Bilder oder Loops für Kurzvideos bieten als digitale Infrastrukturen ein enormes Potenzial für die Wissenschaftskommunikation. Andere Dienste, die das AcitityPub-Protokoll unterstützen, bieten unter Umständen ähnliche Möglichkeiten für die Bereiche Forschungsdaten oder Bildungsressourcen.

Die Installation einer Mastodon-Instanz an einer öffentlichen Hochschule braucht einen langen Atem. Viele Stakeholder und Verantwortliche müssen teils überzeugt und für die Mitarbeit gewonnen werden – möglicherweise müssen andere Aufgaben dafür zeitweise zurückgestellt werden. Doch die anfänglichen, meist überschaubaren Hürden und Risiken lassen sich gemeinsam gut meistern. Neben der engagierten Mithilfe von internen wie externen Kolleginnen und Kollegen sowie der Verteilung der Arbeit auf mehrere Schultern erleichterte außerdem die befristete Pilotierung mit Ausstiegsoption das ganze Vorhaben.

Fazit

Ohne die Erfahrungen und die tatkräftige Unterstützung der Admins anderer Instanzen wäre das Projekt sicher nicht ins Ziel gekommen. Das Moderationsteam pflegt inzwischen einen regen Austausch mit den Fediverse-Akteuren und freut sich auf Zuwachs in der Runde der Hochschulen, die Mastodon-Instanzen betreiben! ◆

QUELLE: STIFTUNG DATENSCHUTZ

Datenschutz bei Mastodon – Leitfaden für den Instanz-Betrieb im dezentralen Netzwerk sowie eine Checkliste, Musterdokumente und Informationen zur praktischen Umsetzung.
https://stiftungdatenschutz.org/praxisthemen/datenschutz-bei-mastodon

KONTAKT

Wer Fragen hat oder sich mit der AG „Academia into the Fediverse" austauschen möchte, kann das Moderationsteam der KIT-Instanz unter der E-Mail-Adresse **mastodon-moderation@lists.kit.edu** erreichen.

Gemeinsam arbeiten, lernen und forschen – in der Academic Cloud

Die Academic Cloud unterstützt Hochschulen und Forschungseinrichtungen mit einer Vielzahl digitaler Werkzeuge. Derzeit greifen bereits über 250 000 Nutzende aus rund 400 Einrichtungen auf die Plattform zu. Ab 2026 ist die Academic Cloud durch ein transparentes Kostenmodell noch einfacher nutzbar und steht teilnehmenden Einrichtungen am Wissenschaftsnetz auch über die föderierten Clouddienste des DFN-Vereins zur Verfügung.

Text: **Max Scheid** (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen, GWDG)

Seit ihrer Einführung vor sieben Jahren hat sich die Academic Cloud stetig weiterentwickelt. Heute bietet sie Hochschulen und Forschungseinrichtungen in ganz Deutschland eine leistungsstarke und datenschutzkonforme Plattform für digitales Arbeiten, Lernen und Forschen. Die Academic Cloud entstand aus der steigenden Nachfrage nach einer hochschulübergreifenden Plattform. Dabei wurde deutlich, dass vorhandene Dienste der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) – dem gemeinsamen Rechen- und IT-Kompetenzzentrum der Georg-August-Universität Göttingen und der Max-Planck-Gesellschaft – auch für andere Einrichtungen interessant sind. Entsprechende Anfragen und Rückmeldungen führten zu der Idee, diese Angebote strukturiert zu bündeln und übergreifend zugänglich zu machen.

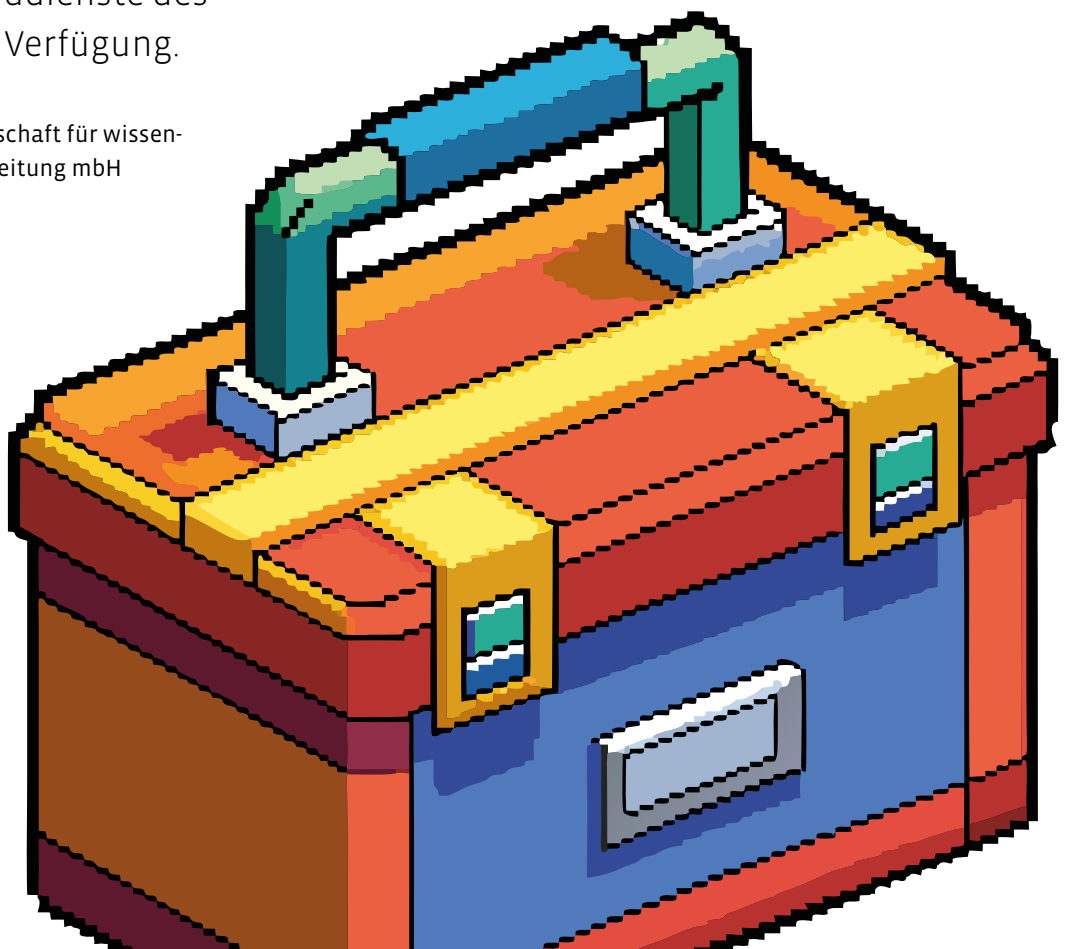


Foto: liudmilashagieva/FreePik

Auf dieser Grundlage initiierte die GWDG 2018 die Academic Cloud, die zunächst aus eigenen Ressourcen aufgebaut und betrieben wurde. Zusätzlich förderte das Niedersächsische Ministerium für Wissenschaft und Kultur (MWK) die Initiative. In Kooperation mit dem Landesarbeitskreis Niedersachsen für Informationstechnik/Hochschulrechenzentren (LANIT) wurde das Vorhaben hochschulübergreifend abgestimmt und umgesetzt. Ein zentrales Merkmal der Plattform ist von Beginn an das Log-in mittels Single Sign-on (SSO), das Nutzenden mit nur einer Anmeldung Zugriff auf alle freigeschalteten Dienste ermöglicht und somit die Nutzung komfortabel und sicher gestaltet.

Ausbau des Dienstportfolios

Seit ihrem Start ist die Academic Cloud kontinuierlich gewachsen. Bis heute wurden sowohl bestehende Angebote weiterentwickelt als auch zahlreiche neue Dienste ergänzt. Dazu zählen beispielsweise *Jupyter* für interaktives Coding, *Pad* für kollaboratives Schreiben in Echtzeit oder *Meet*, ein Videokonferenzsystem mit Funktionen wie Whiteboards, Breakout-Räumen und gemeinsamen Notizen, die digitale Lehre und Zusammenarbeit unterstützen.

In jüngerer Zeit sind zudem KI-gestützte Anwendungen ein wichtiger Bestandteil des Angebots geworden. Die Nachfrage ist hoch – nicht zuletzt deshalb, weil sie datenschutzkonform betrieben werden und unterschiedliche praktische Einsatzfelder abdecken. Mit *Chat AI* lassen sich Large Language Models (LLMs) wie *Llama*, *DeepSeek* oder *Mistral* über eine einfache Chatoberfläche nutzen. Parameter wie Antwortstil oder System-Prompts können angepasst werden, was den Vergleich unterschiedlicher Modelle, die gezielte Steuerung von Antworten oder Einblicke in die Arbeitsweise von LLMs ermöglicht. Mittels RAG-System (Retrieval-Augmented Generation) lassen sich Informationen aus benutzerdefinierten verschlüsselten Dokumentensammlungen (Arcanas) extrahieren, auf deren Grundlage LLMs ihre Antworten generieren. Das RAG-System der Academic Cloud unterstützt Text-, Markdown- und PDF-Dateien. Der Dienst *Voice AI* ermöglicht die Transkription und Übersetzung von Audiodateien. Darüber hinaus kann er in Verbindung mit dem Videokonferenz-Tool *Meet* eingesetzt werden, um in Meetings live mehrsprachige Untertitel zu erstellen und damit das gemeinsame Arbeiten über Sprachgrenzen hinweg zu erleichtern. Mit *Image AI* können außerdem Bilder aus Texteingaben generiert werden. Die Bedienung erfolgt ebenfalls über eine einfache Weboberfläche, sodass sich Ideen schnell und ohne technisches Vorwissen oder hohe Einstiegshürden umsetzen lassen.

Modular, nachhaltig und fair – das neue Preismodell

Das neue Preismodell der Academic Cloud basiert auf einem modularen Baukastensystem. Ziel ist es, die langfristige Verfügbarkeit der Plattform sicherzustellen und gleichzeitig eine transparente sowie faire Abrechnung für alle Einrichtungen zu ermöglichen.

Academic Cloud Basis
Das Basismodul bildet die Grundlage für den Zugang zur Academic Cloud. Es umfasst zentrale Funktionen wie den Authentifizierungsdienst mit verfügbarer Multi-Faktor-Authentifizierung, ein Selfservice-Portal für Nutzende sowie ein Administrationsportal für die Verwaltung von Accounts, Rollen und Berechtigungen. Im Basismodul enthalten sind darüber hinaus einige hilfreiche, kleinere Dienste wie das kollaborative Notizbuch *Pad* und das soziale Netzwerk *Mastodon*.

Kern des Systems ist die Academic ID, das universelle Benutzerkonto der Academic Cloud. Mit ihr können sich Angehörige einer Einrichtung bei allen freigeschalteten Diensten anmelden. Über die Academic ID behalten Nutzende zudem den Überblick über die von ihnen verwendeten Dienste und können persönliche Daten und Sicherheitseinstellungen verwalten.

Nutzende aus den teilnehmenden Einrichtungen können sich unkompliziert über die DFN-AAI mit den gewohnten Zugangsdaten ihrer Heimatinstitution bei der Academic Cloud anmelden.

Um die Zusammenarbeit mit Partnerinnen und Partnern außerhalb der eigenen Institution zu erleichtern und wissenschaftliche Kooperationen über Einrichtungsgrenzen hinweg zu fördern, stellt die Academic Cloud ein Gästemanagement im Administrationsportal sowie die Möglichkeit zur Selbstregistrierung einer Academic ID für Gäste bereit. Externe Personen können so unkompliziert eingebunden werden und erhalten Zugang zu den von der Einrichtung gebuchten oder bereitgestellten Diensten.

Als weiterer Bestandteil kann ein anpassbares Einstiegsportal eingesetzt werden, das auch die Einbindung von Diensten ermöglicht, die eine Einrichtung außerhalb der Academic Cloud betreibt. So entsteht für Nutzende ein zentraler und gebündelter Zugangspunkt zu allen verfügbaren Diensten. Durch die Kennzeichnung des jeweiligen Providers – sei es die GWDG, eine andere Hochschule oder Forschungseinrichtung im Rahmen des kooperativen Modells oder die eigene Institution – bleibt jederzeit transparent, wer den Dienst betreibt.

Individuell konfigurierbar – Dienste und Kontingente nach Bedarf
Über Academic Cloud Basis hinaus können zahlreiche weitere Dienste in der Academic Cloud genutzt werden, die verschiedenste Einsatzbereiche abdecken – von Kommunikation und Kollaboration bis hin zu Forschungsdatenmanagement und KI-gestützten Anwendungen. Eine Übersicht der im Basismodul enthaltenen sowie der flexibel hinzubuchbaren Dienste bietet die Tabelle. Die Preisgestaltung erfolgt über klar definierte Kontingente in insgesamt acht Stufen. Diese reichen vom kleinsten Kontingent für bis zu 30 Nutzende, etwa für Forschungsgruppen, über mittlere Größen mit bis zu 1 000 oder 3 000 Accounts für größere Institute oder Forschungseinrichtungen bis hin zu Kontingenten für ganze Hochschulen und Universitäten mit 30 000 oder mehr

TABELLE DER AKTUELLEN DIENSTE

Dienstname	Dienstbeschreibung
Pad	Kollaboratives Notizbuch
URL-Shortener	Dienst zum Kürzen von URLs
QR-Code-Generator	Dienst zum Erzeugen von QR-Codes
Filesender	Sicherer Datentransfer
Mastodon	Soziales Netzwerk
KI-Tools	Generative KI-Modelle wie Chat AI, Voice AI oder Image AI inkl. Open-Source-Modelle
KI-Modelle OpenAI	Zusätzliche Modelle von Open AI wie ChatGPT
Chemotion	Elektronisches Laborbuch
Cocalc	Coding & Data Analysis, LaTeX-Editor
eduVote	Audience-Response-Tool
Learn	Lernplattform auf Basis von Moodle
ePIC	Persistent Identifier-Dienst
Events	Eventmanagement auf Basis von Indico
Files	Sync & Share- und Cloud-Speicher-Dienst auf Basis von Nextcloud zum kollaborativen Editieren von Dokumenten
GitLab	Quellcode-Verwaltung
GitLab Premium	Quellcode-Verwaltung mit erweitertem Funktionsumfang
GRO.data	Forschungsdatenrepositorium
GRO.plan	Forschungsdatenmanagement
Hub	Soziales Netzwerk auf Basis von HumHub
Jupyter	Coding & Data Analysis
Mail	E-Mail auf Basis von Open-Xchange
Matrix	Föderierter Chat
Meet	Videokonferenzsystem
Projects	Projektmanagement auf Basis von OpenProject
ShareLaTeX	LaTeX-Editor
Survey	Online-Umfragen aus Basis von LimeSurvey
Stack	Computeralgebrasystem
Wekan	Projektmanagement
Whiteboard	Digitales Whiteboard
Wooclap	Audience-Response-Tool

Dienste im Academic-Cloud-Basismodul

Im Baukastensystem zubuchbare Dienste

Nutzenden. Durch die individuelle Wahl der Kontingentgröße pro Dienst lassen sich Kosten gezielt steuern und Ressourcen effizient einsetzen. Dabei gilt: Die Größe des Basismoduls muss stets mindestens der des größten zusätzlich gebuchten Dienstes entsprechen.

Bei einer Buchung über den DFN-Verein gilt eine einjährige Laufzeit mit automatischer Verlängerung. In diesem Rahmen ist die Academic Cloud über die föderierten Dienste in der DFN-Cloud verfügbar, was die Vertragsabwicklung für Einrichtungen deutlich vereinfacht.

Kooperatives Modell

Die Academic Cloud versteht sich nicht nur als technische Plattform, sondern auch als gemeinschaftliches Modell. Neben den von der GWDG betriebenen Diensten können Hochschulen und Forschungseinrichtungen eigene Anwendungen und Services einbringen und so allen Teilnehmenden zur Verfügung stellen. Einrichtungen, die sich mit Diensten beteiligen möchten, sind herzlich eingeladen, Kontakt mit der GWDG aufzunehmen. Auf diese Weise entsteht ein vielfältiges, kooperativ getragenes Portfolio, das Synergien schafft und Doppelstrukturen vermeidet. ◆

ACADEMIC CLOUD

Unter **academiccloud.de/services** finden Sie stets eine aktuelle Übersicht unserer Dienste.

Wenn Sie die Academic Cloud an Ihrer Einrichtung einsetzen möchten, kontaktieren Sie uns gerne unter: **anfrage@academiccloud.de**

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Burckhardtweg 4
37077 Göttingen

Kontakt
E-Mail: support@gwdg.de
Telefon: +49 551 39-30000

Schritt für Schritt zur digitalen Barrierefreiheit – das SHUFFLE-Reifegradmodell

Barrierefreie digitale Angebote sind der Schlüssel zu Chancengleichheit und ein Qualitätsmerkmal für gute Lehre. Trotz eindeutiger rechtlicher Vorgaben wird die Barrierefreiheit an deutschen Hochschulen bislang sehr unterschiedlich umgesetzt. Und genau hier setzt das SHUFFLE-Reifegradmodell an: Das Selbstbewertungstool hilft Einrichtungen, die eigene Barrierefreiheit realistisch einzuschätzen und systematisch Schritt für Schritt umzusetzen.

Text: **Nadine Auer, Gottfried Zimmermann** (Hochschule der Medien, Stuttgart),
Ann-Katrin Böhm (Pädagogische Hochschulen Heidelberg und Freiburg),
Hakan Ali Cetin (Pädagogische Hochschule Freiburg),
Anja Gutjahr (Pädagogische Hochschule Heidelberg)

Die Realität an deutschen Hochschulen ist geprägt von Vielfalt – doch die Bildungswege sind noch nicht für alle gleichermaßen zugänglich. Studierende mit studienerschwerenden Beeinträchtigungen sind eine wachsende Gruppe, deren Bedürfnisse verstärkt in den Fokus von Hochschulpolitik und -entwicklung rücken müssen. Ihr Anteil hat sich in den vergangenen zehn Jahren von acht auf sechzehn Prozent verdoppelt, der Anteil der Studierenden mit psychischen Erkrankungen sogar verdreifacht. Wie gut sind unsere Hochschulen auf diese Entwicklung vorbereitet – und wie können sie ihre Verantwortung für einen chancengerechten Zugang aktiv wahrnehmen? Wie steht es insbesondere um die digitale Barrierefreiheit? Wissen Hochschulen, wo digitale Hürden den Zugang zu Bildung erschweren oder gar verhindern?

Digitale Barrieren entstehen dort, wo Informationen im digitalen Raum nicht selbstständig und diskriminierungsfrei erfahrbar sind und damit eine gleichberechtigte Teilhabe verwehrt wird. Im Hochschulkontext bedeutet dies, dass sämtliche digitalen Angebote – von Lernplattformen über PDFs, Videos und Websites bis hin zu Prüfungssoftware – unabhängig von körperlichen, sensorischen oder psychischen Beeinträchtigungen uneingeschränkt nutzbar sein müssten. Trotz klarer rechtlicher Vorgaben wie WCAG und BITV 2.0 existiert an deutschen Hochschulen jedoch bislang kein einheitlicher Stand in der Umsetzung digitaler Barrierefreiheit. Dabei ist sie eine wesentliche Voraussetzung für Bildungsgerechtigkeit und ein zentrales Qualitätsmerkmal guter Lehre.

Genau hier setzt das Projekt SHUFFLE an. Mit Förderung der „Stiftung Innovation in der Hochschullehre“ wurde in einem Teilprojekt, an dem Mitarbeitende aller Projekthochschulen beteiligt waren, das SHUFFLE-Reifegradmodell entwickelt. Es unterstützt Hochschulen dabei, systematisch zu analysieren, in welchem Maß digitale Barrierefreiheit bereits umgesetzt werden kann. Indem es Stärken und Schwächen sichtbar macht und zugleich konkrete Handlungsschritte benennt, schafft das Modell Orientierung, Transparenz und Motivation – und weist Hochschulen den Weg, ihre digitalen Angebote Schritt für Schritt inklusiver zu gestalten.

Warum ein Reifegradmodell?

Reifegradmodelle haben ihren Ursprung in der Wirtschaft und der IT. Bekannte Beispiele finden sich etwa in der Softwareentwicklung oder im Qualitätsmanagement, wo sie seit Jahrzehnten eingesetzt werden, um Entwicklungsprozesse zu strukturieren und Organisationen bei ihrer Weiterentwicklung zu begleiten. Die Grundidee ist

stets, den aktuellen Stand einer Organisation in einem bestimmten Bereich messbar zu machen, ihn in Stufen einzuordnen und daraus abzuleiten, welche nächsten Schritte sinnvoll und realistisch sind. So verbinden Reifegradmodelle Diagnose und Entwicklungsplanung und schaffen einen klaren Rahmen, um komplexe Prozesse nachvollziehbar zu machen.

Auch an deutschen Hochschulen zeigt sich, wie hilfreich ein solches Instrument sein kann. Denn der Stand der Umsetzung digitaler Barrierefreiheit variiert erheblich: Während einige Hochschulen bereits über umfassende Angebote, feste Strukturen und Schulungen verfügen, stehen andere noch ganz am Anfang. Um in dieser Heterogenität Entwicklungsprozesse anzustoßen, bietet sich ein Selbstbewertungstool an. Es erlaubt den Hochschulen, ihren Status quo realistisch einzuschätzen, ohne dass eine externe Bewertung notwendig ist:

- → **Orientierungshilfe:** Hochschulen erkennen auf einen Blick, wo sie aktuell stehen.
- → **Entwicklungsinstrument:** Handlungsfelder werden sichtbar, Fortschritte messbar.
- → **Handlungsempfehlungen:** Das Modell gibt konkrete Vorschläge, wie einzelne Bereiche gezielt verbessert werden können.
- → **Transparenz:** Fortschritte lassen sich dokumentieren und kommunizieren – sowohl innerhalb der Hochschule als auch gegenüber hochschulübergreifenden Gremien.

Kurz gesagt: Das SHUFFLE-Reifegradmodell macht die komplexe Aufgabe der digitalen Barrierefreiheit greifbar, ohne zu überfordern. Es übersetzt ein abstraktes Querschnittsthema in nachvollziehbare Entwicklungsstufen und ermutigt Hochschulen, systematisch und Schritt für Schritt inklusiver zu werden.

Aufbau und Anwendung des SHUFFLE-Reifegradmodells

Das SHUFFLE-Reifegradmodell betrachtet Hochschulen aus vier zentralen Perspektiven – den Dimensionen:

1. **Struktur** – Wie ist die Hochschule organisatorisch aufgestellt, welche Zuständigkeiten und Prozesse bestehen?
2. **Strategie** – In welchem Maß ist digitale Barrierefreiheit in Leitbildern, Entwicklungsplänen und Steuerungsinstrumenten verankert?
3. **Beratung und Support** – Welche Unterstützungsangebote gibt es für Studierende und Lehrende, um Barrieren im digitalen Raum abzubauen?
4. **Lehren und Lernen** – Wie barrierefrei werden digitale Lehr- und Lernmaterialien gestaltet und eingesetzt?

Diese Dimensionen gliedern sich in insgesamt 19 Handlungsfelder, die für digitale Barrierefreiheit an Hochschulen besonders relevant sind. Jedes Handlungsfeld wird anhand einer präzisen Leitfrage untersucht – etwa das Handlungsfeld „Steuerungsinstrumente“: *„Inwieweit wird die (digitale) Barrierefreiheit der Hochschule in Steuerungsinstrumenten explizit als Ziel thematisiert?“*

Die Antworten führen zu einer Einordnung in eine von fünf Reifegradstufen:

Abbildung 1: Stufen des SHUFFLE-Reifegradmodells

Für jede Ausprägung gibt es praxisnahe Beispiele und qualitative Kriterien, die eine realistische Einordnung erleichtern. Darüber hinaus besteht die Möglichkeit, die Einstufung zu begründen und weitere relevante Informationen anzumerken – dies erleichtert sowohl die Nachvollziehbarkeit als auch ein kollaboratives Arbeiten mit dem Reifegradmodell.

Das Ergebnis wird in einer Netzstruktur visualisiert, die auf einen Blick zeigt, in welchen Bereichen die Hochschule bereits stark aufgestellt ist und wo noch Entwicklungspotenzial besteht.

Das Modell kann auf zwei Arten eingesetzt werden: derzeit als Matrix in

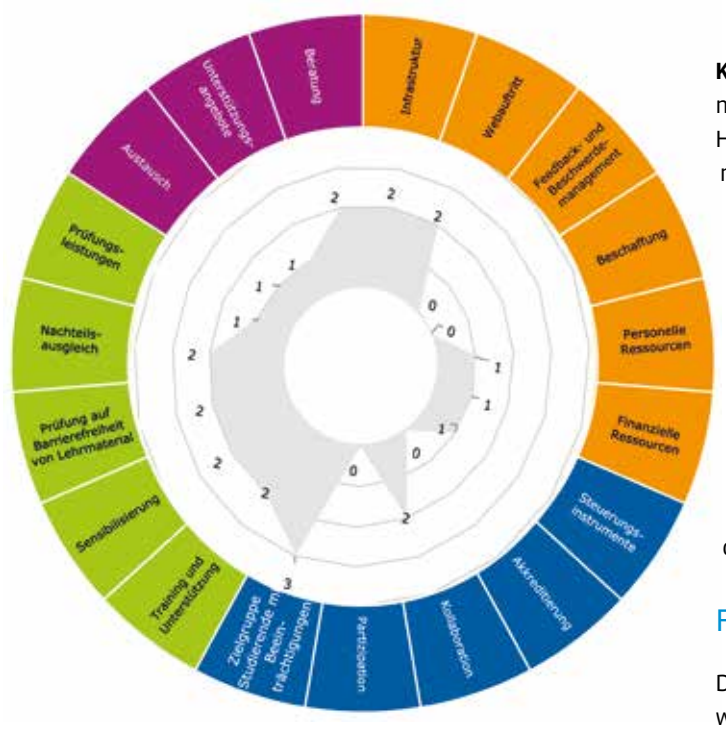


Abb. 2: Beispielhafte Visualisierung des Reifegradmodells als Netzstruktur

MS Excel und künftig über eine Webplattform, auf der die Einstufung über einen Fragebogen erfolgt und damit einfacher zu handhaben ist.

Beide Formate – die Exceltabelle sowie der Fragebogen in der Webanwendung – münden in praxisnahe Handlungsempfehlungen, die sich an den bereits erreichten Stufen orientieren. So wird nachvollziehbar, welche Schritte erforderlich sind, um von einer Stufe zur nächsten zu gelangen, und welche Maßnahmen unmittelbar umgesetzt werden können. Aus den Handlungsempfehlungen können Hochschulen einen praxisnahen Entwicklungsplan ableiten.

Aus der Praxis: Ergebnisse einer Evaluation

Zwischen Sommer 2024 und Frühjahr 2025 wurde das SHUFFLE-Reifegradmodell an sechs Pilothochschulen erprobt und anonym evaluiert. Aus der Testung konnten drei zentrale Mehrwerte abgeleitet werden:

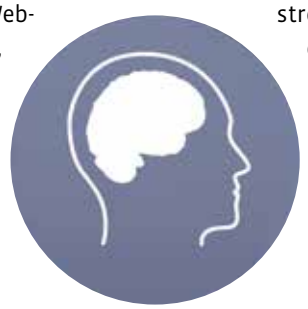
Transparenz: Die beteiligten Hochschulen nutzten die Möglichkeit, sämtliche relevanten Bereiche ihrer Hochschule in einem strukturierten Verfahren systematisch zu erfassen – von den IT-Abteilungen über Lehr- und Lernzentren bis hin zu den Beauftragten für Studierende mit Beeinträchtigungen. Durch diesen umfassenden Blick über die üblichen Zuständigkeitsgrenzen hinweg wurden Synergien sichtbar und gleichzeitig traten ungenutzte Potenziale zutage, die mit verhältnismäßig geringem Aufwand aktiviert werden konnten.

Konkrete Handlungsempfehlungen: Die Datenerhebung zielt nicht nur auf eine Bestandsaufnahme ab, sondern soll Hochschulen ins Handeln bringen, etwa durch die Entwicklung konkreter Maßnahmenpläne. So nutzte beispielsweise eine Hochschule die Ergebnisse, um zusätzliche Schulungsangebote zu konzipieren und Barrieren in digitalen Kursmaterialien konsequent abzubauen.

Verstetigung: Einige Hochschulen nutzten das Reifegradmodell, um über die Ist-Stand-Analyse hinaus Prognosen zu erstellen, potenzielle Herausforderungen frühzeitig zu erkennen und die Planung sowie die Verstetigung relevanter Personalstellen gezielt zu unterstützen. Mit diesem strategischen Ansatz konnten Hochschulen nicht nur ihre interne Entscheidungsprozesse fundierter gestalten, sondern auch überzeugender gegenüber Geldgebern und Gremien argumentieren.

Fazit

Die Anwendung des SHUFFLE-Reifegradmodells macht deutlich, wie wichtig es ist, digitale Barrierefreiheit systematisch, praxisnah und kontinuierlich zu berücksichtigen. Das Modell versteht sich dabei nicht als Prüfinstrument, sondern als Kompass, der Hochschulen Orientierung bietet, Handlungsmöglichkeiten aufzeigt und für Transparenz sorgt.



Die Rückmeldungen der Pilothochschulen unterstreichen diesen Mehrwert: Sie berichten von einer niedrigen Einstiegshürde, einem hohen Erkenntnisgewinn und einem spürbaren Nutzen für die eigene Hochschulentwicklung. Unabhängig vom Stand der Barrierefreiheit kann jede Institution mit einem ersten Schritt beginnen. Das Modell begleitet diesen Prozess, macht Fortschritte sichtbar und motiviert dazu, diesen Weg konsequent weiterzugehen.

Digitale Barrierefreiheit sollte nicht nur als rechtliche Verpflichtung oder als Nischenangelegenheit betrachtet werden, sondern als gemeinsames Anliegen, das Hochschulen nachhaltig bereichert. Sie ist ein Qualitätsmerkmal moderner Hochschulen. Barrierefreie digitale Angebote steigern die Zufriedenheit und Teilhabe der Studierenden, erhöhen die Attraktivität der Lehre und stärken zugleich die Wettbewerbsfähigkeit der Institution. ◆

Weitere Informationen zum SHUFFLE-Reifegradmodell und das Downloadpaket finden Sie unter:
https://shuffle-projekt.de/shuffle-reifegradmodell/

Clever Sparen – Stromkauf mit Machine Learning

Den Bedarf von morgen schon heute kennen? Die direkte Strombeschaffung über die Strombörse erfordert tägliche Prognosen für die benötigten Energiemengen des Folgetages. Mit einem autoregressiven Machine-Learning-Modell zeigt das Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften gemeinsam mit der Technischen Universität München (TUM), wie sich die Genauigkeit dieser Vorhersagen signifikant verbessern – und damit unter dem Strich bares Geld sparen lässt.

Text: **Michael Eichelbeck** (Technische Universität München), **Helmut Reiser** (Leibniz-Rechenzentrum, Ludwig-Maximilians-Universität München), **Jürgen Seidl** (Leibniz-Rechenzentrum), **Fatjon Tushe** (Leibniz-Rechenzentrum, Ludwig-Maximilians-Universität München)

Foto: Urilux / iStock

Strom ist ein kostbares und teures Gut – insbesondere für große Hochleistungsrechenzentren wie das Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften. Die Kosten für die Energie beziehungsweise den Betrieb eines Supercomputers über eine Standzeit von sechs Jahren bewegen sich oftmals in derselben Größenordnung wie die Investitionskosten des Rechners. Darum ist ein effizienter Umgang mit Energie seit vielen Jahren ein wichtiges Anliegen am LRZ und darüber hinaus sogar ein Forschungsschwerpunkt. Jeder Euro, der beim Strom gespart wird, kann für Investitionen genutzt werden und liefert damit mehr Rechenleistung für die Wissenschaft. So spart das LRZ nicht nur durch eine Hochtemperaturwasserkühlung Strom, sondern setzt auf eine besonders smarte Methode der Strombeschaffung und einer Verbrauchsprognose.

Strombeschaffung mittels Bilanzkreis

Für Rechenzentren oder andere Betriebe mit hohem Stromverbrauch kann die direkte Beschaffung von Strom über die Strombörse European Energy Exchange (EEX) in Leipzig weitaus wirtschaftlicher sein als eine Beschaffung über Energieversorger. Voraussetzung ist ein sogenannter „Bilanzkreis“. Über dieses virtuelle Konto wird die Strommenge nicht nur gebucht, sondern auch die Abrechnung von Stromflüssen zwischen Erzeugern, Verbrauchern und dem Stromnetz abgewickelt.

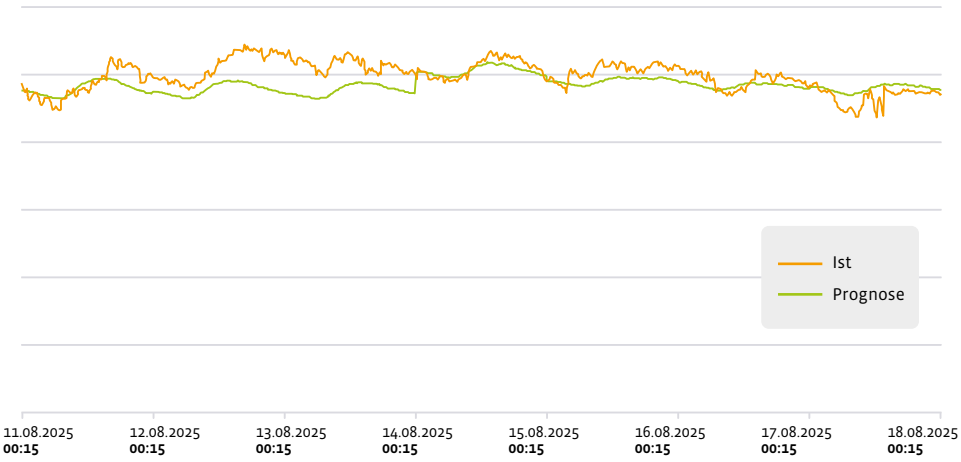


Abbildung 1: Prognose (Grün) und Ist-Verbrauch (Orange) in einer Woche

Seit 2018 übernimmt das LRZ selbst die Rolle des Bilanzkreisverantwortlichen und kauft seinen Strom über einen eigenen Bilanzkreis ein. Die Bundesnetzagentur regelt, wie ein Bilanzkreisvertrag zwischen den Verantwortlichen und dem Übertragungsnetzbetreiber aussehen muss. Ein Bilanzkreismanager (BKL) aufseiten des LRZ sorgt dafür, dass alle Aufgaben und Pflichten, die mit dem Bilanzkreis verbunden sind, zuverlässig erfüllt werden. Und das trägt Früchte: So kam das LRZ deswegen nicht für den Härtefallfond „Energiekosten für außeruniversitäre Forschungseinrichtungen“ (Energiehilfe des Bundes) infrage, weil die Energiekostensteigerung dank dieser Strombeschaffung deutlich unterhalb der vorgegebenen Grenzwerte lag.

Die Beschaffung über die Strombörse ist jedoch mit verschiedenen Risiken verbunden, die finanzielle Auswirkungen haben können. Als staatliche Institution ist das LRZ dazu verpflichtet, den Rahmen und die Vorgaben des staatlichen Haushaltsrechts zu beachten und Risiken zu minimieren:

- **Marktpreisrisiko:** Die Strompreise an der Börse sind starken Schwankungen unterworfen und können durch Faktoren wie Wetter, Brennstoffpreise, politische Entscheidungen (wie CO_2-Abgaben), technische Störungen oder den Ausbau erneuerbarer Energien beeinflusst werden. Marktteilnehmer, die flexibel oder kurzfristig Strom an der Börse einkaufen, laufen Gefahr, bei Preisspitzen deutlich höhere Kosten tragen zu müssen.

- **Mengen-/Volumenrisiko:** Wer seinen Strombedarf im Voraus falsch prognostiziert, muss entweder teure Differenzmengen kurzfristig am Spotmarkt zukaufen oder überschüssig beschaffte Mengen mit Abschlägen abstoßen. Bei stark schwankendem Verbrauch können dadurch erhebliche Mehrkosten entstehen.

Rechenzentren, die die „Grundlastmenge“ gut abschätzen können, sind klar im Vorteil.

Strombeschaffung und Verbrauchsprognose

Das LRZ als Bilanzkreisverantwortlicher – beziehungsweise im Auftrag sein Bilanzkreismanager – kauft und verkauft Strom am Energiemarkt und erstellt Prognosen für den Strombedarf. Eine möglichst exakte Prognose ist wichtig, um das Gleichgewicht zwischen Stromproduktion und -verbrauch sicherzustellen und damit die Stabilität des Netzes zu gewährleisten. Strommengen werden in 15-Minuten-Intervallen bilanziert. Als kleinste Einheit bilden diese die Grundlage für Prognose, Beschaffung und Abrechnung.

An der Strombörse werden verschiedene Terminprodukte gehandelt: Jahres-, Quartals-, Monats-, Wochen- oder Tagesbänder. Ein Rechenzentrum mit gleichmäßigem Grundlastbedarf kann diesen über ein Jahresband decken; jahreszeitliche oder technisch induzierte Schwankungen lassen sich über kurzfristigere Terminmarktprodukte absichern. Alle geplanten Stromflüsse werden dem Netzbetreiber über den Bilanzkreis gemeldet. Dazu gibt der Bilanzkreismanager täglich bis spätestens 15 Uhr eine Verbrauchsprognose für jedes 15-Minuten-Fenster des Folgetages ab. Das Zusammenspiel zwischen der Bedarfsmeldung (Prognose) und der Strombereitstellung wird als Fahrplanmanagement bezeichnet.

Die Differenzen zwischen den Mengen, die über Terminmarktprodukte gekauft wurden, und den Prognosen für den nächsten Tag werden über den Spotmarkt an der Börse zugekauft oder verkauft. Ganz exakt lässt sich der Stromverbrauch jedoch nie vorhersagen. Kommt es in einzelnen Viertelstunden zu Abweichungen von der Prognose, greift die sogenannte Ausgleichsenergie – eine Art Notfallreserve des Netzes. Daraus ergibt sich eine Preishierarchie: Terminmarktprodukte sind in der Regel stabiler und günstiger, Spotmarktprodukte liegen dazwischen, während Ausgleichsenergie die teuerste und volatilste Option darstellt.

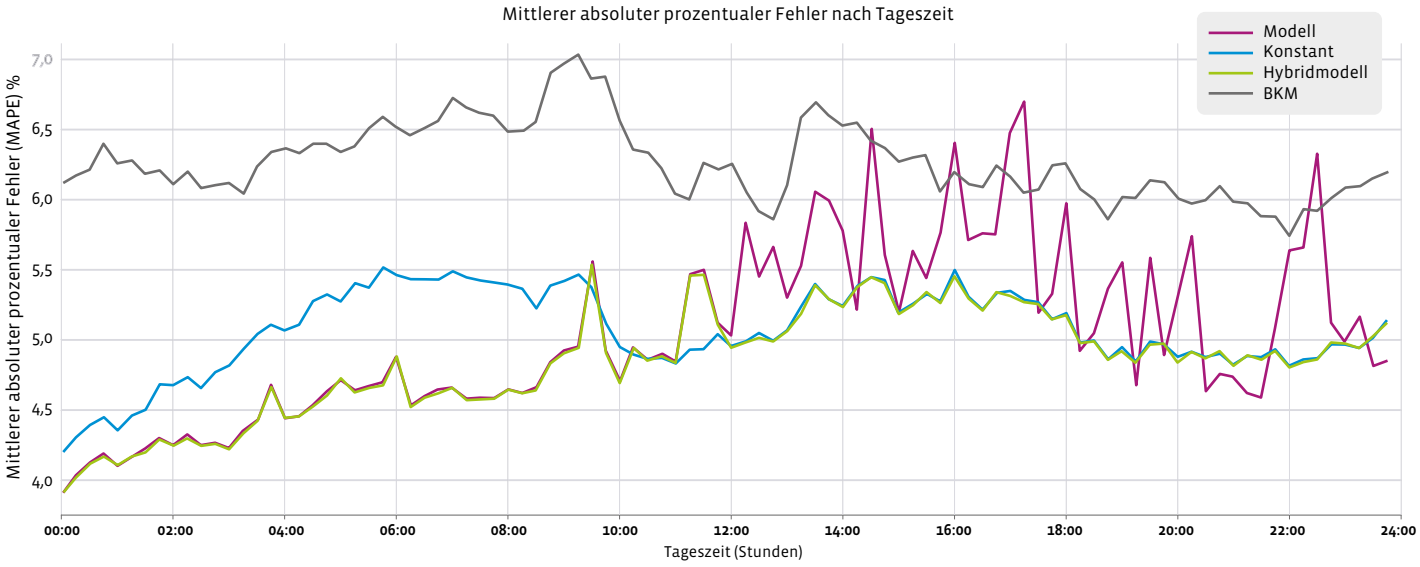


Abbildung 2: Vergleich der Vorhersagefehler verschiedener Ansätze

Vorhersagen treffen: Bilanzkreismanager versus Machine Learning

Interessant ist nun, wie die Tagesprognose erstellt wird und ob es hier Optimierungs- oder Verbesserungspotenzial gibt. Der Bilanzkreismanager setzt ein einfaches, aber überzeugendes Modell ein: Die Mengen der vergangenen beiden Tage werden gemittelt und dienen dann als Prognose für den Folgetag. Abbildung 1 (Seite 37) stellt die Prognose (grün) dem tatsächlichen Verbrauch (orange) gegenüber.

Die spannende Frage ist, ob sich die Bedarfsprognose des Bilanzkreismanagers durch maschinelles Lernen (ML) verbessern lässt. Als Basis für diese Untersuchung wählten LRZ und TUM ein Modell, das in den vergangenen Jahren durch seine Einfachheit und Genauigkeit in der Zeitreihenvorhersage populär geworden ist: DLinear.

In diesem Anwendungsfall nutzt das Modell DLinear als Input die Verbrauchswerte der letzten 33 Stunden sowie eine Repräsentation des Datums und der Uhrzeit. Dieser Input wird in zwei Komponenten aufgeteilt: Eine Trendkomponente, die durch ein gleitendes Mittel von sechs Stunden berechnet wird und eine Saisonkomponente, die die Abweichung von diesem gleitenden Mittel abbildet. Diese werden mithilfe eines einfachen künstlichen neuronalen Netzes jeweils mit nur einer Schicht von Neuronen propagiert und aufsummiert – und liefern dann die Vorhersage.

Der Vorhersagehorizont deckt einen Zeitraum von 33 Stunden ab – neun Stunden bis Mitternacht plus 24 Stunden des darauffolgenden Tages. Das Modell wird mit Daten der Jahre 2019 bis 2023 trainiert. Alle Evaluationen basieren auf den Daten aus dem Jahr 2024. Das Training des Modells benötigt etwa 90 Minuten auf einer Nvidia-H100-GPU (Graphics Processing Unit) und ist in der Programmiersprache Python unter Verwendung der Open-Source-Bibliothek CommonPower implementiert.

Zusätzlich zu dem Machine-Learning-Modell wird eine weitere Vergleichslinie etabliert, die den Durchschnittswert des Verbrauchs der vergangenen 24 Stunden als konstante Vorhersage verwendet. Für den Vergleich der verschiedenen Ansätze wurde der durchschnittliche prozentuale Fehler pro Viertelstunde der Vorhersage des nächsten Tages über alle Tage der Testdaten berechnet. In Abbildung 2 ist gut zu erkennen, dass sowohl das ML-Modell (violett) als auch die konstante Vorhersage (blau) insgesamt genauer sind als das Modell des Bilanzkreismanagers (grau).

Das ML-Modell ist in der ersten Tageshälfte besonders präzise, wird allerdings danach zunehmend instabil. Im Gegensatz dazu ist die konstante Vorhersage in der ersten Tageshälfte ungenauer als das ML-Modell, dafür in der zweiten Tageshälfte deutlich stabiler. Um die Stärken der beiden Ansätze zu kombinieren, wurde ein Hybridmodell (grün) erstellt, das für die erste Tageshälfte das ML-Modell und für die zweite Tageshälfte die konstante Vorhersage verwendet. Insgesamt lässt sich mit dem Hybrid-Modell ein durchschnittlicher relativer Fehler von 4,8 Prozent realisieren, während das BKM-Modell bei einen Wert von 6,3 Prozent liegt.

Simulation der Strombeschaffung

Es ist naheliegend anzunehmen, dass eine genauere Lastvorhersage zu Ersparnissen bei der Strombeschaffung führt. Um tatsächliche Ersparnisse abschätzen zu können, ist jedoch eine Simulation erforderlich. Für diesen sogenannten Rückvergleich (Backtest) wurden die historischen Spotmarkt- sowie Ausgleichsenergiepreise

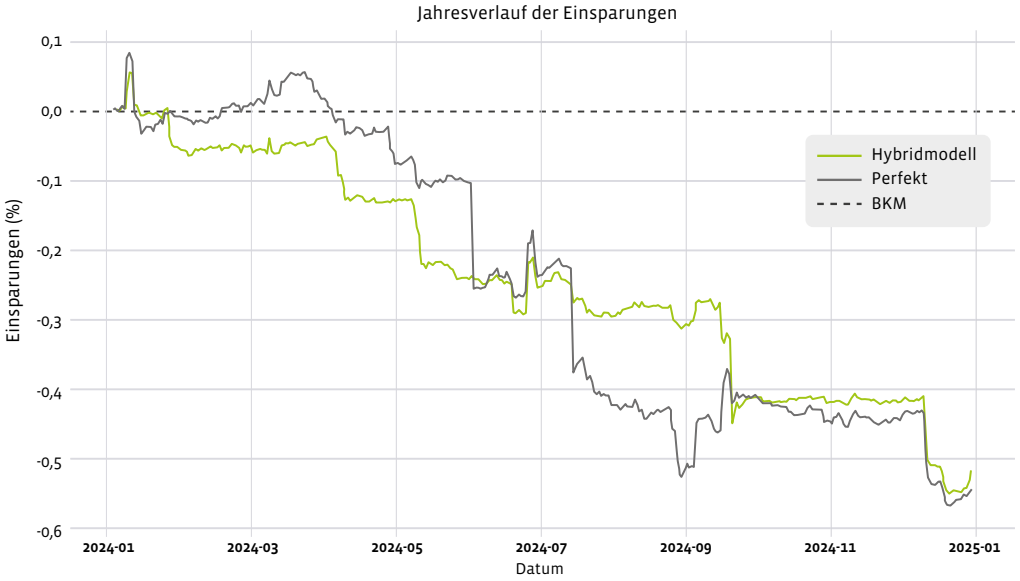


Abbildung 3: Jahresverlauf der Einsparungen

aus dem Jahr 2024 verwendet. Um den 15-minütigen Strombedarf des jeweils darauffolgenden Tages zu bestimmen, wurde die Vorhersage des Hybridmodells genutzt. Der so ermittelte Bedarf wird anschließend zum historischen Spotmarktpreis gekauft. Der damit erstellte Fahrplan ist die Basis für die Berechnung der Ausgleichsenergiemengen am Folgetag. In jedem 15-Minuten-Intervall wird die Abweichung zum Fahrplan bestimmt und zum historischen Ausgleichsenergiepreis beschafft beziehungsweise verkauft.

Anzumerken ist, dass der Ausgleichsenergiepreis (reBAP) in der Realität zur Lieferzeit nicht bekannt ist und vom Netzbetreiber erst im Nachhinein basierend auf den tatsächlich entstandenen Kosten bekannt gegeben wird.

Wie beschrieben, ist es für Großverbraucher üblich, eine gewisse Strommenge langfristig über den Terminmarkt zu beschaffen. Dies reduziert im Allgemeinen den Einfluss der Vorhersagegenauigkeit, da weniger über den Spotmarkt gehandelt wird. In dem hier präsentierten Rückvergleich wurde der Terminmarkt vernachlässigt, um die Vergleichbarkeit zu erhöhen.

Der prozentuale Vergleich der simulierten Einsparungen des Hybridmodells (grün) im Vergleich zum Modell des Bilanzkreismanagers (Nulllinie) wird in Abbildung 3 gezeigt. Über das Jahr 2024 hätten diese bei 0,56 Prozent gelegen, was bemerkenswerterweise nur unwesentlich geringer ist als die auf perfekten Vorhersagen basierenden Einsparungen (grau). Bei einer beispielhaften jährlichen Stromrechnung von fünf Millionen Euro – eine realistische Größenordnung für ein großes Rechenzentrum – würde die jährliche Ersparnis damit etwa 28.000 Euro betragen. Die Hypothese, dass genauere Vorhersagen zu einem Spareffekt führen können, ist damit bestätigt.

Eine interessante Beobachtung ist, dass einige wenige Zeitpunkte mit extremen Ausgleichsenergiepreisen einen großen Einfluss haben. So lag der Preis am Morgen des 3. Juni 2024 teilweise um einen Faktor von 174 über dem Jahresdurchschnitt. Dieses Ereignis ist gut am Abwärtssprung der Kurve der perfekten Vorhersage (grau) in Abbildung 3 zu erkennen. Gerade weil diese Extremfälle schwer vorherzusagen sind, ist eine genauere Bedarfsprognose allgemein wertvoll.

Im Hinblick auf den langfristigen Einsatz eines ML-Modells zur Bedarfsprognose ergibt sich die Frage nach der Anpassung an sich ändernde Lastprofile. Die einfachste Lösung wäre, das Modell in regelmäßigen Abständen mit allen verfügbaren Daten neu zu trainieren. Deutlich effizientere Ansätze werden derzeit im Bereich des sogenannten lebenslangen Lernens intensiv erforscht und könnten hier ebenfalls Anwendung finden.

Fazit

Im Rahmen dieser Arbeit konnten das LRZ und die TUM zeigen, dass mit einem sehr einfachen autoregressiven ML-Modell signifikante Einsparungen bei der Strombeschaffung eines Großverbrauchers möglich sind. Die Daten, die für das Training benötigt werden, sind meistens bereits in geeignetem Format vorhanden. Die Trainingszeit ist vernachlässigbar. Komplexere Strategien mit größeren ML-Modellen und zusätzlichen prädiktiven Inputdaten könnten vermutlich zu weiteren Einsparungen führen und zudem die Stabilität des Stromnetzes durch verlässlichere Lastprognosen verbessern. Mit diesen Erkenntnissen bringen LRZ und TUM nicht nur die Wissenschaft voran, sondern tragen auch in internationalen Gremien wie der Energy Efficient HPC Working Group dazu bei, gemeinsame Regeln und Standards für den nachhaltigen Rechenzentrumsbetrieb der Zukunft zu erarbeiten. ◆

QUELLEN

Zeitreihenprognosen-Modell DLinear: A. Zeng, M. Chen, L. Zhang and Q. Xu, “Are Transformers Effective for Time Series Forecasting?”, AAAI, vol. 37, no. 9, pp. 11121-11128, Jun. 2023

Open-Source-Bibliothek CommonPower: **https://github.com/TUMcps/commonpower**

Informationen zur Strombörse European Energy Exchange (EEX) finden Sie unter: **https://www.eex.com**

Forschung trifft Netzbetrieb – im Projekt bwNET

Steigende Bandbreitenanforderungen, Cloud-Integration, heterogene Endgeräte und ausgefeilte Cyberangriffe stellen Forschungsnetze und Bildungsnetze vor vielfältige Herausforderungen. Das Projekt bwNET verknüpft Forschung und Betrieb, um neue Lösungen von der Idee bis zur Umsetzung zu erproben.

Text: **Oliver P. Waldhorst** (Hochschule Karlsruhe),
Frank Kargl (Universität Ulm),
Michael Menth (Eberhard Karls Universität Tübingen),
Steffen Wendzel (Universität Ulm),
Martina Zitterbart (Karlsruher Institut für Technologie, KIT)

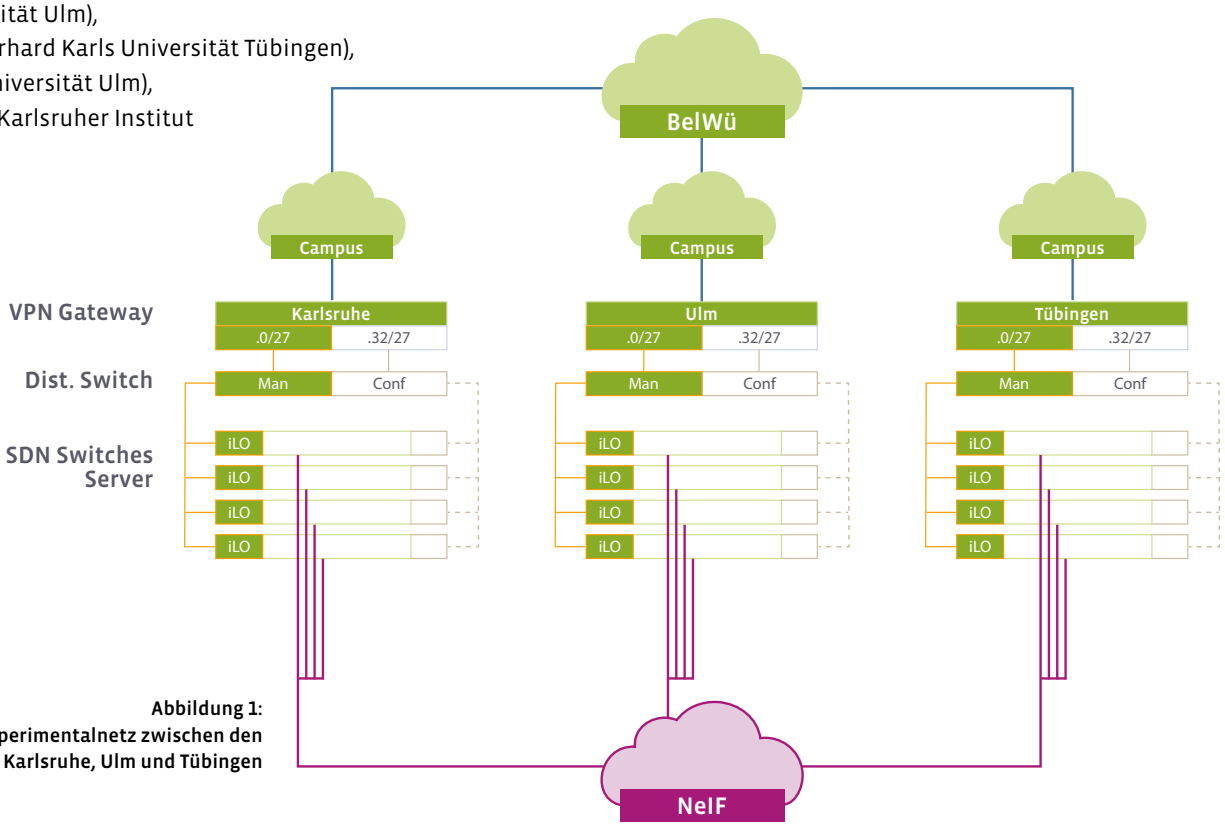


Abbildung 1:
100G Experimentalnetz zwischen den Standorten Karlsruhe, Ulm und Tübingen

An dem in mehreren Projektphasen geförderten bwNET-Projekt (im Folgenden bwNET) sind das Landeshochschulnetz Baden-Württemberg (BelWü), das Karlsruher Institut für Technologie (KIT), die Eberhard Karls Universität Tübingen, die Universität Ulm sowie seit 2020 die Hochschule Karlsruhe beteiligt. In diesem Verbund arbeiten Netzforschende und Netzbetreiber eng zusammen, um innovative Lösungen für die Weiterentwicklung der Hochschulnetze zu erforschen und in die Praxis zu überführen. Besonders berücksichtigt werden dabei spezifische Anforderungen von Forschung und Lehre, die über die reine Bereitstellung von Konnektivität hinausgehen. Gleichzeitig muss der sichere und robuste Betrieb der Netze gewährleistet werden.

Durch die enge Kooperation zwischen Forschung und Betrieb können auf der einen

Seite Forschungsergebnisse schneller Einzug in innovative Lösungen im Betrieb halten, auf der anderen Seite werden Forschende frühzeitig mit praktischen Randbedingungen vertraut. Darüber hinaus ergeben sich für die Netzforschung interessante Möglichkeiten für Experimente nahe an bzw. in operativen Netzen sowie Einsichten in Verkehrsprofile und Daten. Es ist somit eine Win-win-Situation sowohl für den Betrieb als auch für die Forschung.

bwNET – die Umsetzung

Die für diesen Ansatz nötigen personellen Freiräume entstehen durch die Finanzierung von Mitarbeiterstellen in den beteiligten Forschungs- und Betriebsgruppen. Regelmäßige Präsenz- und Onlinetreffen sowie gemeinsame Arbeitspakete und Meilensteine fördern die standortübergreifende Zusammenarbeit zwischen den Forschungs- und den Betriebsgruppen der Campusnetze und des BelWü. An den Standorten arbeiten Beschäftigte aus Forschung und Betrieb oft im selben Büro, was den direkten Austausch und ein unmittelbares „Voneinanderlernen“ erleichtert. Es werden gemeinsame Forschungs- und Entwicklungsthemen sowie experimentelle und prototypische Aufbauten bearbeitet. Ergänzend untersucht das Technology Scouting in kurzfristigen Projekten relevante Technologien im Detail, etwa Switches mit Datenraten jenseits von 100 Gbit/s, programmierbare ASICs, Streaming Telemetry in Switch-Modellen verschiedener Hersteller und die Fähigkeiten von Smart NICs.

Die Verbreitung der Ergebnisse ist ein zentrales Anliegen von bwNET. Die hohe Praxisrelevanz und die realitätsnahen Testumgebungen eröffnen den Forschungsgruppen hervorragende Publikationsmöglichkeiten[1]. Für Rechenzentren und Betriebsgruppen außerhalb von bwNET werden technische Berichte zu praxisnahen Themen sowie Ergebnissen des Technology Scouting oder der TCP/IP-Stack-Optimierung für 100G-Netze veröffentlicht. Zudem bietet bwNET Workshops für Rechenzentrumsmitarbeitende – etwa zu Software-Defined Networking oder Monitoring mit der flowpipeline – an und ist regelmäßig auf praxisnahen Veranstaltungen wie den BelWü Tech Days vertreten.

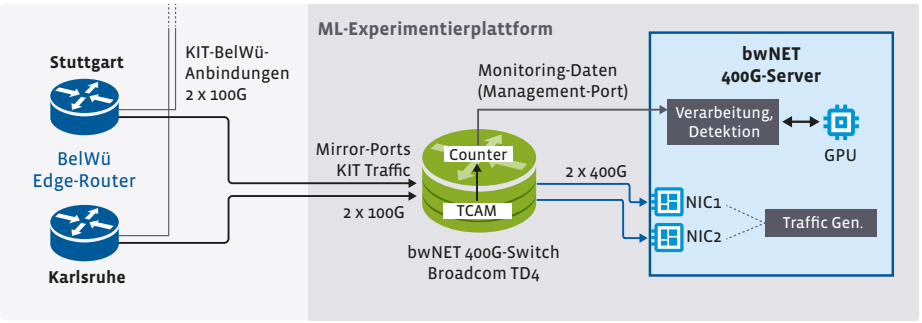
Kooperationen in der Praxis

Die Untersuchung neuester Entwicklungen bei Netz-Hard- und -Software wird durch die gezielte Förderung gemeinsamer Versuchsaufbauten ermöglicht, die von Forschungs- und Betriebsgruppen gemeinsam konzipiert, umgesetzt und betrieben werden. Je nach Reifegrad einer Technologie können dies zunächst vom Produktivbetrieb isolierte Testumgebungen sein. Versuchsaufbauten können jedoch auch parallel zum Produktivbetrieb eingesetzte Systeme umfassen oder sogar direkt in das Produktionsnetz integriert werden.

Isolierte Testumgebung: 100G-Experimentalnetz für Forschungszwecke

Höhere Datenraten im Netz, aber keine Leistungssteigerung der Anwendungen? Ein ärgerliches Phänomen! Verbesserungen erfordern meist eine gezielte Parametrisierung der beteiligten Komponenten. Für entsprechende Experimente wurde in der ersten bwNET-Projektphase mit Unterstützung des BelWü-Betriebs das Netz für Innovation und Forschung (NeIF) mit 100G-Verbindungen zwischen den beteiligten Universitäten aufgebaut (siehe Abb. 1).

Die 100G-Verbindungen bildeten eine landesweite Ringstruktur von Ulm über Stuttgart, Karlsruhe und Tübingen zurück nach Ulm. Damit wurde erstmals eine Plattform geschaffen, die die Untersuchung zeitkritischer Mechanismen wie Staukontrolle, Pufferdimensionierung oder Paketverluste bei 100 Gbit/s unter realen Netzbedingungen ermöglicht. Das einmalige oder mehrfache



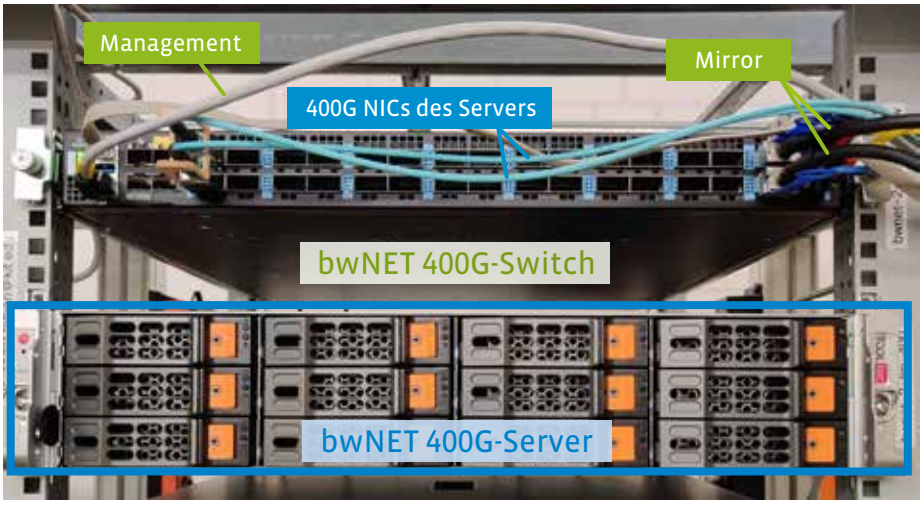


Abbildung 2: Experimentierplattform an Mirror-Ports produktiver Router | *Foto: Timon Krack*

1 https://bwnet2.belwue.de/publications/research-papers

Durchleiten von Paketen durch die Ringstruktur erzeugte zudem definierte Latenzen (6 ms bis 24 ms RTT) ohne künstliche Emulation und erlaubte Experimente unter realistischen Bedingungen, etwa zu Bitfehlern oder variabler RTT. Vergleichsexperimente zeigten, dass der verbreitete Delay-Emulator netem bei hohen Datenraten (ab 10 Gbit/s) deutliche Verfälschungen verursacht, während das reale Testbed authentisches Verhalten liefert.

Die in NeIF durchgeführten TCP-Analysen[2] bildeten eine Grundlage zur Weiterentwicklung von TCP-Varianten für Hochgeschwindigkeitsnetze. Zudem wurde für NeIF ein SDN-basiertes Weiterleitungskonzept auf Basis von OpenFlow entwickelt, über das campusübergreifende Datenflüsse (z. B. bwCloud- oder Back-up-Verkehr) direkt durch das Testbed geleitet werden können[3]. Darauf aufbauend entstanden Konzepte zur Entlastung des BelWü-Core-Netzes, zur redundanten Anbindung von Universitäten und zur Fehlerbehandlung mit hoher Relevanz für den operativen Betrieb.

Experimente (nahe) am Produktivbetrieb: Erkennung von Denial-of-Service-Angriffen

Wie gut funktionieren auf maschinellem Lernen (ML) basierende Verfahren auf realen Verkehrsdaten? Zur Beantwortung dieser Frage bietet bwNET die Möglichkeit, Experimente parallel zum Produktivbetrieb durchzuführen.

Aktuell wird diese Möglichkeit zur realitätsnahen Erprobung eines ML-basierten Systems zur Erkennung von Denial-of-Service-Angriffen genutzt, das zuvor nur auf öffentlich zugänglichen Verkehrsdaten evaluiert werden konnte[4]. Dieses System ist hierzu an Mirror-Ports produktiver Router angeschlossen (siehe Abb. 2). Experimente sind so mit echten Verkehrsdaten aus dem Produktivbetrieb möglich, ohne diesen selbst zu stören. Dies geht weit über die Möglichkeiten hinaus, die Forschungsgruppen mit ihrer eigenen (eingeschränkten) Infrastruktur typischerweise haben. Für die Betriebsgruppen ermöglicht dies eine objektive Bewertung neuer Technologien in der realen Einsatzumgebung.

Prototypischer Einsatz: Zero Trust Service Function Chaining

Wie lässt sich der Zugriff auf sensible Daten absichern, wenn Studierende, Forschende und Mitarbeitende aus Büro, Homeoffice oder unterwegs mit unterschiedlichen Geräten darauf zugreifen? Zero Trust Security[5] beschreibt ein Sicherheitskonzept, das sich an Kontextfaktoren wie Gerätevertrauen, Standort oder Nutzungsverhalten orientiert. Es ersetzt „Trust, but verify“ durch „Never trust, always verify“ und fordert Maßnahmen wie strikte Identitätsprüfung, Least-Privilege-Zugriff und vollständige Verschlüsselung.

Aufbauend auf Forschung zu Zero Trust und Software-defined Networking wurde in bwNET das Konzept des Zero Trust Service Function Chainings (ZTSFC)[6] entwickelt. Es kombiniert Zero-Trust-Zugriffskontrolle und Service Function Chaining (SFC)[7], sodass Sicherheitsfunktionen wie Mehr-Faktor-Authentifizierung, Intrusion Detection, Traffic-Filterung oder Protokollierung kontextabhängig verknüpft und vor zu schützende Systeme geschaltet werden können (siehe Abb. 3).

ZTSFC wurde projektintern realitätsnah erprobt: Die bwNET-Mitarbeitenden nutzten es, um den Zugriff auf das selbst betriebene Overleaf-System zur kollaborativen Dokumentbearbeitung abzusichern. So konnten verschiedene SFC-Ansätze unter realen Bedingungen evaluiert werden[8]. Zudem konnten Mitarbeitende der Rechenzentren frühzeitig mit den neuen Konzepten vertraut gemacht werden, um anfängliche Skepsis gegenüber Zero Trust und SFC abzubauen.

Produktiver Einsatz: Verarbeitung von Flow-Daten mit der flowpipeline

Aktuelle Netzhardware ermöglicht von Haus aus den Export von Flow-Daten, die Statistiken über verarbeitete Netzflüsse liefern. Doch wie können diese Daten effizient und wirkungsvoll für die Analyse und das Monitoring produktiver Netze genutzt

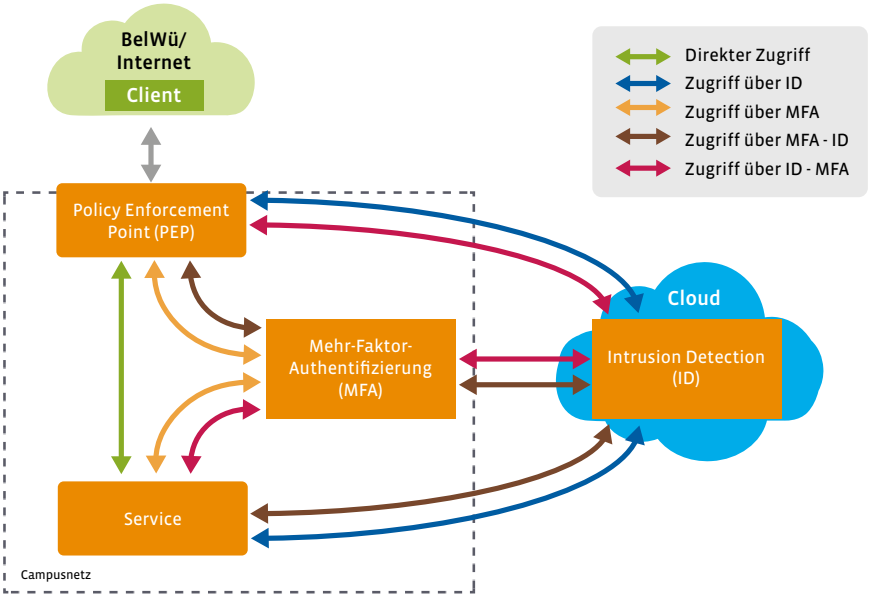


Abbildung 3: Konzept des Zero Trust Service Function Chaining: Der PEP kann Zugriffe bei Bedarf durch eine oder mehrere Service Functions (MFA, ID) leiten

2 (Hock et al. 2019)
3 (Menth et al. 2017)
4 (Kopmann et al. 2022)
5 https://www.forrester.com/report/zero-trust-defined/RES178926
6 (Bradatsch et al. 2023)
7 https://datatracker.ietf.org/doc/html/rfc7665
8 (Bradatsch et al. 2022)

werden? Forschungsarbeiten im Rahmen von bwNET führten zu einem innovativen Werkzeug für das Netzmonitoring. Mit der flowpipeline[9] wurde ein modular aufgebautes System zur hochperformanten Verarbeitung von Flow-Daten (NetFlow, IPFIX, sFlow) entwickelt. Es ermöglicht den Aufbau konfigurierbarer Verarbeitungsketten, bestehend aus Bausteinen („Segmenten“) zum Empfangen, Filtern, Anreichern, Transformieren und Exportieren von Flow-Daten. Dabei werden verschiedene Datenquellen (z. B. Router oder Kafka) sowie unterschiedliche Ausgabeformate für Analyse, Speicherung oder Monitoring unterstützt. Durch die einfache Integration eigener Segmente lassen sich spezifische Anforderungen eines Netzbetreibers flexibel umsetzen.

Die flowpipeline wurde in enger Zusammenarbeit mit BelWü zu einer Softwarelösung weiterentwickelt, die heute im BelWü-Netz dauerhaft für Flow-Monitoring, Traffic-Analysen und Anomalieerkennung produktiv eingesetzt wird. Auch das Rechenzentrum des KIT nutzt die flowpipeline inzwischen im Regelbetrieb, und eine Integration in die Campusnetze der weiteren an bwNET beteiligten Universitäten ist in Vorbereitung.

Fazit und Ausblick

Im Rahmen der bwNET-Projekte wurde deutlich, dass auch in innovationsfreundlichen Rechenzentren die Betriebssicherheit oberste Priorität hat und neue Technologien erst nach gründlicher Erprobung in Betracht gezogen werden. bwNET schafft hierfür den notwendigen Rahmen, um Forschungsergebnisse weiterzuentwickeln und gemeinsam mit den Rechenzentren deren Praxistauglichkeit zu prüfen. Selbst wenn nicht jede Technologie den Sprung in den produktiven Betrieb schafft, profitieren die Rechenzentren dennoch vom frühen Kontakt mit neuen Konzepten. Auf der anderen Seite profitieren die Forschungsgruppen von realitätsnahen Anforderungen und Experimentiermöglichkeiten.

Neben den technischen Ergebnissen tragen die bwNET-Projekte auch zur nachhaltigen Weiterentwicklung der Hochschulnetze bei, indem sie den Führungsnachwuchs fördern. Promovierende erhalten Einblicke in den praktischen Betrieb und entwickeln dadurch ein tiefes Verständnis für die organisatorischen und technischen Herausforderungen, die künftige Leitungstätigkeiten in Rechenzentren prägen werden. ◆

WEITERE BWNET-INNOVATIONEN IM ÜBERBLICK

- **Verteilte IPFIX-Sensorplattform:** Erhebung von vollständigen (unsampled) IPFIX-Flowdaten in einem geografisch verteilten Universitätsnetz basierend auf Open-Source-Software und kostengünstiger COTS-Hardware.
- **Traffic-Generator P4TG:** P4TG ist ein flexibler Hochleistungstraffic-Generator für bis zu 10 x 400 Gbit/s, erweiterbar auf neue Protokolle zum Testen neuer Konzepte wie Segment Routing.
- **Automatisierte Hardwaretests:** Bewertung von Geräteleistungsgrenzen bei Datenraten jenseits 100 Gbit/s unter Verwendung von P4TG und anderen Traffic-Generatoren in reproduzierbaren, automatisierten Geräte-Benchmarks.
- **Firewall Bypass:** Mittels Software-Defined Networking werden Sicherheitsfunktionen wie Firewalls für bestimmte vertrauenswürdige Netzflüsse umgangen, um Ressourcen zu sparen.
- **MalFIX:** skalierbare Bedrohungserkennung auf Basis von IPFIX und Threat Intelligence Feeds.

Mehr Infos unter: **https://bwnet2.belwue.de/**

Diese Arbeiten wurden im Rahmen der bwNET-Projekte durchgeführt, die vom Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK) gefördert werden bzw. wurden. Für den Inhalt des Beitrags sind ausschließlich die Autoren verantwortlich.

QUELLEN:

Bradatsch, Leonard, Marco Haeberle, Benjamin Steinert, Frank Kargl, and Michael Menth. 2022. “Secure Service Function Chaining in the Context of Zero Trust Security.” Proc. IEEE Conf. on Local Computer Networks (LCN) (Edmonton, Canada), September. **https://doi.org/10.1109/LCN53696.2022.9843821.**

Bradatsch, Leonard, Oleksandr Miroshkin, and Frank Kargl. 2023. “ZTSFC: A Service Function Chaining-Enabled Zero Trust Architecture.” IEEE Access 11 (November): **125307–27. https://doi.org/10.1109/ACCESS.2023.3330706**.

Hock, Mario, Maxime Veit, Felix Neumeister, Roland Bless, and Martina Zitterbart. 2019. “TCP at 100 Gbit/s – Tuning, Limitations, Congestion Control.” Proc. IEEE Conf. on Local Computer Networks (LCN) (Osnabrück, Germany), 1–9. **https://doi.org/10.1109/LCN44214.2019.8990842**.

Kopmann, Samuel, Hauke Heseding, and Martina Zitterbart. 2022. “HollywooDDoS: Detecting Volumetric Attacks in Moving Images of Network Traffic.” Proc. IEEE Conf. on Local Computer Networks (LCN) (Edmonton, Canada), 90–97. **https://doi.org/10.1109/LCN53696.2022.9843465**.

Menth, Michael, Mark Schmidt, Daniel Reutter, Robert Finze, Sebastian Neuner, and Tim Kleefass. 2017. “Resilient Integration of Distributed High-Performance Zones into the BelWue Network Using OpenFlow.” IEEE Communications Magazine 55 (4): 94–99. **https://doi.org/10.1109/MCOM.2017.1600177.**

9 https://codeberg.org/BelWue/flowpipeline

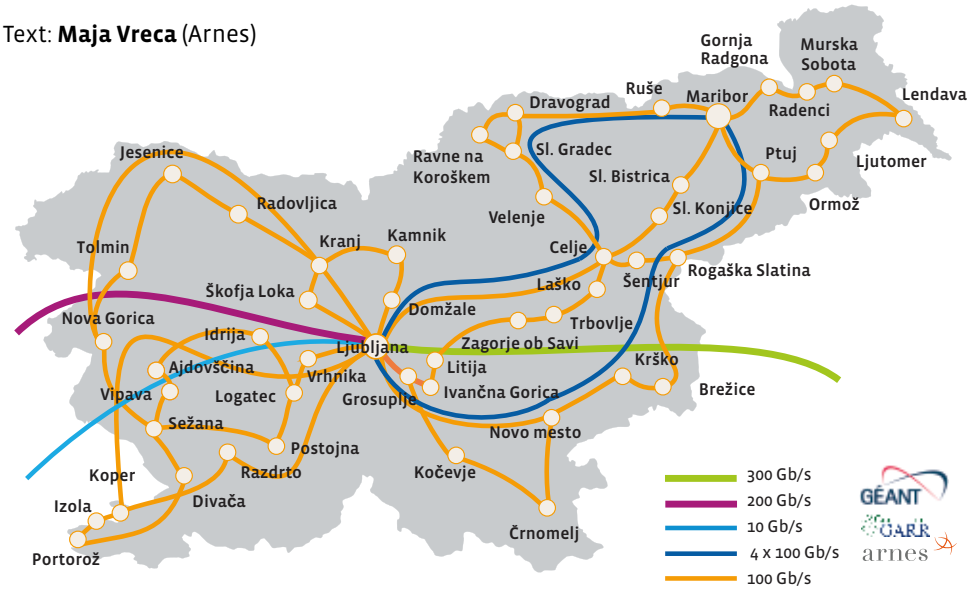
Starke Partner weltweit

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

Rooted in Community: ARNES' Commitment to Social Responsibility

The Academic and Research Network of Slovenia (ARNES) was established in 1992, which coincided with the establishment of many other national education and research networks (NRENs). Since some had already been in operation for some time, we were able to rely on the experience of countries that had already their own NRENs. In some respects, however, we have built our national network on a different foundation.

Text: **Maja Vreca** (Arnes)



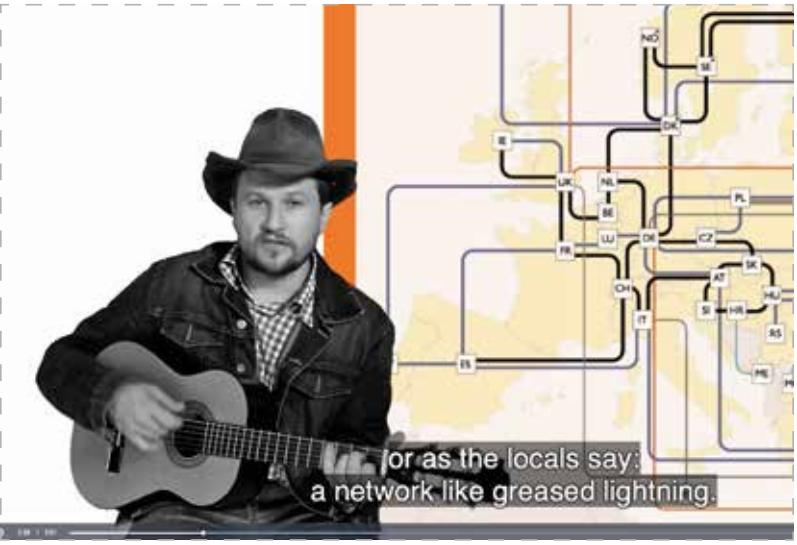
Map of the ARNES network

Slovenia is a small country with just over two million inhabitants, which means that there are not as many universities and research institutes as in larger countries, making it difficult to always closely follow the examples of larger networks.

For this reason, we set a much broader base of user organisations from the very beginning. Accordingly, our membership extends to every kind of public educational institution, from kindergartens to universities. We also provide access to the network and our services to both research organisations and cultural institutions – from libraries to museums and theatres. Beneficiaries of our services include associations and non-governmental organisations recognised by the relevant ministries as important for the wider community, as well as disability organisations and disabled people.

Building resilient infrastructure from the beginning

However, such a diverse base of users also brought many challenges. By providing access



Why read about it when you can rap! Discover ARNES' story in their own unforgettable rhythm:

to the internet for students and pupils, we had to establish strong communication with schools and school professionals from the outset. As early as 1995, we already had to learn how to respond to various abuses by teenagers. Additionally, we had to learn how to help young people and their parents deal with excessive internet use, which appeared in some vulnerable adolescents, and how to respond to various incidents that were often initiated by our young users who used our network for both beneficial aspects of the new medium and others who often went overboard. Like other NRENs and internet service providers, we had to reckon with popular forms of hacking and network disruption, such as persistent distributed denial of service (DDoS) attacks on IRC.

As early as 1995, we established the Slovenian CERT within ARNES, which dealt with network incident response. At the same time, we began to develop "soft" community support skills in dealing with the negative aspects of the use of new technologies.

ARNES is, of course, an internet access provider and a service provider, as is the case for all European NRENs. We offer services and carry out activities that are comparable to other NRENs, from providing AAI identities to providing repositories for open science.

Deep Community Engagement

In its 33 years of operation, ARNES has also expanded greatly and changed many activities, but the basis of what we do is still rooted in our deep involvement in our community and our strong emphasis on social responsibility for the ARNES community and beyond.

One of our non-typical aspects is our financing method. ARNES' services are free of charge for user organisations and eligible individuals. We cover operating costs from funds obtained from ministries and partly from various projects.

ARNES' activities over the years have also included running the Slovenian Internet Exchange from its conception, as it is considered a trustworthy organisation across Slovenia.

Boosting Awareness for a Safer Internet

The Slovenian National Registry and top-level DNS are also part of ARNES, as is the aforementioned Slovenian National CERT (SI-CERT).

In addition to its basic activities, the SI-CERT also leads a high-profile public awareness project called "Safe on the Internet", which disseminates knowledge that helps prevent incidents. It primarily focuses on preventing fraud and intrusions. It shows the actions of fraudsters and fraud patterns and warns of weaknesses that can lead to intrusions.

ARNES is also heavily involved in the other side of awareness activities. It is one of the founding partners of the Safer Internet Centre project - SAFE.SI, which has been running for 20 years and is part of the European INSAFE network. The main target audiences for this awareness work are children and adolescents, their parents and guardians, and educators and teachers.

In addition to these two awareness-raising systems, ARNES has also developed a MOOC for adults in 2014, which includes content related to the SAFE.SI and Safe on the Internet projects, but with a stronger emphasis on spreading digital media literacy and protecting privacy for adults. Of course, no two versions of this course are the same, as the content is regularly updated. Later, a similar MOOC for children was also developed.

Strong in education and support

Raising awareness about the negative aspects of new technologies is not the only topic we educate about. Many of these training courses are intended to support our services and educate in related fields. ARNES has developed a large number of specialised courses in the form of MOOCs and practical workshops. We also spread our knowledge through short videos, lectures, articles and columns, webinars, intensive cooperation with the media and at our events.

We are heavily involved in content cooperation and technical support in preparing content for schools, parents, and students that were created in projects where ARNES is one of the partners. For example, we are currently producing video materials on digital citizenship education for meetings with parents for the educational path with parents that are relevant from kindergarden to high school.

We also participated in an expert group, which, under the auspices of the Medical Chamber, prepared national guidelines for the use of devices with screens for children and adolescents.

User support and user education are extremely important activities for us and our users appreciate it very much. This is what – in addition to ensuring the security and privacy of use for our services – most distinguishes us from global providers.

We also adapt some of our services to members of our community with special demands. For example, we adapted part of the functionality of the ARNES Video Portal to the needs of the Slovenian Film Database.

We take care of the SIO platform, which is the central national point for content intended for the educational community and for the SIO community, which, among other things, enables the creation of online classrooms and courses intended for the wider community, not just our users.

Our close ties with the community are of great help in establishing connections, setting up local networks in schools, coordinating in the field, and preparing training courses. Under our leadership, teacher multipliers – as local ambassadors who know ARNES and our services well – advise schools in their regions, help prepare training courses for school professionals, often bringing expertise in specialized topics and spreading knowledge on different subjects.

Making Face-to-Face Moments a Priority

One of the important points of contact for our communities is the annual ARNES multi-conference "Knowledge Network", which brings together the "Education Network", intended primarily for schools, the "Open Science" conference, the "Citizen Science" conference, and the "SLING Days" conference, which covers HPC and HDPA technologies. Under this umbrella, other content areas often join our main events. Last year, this was a conference on copyright, and this year we were joined by a larger international event – the final conference of the European Year of Digital Citizenship Education 2025, which is part of a bigger project in which ARNES is also involved. Events where participants can meet in-person are high on our priority list.

In recent years and in cooperation with numerous partners, we began organizing the ARNES HackathON, which is held under the honorary patronage of the Slovenian National Commission for UNESCO because all challenge solutions addressed at least one of the 17 UNESCO Sustainable Development Goals. Training courses on open science, supercomputing, data mining, public speaking, and science communication were also prepared for the competitors, and expert assistance and support for HackathON competitors

Creativity in action: Young innovators at the ARNES HackathON put their skills to the test, tackling challenges linked to the UNESCO Sustainable Development Goals with guidance from mentors and expert training | *Photo: Arnes*

were provided by mentors and a panel of experts from various fields addressed during HackathONs.

We also organise other events for the scientific community, such as the Austrian-Slovenian HPC Meeting. We also co-organise many events or join them as partners, such as the annual meeting of the Slovenian Network Operators Group SiNOG or the Open Days of Slovenian Supercomputing Centres.

In addition to organising events that connect communities, we are also involved in coordinating the activities of some communities. For example, we coordinate the activities of the consortium for the development of high-performance computing (SLING) and thus also represent Slovenia in European and global organisations. We also lead the national competence centre for HPC and, as one of the key stakeholders of the Slovenian Open Science Community, we are participating in the new European AI Factories project.

Of course, we're not just about connecting communities, support, and education.. For instance, we are also in the process of building a new data centre to support open science and supercomputing and serve as the one-stop shop for researchers in Slovenia to fulfil their research, data, and computing needs.

From the very beginning, ARNES has maintained close contacts with its community and – just like its expertise – takes its socially beneficial role very seriously. Our community sees our dedication, rewarding us with the status of a professional and trustworthy institution– perhaps our most proud accomplishment. ◆

More informations about the Arnes network:
https://www.arnes.si/en/about-arnes/

HammerHAI: Inside Germany's High-Performance "AI Factory"

Europe is taking AI to the next level. With HammerHAI (Hybrid and Advanced Machine Learning Platform for Manufacturing, Engineering, and Research), one of the continent's first "AI Factories," Germany is creating a powerful hub for training and deploying AI models across science, industry, and society. Coordinated by the High-Performance Computing Center Stuttgart (HLRS) together with other leading German centers for high-performance computing and artificial intelligence, the initiative is centered around a new AI-optimized supercomputer to be installed in 2026.

Text: **Christopher Williams** (High-Performance Computing Center Stuttgart, HLRS)

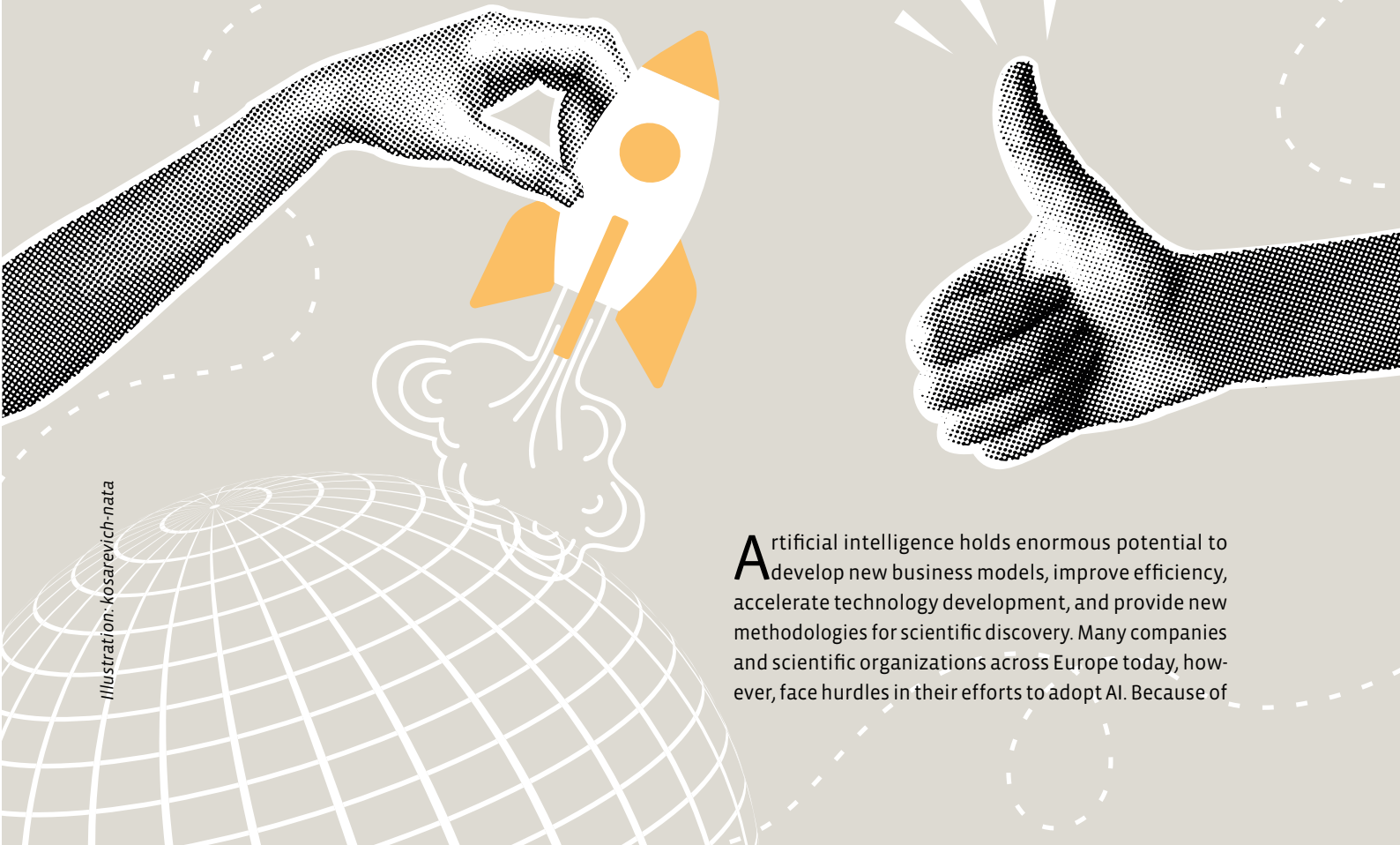


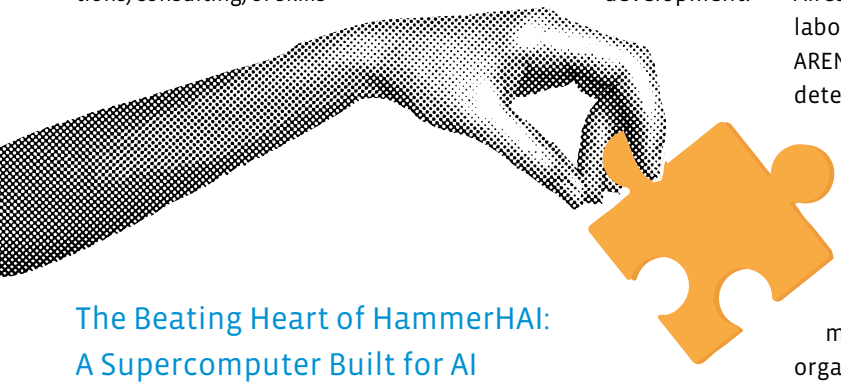
Illustration: kosarevich-nata

Artificial intelligence holds enormous potential to develop new business models, improve efficiency, accelerate technology development, and provide new methodologies for scientific discovery. Many companies and scientific organizations across Europe today, however, face hurdles in their efforts to adopt AI. Because of

limited access to large-scale AI computing infrastructure, a shortage of AI expertise, and data security concerns arising from a current reliance on offshore cloud AI service providers, European SMEs and startups in particular have been finding it challenging to keep pace with AI-driven innovation elsewhere in the world.

In a landmark attempt to jumpstart Europe's AI capabilities, the EuroHPC Joint Undertaking (JU) recently established a European network of what it calls "AI Factories." Conceived as technological ecosystems centered around powerful new AI-optimized supercomputing capabilities, 19 AI Factories are currently being implemented across Europe.

Among the first AI Factories to be announced was the German consortium HammerHAI. Coordinated by the High-Performance Computing Center Stuttgart (HLRS) in partnership with other leading German centers for high-performance computing and artificial intelligence, HammerHAI will make it easier for German and European developers and users of AI applications to access secure, scalable resources for AI model training and inference. With a focus on supporting AI capabilities in the fields of manufacturing, engineering, global challenges, and scientific research, HammerHAI is conceived as a one-stop shop for those in need of AI-capable computing hardware, solutions, consulting, or skills development.



The Beating Heart of HammerHAI: A Supercomputer Built for AI

At the heart of HammerHAI is a new, AI-optimized supercomputer that will soon be installed at HLRS. As of press time, a JU procurement process is underway and the new system, which will provide a high-performance platform for mid- to large-scale deep learning and artificial intelligence applications, is scheduled to arrive early in 2026. Because HLRS is a core facility at the University of Stuttgart and partner in the Gauss Centre for Supercomputing, the new supercomputer will also be accessible via the DFN's X-Win network.

Those interested in beginning to build capabilities for artificial intelligence do not need to wait for the new system to arrive, however. The HammerHAI consortium has already begun implementing services for AI users. "HammerHAI is open for business," said Dr. Bastian Koller, Managing Director of HLRS and lead coordinator of HammerHAI. "There is already a lot of excitement and AI users and technology developers have started approaching us to begin discussing potential applications and planning proof-of-concept studies. These activities are laying a foundation that will enable us and our user community to scale up quickly once the new system becomes available."

HammerHAI Offers a Broad Service Portfolio for AI Developers and Users

Alongside the procurement of the new supercomputer, HammerHAI is developing an extensive service portfolio that offers AI developers and users access to trained models, datasets, tools, and professional education — resources that will accelerate the development and implementation of new AI products. This service portfolio will include compute resources hosted not only by the HammerHAI consortium (which also includes the Leibniz Rechenzentrum, Karlsruhe Institute of Technology, the Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen, and HPC/AI consultancy SICOS BW) but also across a growing network of partner organizations. Using a brokering approach, HammerHAI will promote its partners' services and tools to a wider AI community while also facilitating users' access to them.

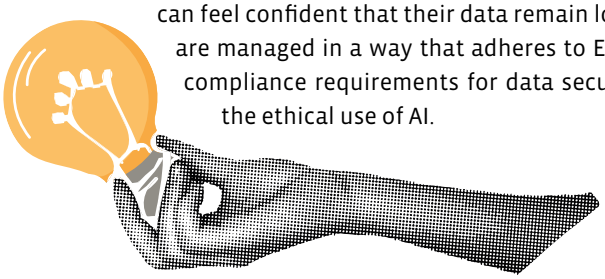
Already, HammerHAI is working with ARENA2036, a state-of-the-art laboratory for automotive research at the University of Stuttgart. ARENA2036 operates a system for object recognition and movement detection in digital twins using point cloud AI that it will make available for training automation systems. In another partnership, HammerHAI is collaborating with AI consultancy and technology developer Seedbox.ai. The company used HLRS's current Hunter supercomputer to train a large language model called KafkaLM in more than 20 European languages. In partnership with HammerHAI, Seedbox has made the model publicly available, offering multilingual capabilities for organizations operating across borders in Europe.

Unlike large-scale commercial AI service providers, HammerHAI emphasizes personalized user support as a key component of its strategy. Conceived as a "concierge service," a team of AI experts ensures that users get easy access to HammerHAI's systems and resources, and can answer technical questions that arise during system usage. Additionally, HammerHAI provides consultancy services for users at all stages of the AI application development pipeline, from strategic planning up through model deployment and monitoring.

"HammerHAI is here to support artificial intelligence solution developers throughout the entire AI life cycle," says Dennis Hoppe, leader of HLRS's Department of Converged Computing and a project manager in HammerHAI. "Whether you are just beginning to explore strategic opportunities for AI, or need support scaling or deploying

an existing application on a larger system, our mission is to provide expertise that can help you achieve your goals more quickly."

HammerHAI, together with the entire network of European AI Factories, is also an important step in securing Europe's technological sovereignty. German researchers, startups, and SME's can feel confident that their data remain local, and are managed in a way that adheres to European compliance requirements for data security and the ethical use of AI.



HammerHAI Partners with University of Edinburgh

The HammerHAI story also continues to develop. In October 2025, the EuroHPC Joint Undertaking announced the creation of 13 "AI Factory Antennas," a new category of competence centers for artificial intelligence that will complement and extend the activities of AI Factories across Europe. HammerHAI will participate as a partner in the UK AI Factory Antenna (UKAIFA), led by the Edinburgh Parallel Computing Centre (EPCC) at the University of Edinburgh. The UKAIFA will establish a bridge between the United Kingdom and the European AI Factory network. Together, HammerHAI and EPCC will undertake a variety of efforts to accelerate the adoption of artificial intelligence in SMEs, startups, industry, and the public sector, demonstrating how artificial intelligence can promote innovation and economic growth across numerous sectors of society. ◆

HammerHAI has received funding from the European High Performance Computing Joint Undertaking under grant agreement No. 101234027. The project is co-funded by the European Commission, the German Federal Ministry of Research, Technology and Space (BMFTR), the Baden-Württemberg Ministry of Science, Research and the Arts, the Bavarian State Ministry of Science and the Arts and the Lower Saxony Ministry of Science and Culture.

International Newsflashes

GÉANT Cybersecurity Campaign 2025 Highlights Cyber Mindfulness in the Age of AI

GÉANT recently launched the program for its 2025 Cybersecurity Campaign, and while the organization and its member national research and education networks (NRENs) are using leading technology and expertise to keep users safe, this year's campaign focuses on a more analog approach: cyber mindfulness as a tool to defend against AI-driven threats.

With the rapid rise of generative AI, malicious actors have a host of new tools and capabilities to manipulate people using deepfakes, voice cloning, AI-generated messages and alerts, and identity fraud. While these tools have advanced, attackers still rely on eliciting a strong emotional response, including urgency, shame, or authority to try and bypass rational decision making online. Accordingly, this year's campaign encourages people online to slow down, be mindful of what you are doing on the internet, and for people to make deliberate choices with their time online.

You can visit the campaign website here: https://security.geant.org/cybersecurity-campaign-2025/ ◆

International Newsflashes

EuroHPC JU Awards Contract to GÉANT to Hyperconnect European Supercomputers

The EuroHPC Joint Undertaking (EuroHPC JU) recently awarded GÉANT a contract to provide ultra-high-bandwidth, secure, pan-European interconnects for the EuroHPC supercomputing infrastructure across the continent. In forging this connection, the Association of European National Research and Education Networks and their connected research institutions – as well as public sector organizations, and industrial and technological stakeholders – will gain a powerful network connection to EuroHPC's computing infrastructure.

The EuroHPC JU launched an open call for tenders last year for a €60 million dollar contract to design, implement, and operate the organization's high-speed, hyperconnectivity infrastructure for the next four years.

Infrastructure improvements have already begun, with the first services becoming available to users in 2026. The investments will bring significant benefits for those relying on EuroHPC JU-funded high-performance computing (HPC) resources, including:

- High-throughput capacity, with transmission speeds targeted in the terabits-per-second range, to enable faster data movement in support of modelling, AI and simulation workloads.
- Robust security architecture designed to safeguard sensitive and cross-border research data.
- Federated design, connecting European, national and regional supercomputing centres into a unified structure.
- High-capacity connections to internet exchanges and data providers, ensuring flexible access for all EuroHPC JU use cases, including users from the public sector and industry.
- Flexible and adaptable services that will allow incorporation of emerging technologies and meet the varying needs of the supercomputing ecosystem.

For more information, please visit:
https://connect.geant.org/2025/09/22/eurohpc-ju-awards-contract-to-geant-to-hyperconnect-european-supercomputers ◆

Supporting Secure Collaboration and Compliance Across Europe: GÉANT Certified Under ISO 27001 Standard

Recently, GÉANT gained certification under the ISO 27001 standard, furthering the organization's commitment to the highest standards of information security management globally. The ISO 27001 standard outlines requirements for an effective information security management system and sets guidelines for how risks are assessed and managed through organizational policies, controls, and continuous improvement practices. The certification provides GÉANT with external validation that the organization's management practices are mature, transparent, and consistent with the highest international standards.

The GÉANT community also gains practical benefits through the certification. The certification supports and enhances eligibility in competitive funding environments, streamlines procurement by clearly demonstrating due diligence, and meets the security requirements increasingly embedded in all cross-border initiatives. All of these goals directly contribute to the EU Cybersecurity Strategy and Digital Decade.

For more information, please visit:
https://connect.geant.org/2025/09/11/supporting-secure-collaboration-and-compliance-across-europe-geants-iso-27001-certification ◆

Collaboration on this Newsflash: Eric Gedenk

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

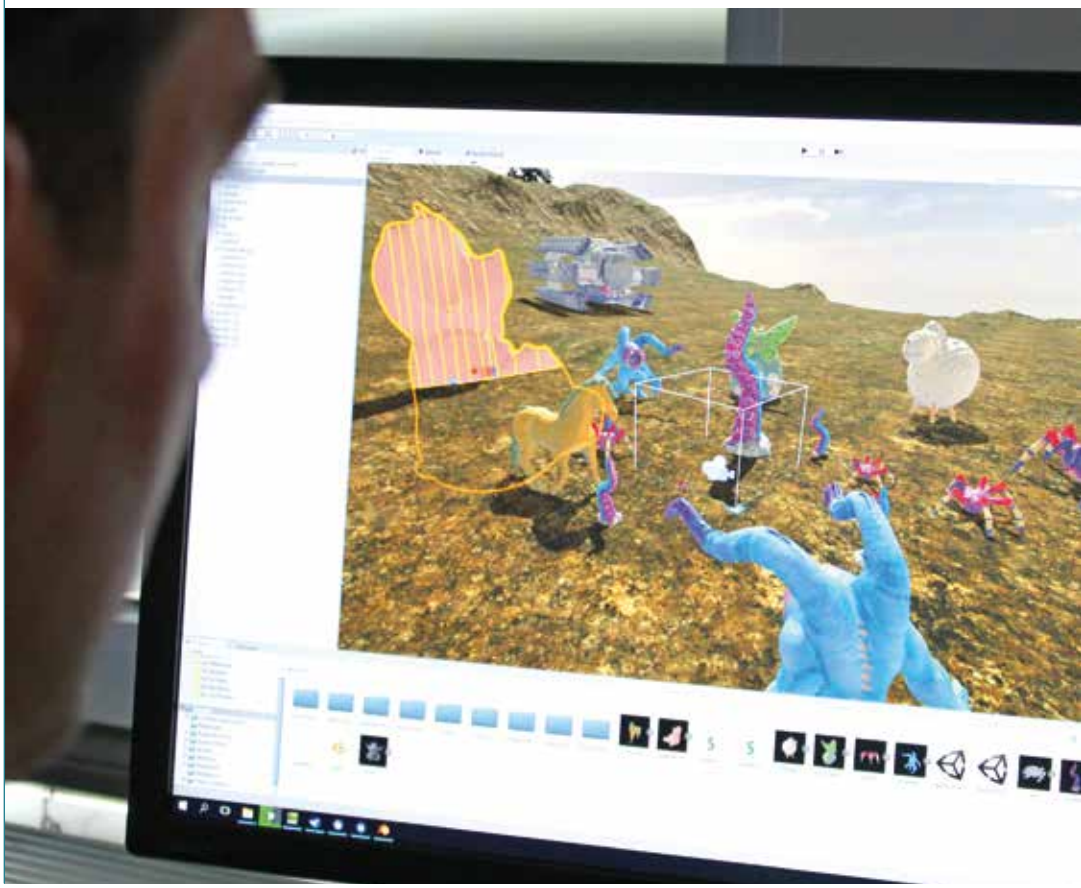
THE FIELD

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.

Game On – at the University of Bayreuth's Game Innovation Lab

Students at the University of Bayreuth can focus their studies on video game design. In the last decade, the university developed its Game Innovation Lab to equip students with a combination of technical skills infused with a strong humanities foundation. A recent exhibit at the Regensburg UNESCO Visitors' Center demonstrates the power of games to educate and entertain.

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



Photos: Universität Bayreuth

Students focused on game design are increasingly venturing into virtual and augmented reality when developing next-generation video games

Uni Bayreuth's Game Innovation Lab encourage students to look beyond creating games that follow the tropes of „superhero power fantasies"

Prof. Jochen Koubek has a "cold love" for video games. Growing up, Koubek enjoyed playing games on his Commadore 64. When he began studying mathematics, informatics, and philosophy at the Technischen Hochschule Darmstadt (the precursor to the Technical University of Darmstadt), Koubek had far less time for recreational gaming, but developed a passion for working at the intersection of cultural and technological phenomena. "I decided to get my PhD in Cultural Studies back in 1997, because I was quite interested in how culture is changing and emerging in the age of the dawning of the internet," he said.

When he joined the University of Bayreuth in 2009, he wanted to expand the university's strength in film studies and film making into new digital media spaces while retaining the institution's focus on students acquiring practical skills in addition to theory. In 2011, the university started a bachelor's degree program for students to focus on both film and games, and in 2015, the university added a graduate program dedicated to studying game theory, game design, game development, and computer science. "These developments helped reactivate my interest in video games," he said. "While I am not often thrilled about the latest triple-A title, I appreciate the value of a good game. We are interested in studying games from a media scholar's perspective, and games' potential in this realm is increasing because of new technologies and the emergence of artificial intelligence."

Five years later, in 2017, the University of Bayreuth applied for and received funding from the State of Bavaria and the German federal government for developing the Game Innovation Lab (GIL). The GIL brings together staff working on the practical, technical side of game development with experts in media studies. Together, students are exposed to both practical and theoretical aspects of game development. This approach has already paid dividends: recently, students Ruben Schäfer and Nic Schilling developed *Salzsammler*, an interactive game for the Regensburg UNESCO World Heritage Visitor Center that not only entertains young visitors, but also gives them a tactile taste of medieval Bavarian history.

As a participating organization in the German Research Network (DFN), the University of Bayreuth can provide students and faculty the network security, reliability, and bandwidth to explore new forms of interactivity and easily collaborate remotely with their peers and the greater gaming community.

Game design is system design

While many young students arrive in Koubek's courses focused on creating the next triple-A studio or developing the next blockbuster game, he draws their attention to developing skills that go beyond successful game development. "Game design is system design," he said. "Understanding how to develop games is understanding formal systems, because they are computer programs at the end of the day. By focusing on system design, we are equipping students to look at other systems – be it business structures, social phenomena, or otherwise – and to understand feedback loops, resource flows, and other more abstract concepts than if you are only looking at this from a technical perspective. Game design is also social design, as you are designing experiences in an interactive, dynamic system."

Koubek and his fellow professors encourage students to look beyond creating games that are purely designed to fall in line with other common tropes used in the most popular games and films—namely, he wants them to depart from the "superhero power fantasies" that drive many games' narratives. "If we look at society and our current time, almost all of our problems are systemic problems," he said. "Sometimes, there is one villain or one bad actor that is causing a major problem, but most of the time, we all want the best outcome for a given situation, but it is getting worse because

Salzsammler lets children explore history through play — an augmented-reality logistics and trade simulator at Regensburg's UNESCO World Heritage Visitor Center that brings a deeper understanding of historical and cultural connections | *Photos: Schilling & Schäfer GbR, Salzsammler Studios*

there are other interdependencies that nobody is considering. Storytelling is important, but if you want to sell a game, you are ultimately selling a system."

The coursework aims at helping students understand video games as a distinct medium, and Uni Bayreuth faculty members focus on getting students to put games into contexts that go beyond pure entertainment.

Salzsammler brings interactivity into World Heritage Visitor Center Regensburg

Several years ago, one of Koubek's GIL colleagues, Robin Hädicke, took his children to the UNESCO World Heritage Visitor Center Regensburg, one of the city's flagship museums. He noticed that his 8-year-old son was not particularly engaged with the exhibits, and when the museum solicited feedback, Hädicke discussed ways that the Uni Bayreuth GIL could help improve engagement and interactivity with younger audiences.

With reliable network connections, students working in the GIL have ample opportunity to experiment in developing virtual and augmented reality systems, among other innovative new avenues for gaming. When the professors discussed an opportunity to develop an engaging, educational, interactive game for the Visitor Center, Schäfer and Schilling began to collaborate on a game that would not only engage younger visitors, but also highlight Regensburg's history river-based trade hub.

"The Game Innovation Lab gave us the space to explore ideas where history becomes interactive," Schilling said. "That support inspired us to design experiences that let kids engage with the past in playful, meaningful ways."

Salzsammler is an augmented-reality logistics and trade simulator, asking players to work together to collect trade goods coming from ships traveling the Danube river. The developers use projectors and motion-tracking software to allow students to "push" boats toward their appropriate docking station while others must move large, three-dimensional dice to deliver the correct trade good. As players grow their trade business, so does medieval Regensburg.

For Koubek, projects like these demonstrate the power of video games to do more than just entertain. "Some students may just play around with this system and move the boats along the river and have fun," he said. "But I think about a game like The Oregon Trail, which was an early educational game about the American Western frontier. Many people even today will say that almost everything they remember about that part of history came from playing that game. It was a much more intense experience, and that is what we want to cultivate in our students." ◆

For more information on Uni Bayreuth's Game Innovation Lab, please visit: **https://www.uni-bayreuth.de/en/transfer-innovation/game-innovation-lab**

For more information on *Salzsammler*, please visit: **https://salzsammler.de/#/**

Wie sicher ist sicher genug?

OVG NRW zu erforderlichen IT-Sicherheitsmaßnahmen im Sinne von Art. 32 DSGVO bei Datenübermittlungen

Bei der Verarbeitung personenbezogener Daten folgt aus der Datenschutz-Grundverordnung (DSGVO) die Pflicht, angemessene Sicherheitsmaßnahmen zu treffen. Welche Maßnahmen konkret zu ergreifen sind, hängt von den Umständen des Einzelfalls ab. Das Oberverwaltungsgericht Nordrhein-Westfalen (OVG NRW) hat sich in seinem Beschluss vom 20. Februar 2025 (Az. 16 B 288/23)[1] nun mit der Frage beschäftigt, welche Sicherheitsmaßnahmen eine Behörde ergreifen muss, um Daten DSGVO-konform zu übermitteln.

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

Foto: topntp26 / Freepik

I. Angemessene Sicherheitsmaßnahmen in der DSGVO

Die Vorschriften der DSGVO beschränken sich nicht allein darauf, die freie Verwendung personenbezogener Daten durch den Verantwortlichen zu beschränken (Art. 6 DSGVO). Der Verantwortliche, der über die Zwecke und Mittel der Datenverarbeitung entscheidet, ist gemäß Art. 32 DSGVO auch verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der Datenverarbeitung zu gewährleisten.[2] Diese Maßnahmen sollen vor allem einen unberechtigten Datenzugriff durch Dritte verhindern. Sofern der Datenverarbeiter keine geeigneten Maßnahmen getroffen hat und es infolgedessen zu einem Datenverlust kommt, kann der Betroffene gemäß Art. 82 DSGVO Schadenersatz vom Datenverarbeiter für erlittene Schäden verlangen.[3] Ein Verstoß gegen Art. 32 DSGVO kann zudem durch Bußgelder der Datenschutzaufsichtsbehörden geahndet werden.[4]

Als mögliche technische und organisatorische Maßnahmen nennt Art. 32 Abs. 1 DSGVO folgende: die Pseudonymisierung und Verschlüsselung personenbezogener Daten (lit. a), die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (lit. b), die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (lit. c) sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (lit. d).

In der Praxis stellt sich für datenverarbeitende Stellen die Frage, welches Maß an IT-Sicherheit im konkreten Fall erforderlich ist.[5] Ein perfektes, absolut sicheres System existiert nicht. Insbesondere menschliche Fehler können stets zu IT-Sicherheitsrisiken führen. Von datenverarbeitenden Stellen darf keine absolute Sicherheit verlangt werden. Dies würde mit unzumutbaren Kosten einhergehen, durch die in vielen Fällen eine Datenverarbeitung unwirtschaftlich werden würde. Entweder würden die Kosten auf die Kunden der datenverarbeitenden Stelle umgewälzt werden oder Datenverarbeitungen könnten seltener vorgenommen werden. Daher besteht an einem unzumutbaren Maß an IT-Sicherheit keinerlei Interesse.

Aus Art. 32 Abs. 1 DSGVO ergibt sich, dass für die konkret zu ergreifenden Maßnahmen der Stand der Technik, die Implementierungskosten, die Umstände der Datenverarbeitung sowie die Wahrscheinlichkeit des Eintritts eines Schadens und dessen voraussichtliche Höhe maßgeblich sind.

Art. 32 Abs. 2 DSGVO nennt zudem als einzelnes relevantes Kriterium für das zu ergreifende Schutzniveau das Risiko, das mit der Datenverarbeitung einhergeht. Ein hohes Risiko, etwa bei einer Vielzahl betroffener Personen oder der Offenlegung besonders sensibler Daten, erfordert es auch, höhere Schutzmaßnahmen zu ergreifen.

Gemäß Art. 32 Abs. 3 DSGVO kann als Faktor auch herangezogen werden, ob spezifische Verhaltensregeln oder Zertifizierungsverfahren für die datenverarbeitende Stelle bestehen und ob diese Verfahren eingehalten wurden. Solche Verhaltensanforderungen können gemäß Art. 40 DSGVO von Verbänden oder anderen Vereinigungen, die datenverarbeitende Stellen vertreten, ausgearbeitet werden. Sie können insbesondere kleinen und mittleren Unternehmen den Verfahrensaufwand deutlich erleichtern. Die Beachtung solcher Verfahrensregelungen kann jedoch lediglich als Indiz für die Einhaltung von Art. 32 DSGVO dienen.

Ausnahmsweise können sich für bestimmte datenverarbeitende Stellen auch konkretere Anforderungen aus spezifischen gesetzlichen Regelungen ergeben. Für Angehörige der Kritischen Infrastrukturen gelten etwa die Bestimmungen der NIS 2-Rl.[6]

---

1 Das Urteil kann unter folgendem Link abgerufen werden: https://nrwe.justiz.nrw.de/ovgs/ovg_nrw/j2025/16_B_288_23_Beschluss_20250220.html (alle Links des Beitrags zuletzt abgerufen am 04.06.2025).

2 Hierzu ausführlich McGrath, Der Stand zwischen den Stühlen, DFN-Infobrief Recht 01/2021. Mit der Frage, ob diese Pflicht durch eine Vereinbarung zwischen dem Verantwortlichen und der betroffenen Person abbedungen werden kann, hat sich ausführlich der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit beschäftigt. Der Vermerk ist abrufbar unter: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Vermerke_und_Stellungnahmen/Vermerk-Abdingbarkeit_TOMs.pdf. Hierzu besteht auch ein Beschluss der Datenschutzkonferenz. Dieser ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf.

3 Müller, ich glaub, es hackt, DFN-Infobrief Recht 4/2024.

4 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat jüngst die Vodafone GmbH wegen Verstoßes gegen Art. 32 DSGVO verwarnt. Die Pressemitteilung ist abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/06_Geldbu%C3%9Fe-Vodafone.html?nn=251944.

5 Zu der Schwierigkeit dieser Feststellung ausführlich McGrath, Der Stand zwischen den Stühlen, DFN-Infobrief Recht 01/2021.

6 Hierzu John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?, DFN-Infobrief Recht 04/2023 und Geiselmann, Heute schon geNISt?, DFN-Infobrief Recht 04/2025.

Für die Mehrzahl der datenverarbeitenden Stellen existieren hingegen keine konkretisierten Sicherheitsanforderungen. Die Frage, ob die ergriffenen Sicherheitsmaßnahmen den Anforderungen von Art. 32 DSGVO genügt haben, verbleibt eine Frage des Einzelfalls, deren Beantwortung selbst vielen Gerichten enorme Schwierigkeiten bereitet. Hierbei wird auch immer zu berücksichtigen sein, welche Sicherheitsmaßnahmen dem aktuellen Stand der Technik entsprechen.

II. Verfahren vor dem VG Köln und OVG NRW

Mit der Frage, ob eine datenverarbeitende Stelle die erforderlichen Sicherheitsmaßnahmen ergriffen hat, musste sich auch das OVG NRW beschäftigen. Dem ging ein Verfahren vor dem Verwaltungsgericht (VG) Köln voraus. Dieses hatte sich mit der Klage eines Geschäftsmanns auseinanderzusetzen, der beruflich mit explosiven Stoffen handelte und sich als wirtschaftlich Berechtigter im elektronischen Transparenzregister eintragen musste. Aus Sorge um seine Sicherheit stellte er bei der zuständigen Behörde einen Antrag, der sich unter anderem darauf richtete, dass seine personenbezogenen Daten ausschließlich mit einer sicheren Ende-zu-Ende-Verschlüsselung verarbeitet und übermittelt werden dürften. Aufgrund seines Berufs behauptete er, dass eine besondere Gefahr bestehe, Opfer schwerer Straftaten zu werden. Der Geschäftsmann sah sein Begehren als nicht befriedigt durch die Behörde an und reichte beim VG Köln einen Antrag auf eine einstweilige Verfügung ein. Demnach sollte das Gericht anordnen, dass die Behörde eine sicherere Verschlüsselungstechnik zu verwenden habe. Er argumentierte, dass die von der Behörde genutzte Transportverschlüsselung (TLS) keinen ausreichenden Schutz biete, da sie nur den Transport verschlüssele. Zudem genüge bereits die verwendete Verschlüsselung TLS 1.2 nicht, da seit 2018 TLS 1.3 Stand der Technik sei. Die Behörde hielt dem entgegen, dass ihr Sicherheitskonzept vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert sei. Die verwendete TLS-Verschlüsselung sei ausreichend. Die Kommunikation innerhalb des Netzes des Bundes werde zudem zusätzlich durch eine sogenannte SINA-Box und Client-Zertifikate abgesichert. Eine Ende-zu-Ende-Verschlüsselung mache das Register für Behörden unbrauchbar, da gesetzlich vorgeschriebene behördliche Abfragen dann unmöglich wären.

III. Unterschiedliche Verschlüsselungstechniken

Für das Verständnis der Gerichtsverfahren ist es entscheidend, zwischen den diskutierten Verschlüsselungsmethoden zu unterscheiden. Im Kern geht es dabei um den Unterschied, ob nur der Übertragungsweg der Daten geschützt wird oder ob die Dateninhalte selbst unlesbar gemacht werden.

1. Transportverschlüsselung

Die Transportverschlüsselung baut einen verschlüsselten Kanal zwischen dem Gerät des Nutzers und dem Zielserver auf. Während der Übertragung sind die Daten in diesem Kanal wirksam vor dem Mitlesen durch Dritte geschützt.

Ein wesentliches Merkmal dieser Methode ist jedoch, dass der Schutz am Zielort endet. Der Server des Betreibers muss die Daten entschlüsseln, um sie weiterverarbeiten zu können.

Der Streit um TLS 1.2 gegenüber TLS 1.3 ist dabei eine Frage der Modernität und Sicherheit des eingesetzten Systems. TLS 1.3 ist das direkte Nachfolgersystem und gilt als sicherer und effizienter, da es auf bekannte Schwachstellen älterer Verschlüsselungsverfahren verzichtet. Dennoch ist TLS 1.2 nach wie vor weit verbreitet, da keine Schwachstellen bekannt sind und so ein Upgrade auf TLS 1.3 nicht als unbedingt notwendig erachtet wird.[7]

2. Ende-zu-Ende-Verschlüsselung

Einen anderen Ansatz verfolgt die vom Kläger geforderte Ende-zu-Ende-Verschlüsselung. Hierbei wird nicht nur der Kanal, sondern der Dateninhalt selbst kryptografisch versiegelt. Die Verschlüsselung findet direkt auf dem Gerät des Absenders statt, und nur der vorgesehene Empfänger kann die Daten wieder entschlüsseln.

7 A10, Hauptunterschiede zwischen TLS 1.2 und TLS 1.3, abzurufen unter: https://www.a10networks.com/de/glossary/key-differences-between-tls-1-2-and-tls-1-3/ [Stand: 26.05.2025].Die Entscheidung kann abgerufen werden unter: https://openjur.de/u/2517924.html.

IV. Beschlüsse des VG Köln des OVG NRW

Das Verwaltungsgericht Köln lehnte in seiner Entscheidung (Az. 13 L 1467/22) den Antrag ab. Es nahm an, dass der Antragsteller nicht ausreichend glaubhaft machen konnte, dass speziell aus der Datenverarbeitung durch das Transparenzregister ein derart hohes und konkretes Risiko für ihn erwächst, welches eine Ende-zu-Ende-Verschlüsselung zwingend erfordern würde. Die allgemeinen Verweise auf seine berufliche Tätigkeit und bereits bestehende Schutzmaßnahmen in anderen Registern reichten dafür nicht aus. Das Gericht bewertete die von der Behörde eingesetzte, BSI-zertifizierte TLS-Verschlüsselung als eine dem Risiko angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahme. Ein verbleibendes Restrisiko bei der digitalen Kommunikation sei als allgemeines Lebensrisiko hinzunehmen.

Gegen die Entscheidung des VG Köln legte der Antragsteller Beschwerde vor dem OVG Münster ein. Auch das OVG Münster teilte jedoch die Auffassung des Antragsgegners und des VG Köln. Es nahm ebenso an, dass der Antragsteller das von ihm behauptete besondere Risiko nicht glaubhaft gemacht habe. Ohne den Nachweis eines solchen erhöhten Risikos lasse sich ein Anspruch auf eine sicherere Verschlüsselungsmaßnahme nicht aus der DSGVO ableiten. Es sei nicht ersichtlich, dass bei der Behörde eine besonders hohe Wahrscheinlichkeit bestehe, Opfer von Hackerangriffen zu werden. Auch das OVG Münster berücksichtigte in seinem Beschluss, dass die Sicherheitstechnik der Behörde vom BSI zertifiziert worden ist. Zudem führte das Gericht aus, dass die TLS-Verschlüsselung nicht die einzige Sicherheitsmaßnahme ist. Es verwies explizit auf die zusätzlichen Sicherungen im Kommunikationsprozess mit anderen staatlichen Stellen, wie die SINA-Box und Client-Zertifikate. Darüber hinaus wurden die im Beschwerdeverfahren ergänzten Ausführungen der Antragsgegnerin berücksichtigt, nach denen bei den jeweiligen Datenübertragungen keine „Zwischenstationen“ existierten, auf denen die Inhalte unverschlüsselt abgelegt wären. Damit wurde angenommen, dass das eingesetzte Verfahren den Anforderungen aus Art. 32 DSGVO genügt.

V. Relevanz für wissenschaftliche Einrichtungen

Auch wissenschaftliche Einrichtungen müssen sich die Frage stellen, welche Sicherheitsmaßnahmen sie zum Schutz personenbezogener Daten ergreifen. Aus den dargestellten Gerichtsentscheidungen ergibt sich, dass ein absoluter Schutz von Art. 32 DSGVO nicht gefordert wird. Maßgeblich ist vor allem die Wahrscheinlichkeit eines Sicherheitsvorfalls und wie hoch in einem solchen Fall der Schaden ausfallen würde. Demnach sind immer die Umstände des Einzelfalls für die konkret zu ergreifenden Maßnahmen entscheidend. In einer anderen Konstellation hat etwa das Oberlandesgericht (OLG) Schleswig in seinem Urteil vom 18. Dezember 2024 (Az. 12 U 9/24)[8] angenommen, dass eine Ende-zu-Ende-Verschlüsselung für den Versand geschäftlicher E-Mails erforderlich sei und eine Transportverschlüsselung nicht genüge. Das VG Frankfurt hat wiederum in einem Beschluss vom 15. Juli 2022 (Az. 5 L1281/22.F)[9] – ähnlich wie die zuvor dargestellten Entscheidungen – eine Transportverschlüsselung als ausreichend betrachtet. Den dargestellten Entscheidungen des VG Köln und des OVG NRW kann konkret entnommen werden, dass die Gerichte Zertifizierungen durch das BSI anerkennen. Diesen kann eine besondere Bedeutung bei der Frage zukommen, ob ein Sicherheitskonzept den Anforderungen von Art. 32 DSGVO genügt. ◆

8 Das Urteil kann unter dem folgenden Link abgerufen werden: https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/NJRE001598708.
9 Das Urteil kann unter dem folgenden Link abgerufen werden https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE220003171.

Automatisierte Kontrollen als Gamechanger?

Datenschutzbehörden prüfen Websites vermehrt mithilfe automatisierter Tools auf ihre Datenschutzkonformität

Seit 2024 nutzen Datenschutzbehörden in Deutschland automatisierte Prüfinstrumente bei ihrer Überwachungstätigkeit. Bisher erfolgten vor allem automatisierte Kontrollen von Websites. Ein Problem bei Websites ist oft eine fehlende oder unzureichende Einbindung von Einwilligungsbannern (auch bekannt als Cookie-Banner), auch und gerade wenn Drittdienste auf der Website genutzt werden. Hochschulen und Forschungseinrichtungen sollten auf einen datenschutzkonformen Web-Auftritt achten.

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

Illustration: kirill_makarov/Adobe Stock

I. Automatisierte Prüfungen von Websites

Die Einhaltung der DSGVO gehört nach Art. 57 Abs. 1 lit. a, lit. f, lit. h DSGVO zu den Aufgaben der Datenschutzbehörden. Zusätzlich überprüfen sie auch die Einhaltung von Teilen des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG). Lange Zeit gab es allerdings wiederholt Kritik, dass die deutsche Behördenlandschaft bei der Durchsetzung von Datenschutzvorschriften nicht konsequent genug sei.[1] Die Knappheit an Personalressourcen, finanziellen Möglichkeiten und technischen Mitteln tat ihr Übriges in Sachen Durchsetzungsdefizit. Doch seit dem

1 Dachwitz/Fanta, 24.5.2023: https://netzpolitik.org/2023/5-jahre-datenschutzgrundverordnung-die-fuenf-groessten-schwaechen-der-dsgvo/ (alle Links dieses Beitrags wurden zuletzt am 28.5.2025 abgerufen).

vergangenen Jahr scheint frischer Wind in einigen Datenschutzbehörden zu wehen. IT-Labore werden etabliert und automatisierte Prüfungstools kommen zunehmend zum Einsatz – bisher vor allem bei der Überprüfung von Websites auf ihre Datenschutzkonformität. Als jüngstes Beispiel ist eine Prüfung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) zu nennen. Mitte April 2025 gab die Behörde bekannt, dass sie 1000 in Hamburg betriebene Websites mithilfe eines automatisierten Tools auf die datenschutzkonforme Einbindung von Drittdiensten überprüft hat.[2] Anlass für die Prüfung waren Beschwerden zum Tracking durch Drittdienste auf Websites, ohne dass die Besucher:innen vorher in das Tracking eingewilligt hatten. Die überprüften Websites wurden nach dem Zufallsprinzip ausgewählt. Bei 185 der geprüften Websites stellte der HmbBfDI Mängel fest.

Der HmbBfDI ist jedoch nicht die erste Behörde, die automatisierte Prüfungstools einsetzt. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überprüfte bereits 2024 mehr als 350 Websites von bayerischen Betreiber:innen teilweise automatisiert.[3] Die Prüfung betraf die Frage, ob beim Öffnen einer Website auf der ersten Ebene des Einwilligungsverarbeitungsbanners (sog. Cookie-Banner) neben der Zustimmungsmöglichkeit auch eine Möglichkeit zur Ablehnung der Verarbeitung vorliegt. Eine Ablehnung soll ähnlich leicht erfolgen können wie eine Zustimmung.[4] 350 Websites genügten den Anforderungen nicht und wurden benachrichtigt. Die Betreiber:innen hatten danach die Möglichkeit, sich zu den Feststellungen zu äußern und die Websites anzupassen.

Durch die automatisierten Prüfungen kann allerdings eine viel größere Anzahl an Websites kontrolliert werden. Im Mai 2024 erklärte die Sächsische Datenschutz- und Transparenzbeauftragte (SDTB), dass ihre Behörde mithilfe eines automatisierten Tools 30000 Websites von Unternehmen, Vereinen und öffentlichen Stellen mit Sitz in Sachsen auf den rechtswidrigen Einsatz von Google Analytics untersucht hat.[5] Auf 2300 dieser Websites wurden die Daten von Google Analytics[6] ohne die Einwilligung der Nutzer:innen erhoben. Die Betreiber:innen wurden im Anschluss aufgefordert, auf ihren Websites nachzubessern. Die Maßnahme zeigte Wirkung. Eine Nachuntersuchung der SDTB im Oktober 2024 ergab, dass viele Websites angepasst wurden.[7]

Weitere Datenschutzbehörden könnten dieser Durchsetzungspraxis folgen und in Zukunft ebenfalls automatisierte Prüfungen durchführen. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit stellte in seinem Tätigkeitsbericht für das Jahr 2024 ein Toolkit vor, das verschiedene Prüf-Tools miteinander verbindet, um eine umfassende technische Analyse von Websites effizient zu ermöglichen. Der Ablauf einer solchen Prüfung und die Funktionen werden in dem Bericht genauer erklärt.[8] Auch der Europäische Datenschutzausschuss (EDSA) bietet seit Anfang 2024 ein Open-Source-Tool für automatisierte Überprüfung von Websites an.[9]

II. Einwilligungen auf Websites und bei Einbindung von dritten Diensten

Beim Betrieb von Websites sind sowohl datenschutzrechtliche Vorgaben nach dem TDDDG[10] als auch nach der DSGVO einzuhalten. In den untersuchten Fällen ging es um Cookie-Banner in unterschiedlichen Konstellationen. Cookie-Banner begegnen Internetnutzer:innen beim Besuch von Websites häufig und informieren über eine geplante Speicherung oder Nutzung von Daten. Cookies selbst sind Textdateien, die beim Aufruf einer Website erzeugt und gespeichert werden.[11] Über Cookies können diese Informationen auf den Endgeräten der Nutzer:innen gespeichert werden. Sie können aber auch

2 Pressemitteilung, 24.4.2025: https://datenschutz-hamburg.de/news/tracking-durch-drittdienste-185-von-1000-geprueften-websites-muessen-nachbessern.

3 Pressemitteilung, 9.4.2024, https://www.lda.bayern.de/media/pm/pm2024_02.pdf.

4 Der Landesbeauftragte für den Datenschutz Niedersachsen und in der Folge auch das VG Hannover beschäftigten sich ebenfalls mit dieser Thematik. Im Urteil wurde festgestellt, dass bei Verwendung einer „Alle akzeptieren“ – auch eine „Alles ablehnen“-Schaltfläche auf der ersten Ebene von Cookie-Banner verwendet werden muss. Siehe dazu Pressemitteilung, 20.5.2025: https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/urteil-zu-manipulativem-cookie-banner-alles-ablehnen-schaltflache-ist-ein-muss-241960.html.

5 Pressemitteilung, 13.6.2024, https://www.medienservice.sachsen.de/medien/news/1076636.

6 Zum Einsatz von Google Analytics siehe Baur, Unmaskiert wird abkassiert!, DFN-Infobrief Recht 8/2019.

7 Tätigkeitsbericht Datenschutz 2024 der Sächsischen Datenschutz- und Transparenzbeauftragten, S. 41, 43, https://www.datenschutz.sachsen.de/download/taetigkeitsberichte/Taetigkeitsbericht_Datenschutz_2024.pdf.

8 53. Tätigkeitsbericht zum Datenschutz für das Jahr 2024, S. 218 ff.: https://datenschutzarchiv.org/fileadmin/Dokumente/2024/TB_Hessen_LfD_53_2024_de.pdf.

9 https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/edpb-website-auditing-tool_en.

10 Zum TDDDG siehe Yang-Jacobi, Telemedien out, Digitale Dienste in!, DFN-Infobrief Recht 8/2024. Genaueres zum Inhalt siehe John, TTDSG – Die Profis in spe, DFN-Infobrief Recht 5/2021.

11 Siehe zu Cookies vor allem John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 1/2022.

zu Trackingzwecken dienen und die Aktivität von Website-Besucher:innen nachverfolgen. Dabei ist es wichtig, dass Nutzer:innen selbst entscheiden können, ob ihre Daten für Nutzungsprofile verwendet werden dürfen.

Im TDDDG finden sich unter anderem die gesetzlichen Regelungen zum Speichern und Abrufen von Informationen auf den Endgeräten. § 25 Abs. 1 TDDDG legt den Grundsatz fest, dass Nutzende einwilligen müssen, wenn Informationen in der Endeinrichtung gespeichert werden oder auf diese auf dem Endgerät gespeicherten Informationen zugegriffen wird. § 25 Abs. 2 Nr. 2 TDDDG regelt eine Ausnahme des Einwilligungsgrundsatzes, wenn die Informationen zur Erbringung des Dienstes erforderlich sind. Sofern die Nutzung bestimmter Funktionen auf einer Website essenziell ist, sind es technisch erforderliche Cookies und es bedarf keiner Einwilligung der Nutzenden. Beispiele sind die Speicherung von Spracheinstellungen oder die Authentifizierung der Nutzenden für die Dauer der Sitzung. Bei technisch nicht notwendigen Cookies, wie zum Beispiel Cookies zu Werbezwecken, ist eine Einwilligung jedoch zwingend erforderlich.[12] Die Einwilligung erfolgt in der Regel über die bekannten Cookie-Banner.[13] Sie muss freiwillig im Sinne des § 25 Abs. 1 TDDDG und des Art. 4 Nr. 11 DSGVO erfolgen. So sollen Cookie-Banner Nutzende bei ihrer Entscheidung nicht leiten (sog. „nudging“). Teilweise werden auch genauere Vorgaben zur Gestaltung vertreten.[14]

In dem Zusammenhang ist eine weitergehende Unterscheidung zwischen First-Party-Cookies, die von der aufgerufenen Website selbst gesetzt werden, und Third-Party-Cookies, die von einer fremden Domain gesetzt werden, möglich. Die technische Notwendigkeit kann bei beiden Cookie-Arten vorliegen. Dritte Dienste können Analyse-Dienste, Karten-Dienste oder auch Social-Media-Plug-Ins/Buttons sein. Sie dienen der statistischen Analyse von Besucherzahlen, Verweildauer oder auch besuchten Seiten und Aktionen oder zeigen Standorte auf einer Karte an. Das Verhalten der Nutzenden kann dadurch erfasst und ausgewertet werden. Gerade bei Drittdiensten, die Informationen in der Endeinrichtung des Endnutzenden speichern, § 25 Abs. 1 TDDDG, oder auch personenbezogene Daten über mehrere Websites hinweg sammeln und umfangreiche Nutzerprofile erstellen, ist eine Einwilligung für eine rechtmäßige Datenverarbeitung notwendig, Art. 6 Abs. 1 S. 1 lit. a DSGVO.[15] Wenn diese also unmittelbar bei Aufruf der Website aktiviert werden und keine Einwilligung erfolgt, liegt ein Verstoß gegen die datenschutzrechtlichen Regelungen vor.

III. Bedeutung für Hochschulen und Forschungseinrichtungen

Die neuen Möglichkeiten von Datenschutzbehörden durch IT-Labore und die darin durchführbaren automatisierten Prüfungen werden vermutlich zu mehr Kontrollen führen. Auch Hochschulen und Forschungseinrichtungen sollten ihre bestehenden und künftigen Websites auf Datenschutzkonformität überprüfen. Dazu gehört neben einer Datenschutzerklärung nach Art. 13, 14 DSGVO auch eine – im Idealfall einrichtungsweit einheitliche – Handhabung von Cookie-Bannern und Drittdiensten. Sofern Dienste Dritter (zu Analysezwecken oder um Standorte anzuzeigen) nicht zwingend notwendig sind, sollte darauf verzichtet werden. Falls Drittdienste dennoch auf den Websites eingebunden werden, ist auf eine gesonderte und wirksame Einwilligung zu achten. Die Drittdienste dürfen dann nur bei den Nutzer:innen aktiviert werden, die die entsprechende Einwilligung erteilt haben. ◆

12 Eine Ausnahme stellen die sogenannten Paywall-Cookies bei Medienkonzernen dar.

13 Um der Vielzahl der Cookie-Banner entgegenzuwirken, sind sogenannte Personal/Privacy Information Management Systeme zur Einwilligungsverwaltung vorgesehen, § 26 TDDDG. Zur am 1.4.2025 in Kraft getretenen Einwilligungsverwaltungsverordnung siehe Schöbel, Das Ende der Cookie-Banner, DFN-Infobrief Recht 3/2025.

14 Bereits 2022 erhob die Verbraucherzentrale NRW Klage gegen Google wegen der Ausgestaltung ihrer Cookie-Banner. Google änderte die Cookie-Banner dahingehend, sodass das Verfahren für erledigt erklärt wurde und ohne Urteil endete, siehe Palenberg, Google brings light into the dark pattern, DFN-Infobrief 2/2023.

15 Dies gilt gerade für Google-Drittdienste, siehe die jüngst ergangene Entscheidung des VG Hannover, Urt. v. 19.3.2025, Az. 10 A 5385/22, BeckRS 2025, 10472, Rn. 76 ff.

Die Kunst des steten Wandels

Alle Fotos: Jürgen Aloisius Morgenroth

Seit dem 1. Oktober 2025 ist Alina Hain neu in der Geschäftsführung des DFN-Vereins. Mit ihren Erfahrungen, einem frischen Blick und klaren Ideen möchte sie die Entwicklung des Vereins und der Geschäftsstelle aktiv mitgestalten. Im Interview spricht sie darüber, was sie antreibt, welche Themen ihr am Herzen liegen und wie sie jenseits des Schreibtischs auftankt.

Im Mai haben Sie Ihre Arbeit beim DFN-Verein aufgenommen, seit Oktober sind Sie offiziell neue Geschäftsführerin. Wie blicken Sie auf die ersten Monate zurück?

Der DFN-Verein zeichnet sich durch seine gute Unternehmenskultur aus. Schon in der Stellenausschreibung wurde viel Wert auf kollegiales und respektvolles Miteinander gelegt. Das zeigte sich auch im Vorstellungsgespräch und den weiteren Gesprächen mit dem Vorstand, der Geschäftsführung und den Bereichsleitungen. Wie gut die Arbeitsatmosphäre aber tatsächlich ist und wie sehr die positive Unternehmenskultur auch praktisch gelebt wird, durfte ich in den vergangenen Monaten selbst erleben. Ich habe mich von Anfang an willkommen gefühlt.

Um mein zukünftiges Arbeitsumfeld besser kennenzulernen, nehme ich bereits seit Mai an allen Gremiensitzungen des Vereins teil. Momentan führe ich Gespräche mit Mitarbeitenden der Geschäftsstelle. Selten habe ich in meiner Berufskarriere so viele Menschen getroffen, die sich seit Jahrzehnten beim gleichen Verein so aktiv einbringen oder beim selben Arbeitgeber tätig sind und ihr Engagement oder ihre Arbeit immer noch als Privileg empfinden. Das macht den DFN-Verein aus.

Was hat Sie an der Position angesprochen?

Als ich die Stellenausschreibung sah, habe ich zunächst gezögert, bevor ich mich beworben habe, da ich mir nicht sicher war, ob mein und das DFN-Profil optimal zueinander passen.

Wie eben schon gesagt, die wertebasierte Unternehmenskultur, der so viel Platz in der Stellenausschreibung eingeräumt wurde, hat mich letztendlich überzeugt, meine Bewerbung abzugeben. Denn wenn das Arbeitsumfeld und die Zusammenarbeit stimmen, dann macht die

Gut angekommen: Alina Hain spricht über Willkommenskultur, Erfahrungen und ihr ganz persönliches Motto

Arbeit nicht nur viel mehr Spaß, sondern führt auch zu besseren Ergebnissen. Die Frage, wie ich arbeiten möchte, spielt für mich mit der Zeit eine immer größere Rolle.

Ich greife die Frage auf. Wie möchten Sie denn arbeiten?
Auf jeden Fall werteorientiert – das bedeutet unter anderem, dass durch die vertrauensvolle Zusammenarbeit jede Person ihren Aufgabenbereich mitgestalten kann. Und ich möchte gestalten.

Ich freue mich sehr darauf, die Abläufe in der Geschäftsstelle weiter zu strukturieren, damit die Arbeit effektiver und einfacher sowohl für alle Mitarbeitenden als auch für die an den DFN-Diensten teilnehmenden Einrichtungen wird. Da ist auch schon vieles passiert in den vergangenen Jahren, an das ich gut anknüpfen kann.

> „Auch wenn ich selbst Juristin bin, mag ich Überregulierung überhaupt nicht."

Meine Maxime ist, dass Prozesse in der Handhabung so einfach wie möglich sein sollen. Auch wenn ich selbst Juristin bin, mag ich Überregulierung überhaupt nicht, die dadurch entsteht, dass auch die kleinsten Risiken möglichst rechtlich abgesichert werden sollen. Ich bin ein Mensch, der gut die Balance halten kann zwischen sinnvollen Lösungen und dem, was rechtlich unbedingt notwendig ist.

Beim DFN-Verein sehe ich mich als Vermittlerin zwischen den technischen und administrativen Zwängen. Das ist meiner Erfahrung nach eine Schnittstelle, die oft Reibung erzeugt und von beiden Seiten manchmal als einschränkend empfunden wird. Hier möglichst gute und pragmatische Lösungen zu finden, die keinen der Bereiche in ihrer eigentlichen Arbeit behindern, ist mein Ziel.

Sie haben eben gesagt, dass Sie sich als Vermittlerin sehen. Wie passen Sie von Ihrer Persönlichkeit her zu dieser Aufgabe?
Mir ist es wichtig, Argumente nachvollziehen zu können sowie Gründe und Bedürfnisse, die dahinterstehen, zu verstehen. Erst dann ist es möglich, sachlich gute Lösungen zu entwickeln. Früher habe ich dazu tendiert, meine eigene Position als Basis für Entscheidungen zu nehmen. Heute – sei es dem Alter oder der Berufserfahrung geschuldet – achte ich viel mehr darauf, was mein Gegenüber zu sagen hat. Gemeinsam getragene Entscheidungen sind in der Regel besser als die Entscheidung einer einzelnen Person, auch wenn diese Spezialistin oder Spezialist auf ihrem Gebiet sein mag. Dazu gibt es sogar wissenschaftliche Untersuchungen.

Seit seiner Gründung hat der DFN-Verein eine Doppelspitze in der Geschäftsführung. Was sind aus Ihrer Sicht die Vorteile?
Ich finde es extrem gut, dass Christian Grimm und ich zu zweit die Position gemeinsam übernehmen. Wir haben noch dazu das Glück, dass wir seinen technischen und meinen administrativen beruflichen Background einbringen und darum Dinge aus unterschiedlichen Perspektiven betrachten können. Ich bin der Überzeugung, dass wir dadurch die Vermittlungsposition zwischen der technischen und administrativen Welt gemeinsam exzellent ausgestalten können. Wenn zwei Menschen die Köpfe zusammenstecken, wird das Ergebnis immer besser sein, als wenn nur eine Person Entscheidungen trifft – gerade bei so verantwortungsvollen Tätigkeiten.

Was charakterisiert den DFN-Verein aus Ihrer Sicht?
Der Aufbau des Vereins und die Governance-Strukturen sind aus meiner Sicht etwas Besonderes. Da wurde bei der Gründung wirklich gute Arbeit geleistet. Die verschiedenen Gremien und Veranstaltungsformate, mit denen die große Wissenschaftscommunity so gut eingebunden ist, sorgen dafür, dass wir technisch am Puls der Zeit bleiben, die Entwicklungen kennen, die unsere Mitglieder antreiben, und ihre Wünsche verstehen – das ist einmalig.

Das mit der ganzen Welt verbundene leistungsstarke Wissenschaftsnetz mit seinen Diensten ist das Alleinstellungsmerkmal des DFN-Vereins. Diese besondere Infrastruktur halten wir nicht nur aufrecht, sondern verbessern sie stetig und passen sie an die relevanten Entwicklungen und Trends an. Denn unsere Aufgabe ist es, unseren Mitgliedern und teilnehmenden Einrichtungen das zu geben, was sie brauchen – und ihnen dabei vielleicht auch zwei Schritte voraus zu sein, damit sie sicher sein können, dass sie durch den Bezug der DFN-Dienste auch mit dem stetigen Wandel mithalten.

Hatten Sie vorher schon Berührungspunkte mit dem DFN-Verein?

Alle drei Einrichtungen, die ich in den letzten neun Jahren mitgeleitet habe, beziehen die DFN-Dienste. Daher kannte ich den DFN-Verein schon vorher als einen verlässlichen IT-Dienstleister. In einer dieser Einrichtungen hatten wir seinerzeit einen Notfall: Bei einem Brand im Serverraum wurden alle Strom- und Datenleitungen zerstört. Die gesamte IT-Infrastruktur fiel aus. Durch die schnelle und professionelle Unterstützung des DFN-Vereins konnten wir in kürzester Zeit wieder an das Wissenschaftsnetz angeschlossen werden und den Anschluss zusätzlich zuverlässiger – weil georedundant – aufbauen. Aufgrund dessen habe ich in der letzten Einrichtung angeregt, dem DFN-Verein beizutreten. So mussten wir diverse IT-Dienstleistungen, die zum Beispiel durch DFN-Fernsprechen oder DFN-Cloud angeboten werden, nicht mühsam auf dem freien Markt selbst beschaffen. Diese guten Erfahrungen haben mich zusätzlich motiviert, mich beim DFN-Verein zu bewerben.

Haben Sie ein persönliches Motto, das Sie durchs Leben trägt?

Mein Motto ist die Kunst des steten Wandels – sowohl privat als auch beruflich. Große disruptive Veränderungen insbesondere im Berufsleben sind meiner Erfahrung nach selten von Erfolg gekrönt. Sich konsequent immer wieder neu zu orientieren und so den Wandel Schritt für Schritt zu meistern, ohne dabei das Ziel aus den Augen zu verlieren – das ist eine echte Kunst, denn sie erfordert Geduld und Beharrlichkeit. Veränderungen mit der Brechstange durchzusetzen, bringt dagegen viel Unruhe und Missmut.

Was hilft Ihnen, nach einem langen Arbeitstag den Kopf freizubekommen?

Ich mache Sport, tanze gerne und lese viel. Aber am liebsten bin ich in der Natur. Wenn ich im Wald bin, fühle ich mich frei und bin ganz bei mir. Das macht mich einfach glücklich.

Das Gespräch führte Maimona Id (DFN-Verein) ◆

Alina Hain | Studium Rechtswissenschaften Europa-Universität Viadrina, Adam-Mickiewicz-Universität Poznań | 1998–2000 Juristin Rechtsanwaltskanzlei Wittemöller Radack & Partner | 2000–2002 Rechtsreferendariat des Landes Brandenburg (Volljuristin) | 2002–2006 Projektleiterin Industrie- und Handelskammer Ostbrandenburg | 2006–2011 Leiterin Gründungsförderung Freie Universität Berlin | 2010–2011 Betriebswirtschaftslehre und Betriebliches Management (MBA) FernUniversität in Hagen | 2011–2016 Referentin Ministerium für Wirtschaft und Europaangelegenheiten des Landes Brandenburg | 2016–2018 Verwaltungsleiterin Leibniz-Institut für Gewässerökologie und Binnenfischerei (IGB) | 2018–2022 Verwaltungsleiterin und Vorstandsmitglied Leibniz-Institut für Gemüse- und Zierpflanzenbau (IGZ) | 2022–2025 Geschäftsführerin (COO) Nationale Organisation Wasserstoff- und Brennstoffzellentechnologie (NOW) GmbH | seit Oktober 2025 Geschäftsführerin im DFN-Verein

Erfolgreiche 18. Tagung der DFN-Nutzergruppe Hochschulverwaltung

Volles Haus, lebhafte Diskussionen und jede Menge Input: Bei der 18. Tagung der DFN-Nutzergruppe Hochschulverwaltung kamen rund 200 Expertinnen und Experten zusammen. Mit hochaktuellen Themen, praxisnahen Einblicken und viel Raum für Austausch traf das Programm genau den Nerv der Hochschulcommunity.

Text: **Inga Scheler** (Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau, RPTU)

Herzliche Begrüßung: Dr. Rainer Bockholt, der Direktor des Hochschulrechenzentrums der Rheinischen Friedrich-Wilhelms-Universität Bonn und ehemalige stellvertretende Vorstandsvorsitzende im DFN-Verein, heißt die Teilnehmenden willkommen und berichtet über Aktuelles aus dem DFN-Verein | *Fotos: Heike Ausserfeld/DFN*

Der Moment, wenn sich nach zwei Jahren Vorbereitung die Türen zum Tagungsraum öffnen, bleibt besonders: Noch ist es still, alles ist vorbereitet – von den Sponsorenplätzen bis zu den Stuhlreihen im Publikum. Jetzt zeigt sich, ob die Planung Früchte trägt. Nach mittlerweile 18 ausgerichteten Tagungen in den vergangenen fast 35 Jahren verfügt das Organisationsteam der DFN-Nutzergruppe Hochschulverwaltung – kurz NuGru – über jede Menge Erfahrung.

Einen besonders schönen Veranstaltungsort im Herzen Bonns stellte die diesjährige Gastgeberin, die Rheinische Friedrich-Wilhelms-Universität Bonn, zur Verfügung. Die 18. Tagung der DFN-Nutzergruppe Hochschulverwaltung fand vom 5. bis 7. Mai 2025 in der Aula des ehemaligen kurfürstlichen Schlosses statt, das seit Gründung der Universität im Jahr 1818 das Universitätshauptgebäude beherbergt und mit dem herrlichen barocken Arkadenhof eine festliche Kulisse für die Veranstaltung bot. Leider war es eine der letzten großen Veranstaltungen, da das Schloss für mehrere Jahre wegen Renovierung geschlossen werden muss.

Nachdem Dr. Inga Scheler, Leiterin der DFN-Nutzergruppe und stellvertretende Leiterin des Regionalen Hochschulrechenzentrums der RPTU Kaiserslautern-Landau die rund 200 Teilnehmenden begrüßt hatte, stimmte Holger Gottschalk – der Kanzler der Universität Bonn – in seinem Grußwort auf das diesjährige Tagungsmotto „(R)evolution der Hochschulverwaltung – KI und Souveränität“ ein. Er betonte, dass Digitalisierung ein wichtiges strategisches Fundament sei und bei Weitem keine Randnotiz.

Im Mittelpunkt des hochkarätigen Programms stand die Frage, wie Künstliche Intelligenz (KI) Verwaltungsprozesse verändert – und welche Anforderungen dabei an Verantwortung, Ethik und digitale Souveränität gestellt werden. Weitere Schwerpunkte der insgesamt acht Themenblöcke waren außerdem Informationssicherheit und Recht. Wie üblich war der Vortrag „Neues aus dem DFN" Teil der Einführung in die Tagung – gehalten von Dr. Rainer Bockholt, Direktor des Hochschulrechenzentrums der Uni Bonn und ehemaliger stellvertretender Vorstandsvorsitzender des DFN-Vereins. Informationen zu DFN-Cloud und DFN-Security steuerten Dr. Dirk Bei der Kellen und Dr. Ralf Gröper vom DFN-Verein bei.

Zum Auftakt forderte Andrea Gerlach-Newman, Kanzlerin der Technischen Hochschule Nürnberg Georg Simon Ohm, eine grundlegende Veränderung von Führungsrollen. Diese sollten künftig mehr Verantwortlichkeit statt Zuständigkeit im Fokus haben. „Wie schaffen wir eine Kultur, die Lust auf das Ausprobieren macht?", fragte die Bundessprecherin der Hochschulkanzlerinnen und -kanzler.

Prof. Ulrike Tippe, Rektorin der Technischen Hochschule Wildau, referierte in ihrer Rolle als Vizepräsidentin für Digitalisierung und wissenschaftliche Weiterbildung der Hochschulrektorenkonferenz (HRK) über KI, digitale Souveränität und Informationssicherheit aus der Perspektive der HRK. Die Forderung nach größeren, länderübergreifenden Verbünden zur Lösung der komplexen Herausforderungen fand im Auditorium großen Anklang.

Rund um das Thema KI in der Hochschulverwaltung gab es eine Reihe interessanter Beiträge, die verschiedene Nutzungsszenarien – teilweise bereits in der Erprobung – vorstellten. Hierbei war das übereinstimmende Credo: Nutzen mit Augenmaß. Sowohl Prof. Dr. Julian Kunkel von der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) als auch Dr. Harald Gilch vom HIS-Institut für Hochschulentwicklung e. V. waren sich einig: KI macht Fehler, das müsse man akzeptieren.

Am zweiten Tag der Veranstaltung stellte Dr. Holger Impekoven, stellvertretender Kanzler der Universität Bonn, vor, wie Transformationsprozesse in der Verwaltung mithilfe von KI angestoßen werden. Unter dem Motto „Entlastung statt Entlassung" erproben dort Mitarbeitende den möglichen Einsatz von KI in der Verwaltung. In „Communitys of practice" werden nicht nur Erfahrungen ausgetauscht, sondern auch Ideen und Strategien zum geordneten Einsatz von KI in administrativen Prozessen entwickelt.

In Block 6 informierte Dr. Lea Beiermann vom Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) über die Fortschritte ihrer Organisation bei der Entwicklung von Open-Source-Lösungen, die ähnlich den Lösungen großer Anbieter integriert eingesetzt werden können. Das Ziel sei, digitale Souveränität im öffentlichen Bereich zu fördern. An einem Vertragsmodell für Hochschulen wurde zum Zeitpunkt des Vortrags gearbeitet.

> Anruf aus dem Jenseits. Warum sich Archive in Digitalisierungsprojekten zu Wort melden.

Ein Highlight war außerdem der Vortrag von Dr. Klaus Nippert, Archivar am Karlsruher Institut für Technologie (KIT). Unter dem Titel „Anruf aus dem Jenseits. Warum sich Archive in Digitalisierungsprojekten zu Wort melden." argumentierte er sehr einleuchtend, warum Archivare raus aus ihren Kellern, Papieren und Pergamenten kommen sollten.

Auch das Rahmenprogramm trug zum Gelingen der Tagung bei. Es führte die Gäste durch den Botanischen Garten sowie das HPC-Cluster „Marvin" und bot zugleich die Gelegenheit, die Beethovenstadt Bonn aus der Vogelperspektive zu erleben – und darüber hinaus ausreichend Zeit zum Austauschen und Netzwerken.

Nach insgesamt drei Tagen, etlichen inspirierenden Vorträgen und Diskussionen sowie dem wertvollen Input der vielen unterschiedlichen Expertinnen und Experten ging die 18. Tagung der DFN-Nutzergruppe Hochschulverwaltung erfolgreich zu Ende. Zahlreiche positive Rückmeldungen bescheinigten dem NuGru-Organisationsteam ein „Weiter so". Die Planungen für die 19. Tagung der DFN-Nutzergruppe sind bereits angelaufen.

Das Schlusswort – traditionsgemäß vom ältesten anwesenden Mitglied der NuGru - hielt Herbert Röbke, ehemals IUK-Koordinator für die Universitätsverwaltungen des Landes Baden-Württemberg. Mit vielen neuen Ideen und Kontakten im Gepäck hieß es für die Teilnehmenden Abschied nehmen – bis zum Wiedersehen bei der 19. Tagung im Mai 2027.

Die DFN-Nutzergruppe dankt allen Vortragenden, Teilnehmenden, Sponsoren und insbesondere den vielen Helferinnen und Helfern, die die Tagung erst möglich gemacht haben. ◆

Seit ihrer Gründung 1991 in Berlin veranstaltet die DFN-Nutzergruppe Hochschulverwaltung alle zwei Jahre eine Tagung. Diese greift aktuelle Themen aus den Bereichen Informations-, Kommunikations- und Medientechnik auf und setzt sie in direkten Bezug zu Themen aus der Hochschulverwaltung. Die 19. Tagung der DFN-Nutzergruppe „Hochschulverwaltung" findet vom 10. bis 12. Mai 2027 in Mannheim statt.

Alle Vorträge der 18. Tagung der DFN-Nutzergruppe Hochschulverwaltung finden Sie unter: **https://www.hochschulverwaltung.de/event/tagung-2025-bonn/**

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 langjähriger Dienstverantwortlicher für DFN-Mail-Support sorgt Michael Röder dafür, dass Viren, Würmer und Trojaner keine Chance haben. Mit dem Thema E-Mail-Abuse-Management im Gepäck besuchte er …

… die TNC25, die vom 9. bis 13. Juni 2025 in Brighton stattfand, um das Thema auf europäischer Ebene voranzutreiben.

An der TNC25, dem jährlich stattfindenden Flaggschiff unter den Events der nationalen Forschungsnetze (NRENs), nahmen dieses Jahr mehr als 900 Personen aus 72 Nationen teil – um unter dem gemeinsamen Motto „Brighter Together" Ideen und Projekte vorzustellen, mit der Community zu diskutieren, Vorträge zu besuchen und nach Herzenslust zu netzwerken.

Die verschiedenen Sessions fanden unter anderem im Brighton Dome statt – einer hochmodernen Event-Location im Herzen der südenglischen Küstenstadt und in direkter Nachbarschaft des Royal Pavillons. Der lokale Ausrichter, das britische NREN JISC, war begeistert, nun endlich sein Versprechen aus 2020 einlösen zu können. Denn eigentlich wollte sich die NREN-Community bereits vor fünf Jahren in Brighton treffen. Wir erinnern uns: Wegen Corona war zu dieser Zeit an internationale Großveranstaltungen mit mehreren hundert Teilnehmenden vor Ort nicht zu denken.

Umso ausgelassener war in diesem Jahr die Stimmung beim gemeinsamen Conference Dinner auf dem Brighton Palace Pier. Der war nämlich exklusiv nur für TNC-Teilnehmende geöffnet. Bunte Lichter, laute Musik und ratternde Fahrgeschäfte: Nach dem Motto „einmal wieder Kind sein" stürzten wir uns mit Begeisterung auf Achterbahn, Autoscooter, Geisterbahn und Co. Natürlich gehörten auch Fish & Chips dazu. Das klingt übrigens leichter, als es tatsächlich war: Die englischen Möwen sind nicht nur besonders groß und hungrig, sie sind offenbar auch sehr risikofreudig und flugbegabt. Wer da nicht aufpasst, wird unfreiwillig zum Futterspender!

Ich selbst durfte in meiner Rolle als Dienstverantwortlicher für DFN-MailSupport im Rahmen des Community Hub „Cybershield" den Austausch zum Thema E-Mail-Abuse-Management initiieren. Während der DFN-Verein mit DFN-MailSupport seit vielen Jahren einen sehr konkret ausgestalteten Dienst für seine Teilnehmereinrichtungen betreibt und stetig weiterentwickelt, werden zentrale E-Mail-Filterdienstleistungen in anderen NRENs teils auf gänzlich andere Art und Weise erbracht. Neben einigen wenigen Ansätzen, die durchaus mit DFN-MailSupport vergleichbar sind, bieten andere NRENs wie beispielsweise HEAnet (Irland) ihrem

Wirkungskreis lediglich den Zugang zu zentral beschafften RBL'en (Real-Time-Block-Listen) an. Andere reichen den Zugriff auf kommerzielle Dienstleistungen unter dem NREN-Label weiter an ihre Teilnehmereinrichtungen. Für diese unterschiedlichen Herangehensweisen gibt es gute Gründe, die in der grundsätzlichen Ausrichtung des NRENs, dessen Finanzierung und Governance, aber auch an der Zusammensetzung der betroffenen Nutzer-Community liegen können.

Angesichts ständig wachsender Angriffsvektoren rund um das allgegenwärtige Kommunikationsmedium E-Mail stellen sich alle NRENs zu Recht die Frage: Wie können wir den Posteingang unserer Nutzerinnen und Nutzer noch sicherer machen? Schon während und auch nach der Session wurde intensiv diskutiert, insbesondere mit den Kolleginnen und Kollegen der NRENs CESNET, RedIRIS, RENATER, SWITCH und SURF. Erste vorsichtige Gedankenspiele schauen auf die großen Erfolge des OCRE-Projekts und denken über zentral koordinierte, paneuropäische Beschaffungsprozesse gemeinsam genutzter Dienstbestandteile nach. Interessiert? Stay tuned!

Mein persönliches Highlight waren die Lightning Talks, die sich größter Beliebtheit erfreuen und mittlerweile zum festen Repertoire der TNC gehören! Hier stellen sich Vortragende aus den unterschiedlichsten Disziplinen der Herausforderung, ihr Thema innerhalb von fünf Minuten auf der großen Bühne vorzustellen. Hier ist von der AI-gestützten Bewertung der Stunts während eines Seilsprungwettbewerbs bis zur Vorstellung eines solar-betriebenen eduroam-Nodes in der afrikanischen Steppe alles dabei – Schleudertrauma im Hippocampus inklusive!

Als während der Abschlussveranstaltung Lise Fuhr (GÉANT CEO) leidenschaftlich über das vertrauensvolle Miteinander in der NREN-Community, deren kollektives Engagement und Anteil an der digitalen Transformation und Souveränität des Forschungsstandortes Europa spricht, sind hinter den Kulissen die Weichen für die TNC 2026 in Helsinki längst gestellt. Das weckt die Vorfreude auf das kommende Jahr. Als besonderer Ausdruck des außergewöhnlichen Veranstaltungsortes wird mir aber noch lange das riesige goldene Pferd in Erinnerung bleiben, das über dem Publikum an der Decke schwebte. In diesem Sinne, wir sehen uns in Helsinki! ◆

Ein Hoch auf die Community: Unter dem Motto „Brighter Together" kamen Fachleute aus der ganzen Welt zur TNC25 in Brighton zusammen, um Ideen und Erfahrungen zu teilen –, aber auch, um Kontakte zu pflegen und gemeinsam inspirierende Momente zu erleben | *Fotos: 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.

90. DFN-Mitgliederversammlung

Was könnte besser zum Auftakt einer Mitgliederversammlung passen – deren Verein Visionen für die Digitalisierung von Forschung und Lehre in tragfähige Infrastrukturen übersetzt – als der Empfang im „Haus der Zukünfte“? Am Montag, 2. Juni 2025, dem Vorabend der 90. Mitgliederversammlung des DFN-Vereins, trafen sich Delegierte der Mitgliedseinrichtungen im Ausstellungsforum Futurium in Berlin.

Nach der Begrüßung durch den Vorstandsvorsitzenden Prof. Dr.-Ing. Stefan Wesner hieß Dr. Gabriele Zipf, Kuratorin des Futuriums, die Gäste willkommen und gab eine Einführung in die nachfolgende Ausstellung. Mit ihren Zukunftsszenarien lieferte die Schau neue Perspektiven, Ideen und Denkanstöße, die sich im Kern um die Frage drehen: „Wie wollen wir leben?“

Am Dienstagmorgen eröffnete der Vorsitzende der 89. Mitgliederversammlung, Dr. Rainer Bockholt, die 90. Mitgliederversammlung in der Berlin-Brandenburgischen Akademie der Wissenschaften. Diese stand auch im Zeichen des Abschieds: Mit einem Moment des Gedenkens ehrten die Anwesenden Prof. Dr. Gerhard Peter, der im Mai 2025 verstarb. 20 Jahre leitete der ehemalige Rektor der Hochschule Heilbronn die Mitgliederversammlungen des DFN-Vereins und prägte so dessen Entwicklung

Gebündelte Kompetenz und Erfahrung: In der Berlin-Brandenburgischen Akademie der Wissenschaften kommen Delegierte der Mitgliedseinrichtungen zusammen, um gemeinsam das Deutsche Forschungsnetz zu gestalten | *Foto: Jürgen Aloisius Morgenroth*

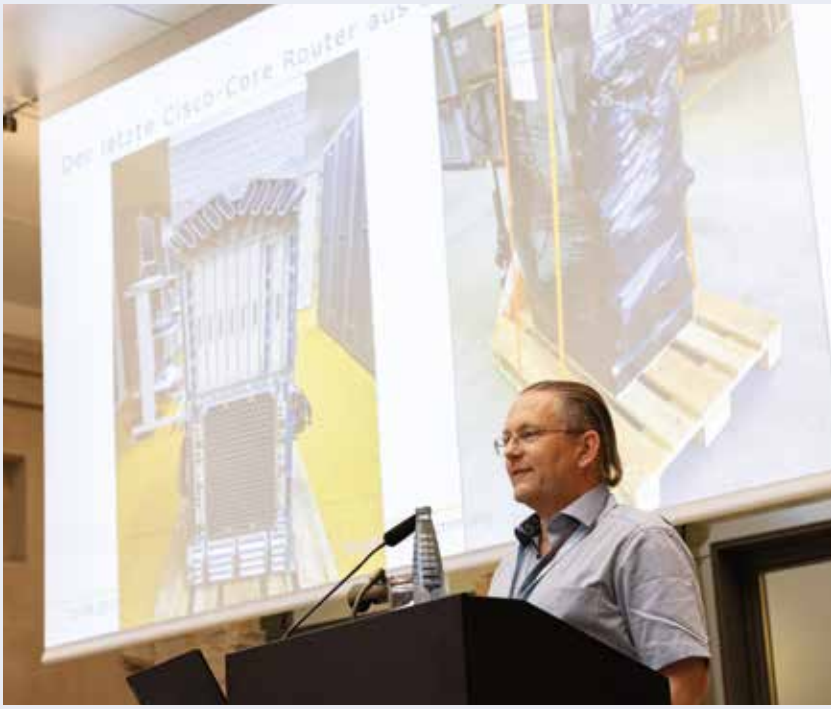
entscheidend mit. Mit hohem Engagement und einer klaren und stets verbindlichen Linie schaffte er es, die Anliegen der Mitgliedseinrichtungen mit den gemeinschaftlichen Interessen im Verein zu verbinden.

Nach dem gemeinsamen Gedenken wandte sich die Versammlung den gegenwärtigen Entwicklungen im Wissenschaftsnetz zu. Auf der Tagesordnung standen neben dem Jahresbericht zu den Aktivitäten des DFN-Vereins 2024 unter anderem die Themen DFN-PKI, der WLAN-Zugangsdienst eduroam sowie das Vorhaben EuroHPC Hyperconnectivity.

In ihrer Vorstellung gab die designierte Geschäftsführerin Alina Hain den Anwesenden einen ersten Einblick in ihren beruflichen Hintergrund. Als Volljuristin mit langjähriger kaufmännisch-administrativer Führungserfahrung erläuterte sie zunächst, wie sehr sie sich auf die Tätigkeit für den DFN-Verein freue – mit seiner wertebasierten Kultur, der komplexen Governance-Struktur und den in der Organisation tätigen Menschen, die sich hochmotiviert für die Weiterentwicklung des Wissenschaftsnetzes und der DFN-Dienste einsetzen. Besonders freute sie sich über die künftig enge Zusammenarbeit mit den Gremien des DFN-Vereins und darauf, gemeinsam mit Dr. Christian Grimm die Geschäftsstelle weiterhin erfolgreich zu führen.

Wir sagen Dankeschön

Nach Vorträgen zu technischen Entwicklungen und strategischen Themen richtete sich der Blick der Mitgliederversammlung zum Schluss auf eine ganz persönliche Wegmarke. Nach rund 30 Jahren außergewöhnlichen Engagements für Forschung und Lehre, davon über 20 Jahre in der Geschäftsführung des DFN-Vereins, wurde Jochem Pattloch mit anhaltendem Applaus verabschiedet. Er dankte den Mitgliedsvertreterinnen und -vertretern sowie dem Vorstand und besonders auch seinem Kollegen Dr. Christian Grimm, der ihn in der Geschäftsführung über lange Jahre begleitet hat, für die vertrauensvolle Zusammenarbeit. Angesichts der positiven Entwicklung der Organisation, der konstruktiven Zusammenarbeit in den Gremien und des gelungenen Übergangs in der Geschäftsführung gehe er mit zwei lachenden Augen und wünsche dem DFN-Verein weiterhin alles erdenklich Gute. ◆



Platz für modernste Infrastruktur: Der stellvertretende Vorstandsvorsitzende Prof. Dr. Helmut Reiser berichtet über den Abbau der alten Cisco-Router im X-WiN | *Foto: Jürgen AloiIsius Morgenroth*

TERMIN

Die 91. Mitgliederversammlung findet am **Mittwoch, 3. Dezember 2025**, in Bonn statt.

Im Mittelpunkt steht der Austausch: Bei der 83. DFN-Betriebstagung diskutieren etwa 320 Teilnehmende Neuigkeiten rund um das Wissenschaftsnetz und seine Dienste | *Foto: Iven Jurk/DFN*

83. DFN-Betriebstagung

Im Zentrum der 83. DFN-Betriebstagung, die am 7. und 8. Oktober 2025 im Leonardo Royal Hotel Berlin Alexanderplatz stattfand, stand erneut der Erfahrungsaustausch rund um aktuelle Herausforderungen und Entwicklungen in den Bereichen Kommunikationsinfrastrukturen, IT-Sicherheit oder kollaborative Dienste. Rund 320 Teilnehmende nutzten die Gelegenheit, sich in neun Fachforen zu informieren, gemeinsam zu diskutieren und zu netzwerken. Zudem verfolgten knapp 140 Interessierte die Plenumssitzung per Livestream.

Am ersten Tag gab es im Plenum wie gewohnt Updates zu den Diensten des DFN-Vereins: Security, Trust & Identity Services, Collaboration Services und Network and Communication Services. Es wurde außerdem auf die GÉANT Cybersecurity Campaign 2025 hingewiesen. Im Fokus steht dieses Mal Cyber-Mindfulness: digitale Achtsamkeit als wirksame Methode gegen KI-gestützte Bedrohungen. Gut besucht waren die Foren Sicherheit, Clouddienste, AAI und Mail, die viele spannende Themen boten. Vielfältig ging es auch am zweiten Tag in den Foren Wissenschaftsnetz, Multimedia, Mobile IT, VoIP und Rechtsfragen weiter. ◆

TERMIN

Die 84. DFN-Betriebstagung findet am **17. und 18. März 2026,** statt.

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

DFN-Diskussionsforum der Kanzlerinnen und Kanzler 2026

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

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

TERMIN

Das DFN-Diskussionsforum der Kanzlerinnen und Kanzler der Hochschulen im DFN-Verein findet am **Montag und Dienstag, 27. und 28. April 2026,** in Berlin statt.

Überblick DFN-Verein

(Stand: 12/2025)

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 14. Wahlperiode sind Mitglieder des Verwaltungsrates:

Kerstin Bein
(Universität Mannheim)

PD Dr. Wolfgang zu Castell
(GFZ Helmholtz-Zentrum für Geoforschung)

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 Geschäftsführung wurden vom Vorstand Dr. Christian Grimm und Alina Hain bestellt.

Die Mitgliedseinrichtungen

Aachen	Fachhochschule Aachen - Technik und Wirtschaft
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Albstadt	Hochschule Albstadt-Sigmaringen
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
	Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit
	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
Diepolz	Private Hochschule für Wirtschaft und Technik gGmbH
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	Agentur für Innovation in der Cybersicherheit GmbH
	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
	Zentrum für Kunst und Medien Karlsruhe
Kassel	Universität Kassel
Kehl	Hochschule für öffentliche Verwaltung Kehl
Kempten	Hochschule für angewandte Wissenschaften, Fachhochschule Kempten
Kiel	Christian-Albrechts-Universität zu Kiel
	Hochschule für Angewandte Wissenschaften Kiel (HAW 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
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	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
	Universität Magdeburg
Mainz	Hochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Katholische Hochschule Mainz
Mannheim	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
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
Neuruppin	Medizinische Hochschule Brandenburg Campus gGmbH
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
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
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/