DFN mitteilungen

Konnektivität weltweit

Start der GN-5-Projekte

Sicher FAIR

IAM4NFDI in der DFN-AAI

Lebenslang gültig

Das Konzept edu-ID

9 770177 689001

Impressum

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

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

ISSN 0177-6894

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

Fotonachweis
Titel: gugacurado/Adobe Stock
Rückseite: strirene/Adobe Stock

Foto: GÉANT Association

Cathrin Stöver
Chief Communication Officer (CCO),
GÉANT Association
Als Expertin der GWK Mitglied
im Wissenschaftlichen Senat
des NFDI-Vereins (Nationale
Forschungsdateninfrastruktur e. V.)

In den vergangenen Jahrzehnten haben Forschung, Innovation und immer schneller werdender Fortschritt speziell in der Informations- und Kommunikationstechnologie unsere Welt für immer verändert. Wir leben in einer spannenden Gegenwart, in der Quantenkommunikation und künstliche Intelligenz Teil unserer täglichen Realität sind.

Als R&D-Gemeinschaft haben wir in der jüngeren Vergangenheit zahlreiche Herausforderungen gemeinsam gemeistert, sind gewachsen, näher zusammengerückt und wortwörtlich enger verbunden. Globale Konnektivität prägt die Art und Weise, wie wir zusammenleben und zusammenarbeiten, und erleichtert die Vernetzung und den Ideenaustausch Forschender. Nie zuvor hatten wir so viele Möglichkeiten für Chancengleichheit, Partizipation und freien Zugang zu Wissen.

Die European Open Science Cloud (EOSC) und die Nationale Forschungsdateninfrastruktur (NFDI) in Deutschland leisten einen wesentlichen Beitrag, indem sie das Management von FAIR-Forschungsdaten und -diensten vorantreiben.

In diesem sich dynamisch entwickelnden multidisziplinären Wissenschaftsumfeld wachsen auch die Anforderungen an einen gemeinsamen, sicheren Datenraum und eine leistungsfähige digitale Infrastruktur mit vertrauenswürdigen Diensten.

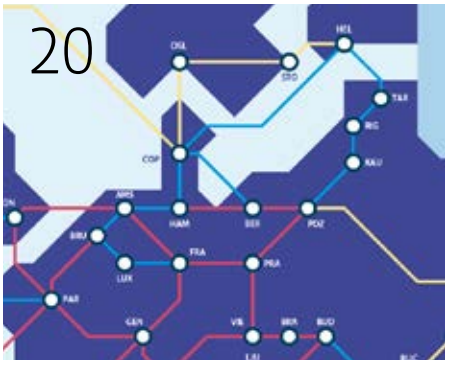
Unter dem Dach der GÉANT Association (NL) bilden das europäische Verbindungsnetz GÉANT und die nationalen Forschungsnetze wie der DFN-Verein das Fundament dieser Infrastruktur, die heute mehr als 50 Millionen Forschende und Studierende in Europa verbindet.

Seit mehr als 20 Jahren sind die GN-Projekte ein wesentlicher Treiber dieses digitalen Fortschritts. Von Beginn an konnten sich die Forschungsnetze auf die stete und großzügige Unterstützung und das Commitment der Europäischen Union verlassen. Mit dem Start des vom Rahmenprogramm Horizon Europe geförderten Projekts GN5 beginnen wir ein neues und spannendes Kapitel für diese erfolgreiche europäische Zusammenarbeit.

Auf ein weiterhin gutes und fruchtbares Miteinander!
Ihre Cathrin Stöver

Inhalt

Wolkenreise – DFN-Cloud als Gesamtpaket
Maßgeschneidert für die Wissenschaft



Fit für die Zukunft – Start der GN5-Projekte
Das beste Netz für Forschung und Lehre

Europa wächst zusammen
Einblicke in ein Erfolgsprojekt geben Leonie Schäfer und Jakob Tendel

Wissenschaftsnetz

International

Sicherheit

Sicherheit³ – drei Jahrzehnte DFN-CERT
Mit den Aufgaben gewachsen

Recht

DFN-Verein

Autorinnen und Autoren dieser Ausgabe im Überblick

1 Thiemo Nordenholz, DFN-CERT (nordenholz@dfn-cert.de); **2** Jochen Schönfelder, DFN-CERT (schoenfelder@dfn-cert.de); **3** Robert Stoy, DFN-Verein (stoy@dfn.de); **4** Dr. Dirk Bei der Kellen, DFN-Verein (beiderkellen@dfn.de); **5** Leif Pullich, Technische Universität Darmstadt (leif.pullich@tu-darmstadt.de); **6** Thomas Haake, Technische Universität Darmstadt (thomas.haake@tu-darmstadt.de); **7** Dr. Christian Grimm, DFN-Verein (grimm@dfn.de); **8** Maimona Id, DFN-Verein (id@dfn.de); **9** Caroline Tuhwezeine Kumwesiga, RENU (ctuhwezeine@renu.ac.ug); **10** Prof. Dr. Klaus-Peter Kossakowski, DFN-CERT (kossakowski@dfn-cert.de); **11** Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **12** Nicolas John, Forschungsstelle Recht im DFN (njohn@uni-muenster.de); **13** Johannes Müller, Forschungsstelle Recht im DFN (johannes.mueller@uni-muenster.de)

Von D(ä)monen und Graphen – das neue Dienstemonitoring im DFN

Im Idealzustand ist das Netz für den Endanwender unsichtbar. Damit diese Illusion möglich wird, müssen Netzbetreiber ganz genau hinschauen, um Fehler und Abweichungen vom Normalzustand schnell zu erkennen. Das gilt auch für das Wissenschaftsnetz X-WiN und die darüber erbrachten Dienste des DFN. Mit dem Monitoring-Tool DMon soll diese Illusion jetzt noch besser gelingen.

Text: **Thiemo Nordenholz, Jochen Schönfelder** (DFN-CERT), **Robert Stoy** (DFN-Verein)

Foto: anita2020 /iStock

Der Teufel steckt im Detail

Eine präzise und aktuelle Sicht auf den Status aller Netzkomponenten, Datenleitungen und Systeme wird durch die Nutzung sogenannter Monitoring-Software ermöglicht. Beim DFN gibt es sehr spezifische Anforderungen an ein solches System und dessen Umsetzung.

Wissenschaftler haben bei ihren oft rechenintensiven Forschungsarbeiten besondere Ansprüche, unter anderem an die Verfügbarkeit der von ihnen genutzten Dienste. Mit einer Verfügbarkeit, die nicht weit von den berühmten fünf Neunen (99,999 %) entfernt ist, erfüllt das X-WiN diese hohen Ansprüche. Um das zu gewährleisten, wird großer Wert auf die stete Sichtbarkeit des aktuellen Betriebszustands gelegt. So wird die Infrastruktur überwacht, um kritische Systemlasten und Zustände lange vor einem potenziellen Ausfall festzustellen und frühzeitig Gegenmaßnahmen einzuleiten. Das

> Das neue Monitoring wird ein integriertes System für die verschiedenen Dienstangebote des DFN bereitstellen.

DFN Network Operation Center (NOC) nutzte hierfür bisher bewährte Monitoring-Software wie mrtg (Multi Router Traffic Grapher) oder Cacti. Diese Software kann jedoch nicht mehr alle Anforderungen an einen flexiblen und möglichst automatisierten Betrieb erfüllen. Außerdem sollte die bisher stark auf einzelne Komponenten oder Leitungen zentrierte Sicht einem breiteren, dienstbasierten Ansatz weichen. Durch die Einbeziehung aller für die Diensterbringung notwendigen Systeme sollte ein vollständiger und stets aktueller Betriebsstatus sowohl für den DFN als Netzbetreiber als auch für die Dienstnutzer abrufbar sein. Das neue Monitoring wird demnach nicht nur das X-WiN überwachen, sondern ein integriertes System für die verschiedenen Dienstangebote des DFN bereitstellen. Dafür braucht es eine Software, die auf der einen Seite eher techniknah die Infrastruktur überwachen kann, auf der anderen Seite aber auch die Möglichkeit bietet, die vielen eher abstrakten Dienste abzubilden, die auf dieser Infrastruktur aufsetzen.

Am Anfang war die Idee

Die erste große Herausforderung bei der Realisierung einer solchen Lösung war der Umgang mit den unterschiedlichen Abstraktionsgraden der darzustellenden Daten. Diese reichen von einem sehr konkreten einzelnen Messwert, zum Beispiel dem Temperaturwert einer CPU, bis zur Darstellung der Verfügbarkeit eines Dienstes, die von der Funktion einer Vielzahl von einzelnen Systemen abhängt. Eine weitere Herausforderung bestand darin, die bereits etablierten Komponenten und Prozesse zu integrieren bzw. zu berücksichtigen. Neben einem bestehenden internen Informationssystem, diversen Messplattformen und Fachportalen gehören dazu auch die vorhandenen Prozesse, auf denen das Tool aufsetzen soll.

Das Tool muss einen komplexen Prozess – von der Erlangung der Messwerte und Umwandlung in Metriken über die Anbindung an bestehende Geschäftsprozesse bis hin zur Darstellung und Auswertung – abdecken. Die auf dem Markt verfügbaren Tools, die im Ansatz einen solchen Prozess unterstützen, hätten mit einem sehr hohen Aufwand angepasst werden müssen.

Es musste daher selbst eine Architektur entwickelt werden, die sowohl direkt erlangte Daten verarbeiten kann, als auch vorsieht, auf bestehende Komponenten aufzusetzen. So sollten die bestehenden Messplattformen weiterverwendet werden, aber es sollte trotzdem ermöglicht werden, neue Datenquellen aufzunehmen.

Das bestehende, DFN-interne Informationssystem bietet eine verlässliche Basis für Infrastrukturinformationen. Hier werden sehr detailliert und umfangreich Fakten über administrative Gebilde wie Dienste und Zuständigkeiten bis hin zu technischen Details wie einzelnen Steckverbindungen dokumentiert. Diese Quelle wird als „Single Source of Truth“ für die zugrunde liegenden Dienstkonstrukte und Infrastrukturen genutzt, um redundante Konfigurationseingaben und damit unnötige Fehlerquellen zu vermeiden.

> „Ein wichtiges Ziel des DFN-NOC war die Entwicklung einer neuen, zukunftsfähigen Basis für das X-WiN-Echtzeitmonitoring, welche insbesondere Möglichkeiten zur weiteren Automatisierung des Monitorings eröffnet und Mittel für maßgeschneiderte Darstellungen und Analysen von komplexen Zustands- und Störungssituationen bereitstellen sollte. Nicht zuletzt soll auch die Echtzeitfähigkeit auf eine noch fein-granularere Basis gehoben werden.“
> *Robert Stoy, DFN-Verein*

Die eigentlichen Monitoring-Daten, die zur Statusbestimmung dienen, werden nicht direkt von den Quellsystemen in das Monitoring gespeist, sondern im Regelfall über sogenannte Kollektoren aggregiert und normalisiert. Hierfür werden verschiedene Standardprotokolle wie SNMP (Simple Network Management Protocol) und NetFlow unterstützt, um eine hohe Bandbreite an Quellsystemen zu ermöglichen. Die Vielfalt an Komponenten, die hier berücksichtigt werden muss, ist sehr groß und wächst bzw. ändert sich stetig. Neben den Routern und Netzwerkswitchen gehören die DWDM-Systeme der Optikplattform ebenso dazu wie USV-Anlagen oder Out-of-Band-Komponenten.

Vom Plan zum Tool

Doch jeder Plan ist nur so gut wie seine Umsetzung. Für das Entwicklungsprojekt mit dem richtungsweisenden Namen DMon (Dienste-Monitoring) wurde mit dem DFN-CERT ein Partner gefunden, der sowohl die Erfahrungen als auch das Know-how hat, um ein solches Projekt erfolgreich umzusetzen.

Im direkten Dialog zwischen dem Entwicklungsteam des DFN-CERT und den Kollegen des DFN-NOC wurde beschlossen, im ersten Schritt das Monitoring des Kernnetzes umzusetzen, um möglichst schnell die bisher genutzte Software abzulösen. Damit sollte neben der Reduzierung des generellen Betriebsaufwands erstmalig eine vollständig automatisierte Darstellung von neuen oder geänderten Datenleitungen ermöglicht werden. Das DFN-NOC war der wichtigste Ansprechpartner für die zu berücksichtigenden User Stories, die Priorisierung der Anforderungen und die Datenbereitstellung.

> „Die Absicht war, auf Grundlage spezifischer Anforderungen eines Dienstes den Rahmen für die allgemeingültige Dienstüberwachung zu konstruieren – eine spannende Aufgabe, da wir weder ein reines Anzeigeinstrument für Netzwerktraffic bauen noch eine eierlegende Wollmilchsau schaffen wollten, deren zahlreiche gut gemeinte Features keinen praktischen Nutzen haben, sondern nur Aufwände verursachen."
> *Thiemo Nordenholz, Entwicklungsteam DFN-CERT*

Die entstandene sehr enge Zusammenarbeit zwischen Entwicklerinnen und Entwicklern (DFN-CERT) und „Endnutzern" (DFN-NOC) war für alle Seiten ein neuer Ansatz, der sicherlich auch ungewohnt und herausfordernd war. Er ermöglichte jedoch eine direkte und zeitnahe Interaktion zwischen den Teams. Zudem förderte die im besten Sinne agile Zusammenarbeit das Verständnis der jeweiligen Arbeit. In mehreren Iterationen setzte das Entwicklungsteam des DFN-CERT die Entwürfe um und erstellte aktualisierte Softwarekomponenten, die dann vom Betriebsteam des DFN-CERT auf einer Testinfrastruktur implementiert wurden. Hierbei war es besonders wichtig, die neuen Schnittstellen und Datenflüsse zwischen den Komponenten zu berücksichtigen. Neben der Arbeit am Testsystem wurde parallel die Produktionsumgebung aufgebaut, die ebenfalls vom DFN-CERT verantwortet wird.

> „In Zukunft wollen wir weitere Dienste und damit weitere Objekte, (z. B. die komplette Optische Plattform) in DMon aufnehmen, um mithilfe der so modellierten Abhängigkeiten die Fehleranalyse einfacher zu machen. Wir benötigen auch mehr Echtzeitfähigkeit auf der Objektmodellierungsseite für unsere Betriebsabläufe, um Umbauten direkt nach deren Durchführung abbilden zu können. Darüber hinaus gibt es noch zahlreiche Wünsche für Darstellungen oder die Nutzung von Daten aus DMon in anderen Systemen."
> *Jochen Schönfelder, Entwicklungsteam DFN-CERT*

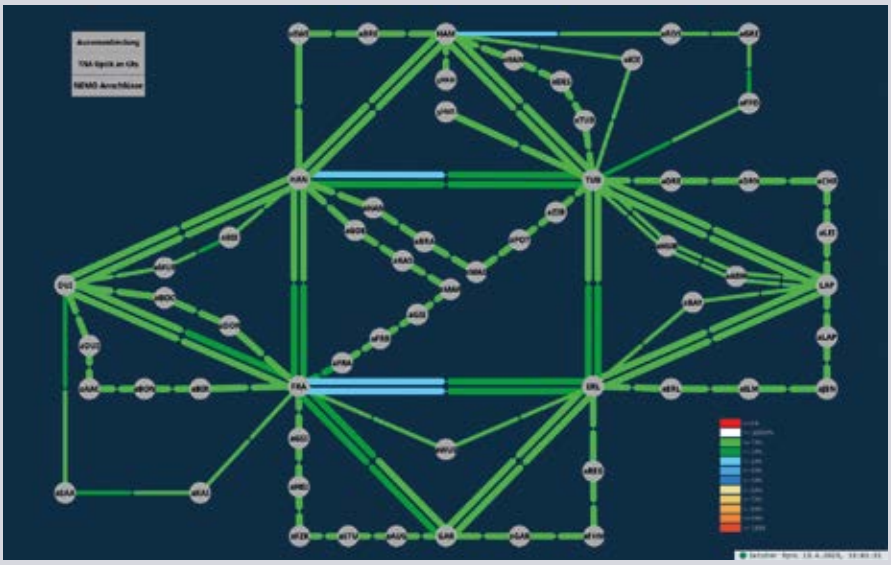
Ein Diagramm sagt mehr als tausend Byte-Worte

Die Datenannahme für das DMon-System besteht aus zwei Softwarekomponenten – der Objektmodellierung, von der die Infrastrukturinformationen aus einer SNMP-Erkundung und einer DAX-Abfrage (siehe DAX-Kasten) verarbeitet und zur Aktualisierung der DMon-Objekte und ihrer Verknüpfungen miteinander verwendet werden, sowie der Metrikerzeugung, in der die Nutzdaten verrechnet und den jeweiligen Objekten zugeordnet werden. Damit das klappt, schreibt die Objektmodellierung ihre Erkenntnisse nicht nur in die zentrale DMon-Datenbank, sondern liefert sie auch direkt an die Metrikerzeugung. Der genaue Weg der Daten wird auf Seite 10 detailliert beschrieben.

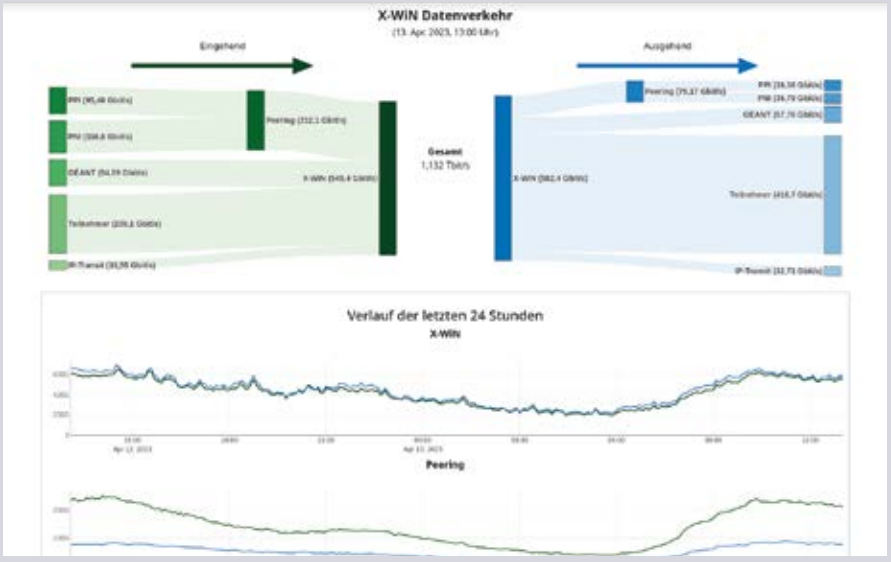
Wenn die Metriken wohlgeordnet und direkt abrufbar in einer Datenbank liegen, muss dieser Datenschatz noch für das menschliche Auge aufbereitet werden. Dabei spielt eine übersichtliche und nutzerfreundliche Oberfläche für ein erfolgreiches Netzwerkmonitoring eine zentrale Rolle. Sie ermöglicht es nicht nur den Fachleuten im NOC, schnell auf alle relevanten Netzwerkinformationen zuzugreifen, sie kann auch die Effizienz erhöhen, indem sie die Navigation durch verschiedene Funktionen und Optionen erleichtert und den Zeitaufwand für die Konfiguration und Verwaltung von Überwachungsregeln minimiert. Auf diese Punkte wurde bei der Entwicklung der grafischen Benutzeroberfläche (engl. Graphical User Interface – GUI) großer Wert gelegt. Aber auch die weitestgehend automatische Darstellung neuer oder angepasster Netzelemente lag stark im Fokus, da die bisher genutzten Tools einen hohen manuellen Pflegeaufwand erforderten.

Wichtigster Bestandteil der zuerst entwickelten Sicht auf das Kernnetz waren die

Das **DAX** ist die weitgehend echtzeitfähige zentrale DMon-Datenbank, welche relevante Topologie- und Dienstedaten aus dem internen Informationssystem des DFN enthält sowie weitere erforderliche Objektinformationen aus den Geräten im Netz.



Lagebild der X-WiN Kernnetzverbindungen als DMon-Weathermap



Darstellung des aktuellen X-WiN-Gesamtverkehrs

Verkehrsdiagramme. Diese zeigen den Datenverkehr, der durch das Netzwerk fließt, sowie weitere Messwerte, welche nahezu in Echtzeit oder in Form von historischen Verlaufsdaten dargestellt werden. Damit ist es möglich, Bandbreitenengpässe, Anomalien im Datenverkehr oder andere Netzwerkprobleme einzugrenzen oder direkt zu identifizieren. Unterstützt wird die Recherche durch vordefinierte Ansichten wie zum Beispiel Top-N-Views, in denen die am stärksten ausgelasteten Kernnetzstrecken oder die Links mit den höchsten optischen Dämpfungswerten dargestellt werden. Eine große Stärke des neuen DMon-Systems ist jedoch, dass individuelle Top-N-Views direkt über die Weboberfläche unter Nutzung aller verfügbaren Metriken sehr einfach „zusammengeklickt" werden können.

Weitere verfügbare Ansichten ermöglichen es, alle an einem Kernnetzknoten-Standort installierten Systeme von der USV-Anlage bis zum Router auf einen Blick zu erfassen und die benötigten Informationen per Diagramm abzurufen.

Das vorerst letzte wichtige Puzzlestück zu einem vollständigen (Netzwerk-) Bild bildet die topologische Sicht. Diese zeigt die physische oder logische Struktur des Netzes einschließlich der Verbindungen zwischen Geräten wie Switches, Router und DWDM-Systeme. Dabei stellen sogenannte „Weathermaps" eine wichtige visuelle Komponente dar. Diese können ein aktuelles Lagebild über alle Kernnetzverbindungen, die Außenanbindungen des X-WiN und wichtige optische Verbindungen übersichtlich darstellen.

> Das vorerst letzte wichtige Puzzlestück zu einem vollständigen (Netzwerk-) Bild bildet die topologische Sicht.

Die gesamte Benutzeroberfläche ist jedoch nicht nur für spezifische Netzwerksichten vorgesehen, sondern sie stellt diese grundlegenden Funktionen auch für andere mögliche Anwendungsszenarien, wie sie bei Anwendungs- oder Servermonitoring benötigt werden, zur Verfügung. Hierfür bilden die für die Entwicklung genutzten, frei verfügbaren und leistungsstarken Werkzeuge eine solide und zukunftssichere Grundlage.

Ein weiterer schon realisierter Anwendungsfall zur Nutzung von DMon-Metriken ist das DFN-Teilnehmerportal. Hier können Teilnehmer die aktuell genutzte Bandbreite einzelner Zugangsverbindungen und der darüber versorgten DFN-Internetdienste, aber auch historische Daten zur Auslastung grafisch abrufen.

Blick in die Zukunft

Neben der aktuell im Endspurt der Integration befindlichen DMon-Alarmierungskomponente soll ein möglichst vollumfänglicher Betriebsstatus durch DMon abgebildet werden. Deshalb modelliert das Entwicklungsteam des DFN-CERT in

einem nächsten Schritt abstraktere Objekte der Netzinfrastruktur, die durch mehrere Ebenen von Betriebs- oder Verwaltungskonstrukten mit den Messwerten der physischen Komponenten verknüpft sind. Ziel hierbei sind die Erfassung und Darstellung betrieblicher Abhängigkeiten und der Auswirkung von Betriebszuständen einzelner Komponenten auf übergeordnete Einheiten. Dadurch sollen schnell erfassbare Übersichten von Dienstverfügbarkeiten ermöglicht werden, in denen auch eine einfache Verfolgung der Ursachen eventueller Beeinträchtigungen möglich wird.

Weiterhin wird an der Integration des Monitorings relevanter Kennzahlen der Optikplattform bis auf „Glasfaser"-Level sowie der Vervollständigung der überwachten Infrastrukturkomponenten (u. a. Zugangskontrolle, Stromversorgung) gearbeitet.

Aber auch Verbesserungen der Echtzeitfähigkeiten an der Basis, das betrifft die Kennzahlenerfassung von Geräten im Netz, sind konkrete Anforderungen. Mittlerweile etabliert sich „Streaming Network Telemetry" als moderne Nachfolgerin des betagten SNMP zur Kennzahlenübermittlung von den Routern und DWDM-Geräten zu den Kollektoren. Damit werden deutliche Verbesserungen in den Update-Intervallen und somit höhere Auflösungen in den Zeitgraphen bis in den Sekundenbereich möglich und dies bei geringerer Belastung der Geräte, die Kennzahlen liefern.

Auch wenn noch viele kleine und große Schritte vor ihnen liegen, sind die Projektbeteiligten mit dem erreichten Meilenstein sehr zufrieden und haben DMon schnell in den Arbeitsalltag integriert. Vor allem die Aussicht, auf Basis einer soliden und aktuellen Plattform das Monitoring des X-WiN zum Nutzen der Teilnehmer zu erweitern, motiviert alle Beteiligten. Nicht zuletzt hat dieses Projekt von Kolleginnen und Kollegen des DFN-CERT und des DFN-Vereins gezeigt, wie ein kleines, aber feines Projektteam gemeinsam erfolgreich sein kann. ◆

Der Weg der Daten

Am Beispiel der von den Kernnetzkomponenten mittels SNMP erhobenen Messwerte lässt sich der Weg der Struktur- und Nutzdaten von den gemessenen Geräten bis in die DMon-Datenbank gut verfolgen.

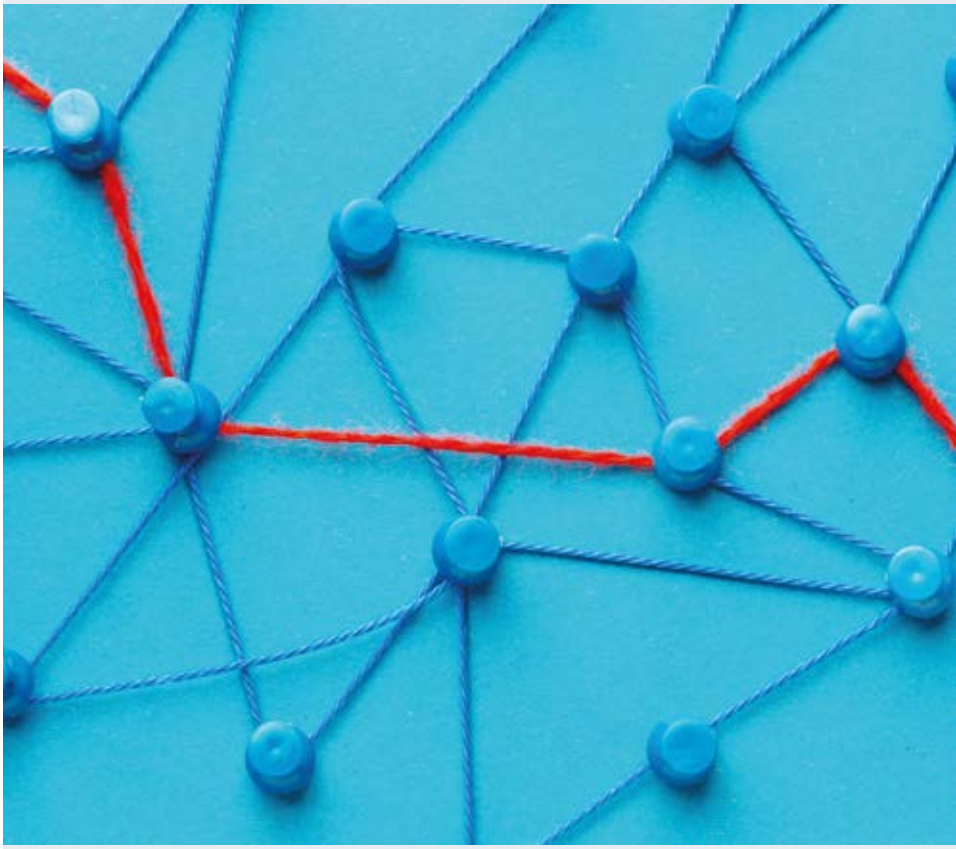


Foto: 2m assets/freepik

Grundsätzlich existiert schon seit einigen Jahren ein redundant ausgelegtes System zur Sammlung von Messwerten von Netzwerk- und Infrastrukturkomponenten per Simple Network Management Protocol (SNMP), das auch DMon als Lieferant von Daten über den Netzbetrieb dient, der sogenannte SNMP-Kollektor.

In regelmäßigen Abständen wird im SNMP-Kollektor eine „Erkundung" der zu überwachenden Geräte ausgelöst. Hierfür wird zunächst über eine DAX-Schnittstelle die Liste der im DFN-internen Informationssystem hinterlegten Systeme abgerufen. Nun ist nicht jeder Messpunkt, der überwacht werden soll, im internen Informationssystem abgebildet – dort wäre ein Detaillierungsgrad zum Beispiel bis hin zu einzelnen Temperaturfühlern in Routingprozessoren unnötig. Deshalb erkundet der SNMP-Kollektor zunächst über gezielte SNMP-Abfragen die Verfügbarkeit und Anzahl bestimmter Elemente und deren Messwerte in einem Gerät.

Die gewünschten Messpunkte und die dafür nutzbaren Abfrageverfahren sind in Abhängigkeit von Gerätetypen und -modellen in einer modularen Architektur abgebildet: Eine unterbrechungsfreie Stromversorgung zum Beispiel muss auf andere Messpunkte hin untersucht werden als ein Router, bei dem eher die Anzahl und Ausprägung der Netzwerkinterfaces interessanter sind als die Kapazität einzelner Batteriemodule wie bei einer USV.

Aus den Ergebnissen dieser Analyse werden wiederum, durch vorgegebene Regeln gesteuert die eigentlichen SNMP-Abfragen im Kollektor konfiguriert. In bestimmten Intervallen ist von den erfassten Komponenten jeweils eine definierte Menge von Messwerten zu erfragen. Damit die Datenerhebung effizient geschieht, wird wenn möglich eine einzige Abfrage pro Messpunkt generiert, um alle relevanten Werte zu erhalten. Diese Methode ist ebenfalls wichtig, um eine Überlastung der Systeme durch Managementverkehr zu vermeiden.

Zusätzlich wird aus dem Ergebnis der SNMP-Erkundung ein Datensatz erstellt, der dem DMon-System zur Modellierung der zu überwachenden „Welt" dient.

Der für die Nutzdaten zuständige Teil des SNMP-Kollektors verwendet diese Abfragekonfiguration und verschickt regelmäßig Anfragen an die Geräte, deren Antworten neben der lokalen Speicherung für die schon vorher bestehenden Konsumenten auch an die DMon-Systeme weitergeleitet werden.

Die Dateneingangskomponenten von DMon erhalten nach einem SNMP-Erkundungslauf den erwähnten Datensatz mit der gefundenen Infrastruktur und damit auch mit den zu erwartenden Messwerten. Um die höheren Abstraktionsebenen mit diesem eher techniknahen Bild verknüpfen zu können, werden von DMon zusätzliche Informationen aus DAX bezogen und aus den zusammengefassten Daten bei Bedarf eine Aktualisierung der in DMon gepflegten Modelle von überwachten Objekten vorgenommen.

Die Nutzdaten, die quasi in stetem Strom von den SNMP-Kollektoren eingeliefert werden, werden im DMon-Dateneingang anhand ihres Ursprungsgeräts und des SNMP-Objektbezeichners (ihrer OID) jeweils den modellierten Objekten in DMon zugeordnet.

Da diese erfassten Daten nicht in jedem Fall 1:1 darstellbar sind, muss häufig noch eine weitere Verarbeitung bzw. Umwandlung erfolgen. Beispielsweise liefern Netzwerkschnittstellen die Menge des durchgeleiteten Datenverkehrs in Form eines durch Überlauf oder Neustart zurückgesetzten byteweisen (und 64 Bit breiten) Zählers – für die meisten Anwendungsfälle ist aber eine Darstellung als Datendurchsatz in bit/s viel interessanter und intuitiver.

An diesem Punkt der Verarbeitung erfolgt somit die Umwandlung von reinen Messwerten in besser nutzbare sogenannte Metriken. Diese normalisierten Werte können nun zusätzlich zur Berechnung und Darstellung weiterer Kenngrößen genutzt werden. So ist es beispielsweise möglich, die Dämpfung einer Glasfaserstrecke aus den gemessenen Signalpegeln an beiden Faserenden zu berechnen.

Die so ermittelten Metriken werden dann den jeweiligen DMon-Objekten zugeordnet und in einer Datenbank gespeichert. Damit stehen diese Informationen den Konsumenten, wie der intern genutzten DMon-Benutzeroberfläche, dem Teilnehmerportal oder der Alarmierungskomponente per standardisierter REST-Schnittstelle, zur Verfügung.

Die erwähnte Metrik-Erzeugung aus SNMP-Messwerten ist nur ein möglicher Lieferant für Metriken. Vorstellbar und geplant sind weitere Komponenten, die aus anderen Datenquellen, wie zum Beispiel der „Streaming Network Telemetry", ebenfalls Metriken an DMon-Objekten erzeugen und in die Datenbank einliefern.

Wolkenreise – DFN-Cloud als Gesamtpaket

Kaum ein IT-Thema polarisiert derzeit mehr als die Frage: On-Premise oder Cloud? Vor allem Fragen zum souveränen Umgang mit den eigenen Daten stehen im Fokus. Zusätzlich angefeuert wird der Diskurs durch KI-Technologien, die den Arbeitsalltag an Universitäten, Hochschulen und Forschungseinrichtungen immer tiefer durchdringen. Auch der DFN ist in diesem Spannungsfeld aktiv – sowohl mit eigenen Ressourcen als auch mit zusätzlichen Technologien aus der Cloud. Hier soll das Beratungsangebot weiter optimiert und professionalisiert werden.

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

Der Trend, Dinge gemeinsam zu nutzen, ist besonders bei jungen Leuten sehr beliebt. Es wird bereits von einer „Shareconomy“ gesprochen. Die Idee dahinter ist genial einfach – alle Dinge, die ich nicht besitzen möchte, leihe ich mir eben. Der Trend zum kollaborativen Konsum sei nicht ganz ungefährlich, warnte das Handelsblatt bereits vor zehn Jahren. Längerfristig angelegten Technologien werde dadurch möglicherweise das Wasser abgegraben. Aber ist das wirklich so? Ist es nicht gerade Sinn und Zweck des DFN-Vereins, Infrastrukturen gemeinschaftlich nutzbar zur Verfügung zu stellen und dadurch neue Verfahren für Forschung und Lehre zu fördern? So ganz neu ist das Thema Cloud für den DFN-Verein jedenfalls nicht – angefangen von gemeinsam genutzter Hardware für den Datentransport im Wissenschaftsnetz bis hin zur Anwendungsebene, wenn es um die Nutzung von Diensten für Videokonferenzen, Fernsprechen und Terminplanungen sowie den WLAN-Zugang teilnehmender Einrichtungen geht.

Cloud-Dienste für die Wissenschaft

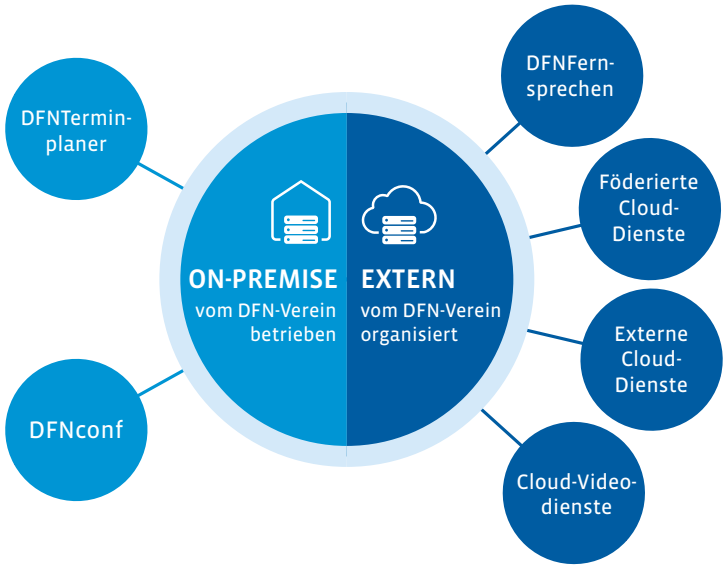
Hinter der Bezeichnung „DFN-Cloud“ verbirgt sich viel mehr als der Zugriff auf externe gewerbliche Cloud-Dienste. So wie in der Meteorologie auch zwischen verschiedenen Wolkenformationen unterschieden wird, so wird beim DFN zwischen Clouds mit jeweils besonderen Spezifika unterschieden. Aktuell werden Dienste aus vier verschiedenen Kategorien angeboten:

1. **DFN-eigene Dienste:** Sie werden auf DFN-Servern on-premise betrieben und vom DFN-Verein administriert. Mehr Datenhoheit geht nicht.
2. **Föderierte Dienste:** Seit geraumer Zeit kooperiert der DFN mit Cloud-Anbietern des öffentlichen Sektors, meist aus dem Umfeld von Universitäten und Forschungseinrichtungen – es wird hier von „Föderierten Cloud-Angeboten“ gesprochen.
3. **Rahmenverträge für cloudbasierte Web- und Videokonferenzdienste:** Damit DFN-Teilnehmer auf cloudbasierte Web- und Videokonferenzdienste zugreifen können, ohne selbst ausschreiben zu müssen, hat der DFN-Verein mit unterschiedlichen gewerblichen Anbietern erfolgreich Rahmenverträge abgeschlossen.
4. **Externe Cloud-Dienste (Kommerzielle Cloud-Dienste):** Die europäische Dachorganisation GÉANT hat Rahmenverträge für kommerzielle Cloud-Dienste ausgehandelt, daran war der DFN-Verein maßgeblich beteiligt. Unter dem Stichwort IaaS+ sind vielfältige Dateninfrastrukturen, Plattformen und Dienste erreichbar – von Spezialanwendungen für Künstliche Intelligenz und Machine Learning über Container-Entwicklungsumgebungen bis hin zu Erdbeobachtungsdiensten.

Für die beiden Cloud-Formate der Punkte 3 und 4 stehen derzeit einige Entscheidungen an: Bei den auf zwei Jahre angelegten „Rahmenverträgen für cloudbasierte Web- und Videokonferenzdienste“ geht es darum zu entscheiden, ob die Verlängerungsoptionen in Anspruch genommen werden oder nicht. Für die auf vier Jahre angelegten Rahmenverträge für Infrastructures as a Service steht 2024 eine Neuausschreibung an.

Die Cloud-Videodienste des DFN

Betrachtet man die Cloud-Videodienste, für die der DFN-Verein als Rahmenvertragspartner fungiert, betrifft das rund 1,3 Millionen Nutzungszugänge zu unterschiedlichen Video- und Webkonferenzdiensten. Aktuell gibt es sieben Rahmenverträge, die regulär bis Mitte März 2024 gültig sind und durch Verlängerungsoptionen auf bis zu vier Jahre ausgedehnt werden können. Bis Ende Juli 2023 wird feststehen, wie es hier weitergeht – idealerweise im Einvernehmen mit den jeweiligen Anbietern der Rahmenverträge.



Dienstangebote im DFN-Bereich Collaboration Services

Letztendlich bleibt es aber eine Entscheidung, die der DFN stellvertretend für seine Mitglieder und teilnehmenden Einrichtungen treffen wird. Die Entscheidungsgrundlage pro oder contra einer optionalen Verlängerung wird aber nicht allein die Bewertung des finanziellen Erfolgs der Dienstanbieter sein können. In einer ausgewogenen Bewertung der Dienstqualität wird auch darauf geschaut, wie die Videodienste sich vertriebsseitig in die Vergabe- und Betriebsprozesse des DFN und seiner teilnehmenden Einrichtungen einpassen lassen. Zusätzlich spielt es eine Rolle, wie sehr ein Videodienst die Weiterentwicklung der nutzenden Einrichtungen beispielsweise durch Softwareschulungen unterstützt, wie sehr die zu bewertenden Dienste dazu beitragen, teilnehmende Einrichtungen bei der Bereitstellung des Dienstes für deren Nutzerinnen und Nutzer zu unterstützen und wie sehr die Anbieter sich um Innovationen ihres Dienstangebotes kümmern. Aus Sicht des DFN muss darüber hinaus auch noch darauf geachtet werden, nicht zu abhängig von einem Anbieter zu werden, um nicht letztendlich preisliche Entwicklungen akzeptieren zu müssen, die nicht im Interesse der DFN-Mitglieder sind. Schon jetzt zeichnet sich eine solche Entwicklung ab, die den Handlungsspielraum der dienstnutzenden Einrichtungen erheblich einschränken könnte.

Workshop zum Start der Neuausschreibung kommerzieller Cloud-Dienste

Bei den kommerziellen Cloud-Diensten gilt es zurzeit, Bedarfe und Anforderungen der DFN-Community für die 2024 anstehende europäische Neuausschreibung der Cloud-Rahmenverträge zu ermitteln. Nach erfolgreicher Beendigung des EU-Projekts Open Clouds for Research Environments (OCRE) im Dezember 2022 stehen die Vorbereitungen dazu im GÉANT-Projekt GN5-1 nun in den Startlöchern. Die aktuellen Rahmenverträge sind bis zum Ende der Laufzeit im Oktober 2024 weiterhin gültig. Als Partner der Wissenschaftscommunity in Deutsch-

land führt der DFN-Verein die Bedarfsermittlung der Folgeausschreibung durch.

Dazu organisierte der DFN-Verein am 20. und 21. April 2023 einen Cloud-Workshop in Osnabrück, um gemeinsam mit Vertretenden der DFN-Teilnehmereinrichtungen erste Gedanken und Ideen auszutauschen und Aspekte für eine möglichst passgenaue Ausschreibung zu identifizieren. Ein Ziel dabei ist es, innovative Technologietrends frühzeitig zu erkennen und dabei die Frage zu beantworten, ob und wie entsprechende Angebote in europäische Ausschreibungen integriert werden können. Beim Workshop kam heraus, dass die aktive Cloud-Community mit der Angebotsvielfalt durchaus zufrieden ist, bei der Produktpräsentation und der Produktplatzierung aber noch Verbesserungspotenzial sieht.

Fotos: Freepik

Der DFN-Verein nimmt mit seinem Cloud-Angebot fördernde und unterstützende Aufgaben oberhalb der Ebene technischer Vernetzung wahr, um Forschenden und Lehrenden Zugriff auf diejenigen Infrastrukturen zu geben, die seitens des DFN-Vereins nur mit erheblichem Aufwand zu betreiben wären. Damit sind insbesondere zeitkritisch hochskalierende Technologien gemeint, für die externe Anbieter mit ihren vielfältigen Cloud-Infrastrukturen besser ausgelegt sind. Es geht aber auch um Dienste, die auf Cloud-Infrastrukturen aufbauen und dabei sehr individuell zu administrieren sind – beispielsweise beim Zugriff auf Daten der satellitengestützten Erdbeobachtung oder der Bereitstellung verlässlicher Processing-Leistung für Anwendungen auf der Grundlage von Echtzeitbetriebssystemen.

Die Abrufzahlen der europäischen Rahmenverträge aus dem vergangenen Jahr zeigen, dass diesbezüglich noch reichlich Luft nach oben besteht. Nur wenige Einrichtungen erzielen Umsatzwerte, die über vier Jahre betrachtet den Schwellenwert für europäische Ausschreibungen erreichen würden. Bemerkenswert ist auch der relativ große Anteil von Einrichtungen, die lediglich für Beträge in geringwertigem Umfang Dienste bei den Cloud-Anbietern bestellen. Vom finanziellen Umfang her betrachtet ist aber nur sehr schwer zu entscheiden, ob die Nutzung eines Dienstes sinnvoll ist oder nicht. Es ist daher auch eine zentrale Aufgabe des DFN-Vereins, dem Anbietermarkt zu vermitteln, dass sich Cloud-Technologien nicht von heute auf morgen durchsetzen lassen. Denn die Frage nach dem Einsatz externer IT-Infrastrukturen greift tief in das Bedürfnis der teilnehmenden Einrichtungen ein, die Hoheit über die eigenen Daten nicht aus der Hand zu geben. Dies ist angesichts nach wie vor unklarer Datenaustauschabkommen mit Staaten außerhalb der EU auch nicht verwunderlich. Der DFN-Verein nimmt die Herausforderungen mit den besonders schützenswerten Daten aus Forschung und Lehre sehr ernst.

Seit Anfang des Jahres werden die Cloud-Angebote des DFN-Vereins weiter gebündelt und nun über den DFN-Bereich „Collaboration Services“ organisiert. Die Bereitstellung von entsprechenden Infrastrukturen, Plattformen und Software soll auf diese Weise weiter optimiert werden, um Synergien zu fördern und mögliche Widersprüche zwischen bundesweiten Ausschreibungen und Ausschreibungen auf europäischer Ebene zu erkennen. Ein Beispiel ist die gesamtheitliche Betrachtung des Microsoft-Portfolios mit dem Videodienst „Teams“ aus dem Videokonferenzrahmenvertrag auf der einen Seite und der Azure-Plattform aus dem GÉANT-Rahmenvertrag auf der anderen. Im Angebot der europäischen Cloud ist die Nutzung von „Teams“ nicht vorgesehen. In dem vom DFN-Verein deutschlandweit ausgeschriebenen Rahmenvertrag der Cloud-Videodienste kann auf diese Videokonferenzsoftware aber sehr wohl zugegriffen werden. Hier spielt die richtige Beratung eine wichtige Rolle. Mit der Bündelung des Angebots möchte der DFN-Verein auf die steigenden Nachfragezahlen und den damit verbundenen Beratungsbedarf reagieren. ◆

Externe Dienste in der DFN-Cloud – Erfahrungsbericht der TU Darmstadt

Nach Beendigung des EU-Projekts Open Clouds for Research Environments (OCRE) zur Organisation von Cloud-Rahmenverträgen für die Wissenschaft starten nun die Vorbereitungen für die Neuausschreibung. Zeit für ein Resümee aus der Praxis: Das Hochschulrechenzentrum (HRZ) der Technischen Universität Darmstadt gibt Einblick, mit welchen Überlegungen es in den Auswahlprozess für einen Serviceprovider gegangen ist und zeigt, welche individuellen Herausforderungen auftreten können.

Text: **Leif Pullich, Thomas Haake** (Technische Universität Darmstadt)

Foto: go2/photocase

Ausgangspunkt für die Nutzung der externen Cloud-Dienste des DFN-Vereins durch das Hochschulrechenzentrum (HRZ) der TU Darmstadt ist ein wachsender Bedarf der universitätseigenen Fachgebiete an Datenspeicher. Es kommen zunehmend Anfragen nach Speichervolumina im Bereich mittlerer zweistelliger bis dreistelliger Terabytes, die mit dem bestehenden Fileservice nicht kurzfristig bedient werden können.

Daher schien es sinnvoll zu prüfen, ob diesem Mangel mit der Wahl eines Serviceproviders für Anwendungen vom Typ „Infrastructure-as-a-Service" (IaaS) aus den OCRE-Rahmenverträgen abgeholfen werden könnte. Der naheliegende Vorteil ist, dass keine eigene Ausschreibung erforderlich ist. Der zweite Vorteil war für uns, dass die Datenschutzanforderungen gemäß DSGVO geregelt sind. Denn Serviceprovider, die Services für europäische Forschungseinrichtungen anbieten, müssten ja dem gesetzlichen Rahmen der EU entsprechen – so unsere anfängliche Erwartung. Im Vergabeverfahren haben alle Anbieter die Unterstützung der DSGVO zugesichert. Allerdings lautet die Empfehlung des DFN-Vereins, außereuropäische Anbieter dahingehend genau zu prüfen und zusätzliche Sicherungen einzubauen. Der hessische Datenschutzbeauftragte gab den Hinweis, unter Umständen auf außereuropäische Anbieter ganz zu verzichten. Weitere Vorteile der DFN-Rahmenverträge sind Preisnachlässe, die Zahlung per Rechnung statt Kreditkarte und der Verzicht auf die Abrechnung ausgehender Datentransfers.

Die IT-Versorgung an der TU Darmstadt ist in großen Teilen dezentral organisiert. Ein Gesamtkonzept für die Aufgabenteilung und Zusammenarbeit zwischen dezentralen und zentralen IT-Betreibern gibt es nicht. Wir beobachten jedoch, dass zunehmend „managed Services" beim HRZ angefragt werden. Die aktuell nachkommende Generation an Wissenschaftlerinnen und Wissenschaftlern ist es bereits gewohnt, IT-Services zu nutzen, und nicht mehr daran interessiert, ihre eigenen Systeme zu betreiben. Es erscheint uns wichtig, dass die zentrale IT-Einheit als Mittlerin und Managementinstanz für IaaS-Cloud-Services agiert. Es kann in der Gesamtbetrachtung weder im Interesse der Universität noch ihrer Einrichtungen liegen, die notwendigen Verfahren, Verträge etc. dezentral und unabhängig voneinander zu bearbeiten.

Anforderungen und Servicemodell

Der Ansatz, den wir zunächst für die Rolle dieser Managementinstanz gewählt haben, basiert auf folgenden Überlegungen zum Zusammenspiel von Cloud-Provider, HRZ und den nutzenden Bereichen in der TU:

- **Rahmenbedingungen:** Das HRZ schafft die Rahmenbedingungen, indem es einen geeigneten Cloud-Provider auswählt und das sogenannte Call-of-Agreement mit dem Cloud-Provider abschließt.
- **Beratung:** Das HRZ berät ggf. zusammen mit dem Serviceprovider die Einrichtungen (interne Kunden) bezüglich der Umsetzbarkeit ihrer Bedarfe sowie der Kosten und begleitet die Einrichtung beim Onboarding auf den Service.
- **Technischer Support:** Für den technischen 1st- und 2nd-Level-Support bei der Nutzung der Services sollen sich die Einrichtungen ohne Umweg über das HRZ direkt an den Support des Serviceproviders wenden können. Das HRZ soll nur dort, wo es direkt involviert ist oder aber im Eskalationsfall hinzugezogen werden.
- **Vermittlung:** Das HRZ trägt ggf. Änderungsanforderungen der Einrichtungen bezüglich Funktionalitäten oder anderer Merkmale des Service an den Serviceprovider heran.
- **Einfache Zuordnung:** Es muss auf einfache Weise möglich sein, den Verbrauch an Cloud-Ressourcen eindeutig einem internen Kunden zuzuordnen. Da keine zentrale Finanzierung zur Verfügung steht, müssen alle Kosten direkt an die Kostenverursacher weitergereicht werden.
- **Zentrales Managementportal:** Beim Management soll einerseits ein zentrales Managementportal dem HRZ einen Gesamtüberblick ermöglichen. Gleichzeitig muss die Möglichkeit bestehen, Anforderungen verschiedener Fachgebiete unabhängig voneinander umzusetzen und erforderlichenfalls administrative Aufgaben an dezentrale Admins zu delegieren. Diese sollen jeweils nur für ihren Bereich berechtigt sein.
- **IT-Kenntnisse im Fachbereich:** Aufseiten des Fachgebiets ist eine hinreichend IT-sachkundige Person erforderlich, mit der die Anforderungen besprochen werden können, und die in der Lage ist, die Nutzenden der Einrichtung zu betreuen sowie Konfigurationsaufgaben und Nutzerverwaltung zu übernehmen. Diese Voraussetzung war am Anfang noch sehr vage, hat im Laufe des Prozesses jedoch an Schärfe gewonnen.
- **Bedarfe:** Wir beschränken uns zunächst auf Speicher, sehen aber die spätere Ausweitung auf Compute-Services oder Container-Services als Weiterentwicklung vor.

Auswahlverfahren

Die Provider-Auswahl verlief in mehreren Stufen: Nach einer ersten Beratung mit dem Cloud-Team des DFN-Vereins bezüglich unserer Anforderungen wählten wir anhand der Anbieterwebseiten diejenigen Provider aus, die für unseren Bedarf infrage kamen. Mit jedem der Anbieter führten wir ein Vorgespräch, um zu prüfen, wie gut unsere Vorstellungen und das Angebot des Providers zusammenpassen. So mussten wir in einem Fall feststellen, dass die Services nicht zu unserem Modell passten, weil sie sich ausschließlich an Rechenzentren richteten und die beschriebene Dreieckskonstellation nicht umsetzbar war.

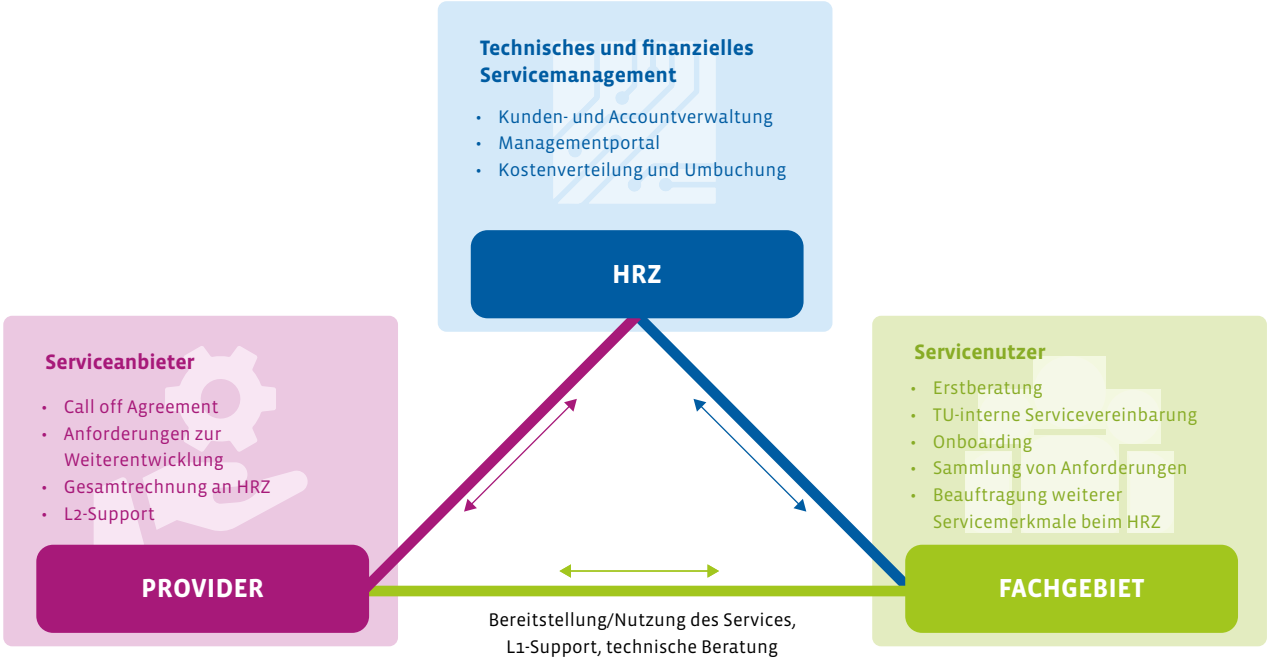
Das in den OCRE-Rahmenverträgen festgelegte Verfahren sieht vor, einen Mini-Schreibtisch-Wettbewerb durchzuführen, wenn mehrere Provider die gewünschte Leistung erbringen. Mithilfe eines vom DFN-Verein bereitgestellten Auswertungstemplates können die Kosten der verschiedenen Angebote verglichen werden. Hier haben uns die Vorgespräche geholfen, überhaupt eine Anfrage formulieren zu können, wenngleich diese aus heutiger Sicht noch sehr unspezifisch erscheint. Aufgrund der unterschiedlichen Abrechnungsmodelle, Preisstaffeln und Gliederung der Services und ihrer Eigenschaften ist es nicht ganz einfach, die Angebote auf vergleichbare Gesamtkosten für die gewünschten Nutzungsszenarien zusammenzurechnen, um sie dann mit dem Auswertungstemplate hinsichtlich der Kosten zu ranken. Als Ergebnis dieses Verfahrens haben wir uns für T-Systems mit der Open Telekom Cloud (OTC) entschieden.

Pilotnutzung

Für die Einführung des Storage-Angebots war von vornherein eine mehrmonatige Pilotphase mit drei bis fünf Fachgebieten vorgesehen, um Know-how zum Management der Cloud aufzubauen und Erfahrungen mit der Nutzung, dem Zusammenspiel der Akteure sowie den erforderlichen Abstimmungen und Prozessen zu sammeln. Diese Erfahrungen sollen in das Design des Service einfließen, mit dem das HRZ dann schließlich produktiv gehen wird.

Parallel zum Auswahlverfahren haben wir daher bereits Fachgebiete angesprochen, um sie für die Pilotnutzung zu gewinnen. Derzeit ist das erste – recht einfache – Projekt angelaufen. Für circa 70 Nutzende verschiedener Arbeitsgruppen werden Forschungsdaten, die lokal auf Clients bearbeitet werden, mittels eines S3-Clients automatisch als individuelles Backup in einem Object Storage gesichert. Im nächsten Schritt soll Speicher für eine größere, fachbereichsübergreifende Gruppe von Forschenden zur Verfügung gestellt werden, die große Bilddaten untereinander austauschen wollen. Hier stehen ausreichend Platz und akzeptable Up- und Download-Raten im Vordergrund, während eine Datensicherung nicht erforderlich ist, da keine längere Speicherung erwünscht ist. Im HRZ selbst gehen die Überlegungen bereits über Speicher hinaus: Hier sollen die Erweiterung der VDI-Systeme mit Virtuellen Maschinen und die Nutzung von Container-Services getestet werden. Andere Interessierte haben sich von der geplanten Pilotnutzung wieder zurückgezogen, weil die Kosten, die für ihr Szenario angefallen wären, zu hoch waren. Hierbei wurde auch deutlich, dass nicht alle Szenarien in der Cloud 1:1 wirtschaftlich umsetzbar sind.

Die bisherigen Aktivitäten zeigen, dass sowohl auf HRZ-Ebene als auch bei den internen Kunden einiges an Überlegungen dazu erforderlich ist, wie sich beispielsweise die



Schematische Darstellung des aktuellen HRZ-Servicemodells

Hochschulrechenzentrum (HRZ) der Technischen Universität Darmstadt | *Foto: HRZ*

organisatorischen und technischen Gliederungsmöglichkeiten, die durch den Provider bereitgestellt werden, sinnvoll für die eigenen Anforderungen und Rahmenbedingungen nutzen lassen. Solange das System und die Implikationen bestimmter Entscheidungen noch nicht ausreichend verstanden werden, ist man als Kunde auf gute Beratung durch den Provider angewiesen.

Erfahrungen

Bereits vor dem Start des ersten Pilotprojekts ergab sich eine Anforderung, die entgegen unseren Erwartungen nicht einfach durch Konfiguration im Managementportal umsetzbar war. Das Fachgebiet wollte eine Quota auf das zur Verfügung gestellte Speichervolumen haben, um sicherzugehen, dass die Kosten durch unbemerkte Fehlkonfigurationen oder unbedachte Nutzende nicht aus dem Ruder laufen. Ein fortlaufendes Monitoring oder eine sofortige Reaktionsfähigkeit auf Alerts, die beim Überschreiten von Schwellenwerten anschlagen, konnten weder das Fachgebiet noch das HRZ sicherstellen.

Es ist klar, dass die Anforderung, eine wirksame Kostenbremse einzubauen, für die meisten unserer internen Kunden von Interesse sein wird. Beim gewählten Servicemodell mit voneinander unabhängigen Kunden sollten entsprechende Einstellungen für die Administration eines Kunden daher leicht im Managementportal realisierbar sein. Die Quota auf dem Object Storage ist derzeit nur dadurch zu erreichen, dass über Gebrauch der API oder auf der Kommandozeile Einzel-Quotas für alle 70 Nutzenden gesetzt werden. In einem Piloten lässt sich Letzteres zwar manuell umsetzen, dies ist aber keine Lösung für den Produktivbetrieb. Ein weiterer Punkt ist die Frage nach einem zentralen „Not-Aus“ für den Speicher, wenn zum Beispiel ein Befall mit Schadsoftware festgestellt wird. Hier gibt es noch keine Lösung, aber der Provider hat signalisiert, sich beiden Punkten widmen zu wollen.

Für die Zukunft wird es auch wichtig sein, Nutzende sowie deren Attribute und Gruppenzugehörigkeiten, die über das Identity Management und die angeschlossenen Verzeichnisdienste geliefert werden können, für die Nutzerverwaltung in der Cloud zugänglich zu machen. Hier haben wir bisher noch keine Erfahrung.

Bei der Abrechnung hatten wir uns ursprünglich gewünscht, dass die Rechnungen vom Serviceprovider direkt an die internen Kunden gestellt werden. Dies ließ sich so nicht umsetzen. Stattdessen bekommt das HRZ pro internem Kunden eine monatliche Rechnung, die intern weiterverrechnet wird. Die Einzelrechnung wird dadurch erreicht, dass jeder Kunde in einem sogenannten Tenant abgebildet wird. Dies ermöglicht neben der separaten Abrechnung auch eine unabhängige Verwaltung der in Anspruch genommenen Ressourcen. Dennoch hat das HRZ die gewünschte technische und finanzielle Gesamteinsicht.

Fazit

Unsere Hoffnung bei der Auswahl eines kommerziellen Cloud-Providers für Forschung und Lehre war, Services zu erhalten, deren Weitergabe an die Einrichtungen der Universität wir im Wesentlichen zentral koordinieren und die in allen Konfigurationsaspekten weitestgehend über ein webbasiertes Interface „einstellbar“ sind. Uns ist jedoch klar geworden, dass die Services derzeit nur bedingt für die endnutzenden Einrichtungen geeignet sind. Sie setzen voraus, dass es entweder eine zentrale IT-Einheit gibt, die mit den Services des Providers einfach zu nutzende Dienste aufbaut oder dass die Einrichtungen über ausreichende eigene Personalressourcen mit entsprechender IT-Kompetenz sowie ausreichende finanzielle Mittel verfügen, um die Cloud-Services nutzen zu können. Der bisher eingeschlagene Lösungsweg wird daher nur einen Teil des Bedarfs decken können. Hier werden wir integrierte Dienste bereitstellen müssen, bei denen es für die Nutzenden unerheblich ist, ob sie ganz oder in Teilen aus eigenen Systemen oder aus der Cloud kommen, solange Funktionalität und Übereinstimmung mit den Regularien für Datenschutz und Sicherheit gegeben sind. Darüber hinaus werfen aber auch Wirtschaftlichkeit und Finanzierbarkeit der Cloud-Nutzung Fragen auf, die noch beantwortet werden müssen. ◆

Weitere Informationen zum Vergabeverfahren für IaaS-Cloud-Services finden Sie unter: **https://www2.dfn.de/dfn-cloud/dienste-nutzen**

Kurzmeldungen

Alles neu macht der Mai – der DFN-Verein modernisiert seine Aggregations-Plattform

Die IP-Plattform des X-WiN verfügt über zwei Router-Plattformen: Die acht „großen“ Router des SuperCore sowie die 50 „kleinen“ der Aggregations-Plattform. Die aktuelle Aggregations-Plattform verrichtet seit Anfang 2017 ihre Arbeit und stellt Dienste mit bis zu 10 Gbit/s bereit. Nach rund sieben Jahren und damit einhergehenden gewachsenen Leistungsanforderungen der Teilnehmer wird es Zeit für ein Upgrade: Die alten Router werden komplett gegen einen neuen Gerätetyp ausgetauscht. Die neuen Systeme versechsfachen die verfügbare Routingkapazität auf 2,4 Tbit/s und bieten damit erstmals die Möglichkeit, an allen Standorten der Aggregations-Plattform Teilnehmer lokal mit 100-Gigabit-Ethernet anzubinden.

Die Migration auf die insgesamt 58 neuen Systeme an 56 Standorten startete am 15. Mai 2023. Geplant ist, die Router an durchschnittlich zwei Standorten pro Woche aufzubauen und die dort angebundenen Dienste zu migrieren. Damit sollten voraussichtlich kurz vor Weihnachten 2023 alle alten Systeme leergezogen und abgebaut sein. Dieser Austausch der Aggregations-Plattform stellt die erste Etappe zur Modernisierung der Router-Systeme im X-WiN dar, die mit Evaluierung, Beschaffung und Roll-out der neuen SuperCore-Router fortgesetzt wird. ◆

Neues vom Teilnehmerportal

Vor zwei Jahren startete das Teilnehmerportal des DFN-Vereins in den Pilotbetrieb. Seit Aufnahme des Produktivbetriebs im November 2021 wurde das Portal erheblich weiterentwickelt und stellt für die DFN-Teilnehmer einen deutlichen Nutzwert dar.

Zusätzlich zur Anzeige von Daten und Informationen zum Kommunikationsdienst DFNInternet bietet das Teilnehmerportal diverse Möglichkeiten zur Interaktion. So können die mittlerweile rund 300 Nutzenden die Kontaktinformationen der Ansprechpersonen ihrer Einrichtung ändern. Außerdem kann eine Referenz übermittelt werden, mit der sich Rechnungen besser zuordnen lassen.

Der Funktionsumfang des Antragsservice im Teilnehmerportal wächst ebenfalls stetig. Neben den bekannten Dienstvereinbarungen für DFNInternet-Dienste können externe DFN-Cloud-Dienste oder IP-Adressen einfach und direkt beantragt werden. Die Aufnahme von Dienstvereinbarungen weiterer DFN-Dienste ist in Planung.

Auch zu betrieblichen Themen bietet das Teilnehmerportal weitere Neuerungen. So können sich Teilnehmer über abgeschlossene und angekündigte Wartungen, die den jeweiligen DFNInternet-Dienst betreffen, informieren und eigene Wartungen ankündigen. Einen weiteren Mehrwert bietet die Möglichkeit, sich die aktuelle und historische Auslastung der eigenen Zugangsverbindungen und DFNInternet-Dienste anzeigen zu lassen.

Das Teilnehmerportal bietet darüber hinaus die Funktion, mit dem DFN-Netzüberwacher in Verbindung zu treten. Störungstickets werden angezeigt und können kommentiert werden. Zudem lassen sich neue Tickets schnell und komfortabel über das Teilnehmerportal eröffnen und nachverfolgen. ◆

Das DFN-Teilnehmerportal finden Sie unter:
https://teilnehmerportal.dfn.de
Haben Sie Fragen? Dann melden Sie sich gerne per E-Mail unter:
teilnehmerportal@dfn.de

Neuer Meilenstein: DFNTerminplaner knackt 1-Million-Marke

Kaum zu stoppen – die neueste Version des DFNTerminplaners hat bei den gleichzeitig abgegebenen Stimmen die 1-Million-Marke geknackt. Wir freuen uns über den großen Zuspruch und entwickeln den DFN-Dienst stetig weiter.

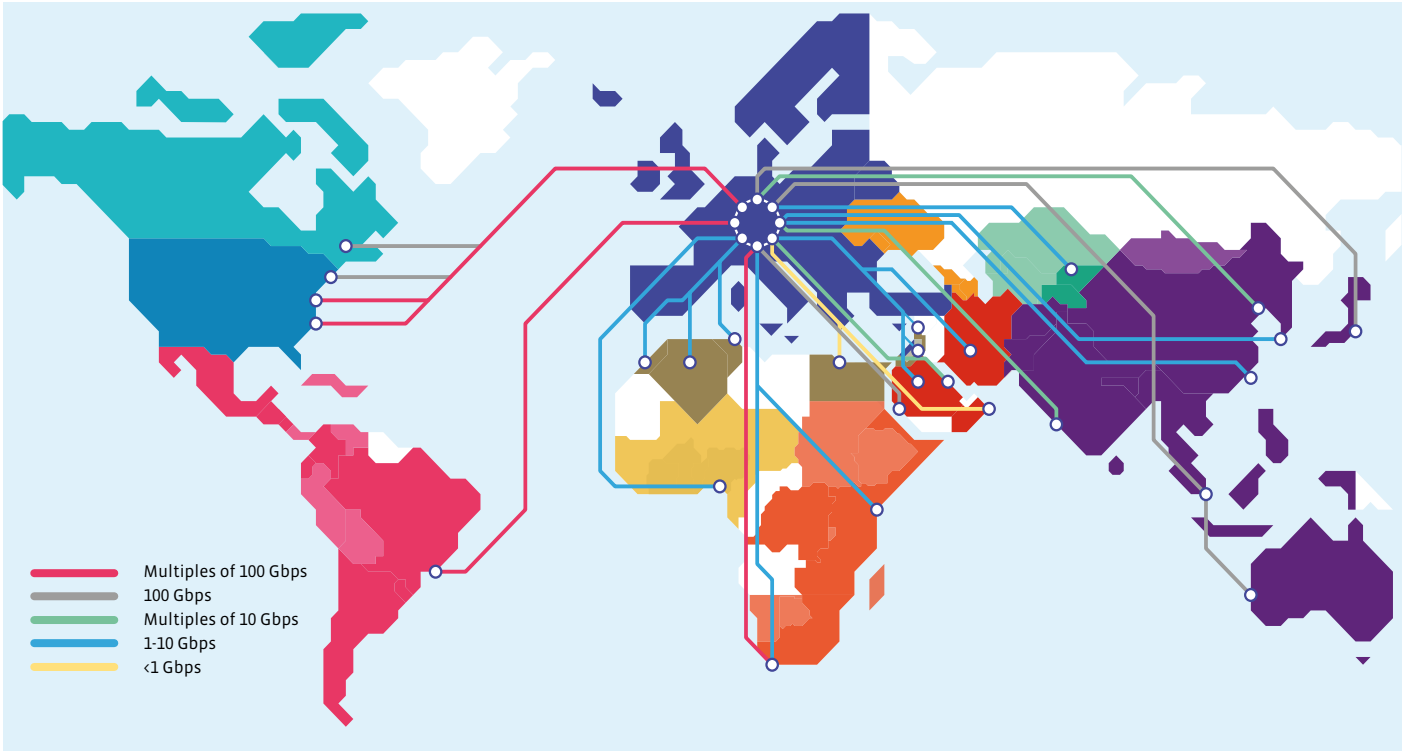
Mit dem aktuellen Release können Termine, Veranstaltungen und Umfragen im Arbeitsalltag schnell und unkompliziert organisiert werden. Feste Termine wie Seminarplätze oder Raumreservierungen lassen sich mit dem Erstellen von Buchungslisten noch bequemer koordinieren. Aktuell werden monatlich knapp 45 000 Abstimmungen neu erstellt und etwa 180 000 E-Mails vom System versendet. ◆

Den DFNTerminplaner finden Sie unter:
https://terminplaner6.dfn.de/

Fit für die Zukunft – Start der GN5-Projekte

Mit den beiden Projekten GN5-1 und GN5-IC1 unter dem EU-Programm Horizon Europe wurde im Januar 2023 die nächste Etappe der GN-Projektreihe eingeläutet. Seit mehr als 20 Jahren entwickeln und betreiben die europäischen nationalen Forschungsnetze unter dem Dach der GÉANT Association eine gemeinsame Backbone-Infrastruktur. Unbescheidenes Ziel: das beste Netz und die besten Dienste für Forschung und Lehre in Europa.

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



Die Konnektivität zu den europäischen und weltweiten Forschungsnetzen über das Verbindungsnetz GÉANT | *Quelle: GÉANT Association*

Nationale Forschungsnetze (National Research and Education Networks, NRENs), zu denen auch der DFN-Verein zählt, leisten mit ihren Diensten seit vielen Jahren einen wesentlichen Beitrag für die rasante Entwicklung von Forschung und Lehre. Die Europäische Union (EU) unterstützt die Zusammenarbeit nationaler Forschungsnetze in Europa, indem sie die GN-Projektreihe fördert. Im Jahr 2000 wurde diese mit dem Projekt GN1 initiiert, mehr als 20 Jahre später befinden wir uns heute mit GN5 in der fünften Auflage. Im Laufe der Jahre haben die Projekte viele Veränderungen durchlebt und sind längst nicht zur Selbstverständlichkeit geworden – jede Beantragung, jede Begutachtung und besonders die Verankerung in den Arbeitsprogrammen der EU sind

immer wieder eine neue Herausforderung. Seit 2014 wird die GN-Projektreihe von der GÉANT Association koordiniert, der Vereinigung aller europäischen nationalen Forschungsnetze.

Mit den beiden Projekten GN5-1 und GN5-IC1 fiel Anfang Januar 2023 der Startschuss für die erste Phase der Projektreihe GN5. Zum Auftakt trafen sich am 31. Januar und 1. Februar 2023 rund 74 Task-Leader, Workpackage-Leader und Koordinatoren in Dordrecht in den Niederlanden zur ersten Project Management Convention. Ziele des Treffens waren, den Rahmen für das zweijährige Projekt GN5-1 abzustecken, neue Kolleginnen und Kollegen einzubinden und ein gemeinsames Verständnis der Ziele und der Zusammenarbeit für die kommenden zwei Jahre zu entwickeln.

EU-Förderprogramm für Forschung und Innovation – Horizon Europe

Die GN5-Projektreihe wird von Horizon Europe, dem wichtigsten Förderprogramm der EU für Forschung und Innovation, finanziert. In Vorbereitung der Projektreihe wurde bereits im vergangenen Jahr zwischen der Europäischen Kommission und der GÉANT Association ein Rahmenvertrag (Framework Partnership Agreement, FPA) geschlossen, der die strategischen Ziele über den gesamten Zeitraum von Horizon Europe festlegt und die Rolle der GÉANT Association und ihrer Mitgliedern definiert. Der Rahmenvertrag wird oft als „empty envelope“ bezeichnet, denn er bereitet lediglich den Weg, damit in den Arbeitsprogrammen von Horizon Europe formelle Ausschreibungen für die einzelnen Phasen der GN5-Projektreihe veröffentlicht werden können. Der Rahmenvertrag legt jedoch weder die Dauer noch das Fördervolumen der einzelnen Projektphasen fest. Die Kernziele fasst der Rahmenvertrag in sechs Aktionsbereichen zusammen.

GN5-1 und GN5-IC1 im Überblick

Wesentliche Ziele von GN5-1 und GN5-IC1 sind die Weiterentwicklung und der Betrieb eines leistungsfähigen, sicheren und kosteneffizienten Verbindungsnetzes zwischen den europäischen nationalen Forschungsnetzen sowie deren globale Anbindung. Diese bereits bestehende Netzinfrastruktur muss an die stetig steigenden Bedarfe an Übertragungskapazität und Verfügbarkeit angepasst werden – mit schnellen Verbindungen bis in den Terabit-Bereich.

37 Partners (including GÉANT Association)

2 Associated Partners (SWITCH, Jisc)

43 Countries

Weitere Schwerpunkte in GN5-1 sind die Erprobung und Organisation von innovativen Diensten. Hier nimmt die seit Jahren etablierte Infrastruktur für Identitäts- und Zugriffsmanagement eine herausragende Rolle ein. Als vertrauenswürdiger Zugang zu den gemeinsamen Datenräumen in Forschung und Lehre ist sie unerlässlich, gleichzeitig muss sie fortwährend auf wechselnde Rahmenbedingungen und Anforderungen reagieren.

Das Projekt GN5-1 besteht aus neun Workpackages mit insgesamt 42 Task-Areas.

GN5-1
Start: 1. Januar 2023
Dauer: 24 Monate
Gesamtbudget: 82 Millionen Euro
(Fördersumme 55 Millionen Euro)

DIE SECHS KERNZIELE DES RAHMENVERTRAGS ZWISCHEN DER EUROPÄISCHEN KOMMISSION UND DER GÉANT ASSOCIATION:

- **Action A:** Understand and respond to the requirements of R&E communities.
- **Action B:** Evolve the Communication Commons towards data-driven research and education.
- **Action C:** Deliver state-of-the-art network connectivity and operational excellence.
- **Action D:** Deliver interoperable and distributed trust and identity infrastructure, security and above-the-net services, and procurement.
- **Action E:** Ensure innovation of key infrastructures and service development as an indispensable part of the GÉANT partnership.
- **Action F:** Strengthen the collaborative ecosystem of GÉANT and the NRENs, and develop the human capital of the GÉANT partnership.

DIE NEUN WORKPACKAGES IM PROJEKT GN5-1

Das Projekt GN5-IC1 ist für drei Jahre angesetzt und durch das Kürzel IC für Intercontinental Connectivity ist dessen Schwerpunkt bereits über den Namen definiert. Im Rahmen des Projektes soll die globale Reichweite des europäischen Verbindungsnetzes verbessert werden, indem Lücken in der Konnektivität geschlossen und bestehende interkontinentale Verbindungen aktualisiert werden. Motivation sind die enormen Datenmengen, die in der Wissenschaft erzeugt, weltweit verteilt und künftig noch stark zunehmen werden.

Eine besondere Herausforderung in diesem Projekt ist das aktuelle Spannungsfeld, in dem es sich bewegt. Einerseits liegt das an der zunehmenden Bedeutung der digitalen Souveränität Europas, die unter anderem mit der von der EU im März 2021 veröffentlichten European Data Gateways Declaration ihren Ausdruck gefunden hat. In der Erklärung wird die Bedeutung der sicheren globalen Netzanbindung Europas betont, wobei auf die Rolle von GÉANT und das erfolgreiche Projekt BELLA zur Verbindung mit Lateinamerika ausdrücklich hingewiesen wird.

Andererseits adressiert das Projekt Ansätze zur besseren Vernetzung globaler Zusammenarbeit in Forschung und Lehre, welche sich nur in enger Abstimmung mit Staaten außerhalb Europas sinnvoll entwickeln lassen. Daher gehört es auch zu den Aufgaben des Projektes, geplante internationale Forschungsvorhaben frühzeitig zu identifizieren und den zukünftigen Bedarf an interkontinentaler Konnektivität zu ermitteln. Darauf aufbauend sollen eine langfristige, international abgestimmte Kapazitätsplanung sowie die dafür notwendigen Investitionen und potenzielle Förderinstrumente vorgeschlagen werden.

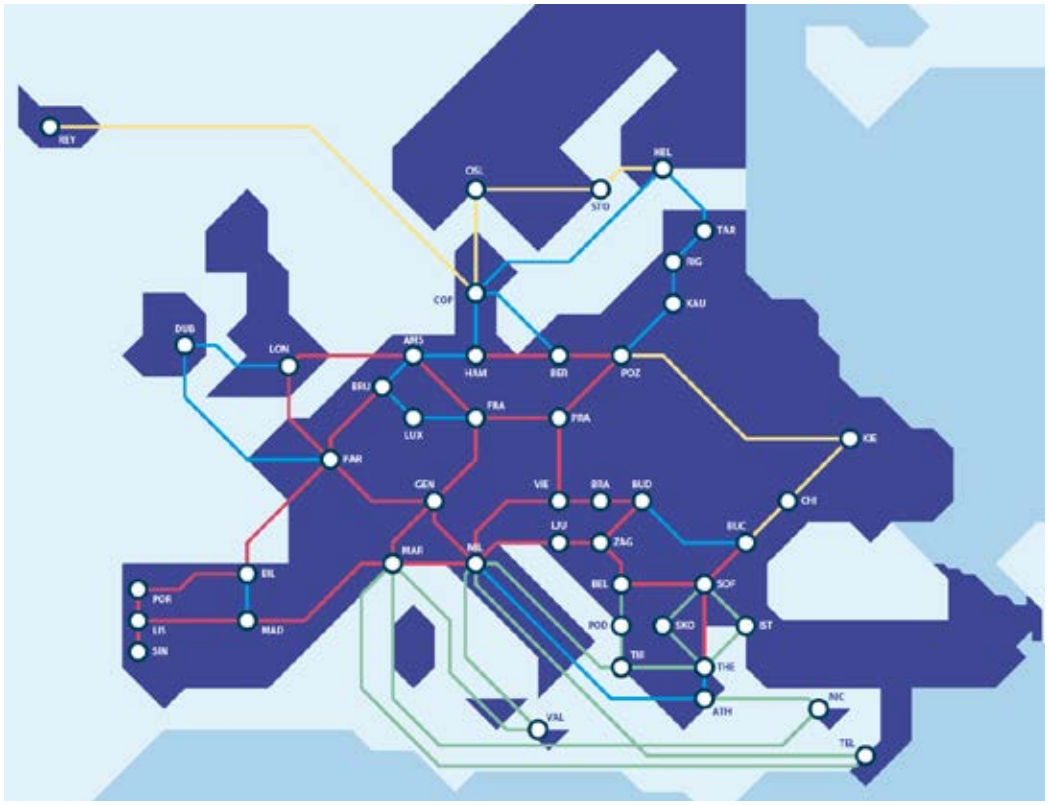
GN5-IC1
Start: 1. Dezember 2022
Dauer: 36 Monate
Gesamtbudget: 18 Millionen Euro
(Fördersumme 15 Millionen Euro)

GÉANT: Ergebnis jahrzehntelanger europäischer Zusammenarbeit

Die GN-Projektreihe hat ein bewegtes Leben hinter sich, in dem es zu einigen Änderungen in der Gestaltung und Ausführung kam. Aus dem 5. Rahmenprogramm der EU wurde von November 2000 bis Oktober 2004 das Projekt GN1 gefördert. Kern des Projektes war die Konsolidierung und Aufrüstung des bestehenden Verbindungsnetzes zwischen den europäischen Forschungsnetzen. Dieses erhielt den Namen „GÉANT – Gigabit European Advanced Network Technology" – wobei der Accent aigu über dem É eine Anlehnung an das französische GÉANT für Gigant war, zur Betonung einer seinerzeit schier unvorstellbar hohen Übertragungskapazität. Das Projekt wurde von der Delivery of Advanced Network Technology to Europe (DANTE) Limited koordiniert, einer 1993 in Cambridge gegründeten Gesellschaft, an der neben dem DFN-Verein 14 weitere europäische Forschungsnetze Anteile hielten.

Dank des großen Erfolges wurde die Projektreihe im 6. und 7. EU-Rahmenprogramm fortgesetzt, entsprechend unter den Kürzeln GN2 und GN3 – bereits in GN3 kam es zu einer zweiten Projektphase GN3plus. Mit GN4 unter dem 8. Rahmenprogramm sollten sich gleich mehrere Änderungen ab 2015 ergeben: Die Koordinierung übernahm die GÉANT Association, welche durch Zusammenschluss von DANTE Limited und der Trans-European Research and Education Networking Association (TERENA) entstanden war. Motivation für den Zusammenschluss war die Organisationsform von DANTE Limited, der nicht alle europäischen Forschungsnetze beitreten konnten – diese waren rein formal stimmlose Beobachter in DANTE Limited und auf „goodwill" der 15 Gesellschafter angewiesen. Demgegenüber war TERENA als Vereinigung aller europäischen Forschungsnetze zwar gut aufgestellt, hatte jedoch seitens der Europäischen Union nicht das Vertrauen als mögliche Koordinatorin eines Großprojektes. Dieses Vertrauen hatte sich DANTE Limited über Jahre hart erarbeitet. In einem mehrjährigen Einigungsprozess, durchaus im Einvernehmen mit der Europäischen Kommission, wurde Ende 2014 der Zusammenschluss vollzogen.

Für GN4 wurde zuerst ein Framework Partnership Agreement (FPA) zwischen Europäischer Kommission und der GÉANT Association geschlossen, welches die Ausschreibung einzelner Projektphasen (Specific Grant Agreements, SGAs) über die Arbeitsprogramme unter Horizon 2020 vorbereitete. Im Ergebnis



Fibre
Spectrum
Connected Regional Network
Leased Capacity

* Die Konnektivität dieser Länder wird vom nordischen Regionalnetz NORDUnet organisiert.

** Die Konnektivität dieser Länder wird über das EU-Projekt EaPConnect2 organisiert.

Infrastruktur des europäischen Backbone-Netzes GÉANT, January 2023 | *Quelle: GÉANT Association*

Das europäische Backbone-Netz GÉANT verbindet die Forschungsnetze folgender Länder miteinander:

Albania	Croatia	France	Ireland	F.Y.R Macedonia	Poland	Spain
Armenia**	Cyprus	Georgia**	Israel	Malta	Portugal	Sweden
Austria	Czech Republic	Germany	Italy	Moldova**	Romania	Switzerland
Azerbaijan**	Denmark*	Greece	Latvia	Montenegro	Serbia	Turkey
Belgium	Estonia	Hungary	Lithuania	Netherlands	Slovenia	Ukraine**
Bulgaria	Finland*	Iceland*	Luxembourg	Norway	Slovakia	United Kingdom

kam es zu drei aufeinander folgenden Projektphasen GN4-1, GN4-2 und GN4-3, wobei die letzte noch durch das separate Projekt GN4-3N zum Ausbau des GÉANT-Backbone ergänzt wurde. Die Projektreihe GN4 endete zum Dezember 2022. Der Ansatz, über ein FPA mehrere aufeinanderfolgende SGAs vorzubereiten, wurde für die Projektreihe GN5 in das 9. Rahmenprogramm übernommen.

Dem dynamischen Werdegang einer mittlerweile über 20 Jahre andauernden Projektreihe steht die hohe Kontinuität gegenüber, mit der die Europäische Union diese Entwicklung unterstützt hat. Es ist schwer vorstellbar, wie die Landschaft europäischer Forschungsnetze ohne diese Unterstützung heute aussehen würde. So wurde in Gesprächen mit hohen Vertreterinnen und Vertretern des Europäischen Parlaments lobend anerkannt, dass es sich bei den GN-Projekten „wohl mit um die europäischsten handelt, die je von der EU gefördert wurden“.

Ist die Fortführung über das aktuelle Rahmenprogramm hinaus damit bereits gesichert? Sicherlich nicht. Alle Seiten eint das Interesse an einem nachhaltigen Fortbestand der GN-Reihe. Unverkennbar sind jedoch die sich abzeichnenden Änderungen an den Rahmenbedingungen zukünftiger EU-Förderung. Die Diskussionen darüber haben bereits begonnen, wichtige Weichenstellungen finden in den kommenden zwei bis drei Jahren – und keinesfalls später – statt. Die große Herausforderung, die GÉANT Association mit ihren Mitgliedern wie dem DFN-Verein fit für die Zeit ab 2028 zu machen, liegt also unmittelbar vor uns.

Christian Grimm war von 2015 bis 2020 Vorstandsvorsitzender der GÉANT Association.

Weitere Informationen zur GN-Projektreihe finden Sie unter: **https://geant.org/projects/**

Vereinte Kompetenzen – der Beitrag des DFN-Vereins zu GN5-1

Koordiniert von der GÉANT Association arbeiten alle europäischen Forschungsnetze in dem Projekt GN5-1 zusammen. Der DFN-Verein ist in sämtlichen neun Workpackages des Projekts vertreten: Aktivitäten zur Steuerung und strategischen Begleitung des Projektes sowie mit hohem Bezug zu DFN-Diensten werden direkt von der Geschäftsstelle ausgeführt, in eher technologie- oder entwicklungsorientierte Tätigkeiten werden gezielt Mitglieds- und Teilnehmerinstitutionen als Unterauftragnehmer einbezogen.

Im Einzelnen sind dies: Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ), Karlsruher Institut für Technologie (KIT) und DFN-CERT Services GmbH (DFN-CERT).

Die Geschäftsstelle des DFN-Vereins übernimmt Aufgaben in folgenden Workpackages:

WP1 – Project Management – umfasst unter anderem die übergeordnete Projektsteuerung einschließlich Governance und Finanzen sowie globale Partnerschaften. Die Geschäftsstelle stellt hierbei auch den Vorsitz des projektinternen Komitees, dem die Qualitätskontrolle aller Projektergebnisse (Deliverables) obliegt.

Die Workpackages WP2 – Marcomms, Events and Policy Engagement – und WP3 – User and Stakeholder Engagement – bedienen die Schnittstellen zwischen der GÉANT Association, den europäischen Forschungsnetzen und der EU untereinander sowie nach außen insbesondere zu Forschungsnetzen auf anderen Kontinenten und relevanten, internationalen Forschungsvorhaben. Die Geschäftsstelle ist in beiden Workpackages mit den Themenfeldern EU Liaison, e-Infrastructure und International Relations befasst.

In WP4 – Above-the-Net Services – ist die Geschäftsstelle mit der Co-Leitung des gesamten Workpackages betraut. Ziel des Workpackages ist es, ein Multi-Cloud-Serviceportfolio aus einer Kombination von kommerziellen Angeboten und communitybasierten Diensten aufzubauen. Schwerpunkte sind die Neuausschreibung der europäischen Cloud-Rahmenverträge sowie die Ausgliederung der Videokonferenz-Software eduMEET in ein unabhängiges Open-Source-Projekt.

Letztes Tätigkeitsfeld ist das WP5 – Trust & Identity Services Evolution and Delivery. Neben dem Betrieb und der Weiterentwicklung wichtiger Komponenten für eduroam engagiert sich die Geschäftsstelle auch für den Dienst eduGAIN, welcher Basis für die globale Föderation von Vertrauensdiensten wie der DFN-AAI ist. Im Hinblick auf sich abzeichnende Entwicklungen im Kontext von EOSC und NFDI ist eine enge Begleitung von besonderem Interesse für den DFN-Verein. ◆

FRIEDRICH-ALEXANDER-UNIVERSITÄT ERLANGEN-NÜRNBERG (FAU)

Workpackages

WP6 – Network Development
Task 1: Technology (Task Lead)
Task 3: Monitoring

WP7 – Network Core Infrastructure, Core Service Evolution, and Operations
Task 2: Network Infrastructure & Services Evolution

WP9 – Operations Support
Task 1: Operations Centre including CERT
Task 2: Software Governance and Support

Schwerpunkte
Für die Anwendungsbereiche „Time & Frequency“ (T&F) und Quantenkommunikation (QuC) untersucht die FAU die Umsetzung der technischen Anforderungen an Datennetze. Im Bereich Netzwerkentwicklung beschäftigt sie sich mit der Weiterentwicklung der Open Source Router Plattform RARE (Router for Academia, Research and Education) sowie mit der Optimierung des Toolkits perfSONAR zur Netzmessung.

KARLSRUHER INSTITUT FÜR TECHNOLOGIE (KIT)

Workpackage

WP5 – Trust & Identity Services Evolution and Delivery
Task 5: T&I Incubator
Task 6: T&I Enabling Communities

Schwerpunkte
Das KIT befasst sich im Projekt mit der Weiterentwicklung der AARC Blueprint Architecture: Hierbei geht es um die Vernetzung im Kontext der European Open Science Cloud (EOSC) und den zuverlässigen Austausch von Identitäten. Darüber hinaus ist das KIT am Aufbau einer OpenID Connect-basierten Föderation beteiligt.

DFN-CERT SERVICES GMBH (DFN-CERT)

Workpackages

WP5 – Trust & Identity Services Evolution and Delivery
Task 1: Operations and Enhancement of eduroam
Task 2: Operations and Enhancement of eduGAIN

WP8 – Security
Task 2: Human Factor
Task 3: Security Products and Services (Task Lead)

Schwerpunkte
Neben der Entwicklung der eduPKI und Unterstützung im Datenschutz ist das DFN-CERT für Design, Organisation und Durchführung von Sicherheitsschulungen wie Blue Team Trainings zuständig. Im Bereich der Security Products and Services wird zusätzlich zur Weiterentwicklung der DDoS-Tools die Integration der verschiedenen Sicherheitstools aus den Bereichen SOC, DDoS, Cyber Threat Intelligence und Vulnerability Assessment koordiniert.

LEIBNIZ-RECHENZENTRUM DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN (LRZ)

Workpackages

WP5 – Trust & Identity Services Evolution and Delivery
Task 2: Operations and Enhancement of eduGAIN (Task Lead)
Task 5: T&I Incubator
Task 6: T&I Enabling Communities

WP6 Network Development
Task 2: Platform

WP8 – Security
Task 1: Security Management
Task 3: Security Products and Services

WP9 – Operations Support
Task 2: Software Governance and Support

Schwerpunkte
Das LRZ ist unter anderem am Trust & Identity Incubator beteiligt, einem Innovationshub für die Entwicklung von Ideen und Projekten. Im Trust & Identity Mentorship (TIM) setzt sich das LRZ dafür ein, junge Talente für die Arbeit im Bereich Research & Education sowie T&I zu begeistern. Im Bereich der Software Governance widmet sich das LRZ der Optimierung und Weiterentwicklung der Code Review Services, im Bereich DDoS-Mitigation werden neue Use Cases entwickelt.

Europa wächst zusammen

Fotos: Christoph Schieder

Als Verantwortliche in internationalen Projekten beim DFN-Verein engagieren sich Dr. Leonie Schäfer und Dr. Jakob Tendel gemeinsam mit ihren Kolleginnen und Kollegen aus anderen europäischen Forschungsnetzen seit vielen Jahren in den Projekten der GN-Reihe. Zum Start von GN5-1 erzählen sie, welche Herausforderungen es zu meistern gilt und wie die Zusammenarbeit in solch einem ambitionierten Großprojekt gelingt.

Seit mehr als 20 Jahren sorgen die nationalen Forschungsnetze (NRENs) mithilfe der von der EU geförderten GN-Projekte für die kontinuierliche Entwicklung des europäischen Backbone-Netzes. Welche Bedeutung hat das für die DFN-Teilnehmer in Deutschland?

Leonie: Die GÉANT-Projekte gewährleisten den Betrieb und Ausbau des europäischen Forschungsnetzes nach aktuellen Anforderungen und in bestmöglicher Qualität. Auch die gemeinsame Entwicklungsarbeit von Diensten wird gefördert und hat viele Synergieeffekte sowohl auf europäischer als

auch auf globaler Ebene. Davon profitieren wiederum die Teilnehmer der NRENs. eduroam und eduGAIN sind die besten Beispiele.

Jakob: Einen beträchtlichen Wert haben die Projekte für die internationale Konnektivität unserer Teilnehmer am Wissenschaftsnetz X-WiN. Um die zunehmenden Datenmengen in Forschung und Lehre verarbeiten zu können, braucht es leistungsfähige Dateninfrastrukturen und Diensteportfolios. Weltweite Kooperationen in großen Forschungskonsortien wären sonst nicht möglich. Europa gehört zu den größten Erzeugern von Forschungsdaten, die aus aller Welt angefragt werden. Für den Forschungsstandort Europa sind die GN-Projekte ein unheimlicher Enabler.

Mit GN5-1 startet eine neue Projektfamilie mit einem neuen Rahmenvertrag unter Horizon Europe. Was ändert sich inhaltlich zum Vorgängerprojekt?

Leonie: Stichwort „Next Generation Network“: In den Vorgängerprojekten GN4-3 und GN4-3N stand der strategische Netzausbau im Fokus. Das europäische Backbone-Netz wurde rundum modernisiert und die Konnektivität zwischen den NRENs verstärkt – insbesondere dort, wo es noch Engpässe oder keine redundanten Verbindungen gab, wie beispielsweise auf Malta und Zypern.

> „Cybersecurity ist national wie international ein absoluter „Hot Topic“!“

Im neuen Projekt GN5-1 liegt der Schwerpunkt auf IT-Sicherheit und Trust & Identity. Cybersecurity ist national wie international ein absoluter „Hot Topic“, der auch aktuell stark beeinflusst wird durch politische Geschehnisse wie den Ukraine-Krieg. Cybersecurity wurde erst im vergangenen Projekt GN4-3 als eigenes Workpackage definiert und ist inzwischen in der Planung fest verankert.

Jakob: Auch das Thema Cloud-Beschaffung bekommt sehr viel Aufmerksamkeit von der EU-Kommission und wird in der europäischen Community stark nachgefragt – nicht zuletzt durch das Projekt OCRE (Open Clouds for Research Environments), das im Dezember beendet wurde. Cloud ist überhaupt ein Buzzword und tatsächlich so etwas wie ein Politikum. Gefühlt ist heute jedes zweite Projekt aufgefordert, seinen Bezug zur European Open Science Cloud (EOSC) irgendwie nachweisen. Als zentrale Initiative führt sie unterschiedlichste Aktivitäten rund um digitale Services zusammen.

Jakob, gemeinsam mit Deiner estnischen Kollegin Maria Ristkok bist Du Workpackage-Leader im Arbeitspaket 4 „Above-the-Net Services“. Was sind Eure Schwerpunkte?

Jakob: Einer davon ist die Neuausschreibung der Cloud-Rahmenverträge aus dem OCRE-Projekt – damals ein separates Projekt und nun Bestandteil unseres Arbeitspakets. Aktuell sind wir gerade dabei, das alte OCRE-Team in das GÉANT-Team einzugliedern und die Ausschreibung vorzubereiten. Im Tagesgeschäft managen wir außerdem die aktuell geltenden Cloud-Rahmenverträge, die der Community seit 2020 aus OCRE zur Verfügung stehen.

Was außerdem neu ist: Im Vorgängerprojekt wurde eine eigene Videokonferenz-Softwarelösung entwickelt: eduMEET ist vollständig quelloffen und Open-Source-lizenziert und integriert sich gut in das Dienste-Ökosystem der Forschungsnetze, wie das AAI Identity Management. Die Software ist bei einer ganzen Reihe von NRENs im Einsatz. Mittlerweile hat eduMEET eine ordentliche Reife erlangt, die weitere Entwicklung wird deshalb nicht mehr im Projekt finanziert. Das schafft Ressourcen für Innovationen. Unsere Aufgabe ist es, eduMEET als tragfähiges, unabhängiges Open-Source-Projekt auszugliedern, das von der Community weiter gesteuert werden kann.

Während Jakob operativ im Projekt tätig ist, hast Du eine ganz andere Rolle bei der Entstehung und Gestaltung von GN5, Leonie.

Leonie: Als Mitglied im GÉANT Project Planning Committee (GPPC) bin ich für die strategische Planung des Projekts verantwortlich. Bislang war das Planungskomitee eher technisch orientiert. Mein Ehrgeiz ist es, andere Aspekte in die Diskussion mit einzubringen, zum Beispiel Trend- und Zukunftsforschung, EU-Innovationspolitik und Geopolitik. Mir liegt strategisches Denken. Darum habe ich kandidiert und wurde bei der GÉANT-Mitgliederversammlung im Frühjahr 2019 in das Komitee gewählt. Die Arbeit im GPPC ist eine sehr spannende, aber auch herausfordernde Arbeit.

Wie wird solch ein großes Projekt geplant und welchen Vorlauf hat es?

Leonie: Die Planungen zu GN5-1 begannen bereits im Sommer 2021 mit einer Konzeptionsphase. Die Struktur von GN5-1 wurde in Anlehnung an GN4-3 entwickelt. Zunächst haben wir uns das aktuelle Projekt angeschaut: Was funktioniert gut, was funktioniert weniger? Unser Resümee war: Die Struktur hat sich bewährt. Darum haben wir diese mit ein paar kleinen Änderungen und ein bisschen Feintuning für GN5-1 adaptiert.

Der nächste Schritt bestand darin, eine Roadmap zu erarbeiten. Dazu wurden mit Expertinnen und Experten aus allen

Leonie Schäfer koordiniert die Beteiligung des DFN-Vereins an internationalen Projekten wie GN5-1. In der GÉANT Association vertritt sie den DFN-Verein als stellvertretende Delegierte und übernimmt im Rahmen der GÉANT-Projekte verschiedene Aufgaben im Bereich EU Liaison, International Relations und Stakeholder Management. Die promovierte Informatikerin forschte mehrere Jahre intensiv an den Themen Computer Supported Collaborative Work, Virtual Reality und Digital Storytelling. Bei der EU-Kommission beschäftigte sie sich als Project Officer unter anderem mit den Schwerpunkten Innovationspolitik und neue Forschungstrends im MINT-Bereich.

NRENs aufwendige Interviews geführt, um die Anforderungen und Inhalte für die verschiedenen Workpackages zu erarbeiten. In verschiedenen Workshops unter Beteiligung aller Mitglieder von GÉANT wurden die Themen anschließend weiter spezifiziert. Dieser Prozess zog sich über anderthalb Jahre hin. Die Herausforderung besteht im Wesentlichen darin, die Ambitionen mit den zur Verfügung stehenden Ressourcen in Einklang zu bringen.

Musstet Ihr Euch Gedanken machen, was die Finanzierung betrifft?

Jakob: Lange Zeit war gar nicht klar, welches Budget wir in den einzelnen Workpackages konkret bekommen, weil ein erheblicher Teil der bereitgestellten Mittel in Hardwarebeschaffung für neue Netzwerkkomponenten des GÉANT-Backbone fließt. Als das geklärt war, gingen die Debatten untereinander los. Wer braucht welches Budget, um seine Arbeit ordentlich erledigen zu können. Dazu kamen weitere Vorgaben aus der Führungsebene. Und so wurde so lange umverteilt, bis die Workpackages standen. Dabei wurden einige Pläne und Hoffnungen ziemlich zurechtgestutzt.

Leonie: Der Rahmenvertrag (Framework Partnership Agreement, FPA) zwischen der Europäischen Kommission, der GÉANT Association und deren Mitgliedern legt die strategischen Inhalte der Partnerschaft für die kommenden sieben Jahre fest. Wie viel Budget für die einzelnen Projektphasen GN5-1, GN5-2 und GN5-3 zur Verfügung steht, hängt unter anderem davon ab, welche Beschaffungen noch benötigt werden. Die Entscheidung für GN5-1 war, die Investitionen in Hardware gleich am Anfang zu tätigen. Dadurch schrumpft das operative Budget selbstverständlich. Natürlich ist es schade, wenn deswegen Ideen nicht umgesetzt werden können. Ich fand den Ansatz auch etwas schwierig, erst viele Ideen einzufordern und dann wieder ad acta zu legen.

Eine Konsequenz aus der Finanzdiskussion ist nun, dass die Projektphase GN5-1 nur zwei Jahre beträgt. Schon jetzt gehen die Diskussionen los, welche Laufzeit GN5-2 haben soll – ob zwei oder drei Jahre. Die Entscheidung, wie lange die jeweiligen Projektabschnitte dauern, ist Gegenstand der Verhandlungen mit der EU-Kommission.

Ihr habt eben die Diskussionen im Vorfeld der Mittelverteilung angesprochen: 39 Partner, verschiedene Länder, unterschiedliche Kulturen. Wie schwierig ist es, auf einen Nenner zu kommen?

Leonie: Die Diskussionen verlaufen im Allgemeinen sehr zivilisiert. Die nationalen Interessen spielen natürlich eine Rolle. Das italienische NREN GARR verfolgt möglicherweise andere Interessen als beispielsweise NORDUnet, der Verbund der skandinavischen NRENs. Da behakeln sich NRENs vielleicht mal, aber die Diskussionen sind stets inhaltlich orientiert und sachbezogen. Die bewährte Projektstruktur hilft bei der Zusammenarbeit der verschiedenen Partner ungemein.

> Jedes NREN ist anders. Es gibt sehr unterschiedliche nationale Rahmenbedingungen.

Jakob: Jedes NREN ist anders. Es gibt sehr unterschiedliche nationale Rahmenbedingungen. Einige sind staatlich und Teil eines Ministeriums. Andere organisieren sich unabhängig vom Staat, so wie wir. Manche erhalten eine große nationale Förderung für bestimmte Technologiethemen, die sie dann oft auch auf GÉANT-Ebene ins Spiel bringen wollen. Andere NRENs wiederum

interessiert dieses Thema möglicherweise weniger. Um dieses Spannungsverhältnis auszutarieren und sicherzustellen, dass keiner zu kurz kommt, wird sehr viel Aufwand betrieben. Bisher funktioniert das jedoch sehr gut.

Wie ordnet sich der DFN-Verein hier ein?

Leonie: Der DFN ist ein wichtiges Mitglied in der GÉANT Association – allein durch unsere Größe, aber auch durch die Bedeutung Deutschlands als wichtiger Standort in der Forschung. So haben wir den größten Datenaustausch aller europäischen NRENs in das GÉANT-Netz. Wir sind jedoch eine vergleichsweise schlanke Organisation. Trotzdem ist der DFN mit seinen Drittmittelpartnern in allen Workpackages sehr präsent – besonders bei den Themen Security und Trust & Identity leisten wir einen deutlich sichtbaren Beitrag. Beispielsweise wurde das vom DFN-CERT entwickelte Tool für Netflow-basierte DDoS-Erkennung und -Analyse NEMO im Projekt aufgegriffen und für eine Anwendung innerhalb des GÉANT-Netzes angepasst.

Gibt es besondere Herausforderungen im Projekt?

Jakob: Eines der größten Probleme für alle NRENs ist der aktuelle Fachkräftemangel. Hoch qualifizierte Leute zu bekommen bzw. zu halten ist sehr schwer. Wenn diese wenigen Fachkräfte dann auch noch für das Projekt abgestellt werden, fehlen sie wiederum auf nationaler Ebene.

> „Eines der größten Probleme für alle NRENs ist der aktuelle Fachkräftemangel."

Bei der Planung unseres Workpackages war das eine echte Herausforderung: Wir mussten genau überlegen, welche Rollen und Kompetenzen wir benötigen. Nicht alle ausgeschriebenen Stellen im Projekt konnten wir bisher besetzen. Das im Vorfeld vereinbarte Arbeitsstundenkontingent mit weniger Leuten zu leisten, ist eine Herausforderung. Das bereitet uns Workpackage-Leadern schon manchmal Kopfschmerzen.

Gibt es gezielte Maßnahmen, um dem Fachkräftemangel zu begegnen?

Leonie: Eine Maßnahme ist Weiterbildung. Im Arbeitspaket 1, Project Management, gibt es den Task Human Capital Development. Der Task hat das Ziel, Mitarbeitende im Projekt weiter zu qualifizieren und das Wissen auch in der Community weiterzugeben. Das wird von der EU-Kommission explizit gefordert. Von Managementkursen bis Technical Trainings ist alles dabei. Im großen Themenbereich Sicherheit bietet zum Beispiel das DFN-CERT viele praxisbezogene Workshops wie das Blue Team Training an.

Welche Kompetenzen und Soft Skills benötigt Ihr für Eure Arbeit im Projekt?

Jakob: Dazu gehört Fachwissen rund um Service-Management, Kommunikation und Vergaberecht. Da ist mein Arbeitspaket etwas untypisch im Vergleich zu den anderen, die meist sehr technologielastig sind. Sich gut strukturieren zu können, ist auch kein Nachteil: Wegen der räumlich

Von Natur aus international: Die gegenüber der DFN-Geschäftsstelle direkt am Alexanderplatz installierte berühmte Weltzeituhr zeigt alle Zeitzonen der Welt an | *Fotos: Christoph Schieder*

Jakob Tendel sorgt im DFN-Verein für die Verbindung zwischen internationalen Projekten und Cloud-Diensten. Der promovierte Meteorologe leitet aktuell das Arbeitspaket WP4 „Above-the-Net Services“ im Projekt GN5-1, das sich mit endanwendernahen digitalen Diensten und der Neuausschreibung der europaweiten Cloud-Rahmenverträge aus dem im vergangenen Jahr beendeten Projekt Open Clouds for Research Environments (OCRE) befasst.

verteilten Teams arbeiten wir überwiegend virtuell miteinander. Das verlangt sehr viel Koordination und strukturierte Formen der Zusammenarbeit. Wenn wir uns persönlich treffen, wie neulich in Amsterdam, arbeiten wir mindestens die Hälfte der Zeit an unserer persönlichen Vertrauensbeziehung, lernen uns besser kennen und haben natürlich auch viel Spaß. Das ist quasi der Treibstoff, der uns in der virtuellen Zeit erlaubt, vertrauensvoll zusammenzuarbeiten. Eine gewisse Offenheit für unterschiedliche kulturelle Hintergründe ist außerdem wichtig. Ich finde es toll, in soich einem multikulturellen Team zu arbeiten.

> „Um Fettnäpfchen zu vermeiden, ist es wichtig, politisch auf dem Laufenden zu sein.“

Leonie: Für meine Arbeit ist interkulturelle Kompetenz die wichtigste Eigenschaft. Das ist oft Learning by doing. Ich habe viel mit osteuropäischen Partnern zusammengearbeitet, die eine ganz andere Mentalität an den Tag legen als die mitteleuropäischen Kolleginnen und Kollegen. Die gemeinsame Vergangenheit als Teil der Sowjetunion spiegelt sich oft im Verhalten wider. Es brauchte eine lange Zeit der Vertrauensbildung, die aber durch eine gute Zusammenarbeit belohnt wird.

Um Fettnäpfchen zu vermeiden, ist es wichtig, bei schwierigen politischen Themen auf dem Laufenden zu sein. Abhängig vom jeweiligen Gesprächspartner sollte man beispielsweise seine Meinung zur Auseinandersetzung zwischen Armenien und Azerbaijan oder zur katalanischen Unabhängigkeitsbewegung nur mit Vorsicht äußern.

Jedes Land funktioniert anders. Um herauszufinden wie, muss man Zeit investieren und viel kommunizieren. Klar lästern wir untereinander auch über unsere kulturellen Unterschiede, aber immer mit einem Augenzwinkern.

Was macht die Arbeit im GÉANT-Projekt für Euch so spannend und lohnenswert?

Jakob: Ich finde es wichtig, dass sich die digitale Transformation auf der Basis gemeinsamer europäischer Werte vollzieht. Dazu gehören Souveränität und Offenheit aber auch informationelle Selbstbestimmung – ohne versteckte Ausbeutung oder Überwachung. Was mich am meisten motiviert, ist die Gewissheit, mich für etwas Gutes einzusetzen, was für die Wissenschaft in Europa einen Mehrwert hat. Ich bin stolz darauf, dass ich den DFN als Workpackage-Leader vertreten und so zum Erfolg dieses europäischen Großprojektes beitragen darf.

Leonie: Das Spannendste für mich ist die weltweite Zusammenarbeit mit anderen NRENs und Einrichtungen. Projekte über Kontinente hinweg voranzutreiben, finde ich extrem herausfordernd. Inhaltlich bin ich immer sehr nah an den aktuellsten Themen, seien es Quantum Computing oder die neuesten Entwicklungen im Bereich Cybersecurity. Hinzu kommt der Bereich Governance & Policy, den ich zunehmend interessanter finde. Mein Herz schlägt für Europa. Ich möchte meinen Beitrag dazu leisten, dass Europa weiter zusammenwächst.

Die Fragen stellte Maimona Id (DFN-Verein)

Kurzmeldungen

Gute Beziehungen: Besuch von WACREN-CEO Dr. Boubakar Barry

Auf Stippvisite: Am 14. Februar 2023 besuchte Dr. Boubakar Barry die Geschäftsstelle des DFN-Vereins. Der Chief Executive Officer (CEO) des regionalen Forschungsnetzes WACREN, West and Central African Research and Education Network, kennt den DFN-Verein seit vielen Jahren. Er freute sich, die DFN-Geschäftsstelle nach fast vier Jahren wieder zu besuchen. Bereits 2006 begann der studierte Kernphysiker und Netzwerkexperte damit, eine Kommunikationsinfrastruktur für West- und Zentralafrika zu entwickeln. Sein Ziel ist es, ein stabiles, sicheres Backbone mit Hochgeschwindigkeitsverbindungen – beispielsweise für Forschungsvorhaben wie das Radioteleskop-Projekt Square Kilometre Array (SKA) – zu schaffen.

Grund des Besuchs waren sowohl Gespräche zur Zusammenarbeit bezüglich Capacity Building im Projekt AfricaConnect3 als auch ein Status-Update zur Vorbereitung des Projekts AfricaConnect4. Gemeinsam mit WACREN erstellte der DFN ein Programm für die WACREN-CEO-Academy zur Weiterbildung von Führungskräften. Den Auftakt bildete 2021 ein mehrteiliges Webinar zum Thema „Business Models for NRENs“. 2022 fand das Webinar „eduroam in Practice“ statt. Weitere Webinare sind für 2023 geplant.

Ziel der AfricaConnect-Projekte ist es, die Entwicklung und den Betrieb leistungsfähiger nationaler und regionaler Kommunikationsnetze für Forschung und Lehre in den afrikanischen und arabischen Ländern zu unterstützen. Dazu gehört unter anderem, die Konnektivität durch den Anschluss an das europäische Forschungsnetz GÉANT zu verbessern und damit den weltweiten Wissenschaftsaustausch Afrikas zu fördern. AfricaConnect3 umfasst insgesamt drei geografische Cluster mit ihren jeweiligen regionalen Netzwerkorganisationen: ASREN in Nordafrika, UbuntuNet Alliance in Ost- und Südafrika und WACREN in West- und Zentralafrika. ◆

#love2eduroam: Neuer Rekord

„Vom zarten Pflänzchen zum Mammutbaum“ – so lautete vor fünf Jahren der Titel zum zehnjährigen Bestehen von eduroam in den DFN-Mitteilungen. Seitdem konnte der weltweite WLAN-Zugangsdienst, der für die internationale Forschungs- und Bildungsgemeinschaft entwickelt wurde, seine Nutzungszahlen rapide steigern – insbesondere im vergangenen Jahr, als die Reisebeschränkungen im Zuge des Pandemiegeschehens wieder gelockert wurden. So wurden auf der von GÉANT betriebenen Monitoring-Plattform 6,4 Milliarden Authentifizierungen für das Jahr 2022 registriert. Gegenüber dem Vorjahr ist das eine Steigerung von 70 Prozent. 2017 waren es laut eduroam-Statistikbericht noch 3,6 Milliarden Authentifizierungen.

Mittlerweile zählt das Aushängeschild der weltweiten National Research and Education Networks (NRENs) registrierte Nutzerinnen und Nutzer in 106 Ländern der Erde. ◆

Weitere Nachrichten zum WLAN-Zugangsdienst gibt es auf der eduroam-Webseite:
https://eduroam.org/eduroam-news-3/

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.

Research and Education Network for Uganda's Journey: Successes, Challenges and the Future

RENU, the Research and Education Network for Uganda, has grown from a small NREN to a fast-growing specialized ICT solutions provider. From the beginning, the focus was on the need to obtain affordable Internet for the Research and Education (R&E) community. With the acquisition of a privately operated network by RENU the cost of Internet gradually came down exponentially, although further reduction of the cost remains high on the NREN's agenda. Since then a lot has happened regarding connectivity.

Text: **Caroline Tuhwezeine Kumwesiga** (RENU)

Introduction

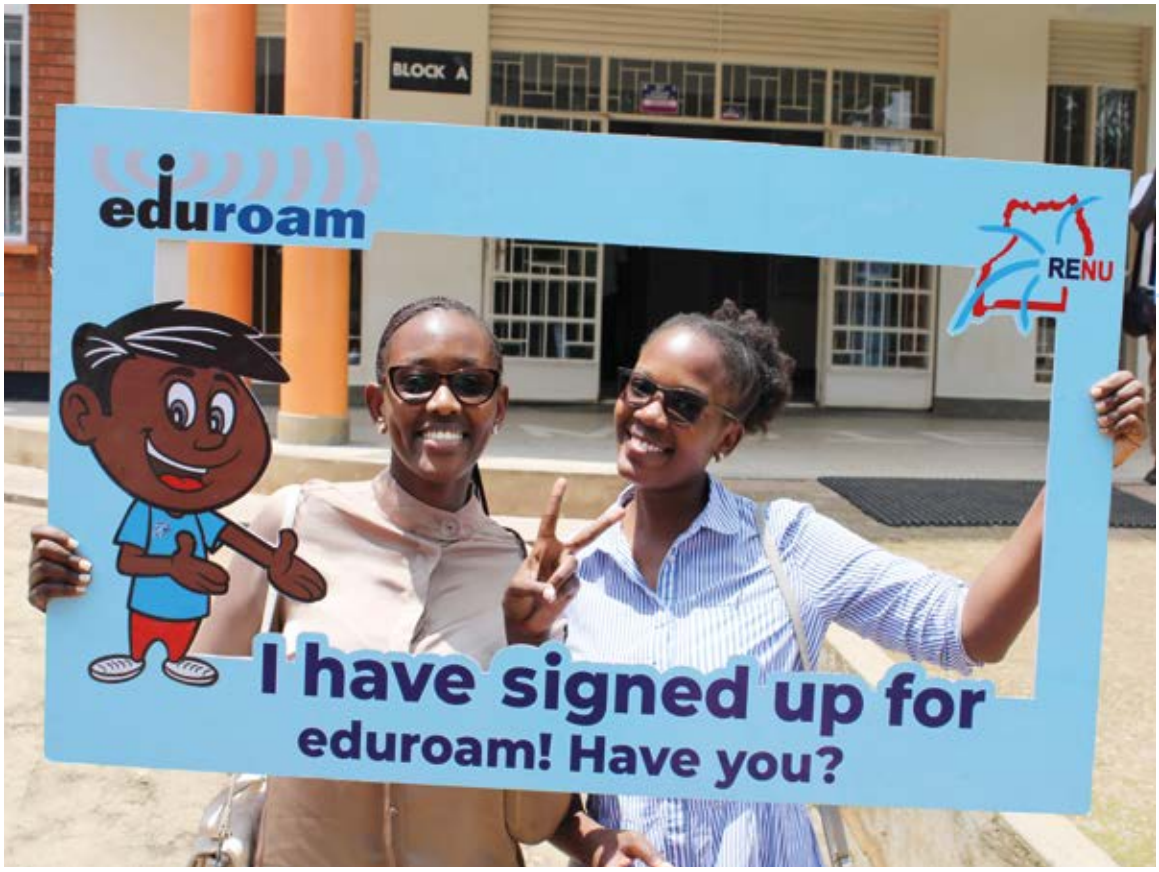
RENU is the National Research and Education Network (NREN) for Uganda, the country also known as the Pearl of Africa, located in the East African Region. RENU is a not-for-profit member-based organization, now serving a total membership of 230 institutions which include universities, other Tertiary Institutions (OTIs), schools and research organisations, with a total of 500 connected sites.

Having been founded in 2006, RENU has grown from a small NREN that focused on just connectivity needs of universities and research organisations, to a fast-growing specialized ICT solutions provider for the entire Research and Education (R&E) community including schools, colleges, universities, Other Tertiary Institutions (OTIs), hospitals and their end users.

The Beginnings

Initially, the idea of RENU started from the desire of a group of Vice Chancellors of universities and Chief Executive Officers (CEOs) of research institutions to form a consortium that would leverage the power of togetherness to negotiate favourable Internet prices from the available Internet Services Providers (ISPs) in order to ease collaboration among researchers, education practitioners and their constituents. It should be noted that the cost of Internet in Uganda at the time was at USD 3,300 per Mbps.

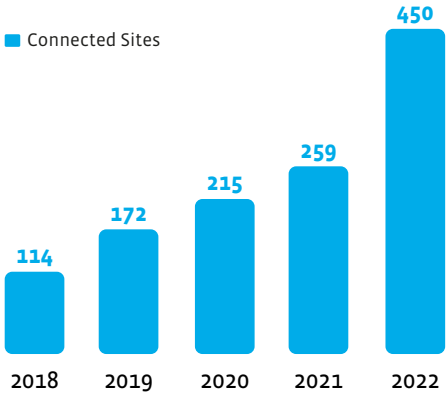
Unfortunately, the consortium's efforts were futile in reducing the prices of Internet, not to mention the poor quality of the connection. This led to a decision for the cooperating universities and research institutions to establish their own privately-operated network which was



Stunning success story: In 2016 RENU was the 75th National Roaming Operator (NRO) for eduroam.

achieved in 2010, when the Uganda Communications Commission (UCC) granted RENU the license to operate the network. In 2014, RENU connected Uganda Christian University (UCU) as the 1st site. With RENU as a player, the cost of Internet gradually came down exponentially, although further reduction of the cost remains high on the NREN's agenda.

CONNECTED SITES OVER THE YEARS



RENU as a Solutions Provider

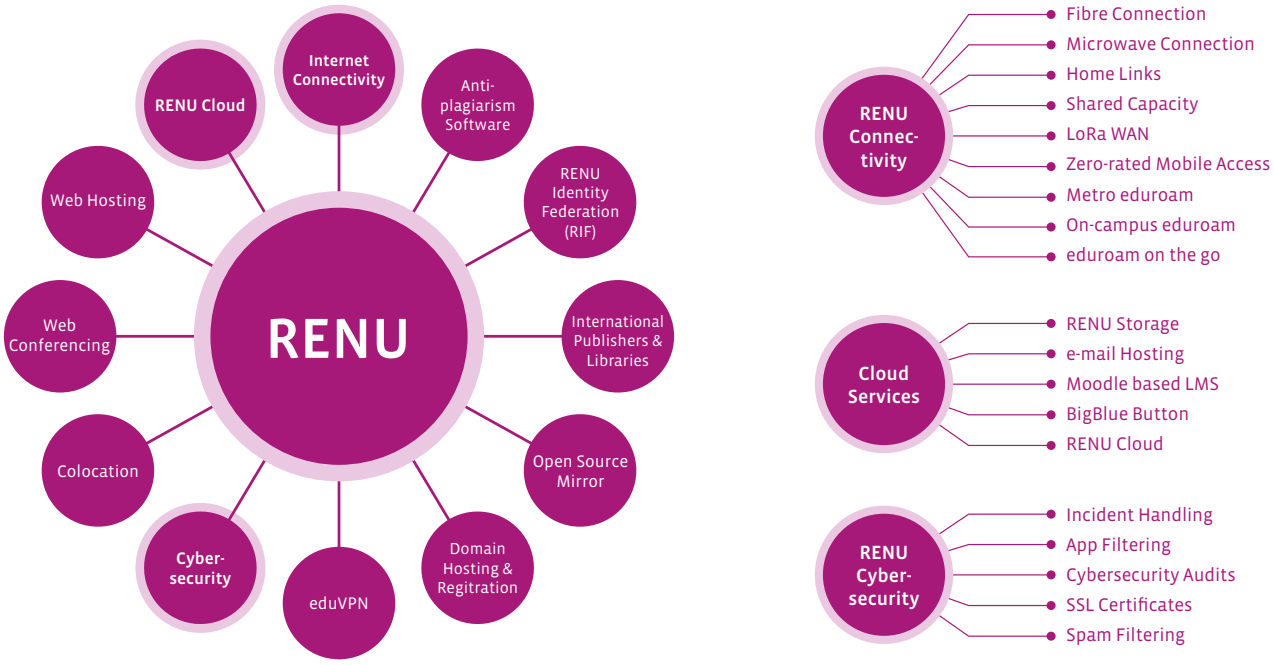
As the RENU network grew, with more institutions joining, there was a challenge that most of the connected institutions did not have solid Local Area Networks (LANs) in their premises, hindering such institutions from fully benefitting from the robust network established by RENU. This compelled RENU to start a capacity building program to equip the ICT staff of its members with the skills needed to establish and maintain robust LANs that communicate well with the RENU network.

In April 2014, RENU in collaboration with the Network Startup Resource Centre (NSRC) and the International Network for Advancing Science and Policy (INASP), commenced the Capacity Building Program that has been implemented alongside other activities targeted to grow the membership.

With the RENU network and a supportive capacity building program in place, member institutions started to enjoy reliable and affordable connectivity, but to RENU, that was just the beginning. RENU's focus had grown beyond just providing an affordable and reliable Internet connection. The solid Internet infrastructure was to later be the underlying force for greater ICT-enabled collaboration among the institutions that RENU was serving.

Indeed, after securing the network, more services started to unfold and to date, RENU's catalogue has registered over 30 services and products, a considerable number of them focusing on the end user. A few of the services that we consider to have been game changers have been elaborated on. Such services and products have made us a little unique not only from the conventional Internet Service Providers (ISPs) at home but also many other African NRENs.

RENU SERVICES AND PRODUCTS



eduroam, Metro eduroam and eduroam on the Go

On 7th January 2016, RENU launched eduroam as a service in Uganda, and was officially recognized as the 75th National Roaming Operator (NRO) for eduroam, a free and secure global Wi-Fi roaming service for the Research and Education (R&E) community. eduroam allows logins that have been assigned to the users by their respective institutions by use of a distributed database. eduroam has now become one of the most sought-after services for research and education institutions as it provides connectivity for staff, lecturers and students as they roam from one campus to another.

Metro eduroam (Off-campus eduroam)

In September 2020, when students and staff of member institutions could not access their institutional networks due to the COVID-19 related institutional closures, RENU extended eduroam (as Metro eduroam) in more than 300 locations in Central Uganda i.e. in the capital city, Kampala, and the towns of Mukono and Entebbe, to bring the much-needed secure Wi-Fi closer to the end users.

At the time of COVID-19 institutional closures, a number of institutions attempted to continue operations remotely but the cost of doing so on the other private networks was high. Additionally, because most of the population was working from their homes, they created a lot of traffic on the masts within their residences which led the connection to deteriorate, making it almost impossible to accomplish any meaningful online activity. This situation is what was behind RENU's motivation to launch Metro eduroam. Metro eduroam hotspots can be accessed in major places of convergence such as student hostels, malls, restaurants, cafés, streets, fuel stations, the airport etc. With Metro eduroam, it was now easy for students and lecturers to locate the eduroam spots closest to them, give or receive instructions or upload course work securely at no cost.

The Metro eduroam reach has nearly doubled in terms of the number of hotspots and geographical coverage, in just a span of two years. In terms of geographical coverage, Metro eduroam has spread from just the initial three cities of Kampala, Mukono and Entebbe, to 14 more towns in other regions across Uganda as well. This incredible growth has been partly attributed to the growing appreciation of eduroam by the member institutions as seen from the gradual increase in the uptake of the service.

The number of institutions connected to eduroam increased from 22 in 2021 to 86 by end of 2022. Besides the appreciation of the service by the members, there has been incredible support from the Internet Society Foundation through the Building Opportunities/Leveraging Technologies (BOLT) Grant, through which 98 new Metro eduroam hotspots were deployed across 14 more towns upcountry, in the first quarter of 2022. Currently, there are over 470 Metro eduroam hot spots across the country. All the Metro eduroam hotspot locations can be found on https://eduroam.renu.ac.ug/.

The number of institutions connected to eduroam is not only critical for the optimal use of our Metro eduroam hotspots but also an inspiration for us to expand the reach of eduroam by deploying more hotspots. This is because more institutions getting connected to eduroam means that more students, staff and researchers are eligible to access and use the Metro eduroam hotspots. It is only after an institution has been connected to eduroam and assigned login accounts that the institution's students and staff are able to fully utilise the eduroam hotspots both on and off-campus. Therefore, having had more institutions joining eduroam in the past two years, there has been remarkable growth in the usage.

Between September 2021 to end of 2022, the Metro eduroam successful logins grew from 609,916 to 11,634,104, new users (unique logins) from 1,556 to 35,831, and average daily peak traffic from 33 Mbps to 170 Mbps.

We also observe that there are domains belonging to institutions from outside Uganda utilizing the eduroam hotspots. Top among these are those shown below:

- student.cbs.dk
- wf.uct.ac.za
- campus.lmu.de
- lshtm.ac.uk

eduroam on the Go! Anytime, Anywhere

eduroam on the Go is another product of an evolution from the traditional on-campus eduroam. It is a pocket-size routing device specially made to enable researchers, university students and other member institutions' staff, to connect to eduroam anytime, anywhere. This means that for the first time, eduroam users do not have to access the free Wi-Fi from only a few fixed locations. Researchers, for example, are able to exchange data while in the field or working away from office.

Another Gamechanger from eduroam family: The pocket-size routing device specially made to enable researchers, university students and member institutions' staff to connect to eduroam anytime, anywhere.

While Metro eduroam came as a great free, secure and trusted off-campus connection to help students and staff of RENU member institutions work and study remotely, our researchers and staff were still experiencing connection challenges whenever they were working in various places that were out of the coverage of the Metro eduroam hotspots. The limitation in coverage is what eduroam on the Go sought to address. eduroam on the Go therefore bears all the characteristics of eduroam, i.e., it is FREE, SECURE, and TRUSTED because it works with the authentication infrastructure and databases of a user's home institution.

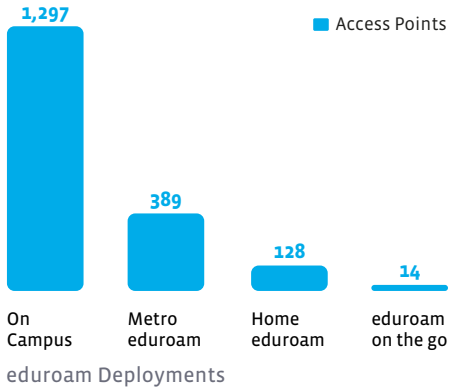
eduroam on the Go gives researchers and university staff secure remote access to their institutional resources e.g. e-books and office databases, anytime, anywhere. It also gives them unlimited access to the Internet since they no longer need to worry about their data bundles running out.

The product was launched on 8th September 2022 with 14 test devices extended to staff through their institutions, and with the plan to roll it out massively in April 2023 after any pain points of the product had been fixed. From the usage of the 14 test devices, some statistics have been shared in the illustrations at the end of this subsection.

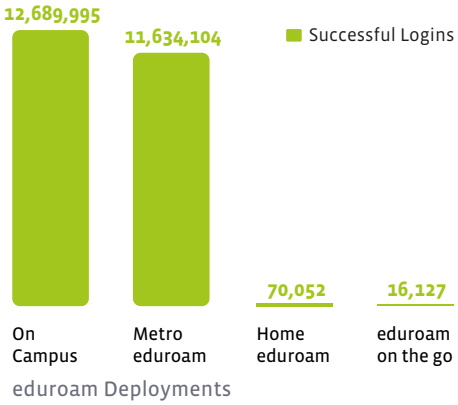
eduroam Home Links

RENU started deploying home links in 2021 as part of the plan to ease access to Internet for staff who were working remotely during the COVID -19 pandemic. Each home link is enabled with an eduroam SSID (Home eduroam). By end of 2022, RENU had deployed a total of 128 home links for staff of member institutions. The home links have since continued to be operational even during the post COVID times and more are being demanded for by member institutions that have flexible work schedules. Below are some graphical representations of some eduroam statistics at the end of 2022.

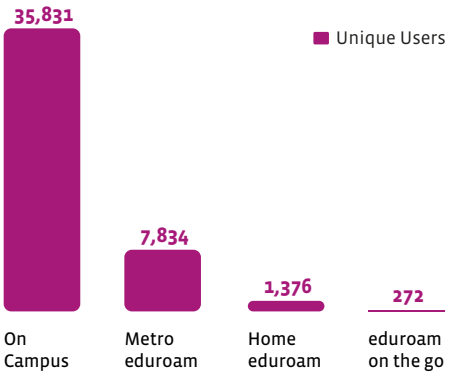
EDUROAM DEPLOYMENTS IN UGANDA



SUCCESSFUL LOGINS



UNIQUE USERS



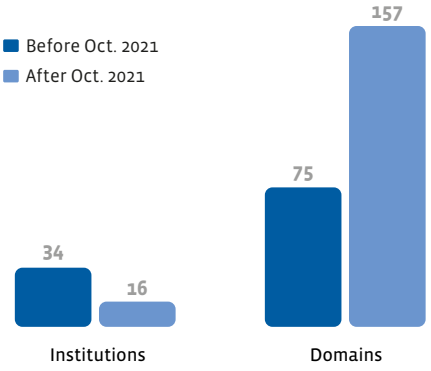
eduroam Deployments

Zero-rated Mobile Access

As already indicated in the first sections of this article, regardless of the other solutions, access to affordable connectivity remains high on the agenda because beyond the institutions we serve, lies a student, a researcher, a teacher, who is facing a lot of difficulty adjusting to the non-conventional ways of teaching or learning, the biggest obstacle being unaffordable access to the respective institutions' e-learning platforms when off-campus. To ease access to online study/teaching to students and staff, on 12th October 2020, RENU launched Zero-rated Mobile Access. To achieve this, RENU arranged with MTN and Airtel Uganda to enable member institutions have their students and staff access the institutions' websites and e-learning portals without having to load a data bundle. In the same way, individuals connected to MTN Uganda now do not need to load a data bundle to access all sites in the "renu.ac.ug" domain.

A year later, zero-rating with Airtel was discontinued after several technical challenges that were experienced in the implementation of the service. During the same year, MTN also declared a change in the setup of the service after technical loopholes were discovered in the previous setup. This affected connectivity on all the domains that had been previously zero-rated. A number of domains were later whitelisted and by the end of 2022, the total number of domains zero-rated with the MTN network stood at 157. Among the zero-rated domains are websites, learning management systems, and web conferencing tools.

RENU ZERO-RATING TREND



A high motivated team of now 52 experts – 29 male 23 female – is working on innovative ways to support education and research institutions in Uganda.

RENU's old Office at House No. 31, Makerere University, Main Campus, Kampala

RENU's new office premises at Plot 6, Mabua Rd, Kololo, Kampala

The Zero-rated Mobile Access service became very handy especially during the 2020 and 2021 lockdowns where a number of institutions were able to hold online classes and seminars by leveraging some of the zero-rated web conferencing tools such as RENU's BigBlueButton. Coupled with the zero-rated Learning Management Systems, RENU's BBB enabled numerous institutions to offer lectures to students/academicians without worrying about the cost of Internet connectivity. With this service, RENU empowered students/academicians from all around the country, especially those outside the reach of Metro eduroam, to access online academic content without worrying about the cost of internet connectivity.

Staffing

RENU is a growing NREN and this is happening at a fast rate. The growth in terms of services, membership and sites had put a lot of pressure on the initially lean staff structure of a typical young NREN. As such, there has been a lot of growth in the staff structure in a span of not more than 5 years. The number of staff has grown from 14 since 2019 to the current 52 staff, 29 male 23 female.

RENU has also been consistent with the mode of staffing. The model commonly used at RENU is recruitment and mentoring of young, energetic and exceptionally bright graduate trainees from our member institutions. The RENU Secretariat ensures that an experienced person leads a section and mentors younger graduates to execute most of the operations. The advantage with the model is that young people are full of fresh ideas, flexible and easier to sustain.

This model of staffing has borne fruits in terms of grooming future team leaders. Currently, 3 out of 6 departments are being headed by staff that joined RENU as graduate trainees, and quite a big number of former graduate trainees have graduated to middle level management.

With the increased number of staff, and volume of operations, it was becoming a little too much for the CEO and the Head of Finance Operations, to continue managing the Human Resource (HR) aspects of the NREN and also manage compliance and risk. Likewise, the space at House No. 31 at Makerere University, Main Campus became too small to accommodate the staff number. Accordingly, RENU had to recruit an Internal Auditor to keep RENU in check of the likely risks that come with growth, a professional Human Resource Officer to cater for the HR needs of RENU, and acquire additional space to accommodate the growing number of staff.

Beginning 2023, the new office space became operational besides the office that is located within Makerere University, with the capacity to accommodate anticipated growth for at least the next 5 years.

Conclusion

The challenges notwithstanding, our focus remains using all the opportunities within our reach to continuously innovate ways to get all our education and research institutions to affordably collaborate for the sake of improving the quality of research and education in our country. To achieve this, we definitely need the continuous support from all our partners including the fellow NRENs. ◆

Sicherheit³ – drei Jahrzehnte DFN-CERT

Seit mehr als dreißig Jahren – genauer gesagt seit dem 2. Januar 1993 – gibt es das Computer Emergency and Response Team (CERT) im Deutschen Forschungsnetz (DFN). Mit seinen umfassenden Dienstleistungen und Beratungsangeboten unterstützt das DFN-CERT damals wie heute die am DFN teilnehmenden Einrichtungen beim Thema IT-Sicherheit und sorgt dafür, dass Cyberangriffe schnell erkannt und in vielen Fällen abgewehrt werden können.

Text: **Klaus-Peter Kossakowski** (DFN-CERT)

Ein Netz wie das Deutsche Forschungsnetz ist mit seinen angeschlossenen Teilnehmern aus Forschung und Lehre heute noch viel mehr als damals ein attraktives Ziel. Es gibt interessante Dinge zu holen – und wenn es eben nur für Angreifer relevante Forschungsergebnisse sind, die ein paar Jahre früher zur Verfügung stehen als vor der offiziellen Veröffentlichung. Aber auch die schnellen Leitungen mit ihren großen Kapazitäten sind ein potenzielles Ziel, denn diese können für DDoS-Angriffe missbraucht werden. Welchen großen Stellenwert Cybersecurity heute hat, konnte man vor 30 Jahren vielleicht schon erahnen, aber nicht in voller Tragweite ermessen.

Gestern, heute und morgen – einfach unverzichtbar

Am 2. November 1988 erfuhren die Nutzenden des Internets sehr drastisch, was ein relativ simpler Computerwurm (eine sich selbstständig im Netzwerk durch Kopieren und Remote Execution verbreitende Malware) bewirken kann. Zehn Prozent der damals weltweit circa 70 000 Rechner wurden lahmgelegt. Vor allem die E-Mail-Server waren betroffen, sodass E-Mail als primäre Basiskommunikation nicht mehr zur Verfügung stand, und zwar im gesamten Internet. Computerviren gibt es schon seit Mitte der achtziger Jahre, das Konzept eines selbstreplizierenden Programms ist jedoch sehr viel älter und beschäftigte schon früh Forschende und Netzwerker. Und es wird in einer Zukunft, in der Artificial Intelligence eine immer größere Rolle spielt, wohl noch sehr viele Generationen beschäftigen.

Schon einen Monat nach dem Internetwurm gründete die Defense Advanced Research Projects Agency (DARPA), eine Behörde des Verteidigungsministeriums der Vereinigten Staaten, an der Carnegie Mellon University (Pittsburgh, PA, USA) „das" CERT. Dieses CERT kümmerte sich in allererster Linie um das Internet, die damit vernetzten Rechner und bot weltweit seine Hilfe an. Mit der Verbreitung des Internets erkannten die ersten Nationalen Forschungsnetze und Regierungseinrichtungen die Notwendigkeit, eigene Ressourcen für den Fall der Fälle vorzuhalten.

Die Vorarbeiten zum DFN-CERT begannen im Sommer 1992. In Skandinavien war bereits 1991 und in den Niederlanden Anfang 1992 ein CERT gegründet worden. Mit den CERT-Gründungen wollte die Wissenschaftsgemeinschaft in Europa der wachsenden Unsicherheit in den immer größer werdenden Netzen entgegentreten.

Klaus-Peter Kossakowski
Professor für IT-Sicherheit an der HAW Hamburg, Geschäftsführer der DFN-CERT Services GmbH

2019: Aufnahme in die FIRST Incident Response Hall of Fame. Seit 2003 ständiger Gast im Ausschuss für Recht und Sicherheit des DFN. Ständiges Mitglied im Programmausschuss des BSI-Kongresses sowie der jährlichen Konferenzen des DFN-CERTs und FIRST.

Die offene, von Vertrauen geprägte Kultur der Wertschätzung und Kooperation in Forschung und Lehre war und ist gefährdet – das hat sich mit geschäftsmäßig agierenden Cyberkriminellen und den politisch oder nationalstaatlich motivierten „State Actors" nur noch deutlicher gezeigt. Und auch wenn Forschung und Lehre nicht als kritische Infrastruktur eingestuft werden, sind sie es doch – kritisch für den Erfolg einer Gesellschaft, kritisch für die Nachhaltigkeit sowie die Qualität des täglichen Lebens. Und so sind

Freiheit und Offenheit auch dadurch gefährdet, dass wir diese zu unserem Schutz immer weiter einschränken müssen. Denn das ist nötig, um der Verpflichtung nachzukommen, die Daten der Studierenden, Lehrenden, Mitarbeitenden und Forschenden in den teilnehmenden Einrichtungen zu schützen.

Das Security Incident Management gehört zu den ganz elementaren Aufgaben: die Fähigkeit, zugesagte Dienste auch bei und trotz Angriffen aufrechtzuerhalten. Die Vertraulichkeit sensitiver Informationen sicherzustellen und zu verhindern, dass Manipulationen an Daten oder Systemen die Reputation oder auch Leib und Leben von Menschen gefährden, ist anerkannte – quasi lebensnotwendige – Voraussetzung für jedwede Digitalisierung unserer Gesellschaft. Das DFN-CERT ist mit dieser kritischen Funktion unverzichtbar.

Alles begann mit einem Computerwurm – für Hans-Joachim Mück und Klaus-Peter Kossakowski (von links): Foto aus einer Reportage des Hamburger Abendblatts vom 25. August 1993 anlässlich der DFN-CERT-Gründung

DIE DFN-CERT SERVICES GMBH

Für mehr Sicherheit im Internet: Mit seiner langjährigen Erfahrung im Aufbau und Betrieb skalierbarer und leistungsfähiger Sicherheitsinfrastrukturen und ihren Diensten – dazu zählt auch der Betrieb fortgeschrittener Zertifizierungsstellen – schützt das DFN-CERT u. a. Rechner und Computernetze vor Angriffen und sorgt für die Sicherheit der elektronischen Kommunikation. Darüber hinaus beteiligt sich das DFN-CERT an Forschungsprojekten zur Entwicklung und Erprobung neuer Sicherheitstechnologien.

Auf dem Postweg – Aktion Anti-Virus

Dass das DFN-CERT damals nach Hamburg kam, war ein Zusammenspiel verschiedener Faktoren. Hier gab es bereits eine kritische Masse an künftigen Fachleuten, sprich eine ganze Generation von Studierenden, die ab April 1988 die Vorlesungen von Prof. Dr. Klaus Brunnstein besuchten. Dieser bot als einer der ersten deutschen Professoren einen ganzen Zyklus IT-Sicherheitsthemen an, die über mehrere Semester gelehrt wurden. So erhielten viele Studierende an der Universität Hamburg eine gute Grundausbildung. Parallel gab es mit dem Virus-Test-Center (VTC) eine Gruppe von Studierenden, die sich konkret mit den praktischen Auswirkungen von Unsicherheit auseinandersetzten. Einige bekamen sogar unter strengsten Auflagen lokal vernetzte Workstations, um Malware auseinanderzunehmen. Andere beantworteten säckeweise Post, als Professor Brunnstein über die Tagesschau zusicherte, alle, die einen frankierten Rückumschlag an das VTC schicken würden, bekämen eine Diskette mit einem selbst entwickelten Melissa-Anti-Virus. Und ja, er musste direkt nach dem Interview zu einer Konferenz ins Ausland. Viele dieser Studierenden sind bis heute überall in Sicherheitsfirmen zu finden. Allen gemein ist, dass sie mit diesem Thema gleichsam „infiziert“ wurden und fortan eine große Verantwortung trugen.

Die Widerstandsfähigkeit stärken – gemeinsam

Aber das DFN-CERT ist nicht nur eine Hamburger Erfolgsgeschichte, hier arbeiten Menschen aus dem In- und Ausland, darunter auch einige, die rein in Telearbeit tätig sind. Mit dem Start der DFN-Security-Operations kann das DFN-CERT nun noch mehr leisten. Denn durch die Auswertung von Sicherheitsereignissen sowohl lokal bei den Teilnehmern als auch bei den genutzten Dienste, können Vorfälle viel schneller erkannt und zum Teil auch abgewehrt werden. Dafür wurde auch der Bereich der „Cyber Threat Intelligence“ als eigenes Team mit eigenen Prioritäten und eigener Außenwirkung aufgebaut. Für uns und alle Teilnehmer gilt, dass wir die Verwundbarkeit wie schon immer insgesamt reduzieren müssen. Aber auch das Thema des Wiederanlaufs und der vollständigen Systemwiederherstellung müssen wir in den Fokus nehmen. Resilienz ist dabei der neue Leitgedanke, den wir jetzt in vielen Kontexten hören. Diese Widerstandsfähigkeit ist extrem wichtig, damit komplexe Infrastrukturen nicht wie in einem Dominoeffekt zusammenfallen.

Trotz aller Veränderungen sind wir über all die Jahre hinweg uns selbst, unserer besonderen Rolle, unseren Zielen und Werten im Kern treu geblieben: Wir sind ein Dienstleister mit eingespielten Teams und viel individuellem Know-how, der sich immer wieder neu orientiert, um Trends aufzunehmen oder auf Herausforderungen zu reagieren. Für den DFN, seine Teilnehmer und unsere weiteren Kunden sind wir der verlässliche Partner für mehr Cybersicherheit und Datenschutz. ◆

Sicher FAIR – der NFDI-Basisdienst IAM

Als erster Basisdienst in der Nationalen Forschungsdateninfrastruktur NFDI geht der Dienst Identity and Access Management (IAM) an den Start. Hierbei geht es um die Implementierung technischer und organisatorischer Lösungen, die ein dezentrales und föderiertes Identitätsmanagement für einen Community-gesteuerten, einheitlichen und sicheren Zugriff auf digitale Ressourcen ermöglichen. Durch die Integration in die DFN-AAI können nicht nur 400 an der DFN-AAI teilnehmende Heimateinrichtungen partizipieren, sondern über eduGAIN potenziell auch Nutzende aus weiteren rund 5000 Hochschulen und Forschungseinrichtungen weltweit.

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

Im Rahmen der Nationalen Forschungsdateninfrastruktur (NFDI) werden aktuell 26 Fachkonsortien sowie der Verbund der Fachkonsortien Base4NFDI, Basisdienste für NFDI, gefördert.

Ziele der NFDI sind es, das Management von Forschungsdaten zu fördern und gemäß den Anforderungen der über die Fachkonsortien repräsentierten Communities weiterzuentwickeln. Wichtige Aspekte sind dabei dauerhafte Verfügbarkeit, Adressierbarkeit, semantische Erschließung, Verknüpfung und Nachnutzbarkeit von Forschungsdaten sowie damit einhergehende Möglichkeiten zur Bearbeitung interdisziplinärer Fragestellungen.

Schon früh hat sich gezeigt, dass unabhängig von der jeweiligen Fachdisziplin bestimmte Grundfunktionalitäten benötigt werden, um Forschungsdatenmanagement insbesondere gemäß der FAIR-Prinzipien betreiben zu können. „FAIR" steht in diesem Zusammenhang für „Findable", „Accessible", „Interoperable" und „Reusable". Forschungsdaten sollten also auffindbar, zugänglich, interoperabel und wiederverwendbar sein.

Der über Base4NFDI geförderte Basisdienst Identity and Access Management (IAM) zielt darauf ab, technische und organisatorische Rahmenbedingungen zu schaffen, um Forschungsdaten und die zu deren Management benötigten Dienste langfristig und nachhaltig „accessible" zu gestalten. Außerdem müssen Interoperabilität sowie Anschlussfähigkeit an andere Infrastrukturen wie die European Open Science Cloud (EOSC) gewährleistet sein. Als Basis hierfür dient eine Authentifizierungs- und Autorisierungsinfrastruktur (AAI). Wie sich die Integration in die DFN-AAI darstellt, wird im Folgenden beschrieben.

Entsprechend dem festgelegten Verfahren für Basisdienste wird derzeit die Initialisierungsphase über Base4NFDI gefördert. Die weiteren Phasen zur Integration und Überführung in den Produktivbetrieb werden zu späteren Zeitpunkten separat behandelt. Dieser Beitrag beschreibt das „große Bild" ohne Bezug zu einzelnen Förderphasen.

Community-AAI

Die Lösung, sämtliche digitalen Ressourcen der NFDI zu föderieren, indem sie einzeln als Serviceprovider in der DFN-AAI verfügbar gemacht werden, ist nicht zielführend. Aufgrund der Rahmenbedingungen, die seitens der Fachcommunities bestehen, muss ein anderer Ansatz gewählt werden.

Zunächst zu den Rahmenbedingungen:

1. Authentifizierung: Nicht alle Forschenden, die Zugriff auf NFDI-Ressourcen erhal-

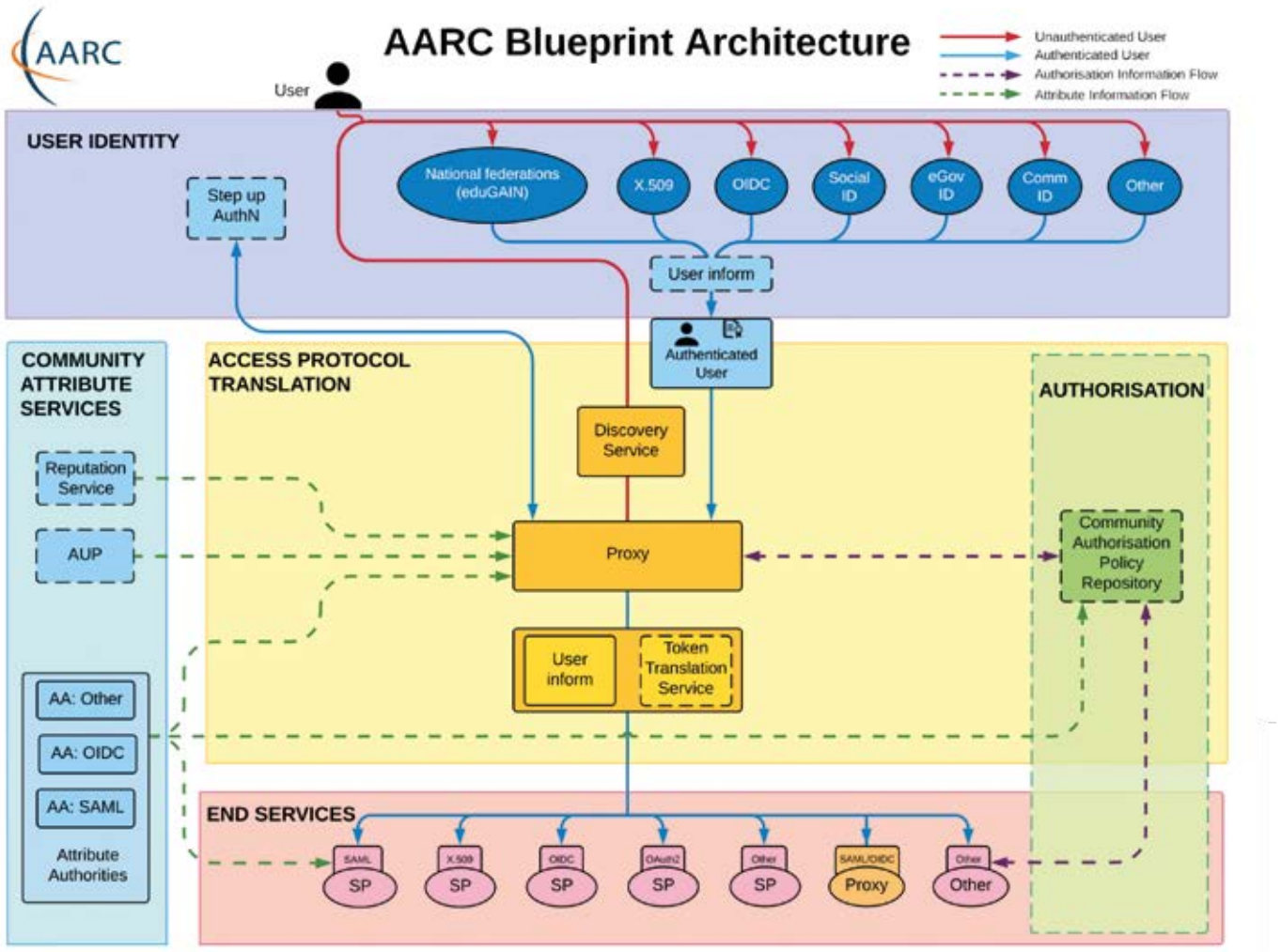


Abbildung 1: AARC Blueprint Architecture | *©GÉANT Association*

ten sollen, haben die Möglichkeit, sich über einen Identity Provider (IdP) aus einer der über eduGAIN vernetzten Föderationen zu authentisieren. Daher müssen weitere Authentifizierungsquellen wie ORCID, Google, Facebook etc. sowie gegebenenfalls ein Homeless-/Gast-IdP an die betreffende AAI angebunden werden.

2. Autorisierung: Das Rechte- und Rollenmanagement für den Zugriff auf Community-spezifische Ressourcen kann sinnvollerweise nur seitens der Fachcommunities bzw. der Fachkonsortien erfolgen. In diesem Kontext wird auch von einer „Virtuellen Organisation" (VO) gesprochen. Das Management der Virtuellen Organisationen in der NFDI obliegt den Fachkonsortien, die ihre jeweiligen Communities repräsentieren. Für den Zugriff auf fachspezifische Ressourcen ist also ein dezentrales VO-Management erforderlich. Die von den Authentifizierungsquellen (z. B. Heimat-IdP) übertragenen Informationen dienen lediglich der Identifizierung der Nutzenden, nicht deren Autorisierung.

3. Technische Kompatibilität: Nicht jede Ressource bzw. deren zugrunde liegende Software unterstützt den Standard SAML (Security Assertion Markup Language), auf dem aktuell noch die meisten Föderationen, z. B. die DFN-AAI, beruhen. In Fällen, in denen andere Single-Sign-on-Standards und Protokolle wie OpenID Connect oder OAuth2 unterstützt werden oder die Zugriffskontrolle zertifikatsbasiert erfolgt, muss ein Token-Translation-Service vor die einzelnen Ressourcen bzw. Dienste geschaltet werden, um hier einen einheitlichen Zugriff zu ermöglichen.

Diese Punkte sind weder neu noch singulär, sondern betreffen Forschungscommunities und -projekte ganz allgemein. Im Rahmen des AARC-Projekts (Authentication and Authorization for Research and Collaboration) wurde in den Jahren 2015 bis 2019 die sogenannte AARC Blueprint Architecture (BPA) entwickelt. Wie der Name schon sagt, bietet die BPA eine Blaupause für eine Community-AAI und trägt insbesondere den drei oben genannten Punkten Rechnung (siehe Abbildung).

Die BPA besteht aus fünf Komponenten, die zur Implementierung von föderierten IAM-Lösungen für Forschungsverbünde, also zu einer Community-AAI, kombiniert werden können:

- **User Identity:** Authentifizierung über AAI, Soziale Medien, ORCID etc.
- **Access Protocol Translation:** IdP-/SP-Proxy, Token-Translation
- **Community Attribute Services:** Rechte, Rollen, VO-Management
- **Authorisation:** Autorisierung, Verwaltung des Zugriffs auf Dienste/Ressourcen
- **End Services:** die eigentlichen Dienste und Ressourcen

Die zentrale Komponente dieses Konstrukts stellt ein Proxy dar, über den praktisch alle Informationen fließen. In Richtung Föderation und etwaiger weiterer Authentifizierungsquellen erscheint der Proxy als Serviceprovider, gegenüber den angeschlossenen Diensten und dem optionalen Token-Translation-Service fungiert er als Identity Provider.

Ergänzt wird diese Architektur durch eine Reihe von Guidelines, die seitens der AARC-Community entwickelt wurden und weiterentwickelt werden. Diese sollen ein Höchstmaß an Interoperabilität sowohl innerhalb von Community-AAIs als auch zwischen Community-AAIs und Infrastrukturen wie EGI oder der European Open Science Cloud (EOSC) sicherstellen.

Im Rahmen des Basisdienstes IAM werden vier Open-Source-Implementierungen der AARC Blueprint Architecture unterstützt, für die ein langfristiger Support seitens der zuständigen Projektpartner gewährleistet ist. Im Rahmen des Basisdienstes IAM werden Workshops und Schulungen veranstaltet, die Fachkonsortien in die Lage versetzen sollen, diese Lösungen selbst zu betreiben. Daneben wird aber auch das Hosting besagter Lösungen angeboten werden: als Community-AAI-as-a-Service, (CAAIaaS).

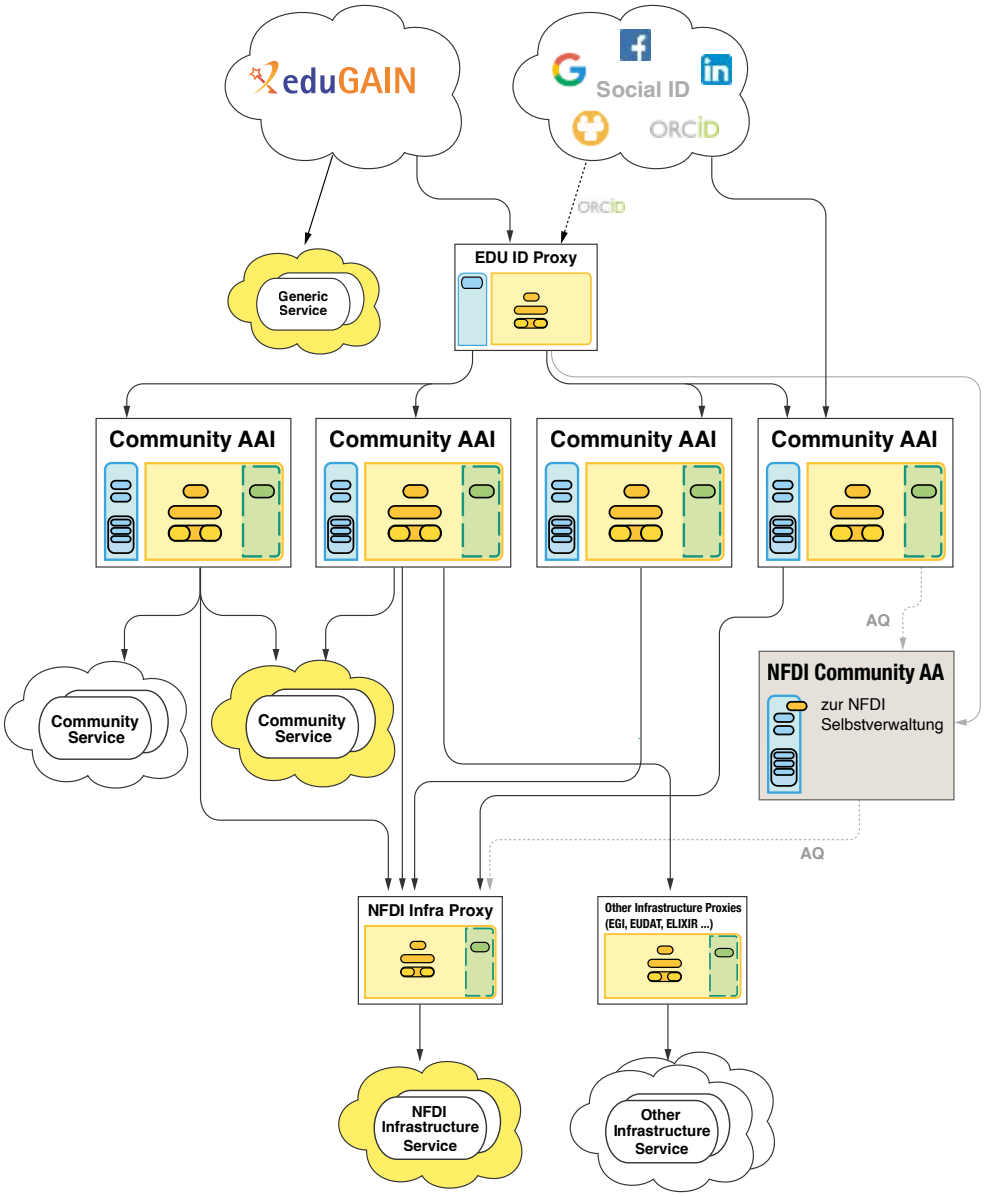


Abbildung 2: Architektur der NFDI-AAI

NFDI-AAI

Wie können nun Community-AAIs im Rahmen einer NFDI-AAI untereinander vernetzt und interoperabel gemacht werden? Auf technischer Ebene geschieht dies durch die Integration der SP-Proxy-Komponenten der Community-AAIs in die DFN-AAI. Auf diese Weise stehen die in der NFDI-AAI zusammengeschlossenen Community-AAIs und deren Ressourcen nicht nur Forschenden aus den ca. 400 an der DFN-AAI teilnehmenden Heimateinrichtungen zur Verfügung, sondern über eduGAIN potenziell auch Nutzenden aus weiteren rund 5000 Hochschulen und Forschungseinrichtungen weltweit. Ergänzt wird die Architektur der NFDI-AAI durch Komponenten wie einen edu-ID-Proxy und einen Infrastruktur-Proxy sowie potenziell eine NFDI-Community-Attribute-Authority für ein Community-übergreifendes Rechte- und Rollenmanagement (Abbildung 2).

Der Infrastruktur- bzw. Infra-Proxy dient als einheitliche Schnittstelle zur Anbindung von Diensten an die NFDI-AAI, die

Community- bzw. konsortienübergreifend verfügbar sein sollen. Wie bei den Community-AAIs werden auch hier unterschiedliche Protokolle und Single-Sign-on-Standards unterstützt.

Der edu-ID-Proxy dient mehreren Zwecken. Zunächst bietet er Nutzenden eine lebenslang gültige, einrichtungsunabhängige, selbst verwaltete, digitale Identität. Dieses Konzept adressiert das Problem der Researcher Mobility. Damit ist der Umstand gemeint, dass Forschende in befristeten Arbeitsverhältnissen häufiger den Arbeitgeber und somit ihre Heimateinrichtung sowie ihre damit verbundene digitale Identität wechseln. Eine unterbrechungsfreie Nutzung von Diensten wie Forschungsdatenrepositorien ist somit nicht möglich. Das edu-ID-System ermöglicht also die nahtlose Nutzung der über die NFDI-AAI verfügbaren Ressourcen und dient zugleich als zentraler Homeless-/Gast-IdP. Weiterhin bietet das edu-ID-System die Möglichkeit, die eigene digitale Identität mit weiteren Accounts zu verknüpfen, die damit verbundenen Daten wie die ORCID iD zu aggregieren und diese bei Bedarf an NFDI-Dienste zu übertragen.

Ein weiterer Baustein der Interoperabilität sind verpflichtende Attribut- und Claim-Profile, die sich sowohl an den AARC- als auch an den EOSC-Guidelines orientieren. Es geht also um die Standardisierung des Austauschs von Nutzenden-Informationen hinsichtlich Syntax, Schemata und Vokabular.

Herausforderung Integration

Auf technischer Ebene wird eine zentrale Aufgabe darin bestehen, die Fachkonsortien im Rahmen der Implementierung einer Community-AAI dabei zu unterstützen, sowohl bestehende AAI-basierte Lösungen als auch weitere digitale Ressourcen als Dienste in die oben skizzierte Gesamtarchitektur der NFDI-AAI zu integrieren. An welcher Stelle ein solcher Dienst angebunden wird, hängt von mehreren Faktoren ab (Abbildung 2).

1. Falls eine Ressource über einen SAML-fähigen Serviceprovider föderiert werden kann, sie eine Zielgruppe über die NFDI hinaus adressiert und der Zugriff nicht über Community-spezifische Autorisierungsregeln gesteuert wird, dann kann der betreffende Serviceprovider als Generic Service direkt in der DFN-AAI angemeldet werden.

2. Wird der Zugriff auf die betreffende Ressource über Community-spezifische Autorisierungsregeln gesteuert, letztlich über das VO-Management einer Fachcommunity, dann sollte dieser als Community Service in die entsprechende Community-AAI integriert werden.

3. Handelt es sich um einen NFDI-internen Dienst, der fachübergreifend genutzt werden soll, so kann dieser als NFDI Infrastructure Service an den Infra-Proxy angebunden werden.

Es ist davon auszugehen, dass insbesondere für die Integration digitaler Ressourcen als Dienste in die NFDI-AAI Softwareentwicklung geleistet werden muss. Daher ist im Basisdienst IAM auch ein Inkubator-Arbeitspaket vorgesehen, in dessen Rahmen entsprechende Entwicklungsarbeiten durchgeführt werden.

Weitere Handlungsfelder

Wie eingangs erwähnt, adressiert der Basisdienst IAM nicht nur technische, sondern auch organisatorische Aspekte der zukünftigen NFDI-AAI und der darin zusammengeschlossenen Community-AAIs. So besteht die wichtigste Aufgabe darin, gemeinsam mit den Fachkonsortien die Governance-Strukturen und -Prozesse für das Management der Virtuellen Organisationen zu etablieren und damit die Grundlage für die nachhaltige Verwaltung der Rechte und Rollen in der NFDI zu schaffen. Hierzu müssen auch juristische Aspekte behandelt werden. Es geht also beispielsweise um die Klärung von Datenschutz- und Haftungsfragen sowie um die Erstellung von Vorlagen für Kooperationsverträge, Acceptable Use Policies etc., die für den Betrieb einer Community-AAI sowie für die Kooperation innerhalb der NFDI-AAI erforderlich sind. Als Ausgangsbasis dient das Policy-Framework der Helmholtz AAI, das sich bereits seit einigen Jahren in der Praxis bewährt hat und seinerseits auf dem Policy Development Kit der AARC-Community beruht.

Weitere Handlungsfelder des Basisdienstes IAM sind die Sicherstellung des langfristigen technischen Betriebs der NFDI-AAI und der darin zusammengeschlossenen Community-AAIs sowie Dissemination, Training und Community Engagement. Dazu gehört die Veranstaltung regelmäßiger Workshops und Infoshares, die unter anderem der Rückkoppelung mit den Fachkonsortien und -communities dienen. ◆

Informationen zum aktuellen Stand des Projektes sowie zur NFDI-AAI gibt es unter:
https://doc.nfdi-aai.de

Mehr Informationen zur AARC Blueprint Architecture finden Sie hier:
https://aarc-community.org/architecture/

Eine für alle – die edu-ID

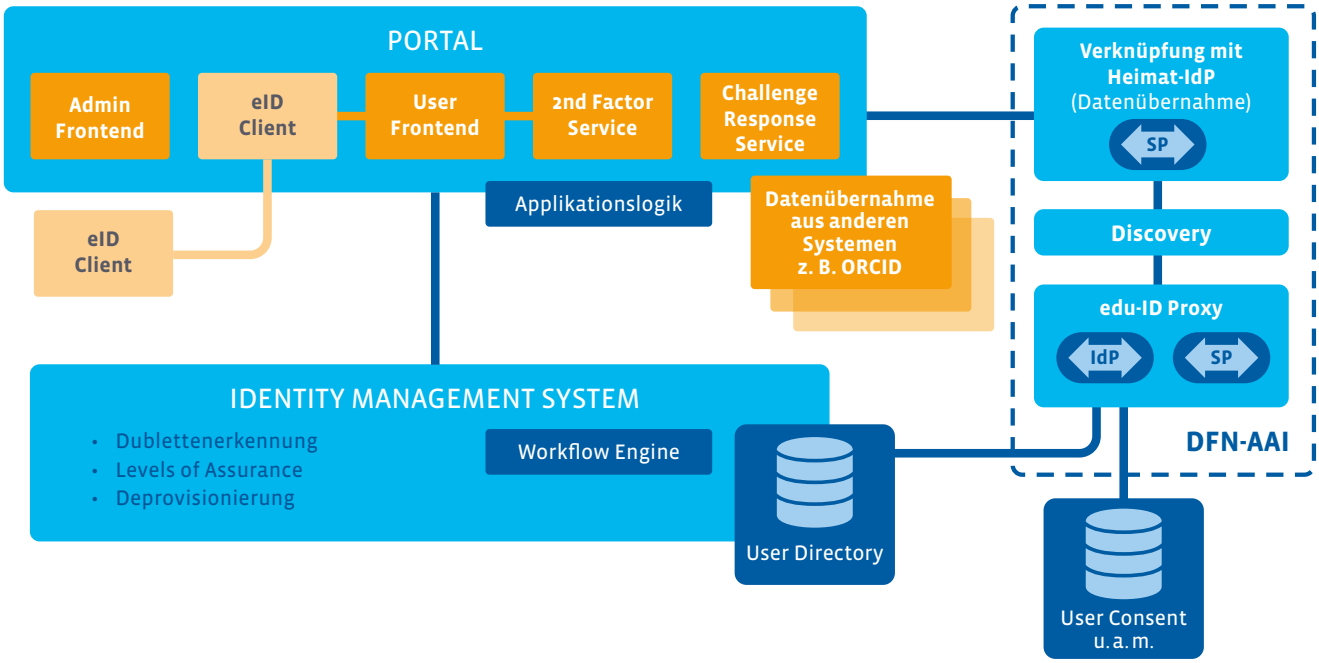
Was ist eine edu-ID? Um es auf eine kurze Formel zu bringen: Es handelt sich um das Konzept einer selbst verwalteten, einrichtungsunabhängigen und lebenslang gültigen digitalen Identität für den Bereich Forschung und Bildung in Deutschland. Nachdem ein Whitepaper zur Positionsbestimmung sowie das technische Konzept Ende vergangenen Jahres veröffentlicht wurden, steht nun der technische Proof of Concept kurz vor der Fertigstellung.

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

Die Lebensdauer einer edu-ID-Identität wird einzig und allein von ihrer Inhaberin bzw. ihrem Inhaber bestimmt. Um lebenslanges Lernen, Forschen und den Zugriff auf die hierfür erforderlichen Ressourcen zu ermöglichen, muss eine solche Identität potenziell lebenslang verfügbar und gültig sein.

In den vergangenen drei Jahren hat eine Arbeitsgruppe des Vereins der „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V. (ZKI) unter Beteiligung des DFN-Vereins und der DFN-CERT Services GmbH das Konzept für eine edu-ID erarbeitet, eine selbst verwaltete, einrichtungsunabhängige und lebenslang gültige digitale Identität für den Bereich Forschung und Bildung in Deutschland. Eine zentrale Aufgabe der Arbeitsgruppe bestand darin, Anwendungsfälle aus den Bereichen Forschung, Bildung und Hochschulverwaltung zu identifizieren, in denen ein edu-ID-System Prozesse und Infrastrukturmaßnahmen erleichtert oder gar erst ermöglicht. Diese Use Cases dienten als Grundlage für die Anforderungsanalyse eines zukünftigen edu-ID-Systems. Als Ergebnis ihrer Arbeit publizierte die Arbeitsgruppe zwei

EDU-ID-SYSTEM: TECHNISCHE KOMPONENTEN



Dokumente. Hierbei handelt es sich einerseits um ein Whitepaper, das darstellt, wie sich das edu-ID-Konzept im Konzert der Systeme für digitale Identitäten in Deutschland und Europa positioniert und welchen Einfluss diese auf die künftige Entwicklung des edu-ID-Konzepts in Deutschland haben. Beim zweiten Dokument handelt es sich um das technische Konzept für das edu-ID-System, dessen Design auf eine nahtlose Integration in die DFN-AAI ausgerichtet ist.

Basierend darauf begann Ende vergangenen Jahres die Proof of Concept-Implementierung des edu-ID-Systems am DFN-CERT, deren Fertigstellung in Kürze erfolgen wird.

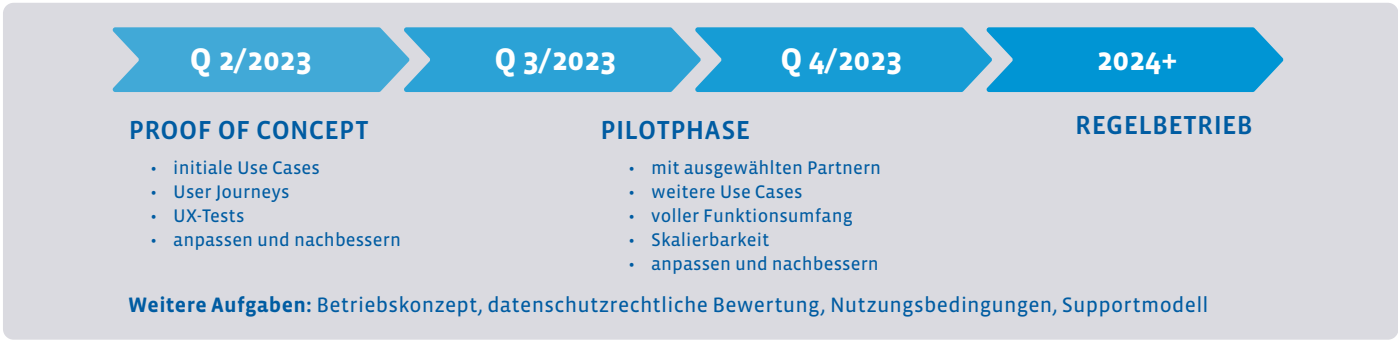
Vorbereitungen für den Pilotbetrieb

Wie geht es dann weiter? Anhand ausgewählter Use Cases aus dem Bibliotheksbereich werden die im technischen Konzept beschriebenen User Journeys durchgespielt. Das edu-ID-Projektteam wird hierbei mit der Staatsbibliothek zu Berlin zusammenarbeiten. Weiterhin sind Tests zur User Experience geplant. Die im Rahmen dieser Validierungstätigkeiten gesammelten Erfahrungen sollen in die weitere technische Projektentwicklung einfließen und die Grundlage für den Pilotbetrieb bilden.

Die Pilotphase ist für die zweite Jahreshälfte 2023 geplant. Gemeinsam mit ausgewählten Einrichtungen und Dienstanbietern aus der DFN-AAI-Community werden die restlichen Use Cases erprobt, die die ZKI-Arbeitsgruppe zu Beginn ihrer Tätigkeit zusammengetragen hat. Auch hier wird es wieder darum gehen, das bestehende Konzept und die Architektur des Systems zu validieren und bei Bedarf entsprechende Anpassungen vorzunehmen. Eine wichtige Rolle wird dabei die Frage der Skalierbarkeit spielen, sowohl auf technischer als auch auf betrieblich-organisatorischer Ebene, insbesondere wenn es darum geht, den Support für die Endnutzenden zu organisieren. Weiterhin müssen bis dahin ein tragfähiges Betriebskonzept erarbeitet sowie alle datenschutzrechtlichen und vertraglichen Fragen geklärt werden. Erst dann kann sinnvollerweise die Aufnahme des Regelbetriebs angegangen werden.

Ausblick

Weiterhin haben sich im Laufe der vergangenen Monate interessante Kooperationsszenarien ergeben, die Anwendungsfälle über die Grenzen der DFN-AAI hinaus in Aussicht stellen. So könnte das edu-ID-System eine Schnittstelle zur Schulföderation VIDIS (Vermittlungsdienst für das digitale Identitätsmanagement in Schulen) bieten, die es Lehramtsstudierenden aus der DFN-AAI heraus ermöglichen würde, auf bestimmte Inhalte von Lernplattformen zuzugreifen, die in VIDIS verfügbar sind. Analoge Überlegungen bestehen für die im Aufbau befindliche Vernetzungsinfrastruktur Digitale Bildung, auch bekannt als Nationale Bildungsplattform – ein Projekt des Bundesministeriums für Bildung und Forschung (BMBF). Hierbei ist darauf hinzuweisen, dass es bei diesen Überlegungen jeweils um eine unidirektionale Verbindung geht, d. h. das edu-ID-System wird nicht als Hintertür für den Zugriff externer Nutzender auf die DFN-AAI dienen. Wir dürfen gespannt sein, wie es mit dem Thema edu-ID weitergeht. ◆



Auf Zenodo finden Sie das Whitepaper zur edu-ID sowie das technische Konzept:
https://doi.org/10.5281/zenodo.7425176
https://doi.org/10.5281/zenodo.7418055

Informationen zu VIDIS finden Sie unter:
https://www.vidis.schule

Informationen zum BMBF-Projekt Digitale Bildung finden Sie unter: **https://bildungsraum.de**

Sicherheit aktuell

Sicherheitsvorfälle bei DFN-Teilnehmern

Foto: przemekklos /Photocase

Der Ausklang des Jahres 2022 sowie auch der Start 2023 waren aus dem Blickwinkel der Sicherheit ausgesprochen düster. Innerhalb von lediglich zwei Monaten erlangte das DFN-CERT Kenntnis von zehn größeren Sicherheitsvorfällen mit teilweise verheerenden Folgen für die jeweils betroffenen Einrichtungen. Dabei konnten die meisten Angriffe auf die Gruppierungen Royal Ransomware und Vice Society zurückgeführt werden. Besonders Letztere erregt aktuell mit zahlreichen internationalen Angriffen auch auf Bildungseinrichtungen mediale Aufmerksamkeit.

Den initialen Zugang zu einem Netzwerk erlangen Angreifende häufig über kompromittierte Anmeldeinformationen, kürzlich wurde aber auch die Ausnutzung von Schwachstellen wie PrintNightmare (Windows Print Spooler) als Angriffsvektor beobachtet. Danach verschaffen sie sich einen Überblick über das Netzwerk der angegriffenen Institution, bevor die Ransomware zum Einsatz kommt. Die Angreifenden exfiltrieren gezielt Daten, die anschließend verschlüsselt werden. Nach Backups wird ebenfalls gezielt gesucht, um diese unbrauchbar zu machen und anschließend eine Lösegeldforderung zu stellen. Bei ausbleibender Zahlung wird gedroht, die Informationen im Internet zu veröffentlichen. Für die Angreifenden gibt es hierbei keinerlei moralische Schranken, wie die Veröffentlichung von Personalausweisen von Schülern und deren Eltern an einer Schule in Großbritannien gezeigt hat.

Diese Sicherheitsvorfälle stellen betroffene Einrichtungen vor eine schwere Aufgabe, da IT-Systeme teilweise wochenlang nicht verfügbar sind – zudem verschlingen sie eine Unmenge Geld, Ressourcen und Energie.

Unterstützung durch das DFN-CERT

„Prävention! Prävention! Schnelle Reaktion!“, so lautet das Mantra des DFN-CERT. Dieses spiegelt sich in den zur Verfügung stehenden Informationssicherheitsdiensten wider. Bei deren effizienter Nutzung kommt dem DFN.Security-Portal eine zentrale Rolle zu: Jede Einrichtung kann sowohl allgemeine als auch speziell für sie verfügbare sicherheitsrelevante Informationen darüber abrufen. Mittels der individuellen Konfiguration kann zudem dafür gesorgt werden, dass Informationen direkt der richtigen Ansprechperson zugestellt werden.

Die Schwachstellenmeldungen stellen einen wichtigen Baustein in den präventiven Diensten dar. Einrichtungen werden beim Bekanntwerden neuer Schwachstellen umgehend benachrichtigt und mit Informationen zu Sicherheitsupdates sowie Mitigationsmöglichkeiten versorgt.

Ein weiterer wichtiger Dienst sind die automatischen Warnmeldungen. Sie informieren über potenzielle Probleme oder Auffälligkeiten, die einen Hinweis auf eine Kompromittierung darstellen. Dieser ursprünglich rein reaktive Dienst wird kontinuierlich um präventive Aspekte erweitert. Für die Meldungen werden interne wie auch externe Datenquellen herangezogen und ausgewertet. In diesem Rahmen spielt die Erweiterung der Sicherheitsdienstleistung über das „Security Operations“-Projekt eine besondere Rolle. Mit der zweiten Stufe der Basisleistungen, die die Untersuchung von Netflows (Cyber Threat Intelligence) mit tagesaktuellen

IoCs (Indicators of Compromise) sowie die Einlieferung und Analyse von Logdaten der Teilnehmer erlaubt, wird der Wert der automatischen Warnmeldungen noch einmal signifikant gesteigert – aktuell befindet sich diese im Roll-Out in den Regelbetrieb.

Aber auch wenn der Worst Case eintritt und Sie sich trotz „Prävention! Prävention!“ mit der Notwendigkeit der „Schnellen Reaktion“ konfrontiert sehen, melden Sie sich bei uns! Wir verfügen durch unsere Vernetzungen mit anderen Sicherheitsteams über zusätzliche Informationen, z. B. IoCs, die wir jedoch aus Sicherheitsgründen nicht alle öffentlich bereitstellen können. In einigen Fällen dürfen wir solche Informationen allerdings mit Betroffenen teilen. Durch das Übermitteln Ihrer Erfahrungen und Analyseergebnisse können Sie uns außerdem helfen, andere Einrichtungen noch effektiver zu schützen. ◆

PKI: Automatisierung bei Serverzertifikaten unabdingbar

In den vergangenen Jahren hat sich die erlaubte Laufzeit von im Betriebssystem oder Browser verankerten Serverzertifikaten immer weiter verringert: von 39 Monaten im Jahr 2015 über ca. 27 Monate ab Mitte 2018 bis zum jetzigen Stand von etwa 13 Monaten seit 2020.

Anfang März 2023 hat Google nun die Absicht bekannt gegeben, eine weitere Verringerung der Laufzeit auf nur noch 90 Tage durchzusetzen. Ein konkreter Zeitpunkt wurde noch nicht genannt. Es ist aber mit einer Umsetzung in den nächsten ein bis zwei Jahren zu rechnen.

Serverzertifikate können damit praktisch nicht mehr sinnvoll manuell verwaltet werden. Es müssen automatisierbare Werkzeuge zum Einsatz kommen, damit nicht für jede Erneuerung das Eingreifen einer Person notwendig ist. In GÉANT Trusted Certificate Services (TCS) stehen verschiedene Möglichkeiten für die Automatisierung bereit. Es wird ein Zugang über das ACME-Protokoll angeboten, das mit zahlreichen Werkzeugen auf allen Serverplattformen verwendet werden kann, z. B. certbot, acme.sh, das Apache-Module mod_md oder win-acme. Alternativ gibt es in GÉANT TCS ein REST-API, das mit wenig Aufwand in eigene Automatisierungs- oder Konfigurations-Management-Lösungen eingebunden werden kann.

Es gibt auch Szenarien, in denen eine Automatisierung nicht sinnvoll oder möglich ist, und in denen die Eigenschaften der im Browser oder Betriebssystem verankerten Serverzertifikate nicht benötigt werden. Beispiele wären die für die Shibboleth-Kommunikation in der AAI verwendeten Zertifikate oder abgeschottete interne Netzwerkgeräte, auf die nur wenige Personen zugreifen. In diesen Szenarien kann eine Migration auf andere PKIs, für die die Anforderungen der Browser- und Betriebssystemhersteller nicht greifen, eine Lösung sein. Hierfür steht die Community PKI des DFN-Vereins zur Verfügung; auch selbst betriebene interne PKIs können verwendet werden.

Handlungsempfehlung:

1. Automatisieren Sie die Ausstellung und Erneuerung von Serverzertifikaten, wo immer es möglich ist. Nutzen Sie hierfür z. B. GÉANT TCS mit dem ACME-Protokoll oder die REST-API.
2. Prüfen Sie die Anwendungsfälle Ihrer Serverzertifikate. Migrieren Sie schwer oder nicht automatisierbare, geeignete Szenarien auf Spezial-PKIs mit länger gültigen Zertifikaten. Hierfür können intern betriebene PKIs oder die Community PKI genutzt werden.

Es ist dringend anzuraten, die weitere Entwicklung nicht einfach abzuwarten, sondern bereits jetzt Aktivitäten zur Automatisierung oder Migration auf Spezial-PKIs zu starten. ◆

Änderungen bei Nutzerzertifikaten: Migration zu GÉANT TCS und „Baseline Requirements for S/MIME Certificates“

Foto: xtock /Adobe Stock

Ab September 2023 treten die „Baseline Requirements for S/MIME Certificates” des CA/Browser-Forums in Kraft. Dieses fast 90-seitige Dokument reguliert erstmals herstellerübergreifend die Prozesse für die Ausstellung von Zertifikaten für die E-Mail-Kommunikation.

Für die DFN-Teilnehmer bedeutet dies: Ab 30. August 2023 werden neue Nutzerzertifikate nicht mehr in der DFN-PKI „Global“, sondern ausschließlich in GÉANT TCS ausgestellt. Dieser Termin wurde bereits Anfang November 2022 kommuniziert.

Es ist damit zu rechnen, dass sich durch die neue Regulierung des CA/Browser-Forums auch bei den E-Mail-Zertifikaten häufigere Änderungen ergeben werden wie in den vergangenen Jahren bei den Serverzertifikaten. ◆

DFN-AAI: Förderung der Initialisierungsphase des NFDI-Basisdienstes Identity and Access Management (IAM)

Die Konsortialversammlung des NFDI-Vereins (Nationale Forschungsdateninfrastruktur e. V.) beschloss am 31. März 2023 die Förderung des Basisdienstantrags „Identity and Access Management for the German National Research Data Infrastructure (IAM4NFDI)“. Damit wird die sechsmonatige Initialisierungsphase des Dienstes finanziert.

Die Förderung des Basisdienstes erfolgt durch den Verbund der Fachkonsortien Base4NFDI. Dieser erarbeitet Konzepte für eine infrastrukturelle Grundversorgung mit Basisdiensten, die künftig disziplinübergreifend allen Fachkonsortien in der NFDI zur Verfügung stehen.

Der künftige Basisdienst Identity and Access Management (IAM) zielt darauf ab, nachhaltige technische und organisatorische Strukturen für den föderierten Zugriff auf Forschungsdaten und die zu deren Management benötigten Dienste zu schaffen. Dabei müssen Interoperabilität mit sowie Anschlussfähigkeit an andere Infrastrukturen wie die European Open Science Cloud (EOSC) gewährleistet sein. Als Basis hierfür dient eine Authentifizierungs- und Autorisierungsinfrastruktur (NFDI AAI), die in die DFN-AAI integriert werden wird. ◆

Weitere Informationen zur NFDI AAI und zu IAM4NFDI finden Sie unter:
https://doc.nfdi-aai.de

Informationen zu Base4NFDI gibt es hier:
https://base4nfdi.de

KONTAKT

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

Mitarbeit an dieser Ausgabe Sicherheit aktuell:
Jürgen Brauckmann, Tine Kahl, Sascha Kriebitzsch, Wolfgang Pempe

CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?

Die NIS-2-Richtlinie ist am 16. Januar 2023 in Kraft getreten und muss nun vom Gesetzgeber umgesetzt werden

Cyberkriminalität ist schon lange kein Novum mehr. Jährlich nehmen digitale Angriffe immer weiter zu und setzen Behörden und Unternehmen zunehmend unter Druck.[1] Auch die technischen Raffinessen der Angreifer entwickeln sich Jahr für Jahr immer weiter. Aus diesen Gründen sah sich der europäische Richtliniengeber berufen, zunächst mit der Netz- und Informationssicherheitsrichtlinie[2] (NIS-Richtlinie) in der Europäischen Union (EU) ein höheres Niveau an IT-Sicherheit zu schaffen. Doch die Umsetzung zeigte, dass es damit nicht genug ist. Es wurde Zeit für ein juristisches Update, die nun in Kraft getretene NIS-2-Richtlinie. Grund genug, um sich in diesem Beitrag einen Überblick über die Richtlinien und Umsetzungen zu verschaffen, die kommenden Änderungen unter die Lupe zu nehmen und damit einen kleinen Ritt durch das europäische Cybersicherheitsrecht zu wagen.

Text: **Nicolas John** (Forschungsstelle Recht im DFN)

Foto: Heiko119 / iStock

1 Zum Beispiel die vergangenen Emotet-Angriffe, hierzu Uphues, Der Feind in meinem Netz – Teil 1, DFN-Infobrief Recht 1/2020; Uphues, Der Feind in meinem Netz – Teil 2, DFN-Infobrief Recht 2/2020.

2 Richtlinie (EU) 2016/1148 zum Sicherheitsniveau von Netz- und Informationssystemen (NIS-Richtlinie), abrufbar unter **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE** (zuletzt abgerufen am 16.3.2023).

I. NIS-Richtlinie

Im Fokus des europäischen Gesetzgebers steht die Pflicht der Mitgliedstaaten, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen und eine sogenannten Kooperationsgruppe zu schaffen, welche die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten erleichtern soll. Außerdem soll für NOtfälle ein Netzwerk an Computer-Notfallteams (CSIRTs) eingerichtet werden, welche die effiziente Zusammenarbeit zwischen den EU-Mitgliedstaaten fördern und das Vertrauen stärken soll. Dies soll auch mithilfe der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) umgesetzt werden.

Darüber hinaus nimmt die NIS-Richtlinie auch Betreiber verschiedener „wesentlicher Dienste“ aus kritischen Versorgungssektoren in Anspruch. Gemeint sind damit IT-Dienste, welche bei einem Sicherheitsvorfall das öffentliche Leben erheblich einschränken würden und deren Aufrechterhaltung daher unerlässlich ist. Hierzu gehören die Energieversorgung, der Verkehrssektor, das Bankenwesen, Finanzmarktstrukturen, Gesundheitsdienstleister, die Trinkwasserlieferung und -versorgung sowie bestimmte Bereiche der digitalen Infrastruktur (v. a. Knotenpunktbetreiber, DNS-Diensteanbieter und TLD-Name-Registries). Neben den Betreibern der wesentlichen Dienste werden auch Anbieter digitaler Dienste wie Onlinemarktplätze, Onlinesuchmaschinen oder Cloud-Computing-Dienste von der NIS-Richtlinie umfasst. Dagegen sind Anbieter sozialer Netzwerke von dem Anwendungsbereich nicht erfasst. Auch kleine Unternehmen sollen nach den Richtlinienvorgaben nicht von den Regelungen erfasst werden. Diese Betreiber und Anbieter sollen verschiedenen Sicherheitsanforderungen und Meldepflichten unterliegen. So schreibt die Richtlinie in Art. 14 den Betreibern der wesentlichen Dienste vor, dass sie unter Berücksichtigung des Stands der Technik „geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen [müssen], um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen“. Im Falle eines Sicherheitsvorfalles, welcher erhebliche Auswirkungen auf die Verfügbarkeit des bereitgestellten Dienstes hat, haben die Betreiber unverzüglich eine Meldung an die zuständige Behörde[3] vorzunehmen.

Für die Anbieter digitaler Dienste verlangt die NIS-Richtlinie ähnliche Verpflichtungen. Art. 16 NIS-Richtlinie schreibt diesen ebenfalls die Vornahme geeigneter und verhältnismäßiger technischer und organisatorischer Maßnahmen vor, um die Sicherheit der Dienste zu gewähren. Darüber hinaus unterfallen die Anbieter ebenfalls einer Meldepflicht, wenn es zu einem Sicherheitsvorfall kommt.

Um diese Anforderungen an die Betreiber und Anbieter zu koordinieren und zu überwachen, sollen die Mitgliedstaaten entsprechende nationale Behörden und Anlaufstellen benennen. Die NIS-Richtlinie trat 2016 in Kraft.

II. Umsetzung in Deutschland

Europäische Richtlinien haben in den Mitgliedstaaten keine unmittelbare Rechtswirkung. Vielmehr bedarf es eines Umsetzungsakts durch den nationalen Gesetzgeber, welcher die Vorgaben einer Richtlinie in nationales Recht formuliert und das dann unmittelbar Geltung findet. Die NIS-Richtlinie strebt dabei eine sogenannten „Mindestharmonisierung“ an. Das bedeutet, dass die Mitgliedstaaten zwar die Vorgaben der Richtlinie umsetzen müssen, aber darüber hinausgehende Regelungen, mit denen ein höheres Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll, durchaus möglich und zulässig sind.[4] Europaweit soll so ein rechtlicher Mindeststandard geschaffen werden, der nationalrechtlich aber unterschiedlich ausgestaltet werden kann. Die NIS-Richtlinie musste bis Mitte 2018 von den Mitgliedstaaten umgesetzt werden.

Der deutsche Gesetzgeber hatte schon vor Inkrafttreten der NIS-Richtlinie mit dem IT-Sicherheitsgesetz aus dem Jahr 2015 eine Vielzahl der Vorgaben aus der NIS-Richtlinie erfüllt. Insbesondere die Pflichten von Unternehmen im Bereich kritischer Infrastrukturen, ihre informationstechnischen Systeme durch angemessene organisatorische und technische Vorkehrungen abzusichern und Meldepflichten der Unternehmen im Falle von Angriffen oder Störungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte der deutsche Gesetzgeber schon vor Inkrafttreten der NIS-Richtlinie reguliert.

Doch nicht alle Vorgaben aus der NIS-Richtlinie waren durch das damalige IT-Sicherheitsgesetz umgesetzt worden, es fehlten vor allem noch die Regelungen zu den Anbietern von digitalen Diensten. Die fehlenden Anpassungen wurden daher mit dem Umsetzungsgesetz der NIS-Richtlinie im Jahr

3 In Deutschland ist hierfür das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig (s. II.).
4 Art. 3 NIS-Richtlinie.

2017 vorgenommen, welche ab Mai 2018 Geltung in Deutschland fanden.

III. Änderungen der NIS-2-Richtlinie

Doch es zeigte sich schon bald nach Ablauf der Umsetzungsfrist, dass auf europäischer Ebene noch weiterer Anpassungsbedarf besteht. Die Richtlinie wurde in den Mitgliedstaaten sehr unterschiedlich umgesetzt. Insbesondere die „wesentlichen Dienste" wurden unterschiedlich definiert, wodurch die Adressaten der Pflichten in den Mitgliedstaaten stark divergierten. Auch die fehlende Überwachung der Umsetzung der Pflichten stellt in der Praxis einen Schwachpunkt der NIS-Richtlinie dar. Außerdem musste mit Blick auf die weiter wachsenden digitalen Bedrohungen festgestellt werden, dass das von der NIS-Richtlinie festgelegte Niveau der Cyberresilienz zu niedrig war.

Um diese und einige weitere Schwachpunkte der NIS-Richtlinie auszubessern und auf die Zunahmen der weiterentwickelten Cyberangriffe zu reagieren, legte die Europäische Kommission einen Vorschlag zur Änderung der NIS-Richtlinie vor, welcher nach der Einigung mit dem Europäischen Parlament und des Rates in der NIS-2-Richtlinie[5] mündete. Mit diesen Regelungen soll nun die Cybersicherheit in Europa modernisiert und auch im Anwendungsbereich erweitert werden.[6]

Die Änderungen betreffen verschiedene Bereiche. Insbesondere der Anwendungsbereich hat weitreichende Änderungen erfahren. So unterscheidet der europäische Richtliniengeber nun nicht mehr zwischen „wesentlichen" und „digitalen" Diensten, sondern nun zwischen „wesentlichen" und „wichtigen" Diensten.[7] Während aber trotz dieser begrifflichen Anpassung weiterhin alle bisherigen Adressaten von der Einordnung erfasst bleiben, kommen darüber hinaus nun neue Adressaten hinzu.

Zu den wesentlichen Diensten gehören Dienste, welche unter die im Anhang I aufgezählten „Sektoren mit hoher Kritikalität" fallen. So gehört nun z. B. der Sektor „Weltraum" zu den hochkritischen Sektoren, welcher Einrichtungen bezeichnet, die vom Boden aus weltraumbezogene Dienste erbringen. Aber auch der ursprüngliche Sektor der digitalen Infrastruktur wurde erheblich erweitert und ordnet nun z. B. Dienste des Cloud-Computing den besonders kritischen

Infrastrukturen zu und erweitert den Sektor darüber hinaus um Anbieter von Rechenzentrumsdiensten, Betreibern von Inhaltszustellnetzen, Vertrauensdiensteanbietern und um Anbieter öffentlicher elektronischer Kommunikationsnetze bzw. -dienste. Daneben gehören die Verwaltung von Informations- und Kommunikationstechnik-Diensten (IKT-Dienste) und auch die öffentliche Verwaltung nun ebenfalls zu den Sektoren mit hoher Kritikalität.

Wichtige Einrichtungen sind dagegen solche, die unter die in Anhang I oder II genannten Dienste fallen und aufgrund ihrer Größe nicht als wesentliche Einrichtung eingeordnet werden (zu dieser „size-cap-rule" unten mehr). Anhang II der Richtlinie benennt die „sonstigen kritischen Sektoren". Während der europäische Richtliniengeber im Rahmen der digitalen Dienste noch immer Anbieter von Onlinemarktplätzen und -suchmaschinen erfasst, zählen nun auch Anbieter von Plattformen für Dienste sozialer Netzwerke zu den erfassten Sektoren. Außerdem gehören auch Post- und Kurierdienste, die Abfallbewirtschaftung, Unternehmensbereiche mit Bezug zu chemischen Mitteln oder Lebensmitteln, das verarbeitende bzw. herstellende Gewerbe in bestimmten Bereichen wie z. B. Medizinprodukte und die Forschung zu den sonstigen kritischen Sektoren.

Mit der Erweiterung und Detaillierung dieses Adressatenkreises macht der europäische Richtliniengeber seine Ankündigung wahr, den Anwendungsbereich erheblich zu erweitern, um eine breite Verbesserung der Cybersicherheit und -resilienz in Europa zu erreichen.

Neu ist auch die oben schon erwähnte sogenannten „size-cap-rule". Diese legt nun als allgemeine Regel fest, dass große und mittlere Unternehmen, die in einem der oben genannten Sektoren tätig sind, von den Regelungen erfasst werden. Diese allgemeine Regelung korrigiert demnach den Schwachpunkt der ursprünglichen NIS-Richtlinie, welche es den Mitgliedstaaten überließ, die Kriterien festzulegen, wann ein Unternehmen unter die Regelungen fiel. Nach der Definition einer in der Richtlinie benannten Empfehlung der Kommission haben mittlere Unternehmen weniger als 250 Mitarbeitende und einen Jahresumsatz von unter 50 Mio. Euro bzw. eine Jahresbilanz von maximal 43 Mio. Euro. Kleine Unternehmen, welche nicht unter die Adressaten fallen sollen, haben maximal 50 Mitarbeitende und einen Jahresumsatz bzw. eine -bilanz

5 Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L1535&from=DE (zuletzt abgerufen am 16.3.2023).

6 Der Richtliniengeber stellt die Probleme der NIS-Richtlinie ausführlich in seinen Erwägungsgründen dar, vgl. ErwG 2 ff. NIS-2-Richtlinie.

7 S. Art. 3 NIS-2-Richtlinie.

von unter 10 Mio. Euro.[8] Mit dieser Regelung werden die unterschiedlichen Umsetzungen der Mitgliedstaaten verstärkt angeglichen. Dennoch lässt der Richtliniengeber weiterhin Ausnahmen in bestimmten Bereichen zu.

Erneuert wurden nun auch die Pflichten der betroffenen Einrichtungen. Die erfassten wesentlichen und wichtigen Einrichtungen müssen weiterhin ihre Präventionsmaßnahmen i. S. v. technischen und organisatorischen Maßnahmen wie z. B. Backups oder Verschlüsselungstechnologien vornehmen und dabei nationale und internationale Standards einhalten. Von diesen Pflichten sind in der NIS-2-Richtlinie nun auch ausdrücklich Lieferketten umfasst.

Weiterhin gelten umfangreiche Meldevorgaben im Falle von erheblichen Sicherheitsvorfällen. Dabei gilt ein Sicherheitsvorfall als erheblich, wenn er entweder „schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann“.[9] Bezüglich dieser Meldepflichten macht der Richtliniengeber nun detailliertere Vorgaben als noch in der NIS-Richtlinie. So gibt der europäische Gesetzgeber ein gestuftes Meldevorgehen vor, nach dem nach spätestens 24 Stunden nach Kenntnisnahme eines erheblichen Sicherheitsvorfalls eine Frühwarnung abzugeben ist und nach spätestens 72 Stunden nach Kenntnisnahme des Sicherheitsvorfalls eine erste Bewertung einschließlich des Schweregrads und seiner Auswirkungen vorgenommen werden muss. Spätestens einen Monat nach Übermittlung der Bewertung des Falls muss außerdem ein Abschlussbericht vorgelegt werden.
Auch die Mitgliedstaaten werden mehr in die Pflicht genommen. Insbesondere die Umsetzung der Cybersicherheitsstrategie und die Anforderungen an die nationalen Aufsichtsbehörden werden in der NIS-2-Richtlinie weiter vertieft. Außerdem gehört es nun zu den Aufgaben der Computernotfallteams, auf Anfrage proaktiv Schwachstellenscans vorzunehmen. Zudem soll die ENISA eine Schwachstellendatenbank aufbauen, um den Mitgliedstaaten schnelleren Zugang zu den erforderlichen Informationen zu verschaffen. Neu sind auch mitgliedsstaatliche Peer-Reviews zur Cybersicherheit.

Verschärft wurden auch die Aufsichts- und Durchsetzungsbefugnisse der nationalen Behörden. Demnach sind neben Warnungen auch Zwangsgelder oder der Ausschluss von Leitungspersonen betroffener Einrichtungen möglich. Außerdem sind Maßnahmen wie Vor-Ort-Kontrollen, Stichproben, Sicherheitsaudits oder die Anforderung von Daten oder Zugängen möglich. Zudem wurden in der Richtlinie umfangreiche Vorgaben zu den Geldbußen festgelegt. So soll der nationale Gesetzgeber bei einem Verstoß einer wesentlichen Einrichtung gegen ihre Pflichten mindestens 10 Mio. Euro oder mindestens 2 Prozent des Vorjahresumsatzes des betroffenen Unternehmens als Höchstbetrag in seiner Umsetzung festsetzen. Bei Verstößen von wichtigen Einrichtungen sollen die Höchstbeträge mindestens 7 Mio. Euro oder 1,4 Prozent des Vorjahresumsatzes im nationalen Umsetzungsgesetz betragen.

Die neue NIS-2-Richtlinie ist am 16. Januar 2023 in Kraft getreten. Die Mitgliedstaaten haben nun bis Oktober 2024 Zeit, die Vorgaben in nationales Recht umzusetzen.

IV. Umsetzungsbedarf in Deutschland

Während die europäischen Institutionen die Überarbeitung der NIS-Richtlinie in die Wege leiteten, war der deutsche Gesetzgeber ebenfalls nicht untätig. Schon vor Inkrafttreten der NIS-2-Richtlinie wurde das IT-Sicherheitsgesetz überarbeitet und trat in seiner neuen Form 2021 in Kraft.

Die Änderungen des sogenannten „IT-Sicherheitsgesetzes 2.0“ betrafen vor allem die Pflichten von Betreibenden kritischer Infrastrukturen (KRITIS-Betreiber) wie z. B. Energie- oder Telekommunikationsunternehmen und Unternehmen im besonderen öffentlichen Interesse (UNIBÖFI), z. B. Unternehmen der Rüstungs- oder Chemieindustrie aus dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Der deutsche Gesetzgeber hatte schon in diesem Gesetzgebungsakt festgelegt, dass auch Zulieferer in den Anwendungsbereich der neuen Regelungen fallen können.

UNIBÖFIs müssen nach diesen Regelungen eine Selbsterklärung über ihre Maßnahmen zum Schutz der IT-Sicherheit vornehmen und sich beim BSI registrieren. In diesem Gesetzesakt wurde aber auch der Begriff der KRITIS-Betreiber um beispielsweise die Abfallentsorgung erweitert. Außerdem müssen sich KRITIS-Betreiber ebenfalls beim BSI registrieren, den Einsatz bestimmter IT-Produkte anzeigen und Programme für die Erkennung von Cyberangriffen verwenden. Im Falle eines Sicherheitsvorfalls müssen beide Kategorien der Betreiber dem

8 Vgl. Empfehlung der Kommission 2003/361/EG.
9 Art. 23 Abs. 3 NIS-2-Richtlinie.

BSI den Vorfall melden und entsprechende Daten zur Verfügung stellen.

Politisch umstritten war insbesondere die Regelung über die Verwendung sogenannter „kritischer Komponenten“, welche der Gesetzgeber bestimmen kann. Grund für die Diskussionen war der Umgang mit Bauteilen des chinesischen IT-Unternehmens Huawei. Nach dem BSIG kann der Einsatz solcher Komponenten verboten werden, wenn die Befürchtung besteht, dass die Verwendung die öffentliche Sicherheit und Ordnung beeinträchtigen kann. Dies kann z. B. der Fall sein, wenn der Hersteller von der Regierung eines Drittstaates kontrolliert wird. Der Einsatz dieser kritischeren Komponenten muss von dem Betreiber vor der Verwendung beim BSI angezeigt werden.

Durch diese umfangreiche Modernisierung der deutschen Sicherheitsgesetze erfüllt der Gesetzgeber schon Teile der NIS-2-Richtlinie und geht partiell wieder darüber hinaus. Allerdings fehlen auch noch Umsetzungsvorgaben, beispielsweise einige der in der Richtlinie benannten Sektoren wie die Raumfahrt, die öffentliche Verwaltung oder die Forschung. Soweit die Vorgaben der Richtlinie im deutschen Recht noch nicht umgesetzt sind, wird der Gesetzgeber mit einem „IT-Sicherheitsgesetz 3.0“ die erforderlichen Änderungen vor Ablauf der Umsetzungsfrist vornehmen müssen.

V. Auswirkungen in der Praxis und Fazit

Schon jetzt sind viele Unternehmen in Deutschland von den Pflichten aus der NIS-Richtlinie und den erweiterten Vorgaben des IT-Sicherheitsgesetzes 2.0 betroffen.[10] Doch dass die Umsetzung der Vorgaben in den Unternehmen dringend erforderlich ist, zeigen die regelmäßigen Cyberangriffe auf verschiedenste Einrichtungen. Die Erhöhung des Schutzniveaus in der Cybersicherheit ist daher von großer Bedeutung.

Aus diesen Gründen wird auch die vollständige Umsetzung der NIS-2-Richtlinie als zu erwartendes IT-Sicherheitsgesetz 3.0 vor allem für Unternehmen, aber auch für entsprechende öffentliche Einrichtungen große Herausforderungen bedeuten. Zwar sieht die NIS-2-Richtlinie für Einrichtungen der öffentlichen Verwaltung Einschränkungen vor,[11]

allerdings wird dem deutschen Gesetzgeber ein großer Spielraum eingeräumt, welche Einrichtungen der öffentlichen Verwaltung schließlich unter den Anwendungsbereich des Umsetzungsgesetzes fallen sollen.[12]

Nicht alle Bereiche der Forschung werden sich ganz neu mit den Anforderungen an die Cybersicherheit konfrontiert sehen. Schon jetzt fallen z. B. Universitätskliniken als Gesundheitseinrichtungen unter den Katalog der derzeit geltenden BSI-Kritisverordnung. Dennoch wird für viele Forschungseinrichtungen und Hochschulen erstmalig neben dem Sektor der öffentlichen Verwaltung insbesondere der neue Sektor der Forschung von Relevanz sein. Forschungseinrichtungen werden in der NIS-2-Richtlinie als Einrichtungen definiert, „deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschließt.“ Letztendlich bleibt hierbei abzuwarten, welche Einrichtungen vom IT-Sicherheitsgesetz 3.0 tatsächlich unter den Sektoren der öffentlichen Verwaltung oder der Forschung erfasst werden. Auch in Bezug auf Bildungseinrichtungen lässt die Richtlinie den Mitgliedstaaten Freiheiten. Insoweit obliegt es auch der Entscheidung des deutschen Gesetzgebers, Bildungseinrichtungen in den Anwendungsbereich einzubeziehen, insbesondere, wenn sie kritische Forschungstätigkeiten durchführen.[13]

Der Forschungsbereich wird in der Richtlinie auch noch anderweitig relevant, denn die Richtlinie sieht im Rahmen der Vorgaben zur nationalen Cybersicherheitsstrategie vor, dass Forschungs- und Entwicklungsinitiativen im Bereich der Cybersicherheit umfasst werden müssen.[14] Außerdem müssen Hochschul- und Forschungseinrichtungen bei der Entwicklung und der Verbesserung des Einsatzes von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur unterstützt werden.[15]

Letztendlich stellt die NIS-2-Richtlinie eine sehr viel stärkere Konkretisierung und Erweiterung der bisherigen Vorgaben der NIS-Richtlinie dar. Der europäische Gesetzgeber zeigt seinen Willen, die Cybersicherheit in Europa zu vereinheitlichen und durch eine enge Zusammenarbeit der Mitgliedstaaten zu verbessern. Ob ihm das schlussendlich gelingt, hängt von den nun zu erwartenden Umsetzungsgesetzen der Mitgliedstaaten ab. ◆

10 Die erfassten Einrichtungen sind in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) benannt.
11 Vgl. Art. 3 Abs. 1 lit. d, Art. 2 Abs. 2 lit. f NIS-2-Richtlinie.
12 Art. 2 Abs. 2 lit. f, Abs. 5 lit. a NIS-2-Richtlinie.
13 Art. 2 Abs. 5 lit. b NIS-2-Richtlinie.
14 Art. 7 Abs. 1 lit. f NIS-2-Richtlinie.
15 Art. 7 Abs. 1 lit. g NIS-2-Richtlinie.

Datenschutz auf Rezept

DSK veröffentlicht Hinweise zur datenschutzkonformen Forschung mit Gesundheitsdaten

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat eine Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung veröffentlicht.[1] Dabei hat sie konkrete Empfehlungen gegeben, die bei der Verarbeitung von Gesundheitsdaten zu Forschungszwecken zu beachten sind, und nannte weitere Hinweise zur Erfüllung der gesetzlichen Anforderungen aus der Datenschutz-Grundverordnung (DSGVO).

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

Foto: spxChrome/iStock

1 Abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/104DSK-Petersberger-Erklaerung.pdf;jsessionid=767CAA5A244C12FBAF2D09268FC67D1F.intranet241?__blob=publicationFile&v=1 (zuletzt abgerufen am 18.01.2023).

I. Der datenschutzrechtliche Schutz von Gesundheitsdaten für Forschungszwecke

Die DSGVO regelt die Anforderungen an den Schutz von personenbezogenen Daten im Rahmen einer Datenverarbeitung. Hierbei werden spezielle Datenkategorien als besonders sensibel und daher schützenswert erachtet. Für deren Verarbeitung gelten folglich höhere Anforderungen. Eine dieser Kategorien stellt auch diejenige der Gesundheitsdaten dar.[2] Diese werden in Art. 4 Nr. 15 DSGVO als personenbezogene Daten definiert, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Die höheren Anforderungen, die für die Verarbeitung von Gesundheitsdaten gelten sollen, werden in Art. 9 DSGVO zum Ausdruck gebracht. Gemäß Art. 9 Abs. 1 DSGVO ist eine Datenverarbeitung von Gesundheitsdaten grundsätzlich verboten. Ausnahmsweise soll eine Datenverarbeitung erlaubt sein, sofern eine der in Art. 9 Abs. 2 DSGVO normierten Ausnahmen vorliegt. Diese sind strenger als die Voraussetzungen, die gemäß Art. 6 DSGVO für die generelle Verarbeitung von personenbezogenen Daten gelten sollen. Art. 9 DSGVO erlaubt etwa die Verarbeitung von Gesundheitsdaten, sofern eine ausdrückliche Einwilligung von der betroffenen Person erteilt wurde (Art. 9 Abs. 2 lit. a DSGVO) oder sofern die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person durchgeführt wurde (Art. 9 Abs. 2 lit. c DSGVO).

II. Privilegierung von Datenverarbeitungen zu Forschungszwecken

Erfolgt die Datenverarbeitung zu wissenschaftlichen Zwecken, ist darüber hinaus jedoch auch zu beachten, dass die DSGVO solche Verarbeitungen grundsätzlich privilegiert. Die grundsätzliche Besserstellung von Datenverarbeitungen zu Forschungszwecken bringt die DSGVO an verschiedenen Stellen zum Ausdruck. Gemäß Art. 14 Abs. 5 lit. b DSGVO kann etwa unter anderem für Forschungsarbeiten die Informationspflicht bezüglich der betroffenen Person bei Datenverarbeitungen entfallen. Auch sieht Art. 89 Abs. 2 DSGVO eine Öffnungsklausel vor, die es den Mitgliedstaaten erlaubt, die datenschutzrechtlichen Betroffenenrechte einzuschränken, sofern durch diese die Forschung ernsthaft beeinträchtigt wird. Sofern bei der datenschutzrechtlichen Bewertung einer Datenverarbeitung keine konkrete Privilegierung aus der DSGVO greift, kann im Rahmen einer Interessensabwägung dennoch zu beachten sein, dass Datenverarbeitungen zu Forschungszwecken durch die DSGVO grundsätzlich privilegiert werden und daher im konkreten Fall das Interesse des wissenschaftlichen Datenverarbeiters besonders schwer wiegt.

III. Die Empfehlungen der DSK

Dieser gegensätzlichen Gesichtspunkte, die im Rahmen der Forschung mit Gesundheitsdaten zu beachten sind, war sich die DSK bei der Formulierung der Petersberger Erklärung bewusst. So weist sie einerseits einleitend darauf hin, dass die Forschung einen hohen medizinischen Erkenntnisgewinn bringen könne, der im Interesse der Allgemeinheit liege. Andererseits erkennt sie auch, dass die DSGVO Gesundheitsdaten als besonders sensibel erachtet. Die Empfehlungen der DSK können daher dabei helfen, im konkreten Fall die Interessen in Einklang miteinander zu bringen.

Dazu formuliert die DSK sieben Empfehlungen zur Verarbeitung von Gesundheitsdaten in der Forschung. Diese Empfehlungen werden durch anschließende Erläuterungen ergänzt. Teilweise weisen diese Empfehlungen Elemente grundlegender Natur auf. So weist Empfehlung 1 darauf hin, dass die Menschen im Mittelpunkt der Datenverarbeitung stehen und nicht zum bloßen Gegenstand der Forschung gemacht werden sollen. Hierzu soll die betroffene Person auch über den rechtlichen Rahmen hinaus in die Verarbeitung eingebunden werden. Die Einbindung könne durch digitale Managementsysteme erfolgen. In den weiteren Ausführungen weist die DSK darauf hin, dass es betroffenen Personen grundsätzlich möglich sein muss, der Datenverarbeitung voraussetzungslos zu widersprechen. Allgemeine Natur hat auch die zweite Empfehlung. Sie gibt den Grundsatz wieder, dass Daten umso umfangreicher genutzt werden können, je höher der Schutz durch geeignete Garantien und Maßnahmen ist. Die dritte Empfehlung nennt als solche konkreten Maßnahmen: die Verschlüs-

2 Vgl. hierzu Mc Grath, Zu Risiken und Nebenwirkungen fragen Sie Ihren Arzt oder Verantwortlichen, DFN-Infobrief Recht 04/2020.

selung, Pseudonymisierung durch eine Vertrauensstelle und die frühestmögliche Anonymisierung. Anonyme Datensätze könnten umfassend durch die Forschung genutzt werden.[3] Mit dieser Empfehlung gibt die DSK lediglich Anforderungen wieder, die sich bereits unmittelbar aus Art. 32 DSGVO ergeben. In den weiteren Erläuterungen konkretisiert die DSK noch die Angaben zur Anonymisierung: Könne der Zweck der Forschung auch mit anonymisierten Daten erreicht werden, so dürfen lediglich solche genutzt werden.

Die vierte Empfehlung beschäftigt sich mit Datenverarbeitungen, bei denen die Datensätze aus unterschiedlichen Quellen stammen und beim Datenverarbeiter verknüpft werden. Durch eine Verknüpfung der Daten sei es einfacher möglich, die betroffene Person zu identifizieren. Nach Einschätzung der DSK liege deshalb ein besonders schwerwiegender Eingriff in die Rechte der betroffenen Person vor, sodass höhere Schutzanforderungen gelten sollen. Durch geeignete Verfahren gilt es sicherzustellen, dass betroffenen Personen der Zugang zu ihren Daten gewährt wird. Durch die Einrichtung besonderer Verfahren müsse garantiert werden, dass die Zusammenführung nur anlassbezogen und temporär erfolge. Durch ein Einwilligungsmanagementsystem erhalten betroffene Personen die Möglichkeit, bei Kenntnis der Risiken der Zusammenführung aktiv zuzustimmen. Besonders konkret ist die Petersberger Erklärung in ihrer fünften Empfehlung. In dieser fordert sie die Einrichtung eines zentralen Registerverzeichnisses durch die Verantwortlichen.[4] Diese sollen hierfür auch verbindliche Qualitätsanforderungen vorgeben. Durch ein solches sollen mehrfache Datensammlungen vermieden werden, auch wenn die Gesundheitsdaten in verschiedenen Registern gespeichert sind. Hierdurch soll auch die Datensammlung transparenter gestaltet sein. Parallel zum Registerverzeichnis wird auch die Schaffung einer zentralen koordinierenden Stelle gefordert. Diese soll Anträge (durch Dritte) zur Nutzung der Gesundheitsdaten veröffentlichen und die Nutzenden dazu verpflichten, die Forschungsergebnisse in anonymer Form zu veröffentlichen. Die letzten beiden Empfehlungen richten sich nicht an Datenverarbeiter selbst. In der sechsten Empfehlung regt die DSK eine gesetzliche Regelung des Forschungsgeheimnisses an, durch das der Umgang mit Forschungsdaten auch aus strafrechtlicher und prozessualer Sicht klargestellt werden soll. Die siebte Empfehlung befasst sich mit der Kontrolle durch die Datenschutzbehörden. Diese sollten standardisierte Anforderungen, insbesondere an die Dokumentation der Verarbeitungsprozesse, festlegen.

IV. Relevanz für Hochschulen

Da sich die Erklärung des DSK unmittelbar mit Datenverarbeitungen zu Forschungszwecken beschäftigt, weist sie eine hohe Relevanz für Hochschulen und andere wissenschaftliche Einrichtungen auf, die Gesundheitsdaten verarbeiten. Im Rahmen der aufgezeigten gegensätzlichen Interessenlage kann die Petersberger Erklärung die datenschutzrechtliche Bewertung der Forschung von Gesundheitsdaten erleichtern. Die Erklärung weist keine verbindliche Natur auf. Da die DSK sich aber aus allen Datenschutzbeauftragten der Länder und dem Bundesdatenschutzbeauftragten zusammensetzt, kommt der Erklärung ein hohes Gewicht zu. Besondere Hilfestellung gibt die Erklärung, sofern sie konkrete Hinweise gibt, die nicht lediglich eine Wiedergabe gesetzlich normierter Pflichten darstellen. Insbesondere sind die Ausführungen zu erhöhten Schutzanforderungen bei der Verknüpfung unterschiedlicher Datensätze zu beachten. Hohe Relevanz weist auch die Forderung auf, ein zentrales Registerverzeichnis zu schaffen, um Datennutzung transparent zu gestalten und mehrfache Datensammlungen zu verhindern. Konkret in der Praxis lässt sich auch die Forderung umsetzen, eine zentrale Stelle für Datennutzungsanträge zu schaffen. ◆

3 Vgl. hierzu Haserück/Kurz, Gesundheitsdaten: Wie man datenschutzkonform und effektiv forschen kann, Deutsches Ärzteblatt 48/2022, abrufbar unter https://www.aerzteblatt.de/archiv/228698/Gesundheitsdaten-Wie-man-datenschutzkonform-und-effektiv-forschen-kann (zuletzt abgerufen am 18.01.2023).

4 Das Führen von medizinischen Registerverzeichnissen ist bereits üblich. So existiert etwa das Deutsche Register Klinischer Studien als anerkanntes Primärregister für die Registrierung von in Deutschland durchgeführten patientenorientierten klinischen Studien. Auch betreibt das RKI beispielsweise ein Zentrum für Krebsregisterdaten, in dem die anonymisierten Daten der Landeskrebsregister auf Bundesebene zusammengeführt werden; vgl. zur datenschutzkonformen Verarbeitung von Gesundheitsdaten durch ein Krebsregister auch das Urteil des VG Hamburg vom 28.7.2022 (AZ 21 K 1802/21).

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.

Im eduroam-Team des DFN-Vereins arbeitet Jan-Frederik Rieckers daran, die Infrastruktur des beliebten Dienstes in puncto Sicherheit stetig zu optimieren. Dafür führte ihn seine bisher am weitesten entfernte Dienstreise …

… zum Frühjahrstreffen der Internet Engineering Task Force (IETF), die vom 25. bis 31. März 2023 in Yokohama (Japan) stattfand.

Dreimal im Jahr treffen sich Fachleute aus aller Welt an immer wechselnden Orten, „to make the Internet work better“, so das Motto des offiziellen IETF-Mission-Statements RFC 3935. In diesem Frühjahr durfte ich diese Mission unterstützen und dafür einmal um die halbe Welt reisen: Die IETF 116 mit dem traditionell dazugehörigen Hackathon am vorherigen Wochenende fand dieses Mal in Japan statt. Gastgeber war WIDE (Widely Integrated Distributed Environment), ein japanisches Internetprojekt, in dem sich diverse Hochschulen und Unternehmen für eine gute Infrastruktur engagieren.

Bei der Ankunft in Tokyo Haneda erlebe ich schon sehr bald einen Kulturschock. Die Schrift ist komplett anders, mal eben etwas in den Übersetzer eintippen ist hier nicht. Auch mit Englisch komme ich nicht so weit. Nach der anfänglichen Orientierungslosigkeit finde ich endlich meinen Weg zum Bahnhof und nehme die Keikyū Line zum Hotel in Yokohama. Dort angekommen muss ich erst mal mit meinem Jetlag fertig werden, acht Stunden Zeitverschiebung zehren doch ordentlich an den Kräften.

Der erste Tag ist verregnet und recht stürmisch. Für mich als Wahl-Bremer das perfekte Wetter, ich fühle mich direkt wie zu Hause. Aber vom Wetter bekomme ich am Wochenende sowieso nicht viel

Für ein gutes Internet: Alan DeKok von FreeRADIUS und Jan-Frederik Rieckers vom DFN fachsimpeln über Designentscheidungen und Implementierungsdetails einer neuen EAP-Methode (von links) | *Fotos: IETF*

mit, denn das ist dem Hackathon gewidmet. 363 Personen haben sich vor Ort dafür angemeldet, der Raum ist voll. Ich sitze in einer Ecke und arbeite an einer Idee für eine neue EAP-Methode. Am Sonntag tausche ich mich mit Alan DeKok, dem Hauptentwickler von FreeRADIUS, über einige Designentscheidungen und Implementierungsdetails der Methode aus.

Die eigentliche Konferenz startet am Montag und pünktlich dazu klart das Wetter auf und die Sonne zeigt sich. Und dann kann ich auf dem Weg vom Hotel zum Konferenzzentrum auch eine saisonale Attraktion Japans beobachten: die berühmte Kirschblüte. Auf meiner täglichen Route komme ich an unzähligen, in voller Blüte stehenden Kirschbäumen vorbei – ein sehr beeindruckender Anblick. Beim Social Event am Donnerstagabend wird in traditionell japanischer Art auf der Bühne ein Blumenarrangement mit Kirschblüten zusammengesteckt. Außerdem habe ich die Möglichkeit, einen kalligrafierten japanischen Spruch als Souvenir mitzunehmen.

Zwischen Kirschblüte und Hackathon: Neben seinem Einsatz für das Internet bleibt auch ein wenig Zeit für Sightseeing | *Fotos: Jan-Frederik Rieckers, DFN*

Doch nun zum eigentlichen Zweck der Reise: Die IETF produziert Internetstandards in verschiedenen Kategorien. Und genau um diese Kategorien ging es für mich. Der 2012 verabschiedete RFC 6614, der den RadSec-Standard beschreibt, ist noch im Status „Experimental". Dieser Status wird gern für neue Protokolle genutzt. So können zunächst Erfahrungen gesammelt werden, bevor die Spezifikation final festgeschrieben wird. Etwas mehr als zehn Jahre später ist das Protokoll nun weit ausgerollt und es gibt eine Vielzahl von Implementierungen, die diesen Standard umsetzen. Und das heißt: Es wird Zeit, die Kategorie zu ändern: vom „Experimental"- zum „Proposed"-Standard. Das erfordert allerdings ein neues Dokument. In diesem Zuge kann man auch gleich noch weitere Punkte ändern oder erweitern, die in den vergangenen zehn Jahren aufgefallen sind.

Da der DFN-Verein dieses Protokoll schon lange einsetzt, habe ich mich für diese Aufgabe freiwillig gemeldet und schon zur IETF 115 im November in London einen ersten Entwurf fertiggestellt. Dort hatten sich Entwicklerinnen und Entwickler verschiedener RADIUS-Software zusammengetan, um eine Working-Group namens „radext" (RADIUS EXTensions) wiederzubeleben. In einer sogenannten Birds-of-a-Feather (BoF)-Session wurde die Zielrichtung der Gruppe diskutiert, die neue Charter wurde kurz vor der IETF 116 in Yokohama von der Internet Engineering Steering Group (IESG) bestätigt. Neben der Änderung der Kategorie stehen auch weitere Änderungen des RADIUS-Protokolls an, z. B. um die Nutzung von MD5 in der Berechnung der Pakete endlich loszuwerden.

Bei der radext-Session am Dienstag sind weder vor Ort noch remote viele Menschen beteiligt. Trotzdem machen wir Fortschritte, diskutieren über einige technische Aspekte und legen die weiteren Schritte fest. Denn wir wollen schon im Herbst 2023 die ersten Dokumente finalisieren. Ein strammer Zeitplan, der von allen Beteiligten viel Einsatz erfordert, vor allem nach der Konferenz, wenn die Diskussionen auf der Mailingliste fortgeführt werden.

Auf dem Rückflug nach Deutschland versuche ich zu entspannen und zu schlafen. Ich freue mich schon auf die nächsten Meetings. Und auch wenn es viel Kraft und Zeit kostet, freue ich mich besonders, dass ich meinen Teil dazu beitragen kann, „to make the Internet work better". ◆

DFN live: Wissen teilen, Erfahrungen weitergeben

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

DFN-Betriebstagung

Wir stellen wieder einmal fest: Die DFN-Community ist die beste und vor allem treueste Gemeinschaft der Welt! Trotz eines bundesweiten Warnstreiks der Gewerkschaften ver.di und EVG am ersten Veranstaltungstag der 78. DFN-Betriebstagung (BT), die vom 28. bis 29. März 2023 stattfand, ließen die Teilnehmenden nichts unversucht, um pünktlich nach Berlin zu kommen. So wurden Fahrgemeinschaften gebildet und ein Teil reiste bereits am Sonntag an. Zum Start am Montag im Leonardo Royal Hotel Berlin Alexanderplatz gab es gut gefüllte Stuhlreihen, gut gelaunte Gesichter und jede Menge Wiedersehensfreude. Insgesamt 234 Teilnehmende waren vor Ort, 102 Leute schauten sich die Plenumsvorträge per Stream an. Auch die Foren waren gut besucht und boten neben Diskussionen viele Neuigkeiten, Infos und Anregungen aus der DFN-Community.

TERMIN

Die 79. DFN-Betriebstagung findet am Dienstag und Mittwoch, **17. und 18. Oktober 2023,** statt.

Lernen, austauschen, Kontakte pflegen: Zweimal im Jahr trifft sich die DFN-Community zur Betriebstagung in Berlin | *Fotos: Nina Bark, DFN*

Auf die kommenden 30 Jahre: Seit 1993 unterstützt und berät das DFN-CERT die Teilnehmer im Deutschen Forschungsnetz in allen Belangen der IT-Sicherheit
Fotos: Nina Bark, DFN

DFN-Konferenz „Datenschutz“

Am 29. und 30. November 2022 fand die 9. DFN-Konferenz „Datenschutz“ im Hotel Hafen Hamburg an den Landungsbrücken statt. Die hybride Veranstaltung zählte 117 Teilnehmende – davon 68 in Präsenz und 49 online zugeschaltet.

Im Auftrag des DFN-Vereins veranstaltet das DFN-CERT seit 2012 die DFN-Konferenz „Datenschutz“. Mit der Veranstaltung kommt der DFN-Verein dem Bedarf von Forschungs- und Wissenschaftseinrichtungen an rechtlicher Unterstützung bei der Umsetzung von Datenschutz nach. Die DFN-Konferenz fördert den Austausch zwischen den für die Einhaltung des Datenschutzes verantwortlichen Personen und bietet die Möglichkeit, Anforderungen mit Vertreterinnen und Vertretern der Datenschutzaufsichtsbehörden sowie mit den eingeladenen Expertinnen und Experten aus der Datenschutzpraxis ausführlich zu diskutieren.

DFN-Konferenz „Sicherheit in vernetzten Systemen“

3 Tage, 20 Vorträge und über 285 Teilnehmende – die Jubiläumsveranstaltung der 30. DFN-Konferenz „Sicherheit in vernetzten Systemen“ fand am Donnerstag und Freitag, 9. und 10. Februar 2023, im Grand Elysée Hotel Hamburg statt und wurde vom DFN-CERT im Auftrag des DFN-Vereins ausgerichtet. Sie bot ein vielfältiges Programm aus technischen und wissenschaftlichen Themen rund um Informationssicherheit: von Security Awareness über E-Mail-Tracking und -Profiling bis hin zu Cyber Threat Intelligence. Und auch das Blue Team Training am Vormittag des ersten Konferenztages war schnell ausgebucht. In dem praxisnahen Format konnten System- und Netzwerkadministrierende, die wenig oder keine Erfahrungen in der Angriffserkennung und -bekämpfung haben, verschiedene Methoden erlernen und mit diesen den simulierten Ernstfall in einer gesicherten Umgebung üben.

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

TERMIN

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

TERMIN

Die 10. DFN-Konferenz „Datenschutz“ findet am **Dienstag und Mittwoch, 28. und 29. November 2023,** in Hamburg statt.

DFN-Mitgliederversammlung

Eine der Stärken des DFN-Vereins ist das breite Mandat seiner Mitglieder. Mit über 350 institutionellen Mitgliedern engagieren sich die Mehrzahl der deutschen Hochschulen und Forschungseinrichtungen sowie forschungsnahe Wirtschaftsunternehmen im DFN-Verein. Die Mitgliedsvertreterinnen und -vertreter treffen sich zweimal jährlich, um gemeinsam die Zukunft des DFN-Vereins zu gestalten.

Die 85. Mitgliederversammlung fand am Mittwoch, 14. Dezember 2022, das erste Mal nach der COVID-19-Pandemie wieder im Wissenschaftszentrum in Bonn statt. Der gesellige Vorabend, der üblicherweise der Kontaktpflege und dem Vernetzen vorbehalten ist, startete mit einer Neuerung: Im Rahmen einer interaktiven Infoveranstaltung stellten die DFN-Mitarbeitenden sich und ihre Arbeit persönlich vor. Besonders neue Mitgliedsvertretende hatten so die Gelegenheit, den DFN-Verein kennenzulernen, sich über Neuigkeiten rund um das Wissenschaftsnetz und seine Dienste zu informieren und alle Fragen zu stellen, die ihnen am Herzen lagen. Gut angenommen wurde der Teleroboter, mit dessen Hilfe die Teilnehmenden mit DFN-Mitarbeitenden ins Gespräch kommen konnten, die nicht vor Ort waren.

Die Leitung steht: Die DFN-Kollegen Jakob Tendel (per Teleroboter) und Dirk Bei der Kellen besprechen letzte Details vor der Infoveranstaltung am Vorabend der Mitgliederversammlung | *Foto: Nina Bark, DFN*

TERMIN

Die 86. Mitgliederversammlung und der Vorabendempfang finden am **Montag und Dienstag, 12. und 13. Juni 2023**, statt.

Die 87. Mitgliederversammlung und der Vorabendempfang finden am **Dienstag und Mittwoch, 12. und 13. Dezember 2023,** statt.

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

Überblick DFN-Verein

(Stand: 05/2023)

Fotos: jackijack / fotolia

Laut Satzung fördert der DFN-Verein die Schaffung der Voraussetzungen für die Errichtung, den Betrieb und die Nutzung eines rechnergestützten Informations- und Kommunikationssystems für die öffentlich geförderte und gemeinnützige Forschung in der Bundesrepublik Deutschland. Der Satzungszweck wird insbesondere verwirklicht durch Vergabe von Forschungsaufträgen und Organisation von Dienstleistungen zur Nutzung des Deutschen Forschungsnetzes.

Als Mitglieder werden juristische Personen aufgenommen, von denen ein wesentlicher Beitrag zum Vereinszweck zu erwarten ist oder die dem Bereich der institutionell oder sonst aus öffentlichen Mitteln geförderten Forschung zuzurechnen sind. Sitz des Vereins ist Berlin.

Die Geschäftsstelle

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

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

Die Organe

Mitgliederversammlung
Die Mitgliederversammlung ist u. a. zuständig für die Wahl der Mitglieder des Verwaltungsrates, für die Genehmigung des Jahreswirtschaftsplanes, für die Entlastung des Vorstandes und für die Festlegung der Mitgliedsbeiträge. Derzeitiger Vorsitzender der Mitgliederversammlung ist Prof. Dr. Gerhard Peter, Hochschule Heilbronn.

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

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

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

Prof. Dr. Frank Jenko
(Technische Universität München)

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

Prof. Dr. Odej Kao
(Technische Universität Berlin)

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

Dr. Karl Molter
(Hochschule Trier)

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

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

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

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

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

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

Der Verwaltungsrat hat als ständige Gäste

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

eine Vertreterin der Hochschulkanzlerinnen und -kanzler:
Dr. Andrea Bör
(Kanzlerin der Freien Universität Berlin)

einen Vertreter der Kultusministerkonferenz:
Jürgen Grothe
(SMWK Dresden)

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

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

Vorstand
Der Vorstand des DFN-Vereins im Sinne des Gesetzes wird aus dem Vorsitzenden und den beiden stellvertretenden Vorsitzenden des Verwaltungsrates gebildet. Derzeit sind dies:

Prof. Dr. Odej Kao
Vorsitz

Dr. Rainer Bockholt
Stellv. Vorsitzender

Christian Zens
Stellv. Vorsitzender

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

Der Vorstand bedient sich zur Erledigung laufender Aufgaben einer Geschäftsstelle mit Standorten in Berlin und Stuttgart. Sie wird von einer Geschäftsführung geleitet. Als Geschäftsführer wurden vom Vorstand Dr. Christian Grimm und Jochem Pattloch bestellt.

Die Mitgliedseinrichtungen

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Technische Hochschule Aschaffenburg
Augsburg	Hochschule für angewandte Wissenschaften, Fachhochschule Augsburg
	Universität Augsburg
Bad Homburg	NTT Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	Berlin-Brandenburgische Akademie der Wissenschaften
	Berliner Institut für Gesundheitsforschung/Berlin Institute of Health
	Berliner Hochschule für Technik (BHT)
	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
	Bundesanstalt für Materialforschung und -prüfung
	Bundesinstitut für Risikobewertung
	Deutsche Telekom AG Laboratories
	Deutsche Telekom IT GmbH
	Deutsches Herzzentrum Berlin
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	European School of Management and Technology GmbH (ESMT)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin (FUB)
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hertie School gGmbH
	Hochschule für Technik und Wirtschaft – University of Applied Sciences
	Hochschule für Wirtschaft und Recht
	Humboldt-Universität zu Berlin (HUB)
	International Psychoanalytic University Berlin
	IT-Dienstleistungszentrum
	Museum für Naturkunde
	NOW GmbH Nationale Organisation Wasserstoff- und Brennstoffzellentechnologie
	Robert Koch-Institut
	Stanford University in Berlin
	Stiftung Deutsches Historisches Museum
	Stiftung Preußischer Kulturbesitz
	Technische Universität Berlin (TUB)
	Umweltbundesamt
	Universität der Künste Berlin
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum Berlin für Sozialforschung gGmbH (WZB)
	Zuse-Institut Berlin (ZIB)
Biberach	Hochschule Biberach
Bielefeld	Hochschule Bielefeld – University of Applied Sciences and Arts (HSBI)
	Universität Bielefeld
Bingen	Technische Hochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Hochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Hochschule Georg Agricola
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern, für Bau und Heimat
	BundesminIsterium für Umwelt, Naturschutz und nukleare Sicherheit
	Deutsche Forschungsgemeinschaft (DFG)
	Deutscher Akademischer Austauschdienst e. V. (DAAD)
	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
	Deutsches Zentrum für Neurodegenerative Erkrankungen e. V.
	Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.
	ITZ Bund
	Rheinische Friedrich-Wilhelms-Universität Bonn
Borstel	FZB, Forschungszentrum Borstel – Leibniz Lungenzentrum
Brandenburg	Technische Hochschule Brandenburg
Braunschweig	Leibniz-Institut DSMZ – Deutsche Sammlung von Mikroorganismen und Zellkulturen GmbH
	Helmholtz-Zentrum für Infektionsforschung GmbH
	Hochschule für Bildende Künste Braunschweig
	Johann Heinrich von Thünen-Institut, Bundesforschungs-institut für Ländliche Räume, Wald und Fischerei
	Julius Kühn-Institut, Bundesforschungsinstitut für Kulturpflanzen
	Physikalisch-Technische Bundesanstalt (PTB)
	Technische Universität Carolo-Wilhelmina zu Braunschweig
Bremen	Hochschule Bremen
	Hochschule für Künste Bremen
	Jacobs University Bremen gGmbH
	Universität Bremen
Bremerhaven	Alfred-Wegener-Institut, Helmholtz-Zentrum für Polar- und Meeresforschung (AWI)
	Hochschule Bremerhaven
Buxtehude	hochschule 21 gemeinnützige GmbH
Chemnitz	Technische Universität Chemnitz
	TUCed – Institut für Weiterbildung GmbH
Clausthal	Technische Universität Clausthal
Coburg	Hochschule für angewandte Wissenschaften, Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus-Senftenberg

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

	Ruprecht-Karls-Universität Heidelberg
Heilbronn	Hochschule für Technik, Wirtschaft und Informatik Heilbronn
Hildesheim	Hochschule für angewandte Wissenschaft und Kunst Fachhochschule Hildesheim/Holzminden/Göttingen
	Stiftung Universität Hildesheim
Hof	Hochschule für angewandte Wissenschaften Hof – FH
Idstein	Hochschule Fresenius gemeinnützige Trägergesellschaft mbH
Ilmenau	Technische Universität Ilmenau
Ingolstadt	BayZiel - Bayerisches Zentrum für Innovative Lehre
	Technische Hochschule Ingolstadt
Jena	Ernst-Abbe-Hochschule Jena
	Friedrich-Schiller-Universität Jena
	Leibniz-Institut für Photonische Technologien e. V.
	Leibniz-Institut für Alternsforschung – Fritz-Lipmann-Institut e. V. (FLI)
Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Hochschule Kaiserslautern
	Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau
Karlsruhe	Bundesanstalt für Wasserbau
	FIZ Karlsruhe - Leibnitz-Institut für Informationsinfrastruktur
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe – Technik und Wirtschaft
	Karlshochschule International University
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Hochschule für angewandte Wissenschaften, Fachhochschule Kempten
Kiel	Christian-Albrechts-Universität zu Kiel
	Fachhochschule Kiel
	Institut für Weltwirtschaft an der Universität Kiel
	IPN Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik
	Helmholtz-Zentrum für Ozeanforschung Kiel (GEOMAR)
	ZBW – Deutsche Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft
Koblenz	Hochschule Koblenz
Köln	Deutsche Sporthochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Katholische Hochschule Nordrhein-Westfalen
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln gGmbH
	Technische Hochschule Köln
	Universität zu Köln
Konstanz	Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)
	Universität Konstanz
Köthen	Hochschule Anhalt
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e. V.
Landshut	Hochschule Landshut – Hochschule für angewandte Wissenschaften
Leipzig	Helmholtz-Zentrum für Umweltforschung – UFZ GmbH
	Hochschule für Grafik und Buchkunst Leipzig
	Hochschule für Musik und Theater „Felix Mendelssohn Bartholdy“
	Hochschule für Technik, Wirtschaft und Kultur Leipzig
	Leibniz-Institut für Troposphärenforschung e. V.
	Mitteldeutscher Rundfunk
	Universität Leipzig
Lemgo	Technische Hochschule Ostwestfalen-Lippe
Lübeck	Technische Hochschule Lübeck
	Universität zu Lübeck
Ludwigsburg	Evangelische Hochschule Ludwigsburg
Ludwigshafen	Hochschule für Wirtschaft und Gesellschaft Ludwigshafen
Lüneburg	Leuphana Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Leibniz-Institut für Neurobiologie Magdeburg
Mainz	Hochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Katholische Hochschule Mainz
	Universität Koblenz-Landau
Mannheim	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	Hochschule Mannheim
	Universität Mannheim
	ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung GmbH
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Philipps-Universität Marburg
Meißen	Hochschule Meißen (FH) und Fortbildungszentrum
Merseburg	Hochschule Merseburg (FH)
Mittweida	Hochschule Mittweida
Mülheim an der Ruhr	Hochschule Ruhr West
Müncheberg	Leibniz-Zentrum für Agrarlandschafts- u. Landnutzungsforschung e. V.
München	Bayerische Staatsbibliothek
	Hochschule für angewandte Wissenschaften München
	Hochschule für Philosophie München
	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e. V.
	Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt GmbH
	ifo Institut – Leibniz-Institut für Wirtschaftsforschung e. V.
	Katholische Stiftungshochschule München
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft
	Technische Universität München
	Universität der Bundeswehr München
Münster	FH Münster University of Applied Sciences
	Westfälische Wilhelms-Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neu-Ulm	Hochschule für Angewandte Wissenschaften, Fachhochschule Neu-Ulm
Nordhausen	Hochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
	Technische Universität Nürnberg
Nürtingen	Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen

Nuthetal	Deutsches Institut für Ernährungsforschung Potsdam-Rehbrücke
Oberwolfach	Mathematisches Forschungsinstitut Oberwolfach gGmbH
Offenbach/M.	Deutscher Wetterdienst (DWD)
	Hochschule für Gestaltung (HfG)
Offenburg	Hochschule Offenburg
Oldenburg	Carl von Ossietzky Universität Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Bundesgesellschaft für Endlagerung mbH (BGE)
Pforzheim	Hochschule Pforzheim – Gestaltung, Technik, Wirtschaft und Recht
Potsdam	Fachhochschule Potsdam
	Helmholtz-Zentrum, Deutsches GeoForschungsZentrum – GFZ
	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam-Institut für Klimafolgenforschung (PIK)
	Universität Potsdam
Regensburg	Ostbayerische Technische Hochschule Regensburg
	Universität Regensburg
Reutlingen	Hochschule Reutlingen
Rosenheim	Technische Hochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	CISPA – Helmholtz-Zentrum für Informationssicherheit gGmbH
	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn Rhein-Sieg
Schenefeld	European X-Ray Free-Electron Laser Facility GmbH
Schmalkalden	Hochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Siegen	Universität Siegen
Sigmaringen	Hochschule Albstadt-Sigmaringen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Hochschule Stralsund
Stuttgart	Cisco Systems GmbH
	Duale Hochschule Baden-Württemberg
	Hochschule der Medien Stuttgart
	Hochschule für Technik Stuttgart
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte Tautenburg
Trier	Hochschule Trier
	Universität Trier
Tübingen	Eberhard Karls Universität Tübingen
	Leibniz-Institut für Wissensmedien
Ulm	Technische Hochschule Ulm
	Universität Ulm
Vallendar	Vinzenz Palotti University gGmbH
Vechta	Universität Vechta
	Private Hochschule für Wirtschaft und Technik gGmbH
Wadern	Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH (LZI)
Weimar	Bauhaus-Universität Weimar
	Hochschule für Musik FRANZ LISZT Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz
Weßling	T-Systems Information Services GmbH
Wiesbaden	Hochschule RheinMain
	Statistisches Bundesamt
Wildau	Technische Hochschule Wildau
Wilhelmshaven	Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth
Wismar	Hochschule Wismar
Witten	Private Universität Witten/Herdecke gGmbH
Wolfenbüttel	Ostfalia Hochschule für angewandte Wissenschaften
	Herzog August Bibliothek
Worms	Hochschule Worms
Wuppertal	Bergische Universität Wuppertal
Würzburg	Julius-Maximilians-Universität Würzburg
	Technische Hochschule Würzburg-Schweinfurt
	Universitätsklinikum Würzburg
Zittau	Hochschule Zittau/Görlitz
Zwickau	Westsächsische Hochschule Zwickau

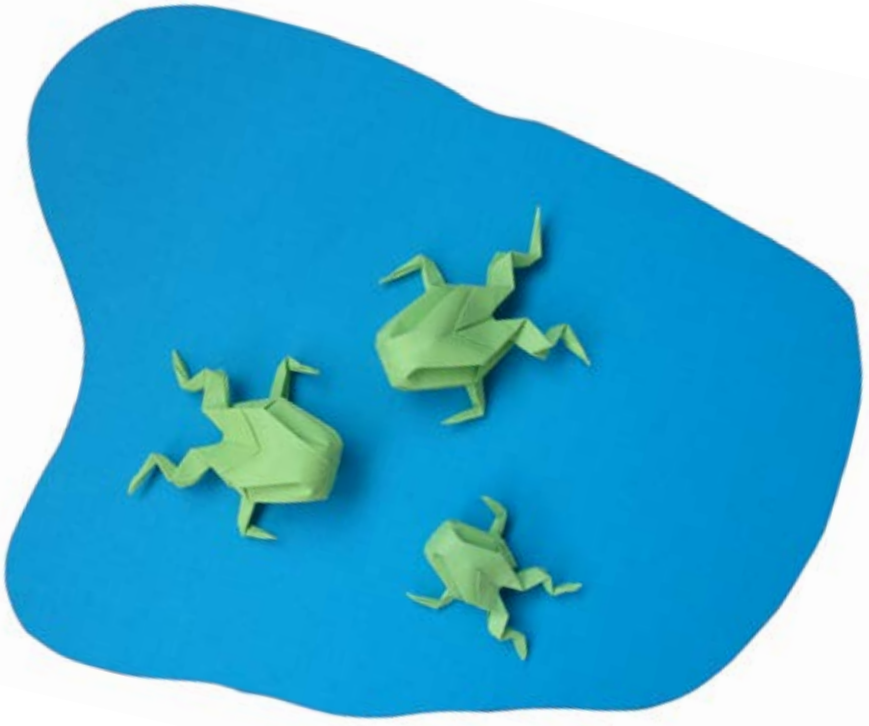
DFN mitteilungen
bieten Hintergrundwissen zu Themen aus der Welt der Kommunikationsnetze und des DFN-Vereins

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

DFN newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

DFN auf twitter
postet und teilt spannende News zum Deutschen Forschungsnetz

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



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