mitteilungen

Fein orchestriert

DFN-Security Operations in der Gesamtkomposition

Onlinelehre unterstützen
neue DFNconf-Rahmenverträge

So was von souverän
digitale Identitäten & Vertrauensdienste

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: trodler / freepik
Rückseite: bruno135_406, nojustice / Adobe Stock

Prof. Dr. Matthias S. Müller
Lehrstuhl für High Performance Computing und Direktor des IT-Centers der Rheinisch-Westfälischen Technischen Hochschule (RWTH) Aachen

Der offene Austausch und die gemeinsame Verwendung von Ressourcen sind hohe Werte in der Wissenschaftsgemeinschaft. Aktuell zeigt sich dies in der disziplin- und länderübergreifenden Bewegung Open Science mit dem Ziel, Forschungsdaten zu teilen und nachzunutzen sowie in dem weltweiten Aufbau verteilter und gemeinschaftlich nutzbarer Forschungsinfrastrukturen.

Demgegenüber stehen wir vor immer größeren Herausforderungen, dieses wertvolle Kapital in Wissenschaft und Forschung umfassend zu schützen. Zunehmend komplexe Cyberangriffe zielen direkt auf die Handlungsfähigkeit der Hochschulen und wissenschaftlichen Einrichtungen ab und richten verheerende Schäden an. Nur durch gesteigerte Anstrengungen können wir den Schutz erhöhen und die Schäden reduzieren. Neben der bloßen Prävention sind darum vor allem die schnelle Detektion und adäquate Reaktion auf Sicherheitsvorfälle in den Fokus gerückt.

„Sicherheit ist kein Zustand, sondern ein Prozess“, so lautet die Redensart. Teil dieses in einem Informationssicherheitsmanagement verankerten Prozesses ist es, die eigenen Maßnahmen zur Sicherheit kontinuierlich zu prüfen, zu hinterfragen, zu verbessern und gegebenenfalls zu ergänzen. Ein wichtiges Kriterium für die Angemessenheit von Maßnahmen ist dabei der Stand der Technik, angesiedelt zwischen den bewährten anerkannten Regeln der Technik und dem weiterentwickelten Stand der Wissenschaft. Der Stand der Wissenschaft von gestern ist der Stand der Technik von heute – und was heute noch Stand der Technik ist, wird morgen nur noch eine anerkannte Regel der Technik sein. Die Mitglieder des DFN-Vereins sind aktive Gestalter dieser Entwicklung.

Informationssicherheit ist eine Aufgabe, der wir uns einrichtungsübergreifend verpflichten müssen. Dafür ist ein gemeinsames Verständnis von Informationssicherheitsprozessen und der dafür notwendigen Technologien und Maßnahmen notwendig. Es gilt, Ressourcen zu bündeln, Kompetenzen bereitzustellen und Informationen zu teilen. Dieser Aufgabe stellen sich die im DFN-Verein organisierten Wissenschaftseinrichtungen beispielsweise, indem sie zusammen mit der Geschäftsstelle und dem DFN-CERT die neuen „Security Operations“ des DFN-Vereins im Pilotbetrieb testen und auf den Regelbetrieb vorbereiten.

Security Operations werden zukünftig ein wichtiger Baustein der Informationssicherheit aller Teilnehmer im DFN werden. Wenn es uns dadurch gelingt, den Stand der Technik in der Breite effizient umzusetzen und wir darüber hinaus gemeinsam den Stand der Wissenschaft kontinuierlich vorantreiben, dann werden wir für die Informationssicherheit viel erreichen!

Herzlichst Ihr
Matthias S. Müller

Inhalt

Mit den Aufgaben wachsen – DFNconf erweitert sein Portfolio
Unterstützung der Onlinelehre – mit Rahmenverträgen für Web- und Videokonferenzdienste

Unentschieden – das Wettrennen um IT-Sicherheit
Nachgefragt – Prof. Dr. Klaus-Peter Kossakowski im Gespräch

IT-Sicherheit reloaded – Security Operations im DFN
Adäquater Schutz für jede Einrichtung – mit Basisleistungen oder erweiterten Leistungen

Wissenschaftsnetz

Interview

Sicherheit

International

Forschung

Quantensimulatoren in der Praxis
Mit Software – komplexe Quanteneffekte nachbilden und testen

Recht

DFN-Verein

Autorinnen und Autoren dieser Ausgabe im Überblick

1 Maimona Id, DFN-Verein (id@dfn.de); **2** Christian Meyer, DFN-Verein (cmeyer@dfn.de); **3** Dr. Ralf Gröper, DFN-Verein (groeper@dfn.de); **0. Abb.** Christine Kahl, DFN-CERT (kahl@dfn.de); **4** Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **5** Stefan Metzger, Leibniz-Rechenzentrum (stefan.metzger@lrz.de); **6** Miran Mizani, Leibniz-Rechenzentrum (miran.mizani@lrz.de); **7** Michael Schmidt, Leibniz-Rechenzentrum (michael.schmidt@lrz.de); **0. Abb.** Christine Glaser, Restena Foundation (christine.glaser@restena.lu); **8** Sascha Schweiger, Friedrich-Alexander-Universität Erlangen-Nürnberg (sascha.schweiger@fau.de); **9** Martin Seidel, Friedrich-Alexander-Universität Erlangen-Nürnberg (martin.m.seidel@fau.de); **10** Owen Mc Grath, Forschungsstelle Recht im DFN (o.mcgrath@uni-muenster.de); **11** Nicolas John, Forschungsstelle Recht im DFN (njohn@uni-muenster.de)

Mit den Aufgaben wachsen – DFNconf erweitert sein Portfolio

Zur Unterstützung der Onlinelehre bietet der DFN-Verein seinen teilnehmenden Einrichtungen seit dem Start des Sommersemesters Rahmenverträge für hochskalierende, cloudbasierte Web- und Videokonferenzdienste an. Dazu gehören sowohl etablierte Cloud-Dienste als auch Produkte aus dem Open-Source-Umfeld. Dabei profitieren die DFN-Teilnehmer in vielerlei Hinsicht.

Text: **Maimona Id**, **Christian Meyer** (DFN)

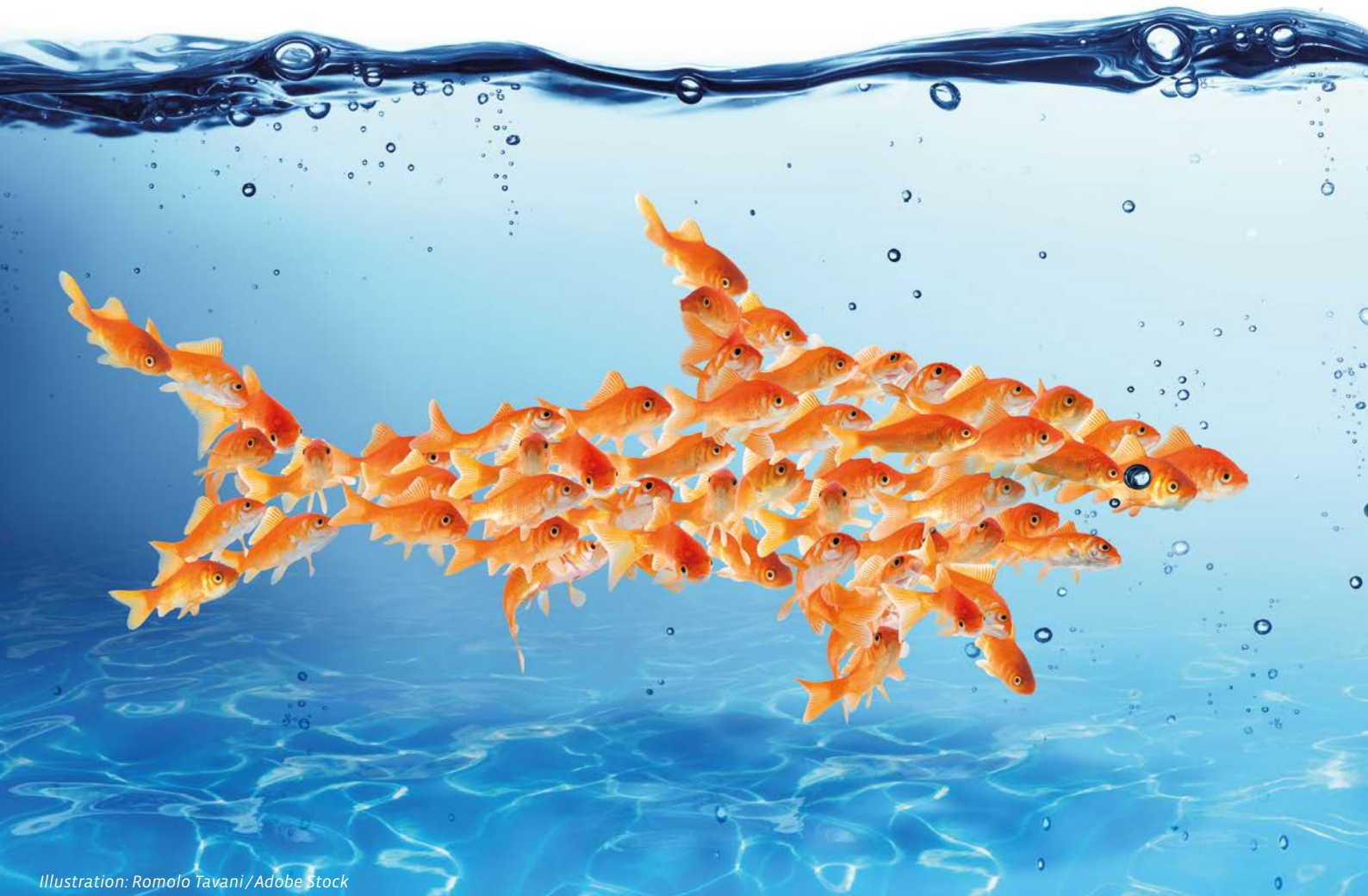


Illustration: Romolo Tavani / Adobe Stock

Zurück auf den Campus, so lautete das Motto der Hochschulen für den langersehnten Start des Sommersemesters 2022 in Präsenz. Zwei Jahre Coronavirus haben Lernen und Lehren nachhaltig verändert und den Menschen wie dem sozialen Miteinander vieles abverlangt. Mit den harten Einschnitten zu Pandemiebeginn und der Notwendigkeit, E-Learning-Veranstaltungen mit mehreren Tausend Teilnehmenden durchführen zu müssen, nahm das Thema Digitalisierung der Lehre in Turbogeschwindigkeit Fahrt auf und stellte auch den DFN-Verein vor große Herausforderungen – insbesondere den Konferenzdienst DFNconf.

Trotz nach wie vor hoher Fallzahlen haben sich das gesellschaftliche sowie das Arbeits- und Hochschulleben normalisiert und die Einrichtungen kehren vorsichtig in den Präsenzbetrieb zurück. Digitale Formate haben sich jedoch ihren festen Platz in der Bildungs- und Forschungslandschaft erobert und werden diese auch weiterhin prägen.

> Der Ausschreibung war eine intensive Diskussion innerhalb des DFN-Vereins vorausgegangen.

Seit dem Start des Sommersemesters Anfang April können am DFN teilnehmende Einrichtungen nun auf eine Reihe attraktiver Rahmenverträge für hochskalierende, cloudbasierte Web- und Videokonferenzdienste zugreifen – das Ergebnis einer EU-weiten Ausschreibung durch den DFN-Verein. Damit möchte der DFN seine Teilnehmer in puncto Onlinelehre entlasten: Der hohe Verwaltungsaufwand eines eigenen Vergabeverfahrens bleibt ihnen dadurch erspart.

Der Ausschreibung war eine intensive Diskussion innerhalb des DFN-Vereins darüber vorausgegangen, mit welchen Maßnahmen die DFN-Teilnehmer bei der Umsetzung onlinebasierter Lehr- und Lernszenarien am besten unterstützt werden können.

Rückblick auf den Beginn der Coronapandemie

Mitte März 2020 wechselten Universitäten, Hochschulen und Forschungsinstitutionen ad hoc in den Notbetrieb und schickten einen Großteil ihrer Beschäftigten zeitgleich ins Homeoffice. Zudem stand der Semesterbeginn vor der Tür. So waren die Einrichtungen gezwungen, digitale Vorlesungen und Prüfungsformate zu entwickeln, um die Lehre so gut es geht aufrechtzuerhalten. Das Ergebnis war ein Ansturm auf die virtuellen Meeting-Räume. Die Meeting- und Teilnehmendenzahlen des Videokonferenzdienstes DFNconf gingen über Nacht durch die Decke. Das führte zu massiven Einschränkungen und Engpässen beim Verbindungsaufbau sowie bei der Dienstqualität.

Für den DFN-Verein hieß das, zügig eine bundesweit einheitliche Lösung zu finden, um die Teilnehmer in dieser schwierigen Lage zu unterstützen. Schnelle Hilfe boten zunächst eine Reihe einfacher Maßnahmen, um den Betrieb der Plattform zu stabilisieren und die steigenden Nutzendenzahlen zu bewältigen. Beispielsweise unterstützte der Hersteller Pexip den laufenden Betrieb mit einer großen Anzahl zusätzlicher Video- und Audiolizenzen, die er entgeltfrei zur Verfügung stellte. Zusätzlich stellten DFN-Mitgliedseinrichtungen schnell und unkompliziert weitere Serverkapazitäten zur Verfügung. Dadurch konnte die Zahl der Konferenzknoten innerhalb von zweieinhalb Wochen vervierfacht werden.

Klar war jedoch, dass DFNconf, das ursprünglich für völlig andere Bedarfe der DFN-Teilnehmer konzipiert worden war, sein Portfolio erweitern musste. Die Konferenzplattform Pexip wurde explizit für die digitale „geschlossene Tür“ konzipiert, d. h. für Meetings mit gesteigertem Schutz- und Sicherheitsbedarf und hohem Standard im Datenschutz.

Bereits lange vor der COVID-19-Pandemie plante der DFN, ein Tool einzubinden, das sowohl Veranstaltungen mit einer großen Anzahl an Teilnehmenden als auch die Einbindung von Lernmanagementsystemen (LMS) zulässt. Ende 2019 brachte der DFN gemeinsam mit den europäischen Partnern im GÉANT-Verbund ein Proof-of-Concept für eine cloudbasierte, hochskalierende Plattform für Videokonferenzen zum Abschluss, bei dem das Produkt Zoom in allen Tests sehr gut abgeschnitten hatte – nicht zuletzt wegen seiner Nutzerfreundlichkeit und seines Funktionsumfangs. Es wurden Verhandlungen mit dem Hersteller aufgenommen, um eine Lizenzierung des Produktes für alle Teilnehmer im DFN zu erzielen. Diese scheiterten jedoch, da die Firma zum damaligen Zeitpunkt keine Rahmenverträge anbot und aufgrund der Krisensituation vom etablierten Geschäftsmodell nicht abweichen wollte. Eine schnelle Lösung war somit gescheitert.

Mit der Community für die Community: Die DFN-Mitglieder votieren für ein Vergabeverfahren

Letztendlich musste der DFN seinen Teilnehmern zu seinem größten Bedauern empfehlen, für eine Übergangszeit in eigener Initiative lokale Lösungen zu organisieren. Hinter den Kulissen wurde unterdessen mit Hochdruck an einer praktikablen und nachhaltigen Lösung gearbeitet.

Auf der 82. Mitgliederversammlung des DFN-Vereins am 8. Juni 2021 fassten die Mitglieder den Beschluss, eine umfassende Ausschreibung für hochskalierende, cloudbasierte Web- und Videokonferenzdienste zu organisieren, um das Portfolio des bestehenden Dienstes DFNconf zu ergänzen und die unterschiedlichen Bedarfe der Einrichtungen zu decken.

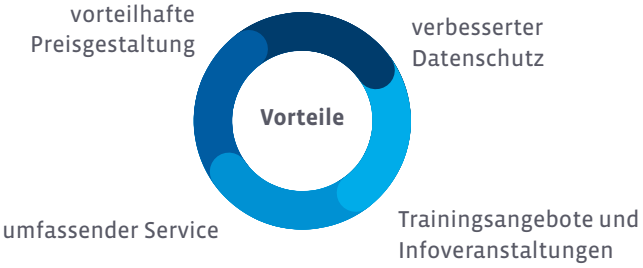
Nach einer intensiven Marktsondierung zwischen Juni und Dezember 2021, bei der auch die Teilnahmebereitschaft der Hersteller geprüft wurde und bereits ein Austausch mit DFN-Teilnehmern erfolgte, wurde das Vergabeverfahren konzipiert.

Zur Erfassung der dafür nötigen Funktionsbeschreibung wurden unter anderem in einem geleiteten Interviewverfahren mit unterschiedlichen Nutzergruppen und Stakeholdern (z. B. Kompetenzzentrum für Videokonferenzdienste (VCC) an der TU Dresden, ZKI-Arbeitskreis Multimedia, DINI-Arbeitskreis Viktas, DACH Nutzergruppe Forschung & Lehre) die Anforderungen innerhalb der Community erarbeitet. Zwingende Kriterien waren eine schnelle Skalierbarkeit bei einer großen Anzahl von Teilnehmenden, Anbindungsmöglichkeiten für Lernmanagementsysteme und ein darauf zugeschnittener Funktionsumfang. Zu den Musskriterien gehörten auch eine unkomplizierte Rollenvergabe in den virtuellen Räumen, Arbeitsgruppenfunktionalität, Single Sign-on und Aufzeichnungsmöglichkeiten. Weitere Aspekte für die Auswahl waren außerdem die Themen Architektur und Betriebsmodell, Anbindungsmöglichkeiten an technische Schnittstellen wie SIP bzw. H.323, Barrierefreiheit und Inklusion sowie Datenschutz und Datensicherheit. Auf Basis dieser Anforderungsanalyse wurde die Ausschreibung im Rahmen eines EU-weiten offenen Verfahrens von Dezember 2021 bis Februar 2022 durchgeführt.

> Sowohl etablierte Cloud-Dienste als auch Produkte aus dem Open-Source-Umfeld wurden ausgewählt.

Aus den zahlreichen Angeboten wurden insgesamt acht Produkte ausgewählt – sowohl etablierte Cloud-Dienste als auch Produkte aus dem Open-Source-Umfeld. Anfang März dieses Jahres konnten die Zuschläge erteilt werden. Damit stehen Rahmenverträge für die Produkte Adobe Connect, BigBlueButton, Blackboard Collaborate, Cisco Webex, Microsoft Teams, OpenTalk, TeamViewer Classroom sowie Zoom zur Verfügung.

Von den guten Konditionen der Rahmenverträge profitieren die DFN-Teilnehmer gleich in mehrfacher Hinsicht. Das sind unter anderem:



Das Interesse am Ergebnis der Ausschreibung sowie am Prozess der Lizenzbestellung ist groß. Insgesamt 600 Teilnehmende informierten sich Ende Februar im Rahmen von Onlineworkshops, die der DFN durchführte. Die ersten Hochschulen haben bereits Lizenzen abgerufen, das Feedback ist positiv. Wie sich die Onlinelehre künftig entwickeln wird und welche Bedarfe die Einrichtungen haben werden, bleibt ein spannendes Thema für den DFN-Verein. Geblieben sind Freude und die Neugierde, gemeinsam mit den Teilnehmern neue Lösungen für Wissenschaft und Lehre mitzugestalten. ◆

WEITERE INFORMATIONEN:

Hintergrundinformationen zum Vergabeverfahren sowie zu den Produkten und Rahmenverträgen finden Sie unter:
https://www.conf.dfn.de/rahmenvertraege/
Die notwendigen Unterlagen zur Bestellung der Lizenzen sowie Beratung erhalten Sie unter:
vertraege@conf.dfn.de oder 030 884299-9125.

Das Kompetenzzentrum für Videokonferenzdienste (VCC) an der TU Dresden unterstützt und berät DFN-Teilnehmer bei der Einsatzplanung, Installation und dem Betrieb von Video- und Webkonferenzdiensten.

Die Kontaktinformationen finden Sie hier:
https://tu-dresden.de/zih/vcc

Kurzmeldungen

DFNFernsprechen: Neue Rahmenverträge abgeschlossen

Foto: BrianAJackson/envato

Mit dem kürzlich beendeten Vergabeverfahren der Leistungen für DFNFernsprechen wird nach Ablauf der aktuellen Rahmenverträge ab 1. Juli 2022 eine neue Vertragsphase beginnen. Im Umfang enthalten sind Anschlussmöglichkeiten für die Telefonie über das Wissenschaftsnetz sowohl für lokal betriebene Telefonanlagen als auch über die zentral im Wissenschaftsnetz betriebene Cloud-Telefonanlage. Auch Mobilfunk und SMS-Gateway sind wieder Bestandteil von DFNFernsprechen. Nach dem erfolgreichen Abschluss der Migration der alten ISDN-Anschlüsse auf Voice-over-IP (VoIP) ist ISDN-Technik nun endgültig nicht mehr Bestandteil des Leistungsportfolios.

Ob Telefonkonferenzen, mobile App, Desktop-App oder Faxlösungen – mit dem Dienstmodul VoIP-Centrex profitieren Teilnehmer von einem umfangreichen Angebot an Funktionalitäten in einer einheitlichen Anwendungsumgebung. Die Verbindungen zwischen Endgeräten und VoIP-Centrex sowie zwischen VoIP-Centrex und der zentralen VoIP-Plattform sind standardmäßig per TLS/SRTP verschlüsselt. Mit einem redundanten Aufbau wird die Konnektivität sowohl innerhalb des Forschungsnetzes als auch in die öffentlichen Telefonnetze sichergestellt.

Der Rahmenvertrag für Direktabrufe von Mobilfunkanschlüssen beinhaltet Sprach-, Nachrichten- und Datenübertragung inklusive Endgeräte sowie LTE- und 5G-Anbindung und Hotspot-Nutzung. ◆

Zum gesamten Portfolio berät Sie das Team von DFNFernsprechen: **DFNFernsprechen@dfn.de**
Weitere Informationen finden Sie unter:
https://dfn.de/dienste/collaboration-services/

Neue Version des Teilnehmerportals in Betrieb

Foto: megaflopp /iStock

Pünktlich zur Betriebstagung am 29. und 30. März 2022 wurde die neue Version des Teilnehmerportals in Betrieb genommen. Die Version wurde um die Versorger- und Delegationsdienste sowie das Dienstpaket erweitert und enthält nun alle Dienste, die mit der neuen Entgeltordnung eingeführt wurden. Damit nimmt die Zahl der Nutzenden weiter zu.

Auch die nächsten Entwicklungsschritte sind bereits klar umrissen: Das nächste große Update wird neben der Komplettierung der Informationen zu Teilnehmeranbindungen die Anzeige von Wartungsmeldungen am Teilnehmerrouter enthalten und Nutzenden die Möglichkeit bieten, eigene Wartungen zu melden. Dies wird die Grundlage bilden, um im Anschluss auch Störungstickets eröffnen und nachvollziehen zu können.

Auch andere Dienste des DFN-Vereins werden in das Teilnehmerportal aufgenommen: So können zukünftig Dienstvereinbarungen für Cloud-Dienste im bereits implementierten Antragsservice ausgefüllt werden. ◆

Haben Sie Interesse am Teilnehmerportal oder sonstige Fragen? Wir beraten Sie gerne!
Sie erreichen uns per E-Mail unter
teilnehmerportal@dfn.de
oder telefonisch unter 030 884299-9137.

Kurzmeldungen

In der Praxis bewährt – die neue Entgeltordnung des DFN-Vereins

Foto: Drazen Zigic / iStock

Am 1. Januar 2022 ist die aktuelle Entgeltordnung in Kraft getreten. Beschlossen wurde die Einführung auf der 80. Mitgliederversammlung des DFN-Vereins – damit ging die Arbeit in der Geschäftsstelle erst richtig los.

Neben der Erstellung von Dienstvereinbarungen für alle Dienstvarianten von DFNInternet und des Dienstpakets musste das Dokumentations- und Informationssystem (GIS) der DFN-Geschäftsstelle den veränderten Gegebenheiten angepasst werden. Aber auch die Anforderungen auf technischer Ebene mussten auf die Systeme in der realen Welt übertragen werden: So wurden die Konfiguration auf der Routerplattform automatisiert bereitgestellt und das Monitoring angepasst. Als Ergänzung zur Entgeltordnung wurde erstmals eine eigenständige Dienstbeschreibung für DFNInternet erstellt und veröffentlicht.

Ein wichtiger Teil der Arbeit bestand zunächst darin, die Fragen der DFN-Teilnehmer zu den neuen Rahmenbedingungen und Möglichkeiten zu beantworten. Unter pandemischen Bedingungen und weitestgehend aus dem Homeoffice heraus war das eine echte Herausforderung, die jedoch erfolgreich gemeistert wurde: Die notwendigen Dienstvereinbarungen wurden bereitgestellt, die IT-Systeme ertüchtigt und nicht zuletzt die Teilnehmer umfassend informiert und beraten.

Die ersten Vereinbarungen zur neuen DFNInternet-Dienstvariante „Versorger“ konnten bereits im letzten Quartal des Jahres 2021 abgeschlossen und damit die Voraussetzungen für eine zeitnahe Umsetzung geschaffen werden. Hierzu werden im Laufe des Jahres in enger Abstimmung mit den Einrichtungen weitere Umstellungen auf die neuen Varianten geplant und realisiert.

Auch die Bereitstellung der gebuchten Bandbreite für Teilnehmer an DFNInternet-Clusterdiensten konnte, begleitet durch eine gezielte Kommunikation in Richtung der Teilnehmer, im März 2022 erfolgreich abgeschlossen werden.

Als Zwischenfazit kann schon jetzt festgestellt werden, dass sich die neue Entgeltordnung in der Praxis bewährt hat und für die kommenden Jahre eine gute und verlässliche Basis für die Nutzung von Diensten des DFN-Vereins bildet. ◆

Die aktuelle Entgeltordnung sowie die Dienstbeschreibung für DFNInternet finden Sie unter: **https://www2.dfn.de/dienstleistungen/dfninternet/entgelte/**

Optimal vernetzt: Umsetzung neuer IP-Transitanbindungen

Der DFN-Verein hat die IP-Transitanbindungen für das Wissenschaftsnetz X-WiN erfolgreich erneuert. Auf Grundlage der aktuellen Ausschreibung des GÉANT World Service (GWS) durch das europäische Forschungsnetz GÉANT erhielten die IP-Transitanbieter Lumen Technologies Germany GmbH für den Standort Frankfurt/M., Arelion - Telia Carrier Germany GmbH (ehem. Telia Carrier) für Hamburg sowie die Deutsche Telekom AG für Düsseldorf den Zuschlag. Im Rahmen dieser Aktualisierung wurde die Anbindungsbreite auf jeweils 100 Gbit/s harmonisiert. Die Umsetzung erfolgte parallel zu den vorhandenen Implementierungen und verlief ohne Störungen für die Teilnehmer am X-WiN.

Durch die aktuellen IP-Transitanbindungen über verschiedene Service-Provider und Standorte profitieren DFN-Teilnehmer von einer optimierten Georedundanz. Bei Ausfall einzelner Anbindungen entstehen so keine Einschränkungen für die Teilnehmer am X-WiN. Seit Inbetriebnahme des aktuellen DFN-Wissenschaftsnetzes X-WiN 2006 verfolgt der DFN-Verein die bedarfsgerechte Dimensionierung seiner Außenanbindungen. Ziel ist eine exzellente Konnektivität zwischen seinen Teilnehmern sowie über leistungsstarke Austauschpunkte mit dem allgemeinen Internet.

Einen ausführlichen Artikel zum Thema Transit & Peering finden Sie in Ausgabe 95 der DFN-Mitteilungen auf Seite 26: https://www2.dfn.de/fileadmin/5Presse/DFNMitteilungen/DFN_Mitteilungen_95.pdf ◆

DFN-MailSupport versorgt mehr als eine Million Endnutzer im X-WiN

Millionenmarke geknackt! Mit Stand 4. Februar 2022 versorgt der Dienst DFN-MailSupport 1 089 128 Nutzer-Mailboxen im Wissenschaftsnetz X-WiN mit seinen Leistungen zur Abwehr unerwünschter und schädlicher – mit Spam oder Malware (Viren, Würmer, Trojaner etc.) infizierter – E-Mails. Das entspricht etwa 25 Prozent aller Endnutzer im X-WiN.

143 Einrichtungen nutzen den Dienst aktuell. Dabei werden die E-Mails über die DFN-Mail-Gateways geleitet und unterliegen dort vielen Checks zur Spam- und Virenerkennung. Erst danach werden sie in die Ziel-Mailserver der Einrichtungen weitergeleitet. Das DFN-MailSupport-Portal bietet Administrierenden die Möglichkeit, selbstständig Konfigurationsparameter einzustellen. Dazu gehören unter anderem Maildomains und Mailserver, aber auch Allow- and Blocklists.

Seit Januar 2012 läuft der Mailfilterservice des DFN-MailSupport-Dienstes im Regelbetrieb. Der Dienst ist nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert und trägt zum hohen Sicherheitsniveau im X-WiN bei.

Das Portal DFN-MailSupport steht bereit unter:
https://www.mailsupport.dfn.de/ ◆

Von A nach B – Kernnetzknoten erfolgreich umgezogen

Foto: Robert Kneschkec / Adobe Stock

Der DFN-Verein betreibt aktuell 65 Kernnetzknoten für das Wissenschaftsnetz X-WiN. In der Regel befinden sich diese in Gebäuden der Teilnehmer und Mitglieder. Viele Standorte wurden bereits ab 2005, in der Frühphase des X-WiN, aufgebaut und haben ein gewisses Alter erreicht. Geplante Sanierungen sowie der Abriss und Neubau von Gebäuden machen den Umzug von Kernnetzknoten jetzt notwendig.

In den vergangenen zwölf Monaten wurden zwei Kernnetzknoten erfolgreich verlegt und an neuen Standorten mit zeitgemäßer Infrastruktur in Betrieb genommen: An der Otto-von-Guericke-Universität in Magdeburg zog der Knoten MAG in eine frisch renovierte Umgebung um, da das bisher genutzte Gebäude abgerissen werden soll. Auch an der Universität Greifswald hatte das Rechenzentrumsgebäude das Ende seiner Lebenszeit erreicht und wurde durch einen Neubau ersetzt, in dem der Kernnetzknoten GRE künftig betrieben wird.

Auf der einen Seite stellen diese Umzüge für die DFN-Geschäftsstelle eine mittlerweile gut geübte Routine dar: Seit 2009 wurden bereits zehn Kernnetzknoten erfolgreich umgezogen. Auf der anderen Seite unterscheiden sich die Projekte im Detail erheblich voneinander. Trotz einer gewissen Standardisierung beim Bau und Betrieb von Rechenzentren gibt es durch individuelle Anforderungen vor Ort unterschiedlichste Ausprägungen der räumlichen und technischen Rahmenbedingungen. Als „Gast“ muss der DFN diese berücksichtigen.

Zudem sind die hohen Anforderungen an den unterbrechungsfreien Betrieb der dort erbrachten Dienste, die Koordination der beteiligten Partner und Dienstleister sowie die langen Zeitspannen jedes Mal eine große Herausforderung – gerade in der „heißen“ Umzugsphase.

Bisher konnten alle Schwierigkeiten überwunden werden, nicht zuletzt durch das Engagement und die große Unterstützung der Kolleginnen und Kollegen vor Ort in den gastgebenden Einrichtungen. Daher an dieser Stelle ein herzlicher Dank an alle Beteiligten für die gute und vertrauensvolle Zusammenarbeit!

Und damit die DFN-Geschäftsstelle nicht aus der Übung kommt, sind schon wieder mehrere Umzüge in Arbeit. Aktuell befinden sich Projekte in Dresden, Göttingen, Ilmenau, Jena und Saarbrücken in der Planung oder bereits in der Umsetzung. ◆

Unentschieden – das Wettrennen um IT-Sicherheit

Cyberangriffe auf Einrichtungen aus Bildung und Forschung haben in den vergangenen Jahren stark zugenommen. Um sich vor ihnen zu schützen, sind weitreichende Maßnahmen notwendig – sowohl technischer als auch organisatorischer Natur. Welche das sind und wie wichtig ein gemeinsames Verständnis für Sicherheitsfragen in der Wissenschaftscommunity ist, erklärt Sicherheitsexperte Prof. Dr. Klaus-Peter Kossakowski im Interview.

Sie sind seit mehr als 35 Jahren als Berater in der Informationssicherheit tätig. Gibt es etwas, was Sie noch überrascht?

Ja, in der Tat. Wie sehr wir immer noch am Anfang stehen! In meinem Beratungsalltag höre ich oft die Frage: Was muss ich tun, um sicher zu sein? Dann frage ich in der Regel zurück: Sicher wovor?

Die erste Hürde für ein Sicherheitskonzept ist, sich darüber Klarheit zu verschaffen, welche Werte konkret geschützt werden sollen und welche Sicherheitsanforderungen sich daraus ergeben. Beispielsweise bei der Frage, ob Daten in der Cloud verschlüsselt werden müssen, ist erst einmal zu klären, welche Daten darauf abgelegt sind: Gesundheitsdaten, Daten zur Religionszugehörigkeit oder Daten für Bezahlvorgänge? Oft mache ich die Erfahrung, dass Verantwortliche das nicht beantworten können.

Streng genommen müsste ich in so einem Fall zum größten Schutz raten, weil ich die Anforderungen nicht kenne und damit das Risiko schlecht einschätzen kann. Aber auf Nummer sicherzugehen und stets die maximale Sicherheit anzustreben, ist definitiv nicht durchsetzbar, nicht finanzierbar – und schon gar nicht notwendig.

Welche Angriffsflächen bieten Hochschulen und Forschungseinrichtungen?

Im Hochschul- und Forschungsbereich haben wir eine offene Kultur und gehen sehr kooperativ miteinander um. Dadurch bieten wir eine größere Angriffsfläche als sehr restriktive und geschlossene Umgebungen.

Besonders empfindliche Bereiche sind die Verwaltung, aber auch das Prüfungswesen. Einrichtungen, die an innovativen Forschungsprojekten und technologischen Neuentwicklungen arbeiten, z. B. in Kooperationen mit Industrie- und Wirtschaftsunternehmen, sind ein begehrtes Angriffsziel. Das ist erwiesene Strategie von bekannten

> „Tatsächlich können Insider-Angriffe deutlich gefährlicher sein als externe Angriffe."

Staaten, sich durch einen privilegierten schnellen Zugriff auf Forschungsergebnisse einen erheblichen Entwicklungsaufwand zu sparen – oft ein Vorsprung von Jahren und nicht zuletzt ein immenser wirtschaftlicher Faktor.

Von wem gehen solche Angriffe aus?

Die Masse der Angriffe geht von externen Angreifern aus. Diese sind Untersuchungen zufolge jung, dynamisch und technisch interessiert. Dabei sind externe Angreifer zunächst im Nachteil, da sie nicht wie Insider über konkretes Wissen der eingesetzten Systeme verfügen, oder sogar direkt mit entsprechenden Berechtigungen auf die Informationen zugreifen können, die das Ziel des Angriffs

Foto: Nina Bark, DFN

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 von FIRST und dem DFN-CERT

darstellen. Tatsächlich können Insider-Angriffe deutlich gefährlicher sein als externe Angriffe. Aber im Gegensatz zu Firmen des Finanzwesens oder der Wirtschaft gibt es in Hochschulen und Forschungseinrichtungen erheblich weniger finanziell relevante Angriffsziele.

Die angegriffenen IT-Systeme und Anwendungen haben sich sehr stark verändert, weniger im Hinblick auf die eingesetzten Kommunikationsprotokolle, als auf die Komplexität und Flexibilität. Die meisten Geräte sind heute frei programmierbar, verfügen über Erweiterungsschnittstellen und können von jedem konfiguriert werden. Allerdings entstehen dabei viele Schwachstellen, die die Systeme erst verwundbar machen.

Ganz andere Möglichkeiten haben Angreifer, die von fremden Staaten gezielt beauftragt oder zumindest gefördert oder geduldet werden. Während die gleichen Schwachstellen durch solche Angreifer ausgenutzt werden, sind die eingesetzten Werkzeuge viel spezieller und eben nicht im Internet für andere Täter verfügbar, sondern eigens entwickelt. Und dieser Aufwand ermöglicht erfolgreiche Angriffe auch auf sehr gut geschützte Einrichtungen wie z. B. den Deutschen Bundestag.

Das klingt, als ob wir uns künftig permanent auf Abwehr einstellen müssen.

Eine ständige Bedrohung, auch für Forschungsnetze, sind sogenannte Verfügbarkeitsangriffe. Sie sind leicht durchzuführen und schwer zurückzuverfolgen. Manchmal gehen sie mit der Forderung einer „Schutzgebühr“ einher. Hier handelt es sich schlicht um die „Digitalisierung“ der Schutzgelderpressung.

Aber es geht auch um Informationen, die attraktiv sind – insbesondere neue Forschungsergebnisse oder Einblicke in Kooperationen mit der Wirtschaft. Informationen gegen Unbefugte zu verteidigen, wird ein ewiges Kopf-an-Kopf-Rennen bleiben. Dabei kochen die Angreifer auch nur mit Wasser. Früher entwickelten die meisten ihre eigenen Werkzeuge selbst. Viele von ihnen waren fachlich so gut wie diejenigen, die die Systeme und Schutzmaßnahmen entwarfen und entwickelten. Heute werden Werkzeuge und Plattformen angeboten, die alle benutzen können, ohne auch nur ansatzweise zu wissen, wie die Angriffe auf Netzwerkebene funktionieren. Das interessiert die Hacker auch gar nicht. Sie haben ein Tool und das bietet ihnen innerhalb kurzer Zeit genügend gekaperte Rechner im Internet, die wiederum als Bot-Netz für weitere Angriffe eingesetzt oder vermietet

werden. Und so gibt es die Leute, die die Werkzeuge entwickeln – wenige im Vergleich – und genügend andere, die diese einsetzen wollen.

Je schneller wir entdecken, dass ein Angriff stattfindet und das Wissen an die richtigen Organisationen weitergeben können, desto eher gewinnen wir das Wettrennen: Computer-Notfallteams werten die Angriffstechniken aus, um neue Trends zu erkennen; Produktsicherheitsteams schließen die Sicherheitslücken in den Produkten; Betroffene müssen ihre Systeme überprüfen und „aufräumen“. Zusammen müssen wir verhindern, dass das kompromittierte System für weitere Angriffe eingesetzt wird, aber auch, dass das Wissen über neue Schwachstellen schnell umgesetzt werden kann. Nur dadurch werden Schäden und Folgeschäden eingedämmt.

Die konkrete und weiter zunehmende Abhängigkeit von sozio-technischen Systemen – die Verquickung zwischen Menschen, die für Systeme verantwortlich sind, und Technik, die Schwachstellen aufweist – sorgen dafür, dass wir fortwährend ein ausreichendes Maß an Aufwand für Sicherheit investieren müssen. Es ist keine Überraschung, dass das die gleiche Diskussionslinie ist, die wir auch in anderen Sicherheitsbereichen gerade beobachten können.

Woher stammen die Angriffswerkzeuge?

Teils werden diese aus sogenannten „Proof of Concept“ weiterentwickelt, da die Demonstration einer Schwachstelle oft bereits das Wissen beinhaltet, wie diese ausgenutzt wird. Andere Werkzeuge werden aus den Sicherheitsupdates abgeleitet, die von den Herstellern bereitgestellt werden, um gerade Schwachstellen zu schließen. Aber indem diese aufzeigen, wo genau eine Schwachstelle vorhanden war, kann daraus – sogar automatisiert – ein Angriff abgeleitet werden.

Und dann gibt es auch gezielte Veröffentlichungen, um z. B. auf eine Schwachstelle aufmerksam zu machen. Die detaillierte Veröffentlichung ist sicherlich in den allermeisten Fällen kontraproduktiv, trotzdem muss es möglich sein, über Schwachstellen zu sprechen. Es gibt schon sehr lange die Diskussion wie eine verantwortungsvolle Aufdeckung, ungenau übersetzt mit „Responsible Disclosure“, so gestaltet werden kann, dass Angreifende keinen Nutzen ziehen können, aber die „Verteidigung“ genügend Informationen hat, um ihre Aufgaben erfolgreich durchführen zu können. Die Diskussion wird weitergehen, aber es ist klar, dass Sicherheitslücken offengelegt werden müssen, wenn Hersteller sich beispielsweise weigern, diese zu schließen – aber ohne, dass Organisationen und Firmen, die diese Schwachstellen noch nicht schließen konnten, gefährdet werden.

Wir wissen heute, dass wir jederzeit bisher noch unbekannten Angriffen ausgesetzt sein können, die dann auch Erfolg haben werden. Doch wer genau betroffen ist und wie groß die Schäden sein werden, hängt ganz entscheidend davon ab, wie gut die jeweiligen Organisationen ihr Informationssicherheitsmanagement aufgesetzt haben und welche lokalen Sicherheitskonzepte Schlimmeres verhindern können.

Was müssen Sicherheitskonzepte leisten?

Notwendig sind Sicherheitskonzepte, die auf die Bedarfe der Einrichtungen zugeschnitten sind. Jedes Konzept muss die Balance halten zwischen der Höhe des Risikos in Form des zu erwartenden Schadens im Verhältnis zu den Kosten der Sicherheitsmaßnahmen und dem Aufwand, diese aufzubauen und in die Prozesse der jeweiligen Einrichtung zu integrieren. Einzelne Aufgabenbereiche wie das Logdatenmanagement oder der Grundschutz von Arbeitsplätzen haben dabei nicht nur eine technische Ebene, sondern auf jeden Fall auch eine organisatorische Ebene, unabhängig von der Wirtschaftlichkeit und Umsetzbarkeit. Zunächst müssen

> „Notwendig sind Sicherheitskonzepte, die auf die Bedarfe der Einrichtungen zugeschnitten sind.“

Sicherheitsziele definiert werden, die dann durch die geschickte Kombination geeigneter Maßnahmen erreicht werden. Dafür benötigt jede Hochschule und Forschungseinrichtung zwingend eine Delegation der Verantwortung an sogenannte Informationssicherheitsbeauftragte, die die Aufgabe haben, ein Informationssicherheitsmanagementsystem aufzubauen. Diese sind geschult darin, interne Gefahrenlagen individuell zu erfassen und zu beurteilen. Erst dann kann eine sinnvolle Abdeckung erreicht werden. Wobei wie immer gilt, dass auch Teilkonzepte bereits Angriffe verhindern oder abwehren können.

Zusätzlich zu den internen Maßnahmen nutzen Einrichtungen externe Dienste von Computer Emergency Response Teams (CERT). Was ist die Aufgabe dieser Fachleute?

Ihre Aufgabe ist es unter anderem, Betroffenen bei erkannten Sicherheitsvorfällen zeitnah zu helfen und Informationen zu aktuellen Schwachstellen zu liefern. CERTs werten aktuelle Angriffsmuster aus, um die bestmögliche Informationslage für die betreuten Einrichtungen zu erreichen. Was wir durch CERTs nicht direkt in den Griff bekommen sind zwei entscheidende Faktoren: Der eine betrifft die teilnehmenden Einrichtungen selbst: Von außen haben CERTs

keinen Einblick in die Organisation und die internen Verantwortlichkeiten. Sie wissen beispielsweise nicht, welche Daten ausgewertet werden, welche verfügbar oder wie diese beschaffen sind. Das können nur die internen Verantwortlichen sowie die eigentlichen Endnutzer lokal beurteilen. Das deckt sich übrigens mit der Bewertung des notwendigen Datenschutzes, die ohne ein detailliertes Verständnis der Verarbeitungsprozesse ebenfalls nicht möglich ist. Dazu kommt, dass die Einrichtungen organisatorisch sicherstellen müssen, dass die Warnmeldungen nicht zuletzt über geeignete interne Kommunikationswege zeitnah weitergegeben werden. Die entsprechende Bearbeitung muss in Prozessen verankert werden, die Teil des Sicherheitskonzepts sind.

Das Bewusstsein für und das Beheben von technischen Schwachstellen sowie die Gewährleistung eines sicheren, zuverlässigen, technischen Betriebs ist wiederum eine ständige Aufgabe, die bei den Rechenzentren liegt.

Was hat es mit dem zweiten Faktor auf sich?

Der zweite Faktor betrifft die Suche nach potenziellen Bedrohungen. Dafür werden Threat-Analysten oder Threat-Hunter eingesetzt. Anhand von Hypothesen und Auswertungen von erfolgreichen Angriffen erkennen und suchen sie bestimmte Muster und Spuren der Angriffswerkzeuge. Ziel ist dabei, Regeln abzuleiten, die automatisiert umgesetzt werden können.

Die lokalen Hochschulrechenzentren sind zwar dafür da, den Betrieb für ihre Einrichtung zu gewährleisten, sie können aber nicht zu weltweit führenden Fachleuten im Erkennen neuer Angriffsmuster werden, zumal dies auch insgesamt unwirtschaftlich wäre. Es ist schneller und zielführender, wenn dafür ausgebildete Analysten Muster extrahieren und in internationaler Zusammenarbeit mit anderen Fachleuten Hypothesen aufstellen und verifizieren, bevor entsprechende Warnungen ausgegeben werden. Was dann vor Ort gebraucht wird, sind wiederum die Verantwortlichen, die die bereitgestellten Informationen weiterbearbeiten. Schlussendlich ist Sicherheit eine gemeinsame Aufgabe von Fachleuten – interner wie externer.

Inwieweit hängt der Erfolg Ihrer Arbeit davon ab, wie gut die Hochschulen aufgestellt sind in puncto Sicherheit?

Der Schutz einer offenen Gemeinschaft wie der Hochschul- und Forschungslandschaft bedarf der Anstrengung aller. Wir stellen uns über Organisationsgrenzen hinweg gegenseitig Rechnerleistungen oder Speicherkapazitäten zur Verfügung und wir bauen unsere eigenen Ergebnisse auf den Forschungsergebnissen anderer auf. Darum muss es auch ein gemeinsames Verständnis für Sicherheitsfragen geben. Das stärkt letztendlich auch unser Zusammengehörigkeitsgefühl, weil jede Einrichtung nicht nur von der eigenen Sicherheit abhängt, sondern auch von der Infrastruktur – Netz und zentrale Dienste – sowie den Ressourcen der anderen Einrichtungen, die wir brauchen und die uns helfen, unsere Leistung zu erbringen.

Sicherheit ist eine Querschnittsaufgabe, die jede Person in einer Organisation oder Gemeinschaft betrifft. Egal, ob ich in der Hochschulverwaltung arbeite oder zu den Studierenden gehöre. Sobald ich eine E-Mail öffne, die eine Malware beinhaltet, habe ich diese quasi in die Infrastruktur bzw. zur Ausführung gebracht. Sicherheitsfragen gehen damit alle an.

Zum Schluss: Was geben Sie dem Nachwuchs in der IT-Sicherheit mit auf den Weg?

Als junger Mensch bewegt man sich hier in einem wahnsinnig spannenden und herausfordernden Themenfeld. Ich nenne ein Beispiel: Zu Beginn des Ukraine-Krieges hat die CERT-Community überlegt, was nun zu machen ist. Innerhalb von einer Stunde organisierten wir eine Videokonferenz mit über 250 CERT-Teams aus ganz Europa und tauschten uns darüber aus, welche Konsequenzen diese Krise hat – für die Kolleginnen und Kollegen aus der Ukraine, aber auch aus Russland und Belarus, mit denen wir über Jahrzehnte zusammengearbeitet haben – aber auch für uns und unsere Zusammenarbeit selbst. Es war äußerst lehrreich, sich bewusst zu machen, dass keiner von uns über alle Informationen verfügt, sondern wir darauf angewiesen sind, uns auszutauschen und eine gemeinsame Vorgehensweise zu entwickeln.

Das Ermutigende im CERT-Bereich ist, dass es über alle Organisationsgrenzen hinweg ein tiefes Verständnis dafür gibt, Verantwortung zu übernehmen und gut zusammenzuarbeiten, weil es gemeinsame Probleme gibt, die wir bekämpfen müssen. Erst hierdurch können wir auch global etwas bewegen und damit einen Unterschied machen!

Die Fragen stellte Maimona Id (DFN-Verein)

IT-Sicherheit reloaded – Security Operations im DFN

Die neuen Security Operations des DFN-Vereins orientieren sich an den spezifischen Bedarfen wissenschaftlicher Einrichtungen und wurden konsequent für heterogene IT-Landschaften konzipiert. Das Ergebnis ist ein leistungsfähiges Portfolio an Sicherheitsdiensten, das sowohl umfangreiche Basisleistungen für alle DFN-Teilnehmer enthält, als auch erweiterte Leistungen für Teilnehmer mit höherem Schutzbedarf. Damit stärkt der Dienst den sicheren Betrieb von Informationsinfrastrukturen zur Unterstützung exzellenter Forschung und Lehre in Deutschland.

Text: **Ralf Gröper** (DFN-Verein), **Christine Kahl** (DFN-CERT)

Security Operations im Überblick

Seit dem Start des Pilotbetriebs am 26. November 2020 für die Einrichtung eines Security Operations Centers (SOC) am DFN-CERT und der damit einhergehenden Einführung der neuen Security Operations (SecOps) im DFN ist viel passiert: Gemeinsam mit inzwischen acht Pilotteilnehmern validieren der DFN und das DFN-CERT die unterschiedlichsten Leistungsmerkmale, um möglichst viele Sicherheitsszenarien in den Einrichtungen abbilden und mehr Sicherheitsvorfälle proaktiv erkennen zu können. Dabei wurden bereits wertvolle Erkenntnisse gewonnen und umgesetzt: Ein Teil der erprobten Leistungsmerkmale setzt erhebliche Mitwirkungspflichten sowie ein hinreichend ausgereiftes Informationssicherheitsmanagement beim Teilnehmer voraus und muss zudem – aufgrund der hohen Aufwände im DFN-SOC – mit einer eigenen Kostenumlage geplant werden.

Für andere Leistungsmerkmale hat sich hingegen gezeigt, dass sie ohne weitere Skalierungseffekte von einer großen Anzahl von Einrichtungen genutzt werden können. Das wird auf DFN-Seite zum einen durch einen hohen Grad an technischer Automatisierung und zum anderen durch die Einbindung der Prozesse in das DFN-CERT Portal bewerkstelligt. Insbesondere in der Softwareentwicklung, der Serverbeschaffung und im Serverbetrieb sind zwar Investments durch den DFN-Verein notwendig. Da aber keine signifikante Kostenskalierung durch hohe Nutzungszahlen erfolgt, können diese Leistungen im Rahmen des Dienst-Pakets angeboten werden, welches z. B. im DFNInternet-Dienst enthalten ist. Auf Teilnehmerseite sind die Voraussetzungen zur Nutzung dieser Basisleistungsmerkmale ebenfalls niedrigschwellig: Die Einbindung in die eigenen Prozesse innerhalb der Einrichtung orientiert sich stark am derzeitigen DFN-CERT-Dienst – das heißt, jeder Teilnehmer, der das DFN-CERT Portal bereits nutzt, wird sich hier schnell zurechtfinden.

Im Ergebnis wird es die Security Operations des DFN künftig in zwei „Geschmacksrichtungen“ geben: einmal mit umfangreichen Basisleistungen für alle am DFN teilnehmenden Einrichtungen und einmal mit erweiterten Leistungen für Teilnehmer, die höhere Anforderungen an ihre Informationssicherheit haben und zudem durch ein geeignetes Informationssicherheitsmanagementsystem (ISMS) in der Lage sind, diese in ihre eigenen Informationssicherheitsprozesse zu integrieren. Im Folgenden werden die aktuellen Pläne zu den Basisleistungen vorgestellt. Die erweiterten Leistungen und der Betrieb des DFN-SOC wurden bereits in früheren Ausga-

> Auch für kleine Einrichtungen, die den IT-Grundschutz OPS.1.1.5 umgesetzt haben und somit bereits über einen zentralen Syslog-Server verfügen, bieten die Security Operations des DFN bei minimalem Aufwand einen maximalen Sicherheitsgewinn.
>
> *Michael Brosig, Leiter IT des Forschungsinstituts für Nutztierbiologie (FBN)*

ben der DFN-Mitteilungen ausführlich beschrieben.

Seit vielen Jahren bietet der DFN-Verein seinen Teilnehmern verschiedene Dienste im Kontext der Informationssicherheit an: Der CERT-Dienst umfasst Schwachstellenmeldungen, Automatische Warnmeldungen, den Netzwerkprüfer sowie die Incident Response. Der DoS-Schutz teilt sich auf in den DoS-Basisschutz für alle Einrichtungen sowie den erweiterten DoS-Schutz für Teilnehmer mit höheren Anforderungen. Im Rahmen der Einführung der Security Operations werden nun diese bestehenden Dienste konsolidiert. Die bisherigen Leistungsmerkmale des DFN-CERT-Dienstes und des DoS-Schutzes sowie die neu konzipierten Leistungsmerkmale der Security Operations werden in einem neuen DFN-Dienst gebündelt. Das vereinfacht das Management der Dienste sowohl auf DFN-Seite als auch auf Teilnehmerseite, da alle Basisleistungen automatisch zur Verfügung stehen. So muss beispielsweise der DoS-Basisschutz nicht mehr gesondert beauftragt werden und die erweiterten Leistungen für Security Operations und der erweiterte DoS-Schutz können als Ergänzung zu diesem konsolidierten Sicherheitsdienst hinzugebucht werden.

Die Basisleistungen der Security Operations sind komplementär und ergänzen sich. Der Teilnehmer kann frei entscheiden, welche der in Abb. 1 dargestellten Leistungsmerkmale er in Anspruch nehmen möchte und welche nicht. Die einzige Ausnahme ist die Zustellung von Warnmeldungen, da der DFN-Verein verpflichtet ist, den Teilnehmern ihm bekannte Hinweise auf Sicherheitsprobleme mitzuteilen.

Die Basisleistungen umfassen zunächst die bekannten Merkmale der Dienste DFN-CERT und DoS-Basisschutz. Hinzu kommen im Rahmen der Einführung der Security Operations weitere Merkmale, die ab Sommer 2022 in drei Phasen ausgerollt werden.

Phase 1: Zustellung von Warnmeldungen mit Domainbezug

Die am DFN teilnehmenden Einrichtungen erhalten derzeit automatisiert Warnmeldungen, wenn beim DFN-CERT Auffälligkeiten im Zusammenhang mit ihren IP-Adressen bekannt geworden sind. Zur Erstellung der Warnmeldungen

SECURITY OPERATIONS: BASISLEISTUNGEN

- **Incident Response:** Unterstützung durch das Incident Response Team (IRT) im Falle eines Sicherheitsvorfalls
- NEU **Zustellung Warnmeldungen:** mögliche Sicherheitsvorfälle mit Bezug zu IP-Adressen des Teilnehmers plus Handlungsempfehlungen (ab 01.07.22 zusätzlich Meldungen mit Bezug zu Internetdomains)
- **Zustellung Schwachstellenmeldungen:** zu vom Teilnehmer betriebenen IT-Systemen
- **Überprüfung eigenes Netz:** auf offen erreichbare Dienste und Schwachstellen durch den Netzwerkprüfer
- NEU **Überwachung IT-Systeme (begrenzte Anzahl):** auf Kompromittierungen durch Logfile-Analyse (geplanter Start 01.01.23)
- NEU **Überwachung IT-Systeme (begrenzte Anzahl):** auf Kompromittierungen durch aktives Dienstemonitoring (geplanter Start 01.07.23)
- **DoS-Basisschutz:** Analyse und Abwehr von DDoS-Angriffen
- **Zugriff DFN-CERT Portal:** Konfiguration der Leistungsmerkmale im Selfservice

beobachtet und analysiert das DFN-CERT eine Reihe von öffentlichen und teilweise nicht öffentlichen Quellen, um Vorfälle zu entdecken, die einen Bezug zu Systemen im DFN besitzen. Das DFN-CERT sammelt, korreliert und normiert diese Daten und stellt jedem DFN-Teilnehmer den Zugriff auf die Daten seiner Einrichtung zur Verfügung – inklusive der Möglichkeit, einrichtungsspezifische Einstellungen zu konfigurieren.

Die produktive Einführung der Basisleistungen erfolgt Mitte 2022 mit der Ergänzung des DFN-CERT-Dienstes um die Verwaltung von Domains. Dies ermöglicht den deutlichen Ausbau der Weitergabe von Warnmeldungen, wenn diese nicht über eine IP-Adresse, sondern über eine Domain einer Einrichtung zugeordnet werden müssen. Für die Verwaltung und Validierung der Domains führt der DFN-Verein Prozesse im DFN-CERT Portal ein, die sich an den bekannten Methoden der DFN-PKI orientieren.

Ein weiterer Bestandteil der Einführung von Security Operations ist der Ausbau der Warnmeldungen, mittels derer die Teilnehmer wichtige Informationen des DFN-CERT erhalten. Die Automatischen Warnmeldungen werden aktuell zweimal werktäglich um 10 und 14 Uhr per E-Mail versendet. Obwohl die Ereignisse, auf denen die Automatischen Warnmeldungen basieren, in Echtzeit über das DFN-CERT Portal eingesehen werden können, ist dieser Ansatz zur Bereitstellung der Daten für die Anforderung der Security Operations nicht ausreichend. Er wird darum dahingehend erweitert, dass bestimmte Meldungen häufiger erstellt und vom Teilnehmer komfortabel automatisch bezogen werden können.

Phase 2: Logfile-Analyse

Die zweite Phase, die für Anfang 2023 geplant ist, dient der Bereitstellung von Schnittstellen zur Übermittlung von Log-Daten an das DFN-CERT. Die Log-Daten werden anschließend anhand der im DFN-CERT vorhandenen Bedrohungsmuster (Indicators of Compromise, IoC) hinsichtlich potenzieller Sicherheitsvorfälle analysiert. Hierfür wird die für die erweiterten Leistungen aufgebaute Struktur der Log-Datenannahme und -analyse so erweitert, dass jeder Teilnehmer in beschränktem Umfang Log-Daten einliefern kann. Die Konfiguration dieses Leistungsmerkmals erfolgt voraussichtlich über das DFN-CERT Portal im Selfservice. Als Ergebnis der Log-Datenannahme und -analyse sollen skalierbare Prozesse zur Endpoint-Security und Servicesicherheit für eine ausgewählte Anzahl von besonders schützenswerten Systemen bei den teilnehmenden Einrichtungen geschaffen werden.

Phase 3: Aktives Dienstemonitoring

Die Realisierung der dritten und aktuell letzten Planungsphase ist für Mitte 2023 vorgesehen. In ihrem Zuge soll das bereits in den erweiterten Leistungen vorhandene Security-Monitoring auch in den Basisleistungen angeboten werden. Für Einrichtungen, die die erweiterten Leistungen nutzen, erfolgt die Konfiguration manuell durch Mitarbeitende des DFN-CERT – und skaliert somit nicht für einen breiten Einsatz. Darum müssen in dieser Phase die Möglichkeiten der Netzmodellierung im DFN-CERT Portal erweitert und auch Hostnamen in die Verwaltung aufgenommen werden. Durch das aktive Dienstemonitoring werden Teilnehmer beispielsweise über in Kürze ablaufende Zertifikate, unbeabsichtigt öffentlich verfügbare Serverdienste und andere, ähnlich gelagerte Sicherheitsmängel, informiert.

SECURITY OPERATIONS: ERWEITERTE LEISTUNGEN

- **Alle Basisleistungen plus Modellierung durch Fachleute des DFN-CERT**
- NEU **Bereitstellung und Betrieb Appliance „SOC-Agent“:** Aggregation von Daten (z. B. Log-Daten) plus vollautomatisierte und manuelle Untersuchung von Kompromittierungen durch Analysten des DFN-SOC
- NEU **Indicators of Compromise, IoC:** Aktive Suche nach neuen, unbekannten Bedrohungsmustern durch Threat Hunter im DFN-CERT
- NEU **Modellierung von Schutzgegenständen:** Regelmäßige Beratung und Unterstützung durch Fachleute des DFN-CERT
- **Erweiterter DoS-Schutz:** Erkennung, Analyse und Abwehr von DDoS-Angriffen

Security Operations: erweiterte Leistungen

Für Teilnehmer mit höherem Schutzbedarf bieten die Security Operations erweiterte Leistungen, die die umfangreichen Basisleistungen ergänzen: Sie decken mehr Bedrohungsszenarien ab und beinhalten eine erweiterte Datenanalyse sowie eine durch die Modellierung der Schutzgegenstände in den SOC-Werkzeugen zielgerichtete Versorgung. Das Plus an Leistungen schlägt sich aber auch auf der Aufwandsseite nieder: Sowohl beim Teilnehmer als auch beim DFN-Verein entstehen signifikant höhere Aufwände und zu erfüllende Voraussetzungen, die für die erfolgreiche Dienstnutzung unabdingbar sind. Die erweiterten Leistungen werden im Rahmen der Kostenumlage des DFN-Vereins künftig mit einer eigenen Kostenumlage angeboten werden.

Für die erweiterten Leistungen wird in den kommenden Jahren ein stetiges Wachstum der teilnehmenden Einrichtungen erwartet. Für einige Teilnehmer stellen die Basisleistungen zunächst einen Startpunkt dar. Im Zuge der zyklischen Verbesserung des eigenen ISMS wird gegebenenfalls ein Punkt erreicht werden, an dem die erweiterten Leistungen der Security Operations notwendig werden und die Voraussetzungen zur Nutzung geschaffen wurden. Zu diesem Zeitpunkt können sich Einrichtungen dann entscheiden, ob sie das Angebot der erweiterten Leistungen der Security Operations des DFN in Anspruch nehmen oder andere Lösungswege wählen.

> „Von der einrichtungsübergreifenden, DFN-weiten Erkennung von Angriffen von innerhalb oder außerhalb des X-WiN und der Anreicherung der Daten mit dem spezifischen Kontext der deutschen Hochschullandschaft erwarten wir eine zielgerichtete Unterstützung unserer Informationssicherheit. Besonders wichtig sind uns dabei die persönlichen Ansprechpartner am DFN-CERT, die die Bedarfe der Wissenschaft seit Jahrzehnten kennen."
>
> *Markus Krieger,*
> *Operative Gruppe (OG) des Rechenzentrums der Universität Würzburg*

ERWARTETE AUFWÄNDE FÜR DIE AUSBAUSTUFEN DER SECURITY OPERATIONS BEI TEILNEHMERN UND BEIM DFN-VEREIN

	BASISLEISTUNGEN	ERWEITERTE LEISTUNGEN
Teilnehmer	**Gering, vergleichbar mit DFN-CERT-Dienst** → Konfiguration der Leistungsmerkmale im Selfservice über das DFN-CERT Portal → (Manuelle) Bearbeitung der erhaltenen Meldungen im Best Effort	**Deutlich höher als Basis** → zentrales Logdaten-Management → Modellierung der IT-Landschaft → Einbindung der einrichtungsspezifischen Meldungen in eigene Prozesse → ISMS der Einrichtung muss hinreichenden Reifegrad haben → Geld- und Ressourcenbudget
DFN-Verein	**Aufwände steigen wenig mit wachsender Teilnehmerzahl und lassen sich im Rahmen der bestehenden Kostenumlage finanzieren** → Aufwände im Wesentlichen zur technischen und betrieblichen Umsetzung → danach hoher Grad der Automatisierung → daher kaum mit Teilnehmerzahl steigende Aufwände	**Aufwände steigen stark mit wachsender Teilnehmerzahl** → aktive manuelle Überwachung → regelmäßige, individuelle Workshops → teilnehmerspezifische Aufbereitung der Meldungen anhand der modellierten IT-Landschaft → Vorbereitung, Roll-out und Wartung der Appliance beim Teilnehmer

Fazit

Die Frage, ob eine Einrichtung die erweiterten Leistungen benötigt oder ob die vielfältig ausgestatteten Basisleistungen ausreichen, muss jede Einrichtung im Rahmen einer Risikoanalyse selbst beurteilen oder mit Unterstützung des DFN-CERT beurteilen lassen. Es ist aber wichtig festzustellen, dass die Nutzung der erweiterten Leistungen der Security Operations eine gewisse Reife des eigenen ISMS voraussetzt. Ist diese noch nicht gegeben, können die erweiterten Leistungen nicht adäquat in die eigenen Prozesse eingebunden werden. Damit Einrichtungen selbst überprüfen können, welche Option für sie geeignet ist, entwickelt der DFN-Verein derzeit ein „Self-Assessment Sheet".

Die neuen Basisleistungen der Security Operations ergänzen die bestehenden Dienste DFN-CERT und DoS-Basisschutz erheblich und können von allen teilnehmenden Einrichtungen ohne weitere Voraussetzungen über das DFN-CERT Portal im Selfservice genutzt werden. Sie sind so konzipiert, dass jede Einrichtung ihr Sicherheitsniveau unabhängig von der Reife des eigenen ISMS nachhaltig ergänzen kann.

Der DFN-Verein schafft im Rahmen der Einführung von Security Operations ein Leistungsportfolio, das über die bestehenden und etablierten DFN-Dienste weit hinausgeht, indem es diese verbessert und ergänzt. Durch die Bereitstellung von Basisleistungen und erweiterten Leistungen wird sichergestellt, dass für jede am DFN teilnehmende Einrichtung der adäquate Schutz geboten wird – unabhängig von der Größe der Einrichtung und unabhängig davon, ob das eigene Informationssicherheitsmanagement noch ganz am Anfang steht oder schon etabliert und ausgereift ist.

Ein großer Dank geht an die Pilotteilnehmer der DFN Security Operations. Bei der technischen und organisatorischen Vorbereitung des Dienstes leisten sie einen wertvollen Beitrag, der allen DFN-Teilnehmern zugutekommt. ◆

In den Ausgaben 98 („Security Operations im DFN – ein neuer Dienst entsteht", S. 36) und 99 („Security Operations im DFN – die technische Basis", S. 30) der DFN-Mitteilungen finden Sie detaillierte Informationen zum Konzept des neuen Dienstes sowie zu den Use Cases der neuen Leistungsmerkmale.

> Die jahrelange Zusammenarbeit mit dem DFN-CERT wird durch das DFN-SOC weiter intensiviert. Wir freuen uns, unsere relevanten Daten jetzt in Echtzeit mit einer größeren Community teilen zu können und erhoffen uns durch Daten anderer Einrichtungen eine weitere Erhöhung unseres Sicherheitsniveaus.
>
> *Jens Hektor,*
> *IT Center der RWTH Aachen*

So was von souverän

Die Welt der digitalen Identitäten ist einem steten Wandel unterworfen. Mit dem Konzept der Decentralised bzw. Self-Sovereign Identity drängen Wirtschaft und Politik auf einen Paradigmenwechsel. Nachdem das Thema nun auch in den Bereichen Bildung, Forschung und Hochschulverwaltung angekommen ist, stellen sich die Fragen, ob und wie sich das Vertrauensgefüge einer akademischen Föderation wie der DFN-AAI auf dieses Konzept abbilden lässt – und welche Konsequenzen ein entsprechender Wechsel des Föderationsmodells hätte.

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

Illustration: Gerd Altmann / Pixabay

Schöne neue Welt: Die digitale Brieftasche

Zu den selbstverständlichen Aufgaben des DFN-Vereins gehört es, das Diensteportfolio gemäß dem jeweiligen Stand der Technik weiterzuentwickeln. Das Maß der Dinge sind hierbei die Bedürfnisse und Anforderungen der teilnehmenden Einrichtungen bzw. der Community. In diesem Zusammenhang verfolgt das Team der DFN-AAI laufend aktuelle Entwicklungen im Bereich digitale Identitäten und Vertrauensdienste. Dazu gehört auch das Konzept der sogenannten Self-Sovereign Identity, das seit einiger Zeit von Wirtschaft und Politik vorangetrieben wird.

Den bislang nachhaltigsten Einfluss auf diese Entwicklung wird mutmaßlich der Anfang Juni 2021 von der Europäischen Kommission veröffentlichte Vorschlag zur Änderung der eIDAS-Verordnung haben, häufig auch als eIDAS 2.0 bezeichnet [1]. Nachdem eIDAS bislang weitgehend auf den öffentlichen Sektor abzielt, sollen die von der geplanten Änderungsverordnung adressierten Vertrauensdienste nun auch für die Privatwirtschaft geöffnet werden. Das Ziel ist, einen einheitlichen europäischen digitalen Binnenmarkt zu schaffen. Eine zentrale Rolle hierbei spielt die Schaffung eines Frameworks für eine europäische digitale Identität, der EUid.

Dabei werden künftig nicht nur Identitätsdaten, sondern auch digitale Nachweise in einer digitalen Brieftasche, der EUid-Wallet, abgelegt. Nachweise und Wallet sollen von den Bürgerinnen und Bürgern eigenverantwortlich verwaltet werden, z. B. auf einem mobilen Endgerät. Nutzende können sich ihre Identitätsdaten sowie Bildungsnachweise und Zertifikate etc. von den jeweils zuständigen Behörden oder Hochschulen für besagte digitale Brieftasche ausstellen lassen. Um sich gegenüber Dritten auszuweisen bzw. bestimmte Nachweise zu führen, wählen sie einfach die passenden in der Wallet abgelegten Daten aus und entscheiden selbst, welche Informationen für diesen Zweck übertragen werden sollen. Daher wird dieses Konzept auch als „selbstbestimmte Identität“ (Self-Sovereign Identity, SSI) bezeichnet. Eine weitere geläufige Bezeichnung ist dezentrale Identität, „Decentralised Identity“, weil in diesem Konzept keine zentrale Stelle existiert, die als alleinige Quelle von Identitätsdaten dient.

Der von der eIDAS 2.0 verfolgte Ansatz ist nicht grundsätzlich neu und wird bereits im Rahmen verschiedener EU-Projekte und Förderlinien verfolgt, z. B. dem European Self-Sovereign Identity Framework (ESSIF) innerhalb der European Blockchain Service Infrastructure (EBSI). Auch für GAIA-X wird ein SSI-basierter Ansatz für das Identity- und Access-Management favorisiert. Auf Bundesebene seien als Beispiele die vier vom Bundeswirtschaftsministerium geförderten Schaufensterprojekte „Sichere digitale Identitäten“ sowie das Projekt DISKURS [2] genannt, das unter anderem auch mögliche SSI-Anwendungsfälle im Kontext des Onlinezugangsgesetzes (OZG) untersucht.

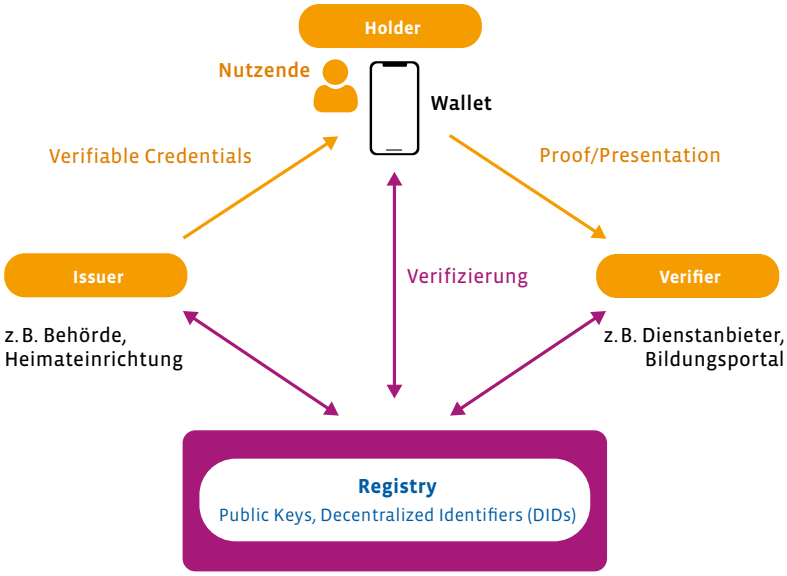


Abbildung 1: SSI: Rollen und Interaktionen

Als Betreiber der DFN-AAI hat der DFN-Verein ein vitales Interesse daran zu untersuchen, welche Konsequenzen ein solcher Paradigmenwechsel mittel- und langfristig für eine als Föderation betriebene Authentifizierungs- und Autorisierungs-Infrastruktur (AAI) wie die DFN-AAI mit sich bringt und wie sich das bestehende Vertrauensgefüge der DFN-AAI ggf. auf das neue Modell abbilden lässt bzw. welche Anpassungen hierfür erfolgen müssten.

Die Brieftasche im Kontext

Doch wie funktioniert das SSI-Konzept, in dessen Zentrum die als „Holder“ bezeichneten Nutzenden mit ihren jeweiligen digitalen Brieftaschen („Wallet“) stehen? Betrachten wir hierzu das Schema der Rollen und Interaktionen (Abb. 1):

WEITERFÜHRENDE INFORMATIONEN

Einen guten Überblick über aktuelle, öffentlich geförderte SSI-Initiativen und -Projekte bietet eine im Januar 2022 veröffentlichte Studie der ENISA [3], die vor dem Hintergrund der geplanten eIDAS-Änderungsverordnung eine Bestandsaufnahme durchführt und sich kritisch mit den eingesetzten Technologien und Standards auseinandersetzt. Mit der Herkunft des Konzepts der Self-Sovereign Identity beschäftigt sich Christian Kahlo in seinem Onlineartikel „Blockchain + SSI = ID?“ [4], in dem der Einsatz von Blockchain bzw. Distributed Ledger-Technologien für SSI-Infrastrukturen kritisch hinterfragt wird. Zu dem Schluss, dass Distributed Ledger-Technologien (DLT) für die Umsetzung des SSI-Konzepts nicht notwendig und eher kritisch zu bewerten sind, kommt auch das BSI in seinem kürzlich veröffentlichten Eckpunktepapier zu Self-Sovereign Identities [5].

Vom Issuer zum Holder

Ein „Holder“ (Person, die die Identität innehat) kann sich bestimmte Eigenschaften (Attribute/Claims) wie das Geburtsdatum oder die Zugehörigkeit zu einer Einrichtung/Abteilung sowie ggf. Nachweise, z. B. Zeugnisse von der jeweils dafür zuständigen Stelle, dem „Issuer“, bestätigen bzw. ausstellen lassen. Hierzu muss sich der Holder zunächst gegenüber dieser Stelle authentisieren. Der Issuer signiert die von ihm herausgegebenen Daten kryptografisch, um deren Echtheit und Ursprung zu bestätigen. Damit dieses Verfahren funktioniert, muss der Issuer über einen sogenannten Decentralised Identifier (DID) in einem Register („Registry“) eingetragen sein. Ein DID verweist stets auf ein Dokument, das weitere Angaben, insbesondere zu Verifizierungsmechanismen, enthält, i. d. R. einen öffentlichen Schlüssel, anhand dessen die Signaturen des Issuers verifiziert werden können.

Diese signierten Daten werden als „Verifiable Credentials“ (VCs) bezeichnet. Zudem können VCs seitens des ausstellenden Issuers mit einer Gültigkeitsdauer versehen und ggf. auch wieder zurückgezogen werden. Diese Verifiable Credentials kann der Holder nun selbst in seiner Wallet auf einem beliebigen Endgerät verwalten und sich damit zu einem späteren Zeitpunkt, z. B. für den Zugriff auf einen Onlinedienst autorisieren, ohne dass der Issuer hierfür in irgendeiner Weise involviert wird.

Vom Holder zum Verifier

Betrachten wir nun die Kommunikation des Holders mit der Stelle, die seine ausgewählten VCs aus der Wallet bzw. eine als Nachweis („Proof“) daraus abgeleitete „Verifiable Presentation“ prüft, dem „Verifier“ oder „Prüfer“. Dabei kann es sich beispielsweise um einen Onlinedienst handeln, der prüft, ob die betreffende Person eine bestimmte Eigenschaft hat, die sie berechtigt, auf gewisse Ressourcen zuzugreifen, z. B. anhand der als VC bestätigten Zugehörigkeit zu einer bestimmten Einrichtung.

Der Verifier muss nun den vom Holder vorgelegten Proof auf seine „Echtheit“ überprüfen. Hierbei gilt, dass alle zur Verifizierung benötigten Informationen – das sind der Issuer, die verwendeten Signaturalgorithmen sowie das öffentliche Schlüsselmaterial – in der bereits oben erwähnten Registry hinterlegt sind und über entsprechende Referenzen im vorgelegten Proof abgerufen werden können. Die Registry entspricht in ihrer Funktion also ein Stück weit den Föderationsmetadaten in einer AAI-Föderation.

Bei dem oben beschriebenen Verfahren zur Ausstellung und Übertragung von Verifiable Credentials haben die Nutzenden die volle Kontrolle darüber, welche Informationen Sie an einen Verifier übertragen. Grundsätzlich bietet das SSI-Konzept die Möglichkeit, die Prinzipien der Datensparsamkeit und der Pseudonymisierung der Nutzenden umzusetzen. Dies hängt jedoch von der Art der Nachweise bzw. der Generierung derselben ab. So macht es beispielsweise einen deutlichen Unterschied, ob zum Altersnachweis das Geburtsdatum oder lediglich die Information übertragen wird, dass die betreffende Person jünger oder älter als 18 Jahre ist.

Vergleich zur AAI

Für die Nutzenden liegt ein Vorteil des SSI-Konzepts darin, dass die für die Ausstellung der Credentials zuständigen Stellen keine Kenntnis und keine Kontrolle darüber haben, wann und wem gegenüber diese verwendet werden.

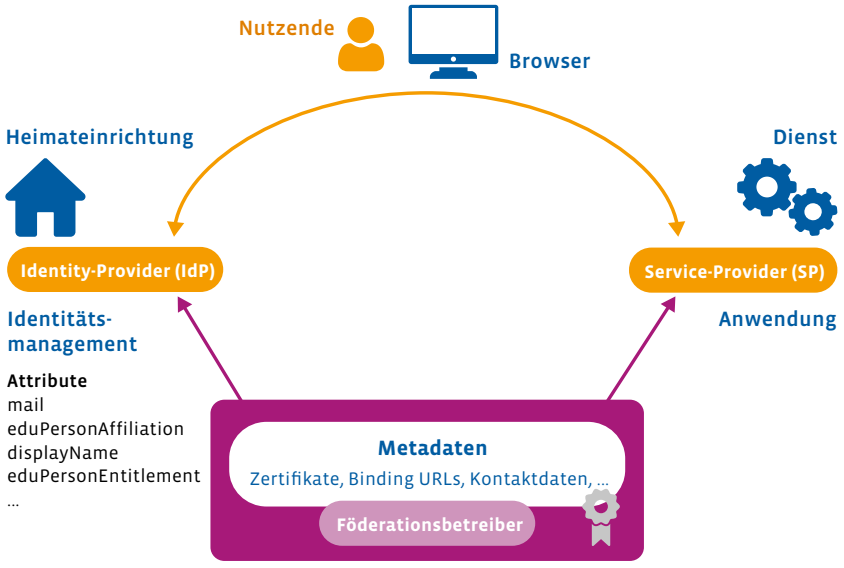


Abbildung 2: Rollen und Interaktionen in einer AAI-Föderation

Im AAI-Konzept (Abb. 2) entspricht die Rolle des Issuers der des Identity-Providers der Heimateinrichtung, der eine Person als Beschäftigte oder Studierende angehört. Möchte jemand in der AAI-Welt via Browser auf einen AAI-Dienst, d. h. einen Service-Provider, zugreifen, erfolgt seitens des Service-Providers ein Redirect über den Browser zum Identity-Provider (IdP) der jeweiligen Heimateinrichtung. Unmittelbar nach erfolgreicher Authentisierung des Nutzers bzw. der Nutzerin am IdP überträgt dieser die zur Nutzung des betreffenden Dienstes erforderlichen Attribute an den anfragenden Service-Provider (SP) – oder auch nicht. Moderne IdP-Implementierungen verfügen zwar über ein sogenanntes User Consent Modul, anhand dessen die Nutzenden die an einen SP zu übertragenden

Daten kontrollieren bzw. freigeben können. Das funktioniert jedoch nur, wenn seitens des IdP-Betreibers bereits eine grundsätzliche Freigabe der benötigten Attribute für den betreffenden SP besteht. Letzteres ist nicht immer der Fall. Das stellt eines der großen Probleme dar, mit denen die DFN-AAI konfrontiert ist. In einer SSI-Infrastruktur hingegen liegt die Entscheidung zur Weitergabe von Daten ausschließlich bei den Nutzenden. Außerdem ist ein Issuer-seitiges User-Tracking nicht möglich.

Nicht ohne Probleme

Grundsätzlich bietet das SSI-Konzept die Möglichkeit, ein hohes Niveau an Datenschutz zu realisieren, wobei es sich bei diesem Konzept bzw. den zugrunde liegenden Standards nicht notwendigerweise um Privacy-by-Design handelt. Vielmehr geht es darum, bei der Implementierung darauf zu achten, alle Möglichkeiten des User-Trackings zu unterbinden und Man-in-the-Middle-Attacks bei der Kommunikation zwischen Holder und Verifier zu verhindern.

Von zentraler Bedeutung bei der Verhinderung von User-Tracking sind die Generierung und das Management von Identifiern, namentlich der Holder-DIDs. Keinesfalls sollte ein Issuer den DID eines Holders in ein Verifiable Credential hineinschreiben, welches dann womöglich noch 1:1 an einen Verifier weitergereicht wird. Außerdem muss die SSI-Implementierung in der Lage sein, pro Verifier einen separaten Holder-DID anzulegen, damit keine dienstübergreifenden User-Profile erstellt werden können und eine pseudonyme Nutzung von Diensten grundsätzlich ermöglicht wird. Dies entspricht dem Prinzip der „targeted“ bzw. „pairwise“IDs in der AAI-Welt.

Noch entscheidender ist es, Man-in-the-Middle-Attacks zu vermeiden. In der Praxis wird einer Person als Holder ein QR-Code angezeigt, wenn es darum geht, bestimmte Credentials an einen Verifier zu übertragen. Wie kann die betreffende Person sicher sein, dass ihre Daten tatsächlich an eine vertrauenswürdige Stelle übertragen werden? Ein möglicher Sicherheitsmechanismus bestünde darin, dass sich Verifier auch ihrerseits gegenüber einem Holder authentisieren müssen. Außerdem könnten die URLs, zu denen Holder-Credentials übertragen werden, in der Registry hinterlegt werden. Auf diese Weise könnte Holder-seitig überprüft werden, ob ein QR-Code bzw. eine URL vertrauenswürdig ist – vorausgesetzt, es besteht Vertrauen in die Instanz, die die Registry betreibt. Dieser Mechanismus ist in der AAI-Welt, in der Binding URLs Bestandteil der vom Föderationsbetreiber signierten Föderationsmetadaten sind, seit Langem etabliert. Vergleichbare Mechanismen scheinen in den aktuellen SSI-Standards bislang nicht vorgesehen zu sein.

Weitere problematische Punkte sind die noch im Fluss befindliche Standardisierung und die vergleichsweise hohe Anzahl an Einzelstandards, die beim SSI-Konzept zum Tragen kommen. Die oben erwähnte ENISA-Studie listet allein sechs Standards auf, weist aber darauf hin, dass die Liste nicht vollständig ist. Im Gegensatz hierzu bieten die im AAI-Umfeld etablierten Standards SAML2 und OpenID Connect einen kohärenten Satz an Spezifikationen, die praktisch alle kritischen Aspekte abdecken. Gegen einen Einsatz im Föderationskontext spricht auch der Umstand, dass derzeit weder für die Modellierung von Informationen zur Verlässlichkeit von Identitäten (Levels of Assurance) noch für die Sicherheit der Authentifizierung von Nutzenden/Holdern gegenüber Issuern entsprechende Standards existieren, die innerhalb einer akademischen Föderation genutzt werden könnten. Selbiges gilt für Attribut-Schemata.

Ein weiteres grundsätzliches Problem ist die Frage, wie ein Holder verlorenes Schlüsselmaterial und/oder Credentials wiederherstellen kann. Ein Backup bei einem Cloud-Anbieter ist vielleicht nicht die allerbeste Idee. Und wie sicher ist eine digitale Brieftasche auf einem Smartphone, für das der Hersteller keine Security-Updates mehr bereitstellt?

Vertrauen

Beiden Konzepten gemein ist der Umstand, dass es einen Vertrauensanker geben muss: eine Instanz, die Regeln festlegt, in deren Rahmen die diversen Akteure an der betreffenden Infrastruktur teilnehmen. Im hier betrachteten Anwendungsfall ist das der Föderationsbetreiber.

REFERENZEN

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity
https://eur-lex.europa.eu/procedure/EN/2021_136
[2] Forschungsprojekt DISKURS
https://www.unibw.de/software-security/forschung/diskurs-disput
[3] ENISA, Digital Identity: Leveraging the SSI Concept to Build Trust
https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust
[4] Christian Kahlo, Blockchain + SSI = ID?
https://medium.com/@ckahlo?p=d7e51d98d050
[5] BSI, Eckpunktepapier für Self-sovereign Identities (SSI)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.html
[6] https://www.switch.ch/de/about/innovation/overview/switch-innovation-lab-self-sovereign-identities/
[7] https://www.surf.nl/files/2021-05/technical-exploration-surf-ledger-based-self-sovereign-identity.pdf

Wie dieses Vertrauen auf technischer Ebene modelliert wird, unterscheidet sich je nach dem Modell, welches wir betrachten. In einer Föderation wie der DFN-AAI bilden die Föderationsmetadaten das technische Rückgrat der Föderation (Abb. 2). Die an der Föderation teilnehmenden Akteure vertrauen den in den Föderationsmetadaten hinterlegten Binding URLs, dem Schlüsselmaterial etc., weil diese Metadaten vom Föderationsbetreiber signiert sind. Im SSI-Modell fehlt dieses Konzept. Bei der Registry handelt es sich um eine i. d. R. verteilte Datenbankanwendung, die nicht wie eine Datei signiert werden kann. Entweder die Akteure vertrauen den Public Keys und den sonstigen in der Registry hinterlegten Angaben einfach, weil sie da sind, d. h. registriert werden konnten, oder das Vertrauen basiert auf einer Signaturhierarchie, einer Root CA (oder mehreren), auf die alle registrierten Public Keys rückführbar sind. In diesem Fall dient eine Public Key Infrastructure (PKI) als Vertrauensanker (Abb. 1).

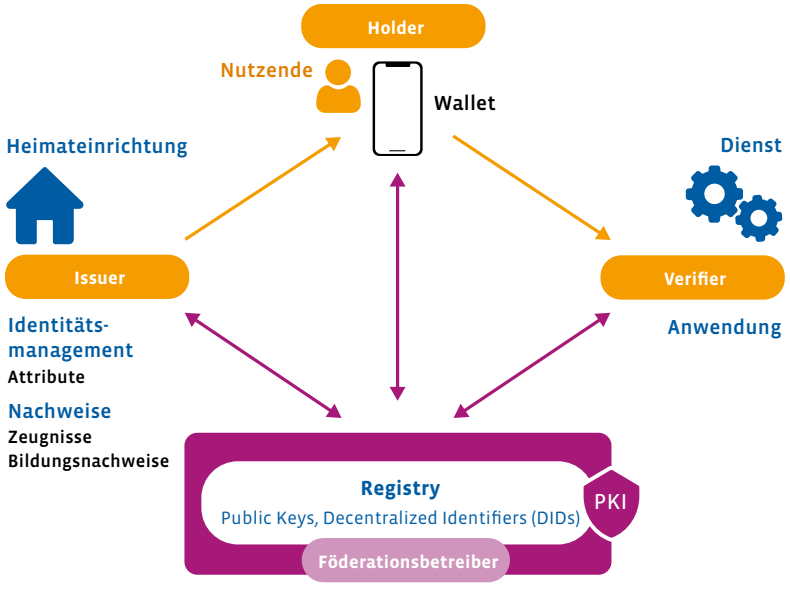


Abbildung 3: Modell einer SSI-basierten Föderation

SSI-Föderation, ja oder nein?

Vorausgesetzt, die oben genannten Probleme werden eines Tages gelöst, wäre es prinzipiell denkbar, eine Föderation gemäß des SSI-Konzept zu modellieren. Die teilnehmenden Heimateinrichtungen würden anstatt eines Identity-Providers eine Issuer-Implementierung betreiben und die Dienstanbieter eine Verifier-Komponente anstatt eines Service-Providers. Anstelle einer Metadatenverwaltung müsste der Föderationsbetreiber eine Registry und eine eigene Root CA bzw. PKI betreiben (Abb. 3). Aufgrund der aktiven Rolle der Nutzenden als Holder, die ebenfalls auf die Registry zugreifen, wäre in einem solchen Modell mit einem weitaus höheren Support-Aufwand seitens des Föderationsbetreibers zu rechnen, als dies in einer klassischen AAI der Fall ist. Von diesem Konzept würden am ehesten die Nutzenden profitieren. Diese wären für den Zugriff auf bestimmte Dienste nicht mehr auf IdP-seitige Attribut-Filtermechanismen angewiesen.

Fazit und Ausblick

Dieser Artikel reflektiert eine vorläufige und kursorische Auseinandersetzung der DFN-AAI mit dem Konzept der Self-Sovereign Identity und ist somit lediglich als Werkstattbericht zu verstehen. Um ein besseres Verständnis hinsichtlich der Vor- und Nachteile dieses Konzepts und dessen Anwendbarkeit auf akademische Föderationen zu entwickeln, beteiligt sich der DFN-Verein als „Contributor“ – nicht geförderter Partner – an einem der Schaufensterprojekte „Sichere digitale Identitäten“ namens IDunion. Im Rahmen dieses Projekts werden auch Anwendungsfälle aus dem Hochschulbereich behandelt. Das Thema „Decentralised Identity“ wird in der kommenden Förderphase des GÉANT-Projects GN5-1, an dem sich der DFN-Verein beteiligen wird, adressiert werden. In diesem Kontext werden auch die Ergebnisse miteinbezogen, die andere Föderationen bei der Analyse und Bewertung des SSI-Konzepts erzielt haben. Insbesondere SWITCHaai (Schweiz) [6] und SURFconext (Niederlande) [7] haben entsprechende Vorarbeiten geleistet.

Letztendlich muss es darum gehen, die Anforderungen und Bedürfnisse der an der DFN-AAI teilnehmenden Einrichtungen auf bestmögliche Weise technisch umzusetzen und auf das Dienstportfolio des DFN-Vereins abzubilden. Der DFN-Verein wird das Thema in jedem Fall weiterverfolgen und die Community über neue Entwicklungen auf dem Laufenden halten. Aktuell stellt das SSI-Konzept keine Alternative zum bestehenden Föderationsmodell der DFN-AAI dar. ◆

Aufbau eines Management-systems – Tools vs. Prozesse

Der Aufbau eines Managementsystems zur Steuerung der Unternehmens-IT ist mit erheblichem Aufwand verbunden, insbesondere für kleine oder mittelgroße Einrichtungen. Anstatt aber viel Geld in spezialisierte Tools zu stecken, ist ein leichtgewichtiger Ansatz in vielerlei Hinsicht von Vorteil. Denn bei der Neugestaltung und Anpassung von Prozessen an die eigene Einrichtung geht es in erster Linie um organisatorische Fragestellungen. Auch die beste Software von der Stange kann eine strukturierte Vorgehensweise nicht ersetzen. Das Leibniz-Rechenzentrum (LRZ) betreibt seit einigen Jahren ein zertifiziertes Managementsystem und setzt dabei voll auf ein generisches Dokumentenmanagementsystem (DCMS).

Text: **Stefan Metzger, Miran Mizani, Michael Schmidt** (Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften, LRZ)

Viele Organisationen im staatlichen sowie im privaten Bereich verfolgen seit mehreren Jahren das Ziel, die Qualität der von ihnen bereitgestellten IT-Dienste oder Produkte zu verbessern – und gleichzeitig genutzte IT-Infrastrukturen und dort verarbeitete Informationen vor Angriffen zu schützen. Orientiert an international anerkannten Standards und Normen wird hierfür in vielen Fällen ein Managementsystem (MS) geplant und etabliert. Die Realität zeigt jedoch, dass Organisationen mit zunehmender Anzahl geschäftskritischer Dienste und einem Anspruch, eine sichere, wirksame und systematisch gemanagte IT-Infrastruktur zu schaffen, einem erheblichen Verwaltungsaufwand für die Erstellung von Richtlinien sowie Prozess- und Verfahrensbeschreibungen gegenüberstehen. Gerade in kleinen und mittelgroßen Organisationen stellt sich die Frage, wie ein MS effektiv aufgebaut werden kann, ohne hohe finanzielle und personelle Ressourcen in unterstützende Software investieren zu müssen. In diesem Artikel wird beispielhaft das Leibniz-Rechenzentrum (LRZ) betrachtet, das seit einigen Jahren selbst ein zertifi-

Foto: twenty20photos

ziertes Managementsystem für die Bereiche IT-Service- und Informationssicherheitsmanagement (SMS und ISMS) betreibt. Mit Ausnahme weniger Prozesse, welche einen hohen Grad an Automatisierung voraussetzen, wurden alle Teile des Managementsystems organisatorisch und mithilfe eines generischen Dokumentenmanagementsystems (DCMS) implementiert.

Am LRZ wird dabei auf ein Wiki-System gesetzt, jedoch können die Konzepte grundsätzlich mit jeder Art von textbasierten DCMS umgesetzt werden. Da ein solches heute in den meisten Organisationen bereits vorhanden ist, kann es sehr einfach für die in einem Managementsystem notwendige Dokumentation genutzt werden, ohne zusätzlichen technischen Overhead oder großen Einführungsaufwand für spezialisierte MS-Tools zu erzeugen. Dies soll im Folgenden an drei zentralen Aspekten eines MS veranschaulicht werden.

Umgang mit Werten, Risiken und Chancen

Ein zentraler Teilbereich in vielen MS ist der Umgang mit Risiken und Chancen innerhalb der Organisation. Dazu gehören die Inventarisierung und Bewertung von Organisationswerten (Assets), die Identifikation von Bedrohungen sowie die Umsetzung angemessener Maßnahmen. Dabei hat sich gezeigt, dass bereits einfache Vorlagen ausreichen, um ein effektives Risikomanagement (RM) zu betreiben. Wichtig sind die organisatorischen Abläufe, die den Lebenszyklus der Assets sowie der Risiken und Maßnahmen widerspiegeln und daher in das DCM eingebettet sein müssen. Unabhängig davon müssen alle bewerteten Risiken und Chancen von der obersten Leitung freigegeben werden, damit entsprechende Ressourcen bereitgestellt werden können. Die Umsetzung sollte anschließend in die anderen Managementprozesse eingebunden werden. Ein einfaches Konzept ist in Abbildung 1 [RM-Konzept] dargestellt. So wurde im Rahmen des Asset-Managements (AM) ein Owner festgelegt, der die fachliche Verantwortung für ein Asset, dessen Schutzbedarf und die Durchführung des RM-Prozesses trägt. Im Kontext des RM kann dieser bei der Durchführung der Risikoeinschätzung von weiteren Personen unterstützt werden. Der Asset Owner liefert ein bewertetes Risiko sowie einen Vorschlag für die Risikobehandlung, die entweder freigegeben oder abgelehnt wird. Dieses Vorgehen entlastet sowohl den Risikomanager als auch die oberste Leitung, da das RM in der Breite der Organisation durchgeführt wird (bottom-up).

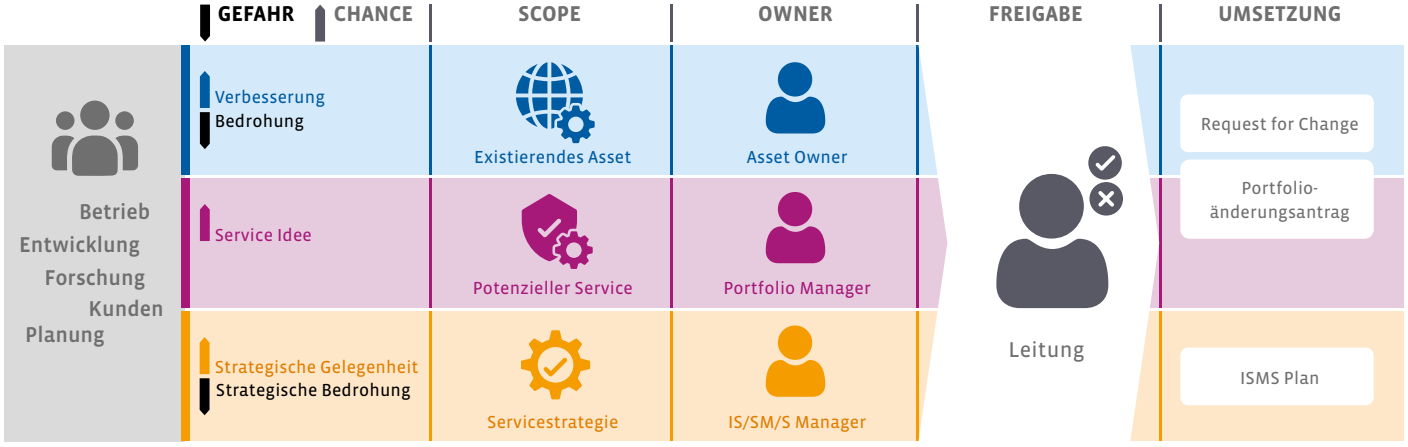


Abbildung 1: RM-Konzept

Die im AM erfassten Werte der Organisation werden im Risikomanagement auf mögliche Risiken hin untersucht. Spezialisierte RM-Tools bieten zwar Möglichkeiten zur einfachen Verknüpfung von Assets, Risiken und Maßnahmen oder eine automatisierte Berechnung der Risikohöhe. Beim Aufbau eines MS sind solche Funktionen jedoch noch nicht notwendig. Besonders in der Anfangszeit sind organisatorische Aspekte die größte Hürde: Das Etablieren der Prozesse, deren Verankerung in allen Bereichen der Organisation und die Sensibilisierung bzw. Schulung des Personals sollten Priorität haben. Das von der ISO-Norm skizzierte Vorgehen zum Umgang mit Risiken und Chancen ist sehr simpel und kann problemlos ohne aufwendige technische Features durchgeführt werden.

MS-Prozesse und Reporting

Ein Managementsystem fordert an vielen Stellen Aufzeichnungen über dessen Zustand und Möglichkeiten, organisatorische Änderungen nachverfolgen zu können. Ein DCMS hilft, derartige Aufzeichnungen strukturiert zu erfassen und zu pflegen. Im Folgenden werden zwei Betriebsprozesse exemplarisch vorgestellt.

Zentral ist das Service-Portfolio-Management, welches die Services entsprechend der Servicestrategie ausrichtet. Viele Organisationen starten hier mit einer Software, um die Services aufzulisten und zu verwalten. Um etwa das Serviceportfolio

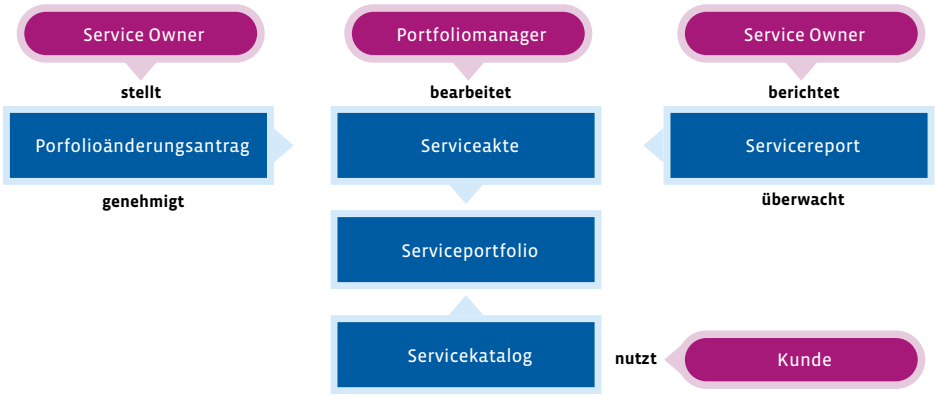


Abbildung 2: SPM-Konzept

aus mehr als 60 externen Diensten zu strukturieren, wurden am LRZ verschiedene Dokumenttypen definiert (Abbildung 2 [SPM-Konzept]). Zu jedem Service existiert eine Serviceakte, die alle Eigenschaften des Services beschreibt und Referenzen auf alle weiteren Dokumente dieses Services enthält. Das Serviceportfolio ist dann als einfache Liste dieser Serviceakten umgesetzt.

Werden die den Service beschreibenden Textbausteine und Attribute in den Serviceakten von den verantwortlichen Service Ownern gepflegt, dann kann der Servicekatalog für die Kunden direkt daraus generiert und dann lediglich um einleitende Worte ergänzt werden. Um Änderungen am Portfolio nachverfolgen zu können, wird für jede relevante Änderung ein Portfolioänderungsantrag angelegt. Dabei handelt es sich um ein eigenständiges Dokument, welches die Inhalte, Gründe, Kosten, Risiken und Chancen einer Änderung beschreibt.

Der Prozessservice Reporting im Servicemangementsystem überwacht die Services des Portfolios. Dafür werden in vielen Organisationen umfangreiche Reporting-Tools etabliert, welche oftmals lediglich dem Zweck dienen, Verfügbarkeitswerte der Dienste aus verschiedensten Monitoring-Lösungen zu aggregieren. Auch hier ist es beim Aufbau eines MS meist wichtiger zu definieren, was Servicequalität für die Organisation konkret bedeutet und wie diese überwacht werden kann, als möglichst viele Kennzahlen mithilfe eines Tools zu erfassen. Anforderungen der Normen lassen sich leicht manuell mit einem eigenständigen Dokument pro Service dokumentieren. Dabei sollte mindestens zwischen den Aspekten Verfügbarkeit und Servicestatus unterschieden werden. Der Servicestatus subsumiert relevante Informationen wie die Einhaltung des Servicelevels, das Auftreten von Ereignissen, durchgeführte Kundengespräche, aufgetretene Beschwerden und die aktuell wahrgenommene Kundenzufriedenheit.

Diese beiden sowie die meisten anderen Prozesse lassen sich somit sehr einfach dokumentieren und organisieren. Auch hier besteht die eigentliche Herausforderung darin, sich zu überlegen, wie die Prozesse in der eigenen Organisation umgesetzt werden können.

Bewertung der Leistung mittels Kennzahlen

Einem PDCA-Ansatz (Plan, Do, Check, Act) folgend gilt es, die Leistung des MS kontinuierlich bspw. anhand von Kennzahlen zu überprüfen und identifizierte Verbesserungspotenziale umzusetzen. Auch hier wird oftmals in komplexe Tools zur Erfassung von Kennzahlen oder zum Task-Tracking investiert.

Erfassen von Kennzahlen

Business-Intelligence-Tools helfen zwar bei der Erhebung von Daten, jedoch nicht bei der Definition einschlägiger Kennzahlen. Deshalb kann es sich gerade in der Anfangszeit eines MS lohnen, mehr Zeit in die Identifikation und Etablierung sinnvoller und hilfreicher Kennzahlen zu investieren als in ihre automatisierte Erhebung.

Ein manuell gepflegtes Tabellenlayout für Prozesskennzahlen ist zu Beginn völlig ausreichend. Dabei ist es ratsam, die Kennzahlen in einfache Messwerte, Performance-Indikatoren und Key-Performance-Indikatoren (KPI) zu unterteilen und lediglich die KPIs in einer prozessübergreifenden Übersicht zu aggregieren. Viele DCMS oder Wiki-Lösungen bieten bereits die Möglichkeit, dynamisch erstellte Tabellen zu generieren. Pro Kennzahl sollten mindestens Titel, Beschreibung, Typ, Zielwert sowie ggf. die Quelle erfasst werden. Abhängig von der Definition der Kennzahl ist eine quartalsweise (und für die meisten Prozesse manuelle) Erhebung ein guter Startwert. Nach deren Erhebung sollten die Kennzahlen einem Review unterzogen und hierin ggf. Korrektur- bzw. Verbesserungsmaßnahmen abgeleitet werden.

Meilenstein- und Aufgabenverwaltung

Unterstützt durch Kennzahlen können im Rahmen der kontinuierlichen Verbesserung stetig Verbesserungspotenziale für das MS identifiziert werden. Neben jenen lassen sich auch Empfehlungen und Nebenabweichungen aus Audits oder Management-Reviews nachverfolgen und die notwendige Nachweisdokumentation für das nächste Audit liefern.

Gänzlich ohne ein spezialisiertes Task-Tracking-Tool hat sich hierfür ein einfacher Ansatz mit einem Dokument je Task und aggregierenden Übersichtsseiten bewährt. Jeder Task wird genau einem Meilenstein – etwa dem nächsten internen Audit oder dem Jahresabschluss – zugeordnet.

Bewährt hat sich auch ein Verfahren, das allen Beschäftigten erlaubt, Tasks mit Relevanz für das MS zu identifizieren und ins Backlog einzufügen. Die Freigabe bzw. Zuordnung des Tasks zu einem Meilenstein erfolgt dann durch die für das MS verantwortliche Person, welche damit auch Ergebnisverantwortliche und Bearbeitungsfrist

des Tasks festlegt. Zudem ist ein regelmäßiges Review der Taskfortschritte durch den MS-Verantwortlichen ratsam, um ggf. nachsteuern oder zusätzliche Ressourcen bereitstellen zu können.

Erfahrungen aus der Praxis

Nach gut vier Jahren praktischer Erfahrung am Leibniz-Rechenzentrum hat sich gezeigt, dass ein DCMS geeignet ist, um darauf aufbauend ein MS zu etablieren. Vorteilhaft war die Flexibilität, die ein textbasiertes Werkzeug dabei lieferte. Gerade beim Aufbau des ersten MS in einer Organisation sind viele Rahmenbedingungen noch nicht klar. Neue Prozesse müssen definiert und dabei zeitgleich in den Betrieb integriert sowie an den Bedarf der Fachabteilungen ausgerichtet werden. Spezialisierte Abläufe, leichtgewichtige Verfahren und regelmäßige Änderungen an Prozessen sind in dieser Anfangsphase recht häufig und in einem DCMS leicht und ohne zusätzliche Kosten oder Entwicklungsaufwand umzusetzen.

Auf der anderen Seite fehlen einem generischen DCMS einige Komfortfunktionen und Möglichkeiten zur Automatisierung, die eine Spezialsoftware bieten würde. So sind in textbasierten Systemen bspw. keine automatischen Berechnungen oder logischen Ableitungen möglich, was häufig zu gewisser manueller Mehrarbeit führt. Da allerdings spezialisierte Produkte ebenfalls Zusatzaufwand (Etablierung, Anpassung, Schulung) erzeugen und sich nicht zwangsläufig an die Anforderungen der eigenen Organisation anpassen lassen, wäre eine Zeitersparnis in Summe tatsächlich erst ab einer hohen Anzahl an dokumentierten Informationen zu erwarten.

Spezialisierte MS-Tools ersetzen nicht den notwendigen Umbau der Prozesse der Organisation, sondern verstecken in vielen Fällen alte Abläufe hinter neuen Softwarelösungen.

Des Weiteren sind fast alle Eingabemöglichkeiten in einem DCMS zwangsläufig Freitextfelder, weshalb die Eingabe nicht beschränkt werden kann. Dies kann schnell dazu führen, dass Felder nicht oder falsch ausgefüllt werden, wodurch zusätzlicher Aufwand zur Bereinigung von Benutzereingaben für alle Beteiligten entstehen kann. Aufklärung, umfangreiche Anleitungstexte und Disziplin der Beschäftigten sind notwendig, um die Nutzbarkeit der Templates zu erhalten.

Bei der Anschaffung eines DCMS ist zu bedenken, dass sich diese in ihrem Funktionsumfang unterscheiden können: Von einer dateibasierten Dokumentenablage bis zu komplexen Wiki-Lösungen kann alles für den Aufbau eines MS genutzt werden. Längerfristig ist es ratsam, ein Produkt zu wählen, das über die reine Textablage mit Versionierung hinausgeht und zusätzliche Features wie Makros für Tabellenfilter, Aggregation zu Übersichtsseiten und eine Definition von (einfachen) Autorisierungsworkflows auf den Dokumenten bietet.

Ein großer Vorteil spezialisierter Produkte ist, dass sie bereits ein definiertes Vorgehen implementieren. Somit erspart sich eine Organisation zwar die Notwendigkeit, eigene (Teil-)Prozesse zu definieren – ein Schritt, der sehr viel Arbeit, Zeit und entsprechende Expertise kostet. Dennoch sollte gut abgewogen werden, ob der organisatorische und technische Aufwand, ein MS von Grund auf zu definieren und zu implementieren, es nicht wert ist: Die gewonnenen Erfahrungen durch die notwendige Analyse der Organisation, die erlangten Kenntnisse der Beschäftigten durch das Definieren eigener Prozesse und Templates sowie die Anpassung des MS an die eigene Organisation sind positive Effekte, die durch den Einsatz einer Standardsoftware (mit vordefinierten Standardprozessen) oftmals nicht erreicht werden. In der Praxis hat sich gezeigt, dass die Hauptproblematik bei der Etablierung eines MS nicht in der zur Verfügung stehenden Technik liegt. Ein MS ist in erster Linie eine organisatorische Herausforderung, welche in ihrer Umsetzung sowohl die Struktur als auch die Abläufe in der gesamten Organisation beeinflusst. Das MS muss an die Kultur der Organisation angepasst sein und das Personal muss eine ganzheitliche, prozessorientierte Denkweise annehmen. Durch den Einsatz von MS-Tools versuchen Organisationen oftmals, genau diese strukturellen Änderungen zu vermeiden. Den notwendigen Umbau der Prozesse der Organisation ersetzen solche Tools jedoch nicht, sondern verstecken in vielen Fällen alte Abläufe hinter neuen Softwarelösungen. Die durch ein MS erhofften langfristigen und strategischen Vorteile eines verbesserten Managements und integrierter Prozesse bleiben dann oftmals leider aus. Daher sollten sich Organisationen beim Aufbau eines MS auf die organisatorischen Aspekte, die Neugestaltung von Geschäftsprozessen und vor allem die Einbindung der Beschäftigten konzentrieren. ◆

Drei Jahre nach der Zertifizierung der Organisation gemäß ISO/IEC 27001 und 20000-1 setzt das Leibniz-Rechenzentrum noch immer auf ein Managementsystem ohne spezialisierte Tools und das ursprüngliche, textbasierte Konzept, welches hier mit Confluence implementiert wurde.

Sicherheit aktuell

Neues Angebot: DFN-Verein Community PKI

Foto: Parradee Kietsirikul / iStock

Als Ergänzung zum browserbasierten GÉANT Trusted Certificate Service (TCS) bietet der DFN-Verein seit Mitte April die neue „DFN-Verein Community PKI“ an, eine nicht im Browser verankerte PKI. Sie ist nicht für die allgemeine Anwendung gedacht, sondern für spezielle Use Cases entwickelt worden.

Die DFN-PKI Global und GÉANT TCS decken die häufigsten Use Cases für Zertifikate ab: Das sind im Browser bzw. Betriebssystem verankerte Zertifikate, die auf öffentlich erreichbaren Webservern eingesetzt werden sowie für die Signatur oder Verschlüsselung von E-Mails. Allerdings gibt es Anwendungsbereiche, in denen diese Zertifikate deutliche Nachteile haben:

- Exakte Vorgabe von Prozessen: Die Abläufe zur Ausstellung sind sehr strikt geregelt. Die Abläufe können sich mit kurzer Vorlaufzeit aufgrund wechselnder Anforderungen drastisch ändern.
- Probleme bei der Automatisierung: Betreibt man Systeme, die keine Automatisierung unterstützen, steigt der Aufwand des regelmäßigen Zertifikatstausches, da die Laufzeiten immer weiter verkürzt werden.
- Interne kritische Systeme: Im Browser bzw. Betriebssystem verankerte Zertifikate haben Ausfallrisiken, da diese bei kleinsten Compliance-Abweichungen innerhalb sehr kurzer Fristen gesperrt werden müssen.
- Client-Authentifizierung: Für die Anmeldung von Personen oder Systemen über Client-Authentifizierung liegt der Fokus auf dauerhafter Stabilität der genutzten Zertifikate und der darin enthaltenen Namen.

PKIs wie GÉANT TCS oder die DFN-PKI Global stützen sich ausschließlich auf die Vorgaben von Microsoft, Google und Mozilla – dadurch nehmen die Nachteile künftig noch zu. Eine interne, nicht verankerte PKI kann zur Lösung beitragen.

Die Vorteile der DFN-Verein Community PKI sind:

- Längere Laufzeiten für Systeme mit kompliziertem Zertifikatstausch (z. B. die DFN-AAI),
- weniger Prozessvorgaben, damit die Nutzung anderer Automatisierungstechniken möglich ist,
- Vermeidung von Ausfallrisiken für kritische Systeme. ◆

Informationsmaterial zur DFN-Verein Community PKI finden Sie unter:
https://www.pki.dfn.de
Bei Fragen kontaktieren Sie gerne die DFN-PCA unter: dfnpca@dfn-cert.de oder 040 808077-580.

Umstieg auf GÉANT TCS: Fristablauf beachten

Foto: korntt1992 / freepik

Die 2021 gestartete Migration der DFN-PKI Global zum Zertifikatdienst GÉANT Trusted Certificate Service (TCS) macht gute Fortschritte. Der Großteil der DFN-Teilnehmer, der die DFN-PKI Global verwendet, hat bereits einen Zugang zu TCS und nutzt diesen aktiv.

Für die Umstellung ist eine wichtige Frist zu beachten: Ab 30.12.2022 können in der DFN-PKI Global keine neuen Serverzertifikate mehr ausgestellt werden. Bis zu diesem Zeitpunkt müssen Einrichtungen ihre Prozesse angepasst haben, um browserverankerte Zertifikate für Server aus GÉANT TCS zu beziehen. Bereits ausgestellte Zertifikate behalten ihre Gültigkeit.

Für Nutzerzertifikate muss der Umstieg auf TCS bis zum 30.12.2023 durchgeführt werden. Wir empfehlen, sich rechtzeitig mit TCS zu beschäftigen, um bei der Umstellung der Prozesse nicht in Zeitnot zu geraten. ◆

Informationsmaterial finden Sie unter:
https://www.pki.dfn.de
Bei Fragen kontaktieren Sie gerne die DFN-PCA unter: dfnpca@dfn-cert.de oder 040 808077-580.

2. Teil des Trainingskurses „IT Forensics for System Administrators“

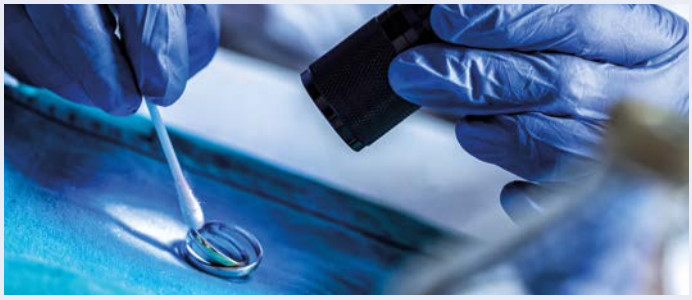


Foto: digicomphoto / iStock

Der im Rahmen des GÉANT-Projekts GN4-3 vom DFN-CERT entwickelte Trainingskurs „IT Forensics for System Administrators“, stieß in der DFN- und GÉANT-Community auf so große Resonanz, dass nun ein zweiter Teil stattfand. Alle Webinare wurden aufgezeichnet und stehen online zur Verfügung.

Der erste Teil beschäftigte sich mit den grundlegenden organisatorischen Schritten zur Bearbeitung forensischer Vorfälle und führte in die Methoden und Werkzeuge zur Sammlung der verschiedenen Formen von Beweisdaten ein. Der zweite Teil, der vom 27. April bis zum 30. Mai 2022 stattfand, knüpfte direkt daran an und legte den Fokus auf die Analyse der gesammelten Beweisdaten eines Vorfalls.

In insgesamt fünf Webinaren lernten die Teilnehmenden niedrigschwellige Werkzeuge kennen, die keine umfangreichen Systeminstallationen benötigen. Sie erhielten einen Einblick in Expertentools wie die Open-Source-Forensik-Plattform „Autopsy“ und das Forensic Framework „Volatility“. Zusätzlich wurden Analysemöglichkeiten mithilfe der Webanwendung CyberChef vorgestellt – auch als „Schweizer Cyber-Taschenmesser“ bezeichnet.

Die Trainingsreihe richtet sich primär an System- bzw. Netzwerkadministratorinnen und -administratoren. Sie ist aber auch für technisch Interessierte aus anderen IT-Bereichen hilfreich. Wer den Trainingskurs verpasst hat, braucht nicht traurig zu sein: Die Webinare wurden aufgezeichnet und stehen mit den Kursmaterialien zum Download bereit.

Die Aufzeichnungen aller bereits durchgeführten Webinare der Trainingsreihe finden Sie unter: https://www.dfn-cert.de/en/Trainings.html#ITForensics ◆

Mehr Sicherheit – mit TLSLookingGlass

Foto: jcomp/freepik

Der Traffic des eduroam-Login wird durch Analysen der (EAP-)TLS-Handshakes kontinuierlich überprüft. Ein Analysetool scannt den Anmeldeprozess im Hinblick auf verwendete TLS-Parameter, z. B. die TLS-Version, Verschlüsselungsalgorithmen und weitere verwendete Sicherungsmechanismen. Ziel dieses passiven Monitorings ist es, frühzeitig zu erkennen, ob eine Gefährdung der Sicherheit vorliegt. Das TLSLookingGlass wurde unter strikter Beachtung der Datensparsamkeit bei personenbezogenen Daten entwickelt. Da für die Darstellung der Sicherheitsparameter keine personenbezogenen Daten notwendig sind, werden diese auch nicht angezeigt.

Mit dem neuen Webtool TLSLooking-Glass haben DFN-Teilnehmer nun die Möglichkeit, auf die analysierten Verbindungsdaten zuzugreifen und diese nach einzelnen Parametern zu filtern. Damit können Fragestellungen noch besser eingegrenzt werden. Der Zugang zur Webapplikation erfolgt über die DFN-AAI. Mithilfe einer Übersichtsseite, die die wichtigsten TLS-Parameter enthält, können eduroam-Administrierende auf einen Blick erkennen, ob es bei der TLS-Implementierung und –Konfiguration Sicherheitsprobleme aufgrund von Fehlkonfigurationen oder veralteter Software gibt. Die Seite wird stetig an aktualisierte Sicherheitsanforderungen angepasst.

In den vergangenen drei Monaten wurden zwei Millionen Endgeräte auf ihre Sicherheit beim TLS-(EAP)-Handshake analysiert. Durch die Ergebnisse der Analysen konnten bereits zahlreiche Einrichtungen über Probleme in ihren RADIUS-Servern informiert werden. Mit dem TLSLookingGlass können sich Einrichtungen nun unkompliziert selbst einen Eindruck zum Stand ihrer Sicherheit beim eduroam-Login verschaffen. ◆

Weitere Informationen finden Sie hier: **https://tlslg.eduroam.de/**
Bei weiteren Fragen erreichen Sie uns unter: eduroam@dfn.de

NFDI-Arbeitsgruppe Identity & Access Management gestartet

Der DFN-Verein ist an der NFDI-Arbeitsgruppe Identity & Access Management beteiligt, die am 29. März 2022 – just während der DFN-Betriebstagung – offiziell ins Leben gerufen wurde. Die Gründung erfolgte im Rahmen eines Treffens der Sektion Common Infrastructures, der die Arbeitsgruppe beigeordnet ist.

Das Sektionskonzept adressiert mehrere Themenbereiche, die als zukünftige Basisdienste für die NFDI relevant sind. Schwerpunkt im Themenbereich AAI ist die Etablierung eines föderierten Identity & Access Managements (IAM) für den Zugriff auf Ressourcen in Multi-Cloud-Umgebungen. Dabei geht es darum, bestehende technische Komponenten in eine NFDI-übergreifende Authentifizierungs- und Autorisierungsinfrastruktur zu integrieren und ggf. um zusätzliche, verbindende Elemente zu ergänzen. Ein wichtiges Ziel ist es, nachhaltige Strukturen zu schaffen, die eine Fortführung des Betriebs nach Ende der Projektförderung ermöglichen. Dazu gehört, eine konsortienübergreifende Governance-Struktur für das Rechte- und Rollenmanagement für den Zugriff auf Forschungsdatenrepositorien, Analysetools und weitere Ressourcen aufzubauen.

Die Arbeitsgruppe wird eine aktive Rolle bei der Etablierung eines IAM-Basisdienstes in der NFDI spielen. Der DFN-Verein bringt hierbei nicht nur Erfahrungen und Kenntnisse aus dem Betrieb der DFN-AAI, sondern auch aus Projekten wie AARC, EOSC Future und GN4 mit ein. ◆

Neues von EasyRoam4Edu

Großes Interesse an EasyRoam4Edu: Immer mehr Einrichtungen – aktuell 82 – nehmen am neuen DFN-Pilotprojekt teil, das im August 2021 gestartet ist. Etwa 1000 Authentifizierungen pro Werktag verzeichnet der Pilotdienst derzeit. EasyRoam4Edu ist nicht nur ein sogenannter Managed eduroam Identity-Provider, der für die Einrichtungen den Aufwand minimiert, eduroam seinen Nutzenden anzubieten, sondern er leistet auch einen Beitrag dazu, die Sicherheit in eduroam zu erhöhen. Über Accounts aus der DFN-AAI ermöglicht EasyRoam4Edu den unkomplizierten, zertifikatsbasierten Zugang zum Dienst eduroam.

EasyRoam4Edu nutzt das Online Certificate Status Protocol (OCSP). Zertifikate, die für die Anmeldung in eduroam verwendet werden, lassen sich innerhalb von Sekunden widerrufen. Des Weiteren können EasyRoam4Edu-Admins die Laufzeit der Zertifikate konfigurieren: Das Minimum beträgt drei Monate, das Maximum 24 Monate.

In EasyRoam4Edu findet ausschließlich das zertifikatsbasierte Authentifizierungsprotokoll EAP-TLS Anwendung. Nutzende melden sich in EasyRoam4Edu nicht mehr mit ihrem Passwort an, sondern nutzen einen zertifikatsbasierten Pseudo-Account.

Mit der Umstellung auf eine hybride Certificate Authority (CA)-Umgebung, bestehend aus Public und Private CAs, gehört der PKI-Wechsel auf den RADIUS-Servern nun der Vergangenheit an. Damit konnten mögliche Abhängigkeiten im Bereich Sicherheitsprotokolle, Warnhinweise der Betriebssystemhersteller sowie häufiger RootCA-Wechsel minimiert und damit das Qualitätsmanagement in eduroam erhöht werden.

Mit dem Server-Update „Demeter“ wurde das Admin-Interface für die Verwaltung der eduroam-Profile erheblich überarbeitet und bietet nun attraktive Funktionen an, die den Administrierenden die Arbeit mit EasyRoam4Edu erleichtern. Zukünftige Features sind bereits in der Queue, z. B. die flexible Konfiguration der Laufzeit von Client-/User-Zertifikaten sowie rechtzeitige Benachrichtigungen, bevor diese ablaufen. ◆

Weitere Informationen finden Sie hier: https://doku.tid.dfn.de de:eduroam:easyroam

MITARBEIT AN DIESER AUSGABE SICHERHEIT AKTUELL:

Jürgen Brauckmann, Christine Kahl, Ralf Paffrath, Wolfgang Pempe, Jan-Frederik Rieckers

KONTAKT

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

Starke Partner weltweit

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

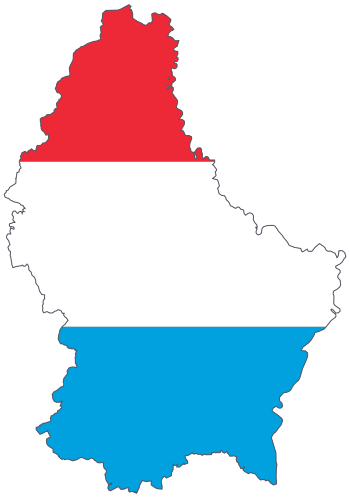


Foto: Belval / Restena

The Restena Foundation is the National Research and Education Network (NREN) for the Grand-Duchy of Luxembourg. This small country, neighbouring Germany, Belgium and France – or DFN, BELNET and RENATER - doesn't need a long introduction. Gathering one of the smallest research and education communities in Europe, Restena also has the chance to work for a country with a strong European orientation, where citizens and workers reflect a multicultural integration.

A single network for education and research

The Luxembourg NREN was created in 1989. It started as a project of the Ministry of Education in Luxembourg under the name of RESTENA for 'Réseau Téléinformatique de l'Éducation Nationale et de la Recherche' (standing for National Education and Research Teleinformatics Network) and aimed to meet the needs of education and scientific research institutions in the country. So the Luxembourg NREN starts its journey as a research project hosted within one of the freshly established public research centre and part of a bright new research and development ecosystem.

Restena – Luxembourgs small multi-faceted NREN

Started as a research project Restena became a network for all levels of education. Today a part of Restena's mission is the management of the country code top-level domain .lu, an essential infrastructure for Luxembourg's economy and society. Collaboration is an essential part of Restena's activities and culture. Restena not only takes part in joining forces within organisations like CENTR or GÉANT, but strongly believes that research and education can only thrive through sharing at all levels – starting at the infrastructure.

Text: **Christine Glaser** (Restena Foundation)

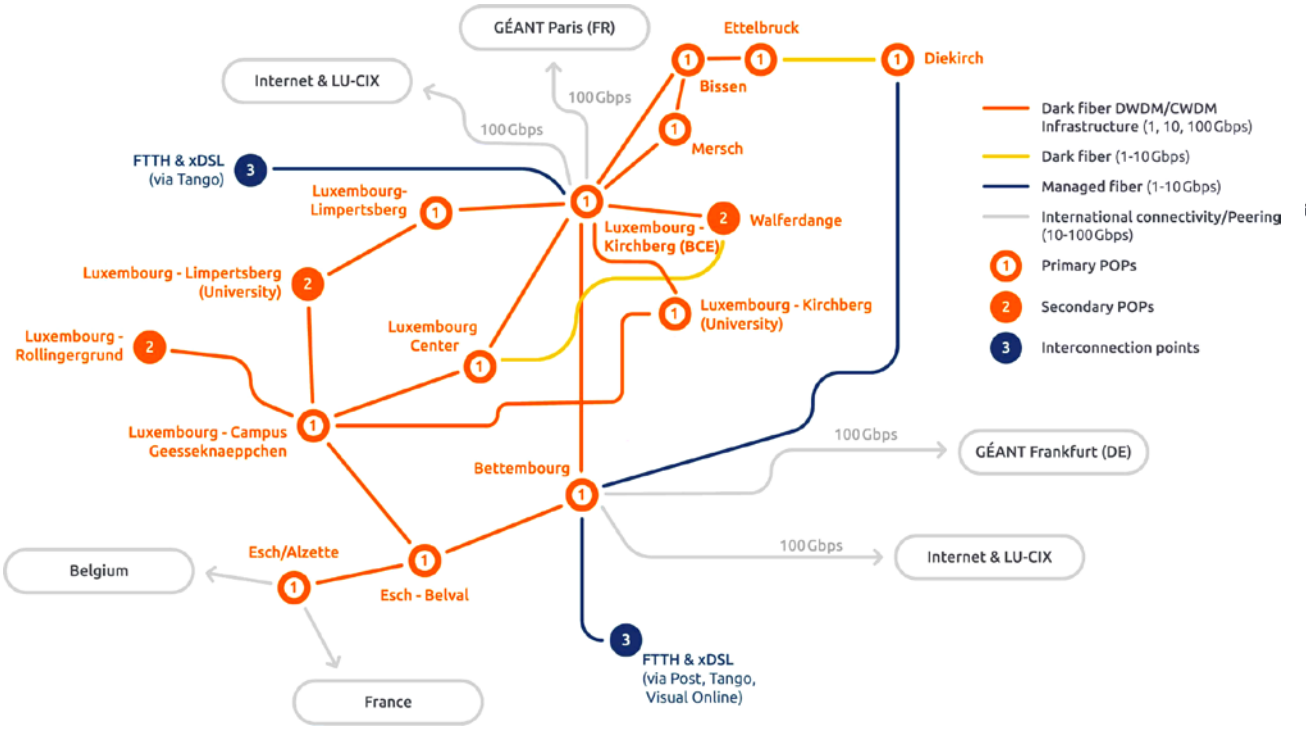
In 2000, in need of its own legal personality, the project became the Restena Foundation – a not-for-profit organisation founded by higher education and research institutions with a governing board appointed by the founding members and funding ministries. Over the years, the board of directors reshaped to take broader internet governance and strategic collaborations into account but remained strongly dedicated to Restena's core mission.

Since its inception, Restena took a slightly unusual approach for defining its community. Where most European NRENs focused on research and higher education, Luxembourg has built a network for all levels of education. While certainly favoured by the country's rather unimpressive size, the strategic choice of connecting as many schools as possible and providing access to email and Internet to all teachers laid the foundation for a large part of today's IT services for education: all secondary schools are connected by fibre with either 1 or 10 Gbps connections, and all teachers and students have access to a variety of services.

Small size but big responsibilities

In line with the Grand-Duchy of Luxembourg's geography and population, the Luxembourg NREN is rather small with its 21 employees and 542 connected organisations. However, the footprint within the local Internet extends well beyond the education and research community. A part of Restena's mission is the management of the country code top-level domain .lu, an essential infrastructure for Luxembourg's economy and society.

The expectations on the NREN and the .lu registry are hugely different – as are the communities that rely on both. However, hosting both services under the same roof and, more importantly, within the same technical body is advantageous: the .lu operations benefit from the broad knowledge and experience that is inherent to any NREN – and the NREN takes advantage of the stringent security and resilience requirements that come with the operation of an essential infrastructure. The latest showcase for the existing synergies is the ISO27001 certification Restena obtained for all its operations.



RESTENA national backbone in Luxembourg

Active in the Luxembourg landscape for 30 years

Restena never tried to restrict its focus on the education and research community but always kept the local environment in sight. When in 1992, 30 years ago, Restena connected Luxembourg to the nascent Internet and started to open .lu domain name registrations, the driving force was the political willingness to help the education and research community seek new resources and establish means to exchange ideas. However, when the telecom operators started to dip their toes in that new environment, the NREN shared its connectivity and helped to bring the internet to a larger public. Even more, as a commercially neutral partner Restena created and operated the first national internet exchange point, LIX, which was later merged into the current exchange called LU-CIX.

Although the internet has lost much of its initial pioneering charm over the decades, Restena remains strongly involved in the national ecosystem. Its staff remains responsible for most technical operations of LU-CIX, and has set up, together with the LU-CIX teams, the national anti-DDoS scrubbing centre on behalf of the Luxembourg government.

Collaboration – as much a mean as an end

NRENs are as much about connecting communities as about connecting machines. Under that premise, it is obvious that collaboration is an essential part of Restena's activities and culture. While the national activities, for example co-starting a LUNOG (Luxembourg network operator group) or taking an active part in CERT.LU (collaboration platform for local CERTs/CSIRTs), are straightforward, it is worth mentioning that Restena not only takes part in joining forces within organisations like CENTR or GÉANT, but strongly believes that research and education can only thrive through sharing at all levels – starting at the infrastructure.

What's next?

No article about a research network could be complete without some musings about the future – as hard as this may be. With research and economy being more and more data-driven, the case for excellent connectivity is easily made. Expected requirements for High-Performance Computing are laid out, and technology is rather well established. It is not so much

the network that looks challenging, but rather the environment it is evolving in. Security processes and technologies have since long crept into the friendly NREN environment and will take even a much larger place in our lives – on one hand draining resources from our raisons d'être, on the other establishing another way of helping our communities by shielding them from some worries.

A different set of changes is triggered by the global internet's ever-increasing role in society. The current focus of lawmakers and regulators is certainly warranted as much for protecting internet users as it would be for making sure that rule of law applies. The risk posed by regulations targeted at specific commercial actors in a fast-lived context needs to be monitored and addressed by the NREN community to avoid collateral damage to our activities.

And finally, Restena as well as all other NREN, must continue to make sure that the local research and education community and the policy-makers remain aware that we have to offer more than just a network, that the whole is bigger than the sum of its parts. ◆

ADDITIONAL INFORMATION:

- Restena Foundation website: **www.restena.lu**
- RESTENA: the story of an infrastructure', a publication produced to mark the Restena Foundation's 20th anniversary: **https://www.restena.lu/en/publications**
- Centre de gestion informatique de l'éducation (CGIE) website, gathering all IT services for education in Luxembourg: **www.cgie.lu**

Kurzmeldung

DFN-Verein organisiert WACREN CEO Academy Workshops

Im Auftrag des west- und zentralafrikanischen Forschungsnetzes WACREN hat der DFN-Verein eine Workshop-Reihe für die WACREN CEO Academy organisiert, die sich insbesondere an CEOs und CTOs der nationalen Forschungsnetze (National Research and Education Networks, NRENs) in West- und Zentralafrika richtet.

Den Auftakt bildete 2021 ein mehrteiliges Webinar zum Thema „Business Models for NRENs". In 2022 wird die Reihe mit Themen wie eduroam und eduGAIN fortgesetzt. Dazu fand am 14. März das Webinar „eduroam in Practice" mit 20 Teilnehmenden statt. Moderiert wurde es vom DFN-Verein und dem französischen Forschungsnetz RENATER. Paul Dekkers vom niederländischen Forschungsnetz SURF erläuterte die Funktionalität von eduroam sowie den Business Case und nannte die aktuellen Herausforderungen. Jan-Frederik Rieckers vom DFN-Verein widmete sich in seinem Vortrag den eduroam-Konfigurationen, beispielsweise welche Basis-Konfiguration notwendig ist, wie diese aufgesetzt wird, welche Kosten dabei entstehen und wie eine Minimal-Konfiguration betrieben werden kann.

Als Beispiel aus der Praxis erklärte Hrachya Astsatryan vom armenischen Forschungsnetz ASNET-AM wie eduroam in Armenien zum Einsatz kommt. Omo Oaiya, Chief Strategy Officer von WACREN, schloss die Veranstaltung mit einem Ausblick auf die bevorstehende eduroam-Roadshow in West- und Zentralafrika. Zwischen den Vorträgen sowie am Ende des Workshops blieb ausreichend Zeit, um mit den Referentinnen und Referenten individuelle Fragen zu klären. ◆

eduroam in Practice: DFN-Kollege Jan-Frederik Rieckers tauchte tief in die technischen Details des Roamingdienstes ein.

Quantensimulatoren in der Praxis

Wer sich schon jetzt näher mit Quantencomputing beschäftigen möchte, bekommt mithilfe von Simulatoren einen guten Einstieg in die Welt von Qubits, Quantennetzen und abhörsicheren Quantenprotokollen. Nicht nur für Forschende bieten softwarebasierte Simulatoren vielfältige Möglichkeiten, mit denen unterschiedliche Bereiche der Quantentechnologie nachgebildet werden können.

Text: **Sascha Schweiger, Martin Seidel** (Regionales Rechenzentrum Erlangen, Friedrich-Alexander-Universität Erlangen-Nürnberg)

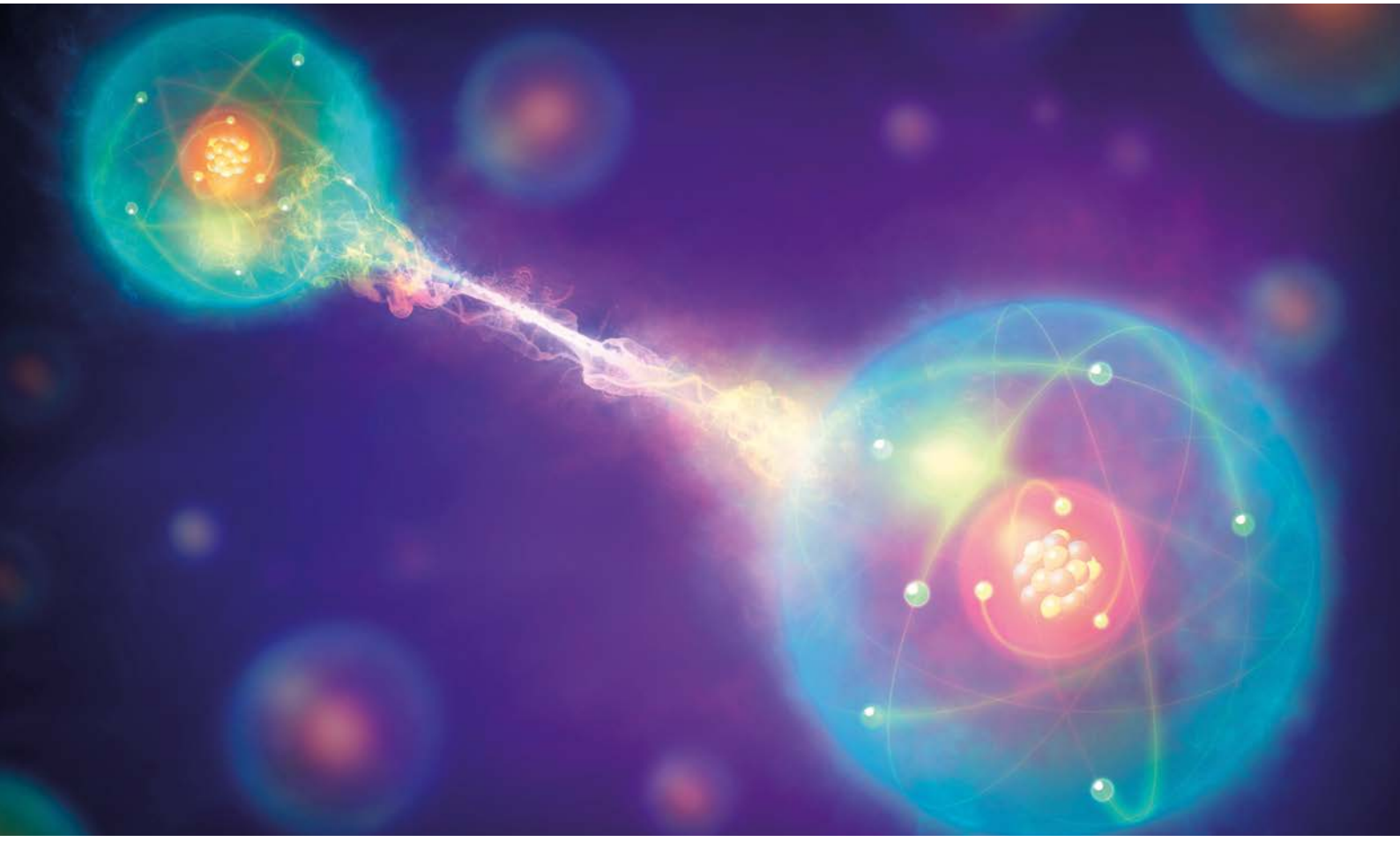
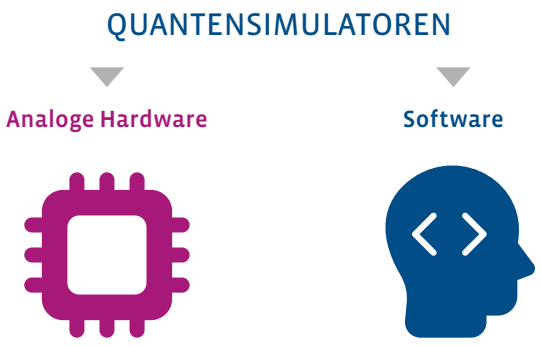


Foto: Science Photo Library / Alamy Stock Photo

Der Begriff und das Feld der Quantensimulation sind noch relativ jung, auch wenn erste Ideen scheinbar bis zur Erkenntnis von Richard Feynman zurückreichen, der erkannte, dass die Rechenleistung herkömmlicher Computer nicht ausreicht, um komplexe Quantensysteme zu berechnen, sondern dass ein „einfacheres“ Quantensystem als „Simulator“ benötigt wird, um ein deutlich komplexeres System nachzubilden. Ein wichtiger Schritt hin zu universellen Quantencomputern.

Quantensimulatoren werden oft analog angewendet mit Systemen, die versuchen, Quanteneffekte durch einfachere, leichter zu kontrollierende analoge Hardwaresysteme nachzubauen. Im Gegensatz zu diesen speziell zugeschnittenen Hardwaresystemen soll es hier um softwarebasierte Simulatoren gehen, mit denen verschiedene Bereiche der Quantentechnologie nachgebildet werden können. Eine solche Software kann beispielsweise zur Simulation der physikalischen Ebene mit Schaltungselementen und Dämpfungseinwirkungen eingesetzt werden. Es gibt aber auch Software, mit der es möglich ist, Routing, Protokolle und verteilte Schlüsselübertragung im Netz zu testen.



Softwarebasierte Quantensimulatoren bieten also bereits jetzt die Möglichkeit, Algorithmen und Softwarelösungen für zukünftige, universell programmierbare Quantencomputer zu entwickeln und zu testen. Mit ihnen lassen sich auch die Auswirkungen und der Einfluss dieser Technologie auf Kommunikationsnetze, Cybersicherheit und Rechenleistung untersuchen. Im

> Die Rechenleistung herkömmlicher Computer reicht nicht aus, um komplexe Quantensysteme zu berechnen.

Bereich von Quantennetzen werden sie beispielsweise eingesetzt, um Quantenrepeater zu simulieren. An Quantenrepeatern wird noch immer gearbeitet. Sobald diese dann jedoch als Hardware verfügbar sind, können die Erkenntnisse aus den Simulationen die Realisierung beschleunigen.

Die verschiedenen Quantensimulatoren

Obwohl es noch kein Regelwerk zur Kategorisierung gibt, lassen sich Quantensimulatoren in verschiedene Klassen unterteilen. Dazu gehören Quantenschaltungssimulatoren, Quantennetzwerksimulatoren und spezielle Anwendungssimulatoren (siehe Tabelle). Schaltungssimulatoren können grundlegende Hardwarekomponenten wie Quantenspeicher, Quantengatter und Quantenzustände wie Verschränkung und Quantenteleportation simulieren. Die Netzwerksimulatoren enthalten oft viele Funktionalitäten der Schaltungssimulatoren, sie sind jedoch dafür konzipiert, den Einfluss und das Verhalten von Quantentechnologien auf Netzwerke zu untersuchen und Protokolle auf Basis dieser Technologie zu entwickeln. Zu den speziellen

ÜBERSICHT ZUM ZUGANG UND ZU SPEZIELLEN ANWENDUNGSBEREICHEN DER SIMULATOREN

SIMULATOR	ZUGANG	SIMULATOR BESONDERS GEEIGNET FÜR
IBM Quantum/Qiskit	webbasierte Plattform mit Quantenhardware/Download	Schaltungen
Quantum Network Explorer	webbasierte Plattform	Netzwerke
QKDSimulator	webbasierte Plattform	spezielle Anwendungen / QKD
SQUANCH	Download / Selbstinstallation	Schaltungen, Netzwerke
QuNetSim	Download / Selbstinstallation	Netzwerke
SeQUeNCe	Download / Selbstinstallation	spezielle Anwendungen / Hardware

Quantensimulatoren zählen Simulatoren, die für bestimmte Anwendungsfälle, wie zum Beispiel QKD (Quantum Key Distribution) entwickelt wurden.

Simulationen auf Plattformen

Mittlerweile existieren einige äußerst umfangreiche und frei zugängliche Onlineplattformen zur Quantensimulation, die den Einstieg in das Thema Quantumcomputing vereinfachen sollen. Dazu gehören zum Beispiel die IBM Quantum Plattform, Google AI und Braket von Amazon.

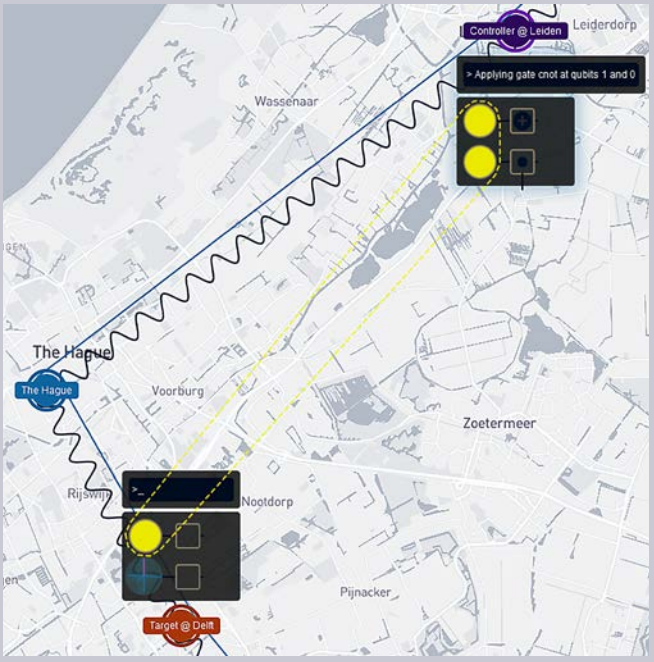


Abbildung 2: Oberfläche von Quantum Network Explorer von QuTech

Bereits seit 2019 bietet das Leibniz-Rechenzentrum (LRZ) einen 42 Qubit starken Simulator – den SuperMUC NG – für Quantencomputing von Intel an, wenn auch erstmal nur für Forschungszwecke. Das LRZ kooperiert ebenfalls mit Atos, um die „Atos Quantum Learning Machine" – den bislang kommerziell leistungsstärksten Simulator – und andere hilfreiche Services für Forschende über die Cloud zur Verfügung zu stellen.

Besonders geeignet für verteilte Anwendungen ist der Quantum Network Explorer, ein von QuTech entwickeltes Onlinetool zum Simulieren und Programmieren. Da bereits Beispiele zur Verfügung stehen, entfällt hier die Installation, und es müssen keine eigenen Circuits programmiert werden. Das Tool ist rein webbasiert und verfügt über eine übersichtliche Visualisierung (siehe Abbildung 2).

Ein Netzwerk, bestehend aus Network Nodes und Network Channels mit einstellbarer „Gate- and Elementary-Fidelity", kann dazu benutzt werden, Qubits mit komplexen Zuständen zu übertragen und damit verteilte Anwendungen zu simulieren. Zwischenschritte werden ausführlich aufgeführt und aufwendig visualisiert. Am Ende werden die Ergebnisse übersichtlich dargestellt. Abbildung 2 zeigt die Visualisierung eines Zwischenschrittes einer „State Teleportation" zwischen Sender und Empfänger, welche über eine Zwischenstation miteinander verbunden sind. In diesem Zwischenschritt sind die für eine Teleportation notwendigen verschränkten Qubits zu sehen.

Mithilfe des IBM Quantum Simulator/Qiskit ist es möglich, über einen Webbrowser seine ersten Quantenschaltungen zu planen, umzusetzen und emulieren zu lassen. Wer einen Zugang hat, kann dann seine Simulationen auf Wunsch bereits jetzt auf echter Hardware mit der IBM Quantum Plattform ausführen lassen.

Die Onlineplattform IBM Quantum/Qiskit kann nicht nur eigens kreierte Quantenschaltungen auf echter Quantenhardware ausführen, sondern ermöglicht es auch, ausschließlich im Webbrowser zu arbeiten, da bereits alle benötigten Tools

> Mithilfe des IBM Quantum Simulator Qiskit ist es möglich, über einen Webbrowser erste Quantenschaltungen zu planen.

on board sind. Mit dem Composer lassen sich Schaltungen erzeugen ohne selbst Codes schreiben zu müssen. Die Wahrscheinlichkeit der möglichen Ergebnisse wird hierfür übersichtlich in einem Histogramm dargestellt. Diese selbst kreierten Schaltungen lassen sich in ein Jupyter Notebook (Python) exportieren oder aber direkt in der integrierten WEB IDE weiterverwenden. Jupyter Notebooks, ehemals IPython Notebooks, sind als interaktive Webdokumente bzw. als Umgebung im eigenen Open-source-Dateiformat „.ipynb" zu verstehen. Die Ein- und Ausgabe erfolgen in jeweils eigenen Zellen und erleichtern so die Verwaltung von Text, Plots und Code in zahlreichen Sprachen. Das hilft zum Beispiel bei der Auswertung von Daten. In Abbildung 3 ist links oben der Composer abgebildet, mit dem sich verschiedene Schaltungen aus klassischen

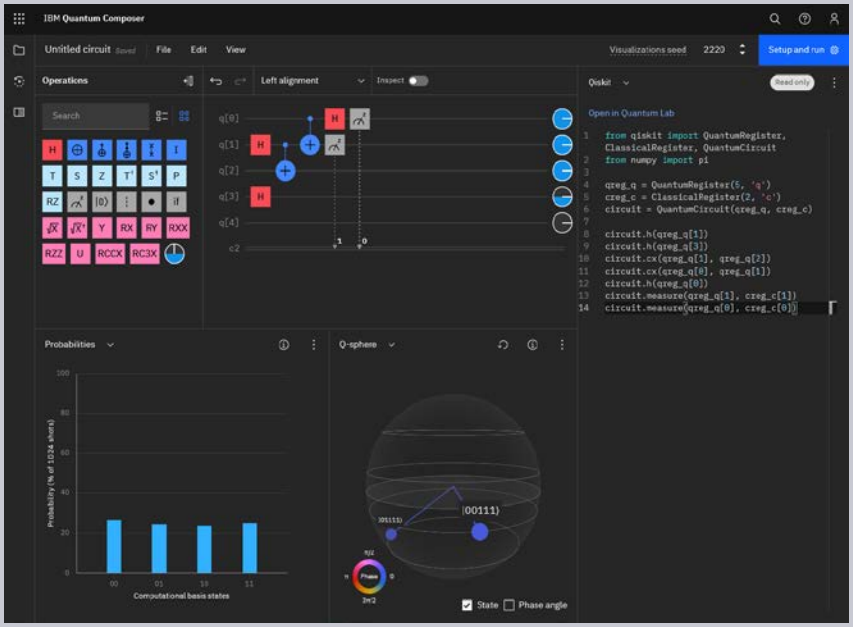


Abbildung 3: Weboberfläche der Simulationsplattform IBM Quantum/Qiskit

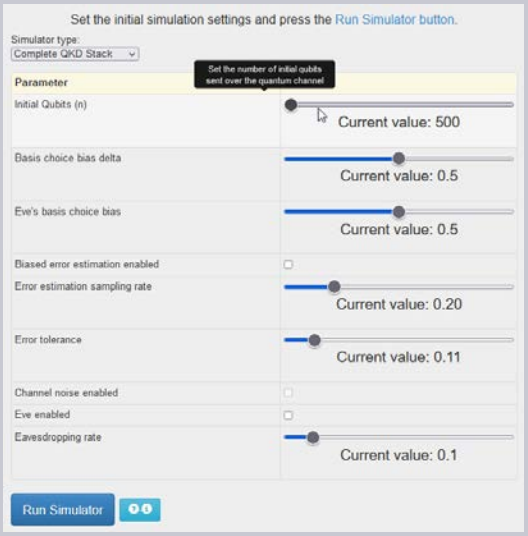


Abbildung 4: Benutzeroberfläche zur Konfiguration der Parameter im QKDSimulator

und Quantengattern zusammenstellen lassen. Zeitgleich zu den Schaltungselementen (links) wird dann der passende Code dazu generiert (rechts). Ein Histogramm wird in nahezu Echtzeit erzeugt (unten links) und zeigt die Verteilung aller möglichen Ergebnisse der Simulation. Die Q-Sphere (nicht zu verwechseln mit der Bloch-Kugel) ist eine alternative Darstellungsmöglichkeit des Histograms.

Um einen Quantenschlüsselaustausch (BB84-Protokoll) zu testen und zu visualisieren, können mit dem Onlinesvimulator QKDSimulator auf einer grafischen Benutzeroberfläche Parameter des Quantenkanals zum Fehlerabgleich und zur Fehlerkorrektur sowie zu Fehlertoleranzraten durch Schieberegler konfiguriert werden (Abbildung 4).

Simulatoren zum Selbstinstallieren

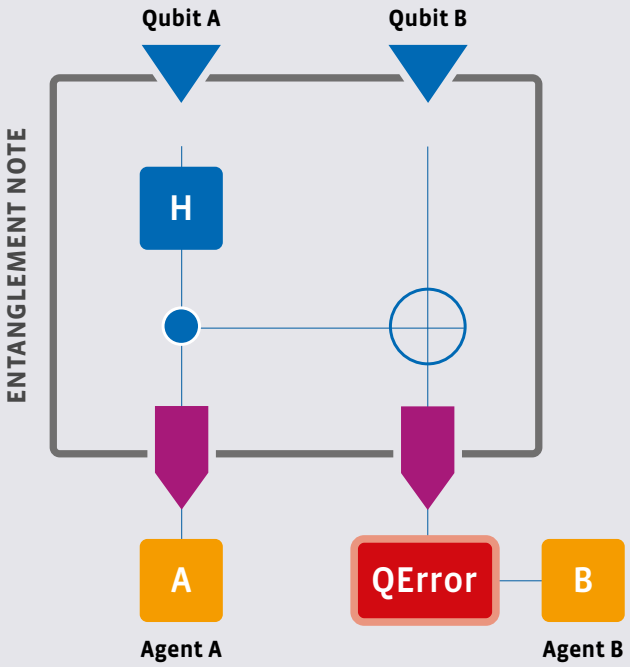
Wer nicht mit webbasierten Plattformen arbeiten möchte, sondern lieber seine eigene Simulationssoftware installieren will, kann auf verschiedene Softwarepakete zugreifen. Diese Pakete sind meist öffentlich zugänglich und je nach Simulator für unterschiedliche Anwendungsgebiete geeignet. Simulatoren wie Netsquid und SeQUeNCe haben den Vorteil, dass sie sehr viele Details liefern, was die Implementierung der physikalischen Schicht sowie der Verbindungsschicht und den Einfluss von Quantenfehlern betrifft. Für den Bereich Quantennetze gibt es Simulatoren, die sich vor allem zum Testen von Protokollen und dem Erstellen von Netztopologien eignen. Dazu zählen zum Beispiel QuNetSim, SQUANCH, SimulaQron und QuISP. Mit QuISP lassen sich sogar Netzwerke mit hundert Knoten simulieren, welche auch Quantenrepeater enthalten können. SQUANCH und QuNetSim eignen sich vor allem zur Erstellung und zum Testen von Netzwerkprotokollen. Wer auf der Anwendungsschicht mit QKD-Protokollen arbeiten möchte, kann zum Beispiel QKDNetSim verwenden.

> Für den Bereich Quantennetze gibt es Simulatoren, die sich zum Testen von z. B. Protokollen eignen.

Simulationsbeispiele für die Bereiche Netzschicht und physikalische Schicht

Den Simulator SQUANCH gibt es als Open-Source-Python-Paket. Die Software ermöglicht das Erstellen von Netzwerktopologien und das Testen von Protokollen, besitzt aber auch Werkzeuge, um Quantentechnologie auf Schaltungsebene zu simulieren. In Abbildung 5 wird die Umsetzung einer Qubit-Verschränkung (Entanglement) gezeigt.

In SQUANCH werden kommunizierende Partner als Agents bezeichnet. In diesen Agents muss je nach Anwendungsfall eine passende Quantenschaltung bzw. Logik in Form von Python-Code implementiert werden, damit diese eine Kommunikation mit anderen Agents im Sinne der Anwendung führen können. Die Agents selbst werden über Quantenkanäle mit eigenen Quantenfehlermodellen, wie sie bei der Übertragung auftreten können, verbunden. In der Abbildung werden zwei unabhängige Qubits A und B über einer Schaltung zur Verschränkung der beiden Qubits dargestellt. Dabei soll auf ein Qubit A zunächst das Hardamard-Gatter (H) angewendet werden, welches das Qubit in eine Superposition versetzen soll. Anschließend wird über ein CNOT-Gatter, das




```
QError
class ShorQChannel(QChannel):
    '''Represents a quantum channel
    with a Shor error applied'''
    def __init__(self, from_agent, to_agent):
        QChannel.__init__(self, from_agent, to_agent)
        # register the error model
        self.errors = [ShorError(self)]
```

Abbildung 5: Entanglement-Schaltung und -Code für Quantenfehler in SQUANCH

die Verschränkung herstellen soll, Qubit A mit Qubit B verbunden. Danach werden die verschränkten Qubits an die beiden Agents (A = Alice und B = Bob) verteilt. Im Quantenkanal von B ist zusätzlich ein Quantenfehlermodell integriert. Der Codeausschnitt zum Fehlermodell ist in der Abbildung als QError aufgeführt.

Der Simulator **QuNetSim** ist ein in Python geschriebenes Paket, das frei erhältlich ist und sich zum schnellen und einfachen Testen von Protokollen eignet. Die Software simuliert die Netzwerkschicht in einem Quantennetz, ohne dass sich die Nutzenden um das Routing zwischen zwei Hosts, die (in-)direkt durch die Netzwerktopologie verbunden sind, kümmern muss. Zudem verfügt der Simulator über Mechanismen zur Kontrolle der Synchronisation im Netz. In QuNetSim können auch ein klassisches und ein Quantennetz parallel in einer Simulation betrieben werden. Im Gegensatz zu SQUANCH müssen in den einzelnen Nodes keine internen Schaltungen definiert werden, sondern es genügt beispielsweise der Befehl „run_protocol(generate_entanglement)“. Abbildung 7 zeigt die Demonstration einer Qubit-Übertragung, wobei ein Netzwerk aus drei Hosts (A, B, C) in QuNetSim definiert wurde und drei Qubits von Host A nach C über Host B gesendet werden.

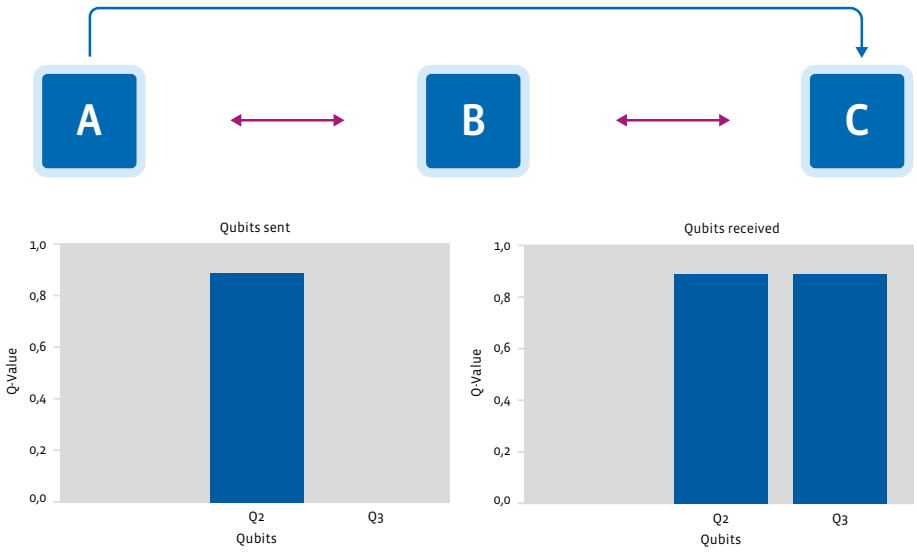
Wie dem Codeausschnitt #Netzwerktopologie in Abbildung 7 zu entnehmen ist, werden die drei Hosts definiert und entsprechend der dargestellten Topologie miteinander verbunden. Der Sender (host_A) und Empfänger (host_B) werden mit einem Protokoll zum Senden beziehungsweise Empfangen eines Qubits initialisiert (#Protokoll zuweisen). Im Protokoll des Senders (#Protokoll Sender) sollen drei Qubits an den Empfänger im überlagerten Zustand (Hadamard-Gatter) übermittelt werden. Wie den Diagrammen auf der rechten Seite der Abbildung 7 zu entnehmen ist, weicht der Zustand der gesendeten von den empfangenen Qubits voneinander ab: Der Grund dafür ist, dass ein Qubit nach der Messung mit einer Wahrscheinlichkeit von 50 Prozent (Bell-Zustand) einen der beiden Werte 0 oder 1 annimmt.

```
node_1.run_protocol(generate_entanglement)
network.quantum_routing_algo = routing_algorithm
choices = ['00', '11', '10', '01']
A.send_superdense(B.host_id, random.choice(choices), await_ack=True)
```

Abbildung 6: Herstellung von Entanglement in QuNetSim

Der Simulator **SeQUeNCe** ist ein frei erhältlicher Open-Source-Simulator, mit dem sich Einflussfaktoren wie beispielsweise Zeit und Dämpfung auf die Erzeugung und Übertragung von Quantenzuständen in Netzwerken simulieren lassen. Dadurch können Abläufe in der Hardware- und Verbindungsschicht getestet werden. Im folgenden Beispiel wird das Barrett-Kok-Protokoll[1] dargestellt. Dies ist ein Verfahren zur Erzeugung von verschränkten Qubits, welches eine hohe Toleranz gegenüber Fehlern wie Detektorausfall und spontane Emission eines Photons auf der Hardwareebene aufweist. Das Protokoll benötigt zur Erzeugung der Verschränkung Zugriff auf zwei Quantenspeicher (Quantum Nodes) und einen BSM (Bell

1 Barrett S D and Kok P 2005 Efficient high-fidelity quantum computation using matter qubits and linear optics Phys. Rev. A 71 060310, https://journals.aps.org/pra/abstract/10.1103/PhysRevA.71.060310




```
#Netzwerktopologie
host_A = Host('A')
host_A.add_connection('B')
host_B=Host('B')
host_B.add_connections(['A','C'])
host_C=Host('C')
host_C.add_connection('B')


#Protokolle zuweisen
host_A.run_protocol(sender)
host_C.run_protocol(receiver)


#Protokoll Sender
def sender(host,receiver,qubits):
    for i in range(qubits):
        qubit=Qubit(host)
        qubit.H()
        host.send_qubit(qubit)
```

Abbildung 7: Qubit-Übertragung mit QuNetSim

State Measurement) Node und regelt dann unter anderem die Synchronisation des Ablaufs der Verschränkung.

Anders als die beiden bereits vorgestellten Simulatoren ist SeQUeNCe sehr hardwarenah orientiert, das heißt, es müssen bei der Erstellung von Simulationen quantenphysikalische Phänomene berücksichtigt werden. Der Codeausschnitt links in Abbildung 8 zeigt die Funktionen, die zur Akquirierung und Synchronisation der beiden Quantenspeicher zur Generierung von Entanglement von Nutzenden implementiert werden müssen. Auch die Funktion zur Erfassung der Simulationsdaten, abhängig von den benutzerdefinierten Parametern (Codeausschnitt rechts in Abbildung 8), muss selbst erstellt werden. SeQUeNCe ist daher komplex und erfordert einen höheren Aufwand bei der Einarbeitung. Jedoch lassen sich mit diesem Simulator Quantennetze realistischer abbilden und das Verhalten, beziehungsweise die Abhängigkeit von verschiedenen Einflussfaktoren wie beispielsweise der Dämpfung, besser untersuchen und grafisch darstellen.

```
# Look for free Quantum memory
eg_rule_condition(memory_info, manager,
# Actions on node 1 when condition meet
eg_rule_action1(memories_info, args):
# Actions on node 2 when condition meet
eg_rule_action2(memories_info, args):
```

```
test(sim_time, cc_delay, qc_atten, qc_dist):
"""
sim_time: Simulationsdauer (ms)
cc_delay: Verzoegerung klassischer Kanal (ns)
qc_atten: Dämpfung Quantenkanal (db/m)
qc_dist: Laenge Quantenkanaele (km)
"""
```

Abbildung 8: Erzeugung von Entanglement in SeQUeNCe mit Codeausschnitten

Zu den Simulatoren:
QKDSimulator: https://www.qkdsimulator.com/
SQUANCH: https://att-innovate.github.io/squanch/overview.html
QuNetSim: https://tqsd.github.io/QuNetSim/
SeQUeNCe: https://sequence-toolbox.github.io/index.html

Zu den Plattformen:
IBM Quantum: https://quantum-computing.ibm.com/
Google AI: https://quantumai.google/quantum-computing-service
Amazon Braket: https://aws.amazon.com/de/braket/
Quantum Network Explorer: https://www.quantum-network.com

Ausblick

Quantensimulatoren eignen sich je nach Kategorie für unterschiedliche Anwendungen und Einsatzgebiete. Verschiedene Angebote von Quantenplattformen ermöglichen es Forschenden, Simulationen auch auf webbasierten Plattformen und realer Quantenhardware zu testen (IBM) oder das Verhalten und die Zustände von Qubits auf dafür ausgelegten Supercomputern (LRZ) zu erproben. Da an Quantenrepeatern noch gearbeitet wird, können Simulatoren helfen, Anwendungen und Protokolle für Netze ohne die dafür benötigte Hardware zu erstellen und zu untersuchen. Mit den daraus gewonnenen Erkenntnissen lassen sich Algorithmen und Programme für Quantennetze schon jetzt umsetzen und bei zukünftiger Verfügbarkeit der Komponenten schneller und einfacher realisieren. ◆

Mehr Informationen zum Thema Quantenforschung und Quanteninternet finden Sie auf **https://www.win-labor.dfn.de/.**

Doppelt lehrt besser

Zur datenschutzrechtlichen Relevanz von Hybridveranstaltungen

Mit der Rückkehr des Lehrbetriebes in die Präsenz treten neue Konzepte auf den Plan. An vielen Universitäten werden Vorlesungen und Veranstaltungen als Hybride zwischen digitaler Lehre und Präsenzlehre angeboten. Der wegen Hygienemaßnahmen nur in Teilen besetzte Hörsaal oder Seminarraum wird hierzu gefilmt und online live gestreamt. Teilweise werden die Vorlesungen für den späteren Konsum aufgezeichnet. Dieses Vorgehen ermöglicht eine teilweise Rückkehr zu den Lehrbedingungen vor der Pandemie und gleichzeitig eine Berücksichtigung der nach wie vor bestehenden Ansteckungsgefahr. Während die datenschutzrechtlichen Probleme digitaler Veranstaltungen bereits öfter Thema des Infobriefs Recht[1] waren, sind die Fallstricke der Hybridveranstaltungen noch nicht beleuchtet worden.

Text: **Owen Mc Grath** (Forschungsstelle Recht im DFN)

Foto: TarikVision / iStock

1 Siehe. z. B.: John, Corona is calling, DFN-Infobrief Recht Sonderausgabe Covid-19/2020

I. Datenschutzrechtliche Problemstellung

Hybride sowie rein digitale Veranstaltungen weisen einen großen Überschneidungsbereich in Bezug auf ihre rechtlichen Probleme auf. In beiden Modi stellt sich die Frage, inwiefern personenbezogene Daten von digitalen Teilnehmenden verarbeitet werden und ob dies gerechtfertigt ist. Auch wenn der Schluss naheliegt, dass sich so eine deckungsgleiche Bewertung der beiden Veranstaltungstypen ergibt, ist dies nicht vollständig der Fall. Die Situation der Teilnehmenden, die digital über ein Endgerät der Veranstaltung zugeschaltet sind, ist in weiten Teilen mit der Situation der rein digitalen Lehre vergleichbar. Für die Zwecke dieser Erarbeitungen wird sich daher auf die Verarbeitungen personenbezogener Daten der in Präsenz Teilnehmenden und insofern von der digitalen Situation abweichenden Konstellation beschränkt.

Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“ (Art. 4 Nr. 1 Datenschutz-Grundverordnung [DSGVO]). Umfasst von diesen Daten sind also auch Bild- oder Tonaufnahmen einer Person. Werden diese verarbeitet, ist der Schutzbereich der DSGVO eröffnet. Der Eingriff in diesen Schutzbereich muss gerechtfertigt sein. Im europäischen Datenschutzrecht gibt es zur Rechtfertigung von Verarbeitungen personenbezogener Daten verschiedene Erlaubnistatbestände. Die Verarbeitung kann zum Beispiel durch ihre Notwendigkeit zur Erfüllung einer vertraglichen Pflicht erforderlich sein. Damit wäre eine Verarbeitung nach Art. 6 Abs. 1 S. 1 lit. b DSGVO rechtmäßig.

Um eine datenschutzrechtliche Einschätzung zu Hybridveranstaltungen geben zu können, ist festzustellen, inwiefern personenbezogene Daten in diesem Kontext verarbeitet werden können. Von großer Relevanz ist insofern die Aufnahme der Teilnehmenden via Videokamera und Mikrofon während der Veranstaltung sowie die Wiedergabe von Bild und Ton in einem Livestream bzw. die Speicherung der Aufnahmen und Zurverfügungstellung an Dritte. Werden hierbei nicht nur der Vortragende, sondern auch Teilnehmende gezeigt, können auch deren personenbezogene Daten betroffen sein.

II. Fallgruppen

Vorliegend ist zur Veranschaulichung zwischen mehreren Fallgruppen zu unterscheiden:

1. Es wird nur der Vortragende gestreamt und ggf. aufgezeichnet. Die sonstigen Teilnehmenden der Veranstaltung sind auf dem Bild nicht wahrzunehmen. Auch die Stimmen der Teilnehmenden sind nicht zu hören. Insofern sind die einzig relevanten personenbezogenen Daten die des Vortragenden.

2. Der Vortragende ist zu sehen und zu hören. Die Teilnehmenden der Veranstaltung sind vereinzelt im Bild zu sehen. Dies kann durch Schnittbilder geschehen, die das Publikum aus verschiedenen Blickwinkeln zeigen oder durch Aufnahmen des Vortragenden, in denen auch Teilnehmende (bspw. deren Rücken) zu sehen sind. Nunmehr werden auch personenbezogene Daten der Teilnehmenden verarbeitet. Diese Verarbeitung wiegt umso stärker, wenn die Veranstaltung nicht bloß live gestreamt wird, sondern auch nachträglich in aufgezeichneter Form zugänglich ist. Gleiches gilt dann, wenn der Stream oder die Aufzeichnung nicht nur einem beschränkten Personenkreis, sondern der Öffentlichkeit zugänglich ist.

3. Der Vortragende ist zu sehen und zu hören. Die Teilnehmenden sind explizit im Bild zu sehen und auch ihre Stimmen sind zu hören. Dieser Fall liegt zum Beispiel dann vor, wenn die Veranstaltung interaktiv ausgerichtet ist und Mikrofon und Kamera eingesetzt werden, um Fragen oder Beiträge der Teilnehmenden aufzunehmen. Hierbei werden diverse personenbezogene Daten aller beschriebenen Personen verarbeitet.

Um die Verarbeitung personenbezogener Daten zu rechtfertigen, müsste ein entsprechender Tatbestand des Art. 6 Abs. 1 S. 1 DSGVO erfüllt sein. Infrage kommen für die vorliegenden Sachverhalte sowohl eine Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO als auch eine Aufgabenausführung im öffentlichen Interesse nach Art. 6 Abs. 1 S. 1 lit. e DSGVO.

Die Einwilligung des Vortragenden zur Aufnahme seiner Person in Bild und Ton einmal vorausgesetzt, stellt sich nur für die Fallgruppen 2 und 3 die Frage, ob eine Rechtfertigung vorliegt.

III. Zur Einwilligung

Eine Einwilligung kann nur dann wirksam erteilt werden, wenn die Anforderungen der Art. 4 Nr. 11 DSGVO und Art. 7 DSGVO erfüllt sind. Dafür muss die Einwilligung unmissverständlich, in informierter Weise und vor allem freiwillig abgegeben worden sein. Freiwillig kann eine Einwilligung nur sein, wenn den Betroffenen durch die Verweigerung der Einwilligung kein wesentlicher Nachteil entsteht. Ein solcher läge zum Beispiel vor, wenn durch Verweigerung der Einwilligung die Teilnahme an einer Veranstaltung versagt wird.

Im Rahmen hybrider Veranstaltungen ließe sich argumentieren, dass es den Besucherinnen und Besuchern der Fallgruppe 2 und 3 durch die Verweigerung der Einwilligung zu der entsprechenden Verarbeitung personenbezogener Daten nicht möglich ist, an der Veranstaltung teilzunehmen. Damit würde sie ein wesentlicher Nachteil treffen. Dabei wird allerdings verkannt, dass gerade der Vorteil von Hybridveranstaltungen in der Möglichkeit der Teilnahme auf digitalem Wege liegt. Zwar kommt es, je nach Ausgestaltung der digitalen Zugänglichkeit, auch hierbei zur Verarbeitung personenbezogener Daten (IP-Adressen, Namen der Teilnehmenden). Diese ist aber zum einen nicht zwingend und zum anderen regelmäßig weniger eingriffsintensiv, wenn man sie mit dem Abfilmen der Gesichter und der Aufnahme der Stimme vergleicht. Nicht zwingend ist die Verarbeitung in diesem Kontext, wenn die Teilnahme an dem Stream der Veranstaltung oder das Ansehen der Aufzeichnung technisch so ausgestaltet ist, dass keine personenbezogenen Daten verarbeitet werden. Ein wesentlicher Nachteil besteht mit Ablehnung der Verarbeitung bei hybriden Veranstaltungen, wie sie Fallgruppe 2 und 3 widerspiegeln, damit nicht zwangsläufig.

Ein wesentlicher Nachteil könnte jedoch noch dadurch entstehen, dass den Betroffenen durch die Verweisung auf die digitale Variante der Hybridveranstaltung eine aktive Teilnahme mit Fragen und Wortbeiträgen nicht möglich ist. Ob das der Fall ist, hängt von vielen Unbekannten im Einzelfall ab und lässt sich damit nur schwerlich pauschal einordnen. So hängt es schon von der Veranstaltung als solcher ab, ob eine aktive Teilnahme erforderlich ist bzw. die Unmöglichkeit dieser tatsächlich einen wesentlichen Nachteil bedeutet. Vortragsveranstaltungen zum Beispiel leben nicht zwangsläufig von einem Austausch zwischen Publikum und Referierenden. Für Seminare hingegen ist ein Austausch essenziell. Des Weiteren kann der digitale Teil der Veranstaltung auch so ausgestaltet sein, dass eine aktive Teilnahme möglich ist. Das ist zum Beispiel dann der Fall, wenn Fragen über ein Chatfenster oder ähnliches gestellt werden können. Auch hierbei kann es dann zu Verarbeitungen personenbezogener Daten kommen. Diese werden aber, wie dargelegt, je nach technischer Ausgestaltung einen geringeren Einschnitt für die Betroffenen bedeuten.

Nach diesen Ausführungen wäre eine mangelnde Freiwilligkeit der Einwilligung nur in bestimmten Fällen anzunehmen. Ein solcher läge zum Beispiel vor, wenn eine Präsenzveranstaltung der Fallgruppe 3 stattfindet, welche eine aktive Teilnahme unbedingt erfordert, und der digitale Zugang zu dieser Veranstaltung keine Interaktion ermöglicht. Lehnt der Betroffene Aufnahmen seiner Person ab, ist ihm eine Teilnahme in Präsenz nicht möglich. Die digitale Variante bietet keine vergleichbare Alternative. Mit Versagung der Einwilligung liegt ein wesentlicher Nachteil vor. Die Einwilligung kann mithin nicht freiwillig abgegeben werden.

Abseits solcher oder vergleichbarer Situationen ist jedoch von der Möglichkeit einer freiwilligen Einwilligung auszugehen. Hierbei sind die Voraussetzungen einer wirksamen Einwilligung im Sinne der DSGVO zu beachten (Art. 7 DSGVO). Insbesondere ist bei einer Aufzeichnung und Zurverfügungstellung der Veranstaltung im Internet auch darauf zu achten, hierfür eine Einwilligung einzuholen.

IV. Zur Aufgabenausführung im öffentlichen Interesse

Die Verarbeitung von personenbezogenen Daten ist auch zulässig, wenn „die Verarbeitung […] für die Wahrnehmung einer Aufgabe erforderlich [ist], die im öffentlichen Interesse liegt“ (Art. 6 Abs. 1 S. 1 lit. e DSGVO). Die Durchführung der Lehre an Hochschulen und wissenschaftlichen Einrichtungen ist dem öffentlichen Interesse zuzuordnen. Problematisch ist allerdings, dass es nach Art. 6 Abs. 3 DSGVO für Art. 6 Abs. 1 S. 1 lit. e DSGVO einer geschriebenen Rechtsgrundlage bedarf. Bei Art. 6 Abs. 3 DSGVO handelt es sich um eine sogenannte Öffnungsklausel. Mit solchen soll dem Gesetzgeber ermöglicht werden, bestimmte Sachverhalte durch konkretisierte Normen selbst näher zu regeln. Soweit ersichtlich liegt für Hybridveranstaltungen allerdings noch keine die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. e DSGVO spezifizierende Norm vor. Soweit ist eine Verarbeitung personenbezogener Daten auch nicht auf diesen Erlaubnistatbestand zu stützen. Werden solche Regelungen beispielsweise im Rahmen des Satzungsrechtes der Hochschule getroffen, ist darauf zu achten, dass sie im Lichte der zu verarbeitenden Daten verhältnismäßig sind. Insofern wäre schon infrage zu stellen, ob das Aufnehmen von Bild und Ton der Teilnehmenden für die Veranstaltung überhaupt erforderlich ist.

Bis eine entsprechende Regelung getroffen wurde, steht Art. 6 Abs. 1 S. 1 lit. e DSGVO allerdings nicht als tauglicher Erlaubnistatbestand zur Verfügung.

V. Fazit

Die Durchführung von Hybridveranstaltungen wird mit Fortschreiten der Pandemie ein relevanter Modus Operandi. Je nach technischer Ausgestaltung werden neben den personenbezogenen Daten der Vortragenden auch die der Teilnehmenden verarbeitet. Eine Rechtfertigung dieser Verarbeitung ist im Einzelfall und je nach digitalem Parallelangebot über eine Einwilligung der Betroffenen möglich.

Eine pauschale Einschätzung verbietet sich jedoch. Diese birgt immer das Risiko eines Verstoßes gegen das europäische Datenschutzrecht. ◆

Ein Tool, die Banner zu knechten

Mit dem Inkrafttreten des Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) ändern sich die Vorschriften für die Einholung von Einwilligungen für Cookies auf Webseiten

Nachdem das TTDSG als neues nationales Datenschutzgesetz seit Dezember die Voraussetzungen für die Einwilligung von Nutzenden der sogenannten „Cookies“ auf Webseiten regelt, stellt sich die Frage, ob und was sich nun geändert hat. Auf den ersten Blick scheint das TTDSG neue Möglichkeiten zu bieten, welche das Chaos der Cookie-Banner auf den Webseiten unterbinden könnten. Doch der zweite Blick zeigt: Es ist noch ein langer Weg dorthin.

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

Foto: Thomas Reimer/Adobe Stock

I. Das neue TTDSG

Am 1. Dezember 2021 ist das neue TTDSG in Kraft getreten. Ziel des Gesetzgebungsverfahrens war es, mehr Rechtssicherheit und Rechtsklarheit im Datenschutzrecht zu schaffen und die Datenschutzvorschriften des alten Telekommunikationsgesetzes (TKG) und Telemediengesetzes (TMG) übersichtlich zusammenzuführen.[1] Außerdem stellt das TTDSG die Umsetzung der ePrivacy-Richtlinie[2] sowie der Cookie-Richtlinie[3] dar. Bisher war die Umsetzung der Richtlinien im TMG nach Ansicht des Europäischen Gerichtshofs (EuGH) nicht ausreichend erfolgt,[4] weshalb der Bundesgerichtshof (BGH) letztendlich in einer Entscheidung[5] eine richtlinienkonforme Auslegung des TMG vornahm.

II. Was sind Cookies?

Als Cookies werden kleine Textdateien bezeichnet, die lokal auf dem Computer des Nutzenden beim Besuch einer Webseite gespeichert werden. Diese Dateien speichern bestimmte Einstellungen oder Informationen zu dem Nutzenden. Die gespeicherten Informationen dienen den Webseitenbetreibenden dazu, den Nutzenden bei einem erneuten Besuch der Webseite wiederzuerkennen und bestimmte Funktionen an diesen anzupassen.

Cookies können dabei unterschiedliche technische Ziele verfolgen. Die Benennung dieser Cookies variiert teilweise, doch stehen hinter den Bezeichnungen die gleichen technischen Absichten. Die sogenannten notwendigen bzw. essenziellen Cookies werden für den Webseitenbesuch zwingend benötigt. Darunter fällt zum Beispiel die Speicherung des Inhalts von Warenkörben. Der Inhalt wird durch das entsprechend gesetzte Cookie nicht „vergessen“, wenn der Nutzende sein Browserfenster schließt.

Performance- bzw. technische Cookies speichern dagegen die vom Nutzenden vorgenommenen Einstellungen auf der Webseite. Beim nächsten Besuch können durch diese Cookies die Einstellungen wiederhergestellt werden, ohne dass sie vom Nutzenden jedes Mal erneut vorgenommen werden müssen. Darüber hinaus lassen sie auch Analysen über die Besuche der einzelnen Unterseiten, die Reihenfolge der besuchten Seiten oder den Standort des Nutzenden zu.

Davon zu unterscheiden sind Tracking-Cookies, welche durch die Verknüpfung von Analysedaten mit der IP-Adresse des Nutzenden eine eindeutige Zuordnung möglich machen und sogar webseitenübergreifend an Dritte weitergegeben werden können. Diese Analysen können auch für Marketingzwecke verwendet werden. Dies ist insbesondere der Fall, wenn Unternehmen daran interessiert sind, welche Webseiten von dem Nutzenden der Seite zuvor schon besucht worden waren.

Für Werbezwecke gibt es zudem noch sogenannte Werbe- bzw. Marketing-Cookies. Diese dienen Werbetreibenden dazu, bestimmte Suchen des Nutzenden zu speichern und mit hierauf abgestimmten Werbeanzeigen zu reagieren. Auch diese Daten über die Nutzenden können mit Dritten, z. B. anderen Unternehmen, geteilt werden. Hierdurch können die auf den Nutzenden zugeschnittenen Werbeanzeigen auch auf anderen Webseiten angezeigt werden und somit gezielter geworben werden.

III. Die Einwilligung

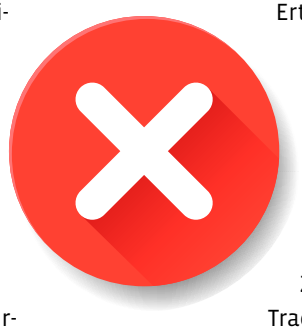
Jede Person, die im Internet surft, kennt sie: die Einwilligungsbanner zur Einholung der Erlaubnis des Besuchenden, bestimmte Cookies im Zusammenhang mit der Nutzung der Webseite speichern zu dürfen. Manche Banner sind übersichtlich gestaltet und bieten neben „Alle akzeptieren“ auch die Optionen „Nur Notwendige“ oder „Individuell“ an. Andere Banner wiederum verschleiern die Optionen und versuchen durch Farbe und Schriftgröße Nutzende in alle Cookies einwilligen zu lassen. Oftmals klickt der oder die Nutzende genervt auf „Alle akzeptieren“, um schnellstmöglich zum eigentlichen Inhalt der Webseite zu gelangen.

Grund für diese sehr unterschiedlichen Ausgestaltungen der Cookie-Banner sind die wenigen Vorschriften an die Ausgestaltung der Banner. Der BGH[6] stellte unter richtlinienkonformer Auslegung des in seiner damaligen Fas-

1 Vertiefend hierzu: John, TTDSG – Die Profis in spe, DFN-Infobrief Recht 5/2021.
2 Richtlinie 2002/58/EG.
3 Richtlinie 2009/136/EG.
4 Zum Urteil des EuGH: Baur, Noch viel zu knabbern, DFN-Infobrief Recht 12/2019.
5 BGH, Urteil v. 28.05.2020, „Cookie Einwilligung II“, Az. I ZR 7/16.
6 BGH, Urteil v. 28.05.2020, „Cookie Einwilligung II“, Az.: I ZR 7/16.

sung geltenden TMGs fest, dass für die Verwendung von technisch nicht erforderlichen Cookies der Webseitenbetreibende eine aktive Zustimmung der Nutzenden einholen muss (Opt-in). Vorausgewählte Kästchen (Opt-out) genügen den Anforderungen der Einwilligung nicht. Weitere Vorgaben existierten nicht.

Diese Auslegung manifestiert der Gesetzgeber nun in § 25 TTDSG ausdrücklich. Danach muss der Nutzende einer Webseite bei der Verwendung von Cookies oder ähnlichen Technologien „auf der Grundlage von klaren und umfassenden Informationen" einwilligen. Für die Ausgestaltung der Informationen und Einwilligung verweist das TTDSG auf die Vorschriften der Datenschutz-Grundverordnung (DSGVO).[7]



Die Einwilligung muss ausnahmsweise nicht erteilt werden, wenn die Speicherung unbedingt erforderlich ist, um den von Nutzenden ausdrücklich gewünschten Dienst überhaupt bereitstellen zu können. Dies entspricht in jedem Fall den essenziellen Cookies, wie beispielsweise der Speicherung des Warenkorbs oder der Login-Daten. Welche Cookies darüber hinaus aber unter die Einwilligungspflicht fallen, legt das TTDSG nicht fest. Insbesondere bei technischen Cookies kann die Grenze zwischen Erforderlichkeit für den „ausdrücklich gewünschten Telemediendienst" und der Einwilligungspflicht schnell verschwimmen. Auch nicht genauer geregelt wird die Ausgestaltung der Cookie-Banner. Insoweit wird den Webseitenbetreibenden weiterhin ein weiter Spielraum gelassen.

IV. Personal Information Management System

Durch die neu geschaffene Regelung des § 25 TTDSG ändert sich zunächst nichts an der bisherigen Praxis. Die Erforderlichkeit der Einwilligung wird normativ festgelegt, ein Ende der Cookie-Banner wird dadurch nicht geschaffen. Doch die Abhilfe könnte durch die Regelungen des § 26 TTDSG erfolgen. Dieser erlaubt die Verwendung von sogenannten „Personal Information Management Systems", kurz PIMS.

1. Was sind PIMS?

PIMS sind Systeme, die den Nutzenden die Möglichkeit geben sollen, mehr Kontrolle über ihre persönlichen Daten zu haben. In Bezug auf Cookies könnte dies dadurch stattfinden, dass mithilfe von PIMS die Nutzenden vorab festlegen können, in welche Nutzung von Cookies eingewilligt wird und in welche nicht. Der Vorteil hieraus besteht darin, dass der einzelne Webseitenbetreibende nicht mehr mit einem Banner die Präferenzen der Nutzenden abfragen muss, sondern anhand des PIMS diese Information direkt erhält.

Außerdem soll das PIMS durch einen Drittanbietenden verwaltet werden. Dieser soll kein Eigeninteresse an der Erteilung der Einwilligung und den verwalteten Daten haben und unabhängig von Unternehmen sein, die ein solches Interesse haben können. Dadurch kann die nutzende Person eine differenzierte Entscheidung über die einzelnen Cookies und ihre Zwecke treffen, ohne durch Farbe und Schriftgröße zu einer Einwilligung beeinflusst zu werden, die sie nicht möchte. Zum Beispiel kann auf diese Weise bestimmten Tracking-Cookies zugestimmt werden, aber die Nutzung von Werbe-Cookies von ausgewählten Unternehmen unterbunden werden.

2. Anerkennungsverfahren für PIMS-Dienstanbietende

Doch zum jetzigen Zeitpunkt ist die Verwendung eines PIMS nur Theorie. Denn das TTDSG normiert nur ein Anerkennungsverfahren für Anbietende eines PIMS-Dienstes. Danach ist es möglich, dass Anbietende von PIMS, welche bestimmte Bedingungen erfüllen, von einer unabhängigen Stelle anerkannt werden. Die Voraussetzungen dieses Anerkennungsverfahrens müssen zuvor aber in einer Rechtsverordnung durch die Bundesregierung festgelegt werden. Für eine flächendeckende Anwendung der PIMS in der Praxis ist es demnach im nächsten Schritt erforderlich, dass die Bundesregierung eine Verordnung schafft, welche die Anforderungen an einen solchen Dienst festlegt. Wann diese kommt, bleibt vorerst offen.

3. Praxisprobleme mit PIMS

Darüber hinaus stellen sich weitere Probleme in der Praxis. Einerseits sind Browserherstellende verpflichtet, die Cookie-Einstellungen der Nutzenden über die Browservoreinstellungen zu beachten, andererseits müssen sie die PIMS-Einstellungen umsetzen. Sollten sich die Einstellungen widersprechen, ist erst mal unklar, welche Einstellungen Vorrang genießen. Der Wortlaut des TTDSG lässt vermuten, dass die Browsereinstellungen vorrangig sind, doch führt das Gesetz das Verhältnis nicht genauer aus.

7 Zur datenschutzrechtlichen Einwilligung siehe Fischer, Ja, ich will!, DFN-Infobrief Recht 03/2020.

Aber auch Webseitenbetreibende müssen sich mit den PIMS nun umfassend auseinandersetzen: nicht nur, dass Schnittstellen geschaffen werden müssen, um Einstellungen von PIMS berücksichtigen zu können und auf der eigenen Webseite umzusetzen. Es zeigt sich auch, dass das TTDSG davon ausgeht, dass eine individuelle Einwilligung Nutzender auf der Webseite weiterhin Vorrang gegenüber den PIMS-Einstellungen haben soll. Für Webseitenbetreibende bleibt damit die Möglichkeit, weiterhin nach einer individuellen Einwilligung in bestimmte Cookies zu fragen, wenn eine Einwilligung über das PIMS nicht vorher schon erteilt wurde. Die Hoffnung, dass Cookie-Banner der Vergangenheit angehören werden, ist daher eher kritisch zu betrachten. Es ist vielmehr zu befürchten, dass die Einwilligungsbanner auf den Webseiten trotz des Einwilligungsmanagements der Nutzenden nicht wesentlich abnehmen werden.

Außerdem offenbart sich ein weiteres Defizit des TTDSG. Während die Missachtung von Einwilligungen der Nutzenden in Cookies nach § 25 TTDSG mit Geldbußen bis zu 300.000 Euro von den Aufsichtsbehörden sanktioniert werden kann, sieht das Gesetz keine entsprechende Regelung vor für die Missachtung von Einwilligungen, welche mittels PIMS getroffen wurden. Telemedien-Anbietende können damit PIMS-Einstellungen ignorieren, ohne Sanktionen befürchten zu müssen.

V. Fazit für Hochschulen und Forschungseinrichtungen

Für Hochschulen und Forschungseinrichtungen als Webseitenbetreibende ändert sich mit dem neuen TTDSG zunächst wenig. Die Einwilligungen der Nutzenden in technisch nicht erforderliche Cookies müssen weiterhin eingeholt werden. In der Abgrenzungsfrage, bei welcher Art von Cookie die Einwilligung erforderlich ist, gibt das TTDSG weiterhin keine genaueren Kategorien zur Hand. Insoweit bleibt zu empfehlen, im Zweifelsfall die Einwilligung zu kritischen Cookies einzuholen.

Bezüglich der Ausgestaltung des Cookie-Banners schreibt das TTDSG nun das Opt-in-Verfahren ausdrücklich vor, um eine Einwilligung des Nutzenden wirksam einzuholen. Da dies dem aktuellen Stand der Rechtsprechung entspricht, sollte an dieser Stelle nicht nachgebessert werden müssen. Sobald die erforderliche Rechtsverordnung für die Einwilligung unter Zuhilfenahme von PIMS von der Bundesregierung erlassen wird, müssen die Webseiten der Hochschulen und Forschungseinrichtungen auch daran angepasst werden.

Insgesamt sind die Vorschriften zum Cookie-Management nur teils gelungen. Zwar werden durch die neuen Normen unanwendbare Vorschriften und damit verbundene Unsicherheiten beseitigt und die aktuelle Rechtsprechung zur Einholung von Einwilligungen in die Nutzung von Cookies manifestiert, doch bleiben weiterhin Fragen bezüglich der Erforderlichkeit einer Einwilligung offen. Die Möglichkeit der Verwendung von PIMS ist zunächst ein Schritt in die richtige Richtung. Doch lässt die normierte Ausgestaltung der Verwendung von PIMS noch zu wünschen übrig. Die neuen Regeln des TTDSG bedeuten nicht nur, dass weiterhin auf eine Rechtsverordnung gewartet werden muss, sondern dass trotz der Verwendungsmöglichkeit weiterhin mit Cookie-Bannern gerechnet werden muss, während besonders dreiste Webseitenbetreibende die Einstellungen der PIMS-Nutzenden sanktionslos ignorieren können. Eine Nachbesserung durch den Gesetzgeber wäre an diesen Stellen wünschenswert. ◆

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. Wo wir überall unterwegs sind, zeigen wir hier.

Als Entwickler des TLSLookingGlass beschäftigt sich Jan-Frederik Rieckers im eduroam-Team insbesondere mit dem Thema Sicherheit. Seine erste Dienstreise nach zwei Jahren Coronapandemie führte ihn …

… nach Wien zum Treffen der Internet Engineering Task Force (IETF), das vom 19. bis 25. März 2022 stattfand.

Haben Sie sich schon einmal gefragt, warum das Internet eigentlich funktioniert? Es ist doch sehr beeindruckend, dass es nicht relevant zu sein scheint, von welchem Hersteller ich meinen Router kaufe. Der eduroam-Login funktioniert technisch immer gleich, ganz egal, ob ich ein Apple- oder ein Android-Smartphone habe. Und mein Thunderbird ruft E-Mails von allen Mailservern ab, egal welche Software die E-Mails im Hintergrund verwaltet. Das alles wäre nicht möglich ohne die Internet Engineering Task Force (IETF).

Seit 1986 treffen sich im Rahmen der IETF-Meetings Forschende und Aktive, um an sogenannten „Requests for Comments" (RFCs) zu arbeiten. In diesen RFCs sind Protokollabläufe standardisiert, sodass alle Geräte miteinander interagieren können, ohne sich vorher untereinander absprechen zu müssen. Der IETF verdanken wir unter anderem Protokolle wie IP, TCP, DNS, TLS, HTTP und viele mehr.

Ich fahre schon am Freitag vor der IETF nach Wien. Denn das Wochenende vor dem Meeting wird für einen Hackathon genutzt. Ziel ist es, die Standards und Entwürfe auf Praxistauglichkeit zu testen. Denn was bringt mir ein Standard, wenn ihn niemand implementieren kann? Mein Projekt, die Implementierung eines bestimmten RFCs, habe ich mir schon vorher ausgesucht, setze mich nun zum Hackathon an einen Tisch und baue mein Material auf. Andere Teilnehmende des Hackathons beschäftigen sich mit anderen Themen. Es ist ein wirklich bunter Haufen und ich komme mit vielen ins Gespräch. Diese Gespräche sind das, was mir in den vergangenen Jahren am meisten gefehlt hat und einer der Gründe, weshalb ich nach Wien gefahren bin. Ich spreche mit einem der Autoren von BRSKI (Bootstrapping Remote Secure Key Infrastructure), einem Protokoll für das Provisionieren von Internet-of-Things-Geräten. Wir diskutieren, wie BRSKI über EAP, dem Protokoll, auf dem eduroam aufbaut, implementiert werden kann.

Am Montag beginnt dann das eigentliche IETF-Meeting. Insgesamt 314 Teilnehmende treffen sich vor Ort, ca. 1000 sind remote zugeschaltet. Als erstmaliger Vor-Ort-Teilnehmer gehe ich am Sonntagnachmittag zu den „Newcomers Quick Connections". Hier lerne ich einige der langjährigen Teilnehmenden kennen und kann schon erste Kontakte knüpfen und Fragen stellen. Wie funktioniert die IETF? Wie kann ich mich einbringen und was sollte ich dafür mitbringen? Wertvolle Informationen, wenn der eigene Entwurf irgendwann mal als RFC ver-

Face-to-Face: die fachlichen Diskussionen, das rege Netzwerken, aber auch der persönliche Austausch sind endlich wieder in Präsenz möglich. *Foto: Stonehouse Photographic / IETF Trust*

öffentlicht werden soll. Auch während der Konferenz werde ich immer wieder angesprochen. Hilfreich dabei ist das Farbband unter meinem Namensschild, das mich als neuen Teilnehmer ausweist. Das erleichtert den Gesprächseinstieg. Denn viele interessieren sich dafür, was mich zur IETF gebracht hat und was ich hier machen möchte.

Die inhaltliche Arbeit findet in Working-Group-Sessions statt, insgesamt 14 Slots und meist acht Sessions parallel. Jeweils eine Working-Group beschäftigt sich immer mit einem speziellen Teilgebiet des Internets, z. B. dem BGP-Routing oder der Erweiterung von IPv6. Die Pausen zwischen den Sessions werden für das Netzwerken und tiefere Diskussionen, die „Hallway Discussions", genutzt.

Die für mich interessanteste Session findet am Dienstagmittag statt – EAP Method Update (emu) heißt die Working-Group, die für meinen Protokollentwurf zuständig ist. Diese Working-Group beschäftigt sich mit dem EAP-Protokoll und hat vor Kurzem z. B. EAP-TLS für die Nutzung mit TLSv1.3 angepasst. Die Agenda ist voll, es bleibt nicht viel Zeit für die Vortragenden. Um die Sitzung zu beschleunigen, habe ich mich schon vor Beginn der Session als Protokollant angeboten. Neben einigen neuen EAP-Methoden, die auch im eduroam-Kontext interessant werden könnten, wird ein Entwurf vorgestellt, der sich mit der Provisionierung von EAP-Konfigurationen auf Endgeräten beschäftigt. Ein interessanter Vorschlag, hat uns dieses Problem in eduroam doch immer wieder Kopfschmerzen bereitet. Ich markiere mir den Entwurf in meinen Lesezeichen für später, den werde ich mir nach dem Meeting genauer anschauen und Feedback geben. Nach einigen weiteren Vorträgen ist endlich mein Entwurf an der Tagesordnung. Wir sind schon im Verzug, sodass ich schnell durch meine Folien rennen muss. Zeit für Feedback in der Session bleibt leider nicht.

Die Zeit vergeht wie im Flug, kaum angefangen ist die IETF am Freitag auch schon wieder vorbei. Der krönende Abschluss ist das Abendessen mit zwei langjährigen Teilnehmenden, mit denen ich bei taiwanesischem Essen über die verschiedenen Internetprotokolle und Eigenheiten der IETF diskutiere. Am Tag darauf sitze ich im ICE und bereite das Meeting nach. Die richtige Arbeit beginnt erst jetzt, denn die technischen Diskussionen finden außerhalb der Meetings auf den vielen Mailinglisten statt. Ich werde sicher auch das eine oder andere Mal meine Meinung kundtun, denn das Feedback aus dem operativen Geschäft ist für die Standardisierung essenziell und so kann ich die DFN-Sicht auf diese Protokolle einfließen lassen und bei der Verbesserung des Internets helfen. ◆

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. Gerade in Covid-19-Zeiten erhält der Austausch innerhalb der Netz-Community – egal ob digital oder physisch – eine besondere Bedeutung.
In welchem Format die jeweiligen Veranstaltungen abhängig vom künftigen Pandemiegeschehen stattfinden, geben wir rechtzeitig über unsere etablierten Informationskanäle bekannt.

DFN-Mitgliederversammlung

Eine der Stärken des DFN-Vereins ist das breite Mandat seiner Mitglieder. Mit über 350 institutionellen Mitgliedern engagiert 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.

Aufgrund des Pandemiegeschehens fand die 83. Mitgliederversammlung am Mittwoch, 15. Dezember 2021, erneut virtuell statt. Themen waren unter anderem die Vorbereitungen auf GN5 Phase 1, den Nachfolger des Ende des Jahres auslaufenden Projekts GN4 Phase 3, und der für dieses Jahr geplante Ausbau der IP-Plattform sowie die Neuvergabe der Teilnehmeranbindungen. Ein wichtiger Berichtspunkt war die Weiterentwicklung des Dienstes Security Operations. Positiv berichtet wurde auch über das Pilotprojekt EasyRoam4Edu, das mit der zertifikatbasierten Anmeldung ohne Username und Passwort dazu beiträgt, die Sicherheit in eduroam zu erhöhen.

TERMIN

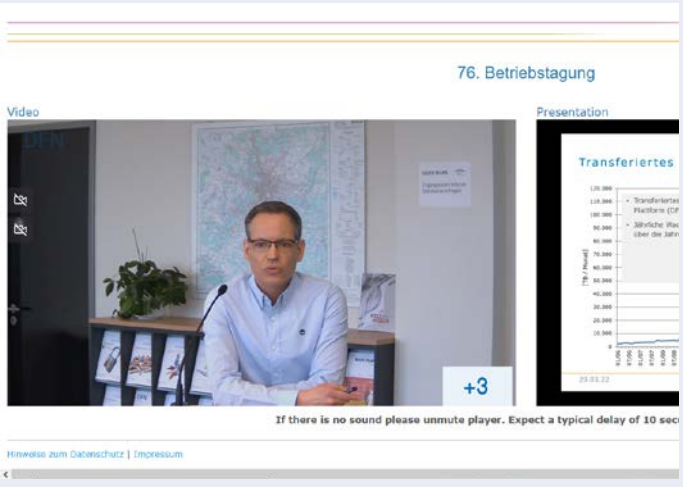
Die 84. Mitgliederversammlung findet am **Dienstag, 14. Juni 2022**, statt.

DFN-Betriebstagung

Toller Auftakt im Frühjahr: Am Dienstag und Mittwoch, 29. und 30. März 2022, traf sich die DFN-Community zur 76. DFN-Betriebstagung (BT) und informierte sich über aktuelle Entwicklungen rund um das X-WiN und die DFN-Dienste. Die Veranstaltung fand wie auch in den vergangenen zwei Jahren aufgrund des aktuellen Pandemiegeschehens online statt. Die Beteiligung war erneut rekordverdächtig: Über 400 Teilnehmende zählte das gemeinsame Plenum, das über die DFNconf-Plattform gestreamt wurde. Und auch die Fachforen von Sicherheit über AAI und Wissenschaftsnetz bis Clouddienste waren mit bis zu 341 Gästen sehr gut besucht. Die zwei Veranstaltungstage waren prall gefüllt mit Neuigkeiten, Infos und Anregungen aus der DFN-Community und die vielen spannenden Vorträge boten wieder jede Menge Stoff zum Austauschen und Vertiefen.

TERMIN

Die 77. DFN-Betriebstagung findet am **Dienstag und Mittwoch, 18. und 19. Oktober 2022,** statt.



Neues vom X-WiN: Stefan Piger, Bereichsleiter Network and Communication Services, gab den Teilnehmenden einen aktuellen Überblick zum Wissenschaftsnetz, unter anderem zum stetig wachsenden Datenvolumen auf der IP-Plattform.

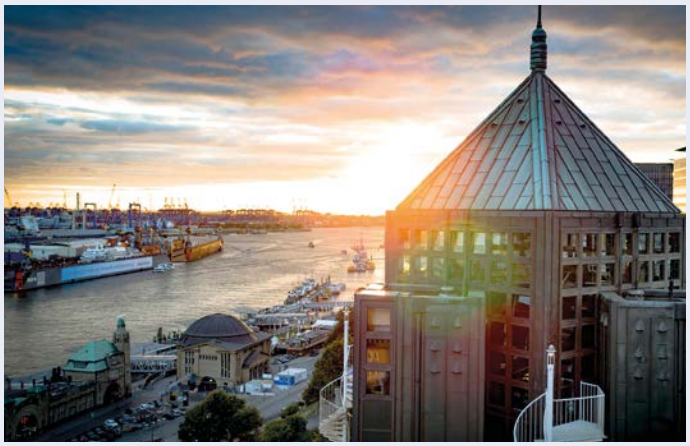


Foto: Hotel Hafen Hamburg

DFN-Konferenz „Datenschutz“

Seit 2012 veranstaltet das DFN-CERT im Auftrag des DFN-Vereins jährlich die DFN-Konferenz „Datenschutz“. Ziele sind unter anderem die Beratung und der Austausch der für die Einhaltung und die praktische Umsetzung des Datenschutzes Verantwortlichen in Forschungs- und Bildungsinstitutionen sowie Behörden. Zugleich bietet die Veranstaltung die Möglichkeit, Anforderungen mit Vertretenden der Datenschutzaufsichtsbehörden und eingeladenen Expertinnen und Experten aus der Datenschutzpraxis zu diskutieren. In den vergangenen zwei Jahren fiel die Veranstaltung pandemiebedingt aus und wurde durch das DFN-Kolloquium „Datenschutz“ ersetzt, das im November 2020 zum ersten Mal online stattfand. Im vergangenen Jahr zählte das Webinar 135 Teilnehmende. Die diesjährige DFN-Konferenz „Datenschutz“ findet voraussichtlich wieder in Präsenz statt.

TERMIN

Die 9. DFN-Konferenz „Datenschutz“ findet am Dienstag und Mittwoch, **29. und 30. November 2022,** in Hamburg statt.

DFN-Konferenz „Sicherheit in vernetzten Systemen“

Vom 2. bis 4. Februar 2022 fand die 29. DFN-Konferenz „Sicherheit in vernetzten Systemen“ statt, die das DFN-CERT im Auftrag des DFN-Vereins jedes Jahr veranstaltet. Mit ihrer explizit technischen und wissenschaftlichen Ausrichtung, einer großen Vielfalt an Beiträgen und Diskussionen sowie durchschnittlich 350 Teilnehmenden hat sich die DFN-Konferenz als eine der größten deutschen Tagungen für Informationssicherheit etabliert.

Wie bereits im vergangenen Jahr fand die Konferenz als Onlinewebinar statt. Die Teilnehmenden profitierten von den vielen praxisbezogenen aktuellen Themen: unter anderem rund um das Informationssicherheitsmanagement, zu Zwei-Faktor- und Multi-Faktor-Authentifizierungen sowie zu der aktuellen gesetzlichen Entwicklung der neuen NIS 2-Richtlinie. Der Nachmittag des dritten Tages blieb traditionell dem Tutorium vorbehalten, das sich diesmal den „Last ten years of security – Lessons learned“ widmete.

TERMIN

Die 30. DFN-Konferenz „Sicherheit in vernetzten Systemen“ findet am **Donnerstag und Freitag, 9. und 10. Februar 2023,** statt.

Aktuelle Informationen rund um das Deutsche Forschungsnetz und seine Veranstaltungen erhalten Sie auch regelmäßig in unserem Newsletter.

Den DFN-Newsletter können Sie unter **www.dfn.de** abonnieren.

Überblick DFN-Verein

(Stand: 06/2022)

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 Ulm)

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:
Hartmut Hotzel
(Bauhaus-Universität Weimar)

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
	Campus Berlin-Buch GmbH
	Deutsche Telekom AG Laboratories
	Deutsche Telekom IT GmbH
	Deutsches Herzzentrum Berlin
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	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
	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	Fachhochschule Bielefeld
	Universität Bielefeld
Bingen	Technische Hochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Hochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Hochschule Georg Agricola
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern, 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
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
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 gGmbH
Ilmenau	Technische Universität Ilmenau
Ingolstadt	DiZ – Zentrum für Hochschuldidaktik d. bayerischen Fachhochschulen
	Hochschule für angewandte Wissenschaften FH 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
	Technische Universität Kaiserslautern
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
	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	Deutsche Telekom, Hochschule für Telekommunikation 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	Hochschule Mannheim
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	TÜV SÜD Energietechnik GmbH Baden-Württemberg
	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
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)
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
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	Hochschule für angewandte Wissenschaften – Fachhochschule Würzburg-Schweinfurt
	Julius-Maximilians-Universität Würzburg
	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/