DFN mitteilungen

Im Dienste der Wissenschaft

40 Jahre DFN-Verein

9 770177 689001

In The Field
Daran forschen unsere Mitglieder

Dein Freund und Helfer?
ChatGPT in der Prüfung

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: SasinParaksa/Adobe Stock
Rückseite: MissesJones, SasinParaksa/Adobe Stock

Prof. Dr.-Ing. Stefan Wesner
Vorstandsvorsitzender im DFN-Verein
Professor für Parallele und Verteilte Systeme
an der Universität zu Köln und Direktor des
IT Center University of Cologne (ITCC)

40 Jahre Deutsches Forschungsnetz, 40 Jahre Wissenschaft im Fokus, 40 Jahre Solidarität – ein Privileg und auch eine besondere Verantwortung, in solch einem Jahr als neu gewählter Vorstand zu starten.

Wir haben Menschen aus unserer Mitte gebeten, uns einen Einblick in ihre ganz persönliche Sicht auf dieses Jubiläum zu geben. Die teils emotionalen Statements sind eine Reise durch die Geschichte des DFN-Vereins. Sie zeigen, welch wichtige Rolle der DFN-Verein bereits in seinen Anfängen für die Zusammenarbeit von Rechenzentren in Deutschland gespielt hat und wie fest verankert er heute in der Wissenschaft ist. Die Erinnerungen machen deutlich, wie herzlich verbunden die Menschen unserem DFN-Verein sind – ja, wie viel Lebensleistung, Freude, Leidenschaft und Vertrauen uns über die Jahrzehnte geschenkt wurden. Das beeindruckt und berührt mich sehr. Von Werten ist die Rede, von Zuverlässigkeit, Kraft und Inspiration. Manches liest sich fast wie eine Liebeserklärung. Der DFN-Verein und die Wissenschaft – ein Bund fürs Leben?

Unser Wissenschaftsnetz verbindet und unterstützt in letzter Konsequenz Menschen. Das sollte bei aller Begeisterung für die darunterliegende Technik nicht vergessen werden! Es steht für die Vielfalt der wertvollen Erkenntnisse, die tagtäglich von der Wissenschaft in nationalen und weltweiten Forschungskooperationen gewonnen werden – zum Wohl von Mensch, Natur und Gesellschaft. Es steht für Kommunikation auf höchstem Niveau und damit für Chancen gegenseitiger Verständigung. Gleichzeitig spiegelt das hohe Verkehrsaufkommen im X-WiN den Gestaltungswillen, den Erfindungsreichtum und die Schaffensfreude unserer teilnehmenden Einrichtungen wider.

Die Herausforderungen für Hochschulen und Forschungseinrichtungen werden weiter steigen. In einer immer komplexer werdenden Welt müssen sie sich zunehmend behaupten. Als starke und zuverlässige Gemeinschaft wollen wir sie dabei auch zukünftig unterstützen. Lassen Sie uns die Erfolgsgeschichte des DFN-Vereins zusammen fortschreiben – feiern Sie mit uns 40 Jahre vertrauensvolle Zusammenarbeit und Solidarität in der Wissenschaft.

Ihr Stefan Wesner

Inhalt

Unabhängig, solidarisch und selbstbestimmt – 40 Jahre DFN-Verein
Welche Ereignisse zur Unabhängigkeit des DFN-Vereins führten, erzählt Prof. Dr. Bernhard Neumair im Interview

Mit Köpfchen – und DFN-MailSupport
Gehirn oder Technik? Bei Sicherheitsvorfällen spielt der Faktor Mensch eine große Rolle

Satellites and Ships
Researchers Combine Data Sources to Study Arctic Warming

Wissenschaftsnetz

Unabhängig, solidarisch und selbstbestimmt – 40 Jahre DFN-Verein
Interview von Maimona Id **8**

Mit Köpfchen – und DFN-MailSupport
von Michael Röder **13**

Erfolgreich verlängert – die DFNconf-Rahmenverträge
von Dirk Bei der Kellen **18**

Kurzmeldungen **20**

Forschung

Satellites and Ships: Researchers Combine Data Sources to Study Arctic Warming
von Eric Gedenk **22**

Building a Town Square for NRENs
Interview von Eric Gedenk **26**

International

International Newsflashes **28**

Sicherheit

Quo vadis, Cybersecurity? Die Cybersicherheitsregulierung der EU
von Dennis-Kenji Kipker **30**

Quickcheck für mehr Cybersicherheit
von Reinhold Hepp und Markus Schäffter **34**

Mit Ausbildung Schule machen
von Maimona Id **38**

Sicherheit aktuell **43**

Campus

ChatGPT – dein Freund und Helfer in der Prüfung?
von Matthias Baume **46**

Mit Ausbildung Schule machen
Die Antwort auf den verschärften Fachkräftemangel in der IT

Recht

Ich glaub, es hackt
von Johannes Müller **52**

Die Bretonage der europäischen Datenstrategie
von Ole-Christian Tech **56**

DFN-Verein

DFN unterwegs **60**

DFN live **63**

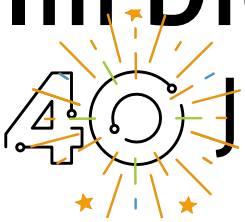
Überblick DFN-Verein **66**

Die Mitgliedseinrichtungen **68**

Autorinnen und Autoren dieser Ausgabe im Überblick

1 Maimona Id, DFN-Verein (id@dfn.de); **2** Michael Röder, DFN-Verein (roeder@dfn.de); **3** Dr. Dirk Bei der Kellen, DFN-Verein (beiderkellen@dfn.de); **4** Eric Gedenk, DFN-Verein (info@impact-scicomm.com); **5** Prof. Dr. Dennis-Kenji Kipker, cyberintelligence.institute (dennis.kipker@cyberintelligence.institute); **6** Reinhold Hepp, Polizeivizepräsident a. D. Ulm (reinhold.hepp@web.de); **7** Prof. Dr. Markus Schäffter, Technische Hochschule Ulm (markus.schaeffter@thu.de); **8** Dr. Matthias Baume, Technische Universität München (matthias.baume@tum.de); **9** Johannes Müller, Forschungsstelle Recht im DFN (johannes.mueller@uni-muenster.de); **10** Ole-Christian Tech, Forschungsstelle Recht im DFN (ole-c.tech@uni-muenster.de)

Im Dienste der Wissenschaft



Jahre DFN-Verein

1981

Vier Ereignisse ebnen den Weg für die spätere Gründung:

1. Das Forschungsinstitut Stanford Research International erstellt eine Studie für das Bundesministerium für Forschung und Technologie (BMFT),
2. Das BMFT unternimmt eine Informationsreise in die USA,
3. Das Hahn-Meitner-Institut (HMI) Berlin – heute Helmholtz-Zentrum Berlin (HZB) – macht einen Vorschlag für einen „Norddeutschen Rechnerverbund“,
4. Die Gesellschaft für Mathematik und Datenverarbeitung (GMD) skizziert Ideen für ein deutsches Forschungsverbundnetz.

1982

Ein OSI-Forschungsnetz soll es sein! Das ist das Ergebnis der ersten Diskussionsversammlung im DESY in Hamburg.

1983

Ein Netz aus der Mitte der Wissenschaft: Die Idee der heutigen Organisationsform wird geboren – eine Gemeinschaft aus Wissenschaft und Industrie als Entwickler und Betreiber des Wissenschaftsnetzes.

1984

Es ist so weit: Am 12. Januar 1984 wird der Verein zur Förderung eines Deutschen Forschungsnetzes e. V. (DFN-Verein) gegründet. Zum Gründungsvorstand gehören Prof. Dr. Zander (2. v. li.), Prof. Dr. Szyperski (3. v. li.) und Prof. Dr. Jessen (nicht im Bild). Das Hahn-Meitner-Institut zählt zu den 11 Gründungsmitgliedern, vertreten durch den damaligen Geschäftsführer Dr. Nettesheim (1. v. li.). Klaus Ullmann (1. v. re.) war einer der ersten Geschäftsführer des DFN-Vereins.

1985

Die erste Ausgabe des Mitgliedermagazins DFN-Mitteilungen erscheint – ein „Ort“, an dem die DFN-Community sich über ihre Erfahrungen und Ideen zum Aufbau des damals größten deutschen Verbundprojekts auf dem Gebiet der Kommunikationstechnik austauschen kann.

1987

Die erste DFN-Betriebstagung findet statt. Das „Klassentreffen“ der DFN-Community dient bis heute dem Austausch von aktuellen Entwicklungen und Neuigkeiten rund um das X-WiN und seine Dienste.

1989

Das Wissenschaftsnetz X.25-WiN geht mit 230 Anschlüssen an den Start. Den Vertrag – der erste privatwirtschaftliche Dienstleistungsvertrag der Deutschen Bundespost – unterzeichnen Bundesminister Dr. Christian Schwarz-Schilling, Friedrich Winkelhage und Prof. Dr. Eike Jessen (von links).

1991

ERWiN kommt! 1991, ein Jahr nach der deutschen Wiedervereinigung, wird das erste deutsche Wissenschaftsnetz X.25-WiN durch ERWiN erweitert. 51 Teilnehmer aus den neuen Bundesländern erhalten Zugang. Die TU Dresden gehört zu den ersten Teilnehmern. Ein Jahr zuvor richtete sie mittels Modem und HDN ein Provisorium zum X.25-WiN ein. Das führte vor lauter Freude zum berühmten „Dresdner Fenstersprung". DFN-Mitarbeiter Hans-Martin Adler stellt ERWiN vor.

1992

Gründung des WiN-Labors am Regionalen Rechenzentrum (RRZE) der Friedrich-Alexander-Universität Erlangen-Nürnberg zur Entwicklung von Software und Tools. Themen heute: Quantennetze und Techniken zur Zeitsynchronisation im Netz.

1993

Der DFN-Verein gründet das Computer Emergency and Response Team (CERT) als eines der ersten CERTs in Deutschland. Mit seinen Dienstleistungen und Beratungsangeboten unterstützt das DFN-CERT damals wie heute die DFN-Teilnehmer beim Thema IT-Sicherheit.

1994

Gründung des ersten europäischen Forschungsnetzes DANTE Ltd als erste länderübergreifende Infrastruktur für wissenschaftliche Kooperationen. Heute sorgt GÉANT für die Konnektivität zu europäischen sowie weltweiten Forschungsnetzen. Das X-WiN ist mit 600 Gbit/s an GÉANT angeschlossen.

1996

Seit Gründung der Forschungsstelle Recht im DFN forschen Juristinnen und Juristen im Auftrag des DFN-Vereins zu rechtlichen Fragen rund um die Nutzung des Deutschen Forschungsnetzes und seiner Dienste.

1997

Aufbau der Gigabit-Struktur – ein Schritt in die neue Dimension der optischen Kommunikationsnetze – startet im Breitbandnetz B-WiN.

2000

Die dritte Netzgeneration, das G-WiN, unterstützt zunächst Übertragungsgeschwindigkeiten von 2,5 GBit/s, später sogar bis zu 10 GBit/s.

2003

Der Dienst DFNRoaming – der Vorläufer von eduroam – ermöglicht reisenden Forschenden weltweit einen einfachen und sicheren Netzzugang. Heute werden pro Jahr mehr als 7,5 Milliarden registrierte Authentifizierungen (Stand 2023) gezählt. Der WLAN-Zugangsdienst ist in mehr als 100 Ländern vertreten.

2006

In eigener Funktionsherrschaft: Mit der vierten Netzgeneration, dem X-WiN, verfügt der DFN zum ersten Mal über ein eigenes flächendeckendes Glasfasernetz inkl. einer Übertragungstechnologie mit frei skalierbaren Bandbreiten. Festakt am DESY: Prof. Juling nimmt das X-WiN feierlich in Betrieb.

2009

Das X-WiN verfügt über 10 000 km Glasfaser. Die doppelte Anbindung der Teilnehmer wird zum Standard.

2024

354 Mitglieder bilden eine starke Gemeinschaft im DFN-Verein, der mit seinem Wissenschaftsnetz Hochschulen, außeruniversitäre Forschungseinrichtungen sowie forschungsnahe Wirtschaftsunternehmen an aktuell 849 Standorten in ganz Deutschland verbindet. Mit einer Gesamtlänge von 10 250 km Glasfaser im Backbone und einem Multi-Terabit-Kernnetz, das sich zwischen 65 Kernnetzstandorten aufspannt, zählt das X-WiN heute zu den größten und leistungsfähigsten Forschungsnetzen weltweit.

Unabhängig, solidarisch und selbstbestimmt – 40 Jahre DFN-Verein

Als Prof. Dr. Bernhard Neumair, ehemaliger Direktor des Scientific Computing Center (SCC) am Karlsruher Institut für Technologie (KIT), 2005 in den Vorstand gewählt wurde, befand sich der DFN-Verein, mehr als 20 Jahre nach seiner Gründung, in einer komplexen Umbruchphase. Das Wissenschaftsnetz, die technische Plattform des DFN, wurde völlig neu konzipiert. Der damalige stellvertretende Vorstandsvorsitzende erinnert sich, welche Ereignisse dazu führten und welche Herausforderungen dies mit sich brachte.

Im Dezember 2005 wurden Sie in den Vorstand des DFN-Vereins gewählt. Da war der Verein 21 Jahre alt. Ihr Draht zum DFN besteht aber schon sehr viel länger.

Nach meinem Studium der Informatik und Elektrotechnik an der TU München habe ich 1987 angefangen, als wissenschaftlicher Mitarbeiter am Lehrstuhl von Heinz-Gerd Hegering an der LMU zu arbeiten. Dieser war zu der Zeit stellvertretender Vorstandsvorsitzender im DFN-Verein und erzählte begeistert von den Fortschritten, wenn er aus Berlin kam. Durch Herrn Hegering habe ich die ersten Pionierjahre und Meilensteine des DFN miterlebt. Danach ging ich zunächst in die freie Wirtschaft. Ich wollte nicht nur forschen, sondern vor allem hands-on arbeiten, ein reales Netz planen und verwirklichen. Und auch hier, bei der DeTeSystem – einer Telekom-Tochter, die den DFN als Kunden betreute – begegnete ich dem Verein wieder.

Es dauerte aber noch ganz schön lange, bis Sie an Bord waren.

Als ich 2003 den Ruf an die Universität Göttingen erhielt und gleichzeitig Geschäftsführer der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) wurde, kamen Herr Hegering und Wilfried Juling, der spätere DFN-Vorstandsvorsitzende – damals schon im Verwaltungsrat – auf mich zu. Zu beiden hatte ich die ganzen Jahre engen Kontakt gehalten. Nach dem Motto, der Neumair ist zurück in der akademischen Welt, fragten sie mich, ob ich mir vorstellen könnte, im Verein aktiv zu werden. Wie Netz funktioniert, wusste ich, und das wiederum wussten die beiden. Der DFN-Verein ist DAS – bitte großschreiben – wissenschaftliche Netz in Deutschland. Wenn man da gefragt wird, dann denkt man nicht lange nach, man freut sich und macht einfach mit. Bei meiner Historie und meinen Erfahrungen war es eine Ehre, sich beim DFN zu engagieren.

Als Sie 2005 in den Vorstand gewählt wurden, befand sich der DFN-Verein in einer Umbruchphase. Was war passiert?

Das waren in der Tat aufregende Zeiten für den DFN-Verein. Zum einen die bahnbrechenden Entwicklungen im Bereich der Kommunikations- und Informationstechnologien, die sich natürlich auch auf das Wissenschaftsnetz auswirkten. Die Liberalisierung des Telekommunikationsmarktes und die damit entstandene Vielfalt der Marktanbieter nach dem Wegfall des Netzmonopols der Telekom eröffneten ganz neue Möglichkeiten für den DFN-Verein. Wir

Foto: DFN

Prof. Dr. Bernhard Neumair | **2010 bis 2024** Direktor des Scientific Computing Center (SCC) am Karlsruher Institut für Technologie, Professur für das Management komplexer IT-Systeme | **2005 bis 2014** Stellvertretender Vorstandsvorsitzender des DFN-Vereins und Vorsitzender des Betriebsausschusses | **2003 bis 2010** Geschäftsführer der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), Professur für Praktische Informatik an der Universität Göttingen | **2001 bis 2003** TSI GmbH München, Leiter der Abteilung Planning | **1998 bis 2001** DeTeSystem GmbH München, Leiter der Gruppe Kommunikationslösungen | **1993 bis 1998** Wissenschaftlicher Assistent am Institut für Informatik der Ludwig-Maximilians-Universität München | **1993 bis 1998** TTI Tectran GmbH, München/Grünwald, Mitglied des wissenschaftlichen Beratergremiums | **1993** Promotion an der Technischen Universität München im Gebiet Leistungsmanagement in Rechnernetzen | **1987 bis 1992** Wissenschaftlicher Angestellter am Institut für Informatik der Technischen Universität München | **1987** Diplom in Informatik an der Technischen Universität München

wollten das Wissenschaftsnetz neu erfinden. Und ausgerechnet zu der Zeit kündigte das Bundesministerium für Bildung und Forschung (BMBF) die bisherige Förderung für den DFN-Verein. Mit dieser hatte der Bund seit Gründung des Vereins 1984 eine Anschubfinanzierung für den Aufbau des Wissenschaftsnetzes und seiner Infrastruktur bereitgestellt – wir sprechen hier von einem siebenstelligen Betrag. Die sogenannte Fehlbedarfsfinanzierung sollte einen finanziellen Ausgleich für die hohen Investitionsbeschaffungen des Netzaufbaus und -betriebs sowie für die DFN-Forschungsprojekte darstellen. Dieses Sicherheitsnetz fiel nun weg.

> „Seiner Bezeichnung als „Selbsthilfe der Wissenschaft“ hat der DFN damit alle Ehre gemacht.“

Mit den Nachwirkungen hatten wir im neu gewählten Vorstand alle Hände voll zu tun. Als gemeinnütziger Verein waren wir zum Beispiel stark eingeschränkt, was die Kreditaufnahme anging und an die zeitnahe Verwendung von Mitteln gebunden. Das war eine nicht zu unterschätzende existenzielle Herausforderung für den Verein, aus der er jedoch gestärkt und vor allem autark hervorging. Mit dem ausgeprägten Solidaritätsbewusstsein der Mitgliederschaft konnte die Finanzierung gestemmt werden. Seiner Bezeichnung als „Selbsthilfe der Wissenschaft“ hat der DFN damit alle Ehre gemacht. Diese Unabhängigkeits- und Selbstbestimmungsbestrebungen sollten sich mit der Planung der vierten Generation des Wissenschaftsnetzes fortsetzen.

Inwiefern war der DFN mit dem neuen Netz selbstbestimmt und wie unterschied es sich von seinem Vorgänger?

Mit dem X-WiN verfügte die Wissenschaft in Deutschland zum ersten Mal über ein eigenes flächendeckendes Glasfasernetz mit Anschlusskapazitäten von bis zu 10 Gigabit pro Sekunde sowie einer eigenen Übertragungstechnologie mit frei skalierbaren Bandbreiten – ein absolutes Novum. Noch beim Gigabit-Netz, dem G-WiN, war es üblich, das Netz mit gemanagten Wellenlängen am Stück zu kaufen – ohne zu wissen, wie es bis ins Kleinste zusammengesetzt ist. Unser Ziel war jedoch, das Netz mit sämtlichen Elementen in eigener Funktionsherrschaft zu betreiben. Dafür wurde eine völlig neuartige Topologie konzipiert. Der Einsatz von WDM-Technologie (Wavelength-Division-Multiplexer, WDM), durch den erstmalig die gleichzeitige Nutzung von mehreren Wellenlängen auf

Prof. Dr. Heinz-Gerd Hegering, ehem. Vorsitzender des Direktoriums des LRZ, ehem. stellv. Vorstandsvorsitzender des DFN: „Mein persönlicher Rückblick auf 40 Jahre DFN, im zwischenmenschlichen Bereich würde man vielleicht von einer Liebeserklärung sprechen, ist ein einziges Loblied – zuallererst auf die Menschen im DFN. Dank der Visionen einiger früher Vordenker und vieler großartiger Mitstreiter, die an diese Visionen glaubten, sie mutig aufgriffen und auch umsetzten gegen anfängliche Widerstände, konnte das Fundament für die selbstbestimmte Solidargemeinschaft „Verein zur Förderung eines Deutschen Forschungsnetzes“ gelegt werden. Wenn es den DFN-Verein nicht gäbe, man müsste ihn erfinden! Ich schließe mit dem Wunsch: Lieber DFN-Verein, vivas, crescas, floreas ad multos felicesque annos!“

Neu im Vorstand: Prof. Dr. Bernhard Neumair und Prof. Dr. Wilfried Juling, zusammen mit Dr. Frank Nolden, wurden 2005 bei der 51. Mitgliederversammlung des DFN-Vereins vom Verwaltungsrat in den Vorstand berufen (v. li.) | *Foto: DFN*

einer Glasfaser möglich war, gehörte zu den wesentlichen Aspekten des neuen Konzepts. Für die Planung der Netzhierarchie und der Zugangsinfrastruktur wurde sogar ein mathematisches Optimierungsverfahren entwickelt.

2004 startete der Umbau mit der europaweiten Ausschreibung über die vier Lose Glasfasern, Veredelung von Glasfasern, Wellenlängen sowie Netzüberwachung. Bereits nach zwei Jahren wurde das X-WiN am 3. Mai 2006 mit einem Festakt am Deutschen Elektronen-Synchrotron DESY in Hamburg in Betrieb genommen. Die Migration vom G-WiN auf das X-WiN in den damals 46 Kernnetzstandorten vollzog sich in zwei Phasen und verlief völlig störungsfrei – auch das eine Meisterleistung. Zudem ging mit der Umgestaltung des Netzes eine massive Leistungssteigerung einher.

Ich komme noch einmal darauf zurück: Was hatte das mit der Unabhängigkeit des Vereins zu tun?

Mit der Möglichkeit, nun in eigener Funktionsherrschaft regelmäßige Leistungssteigerungen der Bandbreiten vornehmen sowie das Netz auf höchste Anforderungen der Teilnehmer flexibel anpassen zu können, festigte der DFN-Verein noch einmal die Souveränität und die internationale Konkurrenzfähigkeit seiner Mitglieder und teilnehmenden Einrichtungen. Denn schon damals gehörte das X-WiN zu den weltweit leistungsfähigsten und innovativsten Kommunikationsnetzen – insbesondere was die Verfügbarkeit und Ausfallsicherheit anging.

Wie hat die neue Topologie zu der höheren Verfügbarkeit und Ausfallsicherheit beigetragen?

Zunächst einmal waren die Kernnetzstandorte im X-WiN doppelt, das heißt über zwei unabhängige Strecken, angebunden. Dadurch konnten nicht nur eine höhere Ausfallsicherheit gewährleistet, sondern auch Wartungen unterbrechungsfrei durchgeführt werden. Bei der Neubeschaffung der Routertechnik wurde insbesondere auf eine redundante Ausstattung der wichtigsten Komponenten geachtet. Alle wichtigen Teile der aktiven Netzelemente waren redundant ausgelegt.

Wenn irgendwo ein Router gebootet werden muss, sind das Ausfälle von maximal zehn Minuten bis eine Stunde. Wenn aber die komplette Technik defekt ist und Komponenten erst wieder besorgt werden müssen, reden wir von einem Zeithorizont von mehreren Tagen. In der Praxis hat es tatsächlich Fälle gegeben, bei denen bedingt durch Brände große Komponenten ersetzt werden mussten. Die Abhängigkeit von der Funktionalität eines Anschlusses, insbesondere bei Großforschungsvorhaben, ist enorm und kann unter Umständen kritisch werden. Mit dem Konzept der Doppelanbindung, insbesondere für die Teilnehmerstandorte, die nicht an

Prof. Dr. Wilfried Juling, ehem. Direktor des SCC am KIT, ehem. Vorstandsvorsitzender des DFN: „Vom X.25-WiN über B-WiN und G-WiN zum X-WiN – von der steten Technologie- und Leistungsentwicklung des vom DFN betriebenen Wissenschaftsnetzes habe ich all die Jahre sehr profitiert, besonders hinsichtlich der nationalen und internationalen Integration des Hochleistungsrechnens. Nicht zu vergessen ist auch ERWiN, das für die schnelle Einbindung der Wissenschaft in den neuen Bundesländern extrem hilfreich war. Als Verwaltungsratsmitglied und Vorstandsvorsitzender des DFN durfte ich neun Jahre unmittelbar an der exzellenten Entwicklung des Deutschen Forschungsnetzes mitwirken. Dafür bin ich sehr dankbar!“

das Kernnetz angeschlossen waren, haben wir dieser erhöhten Abhängigkeit der wissenschaftlichen Einrichtungen Rechnung getragen und konnten damit eine zusätzliche Absicherung gegen Ausfall und Konnektivitätsverlust schaffen.

Die Idee der Doppelanbindung war also ein absoluter Gamechanger.

Das kann man so sagen. Letztendlich hat diese doppelte Anbindung eine langfristige Kundenbindung erzeugt und damit eben ganz hervorragend zur Lösung der Problematik der Fehlbedarfsfinanzierung beigetragen. Und es hat neben neuen Einrichtungen auch frühere Einrichtungen wieder ans Netz gebracht. Ich glaube, heute gibt es nur noch sehr wenige Wissenschaftsinstitutionen, die nicht in irgendeiner Form am X-WiN partizipieren.

In den Folgejahren haben wir die Doppelanbindung im X-WiN weiter ausgebaut. So konnte ab 2009 der Standardanschluss für DFNInternet mit einer doppelten Anbindung angeboten werden. Durch die extreme Komplexität der Planung und Realisierung, die die gesamte Architektur betraf, war das Projekt eine enorme Herausforderung. Es ging um weit mehr als nur um technische Aspekte: In die Ausschreibung, Risikobewertung und Kalkulation des Projekts sowie Konzeption des Betriebsmodells war letztendlich die gesamte Geschäftsstelle eingebunden. Hervorzuheben ist hier der enorme Kraftakt der Mitarbeiterinnen und Mitarbeiter, die dieses Großprojekt gestemmt haben. Da wurde Hervorragendes geleistet. Aus zwei Gründen ist die Doppelanbindung für mich ein echtes Highlight: die technische Komplexität und die Wirkung, die sie in der Mitglieder- und Teilnehmerschaft entfaltet hat.

> „Wir haben es geschafft, eduroam und die DFN-AAI zu flächendeckenden Standardservices auszurollen.“

Gab es andere Schlüsselfaktoren, die ähnliche Wirkung entfaltet haben?

Die eine Seite ist das Kernnetz und DFNInternet, quasi das Kerngeschäft. Dieses wird komplementiert durch sehr wichtige Zusatzdienste. Was ich als absoluten Meilenstein verbuche, ist, dass wir es geschafft haben, eduroam und die DFN-AAI zu communityweiten, flächendeckenden Standardservices ausgerollt zu haben – und zwar europaweit. Gerade wir in Baden-Württemberg setzen stark auf die DFN-AAI, was das Management und die Aussteuerung von wissenschaftlichen Kooperationen unserer Einrichtungen betrifft. Warum ist das für mich ein weiteres Highlight? Erstens sind eduroam und die AAI hochgradig wissenschaftsspezifische Dienste, die für Forschung und Lehre maßgeschneidert sind. Zweitens werden sie weitgehend eigenständig vom DFN-Verein implementiert und betrieben, inklusive umfangreicher eigener SW-Entwicklung.

Die DFN-AAI hatte damals noch einen weiteren Aspekt: Sie war ein Einstieg und der Grundstein für die Weiterentwicklung der Sicherheitsdienste im DFN. In den nachfolgenden Jahren hat sich die Relevanz dieses Dienstes für die teilnehmenden Einrichtungen immer deutlicher abgezeichnet. Der Dienst entfaltet nach wie vor enorme Wirkung.

Ist der DFN-Verein mit diesen Alleinstellungsmerkmalen und seinem maßgeschneiderten Netz konkurrenzlos?

Was den blanken Internetanschluss angeht, kann ich mich durchaus anderweitig versorgen. Mit dem Wissenschaftsnetz habe ich aber eine besonders sichere und zuverlässige Anbindung, die mir außerdem den direkten Übergang in andere Wissenschaftsnetze auf der ganzen Welt ermöglicht. Andere Anbieter verfügen weder über diese über Jahrzehnte gewachsene Vernetzung noch über dieses auf Wissenschaft und Lehre spezialisierte Branchen-Know-how, wie man in der freien Wirtschaft sagen würde. Aber es gibt auch Angebote im DFN-Verein mit einer geringeren Fertigungstiefe, die wir zukaufen und die darum einer gewissen Konkurrenz unterliegen.

Welche meinen Sie?

Wir führen das Interview gerade über die Videokonferenzsoftware Zoom, die sich gerade in der Coronapandemie durchgesetzt hat. Der DFN-eigene Dienst DFNconf wird heute nicht mehr breit genutzt, sondern insbesondere dann, wenn sichere, vertrauliche Gespräche notwendig sind. An diesem Beispiel sieht man aber auch gut, wozu der DFN-Verein in der Lage ist. Mit einer groß angelegten Ausschreibung

Prof. Dr. Hans-Joachim Bungartz, Dekan der TUM School of Computation, Information and Technology, TU München, ehem. Vorstandsvorsitzender des DFN: „Neun Jahre Vorstandsvorsitz in 40 Jahren DFN-Verein: Neben all dem uneingeschränkt Positiven, das sich zum DFN, seinem Tätigkeitsspektrum und seiner Organisationsform sagen lässt, bedeutet das für mich vor allem zahllose wertvolle Erinnerungen, weit mehr Harmonisches und Konstruktives als Dissens, und jeden Tag aufs Neue das Miteinander mit lieben und kompetenten Mitstreiterinnen und Mitstreitern. Die Zahl der Gremien, bei denen ich ein solches Resümee ziehen kann, ist überschaubar und wird überschaubar bleiben. Auch darin liegen Kraft, Erfolg und Nachhaltigkeit des DFN-Vereins begründet."

von Rahmenverträgen für hochskalierende, cloudbasierte Web- und Videokonferenzdienste hat der DFN-Verein dafür gesorgt, dass seine Teilnehmer deutschlandweit Angebote mit höchst attraktiven Konditionen wahrnehmen und sich den Aufwand eigener Ausschreibungen sparen konnten. Die wenigsten Bundesländer haben es geschafft, Zoom auf bestimmte Datenschutzkriterien zu verpflichten. Der DFN-Verein hat es geschafft. Auch das ist ein großer Erfolg.

Gibt es Anforderungen aus der Wissenschaft, die wir nicht bedienen können? Beispielsweise sagte ein HPC-Forscher in einem früheren Interview, dass er Daten noch ganz altmodisch teils auf Datenträgern von A nach B transportiert.

„Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway." Das Zitat stammt aus dem Fachbuch Computer Networks von Andrew S. Tanenbaum, der damit in den 80er-Jahren quasi die Bibel der Netzkommunizierenden geschrieben hat. Es gibt bis heute Anwendungen, beispielsweise im Bereich Archivierung, bei denen dieser Transport von Daten sinnvoll ist. Das ist in keiner Weise schädlich. Diese Limitierungen haben nichts mit dem Wissenschaftsnetz zu tun und resultieren weniger aus der im X-WiN möglichen Bandbreite. Diese können wir nämlich fast beliebig hochdrehen. Im internationalen Vergleich bewegen wir uns mit dem X-WiN schon an der Front aller möglichen Techniken.

Wie alles anfing im DFN, können Sie in der Ausgabe 95 ab S. 8 lesen: **www.dfn.de/wp-content/uploads/2024/01/DFN-Mitteilungen-95.pdf**

Welche Herausforderungen sehen Sie heute für Forschung und Lehre? Und was bedeutet das wiederum für den DFN?

Eine wesentliche Herausforderung für Einrichtungen besteht darin, dass sie immer größere Serviceportfolios benötigen, die sie technisch nicht selbst realisieren können. Das bedeutet letztendlich, dass sie diese durch Ausschreibungsverfahren, durch Einkauf und durch Partnermanagement beschaffen und sich darüber hinaus mit Zertifizierungsfragen oder Fragen der Compliance oder Informationssicherheit auseinandersetzen müssen. Und selbst das können insbesondere kleine Einrichtungen nicht immer leisten. Dafür brauchen sie starke, breit aufgestellte Partner wie den DFN-Verein. Das bedeutet für uns, dass wir uns mit immer umfangreicheren Anforderungen beschäftigen und unter Umständen unser Produktportfolio verbreitern müssen. Ich glaube, gerade für kleine Einrichtungen kann sich der Verein hervorragend positionieren, indem er das Portfolio integrierter anbietet, sodass diese sich das nicht einzeln zusammensuchen müssen.

Die Welt wird leider Gottes in den nächsten 20 Jahren nicht friedlicher. Wir werden das ganze Thema Resilienz und Informationssicherheit sehr viel stärker im Fokus haben. Hier hat der DFN die kleinen Einrichtungen schon sehr gut im Blick.

Was wünschen Sie dem DFN-Verein für die kommenden 40 Jahre?

Ich wünsche dem DFN-Verein, dass er die technischen und betrieblichen Entwicklungen sowie die steigenden Anforderungen aus Forschung und Lehre weiterhin hervorragend meistern wird und die wertvollen Vernetzungsstrukturen, die in 40 Jahren aufgebaut wurden, auch künftig Bestand haben. Sie sind die Basis und die Zukunftssicherung für den Verein. Das gilt noch viel mehr für die Menschen im DFN, die im Dienste der Wissenschaft jeden Tag dafür sorgen, dass Netz und Services einwandfrei funktionieren.

Ich bin zu Beginn in ein Umfeld gekommen, in dem ich auf sehr viele kompetente Menschen getroffen bin – ob in der Mitgliedergemeinschaft oder in der DFN-Geschäftsstelle. Ein Umfeld, in dem die Leute sich engagieren wollen und nicht müssen. Das prägt die Kultur und das Miteinander im Verein. Da ist sehr viel Freude im Spiel und Spaß an der Realisierung. Man trifft auf Gleichgesinnte. Ich freue mich, dass ich meinen Teil zu bestimmten Entwicklungen beitragen konnte. Ich habe das unheimlich gerne gemacht.

Ich wünsche dem DFN weiterhin ein so großartiges Engagement in der Mitgliederschaft, in der Geschäftsstelle und in der Geschäftsführung. Der Verein wird sich sicher auch in der Zukunft als wertvoll für die Wissenschaft erweisen – hoffentlich für die kommenden 40 Jahre.

Das Gespräch führte Maimona Id (DFN-Verein)

Mit Köpfchen – und DFN-MailSupport

Mit der schnelllebigen Entwicklung digitaler Kommunikation passen auch Angreifende ihre Phishing-Methoden stetig an. Waren die Angriffsmuster von Spam- und Phishing-Mails in der Vergangenheit eher zufallsbasiert, so werden schlecht gesicherte E-Mail-Accounts heute gezielt angegriffen. Gehirn oder Technik, sprich Gefahrenbewusstsein oder automatisierte Abwehrtools? Nur mit einem ganzheitlichen Ansatz, der verschiedene Methoden integriert, sowie einer gemeinsamen Weiterentwicklung des Dienstes DFN-MailSupport haben die teilnehmenden Einrichtungen im DFN-Verein die Nase vorn.

Text: **Michael Röder** (DFN-Verein)

Foto: Xavier MARCHANT/Adobe Stock

E-Mail-Verkehr ist ein integraler Bestandteil unserer täglichen Arbeitsabläufe. Für einige gehört das Aussortieren von unerwünschten E-Mails ebenfalls zum beruflichen Alltag – und damit auch das Risiko, welches mit diesen E-Mails einhergeht. Denn nicht jede schadhafte E-Mail kann zweifelsfrei als potenzielles Einfallstor eines Cyberangriffs identifiziert werden. Die Gründe dafür sind vielfältig. Teils werden technische Hilfsmittel nicht richtig eingesetzt. In anderen Fällen sind technische Maßnahmen schlicht nicht in der Lage, den Schadgehalt ohne Restrisiko zu bestimmen. Aber auch der Faktor Mensch ist gefragt: Um dessen Bedeutung im System hervorzuheben, wagen wir die folgende These: Sicherheitsvorfälle – oder zumindest deren verheerende Ausmaße – hätten abgeschwächt oder sogar verhindert werden können, wenn alle Beteiligten umfassend geschult wären und mit dem richtigen Risikobewusstsein gehandelt hätten.

Was macht unbedarfte E-Mail-Nutzung gefährlich?

Weit mehr als eine Maschine neigen wir Menschen zu Fehlern. Die häufigsten Ursachen für menschliche Fehler sind Stress, Unaufmerksamkeit, Fehlinterpretation als Folge von Risikounter- bzw. Selbstüberschätzung oder schlicht mangelndes (Fach-)Wissen.

> Bleiben die Hinweise auf Schadhaftigkeit unterhalb eines vergebenen Schwellenwertes, wird die E-Mail zugestellt.

Führen wir uns das folgende Szenario einmal vor Augen: Eine Person innerhalb eines Unternehmens findet eine E-Mail in ihrem Posteingang, die einen schadhaften Link enthält. Die Nachricht selbst durchlief bereits einige Spam- und Phishing-Filter, die schadhafte Elemente innerhalb der E-Mail erkannt haben. Bleiben die Hinweise auf Schadhaftigkeit unterhalb eines vergebenen Schwellenwertes – um zu vermeiden, dass versehentlich erwünschte Inhalte verworfen werden – wird die E-Mail zugestellt. Die empfangende Person wartet bereits dringend auf diese Nachricht, überfliegt sie, ordnet den Kontext falsch zu, erkennt vertraute Elemente (z. B. bekannte Empfängeradressen, Textpassagen, Kooperationspartner), und verlässt sich auf das üblicherweise zuverlässig funktionierende Mail-Abuse-Management.

Beim Klick auf den vermeintlich unbedenklichen Link wird auf dem Endgerät der Person eine Schadsoftware installiert, die sich über interne Ressourcen im Unternehmen verbreitet, Server attackiert und wichtige Daten entwendet und/oder verschlüsselt.

Sie halten das Szenario für unwahrscheinlich? Dann fragen Sie mal bei den Einrichtungen nach, die bereits von einem Sicherheitsvorfall betroffen waren. Das Gefahrenpotenzial ergibt sich aus der Gesamtmenge einfließender Faktoren, steigendem Stresslevel in einem zunehmend komplexer werdenden Arbeitsumfeld, besserer technischer (KI-)Möglichkeiten bei der Generierung von schadhaften Inhalten und nicht zuletzt aus dem zutiefst menschlichen Bedürfnis nach gegenseitigem Vertrauen.

Wie hat sich das Phishing-Szenario verändert?

Vor einigen Jahren noch waren die Angriffsmuster in Spam- und Phishing-Mails erratisch und zufallsbasiert, nach dem Motto: Generiere genügend Empfängeradressen und verteile diese über einen kurzerhand selbst betriebenen Mail-Versende-Server in der Cloud. Eine kleine Menge der Massen-E-Mails wird real existierende Empfänger erreichen. Eine noch kleinere Menge kann ihren maliziösen Inhalt durch Klicks, Downloads etc. entfalten.

Mit diesen Angriffsmethoden können wir aus heutiger Sicht gut umgehen, denn:

- Gefälschte Absenderadressen sind leicht zu erkennen, u. a. durch Mechanismen im Mail-Protokoll.
- One-Time-Mail-Versende-Server ohne Reputation können gut enttarnt werden.
  - Wer ein seriöser Absender ist, hat Zugriff auf eine Mail-Infrastruktur mit guter Reputation.
  - Und wer eine gute Reputation besitzt, setzt diese nicht leichtfertig aufs Spiel.
- Spam-Mail-Inhalte waren häufig sehr generisch und nicht auf die User zugeschnitten, bspw. dürfte der Erfolg der Prinzessin, die mehrere Millionen Dollar auf Ihr Konto überweisen möchte, heutzutage vernachlässigbar klein sein.

> Spammer greifen schlecht gesicherte, real existierende Postfächer großer Mail-Provider gezielt an.

Diese Methoden haben sich spätestens mit zunehmender digitaler Kommunikation und einsetzender Pandemie seit 2020 stark verändert.

Spammer greifen mittlerweile schlecht gesicherte, real existierende Postfächer großer Mail-Provider gezielt an und übernehmen sie – nach freundlicher Einladung infolge unsicherer Passwörter und/oder fehlender Multi-Faktor-Authentisierung (MFA). Sobald den Angreifenden Benutzername und Passwort vorliegen, können sie nicht nur auf die Inbox zugreifen, sondern erhalten ebenfalls Zugang zum Adressbuch der Postfachbesitzenden. Und damit ist noch nicht Schluss: Die Angreifenden können nun auch E-Mails von diesem Postfach und im Namen des Account-Inhabers versenden. Damit

Prof. Dr. Gerhard Peter, ehem. Rektor der Hochschule Heilbronn, Leiter der DFN-Mitgliederversammlung: „Vom ‚Verein ohne Netz' zu einer der leistungsfähigsten Hochgeschwindigkeitsinfrastrukturen weltweit: Der technische Fortschritt war rasant. Das erste Netz war noch ISO/OSI-basiert, Technologiebezüge wie X-25 und X-400 sind heute nahezu vergessen. Ich bin dankbar, dass ich seit 40 Jahren Teil dieser besonderen Geschichte bin und mich in mehreren Aufgabengebieten einbringen konnte – insbesondere bei der Leitung der Mitgliederversammlungen, die mir sehr viel Freude macht. Dem DFN-Verein wünsche ich, dass die künftige Entwicklung genauso erfolgreich und reibungslos wie in den vergangenen Jahren verläuft."

nutzen sie die gute Reputation des E-Mail-Providers, können beliebige Nachrichten aus dem Postausgang noch einmal an den ursprünglichen Empfängerkreis verteilen und den Inhalt nach Belieben editieren – zum Beispiel eine maliziöse URL einarbeiten. Den Empfangenden wird eine falsche Vertrauensstellung vorgegaukelt, denn sie erkennen sowohl die Absenderadresse als auch potenziell andere Empfangende und den Mail-Inhalt wieder. Ob Empfangende den Schadgehalt rechtzeitig erkennen, ist ein Zufallsspiel. Denn die URL kann sich in der formatierten Ansicht einer E-Mail als eine andere URL ausgeben.

Welche Mitigationsmöglichkeiten gibt es?

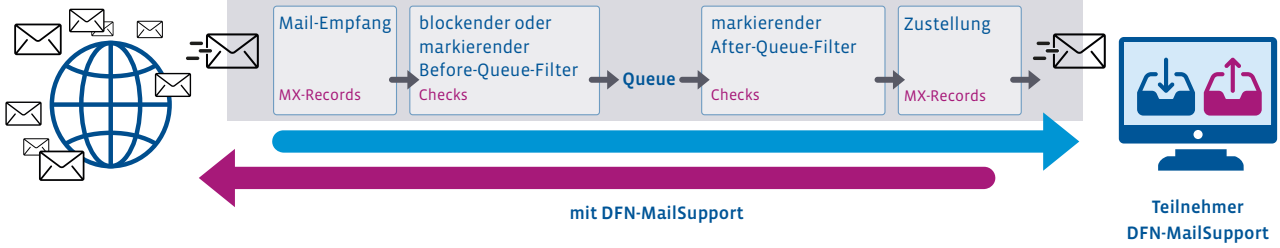
Neben allen technischen Werkzeugen hat jede individuell handelnde Person ein Gehirn. Und diese Ressource ist grundsätzlich allen technischen Möglichkeiten bei Weitem überlegen. Beides gemeinsam – das richtige Gefahrenbewusstsein in Verbindung mit effizienten Filtermaßnahmen – bilden den besten Schutz für das Unternehmen und dessen Ressourcen.

Es ist also unerlässlich, dass alle (!) Personen, die dem Gefahrenpotenzial von Spam-Mails ausgesetzt sind, über das notwendige Know-how im Umgang mit der Technologie und über Risikobewusstsein verfügen. Auf dem Gebiet der Schulungen und Trainings haben sich in der Vergangenheit einige hilfreiche Lösungen etabliert. Es gibt sowohl Schulungsmaßnahmen mit Ausbildenden vor Ort als auch voll automatisierte Schulungskonzepte als Webanwendungen. Die Anpassungsmöglichkeiten für individuelle Inhalte sowie Look & Feel sind vielfältig.

Für welche Variante Sie sich auch entscheiden: Bei der Auswahl sollten auch die

WIRKUNGSWEISE DFN-MAILSUPPORT

Die Einrichtung ist ohne DFN-MailSupport beim Abuse-Management ihrer E-Mails auf sich allein gestellt.



Die Mail-Gateways von DFN-MailSupport werden vor die eigenen Mail-Gateways der teilnehmenden Einrichtungen geschaltet – und können auf Wunsch zusätzlich zu eingehenden auch ausgehende E-Mails filtern.

Prof. Dr. Helmut Reiser, stellv. Leiter des LRZ, stellv. Vorstandsvorsitzender des DFN: „Der DFN-Verein betreibt mit dem X-WiN ein leistungsfähiges Datennetz, ergänzt um nützliche und fortschrittliche Dienste. Dieses bildet die Basis für das Münchner Wissenschaftsnetz des LRZ. Die Vereinsstruktur des DFN ermöglicht eine aktive Teilnahme der Mitglieder. So können wir zusammen maßgeschneiderte Lösungen für die Forschung entwickeln und schnell realisieren. Mit dem Ziel, der Wissenschaft zu dienen, sind wir gemeinsam stark und schlagkräftig."

Frequenz der Auffrischung sowie benutzergruppenorientierte Inhalte in die Entscheidung einfließen. Empfängerinnen und Empfänger von E-Mails sind die „last line of defense" in Ihrer Einrichtung – sorgen Sie dafür, dass sie gut gewappnet sind!

Welche weiteren Mitigationsmöglichkeiten gibt es außerdem im Wissenschaftsnetz?

Mit DFN-MailSupport bietet der DFN-Verein seinen teilnehmenden Einrichtungen ein Abuse-Management-System für ein- und ausgehende E-Mail-Nachrichten an. Der Dienst beinhaltet eine mehrstufige Filterarchitektur, die inhalts-, adress- und reputationsbasiert unerwünschte Mail-Inhalte erkennt. Entsprechend den Bedarfen der teilnehmenden Einrichtung können E-Mails die Filterstruktur ungehindert passieren und werden mit Header-Markierungen versehen oder deren Empfang wird abgelehnt und mit einem entsprechenden Hinweis gegenüber den Versendenden quittiert.

Die Infrastruktur für DFN-MailSupport wird an drei Standorten im X-WiN betrieben. Der Dienst wird im Rahmen eines Informationsverbundes erbracht, der einer Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz unterliegt.

Zusammenspiel mit DFN.Security

DFN-MailSupport wird aktiv, bevor die E-Mail im Postfach der Adressierten auftaucht. Ist die E-Mail einmal angekommen, sind die Nutzenden gefragt. Aber sie sind dabei nicht auf sich allein gestellt, denn der DFN-Verein bietet ein Dienstportfolio, das diensteübergreifend für Sicherheit im Wissenschaftsnetz sorgt.

> Mit DNS-RPZ stellt der Dienst DFN.Security einen Mechanismus bereit, der den Schadgehalt einer URL überprüft.

Mit DNS-RPZ (Domain Name System-Real Time Policy Zone) stellt der Dienst DFN.Security einen Mechanismus bereit, der zum Zeitpunkt des Klicks auf den Link den Schadgehalt einer URL überprüft und gegebenenfalls deren Aufruf unterbindet. Warum ist das notwendig?

„Liebe URL, bist du schädlich?" – „Vorhin noch nicht, jetzt schon!"

Spamversand vollzieht sich in Wellen. Generieren Spammer schadhafte E-Mails und verwenden dabei bisher nicht genutzte Techniken oder Link-URLs, benötigen die Filterlösungen eine gewisse Zeit, um den Schadgehalt zu ermitteln. Es ist das übliche Räuber- und Gendarmspiel, bei dem das Gute dem Bösen zwar schlussendlich auf die Schliche kommt – der Erfolg stellt sich aber üblicherweise mit etwas zeitlichem Versatz ein.

Was bedeutet das für unsere Spamfilter? Während die ersten E-Mails einer neuen Spamwelle mit hoher Wahrscheinlichkeit unbemerkt den Filter passieren können, werden die nächsten Wellen desselben Bedrohungsszenarios schon nach kurzer Zeit mit großer Zuverlässigkeit als schadhaft erkannt, entsprechend markiert und in den Postfächern der Einrichtungen in dafür vorgesehene Ordner einsortiert (meist „Posteingang" oder eben „Spamverdacht", „Werbung" o. Ä.). Trotzdem liegen die ersten E-Mails aus der neuen Spamwelle in den Postfächern, und zwar mit dem schadhaften Link – Sie erinnern sich an das Szenario zu Beginn? Die schadhafte URL würde nun von jeder URL-Blockliste sicher erkannt und die E-Mail markiert oder deren Empfang abgelehnt werden – nur leider wird die E-Mail kein zweites Mal bei den Filtern von DFN-MailSupport vorbeikommen. Und hier kommt die DNS-RPZ ins Spiel.

Der Mehrwert einer DNS-RPZ

Die DNS-RPZ wird in das Domain Name System der teilnehmenden Einrichtung integriert. Kurz erklärt: Das DNS löst alle Namensaufrufe wie bspw. www.dfn.de in Adressaufrufe im Internet auf. Diese Adressen sind meist eher maschinenlesbar. Bei jedem Aufruf einer URL aus dem internen Netz heraus wird das DNS der teilnehmenden Einrichtung also aktiv.

Da liegt es doch nahe, vor jedem Klick auf einen Link noch einmal nachzusehen, ob die aufgerufenen URL mittlerweile immer noch unbedenklich sind. Und genau das tut

Prof. Dr. Ulrike Tippe, Vizepräsidentin der Hochschulrektorenkonferenz (HRK), ständiger Gast im DFN-Verwaltungsrat: „In Sachen Informationssicherheit bzw. Cybersicherheit arbeiten wir gern mit dem DFN zusammen. Die Zusammenarbeit kommt auch in gemeinsam durchgeführten Sitzungen zum Ausdruck. Dabei schätzen wir besonders die rechtliche Expertise des DFN sowie die entsprechenden Beratungsangebote, auf die wir selbstverständlich verweisen. Auch im DFN-Verwaltungsrat wirke ich gern im Sinne dieser Zusammenarbeit mit."

DFN-MAILSUPPORT AUF EINEN BLICK
(Stand April 2024)

172 Teilnehmer
haben eine Dienstvereinbarung für DFN-MailSupport abgeschlossen.

97 Mio. E-Mails
prüft DFN-MailSupport im Schnitt pro Monat.

55 % aller eingehenden E-Mails
werden als schadhaft oder unerwünscht markiert.

21 % unerwünschter E-Mails
werden über RealTime-Blocklisten identifiziert.

die DNS-RPZ. Sie überprüft die URL unter Zuhilfenahme aktueller URL-Blocklisten und erlaubt den Nutzenden entweder deren Aufruf oder blendet bspw. eine Warnmeldung ein.

Einschränkungen der DNS-RPZ

Bei allem Grund zur Freude: Auch eine DNS-RPZ allein kann nicht die Allheilsbringerin sein. Sie funktioniert aktuell nur dann, wenn Nutzende sich in ihrer Heimateinrichtung befinden oder eine VPN-Verbindung ins interne Netz hergestellt haben. Öffentliche WLAN- oder mobile Datenverbindungen verwenden eigene DNS und verfügen sehr wahrscheinlich nicht über ein solches Feature. [siehe auch DFN-Mitteilungen „Kampf gegen Phishing – neue Abwehrkomponente in DFN.Security", C. Kahl]

> Auch eine DNS-RPZ allein kann nicht die Allheilsbringerin sein.

Gemeinsam weiterentwickeln

Seit mehr als zehn Jahren existiert der Dienst DFN-MailSupport und versorgt mittlerweile 172 Einrichtungen im Wissenschaftsnetz. Dabei übernimmt der Dienst eine Aufgabe, die in jeder Einrichtung zwingend erforderlich ist und gleichzeitig in der lokalen Umsetzung der Einrichtungen innerhalb der X-WiN-Teilnehmerlandschaft nur wenige Unterschiede aufweist.

Bei der Weiterentwicklung des Dienstes entfaltet sich ein weiterer Mehrwert der produktiv und kreativ zusammenarbeitenden DFN-Community: Die Einrichtungen, die sich im DFN-Verein organisieren, haben die Möglichkeit, den Dienst gemeinsam weiterzuentwickeln und an die Bedürfnisse ihres Wirkungskreises anzupassen. Zuletzt ist intensiv an der Neugestaltung der vertraglichen Grundlage für die Auftragsdatenverarbeitung gearbeitet worden. Mit zunehmender Anzahl von Diensten, die personenbezogene Daten verarbeiten, hat sich der DFN-Verein dazu entschlossen, ein entsprechendes Rahmenvertragswerk zu erarbeiten. Dieses neue Vertragswerk wird im Laufe des Jahres allen Einrichtungen zur Verfügung stehen, die am Dienst DFN-MailSupport teilnehmen. Und was passiert danach? Das hängt auch von Ihnen ab – bringen Sie sich gern ein! ◆

Bei Fragen und Anregungen zum Dienst DFN-MailSupport erreichen Sie uns unter: **mailsupport@dfn.de**

Erfolgreich verlängert – die DFNconf-Rahmenverträge

Mit der nun wirksam gewordenen Verlängerung der DFNconf-Rahmenverträge für cloudbasierte Web- und Videokonferenzdienste erhalten teilnehmende Einrichtungen Planungssicherheit weit über 2026 hinaus. Im Dialog mit den Rahmenvertragspartnern wird eine Weiterentwicklung der bestehenden Produkte entlang der Bedarfe der DFN-Community angestrebt.

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

Die im vergangenen Jahr mit allen Vertragspartnern erfolgreich vereinbarte Verlängerung der DFNconf-Rahmenverträge für cloudbasierte Web- und Videokonferenzdienste ist im März 2024 in Kraft getreten. Damit haben DFN-Teilnehmer nun die Möglichkeit, für weitere zwei Jahre Leistungen auf Grundlage von EVB-IT-Verträgen zu beauftragen. Das bedeutet ein hohes Maß an Planungssicherheit und Kostenstabilität. Die Laufzeit der sieben Rahmenverträge erstreckt sich bis März 2026. Die Beauftragungen via EVB-IT können jeweils einmal verlängert werden, bevor die EVB-IT-Verträge erneut ausgefüllt werden müssen. Praktisch sind so Nutzungsmöglichkeiten bis Anfang 2028 denkbar.

Die DFNconf-Rahmenverträge beinhalten folgende Produkte: Zoom X (Telekom Deutschland GmbH), Cisco Webex (Deutsche Telekom Business Solutions GmbH), BigBlueButton (infra.run GmbH), MS Teams (DrVis Software GmbH), Adobe Connect (reflact AG), OpenTalk (OpenTalk GmbH) und Class Collaborate (asknet Solutions AG).

Foto: Alena/Adobe Stock

Der mit den Anbietern erzielte Konsens ist keine Selbstverständlichkeit, denn nicht alle Vertragspartner können sich über eine große Nachfrage nach den von ihnen vertriebenen Produkten freuen. Mit der groß angelegten Ausschreibung der Rahmenverträge war ursprünglich das Ziel verbunden, den teilnehmenden Einrichtungen im Wissenschaftsnetz nicht nur ein umfangreiches Angebotsspektrum bieten zu können, sondern im gleichen Maße eine Nutzungsvielfalt zu erreichen. De facto reduziert sich die

Gisela Maiß, ehem. Mitarbeiterin im DFN: „Wir waren nicht unvorbereitet! Schon das Berliner Rechnernetz hatten wir – Klaus Ullmann, Martin Wilhelm, Renate Schroeder und ich – auf den Weg gebracht und nun hoben wir 1984 das DFN mit aus der Taufe. Mein Ding war die „Grafik in Netzen“ und es sollte über viele Jahre so bleiben bis zum heutigen Dienst DFNconf. Denn wie meine Kollegen schon damals wussten: Ein Bild sagt mehr als 1000 Worte. Und überhaupt die Kollegen – wir wuchsen zu einer coolen Gruppe heran, mit der die Arbeit Spaß machte!“

Nutzung auf wenige Produkte, obwohl alle Produkte die vom DFN gestellten Anforderungen vollständig erfüllen.

Verschiedene Weiterentwicklungen geplant

Eine Weiterentwicklung der bestehenden Produkte entlang der Bedarfe der DFN-Community zeichnet sich ab: So soll bei ZOOM X der Nutzwert der Software durch Softwareentwicklung und -zukauf gefördert werden. Ein Add-on ist beispielsweise „Zoom Events“, mit dem die Abwicklung virtuell oder hybrid

> Wichtige Themen sind Informationssicherheit und digitale Souveränität.

angelegter Veranstaltungen effizienter gestaltet werden kann. Weitere interessante Entwicklungen sind Funktionen wie „Studio“ oder „Clips“. Mit dem Add-on „Studio“ kann das Aussehen einer Konferenz nach Nutzerwünschen gestaltet werden. „Clips“ bietet die Möglichkeit, Bildschirmaufzeichnungen zu erstellen. In ihrer monatlichen „Open Hour“ stehen sowohl der Softwarelieferant als auch dessen Vertriebspartner Rede und Antwort.

Mit Cisco Webex konzentriert sich die Deutsche Telekom Business Solutions auf den direkten Kontakt mit Nutzerinnen und Nutzern und ist mit ihren zuständigen Ansprechpersonen regelmäßig auf relevanten Veranstaltungen unter anderem bei der DFN-Betriebstagung oder den Tagungen der ZKI (Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V.) vertreten. Das gilt auch für das Berliner Unternehmen infra.run Service GmbH, das den Cloud-Videodienst BigBlueButton (BBB) anbietet. Die Community der Open-Source-Software in den teilnehmenden Einrichtungen, die BigBlueButton in Eigenregie hosten oder sich direkt an der Weiterentwicklung beteiligen und dazu eigene Ressourcen einsetzen, ist sehr stark. Bei der im November 2023 in Berlin stattgefundenen Tagung Online Educa Berlin (OEB) wurde deutlich, dass BBB in seiner Roadmap bevorzugt KI-Unterstützung für Lehrende adressiert.

Von den vier anderen Rahmenvertragspartnern ist derzeit vor allem die asknet Solutions AG mit dem Produkt Class Virtual Classroom aktiv. Diese Software ist als Add-on zum Rahmenvertrag von Class Collaborate verfügbar und verspricht zielgerichtete Unterstützung insbesondere in Lehr- und Lernszenarien – hier im Bereich der Learning Analytics zwecks Leistungsbeurteilung der an einem Webinar teilnehmenden Personen. Class setzt auf Zoom auf und neuerdings auch auf Microsoft Teams, wodurch sich asknet zusätzliche Marktchancen erhofft. Dies spiegelt sich auch im regelmäßigen Angebot von Webinaren wider. Das Produkt Class wird im Rahmen der Messe Learntech und auf der OEB vorgestellt werden.

Den Rahmenvertrag zu Microsoft Teams hält die DrVis Software GmbH aus Garching, die als „First Tier Cloud Solutions Provider“ von Microsoft auftritt. Vorteile sieht die Anbieterin vor allem im Bereich der Informationssicherheit, die bei Microsoft – Stichwort Multi-Faktor-Authentisierung (MFA) – bereits mitgeliefert wird. Hinsichtlich der europäischen Datenschutz-Grundverordnung (DSGVO) sei dies ein wichtiges Thema. Ähnlich argumentiert die OpenTalk GmbH, die als einzige ihre eigene Software über die Rahmenverträge anbietet – neuerdings auch als Open-Source-Software über das Portal „Open CoDE“. Sie adressiert damit vor allem Anwendende aus dem öffentlichen Sektor mit besonderen Anforderungen an digitale Souveränität.

Die reflact AG (Oberhausen) ist mit ihrem Produkt Adobe Connect, das kürzlich ein Versionsupdate erfahren hat, regelmäßig auf der Learntec präsent. Das Unternehmen vermarktet die Software im DFN-Kontext mit den Attributen flexibel, interaktiv und gut integrierbar als „Virtuelle Lehre 2.0“ und setzt auf didaktische Funktionen als Alleinstellungsmerkmal.

Für den DFN-Verein wird es spätestens ab dem zweiten Quartal 2025 wieder spannend in Sachen DFN-Rahmenverträge für cloudbasierte Web- und Videokonferenzdienste. Sofern es dem Wunsch der Vereinsmitglieder entspricht, wird es zu einer Neuausschreibung kommen, um die auslaufenden Rahmenverträge ab 2026 mit einem Nachfolgeformat zu erneuern. ◆

Bei allen Fragen rund um die DFNconf-Rahmenverträge wenden Sie sich bitte per E-Mail an: **vertraege@conf.dfn.de**

Informationen zum Dienst DFNconf finden Sie unter: **www.conf.dfn.de**

Kurzmeldungen

Vier Millionen abgegebene Stimmen im DFNTerminplaner

Kleine Wasserstandsmeldung: Der Terminplaner (Version 6) hat die 4-Millionen-Marke bei den abgegebenen Stimmen der laufenden Umfragen weit überschritten. Dazu haben wir 500 000 Terminabstimmungen gezählt, rund 27 000 Buchungslisten und fast 4 400 Umfragen. Pro Monat versendet das System inzwischen mehr als 200 000 E-Mails. Die aktuellen Zahlen sind eine tolle Motivation für uns, den DFNTerminplaner stetig weiterzuentwickeln. Derzeit arbeiten wir mit Hochdruck an der AAI-Anbindung des Terminplaners. Wir halten Sie auf dem Laufenden. ◆

Zum DFNTerminplaner geht es hier:
https://terminplaner6.dfn.de

OCRE 2024: Auswertung der Angebote für Cloud-Rahmenverträge gestartet

Im Rahmen des GÉANT-Projekts GN5-1 konnten sich bis Mitte Mai 2024 Anbieter kommerzieller Cloud-Dienste auf das EU-weite Vergabeverfahren für die Beschaffung in OCRE 2024 (Open Clouds for Research Environments) bewerben. Der Leistungsumfang der Neuausschreibung konzentriert sich auf Cloud-Services aus den Bereichen IaaS+ (Infrastructure as a Service). Das beinhaltet Dateninfrastrukturen, Plattformen und Dienste für Künstliche Intelligenz (KI), maschinelles Lernen, Container-Entwicklungsumgebungen bis hin zu Erdbeobachtungsdiensten. Das Plus bezieht sich auf Mehrwertdienste wie Beratungsleistungen und Unterstützungsangebote beim Einstieg, Umstieg und Ausstieg zu Cloud-Diensten.

Ein internationales Team von Cloud-Verantwortlichen aus den verschiedenen europäischen Forschungsnetzen, in dem auch Kollegen aus dem DFN-Verein mitwirken, arbeitet nun an der Sichtung, Bearbeitung und Evaluierung der eingegangenen Angebote. Mit einer Beitrittserklärung ist der DFN-Verein offiziell am Verfahren beteiligt. Bereits 2023 und Anfang 2024 führte der DFN verschiedene Workshops und Webinare durch, um gemeinsam mit teilnehmenden Einrichtungen die Anforderungen der Wissenschaftscommunity in Deutschland zu erheben und zu analysieren. Im Anschluss wurden die Ergebnisse dieses Prozesses und das weitere Vorgehen mit GÉANT abgeglichen.

Ab Dezember 2024 stehen die neuen Verträge mit einer Laufzeit von fünf Jahren zur Verfügung und knüpfen nahtlos an die aktuellen Verträge an. ◆

Informationen zur DFN-Cloud erhalten Sie unter:
www.dfn.de/dienste/cloud

Für die Forschungsgemeinschaft entwickelt: Webkonferenzen mit eduMEET

Unter dem Dach der GÉANT Association betreiben und entwickeln die europäischen Nationalen Forschungsnetze (National Research and Education Networks, NRENs), zu denen auch der DFN-Verein gehört, eine gemeinsame Kommunikationsinfrastruktur für Forschung und Lehre, bestehend aus Netz und IT-Diensten. Dazu gehört auch die WebRTC-basierte Videokonferenzsoftware eduMEET, die auf die Anforderungen der Wissenschaftscommunity zugeschnitten ist. Im Gegensatz zu vielen kommerziellen Produkten ist eduMEET vollständig quelloffen sowie Open Source-lizenziert und kann so von der Community weiterentwickelt werden. Bei einigen NRENs ist der Videodienst bereits im Einsatz.

Im Rahmen einer Workshopreihe zum Videokonferenzdienst prüft der DFN-Verein in Deutschland nun gemeinsam mit teilnehmenden Einrichtungen mögliche Nutzungs- und Einsatzszenarien. Ziel der Veranstaltungen ist es, neben administrativen Aspekten auch die Möglichkeiten und Grenzen der Software in Lehr- und Lernsituationen zu untersuchen. Die jeweiligen Erkenntnisse werden dabei mit den Anforderungen an ein Betriebskonzept abgeglichen, um zu einem möglichst umfassenden Gesamtbild der Software zu gelangen.

Positiv bewertet wurde in der Auftaktveranstaltung die runderneuerte Softwarearchitektur. Die Modularisierung sorgt bei Installationen on-prem oder im föderierten Einsatz dafür, dass Einrichtungen mit dezentralen Standorten ihre Netzlast bzw. den Datentransfer durch Durchgangsnetze optimieren können und dass außerdem ein hohes Maß an Ausfallsicherheit erreicht wird. Eine andere Diskussion hatte die Frage zum Inhalt, ob eduMEET auch als Entwicklungsumgebung für KI-Anwendungen Einsatz finden könnte, um entsprechende Funktionen anwendungsnah und realistisch zu erproben. Darüber hinaus stieß die Möglichkeit, ultrahochauflösende Videoformate – sogenanntes 4K-Video – verarbeiten zu können, auf Interesse. Die Ergebnisse der Workshopreihe werden Ende 2024 beim Administratoren-Workshop des Kompe-

Dr. Andreas Vogel, von 1984 - 2000 zuständiger Referent im Bundesministerium für Bildung und Forschung (BMBF): „Bereits in den 80er-Jahren – noch unter den Beschränkungen des Postmonopols – schuf der DFN-Verein nicht nur eine leistungsfähige Kommunikationsinfrastruktur für die Wissenschaft in Deutschland, sondern prägte auch die europäische Wissenschaftskommunikation maßgeblich mit. Zugleich wurde das Deutsche Forschungsnetz als nationales Projekt zum Vorreiter und Modell wissenschaftlicher Selbstorganisation über die föderalen Grenzen hinweg – auch für andere Bereiche der Wissenschaft."

tenzzentrums für Videokonferenzdienste (VCC) in Dresden vorgestellt. ◆

Weitere Informationen zu eduMEET gibt es unter: **https://edumeet.org/**

Vergabeverfahren für Teilnehmeranbindungen an das DFN-Kernnetz beendet

Mit dem erfolgreichen Abschluss des europaweiten Vergabeverfahrens für Teilnehmeranbindungen (TNA) wurde ein wichtiger Meilenstein auf dem Weg zum „Fitmachen" des Wissenschaftsnetzes für die Zukunft erreicht. Erstmals wurden im Wettbewerb Bandbreiten von 100 Gbit/s für diese Anbindungsart abgefragt. Aber auch die „Brot und Butter"-Kategorien von 1 Gbit/s und 10 Gbit/s zur einfachen oder redundanten Anbindung von Teilnehmerstandorten waren Teil des Verfahrens.

Nach gründlicher Auswertung der Angebote wurden Zuschläge an 15 Carrier erteilt, mit denen Rahmenverträge zur Bereitstellung und Überlassung von Teilnehmeranbindungen abgeschlossen wurden. Im Ergebnis wurde eine vollständige Abdeckung aller abgefragten Teilnehmerstandorte mit entsprechend zuschlagsfähigen Angeboten erreicht. Darüber hinaus – und nicht weniger wichtig – wurde eine signifikante Kostenreduktion für den größten Ausgabeposten im Haushalt des DFN-Vereins erzielt. Dieses nach Jahren hoher Inflationsraten nicht selbstverständliche Resultat gibt Sicherheit für eine solide und tragfähige Weiterentwicklung des Wissenschaftsnetzes und des Dienstes DFNInternet.

Die Planung zur Umsetzung der Ergebnisse ist bereits in vollem Gange, sodass die Beauftragung der Carrier zeitnah erfolgen kann. Teilnehmer, bei deren Anbindungen Änderungen notwendig sind, werden wie gewohnt rechtzeitig informiert. ◆

Weitere Informationen zum Wissenschaftsnetz finden Sie unter: **www.dfn.de/netz**

Volumendaten im Teilnehmerportal einsehbar

Auf einen Blick: Mit dem neuesten Release im Teilnehmerportal des DFN-Vereins können Nutzende nun zusätzlich zur Auslastung der eigenen Zugangsverbindungen auch die Volumendaten ihres DFNInternet-Anschlusses überwachen. Die neue Funktion zeigt an, wie viele Daten – sowohl eingehende als auch ausgehende – in einem definierten Zeitraum übertragen wurden. Das gilt für alle Regel-, Versorger- und Clusteranschlüsse in der Variante „VLAN (Virtual Local Area Network) pro Dienst". Eine Ausnahme bildet das Modell „VLAN für alle", für das eine Anzeige nicht möglich ist.

Auf Wunsch unterstützen die Kolleginnen und Kollegen des DFN-NOC Sie gerne bei einem Wechsel des Modells: noc@noc.dfn.de

Kompakt und übersichtlich: Neben sämtlichen Stammdaten, technischen Parametern und Informationen zur Teilnehmeranbindung wie Übertragungskapazität, verwendete Schnittstellen und Installationsorte etc. bietet das Teilnehmerportal weitere Funktionen an. Neben Diensten wie DFNInternet und DFN.Security können Nutzende auch externe DFN-Cloud-Dienste oder IP-Adressen einfach und direkt beantragen und sich über abgeschlossene und angekündigte Wartungen informieren sowie eigene ankündigen. Darüber hinaus besteht die Möglichkeit, sich mit dem DFN-Netzüberwacher zu verbinden. Neue Tickets lassen sich über das Teilnehmerportal schnell und komfortabel eröffnen und nachverfolgen. ◆

Neugierig geworden? Bei allen Fragen zum Teilnehmerportal beraten wir Sie gerne per E-Mail unter **teilnehmerportal@dfn.de** oder telefonisch unter **030 884299-9137**

Informationen zum Dienst DFNInternet finden Sie unter: **www.dfn.de/dienste/network-and-communication-services/**

THE FIELD

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

Satellites and Ships: Researchers Combine Data Sources to Study Arctic Warming

The multidisciplinary German consortium (AC)³ is focused on understanding what drives warming in the arctic. Scientists and engineers from across the country rely on DFN's X-WiN national research and education network to access and organize data from far-flung remote sensing instruments and to efficiently share insights in pursuit of better understanding the precious, rapidly changing arctic.

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

Researchers journey to the arctic on *Polarstern* to better understand how and why sea ice is melting away | *Photo: Gunnar Spreen*

Prof. Dr. Joachim Mnich, Direktor für Forschung und Computing am CERN, ehem. Mitglied im DFN-Verwaltungsrat: „Ich hatte die Ehre, die Entwicklung des DFN neun Jahre lang als Mitglied des Verwaltungsrates aus nächster Nähe zu begleiten. Für einen Teilchenphysiker wie mich, der ja sehr große Mengen wissenschaftlicher Daten in großen Kollaborationen produziert und auswertet, ist eine sehr enge nationale und internationale Vernetzung unabkömmlich. Die bedeutende Rolle, die der DFN auf dieser Ebene innehat, kann meines Erachtens nicht überschätzt werden. Deshalb wünsche ich dem DFN auch für die nächsten Jahrzehnte viel Erfolg!“

In the late 1800s, scientists studying the arctic began hypothesizing that the increase in carbon emissions corresponding to rapid, global industrialization could be influencing the Earth's climate. In recent decades, technological advancements such as high-altitude aircraft, satellites, and high-speed networks provided new tools for researchers measuring small-scale changes to the arctic that could have major implications for the long-term climate health of our planet.

These tools help scientists keep track of the arctic's seasonal and annual changes in ice thickness, temperature, and concentrations of particulate matter and other pollutants in the atmosphere. Unfortunately, the data is painting an increasingly dreary picture: the world's largest climate consortium, the Intergovernmental Panel on Climate Change (IPCC), an international body headquartered in Geneva, Switzerland, has unequivocally stated that since detailed studies began in the 1970s, the Earth has been warming at an accelerated rate, and that the rate is at least double as fast in the arctic as it is near the equator. This phenomenon is known as arctic amplification.

In the interest of better understanding what is driving accelerated arctic warming, a multi-disciplinary, multi-institutional team of researchers in Germany in 2016 received funding from the German Research Foundation (DFG) for a project titled, “Arctic Amplification: Climate-Relevant Atmospheric and Surface Processes and Feedback Mechanisms,” or simply (AC)³. Headquartered at the University of Leipzig with principal investigators from that institution, the University of Bremen, and the University of Cologne, the project brings together climate scientists, oceanographers, atmospheric scientists, information technology specialists, and others to understand the main factors driving these changes.

“We all focus on covering different aspects of what is needed to understand what is driving these changes,” said Dr. Gunnar Spreen, (AC)3 vice-speaker and researcher at the University of Bremen and a principal investigator on (AC)3 subprojects focused on studying sea ice changes. “Here in Bremen, we are known for a focus on remote sensing satellite data. Each institution has its specialties that it brings to the consortium.”

Now in the project's third and final phase, Spreen and his collaborators are focused on translating a massive trove of data coming from these different sources to better understand the processes causing this accelerated behavior compared to other parts of the world.

Data convergence determines arctic amplification drivers

Much of Spreen's research focuses on using data from research ships and aircrafts to get a clearer understanding of data coming from satellites. In fact, in 2019-2020, he was aboard the research vessel Polarstern – operated by the Alfred Wegener Institute, one of the (AC)³ project partners – for 5 months as part of the year-long MOSAiC ice drift expedition. “Gathering close-up data from ships helps us understand and interpret our satellite data better,” he said.

In (AC)³, his group is focused on understanding how certain feedback loops can compound sea ice melt. Among other topics of interest, the team has focused in recent years on surface albedo effects, or how the light reflects or absorbs on different surfaces and how that can indirectly increase ice melting.

During the project's second phase that just recently ended, the team used data coming from instruments on board Polarstern, aircraft recording high-resolution videos of the arctic, and satellite imagery measuring temperature, radiation, pollutants present, and many other data points to see where and when albedo effects play the strongest role in accelerating sea ice melt. The team found that warming did not purely correspond to seasonal effects – it did not uniformly melt faster as the arctic transitioned from spring to summer – but were heavily influenced more by pools of melted ice forming on the ice surface, called melt ponds.

When ice is thick and largely snow covered, the abundance of white reflects most light hitting the ice surface. When puddles start to form, though, they create darker patches along the ice that absorb more light, which generates more heat,

From measuring sea ice thickness to taking sensitive samples to collect data during arctic expeditions, researchers like Spreen (center right image, middle, next to his colleagues Lena Buth and Andreas Walbröl) use a combination of observations from satellites and computer modelling to paint a vivid picture of sea ice changes in the arctic.

Photos: Gunnar Spreen

Prof. Dr. Dr. Thomas Lippert, Direktor des Jülich Supercomputing Centre (JSC): „Als langjähriges Mitglied gratuliert das Forschungszentrum Jülich dem DFN-Verein zum 40-jährigen Bestehen und bedankt sich für die allzeit zuverlässige Zusammenarbeit bei Standarddiensten und gemeinsamen wissenschaftlichen Projekten sowie der Unterstützung bei Spezialanforderungen zum Beispiel des vom JSC betriebenen europäischen DEISA-/PRACE-Backbones. Dass der DFN über Jahrzehnte ein Forschungsnetz und flankierende Dienste auf höchstem Niveau betreibt und weiterentwickelt, ist ein herausragendes Beispiel dafür, was die deutsche Wissenschafts- und Forschungslandschaft gemeinsam erreichen kann. Wir wünschen dem DFN weiterhin eine glückliche Hand bei diesen Aufgaben."

which melts more ice and ultimately creates more puddles – the textbook definition of a positive feedback loop contributing to sea ice melt in summer.

Spreen noted that melt ponds play a nuanced but significant role in driving arctic warming, and by furthering our understanding of this process, the consortium creates its own positive feedback loop of sorts: many climate simulations run by computational climate scientists calculate sea ice changes as largely seasonally driven phenomena, and his team's work helps improve these researchers' models for more accurate simulations of future climate scenarios.

Research and education networks help enable large consortia

(AC)³ consists of 22 scientific projects across five different research clusters, but a sixth cluster is focused on one of the biggest challenges for the project: managing, moving, securing, sharing, and organizing terabytes worth of data.

"The greater project has consistently had more than 20 scientific sub-projects, and many of them have multiple principal investigators that are at different institutions. It is a very interconnected project," said Dr. Matthias Buschmann, researcher at the University of Bremen and principal investigator on the "INF" subproject dedicated to the project's data management needs.

Buschmann's team not only ensures that data is accessible to researchers across the wider consortium, but also that data is being managed according to the so-called "FAIR" principles of data management – that the data are findable, accessible, interoperable and reusable. He credited the German Research Network's (DFN's) X-WiN national research and education network for enabling high-speed data movement between institutions but gave his highest praise to the network's reliability. "It is at the point where most people in the project don't have to think about sending or receiving data, and that is exactly what you want from infrastructure – you should not need to think about it and whether it works or not," he said.

Buschmann noted that while some sub-projects have minor data management needs, satellites taking daily snapshots of a large geographic region or airplanes taking hours of video footage generate massive amounts of data that needs to not only move efficiently from one point to another, but also need to be strategically managed to avoid moving large volumes of data more than necessary. The INF team develops proactive strategies to minimize superfluous data movement and ensure efficient data retrieval and access for the research teams.

As part of the greater (AC)³ project, Buschmann sees his group's role not only as helping researchers efficiently move and manage large datasets, but also ensuring the long-term archival of data recorded by the consortium, making them accessible to subsequent research teams interested in arctic amplification research. For Spreen, the wealth of data collected during the 12-year project is its greatest achievement. "The legacy that we want to leave with this project is the data," he said. "In following these FAIR principles of data management, we are making sure that this data is well documented and accessible for others. In doing this part well, we make the work easier for my group and everyone else." ◆

MORE INFORMATION:

Arctic Amplification websiteProject:
www.ac3-tr.de

IPCC Sixth Assessment Report, Working Group III:
www.ipcc.ch/report/ar6/wg3/

AMS Journals: Atmospheric and Surface Processes, and Feedback Mechanisms Determining Arctic Amplification: A Review of First Results and Prospects of the (AC)³
https://journals.ametsoc.org/view/journals/bams/104/1/BAMS-D-21-0218.1.xml

THE FIELD

Building a Town Square for NRENs

In 2015, CEOs of various national research and education networks (NRENs) around the globe came together with a desire to raise awareness about the impacts NRENS have on their nations' respective research communities. Australia's NREN AARNet supported developing a website that would showcase research highlights and other innovative achievements enabled by NRENs globally. AARNet's Jane Gifford was inspired to model the site after the popular blog, Humans of New York, to give voice to the diverse perspectives of NRENs in different countries.

Jane Gifford, Director Marketing and Communications at AARNet, Australia's Academic and Research Network.
She is leading the In The Field blog project bringing to life a global collaboration platform for showcasing stories about inspiring people & projects enabled by the world's 120+ NRENs.
She has worked in Australia and internationally including a. o. BBCTV, the University of New England, British Vogue, Vogue Australia and Architectural Digest | *Foto: Benny Capp*

What was your motivation for getting this blog going, and how were you able to get so many NRENs to participate?

A global outlook and the ability to overcome the tyranny of distance of Australia's geographical location by connecting our researchers and educators to the rest of the world is fundamental to AARNet's existence. Being a globally focused organization has always been part of our philosophy. In 2014, members of the Global NREN CEO Forum asked their respective communications staff to collaborate and produce a series of case studies that highlight the importance of global connectivity to governments, funding agencies and other stakeholders.

After we produced a couple of case studies, I started thinking, "we should just do a website," because I was comfortable managing that and knew it would have more reach than sending out individual PDFs of case studies, and we could include a greater variety of stories and topics. I wanted this to be a grassroot

Prof. Dr. Dieter Kranzlmüller, Vorsitzender des Direktoriums des LRZ, Mitglied im Strategischen Beirat des DFN: „40 Jahre DFN-Verein – das sind vier Jahrzehnte vertrauensvolle Zusammenarbeit und gegenseitige Inspiration zwischen DFN und Leibniz-Rechenzentrum. Gemeinsam machen wir uns stark für eine exzellente, nützliche IT-Infrastruktur für Wissenschaft und Forschung, außerdem für Sicherheit und Zuverlässigkeit der IT-Dienste. Herzlichen Glückwunsch aus Garching – wir freuen uns schon auf die nächsten 40 Jahre und viele gemeinsame IT-Projekte!“

communications initiative, so I pitched it to several NRENs, including GÉANT (the pan-European network) and its MarComms special interest group whose members are from all around the world. Everyone thought it was an excellent idea and wanted to participate. The Global CEO Forum CEOs endorsed it and the contributions came rolling in from NRENs in Europe, Latin America, North America, Africa and the Asia Pacific. In fact, we had more than 100 stories on the blog within a couple of months, and the site quickly outgrew what it was initially envisioned to do, so we rebuilt it a couple of years later into what it is today. We've been able to keep up external engagement because we designed it as a tool for NRENs across the globe to use as they need to. Whether it is technical staff, a communications person at an NREN, or the CEOs themselves, they have a place to find and tell stories about the global nature of NRENs.

Why do you feel it is important for NRENs to have a space like this? What added value do you think In the Field brings to NRENs? What about more general readers outside the industry?

There isn't a one-size-fits-all answer for the larger community. For instance, it is a useful tool for emerging NRENs, because they often do not have a full communications staff to support them. In many cases, they are just beginning to talk to their governments about setting up their network, and they can use stories on the blog as a way to point to innovations happening elsewhere to show what is possible. But staff at established NRENs also regularly send me feedback about its value in providing supporting materials when they are talking to key stakeholders and funding agencies. While we do not consider the general public our target audience, we publish these stories so that if they come by the site, they can learn a little more about what a research and education nework does and how it connects to research in their home region and globally.

How have you been able to maintain a consistent tone for blog when it is coming from so many different places? What do you consider the biggest success of In the Field to date?

At the beginning, I agonized a lot over editing, and tried to focus the bulk of the stories on the people benefitting from a technology rather than the technology behind it. Not only was that labor-intensive for me, it also did not cover the full range of NRENs' communications needs. I might choose to do some light rewriting to focus on the outcome a little more. We are also proactive – we will seek out content from the NRENs' own websites and put together short summaries to post on the blog and share that with them, and they appreciate that.

As for measuring success, I think one of the biggest achievements with In the Field is that it serves as a true example of collaboration. Both technical staff and communications and marketing employees from many NRENs have been involved in contributing and promoting content for the site. And that collaboration is truly global, which demonstrates the true global nature of collaboration between NRENs. We've highlighted interesting news around 109 NRENs across about 450 articles, and many of those articles are timeless—they are as interesting now as they were when they were first published because often, they are talking about large scientific projects that run over a long period of time. Our site's articles show the breadth of activities NRENs are involved in and the value they provide for research and education sector and society more broadly. It is a great place to show what we all do in a meaningful way.

Interview by Eric Gedenk

THE FIELD

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

International Newsflashes

CANARIE, ESnet, GÉANT, and Internet2 Unveil Highest Capacity Transoceanic Connectivity for Research and Education

Internet2, in a joint effort with CANARIE, the Energy Sciences Network (ESnet), and GÉANT, announced today a major expansion to 400 gigabit-per-second (Gbps) transoceanic circuit capacity dedicated to transferring research and education (R&E) data. As part of the Advanced North Atlantic (ANA) collaboration, this marks a significant achievement in high-speed connectivity between North America and Europe, supporting data-intensive science globally.

ANA's network expansion supports multinational, data-intensive science collaborations, including the Large Hadron Collider (LHC), the world's largest and most powerful particle accelerator, and the Square Kilometer Array (SKA), the ongoing effort to build the world's largest radio astronomy observatory. It adds much-needed capacity for transmitting instrument findings to researchers globally, enabling ground-breaking discoveries. The joint effort adds three 400 Gbps spectrum circuits between exchange points in the U.S., U.K., and France. The new connections utilize the record-breaking 400 terabits per second (Tbps) trans-Atlantic Amitié subsea cable system completed in July 2023, which spans 6,783 kilometers (4,215 miles). ◆

GÉANT Boosts Trans-Mediterranean R&E Connectivity with €40 Million Agreement for MEDUSA Submarine Cable

Representatives of GÉANT recently signed an agreement for delivering the "MEDUSA" Submarine Cable Project, an ambitious project aimed at connecting North Africa and the European Union with a high-capacity fiber optic submarine cable system. The entire project is set to cost €342 million, with €40 million specifically earmarked for research and education collaborations between the regions.

MEDUSA is the European Commission's first digital "Global Gateway" project. The agreement signing marks an important step for implementing MEDUSA, and follows the initial announcement in November, 2022 and a Contribution Agreement signed between the European Commission and the European Investment Bank.

GÉANT's involvement in MEDUSA will build on the experience of the successful BELLA programme, the pathfinder initiative that co-funded the EllaLink submarine cable and directly connected Europe and Latin America for the first time. ◆

For more information, read the full releases on Connect online:
https://connect.geant.org/

Twinning is back

In the 1990s, DFN launched a partnership programme with the Kenyan national research and education network (NREN), KENET. Over the years, the programme included several mutual visits and active support in building the NREN infrastructure in Kenya. This so-called "twinning" arrangement provided advanced capacity, ultimately building opportunities for KENET engineers while also promoting joint research.

While the DFN-KENET activities have declined in recent years, the idea is now being revived in the form of GÉANT's NREN Twinning Programme, under coordination by DFN. The initiative began in the summer of 2023 at the TNC conference in Trieste based on a request from CEOs at the conference's CEO session. As a result, participating centers quickly produced a candidate list and agreed on a project framework. The new phase of the GÉANT Twinning Programme started with two partnerships: MAREN, the Malawian NREN, and ASNET-AM, the Armenian NREN, formed the first team. SIKT, the Norwegian NREN, and RENU, the NREN from Uganda, formed the second team. These initial projects were planned to last six months. Although no budget was initially earmarked for the pilot projects, it soon became clear that at least a minimal budget for mutual visits was necessary to establish a good relationship between the partners. The pilot projects made good progress and have now submitted their final reports.

The collaboration between SIKT and RENU focused on deploying Campus Network Management as a Service (CNMAS). The service was successfully introduced in Uganda and is now expanding RENU's

Jacqueline Struyken, Mitarbeiterin im DFN: „Im Forschungsumfeld kennt man sich! Die Dienste des DFN gehören für mich seit mehr als 15 Jahren zum Arbeitsalltag. Und seit dem letzten Jahr gehöre ich zum DFN-Verein und freue mich, jetzt aktiv mitwirken zu können. Den Einstieg haben mir die Kolleginnen und Kollegen leicht gemacht und mich sehr herzlich aufgenommen. Mit Rat und Tat stehen sie mir immer zur Seite. Hier lassen sich kleine Probleme schnell lösen und Großes umsetzen!“

service portfolio, with the first users already utilising the new service. The second pairing focused on topics such as high-performance computing (HPC), the next-generation internet protocol, IPV6, and marketing and communications (MarComms). Both partners, ASNET and MAREN, have recently acquired an HPC system and exchanged experiences in using this new resource. Conducting training sessions on topics related to MarComms was the predominant activity. There will be a lightning talk about this twinning pilot project at TNC 2024.

The GEANT Twinning Programme will continue during the next GEANT project phase, GN5-2. There is already a waiting list of interested candidates. The aim is to broaden the scope and focus not only on twinning partnerships with African NRENs, but also to invite emerging NRENs from other parts of the world, such as from Latin America or Asian countries. ◆

DFN attends the EuroHPC Summit 2024

This year’s EuroHPC Summit Week took place in Antwerp, Belgium. The annual conferences aim to bring together key stakeholders in European supercomputing, including representatives from the public and private sectors and policymakers from the European Union and national governments.

The summit provides an opportunity for European high-performance computing (HPC) enthusiasts to share the latest technological advances, foster collaboration, identify current and future needs in European HPC space – ultimately helping shape the development of European supercomputing. This year's summit attracted over 700 participants from 45 different countries.

In addition to core HPC topics, the conference program also focused on emergent technologies like artificial intelligence (AI) and quantum computing, as well as chip production in Europe. AI was a particularly hot topic, as the European Commission recently unveiled a plan to create 'AI factories' across the EU. The plan would provide AI start-ups access to supercomputers to develop their own models rather than relying on models developed by US tech giants.

Discussions continue about changing the EuroHPC mandate to have a stronger AI focus. The plans surrounding European AI factories in Europe is still being finalized, including deciding whether individual factories will have specific thematic focuses.

At the conference, EuroHPC representatives presented a new, separate category for AI projects in the peer review process. By having their own peer review process, reviews will be able to better compare AI projects with each other and better organise the application process, currently designed primarily to serve classical-computing-focused scientific projects for academic and industrial users.

Participants also focused on quantum computing at the summit. The EuroHPC JU will procure at least two quantum computers in 2024 with a total EU contribution of €20 million. The quantum computers will be integrated into existing supercomputers operated by select host institutions. EuroHPC leadership have already developed a selection process that ensures technological and architectural diversity so that users have access to different types of quantum systems.

Overall, the summit was a lively conference with a series of panel discussions that also engaged with the audiences. The Summit Week was not a "user conference," as such—there was only one session that focused on examples of what can be achieved in science and research with HPC. There is a tendency, however, to revise the concept of the conference to include more user-orientated sessions. ◆

More information:
www.eurohpcsummit.eu

Collaboration on this Newsflash:
Leonie Schäfer, Eric Gedenk

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

Quo vadis, Cybersecurity? Die Cybersicherheits-regulierung der EU

NIS-1, NIS-2, Cybersecurity Act oder Cyber Resilience Act – nicht nur einschlägig bewanderte IT-Sicherheitsbeauftragte mussten sich in den vergangenen Jahren mit dem komplexen Ökosystem von Regularien und Rechtsvorschriften auseinandersetzen. Cybersicherheit hat vielfältige Anforderungen, die bei den gesetzlichen Vorgaben nicht enden. Es wird Zeit für einen ganzheitlichen Blick auf die Regulierung der Sicherheit informationstechnischer Systeme.

Text: **Dennis-Kenji Kipker** (cyberintelligence.institute)

Keine Angst vor neuen gesetzlichen Vorgaben – so lautete das Credo von Prof. Dr. Dennis-Kenji Kipker bei der 31. DFN-Konferenz „Sicherheit in vernetzten Systemen“ | *Foto: DFN*

Nicht nur die Welt, sondern auch das Recht der Cybersicherheit befindet sich in einem erheblichen Umbruch: Seit der Coronapandemie 2019 hat sich die Bedrohungslage für die Sicherheit von vernetzten IT-Systemen nicht nur signifikant erhöht, sondern ganz erheblich verschärft. Globalpolitisch relevante Ereignisse wie der Beginn des Russland-Ukraine-Kriegs 2022, der Krieg in Israel seit dem vergangenen Jahr und die geopolitischen Spannungen zwischen der Volksrepublik China und Taiwan zeigen, dass sich die Welt in einem fragilen Zustand befindet. Dementsprechend ist es auch nur folgerichtig, wenn die Europäische Union zu dem Schluss kommt, dass man in Sachen Cybersicherheitsregulierung seit der ersten Netz- und Informationssicherheitsrichtlinie aus dem Jahr 2016 zwar viel erreicht hat, aber noch lange nicht am Ende angelangt ist.

„Cybercrime as a business“ – ein florierendes Geschäftsmodell

Was man vor allem den Betreibern von Kritischen Infrastrukturen und digitalen Dienstanbietern wie Cloud-Services, Onlinemarktplätzen und Onlinesuchmaschinen juristisch bislang aufbürdet, ist eigentlich nichts anderes als ein Informationssicherheitsmanagementsystem (ISMS), in dem die Cybersicherheit in einen rechtlich gefassten Prozess übertragen wird, der neben der Realisierung eines angemessenen Stands der Technik auch dessen

Prof. Dr. Thomas Hoeren, Leiter der Forschungsstelle Recht im DFN an der Universität Münster, ständiger Gast im DFN-Ausschuss für Recht und Sicherheit: „Der DFN ist seit Jahrzehnten nicht nur Garant für Netzzugang und Netzsicherheit an deutschen Forschungseinrichtungen, sondern auch Motor der deutschen und europäischen Internet-Governance-Diskussion. Es war und ist eine Freude und Ehre, diese wichtige gesellschaftliche Rolle über 30 Jahre im Ausschuss für Recht und Sicherheit und in der Forschungsstelle Recht begleiten und gestalten zu dürfen. Und ich freue mich auf viele weitere Jahre zu spannenden Themen wie etwa dem europäischen Datenrecht oder zu internationalen Rechtsfragen der Cybersecurity."

fortlaufende Überprüfung und die Meldung von Sicherheitsvorfällen voraussetzt.

Doch uns allen wird mit jedem neuen Tag, an dem wir auf die mediale Berichterstattung zu Cyberangriffen schauen, klar, dass unsere Welt nicht nur aus Kritischen Infrastrukturen und digitalen Diensteanbietern besteht – und dass theoretisch jedes Unternehmen, jede öffentliche Einrichtung und jede Einzelperson zu einem Opfer von Cyberangriffen werden kann. Es kommt nicht darauf an, wie groß oder präsent ich in der öffentlichen Wahrnehmung bin, sondern vor allem darauf, ob es bei mir wirtschaftlich etwas zu holen gibt. Und das ist letztlich auch der Grund dafür, weshalb „cybercrime as a business" als Geschäftsmodell zurzeit weltweit floriert.

„Resilienz" ist das neue Schlagwort

„Resilienz" lautete seinerzeit das Motto der Stunde, und heute mehr denn je. Diese Erkenntnis hatte zwangsläufig auch die Europäische Union, als sie im Dezember 2020 – unter dem Eindruck einer hochvulnerablen europäischen Gesellschaft inmitten des ersten Coronawinters – ihre neue Cybersicherheitsstrategie verkündete.

> Cyberresilienz ist nicht nur ein nettes Gimmick.

Wir müssen uns bewusst sein, dass Cyberresilienz schon lange nicht mehr nur ein nettes Gimmick oder zusätzliches Feature ist, mit dem ich mein Unternehmen oder meine Produkte versehe, sondern ein ganz essenzieller Bestandteil für die Antwort auf die Frage, ob ich im digitalen Raum auf Dauer überlebe oder nicht. Folglich geht es bei der Regulierung von Cybersicherheit schon lange nicht mehr um bloße abstrakte Compliance-Pflichten, die erfüllt werden, sondern um die Frage des Fortbestehens von Unternehmen und der Sicherheit von Staaten und ihren Bürgerinnen und Bürgern.

Ganzheitlicher Blick auf die Cybersecurity-Regulierung ist notwendig

Auch deshalb ergibt es Sinn, einen ganzheitlichen Blick auf die Regulierung der Sicherheit informationstechnischer Systeme zu wagen. Sowohl der nationale als auch der europäische Gesetzgeber haben hier in den letzten fast zehn Jahren einiges geleistet. Auf der nationalen Ebene in Deutschland nahm die rechtliche Regulierung von Cybersicherheit mit dem ersten

Christian Zens, Kanzler der Friedrich-Alexander-Universität Erlangen-Nürnberg, stellv. Vorstandsvorsitzender des DFN: „Als Kanzler war es für mich eine Ehre, aber auch eine Herausforderung, in den Kreis der ITler aufgenommen zu werden. Nach mehr als sechs Jahren fühle ich mich immer noch wohl, auch wenn mein Sprachverständnis gelegentlich Übersetzungshilfen benötigt. Es begeistert mich, dass der DFN-Verein mit seinen Werten die bundesweite Organisation für Hochschulen und Wissenschaftseinrichtungen ist, die dank des Engagements ihrer Mitglieder dafür sorgt, dass sie Spitzenleistungen bringen kann. Weiter so!“

IT-Sicherheitsgesetz (IT-SiG) ihren Anfang und gab bereits viele Anforderungen aus der nur ein Jahr später 2016 folgenden europäischen NIS-1-Richtlinie vor. Doch damit nicht genug: Im Jahr 2019 folgte schon der nächste, in allen Mitgliedsstaaten unmittelbar geltende Rechtsakt der EU-Gesetzgeber, der sogenannte „Cybersecurity Act“ (CSA). Dieser verschaffte der ENISA als europäischer Cybersicherheitsbehörde ein permanentes Mandat und legte zugleich den Grundstein für ein einheitliches europäisches Zertifizierungsschema für Cybersicherheit – zum Beispiel für Cloud-Sicherheit oder sichere 5G-Kommunikation.

> Hinsichtlich der Resilienz einer Gesellschaft kommt es nicht ausschließlich auf deren versorgungsrelevante Infrastruktur an.

Deutschland erkannte schon geringe Zeit später, dass die Absicherung von IT-Systemen nicht nur eine Aufgabe der Kritischen Infrastrukturen sein kann. Hinsichtlich der Resilienz einer Gesellschaft kommt es nicht ausschließlich auf deren versorgungsrelevante Infrastruktur an, sondern auch auf den digitalen Wirtschaftsschutz, da ein Staat ohne funktionierende Wertschöpfung in ganz ähnlicher Weise vulnerabel sein kann. Deshalb enthielt das zweite IT-Sicherheitsgesetz von 2021 erstmals Pflichten für die Cybersicherheit von sogenannten „Unternehmen im besonderen öffentlichen Interesse“, die einen volkswirtschaftlich herausragenden Stellenwert einnehmen. Darunter waren die in Deutschland nach Wertschöpfung größten Unternehmen zu fassen – allen voran die großen DAX-Konzerne – und deren Zulieferer, womit erstmalig auch der Mittelstand in den Fokus der gesetzlichen Cybersecurity-Pflichten rückte.

Die regelmäßige Publikation zur DFN-Konferenz „Sicherheit in vernetzten Systemen“ ist in der Deutschen Nationalbibliografie abrufbar | *Foto: DFN*

Mit dieser Art von Vorgabe zu digitaler Resilienz war Deutschland seiner Zeit voraus – prompt folgte, wieder ein Jahr später, der EU-Gesetzgeber mit der mittlerweile viel zitierten NIS-2-Richtlinie, die zurzeit – voraussichtlich bis zum Jahr 2025 – mit dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in das nationale Recht umgesetzt wird. Dies nimmt der nationale Gesetzgeber zum Anlass, gleich das gesamte deutsche IT-Sicherheitsrecht einmal komplett „auf links“ zu drehen. Und dass es bei der Cybersecurity Compliance tatsächlich auch um die ganzheitliche Perspektive geht, machte wiederum die Europäische Union deutlich, indem sie im Frühjahr 2024 den Cyber Resilience Act (CRA) verabschiedete, der verbindliche Vorgaben für die Cybersicherheit aller Arten von Produkten mit digitalen Elementen bestimmt – unabhängig davon, ob sie im B2B- oder B2C-Kontext Verwendung finden.

Mehr Interdisziplinarität für das Handling der Vorschriften

Sich in diesem komplexen Ökosystem von Rechtsvorschriften zurechtzufinden, die

Dr. Rainer Bockholt, Direktor des Hochschulrechenzentrums der Rheinischen Friedrich-Wilhelms-Universität Bonn, ehem. stellv. Vorstandsvorsitzender des DFN: „Denke ich an „40 Jahre DFN“, denke ich: Super Community! Bewundernswerte Weitsicht der Gründerinnen und Gründer. Höchste Leistungsfähigkeit und absolute Zuverlässigkeit, sowohl technisch als auch menschlich. Technische Innovationen, neue Dienste! Dabei das Ohr immer ganz nah an der Mitgliedschaft. Tipptopp. Es ist schön, dazuzugehören! Mein Wunsch für die Zukunft des DFN: Gerne weiter so!“

alle in ihrem Wesensgehalt mit Cybersicherheit zu tun haben, ist zweifelsohne eine erhebliche Herausforderung. Doch nicht nur Manager, Produktentwickler und IT-Sicherheitsbeauftragte in den betroffenen Unternehmen sind dieser Bürde ausgesetzt, sondern genauso die zuständigen Behörden und die Rechtsberater, die die Umsetzung zu begleiten haben.

> Das Recht und vor allem das Technikrecht sind schon jetzt deutlich interdisziplinärer als jemals zuvor.

Dies fängt bei der Identifizierung der betroffenen Einrichtung an (ob diese in den Anwendungsbereich einer gesetzlichen Vorschrift fällt), geht weiter über die erforderlichen Maßnahmen zum Risikomanagement in der Cybersicherheit und endet schließlich bei der Frage, wie mit Kunden und Vertragspartnern zukünftig umzugehen sein wird – ob beispielsweise bestehende vertragliche Regelwerke zum Outsourcing oder zur Sicherstellung der (digitalen) Lieferkette unter den Gesichtspunkten der Cybersicherheit ausreichend sind.

Klar ist damit: Das Recht und vor allem das Technikrecht sind schon jetzt deutlich interdisziplinärer als jemals zuvor – und diese Tatsache muss sich zwangsläufig auch in der Ausbildung der für die Umsetzung der neuen Regularien dringend benötigten Fachkräfte niederschlagen. Soweit es um Cybersecurity Compliance geht, kann die Frage, wer am besten hierfür personell abzustellen ist, somit nicht mehr zweifelsfrei beantwortet werden: Braucht es einen Juristen mit technischem Know-how oder einen Ingenieur, Techniker oder Informatiker mit juristischem Know-how? Und darüber hinaus: Über welche betriebswirtschaftlichen Kenntnisse muss ich eigentlich verfügen, um herauszufinden, ob eine Maßnahme im Sinne der gesetzlich angeordneten Risiken-Kosten-Abwägung wirklich angemessen ist?

Letztlich entscheidet niemand im „luftleeren Raum“

Sicherlich haben gerade jetzt, da zentrale gesetzliche Vorschriften wie NIS2 und der CRA noch nicht einmal in das nationale Recht umgesetzt bzw. final verabschiedet worden sind, ganz viele Unternehmen und betroffene Einrichtungen mehr Fragezeichen als Antworten im Kopf. Das ist aber keinesfalls schlimm und man sollte es tunlichst vermeiden, sich von abstrakten gesetzlichen Vorgaben abschrecken zu lassen – denn letztlich wissen es aktuell weder der Gesetzgeber noch Behörden wie das BSI deutlich besser. Best Practices brauchen erst einmal ihre Zeit, um sich zu etablieren. Branchenverbände müssen sich erst noch zusammensetzen, um branchenspezifische Sicherheitsstandards zu bestimmen. Und auch ein TÜV-Gutachter oder ein BSI können ihre Entscheidungen nicht im „luftleeren Raum“ treffen, sondern brauchen Orientierung und Anhaltspunkte. Gute Cybersicherheit ist eben ein Prozess und kein Produkt, das man sich einfach so fertig in den Raum stellt – und das gilt selbstredend auch für die gesetzlichen Vorschriften.

Cybersicherheit – keine lästige Bürde, sondern gewinnbringender Innovationsprozess

Wo stehen wir also und in welche Richtung geht unsere Reise in den nächsten Jahren? Nun, den gesetzlichen Weg zu mehr Cybersicherheit haben wir wie gezeigt bereits eingeschlagen – was per se nichts Schlechtes ist, denn wo ich zumindest eine Guideline habe, weiß ich zugleich auch, was ich tun muss, um schlimmstenfalls Schadensersatz- und Haftungsansprüche abzuwehren und bestenfalls neue Aufträge zu generieren. Und damit wären wir auch schon beim ganz entscheidenden Punkt angelangt: Cybersicherheit mag in Anbetracht der ganzen neuen gesetzlichen Regelungen, die man nun umsetzen muss, zunächst noch wie eine Bürde erscheinen, aber sie lässt einen bei gelungener Umsetzung nicht nur ruhiger schlafen, weil Geschäftsprozesse und digitale Produkte nicht ohne Weiteres kompromittiert werden können, sondern sie schafft auch Raum für neue Lösungen, Wettbewerbsvorteile und Innovation. Das sehen wir bereits jetzt: Für gute IT kommt es nicht allein auf ihre Funktionalität und Wirtschaftlichkeit an, sondern insbesondere darauf, ob sie verlässlich und vertrauenswürdig ist – und das setzt eben eine gute Cybersecurity und entsprechende Risikomanagementprozesse voraus. Nichts anderes schreiben im Endeffekt die gesetzlichen Vorgaben vor. ◆

Quickcheck für mehr Cybersicherheit

Die klassischen Vorgehensmodelle zum IT-Sicherheitsmanagement eignen sich wegen ihrer Struktur und Komplexität nur bedingt für kleine und mittlere Bildungseinrichtungen, da diese meist nicht über die ausreichenden personellen und finanziellen Ressourcen verfügen. Ein checklistenbasiertes Self-Assessment, das zur Prävention gegen Cyberkriminalität entwickelt wurde und auf einer an der Kriminalistik orientierten Gefährdungsanalyse basiert, ermöglicht einen Quereinstieg in die gängigen Standards und Best Practices der Cybersicherheit.

Text: **Reinhold Hepp** (Polizeivizepräsident a. D. Ulm), **Markus Schäffter** (Technische Hochschule Ulm)

Cyberkriminelle nehmen Bildungs- und Forschungseinrichtungen immer stärker ins Visier. Laut Microsoft werden in Europa durchschnittlich zehn Millionen Geräte mit Microsoft-Betriebssystem aktiv angegriffen (Zahlen vom April 2024), knapp 80 Prozent dieser Geräte werden von Bildungseinrichtungen selbst betrieben. Bereits im Jahr 2023 antwortete die NRW-Wissenschaftsministerin Ina Brandes auf eine Anfrage im Landtag, dass sämtliche Hochschulen Nordrhein-Westfalens in den vergangenen fünf Jahren angegriffen wurden mit unterschiedlichem Schadensausmaß. Unterstützt durch eine stärkere Arbeitsteilung und Spezialisierung der Cyberkriminellen sowie den Einsatz von Künstlicher Intelligenz (KI) sind Cyberangriffe seitdem deutlich gefährlicher geworden.

Sicherheitsexperten bringen es gerne wie folgt auf den Punkt: Es gibt zwei Arten von Organisationen: Diejenigen, die bereits erfolgreich gehackt wurden und diejenigen, die es nur noch nicht bemerkt haben.

Foto: 6.1m assets/freepik

Prof. Dr. York Sure-Vetter, Direktor der Nationalen Forschungsdateninfrastruktur (NFDI) e. V., Mitglied im Strategischen Beirat des DFN: „Der DFN-Verein ist unverzichtbar, wenn es um Konnektivität für die Wissenschaft geht – und damit Garant für den Basisdienst Identity and Access Management der Nationalen Forschungsdateninfrastruktur (NFDI). Vielen Dank für die tatkräftige Unterstützung und herzlichen Glückwunsch!“

Die Technische Hochschule Ulm, die Universität Ulm, das Polizeipräsidium Ulm, die Industrie- und Handelskammer Ulm sowie die Handwerkskammer Ulm haben gemeinsam einen neuen Ansatz der Prävention gegen Cyberkriminalität getestet. Ähnlich den polizeilichen Vor-Ort-Beratungen zum Schutz vor Einbruch und Diebstahl wurde ein Beratungskonzept zum Schutz vor Cyberangriffen entwickelt. Ziel ist es, die kriminalitätsfördernden Faktoren wie einfache Tatgelegenheit, geringes Täterrisiko und hohen Tatertrag systematisch zu reduzieren.

Wie ein Angreifer zu denken, ist der erste Schritt

Die Grundidee ist dabei vergleichsweise einfach: Welche Motivation und Erfolgsfaktoren treiben Cyberkriminelle an, Bildungseinrichtungen, Kommunen und Unternehmen anzugreifen?

Es sind vor allem die folgenden Aspekte, die Cyberangriffe für Kriminelle attraktiv machen:

- **Die günstige Tatgelegenheit**
  Die Vielzahl von Sicherheitslücken und die gerade in kleinen und mittleren Organisationen begrenzten finanziellen und personellen Ressourcen zum Schutz vor Cyberangriffen erleichtern Angriffe, die bequem über das Internet erfolgen können.

- **Der geringe Tataufwand**
  Angriffswerkzeuge und das Wissen um ihre Anwendung sind leicht verfügbar und spezialisierte Unterstützung ist bequem über das Darknet zu beziehen (Hacking-as-a-Service).

- **Ein hoher Tatertrag**
  Sogar Angriffe auf Bildungseinrichtungen stellen ein lukratives Geschäftsmodell dar, selbst wenn keine großen Lösegeldsummen zu erwarten sind. Denn frei nach dem Motto „auch Kleinvieh macht Mist“ werden kleinere Beträge häufiger gezahlt als Millionensummen.

- **Ein geringes Täterrisiko**
  Das Zerschlagen krimineller Vereinigungen erfordert aufwendige internationale Polizeiarbeit. Festnahmeerfolge sind eher selten. Hinzu kommt das große Dunkelfeld nicht angezeigter Straftaten.

Das Ziel vor Augen: Weg von der Gießkanne hin zur gezielten Prävention

Die hohe Tätermotivation und die zunehmende Fokussierung organisierter Kriminalität auf „leichte Opfer“ bedeutet für kleinere und mittlere Unternehmen, Behörden und Bildungseinrichtungen, sich systematisch mit dem Thema Cybersicherheit zu beschäftigen und die Resilienz durch einen gezielten und ganzheitlichen Präventionsansatz gegen IT-Krisen zu verstärken. Dabei helfen die einschlägigen Standards und Best Practices, aber es reicht nicht mehr aus, nach dem Gießkannenprinzip vorzugehen und sich mit Firewalls und Virenschutz zufriedenzugeben. In Zukunft wird es entscheidend sein, das eigene Schutzniveau präzise an die jeweils aktuelle Gefährdungslage anzupassen und Schutzmaßnahmen dort zu verstärken, wo Cyberkriminelle typischerweise nach Eingangstoren suchen. Eine Unterstützung bietet der von der Technischen Hochschule Ulm und der Universität Ulm entwickelte Ansatz einer 360-Grad-Cybersicherheitsanalyse, welcher in der Version 0.2 bei der 31. DFN-Konferenz „Sicherheit in vernetzten Systemen“ vorgestellt wurde.

> Die Analyse erfolgt mithilfe eines Fragebogens.

Die Vorgehensweise unterscheidet sich grundlegend von der klassischen Methode, Standards und Best Practices checklistenbasiert in aller Breite umzusetzen. Statt darauf zu setzen, ein möglichst gleichmäßiges Sicherheitsniveau in allen Handlungsfeldern der IT-Sicherheit zu erlangen, geht es darum, die wichtigsten für die jeweilige Organisation relevanten IT-Risiken zu identifizieren. In Form einer Sicherheitsanalyse wird der Schutz gegen diese Risiken auf den Prüfstand gestellt. Um die Analyse effizient durchführen zu können, erfolgt sie mithilfe eines Fragebogens. Im ersten Schritt werden Fragen zu typischen Schutzmaßnahmen der Cybersicherheit gestellt und automatisiert ausgewertet. Das Ergebnis der Auswertung identifiziert die Stärken und Schwächen im individuellen Sicherheitsmanagement. Im zweiten Schritt erfolgt eine Fokussierung auf diejenigen Handlungsfelder, welche den größten Handlungsbedarf aufweisen. Mithilfe tiefergehender Detailfragen zu diesen Handlungsfeldern können konkrete

Handlungsempfehlungen ausgesprochen werden. Diese zeigen, welche Schutzmaßnahmen ergänzend zu den bereits Bestehenden umgesetzt werden sollen, um der aktuellen Gefährdungslage gerecht zu werden. Bei Bedarf kann der Kontakt zu spezialisierten Dienstleistern hergestellt werden. Eine Wiederholung dieses Ablaufs führt zu einem zunehmend detailreicheren Bild und hilft dabei, das individuelle Schutzniveau schrittweise dort zu erhöhen, wo Investitionen den größten Nutzen bringen (Abbildung 1: Ablaufprozess).

Sie sind eingeladen, an der Fortentwicklung teilzunehmen

Die Cybersicherheitsanalyse wird fortlaufend weiterentwickelt und liegt aktuell in der Version 0.4 vor. Die Umstellung des Fragebogens von einem interaktiven PDF-Dokument hin zu einer webbasierten Portallösung ist in Vorbereitung.

Wenn Sie sich selbst einen Eindruck verschaffen möchten, so fordern Sie gerne den PDF-Fragebogen an, füllen diesen aus und senden ihn per E-Mail an die Autoren. Sie erhalten dann bei Rücksendung des Fragebogens einen automatisiert erstellten Bericht, der auf der Grundlage Ihrer Antworten Hypothesen zum Umsetzungsstand der Cybersicherheit (diese umfasst die IT- und die Informationssicherheit) formuliert und diese in Form einer Stärken-Schwächen-Analyse im Vergleich zu den einschlägigen Best Practices sowie zur Peer-Gruppe vergleichbar großer Organisationen zusammenfasst, ähnlich wie in der Abbildung 2 (Radar) dargestellt.

Dabei stellen die Speichen im Diagramm die aktuelle Umsetzung der einschlägigen Schutzmaßnahmen in den einzelnen Handlungsfeldern der Cybersicherheit (Governance, Sicherheitsmanagement, sicherer IT-Betrieb, Netzwerksicherheit, physische Sicherheit usw.) dar. Die ausgefüllte Fläche entspricht dabei dem Umsetzungsstand der Cybersicherheit im Unternehmen.

Diese Fläche ist wie ein Fallschirm: Je größer und gleichmäßiger die Fläche ist, desto größer die Schutzwirkung. Die gestrichelte Linie stellt im Vergleich dazu den durchschnittlichen Umsetzungsstand in der Peer-Gruppe dar, basierend auf den einschlägigen Studien zur Cybersicherheit. Die aktuell verfügbaren Studien lassen einen Vergleich zu Wirtschaftsunternehmen mit einer vergleichbaren Anzahl an Beschäftigten zu.

> Die individuelle Stärken-Schwächen-Analyse ermöglicht es, IT-Risiken zu identifizieren.

Die individuelle Stärken-Schwächen-Analyse ermöglicht es nun, die kritischen IT-Risiken zu identifizieren und darauf aufbauend konkrete Handlungsempfehlungen zur zielgerichteten Verbesserung des aktuellen Sicherheitsniveaus auszusprechen, verbunden mit Verweisen auf die in den einschlägigen Best Practice-Katalogen enthaltenen technischen, organisatorischen und verhaltensrelevanten Schutzmaßnahmen. Diese Empfehlungen werden in Zukunft um praxisnahe Handlungsempfehlungen, basierend auf den Erfahrungen spezialisierter Sicherheitsdienstleister, ergänzt werden.

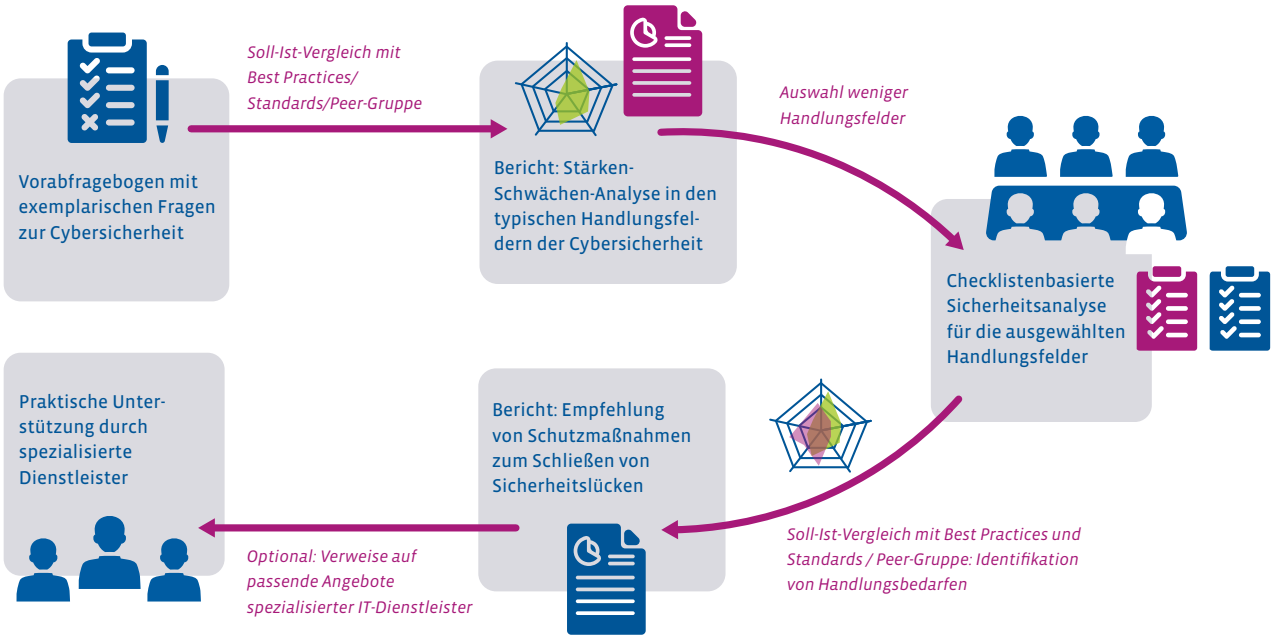


Abbildung 1: Ablaufprozess

Dr. Christa Radloff, ehem. Leiterin des IT- & Medienzentrums der Universität Rostock, ehem. Mitglied im Verwaltungsrat und Betriebsausschusses des DFN: „In den vergangenen 40 Jahren hat der DFN-Verein es geschafft, erfolgreich Gemeinschaft zu bilden und die oft unterschiedlichen Interessen zu bündeln. Auf Basis der engagierten Arbeit der Mitglieder, gemeinsam mit der Kompetenz der Mitarbeiterinnen und Mitarbeiter in der Geschäftsstelle, wird es dem DFN sicher auch in Zukunft gelingen, neue Herausforderungen im Sinne der Gemeinschaft zu bewältigen."

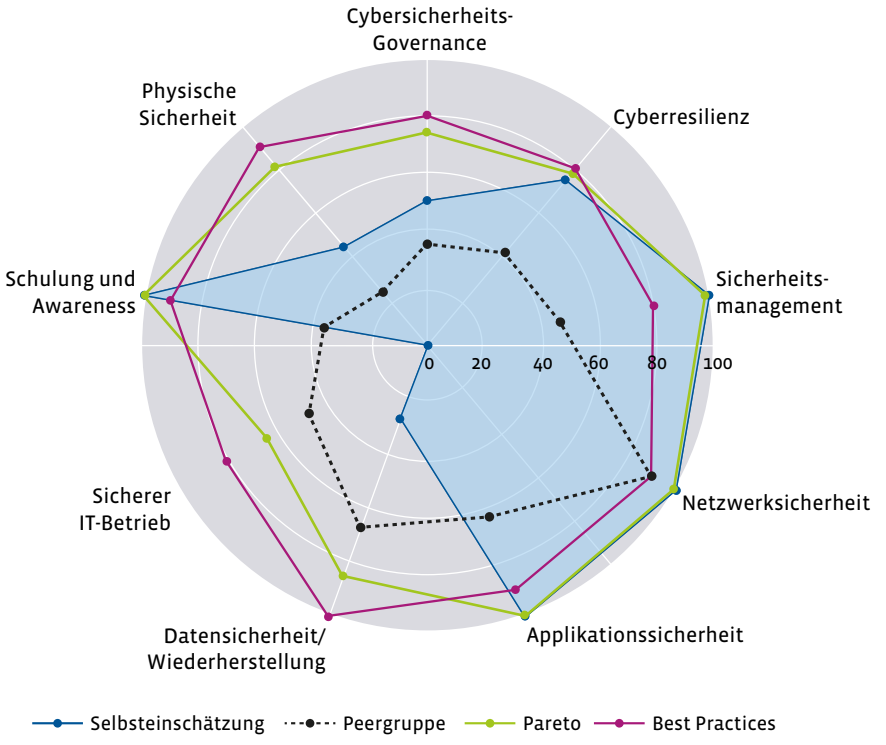


Abbildung 2: Radar

QUELLEN

Microsoft Security Intelligence: Most affected industries: **https://www.microsoft.com/en-us/wdsi/threats**

Ein erweitertes Paper der 360-Grad-Cybersicherheitsanalyse ist abrufbar unter: **www.researchgate.net/profile/Markus-Schaeffter/research**

Nehmen Sie an der Cybersicherheitsanalyse der Technischen Hochschule Ulm teil und unterstützen Sie uns bei der Weiterentwicklung des Konzepts. Den Fragebogen für Bildungseinrichtungen können Sie unter folgender E-Mail-Adresse anfordern: **markus.schaeffter@thu.de**

Sofortmaßnahmen zur Cybersicherheit

Die Ergebnisse der bisherigen Auswertungen decken sich, wenig überraschend, in ihren Kernaussagen mit einschlägigen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Digital-Branchenverbands Bitkom. Für die Prävention ist es von entscheidender Bedeutung, klare Ziele zu setzen, Verantwortung zu delegieren und die Nutzenden regelmäßig auf typische Angriffsmuster aufmerksam zu machen. Eine übergeordnete Sicherheitsrichtlinie als Managementauftrag ist der erste Schritt, ergänzt durch Sicherheitsrichtlinien zu zentralen Themen der Cybersicherheit.

Von essenzieller Bedeutung ist die Unterrichtung und Sensibilisierung zu aktuellen Risiken und gebotenen Schutzmaßnahmen – nicht nur der IT-Nutzenden, sondern auch der Systemverantwortlichen im IT-Betrieb und in den Fachabteilungen. Um im Krisenfall schnell und richtig reagieren zu können, sind Krisenteams einzurichten, u. a. auf Leitungsebene, für den IT-Betrieb, für die interne und externe Kommunikation sowie für Compliance und Datenschutz. Durch die Fachverantwortlichen sind Notfallpläne mit konkreten technischen und organisatorischen Reaktionsmaßnahmen zu entwickeln. Dazu gehört, über krisenfeste Kommunikationsmittel zu verfügen, nicht nur untereinander, sondern auch zur Cybersicherheitsagentur des Landes bzw. zur polizeilichen Forensik, zur Datenschutzaufsicht (Meldung potenzieller Datenpannen binnen 72 Stunden) und zu auf IT-Krisenmanagement spezialisierten Dienstleistern.

Insbesondere der Bereich Außenkommunikation muss vorbereitet sein, um im Krisenfall schnell alle relevanten Stakeholder sowie die Öffentlichkeit informieren zu können. Professionelle Offenheit und weniger „Salamitaktik" ist hier der Schlüssel zum Erfolg. Alternative Web- und Mail-Server sind für den Krisenfall vorzuhalten, inklusive vorbereiteter und inhaltlich abgestimmter Verlautbarungen und Pressetexte, die anschließend nur noch in Feinheiten anzupassen sind. ◆

Mit Ausbildung Schule machen

Der erste Auszubildende im DFN-CERT hat seinen Abschluss mit Bravour gemeistert und gleich im Anschluss einen Arbeitsvertrag unterschrieben. Ausbilden für den Eigenbedarf lautet die Antwort auf den verschärften Fachkräftemangel – ein Lernprozess nicht nur für die Auszubildenden, sondern für das ganze Unternehmen.

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

Schrauben gehört dazu: Als angehender Fachinformatiker muss Antonio (rechts, mit seinem Ausbilder Mathias Baggendorf) auch das Innenleben eines Computers kennen | *Alle Fotos: Dieter Stolte, DFN-CERT*

Prof. Dr. Klaus-Peter Kossakowski, Geschäftsführer der DFN-CERT Services GmbH, ständiger Gast im DFN-Verwaltungsrat und im Ausschuss für Recht und Sicherheit: „Seit über 30 Jahren im Dienst des DFN-Vereins: Keiner von uns weiß morgens mit Sicherheit, was der Tag bringen wird. Die eine oder andere Einrichtung erlebt möglicherweise eine böse Überraschung. Aber bei einer Sache bin ich mir sehr sicher: Hand in Hand mit dem DFN-Verein hilft das DFN-CERT teilnehmenden Einrichtungen im Wissenschaftsnetz schnell und unkompliziert bei Sicherheitsvorfällen jedweder Art. Und das wird auch die kommenden 40 Jahre so bleiben!“

Hätte jemand Antonio Rodriguez Yorca vor sechs Jahren in Spanien prophezeit, dass er mit 24 Jahren als fertiger Kfz-Mechatroniker noch einmal in Deutschland die Schulbank drücken würde, er hätte gelacht. Seit Januar hat er sein Abschlusszeugnis als frisch gebackener Fachinformatiker für Systemintegration in der Tasche und dazu noch eine Festanstellung bei der DFN-CERT Services GmbH. Der Weg dorthin war lang, streckenweise steinig und führte ihn 2018 von Almerimar in Andalusien ins verregnete Hamburg.

Ausbilden für den Eigenbedarf

Seit zweieinhalb Jahren bildet das DFN-CERT in der Elbmetropole im Bereich Fachinformatik aus – zunächst in der Fachrichtung Systemintegration, später folgte Anwendungsentwicklung. Ein Novum für den Sicherheitsdienstleister, der 1993 als reines Computernotfallteam für die teilnehmenden Einrichtungen im Deutschen Forschungsnetz (DFN-Verein) gegründet wurde. Warum nach fast 30 Jahren erstmalig eine Fachausbildung angeboten wurde?

> Unser Ziel ist es, alle Auszubildenden in ein festes Arbeitsverhältnis zu übernehmen.

„Dieser Schritt war ein wenig aus der Not heraus geboren. Uns fehlt zunehmend das Fachpersonal, das wir für die stetig wachsenden Aufgaben und Herausforderungen in den Bereichen IT-Betrieb und Softwareentwicklung dringend benötigen. Wir bilden daher ausschließlich für den eigenen Bedarf aus. Unser erklärtes Ziel ist es, alle Auszubildenden nach Beendigung ihrer Ausbildung in ein festes Arbeitsverhältnis zu übernehmen“, erklärt Mathias Baggendorf. Nicht nur Akademikerinnen und Akademiker sind im IT-Bereich gefragt, sondern auch Fachkräfte mit einer fundierten betrieblichen Ausbildung. Laut dem Branchenverband Bitkom hat der Fachkräftemangel im IT-Bereich einen neuen Höchststand erreicht. Insbesondere IT-Security-Fachkräfte sind begehrt. Ein wichtiger Aspekt sei außerdem, dass sie es mit dem hauseigenen Ausbildungsgang in der Hand haben, welches Wissen konkret vermittelt wird, ergänzt Thiemo Nordenholz. Er und Mathias sind die beiden offiziellen Ausbilder für insgesamt fünf Azubis im DFN-CERT. Angefangen haben sie mit einem Auszubildenden mitten in der Coronapandemie.

Aller Anfang ist schwer

Anderthalb Jahre Vorlauf brauchten Mathias und Thiemo bis zum Start der Ausbildung. Zu Beginn standen etliche Fragen im Raum: Wie sehen die gesetzlichen Rahmenbedingungen aus? Welche Ressourcen benötigt ein Unternehmen für die Ausbildung? Und welche Voraussetzungen müssen Ausbilderinnen und Ausbilder erfüllen? Die fehlenden Antworten lieferten die Expertinnen und Experten der Handelskammer Hamburg. Als Partner der Ausbildungsbetriebe beraten und unterstützen sie Unternehmen dabei, ein Ausbildungskonzept zu entwickeln. Der gesetzliche Ausbildungsrahmenplan gibt die fachlichen Inhalte vor, die durch den Betrieb vermittelt werden müssen. Für die Fachrichtung Systemintegration sind das unter anderem das Konzipieren und Administrieren von IT-Systemen und das Installieren und Konfigurieren von Netzwerken. Kurzum: Fachinformatikerinnen und Fachinformatiker für Systemadministration sind die ersten Ansprechpersonen im Betrieb, wenn Störungen von IT-Systemen oder des Netzwerks auftreten.

Zwingend notwendig für die offiziellen Betreuenden im Betrieb ist die sogenannte Ausbildereignung. Bevor der erste Azubi eingestellt wurde, mussten Mathias und Thiemo die erforderlichen arbeitspädagogischen Kenntnisse in einem zweiwöchigen Lehrgang erlernen und diese zusammen mit ihren fachlichen Fähigkeiten nach der Ausbilder-Eignungsverordnung in einer Prüfung nachweisen. „Ich war überrascht, was wir als Vorbereitung auf die Prüfung alles lernen mussten: Methodik, Didaktik, fast wie im Lehramt“, sagt Mathias. Sie sind aber nicht die Einzigen, die sich an der Ausbildung im DFN-CERT beteiligen. Ein Team aus insgesamt sechs Leuten bestreitet die Betreuung. Einmal im Monat trifft sich die Gruppe, um sich auszutauschen, zu planen und aktuelle Herausforderungen zu besprechen.

Die Ausbildung in Deutschland ist überwiegend dual aufgebaut. Das heißt, etwa ein Drittel der Ausbildung erfolgt in der Schule in Unterrichtsblöcken von drei bis vier Wochen und zwei Drittel, circa sechs bis acht Wochen am Stück, in Vollzeit im Betrieb. Der Tagesablauf im DFN-CERT ist für die Azubis strukturiert. Am Vormittag findet eine etwa einstündige Lerneinheit statt, die durch einen Betreuenden vorbereitet und

Mathias Baggendorf, Diplominformatiker im Projekt- und Entwicklungsteam der DFN-CERT Services GmbH, ist für die angehenden Fachinformatiker (m/w/d) für Systemintegration zuständig.

durchgeführt wird. In dieser wird ein ausgewähltes Thema, beispielsweise das OSI-Referenzmodell, gemeinsam erschlossen. Ergänzend werden verschiedene Übungsaufgaben gestellt, mit denen sich die Azubis eigenständig bis zum frühen Nachmittag beschäftigen. Nachdem die Aufgaben mit den Betreuenden besprochen wurden und mögliche Fragen geklärt sind, verbringen die Azubis den restlichen Arbeitstag in der ihnen zugeordneten Fachabteilung, schnuppern in das Tagesgeschäft und lernen die konkreten Arbeitsabläufe in ihrem späteren Tätigkeitsfeld kennen.

> „Als Antonio seine Ausbildung antrat, galt der Ausnahmezustand.“

Als Antonio am 1. August 2021 unter Pandemiebedingungen seine Ausbildung zum Fachinformatiker für Systemintegration beim DFN-CERT antrat, war das in dieser Form noch nicht möglich. Es galt der Ausnahmezustand. Nur einmal in der Woche durfte er sich mit seinem Ausbilder Mathias mit Abstand und Maske im Büro treffen, um den Ausbildungsplan zu besprechen. Den Rest der Woche lernte er von zu Hause aus. „So isoliert zu lernen fiel mir sehr schwer“, gibt der gebürtige Spanier zu, der zudem noch der erste und einzige Auszubildende war zu der Zeit. Sehr viel zusätzliches Eigenstudium investierte er, um am Ball zu bleiben.

Sein Wunsch, in Deutschland zu arbeiten und zu leben, reifte 2017 mit einem Besuch bei einem Verwandten in Hamburg – einen Ausflug zum Nürburgring machen und ein paar Runden drehen, das war der Plan. Danach absolvierte er ein Praktikum für Kfz-Sicherheit. Zurück in Spanien begann er zunächst, Ingenieurwesen zu studieren. Aber Deutschland ließ ihm keine Ruhe. Jetzt oder nie, dachte er sich und kehrte ein Jahr später mit einer deutschen Zeitarbeitsfirma zurück nach Hamburg – mit zunächst wenig deutschen Sprachkenntnissen. „Alles, was ich an Deutsch kann, habe ich mir im Rahmen der Arbeit angeeignet“, sagt er. Etwa drei Jahre arbeitete er in seinem erlernten Beruf, sah aber zunehmend keine Entwicklungsmöglichkeiten mehr für sich. Sein Entschluss, die Branche zu wechseln, stand. „Ich hatte schon immer ein riesiges Interesse an Computern und Technik“, erzählt Antonio. Bereits in der Schule sei er der Nerd gewesen, der für die Mitschüler deren Computerprobleme gelöst habe.

Die Chemie muss stimmen

Antonios Enthusiasmus war es auch, der Mathias und Thiemo im Vorstellungsgespräch überzeugte. Ihnen kommt es in erster Linie auf die Motivation und die Persönlichkeit an. Die Chemie muss stimmen, schließlich wollen die beiden künftige Kolleginnen und Kollegen ausbilden. „Rein fachliche Qualifikationen sind für uns nicht ausschlaggebend. Mir ist wichtig, dass jemand wirklich zu uns passt. Das DFN-CERT arbeitet mit vertraulichen Daten, da benötigen wir Kolleginnen und Kollegen, auf die man sich absolut verlassen kann“, sagt Mathias. „Wenn uns jemand schon im Bewerbungsschreiben von seiner Leidenschaft für den Beruf überzeugen kann, dann ist uns das wichtiger als eine Zwei in Mathe“, bekräftigt Thiemo. Entscheidend sei nicht immer die Papierlage, sprich die Bewerbungsunterlagen, sondern der menschliche Aspekt.

Thiemo Nordenholz, aus dem Projekt- und Entwicklungsteam der DFN-CERT Services GmbH, ist für die angehenden Fachinformatiker (m/w/d) für Anwendungsentwicklung zuständig.

Reden ist Gold

Ein wichtiges Instrument des Ausbildungskonzepts sind engmaschige Feedbackgespräche zwischen Ausbilder und Auszubildenden. Letztere kennen in der Regel das Berufsleben noch nicht und müssen in das Sozialgefüge Betrieb erst hineinfinden. „So merken wir rechtzeitig, falls jemand beim Lernen den Anschluss verliert oder anderweitig Schwierigkeiten hat“, sagt Thiemo.

> „Wir stehen in der Verantwortung, dass unsere Azubis ihre Ausbildung schaffen.“

Außerdem sei dieser Austausch auch eine wertvolle Rückmeldung für die Ausbilder, ob sie das Wissen gut vermittelt haben. „Negatives Feedback musst du dir als Ausbilder aktiv abholen. Denn auch als Ausbilder will ich mich entwickeln und verbessern. Letztendlich stehen wir in der Verantwortung, dass unsere Azubis ihre Ausbildung schaffen“, betont Mathias.

Hartmut Hotzel, ehem. Leiter des Rechenzentrums der Bauhaus-Universität Weimar, ehem. ZKI-Vorsitzender: „Beim ersten Kontakt war der DFN nur eine „Blackbox“. Heraus kamen wichtige Dienste, aber in der großen Mitgliederversammlung war es eher „Frontalunterricht“. Beim zweiten Kontakt kamen die Personen zum Vorschein, die im Vorder- oder im Hintergrund arbeiteten. Und ab dann wurde es immer persönlicher, egal ob noch formal korrekt oder berlinerisch. Und je länger der Kontakt anhielt, desto mehr kam der „Wohlfühlfaktor“ hinzu: Arbeit kann auch Spaß machen mit den richtigen Personen im Team!“

Nicht nur über fachliche und didaktische Skills sollten Ausbilder verfügen, auch Empathie im Zwischenmenschlichen und Sensibilität für die verschiedenen Persönlichkeiten der Azubis sind hilfreich. „Die Zeit vor Antonios Abschlussprüfungen und Abgabe seiner Projektarbeit war ziemlich heiß. Er hatte seine Ausbildung auf zweieinhalb Jahre verkürzt und stand sehr unter Druck“, erinnert sich Mathias. Auch Antonio wird diese Zeit nicht so schnell vergessen. Zum Lernstress nach einem Acht-Stunden-Tag kam noch die Sorge, in den Abschlussprüfungen zu versagen. „Zum Glück konnte ich mit Mathias und meinen Kolleginnen und Kollegen über alles reden. Mathias‘ Zuspruch ‚wir schaffen das gemeinsam‘ hat mir Mut gemacht“, sagt Antonio.

Die Ausbildungsprüfungen fallen ausschließlich in den Hoheitsbereich der Industrie- und Handelskammern und werden von diesen organisiert. Die Prüfung der Fachinformatiker wird in zwei Teilen absolviert: Der erste Teil wird nach anderthalb Jahren abgelegt und besteht aus einer schriftlichen Klausur über 90 Minuten. Der zweite Prüfungsteil am Ende der regulär dreijährigen Ausbildung beinhaltet neben drei weiteren 60-minütigen schriftlichen Klausuren auch eine praktische Projektarbeit. Für die Vorbereitung und Durchführung stehen den Auszubildenden insgesamt 35 Stunden zur Verfügung. Während dieser Zeit sind sie von jeglicher betrieblichen Arbeit freigestellt. Anschließend erfolgt die mündliche Verteidigung des Projektthemas vor dem Prüfungsausschuss. Für seine Projektarbeit erstellte Antonio ein Konzept zur Optimierung und zum Monitoring des WLAN-Netzes im DFN-CERT. „Das hat auf der einen Seite einen echten Mehrwert für unsere Firma, auf der anderen Seite motiviert es die Auszubildenden viel mehr, wenn sie ein reales Problem lösen können“, betont Mathias.

Hardware für die Hosentasche: Das DFN-CERT stellt Antonio und seinen Mitauszubildenden Lehrmaterialien wie den Einplatinencomputer Raspberry Pi zur Verfügung.

An der Praxis entlang entwickeln

In den fast drei Jahren Ausbildung im DFN-CERT hat sich das Lehrkonzept stark weiterentwickelt. Waren die Inhalte zu Beginn eher theorielastig, so verfolgen sie heute einen aufgabenorientierten Ansatz. „Wir hatten am Anfang keinen Masterplan für die Ausbildung. Wir haben ein Konzept entworfen, geschaut, wie es in der Realität funktioniert und dann sukzessive nachgebessert. Heute arbeiten wir viel mehr mit konkreten Beispielen aus unserer fachlichen Praxis“, erklärt Mathias.

> „Das Vorwissen der Azubis ist sehr unterschiedlich.“

Erstaunt waren die beiden Ausbilder auch, wie unterschiedlich das Vorwissen der Azubis ist. Das reicht von „Hier ist der Knopf zum Einschalten“ bis hin zu ausgeprägten Kenntnissen in Programmiersprachen. „Aber auch mit gefährlichem Halbwissen oder falschem Wissen müssen wir teils aufräumen“,

gibt Thiemo zu. Um einen einheitlichen Wissensstand aufzubauen, beginnen sie heute mit Basics wie etwa dem Aufbau und den Kernfunktionen eines Computers. Daraus hat sich nun das umfangreiche Modul „IT-Grundlagen“ entwickelt. Dieses behandelt neben dem Aufbau der Hardware Themen wie Speicherarten, Datenprotokolle oder Möglichkeiten der Datenübertragung.

„Gehirnkater statt Muskelkater“

Antonio brachte bereits gute Vorkenntnisse mit. Was ihm mehr zu schaffen machte, war nicht nur die Umstellung von einer körperlich aktiven Tätigkeit als Kfz-Mechatroniker auf eine permanent vor dem Bildschirm sitzende Beschäftigung, sondern auch das viele Analysieren und Grübeln über die Arbeit, das sich auch nach Feierabend nicht einfach abstellen lässt. „In der IT startest du oft mit einem Problem und hast zum Schluss eine Verkettung verschiedenster Probleme. Wie bei einer Zwiebel geht es immer tiefer in die nächste Schicht“, sagt er. Die Diagnose sei wesentlich komplexer als bei einem Auto. Das A und O bei dieser Arbeit sei, Ruhe zu bewahren und strukturiert vorzugehen, wenn es hektisch wird. Gleichzeitig ist die Lösung eines Problems aber auch das, was ihn an seinem neuen Beruf am meisten befriedigt. „Gehirnkater statt Muskelkater“, bringt er es auf den Punkt. Als ITler dürfe man nie aufhören zu lernen. Eine IT-Technik, die heute aktuell ist, kann morgen schon veraltet sein.

AUSBILDUNG ZUM FACHINFORMATIKER (M/W/D)

Mögliche Fachrichtungen:
- Systemintegration
- Anwendungsentwicklung
- Daten- und Prozessanalyse
- Digitale Vernetzung

Ausbildungsdauer: 36 Monate

Prüfungen:
- Abschlussprüfung Teil 1 nach 18 Monaten, schriftliche Prüfung (90 Min.)
- Abschlussprüfung Teil 2 zum Ende der Ausbildung, 3 schriftliche Prüfungen (je 60 Min.), praktische Projektarbeit mit Präsentation und mündlicher Verteidigung

Fachrichtungsübergreifende Fertigkeiten und Kenntnisse
- Planen, Vorbereiten und Durchführen von Arbeitsaufgaben
- Informieren und Beraten von Kundinnen und Kunden
- Beurteilen marktgängiger IT-Systeme
- Entwickeln, Erstellen und Betreuen von IT-Lösungen
- Durchführen und Dokumentieren von qualitätssichernden Maßnahmen
- Umsetzen, Integrieren und Prüfen von Maßnahmen zur IT-Sicherheit und zum Datenschutz
- Erbringen von Leistungen und Auftragsabschluss
- Betreiben von IT-Systemen
- Inbetriebnahme von Speicherlösungen
- Programmieren von Softwarelösungen

Ergänzende Ausbildungsinhalte (Anwendungsentwicklung):
- Konzipieren und Umsetzen von kundenspezifischen Softwareanwendungen
- Sicherstellen der Qualität von Softwareanwendungen

Ergänzende Ausbildungsinhalte (Systemintegration):
- Konzipieren und Realisieren von IT-Systemen
- Installieren und Konfigurieren von Netzwerken
- Administrieren von IT-Systemen

Fazit

Das Resümee von Thiemo und Mathias nach Beendigung des allerersten Ausbildungsganges fällt sehr positiv aus. War es zu Beginn noch etwas hektisch, hat sich mittlerweile

> „Den ersten Kollegen selbst ausgebildet zu haben ist ein echter Gewinn.“

eine Routine eingestellt. Trotz der vielen Pionierarbeit hatten sie eine Menge Spaß und haben auch viel gelernt – über sich selbst und über ihre Fähigkeiten als Ausbilder. Beide würden den Weg jederzeit wieder gehen. „Den ersten Kollegen selbst erfolgreich ausgebildet zu haben, ist ein echter Gewinn für unsere ganze Firma. Ich bin mir sicher, dass wir diesen Erfolg mit den kommenden Ausbildungsjahrgängen weiter fortsetzen werden!“, sagt Mathias. „Wir bilden zwar Leute aus, die hinterher überall arbeiten können. Aber in erster Linie können und sollen sie das bei uns“, betont Thiemo. Jeder Azubi, der übernommen wird, ist ein Gewinn und eine Investition in die Zukunft des DFN-CERT.

Auch Antonio blickt zuversichtlich auf seine berufliche Entwicklung. Ihn interessieren unterschiedliche Bereiche in der IT. Zuerst möchte er mehr Erfahrung sammeln – um seinen künftigen Berufsweg besser zu finden, aber auch, um sein Wissen einmal weitergeben zu können, genau wie Mathias und Thiemo. Für die Chance, die ihm das DFN-CERT gegeben hat, wird er immer dankbar sein, sagt er. Hamburg ist mittlerweile seine zweite Heimat geworden. Mit seiner Freundin, die er in der Hansestadt kennengelernt hat, ist er zusammengezogen. Die norddeutsche Kultur und Lebensart haben es ihm angetan, und auch das typisch norddeutsche Wetter gehört für ihn dazu. Das Einzige, mit dem er sich nicht anfreunden kann, sind Matjes und Mettbrötchen. „Das kann meine Freundin schon zum Frühstück essen. Da dreht sich mir der Magen um“, sagt er lachend. ◆

Sicherheit aktuell

Hockenheim-Ring GmbH ist offizieller eduroam-Service-Provider

Wenn im August wieder der internationale Wettbewerb der Formula Student Germany (FSG) ausgetragen wird, ist eduroam offiziell mit an Bord. Der DFN-Verein freut sich, die Hockenheim-Ring GmbH als neuen eduroam-Service-Provider zu begrüßen. Service-Provider, die den Dienst eduroam außerhalb von Universitäten, Hochschulen und Forschungseinrichtungen anbieten, leisten mit ihrer Initiative einen wichtigen Beitrag für Wissenschaft und Lehre – sowohl national als auch international.

Auf Initiative der Formula Student Germany e. V. und der DFN-Geschäftsstelle in Berlin kam die Vereinbarung, die Anfang März 2024 unterzeichnet wurde, zustande. Mit der sicheren und zuverlässigen WLAN-Verbindung können die Studierenden vor Ort auf ihre Wettbewerbspräsentationen und Konstruktionsdaten zugreifen und sich untereinander austauschen. Ob Kanada, Israel, Indien oder Kasachstan – beim FSG-Konstruktionswettbewerb treten jedes Jahr Studierende aus aller Welt an. Die Aufgabe der Hochschulteams ist es, einen einsitzigen Rennwagen nicht nur zu konstruieren, sondern auch selbst zu bauen. Dabei messen sie sich in verschiedenen Disziplinen, u. a. Geschwindigkeit, Leistung, Energieeffizienz, Design und sogar Finanz- und Vertriebsplanung. Höhepunkt des Wettkampfes ist das fünftägige Rennen auf der berühmten Formel-1-Strecke am Hockenheimring. Hier gewinnt nicht das schnellste Auto, sondern das Team mit dem besten Gesamtpaket. ◆

Informationen zu eduroam gibt es unter: **https://eduroam.org/**

DFN-Dokumentationen sowie Erweiterungen zu eduroam: **https://doku.tid.dfn.de/de:eduroam:about**

Informationen zur FSG-Veranstaltung gibt es unter: **www.formulastudent.de/fsg/**

eduroam an Bord: Die einsitzigen Rennwagen sind auf der Formel-1-Strecke am Hockenheimring am Start
Foto: Axel Grobe/Formula Student Germany

DFN.Security: DNS-RPZ ist in Betrieb

Mit DNS-RPZ (Domain Name System-Response Policy Zone) ist die neueste Erweiterung des Dienstes DFN.Security im März 2024 in Betrieb gegangen. Damit steht eine aktive Abwehrkomponente insbesondere gegen Phishing-Angriffe zur Verfügung.

In dem Verfahren werden bösartige Domains identifiziert und die Informationen dazu nach bestimmten Richtlinien in sogenannten „Response-Policy-Zonen" gelistet und bereitgestellt. Sofern Nutzerinnen und Nutzer eine Domain mit schädlichen Inhalten ansteuern, blockiert ein rekursiver DNS-Resolver – ein Server, der Domainanfragen in IP-Adressen übersetzt und diese Anfragen auswertet – den Zugriff und kann sie wahlweise automatisch auf eine sichere Landingpage umleiten. Nutzende werden auf der Landingpage über den Sachverhalt informiert.

Wenn ein DFN-Teilnehmer die Logdaten des DNS-Resolvers in die Logdatenanalyse von DFN.Security einspeist, werden außerdem Warnmeldungen an die benannten Sicherheitskontakte der Einrichtung erzeugt.

Der zusätzliche Schutz durch DNS-RPZ kann in Ausnahmefällen zu Einschränkungen für Endnutzende führen, wenn eine Domain fälschlicherweise in die zu blockierende Zone eingetragen wurde. Derartige „False Positives" können dem DFN-CERT gemeldet werden, um eine zügige Bereinigung der Zone zu erwirken und den Zugriff auf die Domain wieder freizugeben.

Aktuell werden Teilnehmern Zonen vom Schweizer Forschungsnetz Stiftung →

Sicherheit aktuell

SWITCH und dem DFN-CERT bereitgestellt. Letztere umfassen derzeit noch relativ wenig Daten, sind aber bereits definiert, um bei dem geplanten Ausbau des Dienstbestandteils die Anpassungsaufwände für die Teilnehmer niedrig zu halten. Der Großteil der Nutzdaten wird derzeit über die Zonen von SWITCH ausgeliefert, die mehrere Monate durch das DFN-CERT evaluiert und anschließend durch einen mehrwöchigen Pilotbetrieb mit fünf Teilnehmern getestet wurden.

Voraussetzung für die Nutzung des Dienstmerkmals DNS-RPZ ist die Unterzeichnung der Dienstvereinbarung von DFN.Security (Basisleistungen sind ausreichend) und der Einsatz einer RPZ-fähigen DNS-Software. ◆

Informationen zum neuen Dienstbestandteil sowie Hinweise für Administrierende inklusive eines Konfigurationsbeispiels anhand des DSN-Servers BIND (Berkeley Internet Name Daemon) finden Sie unter: **www.dfn-cert.de/leistungen/security-operations**

Das PDF-Dokument „DNS-RPZ_Grundlegende_Informationen“ enthält ein Formular zur Abfrage der für die Konfiguration notwendigen Teilnehmerdaten. Wenn Sie DNS-RPZ nutzen möchten und die vorgenannten Voraussetzungen bereits erfüllen, senden Sie das ausgefüllte Formular an **dns-rpz@dfn-cert.de**.

Im Anschluss richten wir den Abruf der Zonen für Sie ein und übermitteln Ihnen die Informationen für die Konfiguration.

WLAN-Log-in vereinfachen – ein Blick in die Zukunft

Weg mit Passwörtern! So lautet seit einiger Zeit die Devise beim WLAN-Log-in in WPA2-Enterprise-Netzen wie eduroam. Die komplizierte Konfiguration von WLAN-Endgeräten ist schon seit Langem ein Problem und immer wieder werden Lösungen dafür gesucht. Denn bei einem falsch konfigurierten Endgerät reicht ein schnell eingerichteter bösartiger Access-Point, um das individuelle WLAN-Passwort von Nutzenden auszulesen. Und wenn keine dienstspezifischen Passwörter genutzt werden, erhalten Angreifende Zugriff auf den gesamten Einrichtungsaccount der Betroffenen. Eine Möglichkeit, das Auslesen von Passwörtern zu verhindern, sind zertifikatsbasierte Log-ins. Die Geräte erhalten ein gerätespezifisches Zertifikat, mit dem sie sich im WLAN einloggen. Aber auch das Zertifikat muss konfiguriert werden. Dafür ist ein mehr oder weniger umständlicher Provisionierungsprozess für die verschiedenen Betriebssysteme notwendig. Dazu muss das Zertifikat regelmäßig, meist in manuellen Schritten, erneuert werden.

Was wäre, wenn wir das alles nicht bräuchten? In Kooperation mit dem luxemburgischen Forschungsnetz Restena arbeitet der DFN-Verein an einer neuen Log-in-Methode für WLANs. Als Basis dienen FIDO-Keys. Die FIDO Alliance hat einige Protokolle spezifiziert, die die Sicherheit vor allem im Web verbessern sollen – zunächst mit einer Spezifikation für einen zweiten Faktor (U2F). Später wurde zusammen mit dem W3C der Standard WebAuthn entwickelt, mit dem Passwörter komplett ersetzt werden können. Grundlage hierfür ist eine vertrauenswürdige Umgebung, beispielsweise über einen Hardware-Token oder über eine sichere Implementierung im Kern des Betriebssystems, die asymmetrische Schlüsselpaare generiert und verwaltet.

Für jede neue Registrierung wird ein Schlüsselpaar generiert, auch Credential oder Passkey genannt, das kryptografisch an die spezielle Domain gebunden ist. Im Web bieten immer mehr Webseiten die Möglichkeit, sich statt mit Username und Passwort mit einem Passkey anzumelden.

Passkeys schützen vor einer Vielzahl von Angriffen, beispielsweise vor Phishing und durch die Bindung an die Domain auch vor Imitationen von Webseiten unter einer falschen Adresse.

Aber einen einmal erstellten Passkey könnte man nicht nur für Web-Log-ins nutzen, sondern auch in anderen Szenarien wie dem WLAN-Log-in. Das Praktische daran: Fast jedes aktuelle Endgerät besitzt schon heute die Möglichkeit, Passkeys zu erstellen und zu verwalten. Für den WLAN-Log-in müssen dann keine Zugangsdaten mehr konfiguriert werden. Es fallen aber nicht nur Passwort und ggf. sogar der Username weg, auch die umständliche Konfiguration von Root-Zertifikaten und Servernamen, die immer wieder für Kopfschmerzen bei allen Beteiligten sorgt, ist nicht mehr nötig. Für Server-Admins werden die Konfiguration und Wartung stark vereinfacht, und auch ein Zertifikatswechsel ist bei dieser neuen Log-in-Methode ohne große Umstellungsphase möglich.

Aktuell ist die Log-in-Methode noch in der Designphase und soll bei der Internet Engineering Task Force (IETF) standardisiert werden. Das Interesse ist hoch und damit auch die Hoffnung, dass

Hans-Martin Adler, ehem. Mitarbeiter im DFN: „Kurz nach dem Mauerfall im November 1989 nahmen drei Wissenschaftsinstitutionen der DDR, die TU Dresden, das Institut für Hochenergiephysik (IfH) in Zeuthen (heute DESY) und die Humboldt-Universität zu Berlin Kontakt zum DFN-Verein auf und baten um den Anschluss an das Wissenschaftsnetz. Bereits im Frühjahr 1990 konnten wir die Zugänge über das Institut für Informatik und Rechentechnik (IIR) realisieren, wie durch den „Dresdner Fenstersprung“ dokumentiert ist. Damit legten wir im DFN-Verein den Grundstein zur Integration der wissenschaftlichen Einrichtungen in den neuen Bundesländern.“

diese neue Methode schnell Einzug in die verschiedenen Betriebssysteme erhält. Auch eduroam als weltweit verfügbarer föderierter WLAN-Zugangsservice für die Wissenschaft kann von dieser Entwicklung profitieren. Die Unterstützung von FIDO-Keys hat das große Potenzial, sowohl die Sicherheit als auch die Usability von eduroam weiter zu verbessern. Wie genau die Methode funktioniert und welche Vorteile sie für Nutzende und Admins bringt, werden wir in der kommenden Ausgabe der DFN-Mitteilungen ausführlich vorstellen. ◆

WEITERE INFORMATIONEN:

How FIDO Works: **https://fidoalliance.org/how-fido-works**

Aktueller Internet-Draft bei der IETF: **https://datatracker.ietf.org/doc/draft-janfred-eap-fido**

KONTAKT

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

Mitarbeit an dieser Ausgabe Sicherheit aktuell:
Christine Kahl, Ralf Paffrath, Ralf Gröper, Heike Ausserfeld, Jan-Frederik Rieckers

DFN-PKI Global im Erhaltungsbetrieb

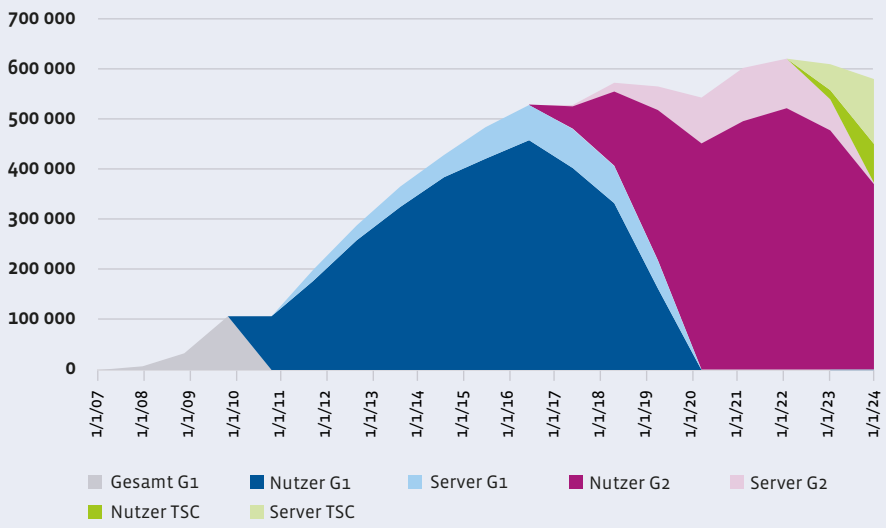
Ende Januar 2024 sind die letzten Serverzertifikate in der DFN-PKI im Sicherheitsniveau Global regulär abgelaufen. Damit ist ein weiterer Meilenstein der Transition in den neu eingeführten Trusted Certificate Service von GÉANT (TCS) sowie in die DFN-Verein Community PKI erreicht.

Da nun die Schwellwerte aus der BSI-Kritisverordnung unterschritten sind, ist die DFN-PKI „Global“ nicht mehr als Kritische Infrastruktur beim BSI registriert.

Die noch gültigen Nutzerzertifikate bleiben weiter gültig und laufen in den kommenden drei Jahren regulär aus. Die DFN-PKI „Global“ ist somit im Erhaltungsbetrieb. Es werden weiterhin Sperrinformationen per Certificate Revocation List (CRL) und Online Certificate Status Protocol (OCSP) bereitgestellt und auch das Audit des Europäischen Instituts für Telekommunikationsnormen (ETSI) und die entsprechende Zertifizierung werden bis zum Ende des Erhaltungsbetriebs aufrechterhalten.

In der Grafik zur Entwicklung ist unter anderem zu erkennen, wie nach einer Phase des stetigen Wachstums der Zertifikatszahlen in der ersten Generation der DFN-PKI Global der Übergang zur zweiten Generation unter einer neuen Root-CA erfolgt ist – und ab 2022 dann der Übergang zu TCS. Durch die jeweilige mehrjährige parallele Bereitstellung der PKIs hat der DFN-Verein diese Umstellungen für die Teilnehmer so wenig disruptiv wie möglich durchgeführt. ◆

NUTZER- UND SERVERZERTIFIKATE



ChatGPT – dein Freund und Helfer in der Prüfung?

Die Bachelor-Studierenden im Kurs „Aerospace Materials Sciences and Processes“ an der TU München haben erstmalig eine digitale Prüfung absolviert, bei der das KI-Tool ChatGPT nicht nur geduldet, sondern explizit erlaubt war. Auf Basis des existierenden Erkenntnisstands zum Chatbot hat das Prüfungsteam ProLehre gemeinsam mit dem Lehrstuhl für Carbon Composites die freiwillige und nicht benotete Pilotprüfung konzipiert und durchgeführt, um erste Erfahrungen im Rahmen einer größeren Klausur sammeln zu können. Die Pilotprüfung wurde im Anschluss mit einem Fragebogen evaluiert.

Text: **Matthias Baume** (TU München)

Sprachmodelle wie deren bekanntester Vertreter „ChatGPT“ haben bereits eine jahrzehntelange Geschichte. Die Anfänge der „Large Language Models“ (LLM) reichen zurück bis in die 1940er-Jahre. Bereits damals entwickelten Wissenschaftler die ersten neuronalen Netze als ein digitales Abbild der biologischen Nervenzellstrukturen. Die Entwicklungen verliefen zu der Zeit weitgehend ohne allgemeines Interesse in der Gesellschaft oder der akademischen Welt zu erregen. Eine erste praktische Anwendung derartiger Sprachmodelle wurde von Joseph Weizenbaum im Jahr 1966 in der Form eines Chatbots – einer Anwendung zum sprachlichen Austausch mithilfe von eingegebenen Sätzen – entwickelt. Sein Chatbot „ELIZA“ imitierte einen Psychologen und konnte bereits einfache natürlich-sprachige Kommunikation bewältigen.

Eine digitale Hörsaalprüfung an der TU München – bald auch mit ChatGPT? | *Foto: TU München*

Prof. Dr. Gerhard Wellein, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), stellv. Vorstandsvorsitzender des NHR-Vereins:
„Schnelle Rechner benötigen schnelle und zuverlässige Netze. Mit seiner Infrastruktur ist der DFN-Verein ein verlässlicher und zukunftsweisender Partner für das Nationale Hochleistungsrechnen (NHR). Wir vom NHR-Verein fühlen uns dem DFN besonders verbunden – er hat uns aus der Taufe gehoben und zum Laufen gebracht. Dafür sind wir dem DFN besonders dankbar. Mit Blick auf Themen wie künstliche Intelligenz und Forschungsdaten freuen wir uns auf die weitere Zusammenarbeit."

Der große Durchbruch in der Öffentlichkeit gelang im Jahr 2022 durch das deutlich weiter entwickelte und komplexere Sprachmodell „ChatGPT" der Firma OpenAI. Dieses mit etwa 175 Milliarden Parametern und circa 300 Milliarden Textelementen ausgestattete Modell konnte nun eine flüssige Unterhaltung führen und vielerlei praktische Anfragen sowie unterschiedlichste Aufgabenstellungen erledigen – und ebnete KI fast über Nacht den Weg in nahezu alle Bereiche des öffentlichen Wirkens wie auch in die gesamte Bildungslandschaft. Weitere große Sprachmodelle (zum Beispiel 2018 BERT, 2022 LaMDA von Google oder 2023 Llama von Meta) wurden entwickelt und mit immer komplexeren Datenbeständen trainiert.

Einsatz großer Sprachmodelle im Bildungsbereich

Große Sprachmodelle können mittlerweile in vielen beruflichen wie auch privaten Aktivitäten sowie insbesondere im Bildungsbereich eine Vielzahl an Unterstützung bereitstellen: Für Lehrende erstellt ChatGPT auf Wunsch geeignete Unterrichtsskizzen, Übungsaufgaben oder auch Fallbeispiele für den Unterricht. Das Modell kann Prüfungen konzipieren, Erläuterungen alters- und bedarfsgerecht verfassen oder sogar einen einfachen Programmiercode schreiben und verbessern. Lernende kann das Sprachmodell dabei unterstützen, Texte zusammenzufassen oder schwierige Textpassagen einfacher zu formulieren. Es kann beim Verstehen von vorhandenen Aufgabenstellungen helfen, Übersetzungen erstellen oder zu einem konkreten Unterrichtsstoff passende Fragen formulieren.

Trotz der häufig überzeugend wirkenden Antworten und Texte ist bei der praktischen Arbeit mit großen Sprachmodellen, insbesondere bei Faktenwissen, Vorsicht geboten.

> Bei der Arbeit mit Sprachmodellen, insbesondere bei Faktenwissen, ist Vorsicht geboten.

Die Modelle liefern zwar gut formulierte und häufig sehr verständliche und passende Rückmeldungen, diese sind jedoch nicht auf Denkprozesse zurückzuführen, sondern stellen das Ergebnis einer hochkomplexen, wahrscheinlichkeitsbasierten Zusammenstellung von vorher verarbeiteten Trainingsdaten dar. Somit ist es durchaus möglich, dass zwar sinnvolle, aber dennoch falsche Informationen als Antwort auf eine eingegebene Frage ausgegeben werden.

ChatGPT in Prüfungen

Ein viel diskutiertes Thema der vergangenen Monate ist das Spannungsfeld „ChatGPT in Prüfungen". Daraus ergeben sich verschiedene Optionen der praktischen Herangehensweise:

- **Ausweichen:** Da verschiedene traditionelle Prüfungsformen wie mündliche Prüfungen oder Prüfungen mit Papier und Stift für den ChatGPT-Einsatz kaum oder überhaupt nicht geeignet sind, kehren einige Dozierende zurück zu klassischen Papierprüfungen, weg von digitalen Prüfungsformen, um die Möglichkeit der KI-Nutzung auf diese Weise zu umgehen.
- **Verbieten:** Prinzipiell ist es aus Sicht verschiedener rechtlicher Einschätzungen zulässig, die ChatGPT-Nutzung durch eine entsprechende Erklärung für eine Prüfung zu verbieten. Unklar ist jedoch, wie insbesondere bei unbeaufsichtigten Onlineprüfungen ein zweifelsfreier Nachweis erbracht werden kann.
- **Dulden oder ignorieren:** Diese Herangehensweise wird häufig in der Praxis genutzt. Fraglich ist hierbei jedoch, wie im Täuschungsfall vorzugehen ist, wenn für die Prüfung keine Rechtssicherheit (wie ein Verbot) geschaffen wurde.
- **Erlauben:** Vielfach diskutiert wird die Vorstellung, ChatGPT innerhalb der Prüfung zu erlauben bzw. sogar aktiv einzubringen. Hierbei sind allerdings verschiedene Rahmenbedingungen zu beachten, wie das Sicherstellen einer eigenständigen Prüfungsleistung sowie die Gleichstellung der Studierenden bzgl. des eingesetzten Sprachmodells.

Insbesondere für den letztgenannten Fall gibt es jedoch kaum praktische Erfahrungen und Erkenntnisse, wie Studierende konkret mit ChatGPT arbeiten oder welche Voraussetzungen für eine sinnvolle und erfolgreiche ChatGPT-Prüfung notwendig sind.

Konzept und Inhalt der ChatGPT-Pilotprüfung

Die aktuellen Entwicklungen in Bezug auf den unterstützenden Einsatz von KI in summativen Prüfungen führten beim Prüfungsteam von ProLehre an der TU München zu dem Entschluss, auf der Basis des existierenden Erkenntnisstands eine „Pilot-ChatGPT-Prüfung" zu konzipieren, durchzuführen und zu evaluieren. Ziel dieser freiwilligen und nicht benoteten Pilotprüfung war es, erste Erfahrungen mit einer größeren Klausur zu sammeln, in der ChatGPT explizit eingebunden und teilweise zum Bearbeiten der Aufgabenstellungen erforderlich ist. Die Pilotprüfung wurde im Anschluss mit einem speziellen Fragebogen evaluiert, um nicht nur die Prüfungsergebnisse der Studierenden, sondern auch deren individuelle Erfahrungen bei der Nutzung von ChatGPT im Prüfungskontext aufgreifen zu können.

Den inhaltlichen Rahmen für die Prüfung lieferte das englischsprachige Bachelorseminar „Aerospace Materials Sciences and Processes" des Lehrstuhls für Carbon Composites. Die Prüfung selbst beinhaltete mehrere fachspezifische Fragen zum bisherigen Unterrichtsstoff der Studierenden, jedoch wurden zwei unterschiedliche Fragenausprägungen gewählt: Ein Teil der Fragen konnte (beim Beherrschen des Lernstoffs) gut ohne ChatGPT beantwortet werden, für mehrere andere Fragen war ChatGPT hilfreich oder sogar erforderlich.

> Die Pilotprüfung wurde im Anschluss mit einem Fragebogen evaluiert.

Im Moodle-Prüfungskurs war eine ChatGPT-Eingabemöglichkeit während der gesamten Prüfung für alle Teilnehmenden verfügbar und jederzeit nutzbar. Die Prüflinge konnten somit vollkommen eigenständig entscheiden, ob und wann sie das Sprachmodell als Unterstützung heranziehen wollten.

Was ist bei der Pilotprüfung herausgekommen?

Die teilnehmenden Studierenden bearbeiteten die Aufgaben der Prüfung sehr konzentriert und ein großer Teil (99 von 116) beantwortete auch den begleitenden Fragebogen. Dabei ergab sich eine Vielzahl neuer Erkenntnisse zur Nutzung von KI-Tools und im Speziellen zum Einsatz von ChatGPT in der Prüfung.

Die Ergebnisse fielen – verglichen mit einer typischen Abschlussklausur – von der Punkteverteilung ähnlich aus, jedoch war die Prüfung aufgrund des Pilotcharakters

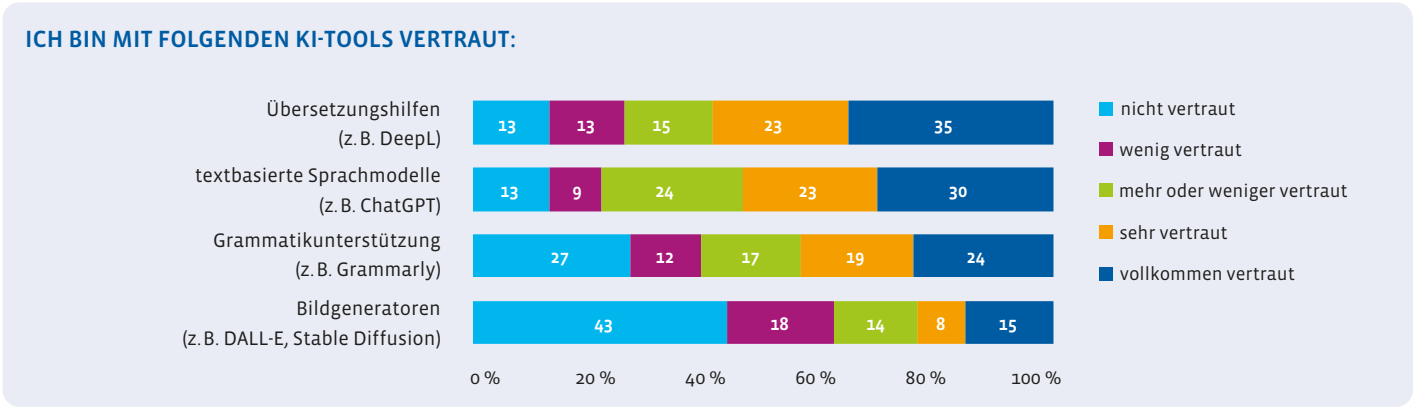


Abbildung 1: Vertrautheit mit KI-Tools (n=99)

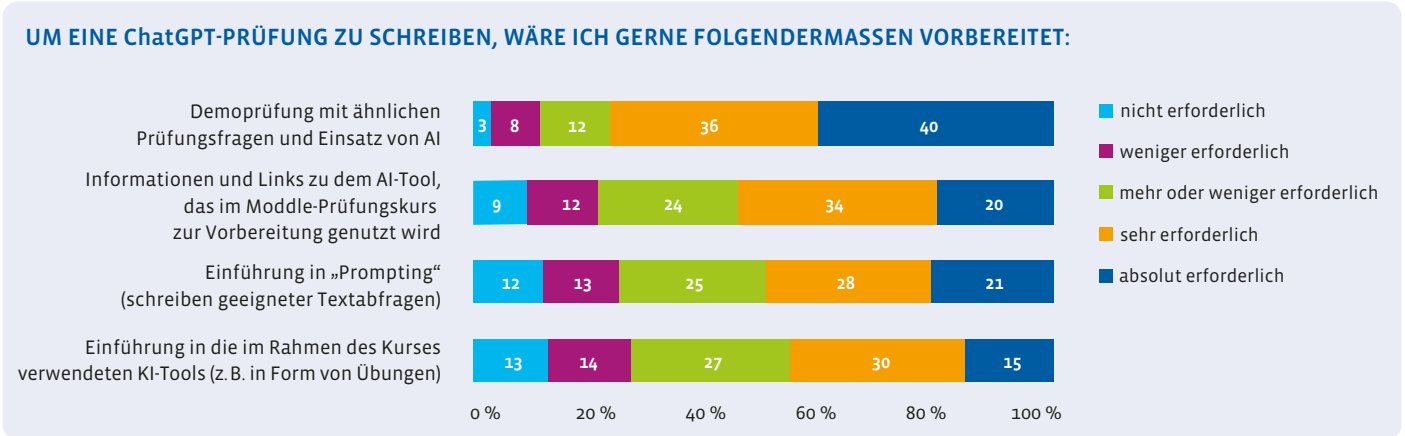


Abbildung 2: Vorbereitung auf eine ChatGPT-Prüfung (n=99)

Angela Lenz, Mitarbeiterin im DFN: „Als ich 2004 zur 20-Jahr-Feier des DFN-Vereins meinen ersten Auftritt hatte, habe ich ja nicht geahnt, was auf mich zukommen wird: unfassbar schöne Momente, so viele liebe Menschen, eine Gemeinschaft, die Erfolge feiert und an Herausforderungen gemeinsam arbeitet, in der wir oft Tränen lachen oder auch mal weinen. Jetzt feiern wir alle gemeinsam die 40 Jahre des DFN-Vereins. Ich freu mich einfach, ein kleiner Teil davon zu sein und auf die nächsten Jahrzehnte. Eine dicke Umarmung für alle!“

deutlich kürzer und daher nicht vollkommen vergleichbar.

Vertrautheit mit KI-Tools

Die Befragten sind in Bezug auf KI-Tools, besonders mit Übersetzern und textbasierten Sprachmodellen, vertraut. Die geringsten Erfahrungen haben die Teilnehmenden mit KI-Bildgeneratoren wie DALL-E oder Stable Diffusion (Abbildung 1).

Vorbereitung auf eine ChatGPT-Prüfung

Um gut vorbereitet zu sein, wünscht sich der Großteil der Befragten insbesondere eine Demo-Prüfung mit ähnlichen Prüfungsfragen wie sie in der Prüfung selbst gestellt werden (Abbildung 2).

Anscheinend immer noch notwendig sind zusätzliche Informationen zu den KI-Tools sowie eine Einführung ins „Prompten“, das heißt das Verfassen möglichst passender Textanfragen. Weniger als die Hälfte der Teilnehmenden möchten im Kurs explizit in die verwendeten Tools eingeführt werden. Eine derartige Einführung würde sicherlich einige Zeit in Anspruch nehmen, die möglicherweise beim Erlernen der eigentlichen Seminarinhalte dann fehlt.

Nutzung von ChatGPT für Prüfungsfragen

Obwohl ChatGPT nicht für jede der Prüfungsfragen erforderlich war, wurde das Tool bei allen Fragen (zumindest von einem Teil der Studierenden) genutzt. Jedoch erfolgte der Einsatz von ChatGPT hier in unterschiedlicher Intensität: Während beispielsweise bei Frage 1 (ChatGPT nicht erforderlich) nur 32 Teilnehmende ChatGPT für die Lösung in Anspruch nahmen, nutzten bei den Fragen 2 und 5 (ChatGPT hilfreich bzw. erforderlich) mehr als die Hälfte ChatGPT als Unterstützung (Abbildung 3).

Dies zeigt, dass die Prüflinge tendenziell auch diejenigen Fragen bevorzugt mit dem Sprachmodell bearbeiten, die sie selbst nicht ohne Hilfe beantworten können.

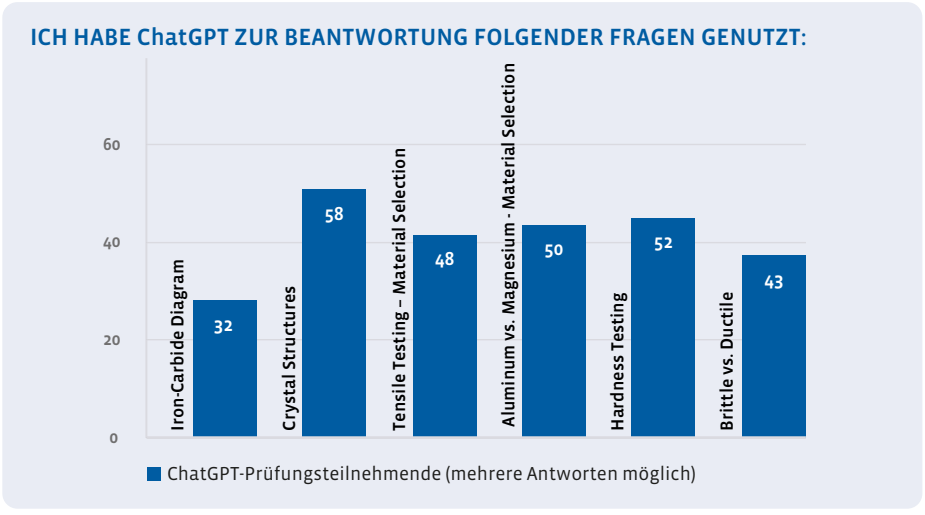


Abbildung 3: Beantwortung der Prüfungsfragen mit ChatGPT

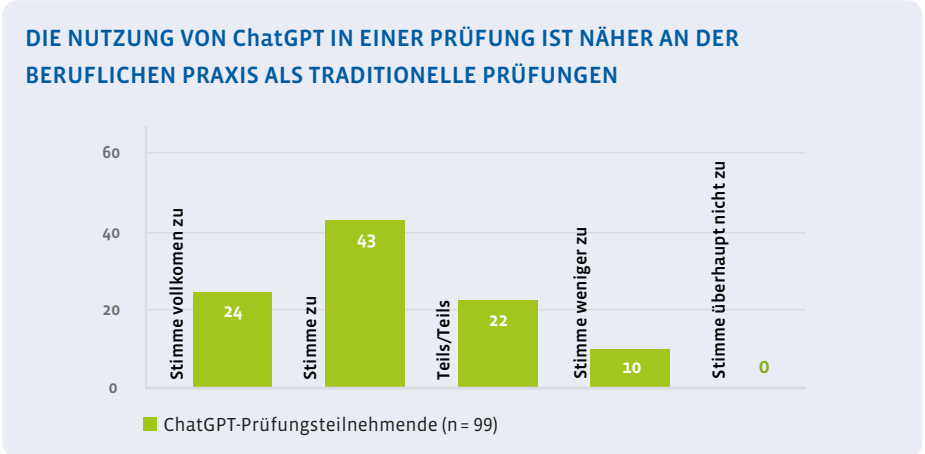


Abbildung 4: Vorbereitung einer ChatGPT-Prüfung auf die spätere Berufstätigkeit

Nutzen einer ChatGPT-Prüfung für die spätere Berufstätigkeit

Innerhalb der durchgeführten Befragung ist u. a. eine Frage relativ spannend: Wie sehen die Teilnehmenden den Nutzen derartiger

Prüfungen für die spätere Berufstätigkeit? (Abbildung 4, S. 49)

Hier zeigt sich, dass ein großer Teil der Prüflinge (67 %) damit (sehr) übereinstimmt, dass eine ChatGPT-Prüfung näher auf die spätere Berufstätigkeit vorbereitet als eine entsprechende „klassische" Hochschulprüfung. Nur zehn Prozent der Befragten sind hierbei anderer Ansicht.

Es wird klar ersichtlich, dass es weitere Erfahrungen – sowohl vonseiten der Dozierenden als auch vonseiten der Studierenden – mit derartigen Prüfungen bedarf, um eine möglichst sinnvolle Einschätzung der neuen Prüfungsform zu erhalten.

Fazit

Die rasanten Entwicklungen von Sprachmodellen und deren Einsatz im Bildungsbereich haben bereits in den vergangenen Monaten deutliche Spuren hinterlassen. Viele Einsatzfelder werden diskutiert, einige davon auch bereits aktiv in den Studienalltag einbezogen. Prüfungen kommt hierbei eine Sonderrolle zu, denn Neuerungen und Experimente sind in diesem Themenfeld nicht immer einfach umzusetzen. Dies gilt auch für Prüfungen mit der aktiven Einbindung von ChatGPT oder anderen Sprachmodellen.

Für derartige Prüfungen werden in jedem Fall einige Lerneffekte bei allen Beteiligten erforderlich sein: Prüfungsverantwortliche müssen die passenden Rahmenbedingungen schaffen und Aufgabenstellungen konzipieren, bei denen – trotz KI-Einsatz – eine sinnvolle Bewertungsgrundlage für die Prüflinge und deren Kenntnisstand gegeben ist. Studierenden werden – ähnlich wie beim ersten Einsatz eines Taschenrechners – zunächst Erfahrungen zur sinnvollen und effektiven Nutzung sammeln müssen. Denn viele Aufgabenstellungen lassen sich letztlich am schnellsten und effizientesten mit einem gut gelernten und schnell abrufbaren Wissensschatz als Basis lösen.

WIE SEHEN DOZIERENDE UND MITARBEITENDE DEN EINSATZ VON CHATGPT IN HOCHSCHULPRÜFUNGEN?

Hier gibt es sehr unterschiedliche Sichtweisen: Während einige wenige Dozierende sich den Einsatz von ChatGPT in Prüfungen vorstellen können oder sogar schon konkrete Umsetzungspläne haben, stehen andere den Entwicklungen im Bereich der KI in Prüfungen eher zurückhaltend bis ablehnend gegenüber.

Dr.-Ing. Daniel Renjewski

„Im kommenden Sommersemester halte ich eine Lehrveranstaltung ‚Angewandte Biorobotik', in der ich erstmals ChatGPT aktiv einsetzen möchte. Die Bewertungen finden in Form einer Portfolioprüfung mit mehreren Teilnoten statt und ChatGPT kann hierbei jederzeit von den Studierenden genutzt werden. Auch das Potenzial, die Bewertung der Abgaben durch ChatGPT zu unterstützen, möchte ich testen. Wir werden die Studierenden mehrfach während des Semesters befragen und ich bin schon sehr gespannt, welche Erfahrungen alle Beteiligten mit diesem neuen Konzept machen werden!"

Carina Schauer

„Sprachmodelle wie ChatGPT werden in der Arbeitswelt und im akademischen Bereich eine immer größere Rolle einnehmen. Es ist daher wichtig, Studierende auf ihre zukünftigen Anforderungen vorzubereiten, um gezielt und effektiv Aufgabenstellungen mit KI-Unterstützung zu lösen. Studierende haben in der Umfrage im Rahmen der ChatGPT-Pilotprüfung angegeben, dass sie sich darauf nicht hinlänglich vorbereitet fühlen. Daher sollte vorrangig in praxisnahen Übungseinheiten der Umgang mit KI-Tools vermittelt und im nächsten Schritt in Prüfungen mit KI-Einsatz unter Beweis gestellt werden."

Apl. Prof. Dr. Felix Ehrlenspiel

„Ich verfolge die KI-Entwicklungen interessiert, bisher hat sich dies aber noch nicht auf meine Prüfungen ausgewirkt. Derzeit ist mir wichtig, dass wir digitale Prüfungen auch in größeren Kohorten reibungslos z. B. im Hörsaal abwickeln können. Der ChatGPT-Einsatz ist hierbei nicht zugelassen und wir müssten den entsprechenden Prüfungsversuch beenden, falls ein Prüfling offensichtlich unerlaubte KI-Tools in der Prüfung einsetzt."

Peter Castellaz, Leiter des Referats 42 im Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg: „Schon seit über 13 Jahren kenne und schätze ich den DFN als aufrichtigen und verlässlichen Kooperationspartner des Landes Baden-Württemberg und unseres Landeshochschulnetzes BelWü. Der Beginn dieser sehr erfolgreichen Kooperation reicht zurück in die 80er-Jahre des vorigen Jahrhunderts. Ich gratuliere herzlich zum Jubiläum und freue mich auf die nächsten 40 Jahre!“

Ohne sinnvolle Nutzungsstrategie wird die zunächst als Heilsbringer wahrgenommene KI in der Prüfung schnell zur Überforderung. Derartige Tendenzen ließen sich auch in der Pilot-ChatGPT-Prüfung an der TU München ganz klar wahrnehmen. Mehrere der Prüfungsaufgaben, die bereits in „echten“ Prüfungen eingesetzt wurden, lieferten dort tendenziell bessere Punktzahlen als mit ChatGPT-Nutzung. Der intensive KI-Einsatz kostet in der Prüfung möglicherweise einfach zu viel Zeit. Denn die notwendigen Schritte wie „Aufgabenstellung in die KI-Maske reinkopieren“, „KI-Ausgabe abwarten“, „Ausgabe bewerten“, „Passendes in die Prüfung übernehmen“ etc. sind häufig weniger effizient als Gelerntes aus dem Kopf abzurufen.

Dennoch zeigt sich aus der Befragung der Prüflinge klar der wahrgenommene Mehrwert derartiger Prüfungen für die zukünftige Arbeit und das Berufsleben. Es ist mit hoher Wahrscheinlichkeit anzunehmen, dass KI-Tools in ein immer breiteres Spektrum der Arbeitswelt integriert werden. Die effektive Arbeit mit KI zur Lösung von Aufgabenstellungen – auch unter Zeitdruck – wird möglicherweise eine immer wichtigere Kompetenz darstellen.

Die Bandbreite von Meinungen zum KI-Einsatz aufseiten der Studierenden und auch der Dozierenden ist nach wie vor groß und es wird ersichtlich, dass ChatGPT-Prüfungen noch lange nicht im Hochschulalltag angekommen sind. Die Prüfung an der TU München kann jedoch ein erster Schritt auf „Neuland“ sein, um mehr Erkenntnisse zum KI-Einsatz in dem sensiblen und zugleich für den Studienabschluss hochrelevanten Thema Prüfungen zu sammeln und die bisherigen Ideen weiterzuentwickeln. In einigen Monaten, nach weiteren Erfahrungen und Evaluationen wird sich zeigen, inwieweit Prüfungen mit aktiver Einbindung von Sprachmodellen und anderen KI-Tools im Prüfungsgeschehen eine höhere Akzeptanz erfahren werden oder ob traditionelle Prüfungsformen weiterhin die Norm sind. ◆

AUSGEWÄHLTE LITERATUR ZUM THEMA

1. **Baume, Matthias; Dörfler, Eva; Etchegaray Bello, Margarita; Schauer, Carina (2024):** Summative Exams with the Use of ChatGPT. Vision or realistic Alternative to traditional Exams? In: Louis Gómez Chova, Chelo González Martínez und Joanna Lees (Hg.): INTED 2024. Conference proceedings: 18th annual International Technology, Education and Development Conference: 4-6 March 2024, Valencia (Spain). Valencia: IATED Academy (INTED proceedings (Internet)), S. 3980–3990. Online verfügbar unter **https://library.iated.org/publications/INTED2024**, (zuletzt geprüft am 12.04.2024).
2. **Fleck, Tilmann (2023):** Prüfungsrechtliche Fragen zu ChatGPT. Handreichung der Stabsstelle IT-Recht der bayerischen Universitäten. Hg. v. Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen. Online verfügbar unter **www.rz.uni-wuerzburg.de/fileadmin/42010000/it-recht/ChatGPT_Pru__fungsrecht_v2.pdf**, (zuletzt geprüft am 21.12.2023)
3. **Fleischmann, Andreas (2023):** ChatGPT in der Hochschullehre. Wie künstliche Intelligenz uns unterstützen und herausfordern wird. Hg. v. Neues Handbuch Hochschullehre. Online verfügbar unter **www.nhhl-bibliothek.de/de/handbuch/gliederung/#/Beitragsdetailansicht/243/3700/ChatGPT-in-der-Hochschullehre---Wie-kuenstliche-Intelligenz-uns-unterstuetzen-und-herausfordern-wird**, (zuletzt geprüft am 21.12.2023).
4. **Heckmann, Dirk (2023):** Examen mit oder trotz ChatGPT? Ideen für einen rechtssicheren Prüfungskulturwandel. Multimedia Kontor Hamburg. Online, 14.03.2023. Online verfügbar unter **www.mmkh.de/fileadmin/veranstaltungen/netzwerk_landesinitiativen/KI-Generatoren/2023-03-14_KI-Generatoren_Heckmann.pdf**, (zuletzt geprüft am 25.01.2024).
5. **Weizenbaum, Joseph (1966):** ELIZA - a computer program for the study of natural language communication between man and machine. In: Commun. ACM 9 (1), S. 36–45. DOI: 10.1145/365153.365168.

Bei Fragen zum Einsatz von ChatGPT in digitalen Prüfungen erreichen Sie das Team der zentralen wissenschaftlichen Einrichtung ProLehre | Medien und Didaktik der TU München unter: **info@prolehre.tum.de**

Ich glaub, es hackt

EuGH-Urteil zu Haftungsrisiken infolge eines Hackerangriffs: Angst vor Datenmissbrauch als immaterieller Schaden

Der Europäische Gerichtshof (EuGH) – Urteil vom 14.12.2023 – C-340/21[1] – hat sich in jüngster Zeit mit den Voraussetzungen und Rechtsfolgen eines datenschutzrechtlichen Schadensersatzanspruchs aufgrund eines Verstoßes gegen die IT-Sicherheitspflichten beschäftigt. Das Urteil stärkt das Verständnis für Haftungsrisiken, die bei Datensicherheitsverstößen auftreten können.

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

Foto: baona/Adobe Stock

1 Die Pressemitteilung des EuGHs zum Urteil kann unter dem folgenden Link nachgelesen werden https://curia.europa.eu/jcms/jcms/p1_4220393/de/ (zuletzt abgerufen am 08.03.2024).

Dr. Peter Kaufmann, Mitarbeiter im DFN: „Wir schreiben das Jahr 1990. Unangefochten hält die Deutsche Bundespost (DBP) das Netzmonopol mit Transferraten von 64-Kbit/s Datex-P und 2*64-Kbit/s ISDN. Beim DFN sind wir beim Übergang auf 2 Mbit/s und experimentieren im Testbed zwischen der Uni Erlangen und dem LRZ bereits mit 10 Mbit/s. Daraufhin die ungläubige Frage von der DBP, deren Kupferleitungen wir für das Wissenschaftsnetz brauchen: „Welche Nutzer können denn damit etwas anfangen? Das braucht doch niemand!“ Ende der Geschichte: Wir nahmen die Testleitung damals dennoch erfolgreich in Betrieb – und damit begann die Ära der Hochgeschwindigkeitsdatennetze im DFN.“

I. Haftungsrisiken aufgrund von Verstößen gegen die Datensicherheit

Cybersicherheit ist infolge der hohen Anzahl von Hackerangriffen in der jüngsten Zeit immer stärker ins öffentliche Bewusstsein gerückt.[2] Als mögliche finanzielle Schäden eines Cybersicherheitsangriffs sind der Kontrollverlust über wertvolle Daten und mögliche Lösegeldforderungen von Hackern weitestgehend bekannt. Darüber hinaus darf jedoch das Risiko einer zivilrechtlichen Haftung nicht vernachlässigt werden. Dies kann in Form eines datenschutzrechtlichen Schadensersatzanspruchs gemäß Art. 82 Datenschutz-Grundverordnung (DSGVO) geltend gemacht werden. Der datenschutzrechtliche Schadensersatzanspruch ist die momentan wohl am stärksten diskutierte Thematik im Datenschutzrecht. In letzter Zeit sind mehrere Urteile zu der Frage ergangen, unter welchen Voraussetzungen nicht nur materielle, sondern auch immaterielle Schäden eines Datenschutzverstoßes zu ersetzen sind.[3] Ein solcher Datenschutzverstoß kann auch durch einen Hackerangriff erfolgen. Werden dabei personenbezogene Daten „gestohlen“, ist es möglich, dass die betroffenen Personen den Verantwortlichen in Anspruch nehmen, dessen Dateisystem infolge unzureichender Schutzmaßnahmen gehackt wurde.

II. Anforderungen an die Datensicherheit in Art. 32 DSGVO

Art. 32 DSGVO trifft Regelungen zu den Sicherheitsanforderungen, die der Verantwortliche einer Datenverarbeitung für personenbezogene Daten treffen muss. Diese dienen dem Schutz von personenbezogenen Daten, sollen also gemäß Art. 4 Nr. 12 DSGVO die Vernichtung, den Verlust, die Veränderung oder die Offenlegung von personenbezogenen Daten verhindern, sofern diese unbeabsichtigt oder rechtswidrig wären. Art. 32 Abs. 1 DSGVO trägt gemeinsam mit Art. 24 DSGVO den Verantwortlichen und Auftragsverarbeitern auf, technische und organisatorische Maßnahmen (kurz TOMs) festzulegen, um ein angemessenes Schutzniveau sicherzustellen. Verantwortliche und Auftragsverarbeiter müssen die Risiken ihrer jeweiligen Verarbeitung reflektieren und risikoadäquate Maßnahmen ergreifen, die zu einem möglichst hohen Maß an Datensicherheit führen. Aus Art. 32 Abs. 1 DSGVO lässt sich ein Katalog verschiedener TOMs entnehmen, der nicht abschließend ist. Er gliedert sich in konkrete Maßnahmen wie z. B. die Pseudonymisierung (Abs. 1 lit. a) und in abstrakte Maßnahmen, die eher Zielvorgaben ähneln (lit. b und c). Welche Maßnahmen Verantwortliche und Auftragsverarbeiter ergreifen, steht grundsätzlich in ihrem eigenen Ermessen, sofern sie ein dem Risiko angemessenes Schutzniveau gewährleisten. Die Orientierung des Schutzniveaus an dem Risiko im Einzelfall ist als Ausprägung des risikobasierten Ansatzes einzuordnen, der sich in der DSGVO häufig findet.

Werden die erforderlichen, dem Sicherheitsrisiko entsprechenden Pflichten verletzt, liegt ein Verstoß gegen Art. 32 DSGVO vor. Resultiert dieser in einem Sicherheitsvorfall, der den betroffenen Personen einen Schaden zufügt, können diese gemäß Art. 82 DSGVO Schadensersatz verlangen. Zu den konkreten Anforderungen hat nun der EuGH Stellung genommen.

III. Sachverhalt des EuGH-Urteils

Infolge eines Cyberangriffs auf die bulgarische Nationale Agentur für Einnahmen (NAP) wurden 2019 personenbezogene Daten von mehr als sechs Millionen Personen im Internet veröffentlicht. Einige Hundert von ihnen, darunter die Klägerin des Ausgangsverfahrens, verklagten daraufhin die NAP auf der Grundlage von Art. 82 DSGVO auf Ersatz des entstandenen immateriellen Schadens. Dieser ergebe sich aus einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO und insbesondere aus einer Verletzung der Sicherheit, die dadurch verursacht worden sei, dass die NAP gegen ihre Verpflichtungen aus Art. 5 Abs. 1 Buchst. f sowie aus Art. 24 und 32 DSGVO (TOMs) verstoßen habe. Der Schaden der Klägerin bestehe in der Befürchtung, dass ihre personenbezogenen Daten künftig missbräuch-

2 Vgl. John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?, DFN-Infobrief Recht 04/2023.

3 Vgl. Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht, 07/2023; ausführlich zum Ersatz immaterieller Schäden infolge eines Datenschutzverstoßes, Müller, Morgen Kinder werden wir klagen, DFN-Infobrief Recht 12/2022.

Thomas H. Brunner, ehem. Geschäftsführer des Schweizer Forschungsnetzes, Stiftung Switch, ehem. Mitglied im Strategischen Beirat des DFN: „Am Anfang der Wissenschaftsnetze in Europa haben wir Schweizer viel vom großen Bruder DFN gelernt. Heute sind wir stolz, dass der DFN auch vom kleinen Switch zum Beispiel das AAI-Konzept übernommen hat. Von Beginn an haben wir uns zusammen mit unserem lieben Kollegen Klaus Ullmann stark für die Zusammenarbeit der europäischen Wissenschaftsnetze eingesetzt, es hat via RARE, TERENA und DANTE zum heutigen GÉANT geführt. Ich hoffe, der DFN wird in den nächsten 40 Jahren diesen Erfolg weiter tatkräftig unterstützen."

lich verwendet würden. Die NAP verteidigte sich und legte unter anderem Dokumente zum Nachweis dafür vor, dass sie alle erforderlichen TOMs ergriffen habe. Ihrer Ansicht nach seien Angst und Befürchtungen zudem auch nicht als immaterielle Schäden ersatzfähig. Überdies könne sie nicht für die schädlichen Folgen dieser Verletzung verantwortlich gemacht werden, da sie selbst durch Personen, die nicht ihre Bediensteten seien, böswillig geschädigt worden sei.

Das erstinstanzliche Verwaltungsgericht der Stadt Sofia schloss sich der Auffassung der NAP an und wies die Klage mit Entscheidung vom 27. November 2020 ab.

Die Klägerin des Ausgangsverfahrens legte gegen diese Entscheidung Kassationsbeschwerde beim Obersten Verwaltungsgericht in Bulgarien ein. Sie stützt ihr Rechtsmittel darauf, dass das erstinstanzliche Gericht bei der Verteilung der Beweislast hinsichtlich der von der NAP ergriffenen Sicherheitsmaßnahmen einen Rechtsfehler begangen habe. Ferner sei die Befürchtung eines möglichen künftigen Missbrauchs ihrer personenbezogenen Daten ein tatsächlicher immaterieller und kein hypothetischer Schaden.

IV. Relevante Rechtsfragen

Das Oberste Verwaltungsgericht Bulgarien legte dem Europäischen Gerichtshof mehrere Rechtsfragen vor. Besonders relevant ist die Frage, ob jede unbefugte Offenlegung von Daten einen Verstoß gegen die Anforderungen in Art. 24 und 32 DSGVO indiziert. Ihre Bejahung durch den EuGH würde bedeuten, dass bei jedem erfolgreichen Hackerangriff, der personenbezogene Daten betrifft, ein Pflichtenverstoß des verantwortlichen Datenverarbeiters anzunehmen ist. Für den Fall, dass der EuGH die Frage verneint, wollte das Oberste Verwaltungsgericht in Bulgarien wissen, wer die Beweispflicht dafür trägt, dass die Maßnahmen zur Wahrung der Datensicherheit angemessen im Sinne von Art. 32 DSGVO waren.

Darüber hinaus wurden relevante Fragen zum Schadensersatzanspruch nach Art. 82 DSGVO gestellt. Der EuGH sollte die Frage beantworten, ob bei einem Verstoß von Dritten gegen die DSGVO der Verantwortliche selbst von der Haftung befreit wird. Bei Bejahung dieser Frage wären die Haftungsrisiken eines Datenverarbeiters durch einen Hackerangriff weitestgehend reduziert, da die unmittelbare Offenlegung der Daten durch die Hacker und nicht durch die Verantwortlichen der Datenverarbeitung erfolgte. Darüber hinaus wollte das nationale Gericht wissen, ob Sorgen, Befürchtungen und Ängste einer von einem Hackerangriff betroffenen Person vor einem möglichen künftigen Missbrauch der personenbezogenen Daten einen immateriellen Schaden darstellen.

V. Das Urteil des EuGHs

Der EuGH stellte zunächst klar, dass nicht jede unbefugte Offenlegung personenbezogener Daten für die Annahme genügt, dass die getroffenen technischen und organisatorischen Maßnahmen ungeeignet im Sinne von Art. 24 und 32 DSGVO waren. Dies begründet er unter anderem damit, dass der Unionsgesetzgeber die Sicherheitsrisiken lediglich „eindämmen" wollte, ohne zu behaupten, dass sie vollkommen beseitigt werden würden. Diese Ansicht des EuGHs entlastet die Haftungsrisiken von Datenverarbeitern erheblich. Nicht jeder Cybersicherheitsvorfall erlaubt hiernach den Rückschluss, dass der Verantwortliche seine Sicherheitsrisiken verletzt hat.

Zu der Beweislast bezüglich der Angemessenheit der Maßnahmen führt der EuGH aus, dass diese bei dem verantwortlichen Datenverarbeiter liegt. Er muss demnach nachweisen, dass TOMs, die er getroffen hat, ein angemessenes Datensicherheitsniveau gewahrt haben. Denn gem. Art. 5 Abs. 2 DSGVO gilt, dass der Verantwortliche nachweisen können muss, dass er die in Art. 5 Abs. 1 DSGVO aufgestellten Grundsätze einhält. Zu diesen Grundsätzen zählt auch die durch Art. 32 DSGVO konkretisierte Pflicht zur Einhaltung der Datensicherheit. Ebenso lasse sich dem Wortlaut von Art. 24 und Art. 32 DSGVO entnehmen, dass dem Verantwortlichen die Beweislast zur Einhaltung der Schutzpflichten obliege. Darüber hinaus würde der datenschutzrechtliche Schadensersatzanspruch seine Wirkung teilweise verlieren, wenn die betroffene Person als Klä-

Jürgen Grothe, Referent im Referat 33 des Sächsischen Staatsministeriums für Wissenschaft, Kultur und Tourismus, ständiger Gast im DFN-Verwaltungsrat:
„Im Zuge der „Ost-Erweiterung“ des Wissenschaftsnetzes in der Variante ERWiN begegnete ich dem DFN-Verein 1991 erstmalig als junger Assistent am Dresdner Referenzzentrum – und bin ihm seitdem verbunden. Ich erinnere mich, dass ich damals die erforderlichen BNC-Kabel zu meinem PC selbst an die Wand nagelte. Es waren abenteuerliche Zeiten: mit 9,6 Kbit/s an der Welt angeschlossen zu sein – ein Wunder und Erlebnis. X.25 galt als großer Fortschritt. Nun ist der DFN erwachsen und in die besten Jahre gekommen. WiN/ERWiN, B-, G- und X-WiN – und immer kommt noch etwas Neues und Hilfreiches aus diesem Verein: eine stabile, innovative und sichere Datennetz-/Dienste-Entwicklung als Selbstversorgung für die Wissenschaft. Gerne weiter so! Danke.“

ger nachweisen müsste, dass der Verantwortliche seine Pflichten nicht eingehalten hat.

Zum Schadensersatzanspruch selbst hat der EuGH ausgeführt, dass der Verantwortliche von seiner Schadensersatzpflicht nach Art. 82 Abs. 1 und 2 DSGVO nicht allein deshalb befreit ist, weil dieser Schaden Folge einer unbefugten Offenlegung von personenbezogenen Daten durch „Dritte“ im Sinne von Art. 4 Nr. 10 DSGVO ist. Sofern also Cyberkriminelle selbst unmittelbar verantwortlich für einen Datenschutzverstoß sind, steht dies einer Haftung des Datenverarbeiters nicht entgegen, sofern dieser seine Pflichten aus Art. 24 und 32 DSGVO verletzt hat.

Zum Inhalt eines möglichen Schadensersatzanspruchs gegen den Datenverarbeiter gab der EuGH an, dass als immaterieller Schaden bereits die Befürchtung in Betracht käme, dass personenbezogene Daten durch Dritte missbräuchlich verwendet werden könnten. Hierbei wiederholte er seine vorherige Rechtsprechung, dass der Ersatz eines immateriellen Schadens nach Art. 82 Abs. 1 DSGVO nicht davon abhängig gemacht werden dürfe, dass eine gewisse Erheblichkeit erreicht werde.[4] Zudem unterscheide die DSGVO nicht, ob der von der betroffenen Person behauptete „immaterielle Schaden“ mit einer bereits erfolgten missbräuchlichen Verwendung ihrer personenbezogenen Daten durch Dritte verbunden sein muss oder ob er mit Angst vor einer solchen Verwendung in der Zukunft verknüpft sei. Allerdings muss die betroffene Person nachweisen, dass die Folgen des Verstoßes einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen. Unter Verweis auf Erwägungsgrund 85 der DSGVO begründet der EuGH, dass der Verlust der Kontrolle über personenbezogene Daten bereits einen möglichen Schaden darstellt. Dieses sehr weite Schadensverständnis relativiert der EuGH dann jedoch auch wieder teilweise, indem er erneut auf seine vorherige Rechtsprechung verweist, nach der die betroffene Person nachweisen muss, dass sie tatsächlich einen Schaden erlitten hat.[5] Das jeweilige nationale Gericht müsse im individuellen Fall überprüfen, ob die behauptete Befürchtung der betroffenen Person auch als begründet angesehen werden kann.

VI. Auswirkungen des Urteils für wissenschaftliche Einrichtungen

Auch wissenschaftliche Einrichtungen sind in jüngster Zeit wiederholt Opfer von Cyberangriffen geworden. Es ist davon auszugehen, dass hierbei auch personenbezogene Daten verloren gegangen sind. Als Verantwortliche der jeweiligen Datenverarbeitungen müssen sie die notwendigen technischen und organisatorischen Maßnahmen treffen, um die Sicherheit der Daten zu garantieren. Anders als bei privaten Unternehmen kann eine etwaige Pflichtverletzung durch öffentliche Einrichtungen nicht durch Bußgelder geahndet werden.[6] Damit bilden zivilrechtliche Schadensersatzansprüche gemäß Art. 82 DSGVO das primäre Haftungsrisiko für öffentliche Forschungseinrichtungen, die Opfer von Hackerangriffen werden. Das Verständnis für die Haftungsrisiken kann nun durch das Urteil erheblich geschärft werden. Universitäten werden zunächst durch die Entscheidung, dass nicht jede unbefugte Offenlegung automatisch zur Annahme eines Verstoßes gegen Art 32 DSGVO führt, entlastet. Gleichzeitig müssen Forschungseinrichtungen gegebenenfalls imstande sein, nachzuweisen, dass sie ausreichende Maßnahmen zum Schutz der Datensicherheit getroffen haben. Hierzu sollten getroffene TOMs sorgfältig dokumentiert werden. Kann eine Forschungseinrichtung nicht darlegen, dass sie die erforderlichen Sicherheitsmaßnahmen getroffen hat, ist sie für Schäden verantwortlich, die infolge der Nachlässigkeit – auch durch Dritte – entstehen. Mögliche Schäden können auch in Form plausibel dargelegter emotionaler Einschränkungen bestehen, wie der Furcht vor einer zukünftigen missbräuchlichen Verwendung ihrer Daten durch Dritte. ◆

4 Hierzu Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023.
5 Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023.
6 Vgl. Müller, Bußgeldberechnung für Dummies, DFN-Infobrief Recht 10/2022.

Die Bretonage der europäischen Datenstrategie

Lähmt das Cybersicherheitsrecht die europäische Datenwirtschaft?

Der European Cyber Resilience Act (CRA) hat ein ambitioniertes Ziel: Er soll verbindliche Cybersecurity-Anforderungen für Hardware- und Softwareprodukte mit digitalen Elementen auf dem gesamten europäischen Binnenmarkt schaffen. Hersteller werden dadurch für die Sicherheit ihrer Produkte über die gesamte Lebensdauer verantwortlich gemacht.

Text: **Ole-Christian Tech** (Forschungsstelle Recht im DFN)

Foto: vxnaghiyev/Adobe Stock

Peter Grosse, ehem. Leiter des Rechenzentrums der Universität zu Kiel, ehem. Versammlungsleiter der DFN-Mitgliederversammlung: „Als Vorsitzender der DFN-Mitgliederversammlung stellte ich bei einem laufenden Tagesordnungspunkt fest, dass die Anzahl der Wortmeldungen weit über die eigentlich geplante Mittagspause hinausgehen würde. Daraufhin schlug ich den Mitgliedern vor, den Tagesordnungspunkt zu unterbrechen und die vorliegenden Wortmeldungen nach der Mittagspause anzuhören. Da kein Widerspruch erfolgte, konnte ich die Mitglieder mit „gutem Appetit" in die Pause schicken. Nach der vereinbarten Zeit trafen wir uns, um die Liste der Wortmeldungen abzuarbeiten. Die erste Wortmeldung antwortete mit „hat sich erledigt". Die Folgenden antworteten fast gleichlautend, bis die Liste erschöpft war. Das unerwartete Ergebnis der Mittagspause verblüffte mich so, dass ich ein Grinsen nicht unterdrücken konnte. Da meine Belustigung offenkundig wurde, folgte ein längeres Beifallsklopfen der Mitglieder."

I. Der Cyber Resilience Act im Überblick[1]

Durch den CRA sollen nicht nur der gemeinsame Markt und der Verbraucher geschützt, sondern zugleich auch die gesamte Datenstrategie der EU abgesichert werden, da das Sicherheitsrecht (NIS-2, CSA, CRA)[2] über allen Datenräumen thront und das entfesselte, industrieübergreifende Teilen und Nutzen von Daten absichert.

Der CRA ist die erste Verordnung der Europäischen Union zur sektorübergreifenden, horizontalen Stärkung der Cybersicherheit von Produkten mit digitalen Elementen.[3]

Ende 2023 wurde im Trilogverfahren die politische Einigung erzielt. Bereits 2024 soll diese Fassung verabschiedet werden und dann, nach weiteren 36 Monaten, in allen Mitgliedstaaten unmittelbar Anwendung finden.

Hintergrund des Gesetzes ist die Erkenntnis, dass sich Cybersicherheitslecks bei Produkten im Binnenmarkt auch im gesamten europäischen Datenraum auswirken und daher ein einheitliches Sicherheitsniveau erforderlich ist.

Einerseits soll hierfür das Sicherheitsniveau der Produkte insgesamt erhöht und durch entsprechende Sicherheitsupdates auch beibehalten werden.

Andererseits sollen Informationsasymmetrien zulasten der Endnutzer und Verbraucher abgebaut werden, etwa durch Informationspflichten für den Hersteller.

Der Pflichtenkatalog für die Hersteller umfasst dabei Prozess- und Dokumentationspflichten (aufgelistet in Art. 10 CRA-E) sowie Meldepflichten (Art. 11 CRA-E).

Bei genauerem Blick verfolgt der CRA also mit dem Regelungszweck der Cybersicherheit zugleich auch den Käufer- und Verbraucherschutz.

Damit aber nicht genug. In Erwägungsgrund 17 zum CRA erklärt die Kommission: „Durch den Schutz von Verbrauchern und Organisationen vor Cybersicherheitsrisiken sollen die in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen auch dazu beitragen, den Schutz personenbezogener Daten und den Schutz der Privatsphäre natürlicher Personen zu verbessern." Das Gesetz soll also zudem auch Synergieeffekte im Zusammenspiel mit der Datenschutz-Grundverordnung (DSGVO) erzeugen und somit dem Datenschutz dienen.

1 Vertiefend hierzu Palenberg, Cyberangriff ade mit dem CRA-E? in DFN-Infobrief Recht 9/2023 S. 2ff.
2 Die NIS-2-Richtlinie (Network and Information Security (NIS) Directive) ist am 16.01.2023 in Kraft getreten und enthält die Cyber- und Informationssicherheit von Unternehmen, siehe hierzu John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS? in DFN-Infobrief Recht 4/2023; der Cyber Security Act (CSA) ist seit dem 27. 06 2019 in Kraft und enthält einen Zertifizierungsrahmen für IT-Produkte.
3 Kipker in: Ebers, StichwortKommentar Legal Tech, Cybersecurity Rn. 24.

Torsten Prill, Freie Universität Berlin, Vorsitzender des ZKI, ständiger Gast im DFN-Verwaltungsrat: „Mit seinen innovativen Lösungen leistet der DFN seit vier Jahrzehnten einen wesentlichen Beitrag zur Stärkung des Wissenschaftsstandortes Deutschland und zur nationalen sowie internationalen Vernetzung von Forschung und Lehre. Der DFN hat mich in meiner Arbeit stets begleitet. Ich bin überzeugt, dass er auch weiterhin eine zentrale Rolle bei der Gestaltung unserer digitalen Zukunft spielen wird. Ich wünsche dem DFN-Verein alles Gute und freue mich auf viele weitere Jahre der innovativen Zusammenarbeit."

II. Ein Datenminimierungsgrundsatz im CRA?

Dabei verfolgt auch der CRA – ähnlich wie bereits die DSGVO – keinen absoluten Schutz, sondern eine Risikobewertung und ein dem Risiko angemessenes Schutzniveau. Dies bestätigt Art. 10 Abs. 2 CRA, der eine Verpflichtung der Hersteller zur Bewertung der Cybersicherheitsrisiken normiert.

So weit, so gut, scheint es. Der CRA schafft also, was er verspricht: resiliente und sichere Verarbeitungs- und Übermittlungsumgebungen, um die Datenwirtschaft anzukurbeln. Bei genauerer Lektüre des Entwurfs taucht jedoch ein Fremdkörper in dem Regelwerk auf: Anhang I Abschnitt 1 trägt den unschuldig anmutenden Titel „Sicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen". Dahinter verbirgt sich in Absatz 3 lit. e jedoch folgende Formulierung: „Auf der Grundlage der Risikobewertung gemäß Artikel 10 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,(...) die Verarbeitung personenbezogener oder **sonstiger Daten**[4] auf solche, die angemessen und relevant sind, und auf das für die bestimmungsgemäße Verwendung des Produkts erforderliche Maß beschränken (‚Datenminimierung')."

Ein Grundsatz der Datenminimierung für nicht personenbezogene Daten? Der Grundsatz der Datenminimierung – umgangssprachlich auch Datensparsamkeit genannt – ist bisher fast ausschließlich im Kontext mit der DSGVO aufgetaucht.

III. Der Datenminimierungsgrundsatz im Datenschutzrecht

Abgeleitet wird dieser aus Art. 8 Abs. 1 und 2 der Charta der Grundrechte der Europäischen Union (GRCh) und dem informationellen Selbstbestimmungsrecht in den Mitgliedstaaten, in Deutschland also Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 Grundgesetz (GG).[5] In Artikel 5 Abs. 1 lit. c DSGVO erhält die Datenminimierung sogar den Rang eines allgemeinen Grundsatzes für die Verarbeitung personenbezogener Daten.

Der Datenminimierungsgrundsatz nach der DSGVO verbietet die Verarbeitung personenbezogener Daten, die angesichts des Verarbeitungszwecks inadäquat, unerheblich oder entbehrlich sind. Diese Kriterien sind im Einzelfall durchaus wertungsoffen und können in der Praxis zu einer gewissen Rechtsunsicherheit führen. Diese Rechtsunsicherheit nimmt der europäische Gesetzgeber jedoch bewusst in Kauf, da die informationelle Selbstbestimmung des Betroffenen als Rechtsgut von Verfassungsrang auf dem Spiel steht.

Insbesondere da, wo zahlreiche für sich genommen unverfängliche personenbezogene Daten kombiniert werden, kann durch die Kombination dieser Punkte womöglich ein detailliertes Persönlichkeitsprofil erstellt oder es können sogar besonders sensible persönliche Daten ermittelt werden.[6]

Was für personenbezogene Daten aber sinnvoll ist, kann für „sonstige Daten" zu einem echten Hemmnis werden.

IV. Das Problem

Hersteller sollen Produkte so designen, einstellen und instand halten, dass sie nur die für den jeweils im Vorhinein definierten Produktzweck unbedingt erforderlichen Daten verarbeiten, selbst wenn dies nur harmlose Maschinendaten oder z. B. Wetterdaten sind.

Ein Einsatz dieser Daten für eine spätere Sekundärnutzung ist dadurch erheblich erschwert, schließlich mangelt es bei strenger Beachtung der Datensparsamkeit bereits an deren Verfügbarkeit. Un-

4 Hervorhebung durch den Autor.
5 So etwa auch Spiecker gen. Döhmann/Bretthauer in: Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz, G 2.4.56.
6 Zu dem Problem der „Daisy Chains" siehe bereits Tech, Doppelgänger Delights: How to prevent the perfect impersonation (Or Not) in DFN-Infobrief Recht 4/2023.

Carola Domke, Mitarbeiterin im DFN: „Liebe Frau Schulz (heute Domke), ich habe da was. Mit dieser herzlichen Begrüßung von einem unserer damaligen Geschäftsführer, Dr. Klaus-Eckart Maass, fingen die meisten meiner Arbeitstage an. Als ich 1986 zum DFN-Verein kam, waren wir nur eine Handvoll Leute, echte Pioniere. Die meisten kamen aus dem Hahn-Meitner-Institut, HMI (heute Helmholtz-Zentrum Berlin, HZB). Hier wurde die Idee eines Deutschen Forschungsnetzes für die Wissenschaft ursprünglich geboren. Alles war sehr familiär und ungezwungen. Diese aufregende Zeit des Aufbaus des DFN-Vereins werde ich nie vergessen!“

klar ist damit insbesondere das Regelungsziel mit Blick auf den Anfang 2024 in Kraft getretenen Data Act, dessen erklärtes Ziel eine effiziente und niedrigschwellige Datennutzung ist.[7]

V. Kritik

Ein Grundsatz der Datenminimierung für nicht personenbezogene Daten wirkt wie der etwas plumpe Ansatz „Keine Verarbeitung ist die sicherste Art der Verarbeitung“. Sicher ein risikoaverser Ansatz, jedoch keiner, den sich ein europäischer Binnenmarkt im globalen Wettbewerb leisten kann.

Ein klassisches Beispiel der fast schon naiven Überregulierung also?

Hierzu findet sich im Zusammenhang mit dem verantwortlichen EU-Kommissar für den Binnenmarkt Thierry Breton (in dessen Zuständigkeit auch die Datenstrategie fällt) ein interessanter Neologismus: bretonieren [bʁe:toˈni:ʁən].[8] Es bedeutet so viel wie „durch schlechte und von falschen, sachfremden Interessen geleitete Regulierung technologische und ökonomische Chancen bereits im Keim zu ersticken.“

Was auf den ersten Blick wie die lobenswerte und konsequente Weiterentwicklung eines etablierten und fundamentalen Grundsatzes der DSGVO scheint, birgt jedoch hinsichtlich der bisherigen Datenstrategie der EU einige Probleme.

Das erklärte Ziel der Datenstrategie war ursprünglich einmal, Datenoligopole aufzubrechen und Daten im europäischen Binnenraum möglichst frei zirkulieren zu lassen, um Erkenntnisse und Wertschöpfung aus diesen zu generieren. Dass dieses Ziel mit dem Datenschutz in Einklang zu bringen ist, ist offensichtlich. Nicht umsonst postulierte jeder Rechtsakt der Datenstrategie schon fast gebetsmühlenartig, er stehe im Einklang mit der DSGVO.[9]

Vor diesem Hintergrund erscheint ein Datenminimierungsgrundsatz im CRA zwar redundant – schließlich hat die DSGVO ja Vorrang[10] –, aber zumindest unschädlich. Für die „sonstigen Daten“ hingegen führt der Grundsatz zu einem Problem: Das eigentliche, übergeordnete Ziel der gesamten Datenstrategie wird hierdurch konterkariert. Erkenntnis und Wertschöpfung resultieren häufig gerade erst aus der Sekundärnutzung von Daten, also der Nutzung zu einem anderen Zweck als dem der ursprünglichen Datenerhebung. Erst durch große Datenmengen (Big Data) können Muster erkannt werden, nach denen womöglich gar nicht gezielt gesucht wurde. All dies wird nun erschwert, da der Datenminimierungsgrundsatz bereits die Menge an erhobenen Daten auf ein (willkürliches) Minimum begrenzt.

Gut gemeint ist eben nicht immer gut gemacht.

VI. Ausblick

Mit Inkrafttreten des CRAs werden die Compliance-Anforderungen im Bereich der IT-Sicherheit nun weiter erhöht. Die Vermischung von IT-Sicherheitsrecht mit anderen, sachfremden Erwägungen macht die Handhabung für Hersteller und die gesamte Lieferkette jedoch undurchsichtiger. Jedenfalls die unter der DSGVO geltende Gewissheit, ohne personenbezogene Datenverarbeitung relativ frei schalten und walten zu können, ist damit dahin. Die Euphorie der Datenwirtschaft über die Datenstrategie und das große Sammeln und Wertschöpfen könnte hierdurch gedämpft werden. ◆

---

7 Siehe hierzu vertiefend Müller, Die Daten sind frei? In DFN-Infobrief Recht 3/2024 und Schaller, Data Act: Mehr Daten für alle – check! in DFN-Infobrief Recht 6/2022.

8 Siehe hierzu auch Franz, https://www.cr-online.de/blog/2023/12/11/bretonieren-b%CA%81e%CB%90to%CB%88ni%CB%90%CA%81%C9%99n (zuletzt abgerufen am 30.04.2024).

9 So auch Veil, ZGI 2022, 197 (197); Genauer: Der Data Act Entwurf (COM(2022) 68 final) in Erwägungsgrund 7; der EHDS-VO Entwurf (COM(2022) 197 final) in Art. 1 Abs. 4; und der DGA Entwurf (COM(2020) 767 final) in Erwägungsgrund 3.

10 So auch ausdrücklich Erwägungsgrund 17 zum Cyber Resilience Act.

DFN unterwegs

Der Begriff Netz ist schon Teil unseres Namens. Und gut vernetzt sind auch unsere Mitarbeiterinnen und Mitarbeiter – weit über die Grenzen unserer technischen Infrastruktur hinaus. Wo wir überall unterwegs sind, zeigen wir hier.

Als Koordinatorin für internationale Beziehungen und Projekte im DFN-Verein arbeitet Leonie Schäfer mit Kolleginnen und Kollegen anderer nationaler Forschungsnetze rund um den Globus zusammen. Anfang des Jahres führte ihre Reise sie nach …

… Accra, der Hauptstadt von Ghana, am Golf von Guinea. Dort war sie Mitveranstalterin des Workshops „Business Models and the Expansion of the NREN's Service Portfolio", der am 16. und 17. Januar 2024 stattfand.

Nicht nur Wissenschaftlerinnen und Wissenschaftler arbeiten länderübergreifend zusammen, auch Forschungsnetze (National Research and Education Networks, NRENs). Diese gibt es in fast jedem Land und auf jedem Kontinent. Zum regionalen Forschungsnetz WACREN (West and Central African Research and Education Network) gehören 15 NRENs unter anderem aus Ghana, Togo, Senegal, Nigeria und Mali. Viele dieser NRENs sind klein oder gerade am Entstehen. Besonders groß war daher das Interesse von WACREN, seinen NRENs einen Workshop zu Geschäftsmodellen und zur Entwicklung von Diensten anzubieten. Einen solchen Workshop hatte ich bereits in einem anderen Kontext veranstaltet. Boubakar Berry, der CEO von WACREN, lud mich ein, den gleichen Workshop im Rahmen der WACREN CEO Academy durchzuführen. Teilnehmende waren die CEOs und Geschäftsführende der WACREN-NRENs, die aus verschiedenen Ländern angereist waren.

Gearbeitet wurden mit dem Business Model Canvas und dem Value Proposition Canvas. Diese boten eine gute Grundlage, um die jeweiligen Geschäftsmodelle skizzieren und vergleichen zu können. Der Value Proposition Canvas war für die Teilnehmenden ein guter Startpunkt, um ihre „Kundschaft" und das

Unterstützung für kleine und junge Forschungsnetze: Dr. Boubakar Berry, CEO des regionalen Forschungsnetzes WACREN, und Dr. Leonie Schäfer haben den Workshop für CEOs und Geschäftsführende von westafrikanischen NRENs organisiert | *Fotos: DFN*

Robert Stoy, Mitarbeiter im DFN: „In meinen Anfängen in den 90ern durfte ich am Rechenzentrum der Uni Stuttgart am Betriebskonzept für das neue G-WiN mitarbeiten. Die Bandbreiten lagen bei 100 Mbit/s, Engpässe waren an der Tagesordnung. Seit meinem Wechsel zum DFN-NOC in Stuttgart zur Jahrtausendwende, haben wir unser Netz durch mehrere Generationen gebracht. Heute betreiben wir ein eigenes DWDM-Netz, bauen die nächste X-WiN Generation mit Bandbreiten von 400 Gbit/s und völlig neuen Routern. Durch die hohe Kompetenz im Betrieb, die dafür nötige Netzperformance permanent sicherzustellen, ist die Dienstqualität stetig gewachsen – eine imposante Entwicklung!“

Gemeinsam stark: Zum großen Erfolg des Workshops trug auch der intensive Austausch unter den NREN-Chefs der Region bei | *Foto: WACREN*

eigene Serviceportfolio zu reflektieren. Die intensiven Diskussionen und der Austausch in der Gruppe, auch nach Beendigung des Workshops, machen unter anderem den nachhaltigen Erfolg der Veranstaltung aus. Das Ziel, den Teilnehmenden wertvolle Starthilfe geleistet zu haben, scheint erreicht.

Die Herausforderungen für NRENs in Westafrika sind ähnlich zu denen in Europa. An erster Stelle gilt es, die jeweiligen Regierungen von der Notwendigkeit zu überzeugen, ein NREN zu unterstützen und zu finanzieren. Zu den Themen gehören die mangelnde Digitalisierung der Hochschulen und die Entwicklung eines, an die Bedarfe der Mitglieder angepassten, Serviceportfolios. Auch die politische Situation in der von Unruhen geprägten Region spielt natürlich eine Rolle. Nun liegt es an den jeweiligen CEOs und ihren Teams, das Erarbeitete umzusetzen.

Außerdem war da noch Afrika, der mir unbekannte Kontinent. Mein zugegebenermaßen sehr subjektives Bild war bislang geprägt von Medienberichten über Dürre und Hungersnöte, Diktaturen und Bürgerkriegen, Epidemien und Entwicklungshilfe. Entsprechend vorsichtig war meine Annäherung. Bei der Ankunft begrüßte mich Ghana mit 30 Grad und strahlendem Sonnenschein, abgeflogen war ich in Berlin bei null Grad und Schnee. Die Ghanaer kamen mir sehr freundlich entgegen, stolz darauf, mir ihr Land zu zeigen. Zwei Mitarbeiterinnen von WACREN boten sich an, mit mir eine Tour durch die Stadt zu machen und zeigten mir die Sehenswürdigkeiten und Märkte. Letztere sind bunt, laut und vielfältig. Von der Kokosnuss über das Auto-Ersatzteil bis hin zu neuen Schuhen gibt es dort alles zu kaufen. Handeln ist obligatorisch. Daneben gibt es aber auch die modernen Shoppingmalls mit den Markenprodukten aus aller Welt.

Das Zentrum von Accra ist sehr großstädtisch mit Hochhaustürmen von Banken, Hotels und Versicherungen. Accra hat etwa 2,6 Millionen Einwohner und breitet sich in der Fläche aus. In Accra gibt es viele „Gated Communitys“ mit modernen Wohngebäuden, hohen Mauern und Wachleuten am Eingang. Überhaupt ist Sicherheit ein großes Thema. Auch der Kontrast zwischen arm und reich, Menschen, die auf der Straße leben und denjenigen, die mit ihren SUVs durch die Gegend fahren und in den Shoppingmalls einkaufen können, ist schon markant.

Eine weitere Herausforderung ist die Infrastruktur des Landes. Es gibt viel Verkehr und wenig gut ausgebaute Straßen. Man kommt nur langsam voran. Bahnverkehr in Ghana gibt es kaum noch. ÖPNV existiert nur bedingt in Form der sogenannten Tro-Tros (für den öffentlichen Transport umgebaute Kleinbusse), die jedoch die

Eigenart haben, erst loszufahren, wenn sie komplett voll sind, und unterwegs spontan anzuhalten. Abgesehen von den Start- und Endpunkten der TroTro-Stations gibt es keine Bushaltestellen. Taxis gelten als unsicher, zumindest für Europäer. Von daher ist die persönliche Fortbewegung eine Herausforderung. Online-Vermittlungsdienste wie Uber, Bolt und Yango gelten als die sicherste Fortbewegungsart und sind recht preisgünstig.

Wirtschaftlich scheint es Ghana recht gut zu gehen. Das Land exportiert Gold und Öl und ist der zweitgrößte Exporteur von Kakaobohnen. Neuerdings stellt das Land auch selbst Schokolade her. Stoffe und wunderschöne Textilien mit bunten Mustern sind ebenfalls ein Exportartikel. Das Land liegt nah am Äquator, es gibt zwei Regenzeiten pro Jahr. Entsprechend fruchtbar ist der Boden und reichhaltig das Angebot an Nahrungsmitteln. Typisch für die westafrikanische Küche sind gut gewürzte Soßen, Reis, Huhn und Ziegenfleisch. Beliebt sind auch Banku und Fufu, eine Art Kloßeinlage für Suppen aus Mais- und Maniokmehl (auch Cassava genannt). Ansonsten ist die Ananas das Obst der Wahl.

Insgesamt war mein Eindruck von Ghana sehr positiv und entsprach ganz und gar nicht meinem teils negativen, durch die Medien vermittelten Afrikabild. Im Gespräch mit den Workshop-Teilnehmenden erfuhr ich dann aber doch einiges über die koloniale Vergangenheit der westafrikanischen Länder und deren aktuelle Konfliktherde. Die Unabhängigkeit von den ehemaligen Kolonialherren Großbritannien, Frankreich und Portugal ist nach wie vor ein großer Faktor, das koloniale Erbe prägt die Länder noch heute. Dies wird vor allem sichtbar an der Sprache, dem Schulsystem und an den Infrastrukturen, außerdem an der Gewohnheit Tee zu trinken und Porridge zum Frühstück zu essen. Ein Studium in Großbritannien oder Frankreich gehört in vielen afrikanischen Ländern nach wir vor zum guten Ton.

Die Flugzeit von Amsterdam nach Accra betrug nur sechs Stunden und der Zeitunterschied war minimal. Eigentlich ist es somit nur ein kurzer Sprung, gefühlt war es aber doch eine weite Reise. In Europa hört man nicht viel über West-Afrika, das könnte man durchaus ändern. Dort gibt es viel Potenzial. Die Zusammenarbeit mit den CEOs der west-afrikanischen NRENs sehe ich als einen wichtigen Schritt zur Verbesserung der Beziehungen zwischen Europa und West-Afrika. ◆

Eine Reise wert: Mit ihren bunten quirligen Märkten und zahlreichen Sehenswürdigkeiten wie dem Black Star Gate – dem nationalen Symbol für Ghanas Unabhängigkeit – bietet die Hauptstadt Accra vielfältige Eindrücke | *Fotos: Leonie Schäfer, DFN*

DFN live: Wissen teilen, Erfahrungen weitergeben

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

DFN-Betriebstagung

Die 80. DFN-Betriebstagung, die am 19. und 20. März 2024 im Leonardo Royal Hotel Berlin Alexanderplatz stattfand, ging mit vielen aktuellen Themen, frischen Eindrücken, spannenden Gesprächen – wie etwa bei der Podiumsdiskussion zur Frage „Startet die Cloud mit OCRE 2024 nun endlich auch in Deutschland durch?“ – zu Ende. Und auch dieses Mal wurde die Zahl der Teilnehmenden getoppt. Insgesamt 309 Besucherinnen und Besucher verzeichnete die Präsenzveranstaltung. Mehr als 103 Leute schauten sich die Plenumsvorträge im Stream an.

Die kommende Betriebstagung im Herbst steht ganz im Zeichen unseres 40. Geburtstags. Feiern Sie mit und lassen Sie sich überraschen!

TERMIN

Die 81. DFN-Betriebstagung findet am **Dienstag und Mittwoch, 8. und 9. Oktober 2024,** statt.

Treffpunkt Berlin: Zweimal im Jahr kommen Fachleute aus den am Wissenschaftsnetz teilnehmenden Einrichtungen bei der BT zusammen, um aktuelle Themen rund um Netz und Dienste zu diskutieren | *Fotos: Stella Lenz, DFN*

87. DFN-Mitgliederversammlung: Wahl eines neuen Verwaltungsrats und Vorstands

Vertreterinnen und Vertreter der DFN-Mitgliedseinrichtungen wählten auf der 87. Mitgliederversammlung am 13. Dezember 2023 im Wissenschaftszentrum in Bonn einen neuen Verwaltungsrat: Der dreizehnköpfige erweiterte Vorstand ernannte im Anschluss Prof. Dr.-Ing. Stefan Wesner von der Universität zu Köln für die Dauer von drei Jahren zum neuen Vorsitzenden. Der Direktor des IT Center Cologne (ITCC) und Professor für Parallele und Verteilte Systeme übernimmt den Vorsitz von Prof. Dr. Odej Kao von der Technischen Universität Berlin, der den Vorstand seit 2020 leitete.

Professor Wesner ist dem DFN-Verein seit Längerem verbunden: Von 2013 bis 2022 war er bereits DFN-Mitgliedsvertreter für die Universität Ulm, seit 2022 vertritt er die Universität zu Köln im DFN-Verein. Seit 2020 gehört er dem DFN-Verwaltungsrat an.

Als stellvertretender Vorstandsvorsitzender neu ernannt wurde Prof. Dr. Helmut Reiser, der stellvertretende Leiter des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften und Professor an der Ludwig-Maximilians-Universität München. Er ist seit 2009 Mitgliedsvertreter und seit 2014 Mitglied im Betriebsausschuss des DFN. Er folgt auf Dr. Rainer Bockholt, Direktor des Hochschulrechenzentrums der Rheinischen Friedrich-Wilhelms-Universität Bonn, der das Amt als stellvertretender Vorsitzender von 2014 bis 2023 ausübte und nach zweimaliger Wiederwahl sowie insgesamt drei Wahlperioden gemäß der Satzung des Vereins nicht mehr gewählt werden konnte. Als stellvertretender Vorstandsvorsitzender erneut bestätigt wurde Christian Zens, Kanzler der Friedrich-Alexander-Universität Erlangen-Nürnberg.

TERMIN

Die 88. Mitgliederversammlung und der Vorabendempfang finden am **Montag und Dienstag, 10. und 11. Juni 2024,** (nach Redaktionsschluss der DFN-Mitteilungen) statt.

Die 89. Mitgliederversammlung und der Vorabendempfang finden am **Dienstag und Mittwoch, 3. und 4. Dezember 2024,** statt.

Der neu gewählte Verwaltungsrat des Vereins (v. li.):

Dr. Hartmut Plehn
Prof. Dr. Frank Jenko
Prof. Dr. Helmut Reiser
Kerstin Bein
Christian Zens
Dr. Holger Marten
Prof. Dr.-Ing. Stefan Wesner
Dieter Lehmann
Dr. Lars Köller
PD Dr. Wolfgang zu Castell
Ilona Glaser
Peter Gietz
Prof. Dr.-Ing. Günter Schäfer
(o. Abb.)
Foto: Frank Homann

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. Zum zehnten Jubiläum fand die Konferenz am 28. und 29. November 2023 mit 130 Teilnehmenden im Hotel Hafen Hamburg an den Landungsbrücken statt.

Dr. Jan K. Köcher (vorne auf dem Podium) eröffnet die 10. DFN-Konferenz „Datenschutz“. Für sein jahrelanges großes Engagement, das wichtige Thema Datenschutz nachhaltig aufzubereiten und in den Fokus zu rücken, wurde er bei der Jubiläumsveranstaltung geehrt | *Foto: Nina Bark, DFN*

TERMIN

Die 11. DFN-Konferenz „Datenschutz“ findet am **Dienstag und Mittwoch, 26.11. und 27.11.2024,** statt.

Wichtiger denn je: Mit ihrem vielfältigen Format rund um das Thema Informationssicherheit vernetzt die Siko Expertinnen und Experten aus Forschung und Bildung | *Foto: Nina Bark, DFN*

TERMIN

Die 32. DFN-Konferenz „Sicherheit in vernetzten Systemen“ findet am **Dienstag und Mittwoch, 11. bis 12. Februar 2025,** statt.

DFN-Konferenz „Sicherheit in vernetzten Systemen“

Die 31. DFN-Konferenz „Sicherheit in vernetzten Systemen“ fand mit 330 Teilnehmenden am Dienstag und Mittwoch, 30. und 31. Januar 2024, im Grand Elysée Hotel Hamburg statt und wurde vom DFN-CERT im Auftrag des DFN-Vereins veranstaltet. Das Programmkomitee hatte wieder einmal ein tolles Programm aus Themen rund um die Informationssicherheit auf die Beine gestellt – von Cybersicherheitsregulierung über adaptive Detektion mittels Open-Source-Forensik bis hin zu Threat Hunting mithilfe von Künstlicher Intelligenz.

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

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

Überblick DFN-Verein

(Stand: 06/2024)

Foto: jackijack / fotolia

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

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

Die Geschäftsstelle

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

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

Die Organe

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

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

Kerstin Bein
(Universität Mannheim)

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

Peter Gietz
(DAASI International GmbH)

Ilona Glaser
(Deutscher Wetterdienst)

Prof. Dr. Frank Jenko
(Technische Universität München)

Dr. Lars Köller
(Technische Hochschule Ostwestfalen-Lippe)

Dieter Lehmann
(Universität Leipzig)

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

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

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

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

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

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

Der Verwaltungsrat hat als ständige Gäste

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

einen Vertreter der Hochschulkanzlerinnen und -kanzler:
Dietmar Smyrek
(Hauptberuflicher Vizepräsident für Personal, Finanzen und Hochschulbau der Technischen Universität Braunschweig)

einen Vertreter der Kultusministerkonferenz:
Jürgen Grothe
(SMWK Dresden)

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

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

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

Prof. Dr.-Ing. Stefan Wesner
Vorsitz

Prof. Dr. Helmut Reiser
Stellv. Vorsitzender

Christian Zens
Stellv. Vorsitzender

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

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

Die Mitgliedseinrichtungen

Aachen	Fachhochschule Aachen - Technik und Wirtschaft
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Technische Hochschule Aschaffenburg
Augsburg	Technische Hochschule Augsburg
	Universität Augsburg
Bad Homburg	NTT Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	Berlin-Brandenburgische Akademie der Wissenschaften
	Berliner Institut für Gesundheitsforschung/Berlin Institute of Health
	Berliner Hochschule für Technik (BHT)
	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
	Bundesanstalt für Materialforschung und -prüfung
	Bundesinstitut für Risikobewertung
	Deutsche Telekom AG Laboratories
	Deutsche Telekom IT GmbH
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung e. V. (DIW)
	European School of Management and Technology GmbH (ESMT)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hertie School gGmbH
	Hochschule für Technik und Wirtschaft Berlin
	Hochschule für Wirtschaft und Recht Berlin
	Humboldt-Universität zu Berlin
	International Psychoanalytic University Berlin gGmbH
	IT-Dienstleistungszentrum Berlin
	Leibniz-Gemeinschaft e. V.
	Museum für Naturkunde – Leibniz-Institut für Evolutions- und Biodiversitätsforschung
	NOW GmbH Nationale Organisation Wasserstoff- und Brennstoffzellentechnologie
	Robert Koch-Institut
	Stanford University in Berlin
	Stiftung Deutsches Historisches Museum
	Stiftung Preußischer Kulturbesitz
	Technische Universität Berlin (TUB)
	Umweltbundesamt
	Universität der Künste Berlin
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum Berlin für Sozialforschung gGmbH
	Zuse-Institut Berlin (ZIB)
Biberach	Hochschule Biberach
Bielefeld	Hochschule Bielefeld
	Universität Bielefeld
Bingen	Technische Hochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Hochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Hochschule Georg Agricola
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern und für Heimat
	Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz
	Deutsche Forschungsgemeinschaft
	Deutscher Akademischer Austauschdienst e. V.
	Deutsches Zentrum für Luft- und Raumfahrt e. V.
	Deutsches Zentrum für Neurodegenerative Erkrankungen e. V.
	Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.
	Informationstechnikzentrum Bund
	Rheinische Friedrich-Wilhelms-Universität Bonn
Borstel	Forschungszentrum Borstel – Leibniz Lungenzentrum
Brandenburg	Technische Hochschule Brandenburg
Braunschweig	Leibniz-Institut DSMZ – Deutsche Sammlung von Mikroorganismen und Zellkulturen GmbH
	Helmholtz-Zentrum für Infektionsforschung GmbH
	Hochschule für Bildende Künste Braunschweig
	Johann Heinrich von Thünen-Institut, Bundesforschungs-institut für Ländliche Räume, Wald und Fischerei
	Julius Kühn-Institut, Bundesforschungsinstitut für Kulturpflanzen
	Physikalisch-Technische Bundesanstalt
	Technische Universität Braunschweig
Bremen	Constructor University Bremen gGmbH
	Hochschule Bremen
	Hochschule für Künste Bremen
	Universität Bremen
Bremerhaven	Alfred-Wegener-Institut, Helmholtz-Zentrum für Polar- und Meeresforschung
	Hochschule Bremerhaven
Buxtehude	hochschule 21 gemeinnützige GmbH
Chemnitz	Technische Universität Chemnitz
	TUCed – An – Institut für Transfer und 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
	Technische Universität Darmstadt
Deggendorf	Technische Hochschule Deggendorf
Dortmund	Fachhochschule Dortmund
	Technische Universität Dortmund
Dresden	Evangelische Hochschule Dresden
	Helmholtz-Zentrum Dresden-Rossendorf e. V.
	Hannah-Arendt-Institut für Totalitarismusforschung e. V.
	Hochschule für Bildende Künste Dresden
	Hochschule für Technik und Wirtschaft Dresden
	Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden e. V.
	Leibniz-Institut für Polymerforschung Dresden e. V.
	Sächsische Landesbibliothek – Staats- und Universitätsbibliothek
	Technische Universität Dresden
Dummerstorf	Forschungsinstitut für Nutztierbiologie (FBN)
Düsseldorf	Hochschule Düsseldorf
	Heinrich-Heine-Universität Düsseldorf
	Information und Technik Nordrhein-Westfalen (IT.NRW)
	Kunstakademie Düsseldorf
	Robert Schumann Hochschule Düsseldorf
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Hochschule Emden/Leer
Erfurt	Fachhochschule Erfurt
	Universität Erfurt
Erlangen	Friedrich-Alexander-Universität Erlangen-Nürnberg
Essen	Folkwang Universität der Künste
	RWI – Leibniz-Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Europa-Universität Flensburg
	Hochschule Flensburg
Forchheim	Institut für Nanotechnologie und korrelative Mikroskopie gGmbH
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Deutsche Nationalbibliothek
	DIPF | Leibniz-Institut für Bildungsforschung und Bildungsinformation
	Frankfurt University of Applied Sciences
	Johann Wolfgang Goethe-Universität Frankfurt am Main
	Philosophisch-Theologische Hochschule St. Georgen e. V.
	Senckenberg Gesellschaft für Naturforschung
Frankfurt/O.	IHP GmbH – Institut für innovative Mikroelektronik
	Stiftung Europa-Universität Viadrina
Freiberg	Technische Universität Bergakademie Freiberg
Freiburg	Albert-Ludwigs-Universität Freiburg
	Evangelische Hochschule Freiburg
	Katholische Hochschule Freiburg
Freising	Hochschule Weihenstephan-Triesdorf
Friedrichshafen	Zeppelin Universität gGmbH
Fulda	Hochschule Fulda
Furtwangen	Hochschule Furtwangen
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH
	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften
Gatersleben	Leibniz-Institut für Pflanzengenetik und Kulturpflanzenforschung (IPK)
Geesthacht	Helmholtz-Zentrum hereon GmbH
Gelsenkirchen	Westfälische Hochschule
Gießen	Technische Hochschule Mittelhessen
	Justus-Liebig-Universität Gießen
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GWDG)
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	Universität Greifswald
	Friedrich-Loeffler-Institut, Bundesforschungsinstitut für Tiergesundheit
Hagen	Fachhochschule Südwestfalen
	FernUniversität in Hagen
Halle/Saale	Leibniz-Institut für Wirtschaftsforschung Halle e. V.
	Martin-Luther-Universität Halle-Wittenberg
	Burg Giebichenstein Kunsthochschule Halle
Hamburg	Bundesamt für Seeschifffahrt und Hydrographie
	Deutsches Elektronen-Synchrotron DESY
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	DFN – CERT Services GmbH
	HafenCity Universität Hamburg
	Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg
	Hochschule für Angewandte Wissenschaften Hamburg
	Hochschule für bildende Künste Hamburg
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg
	Universität Hamburg
Hameln	Hochschule Weserbergland
Hamm	Hochschule Hamm-Lippstadt
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe
	Hochschule Hannover
	Gottfried Wilhelm Leibniz Bibliothek – Niedersächsische Landesbibliothek
	Gottfried Wilhelm Leibniz Universität Hannover
	HIS Hochschul-Informations-System eG
	Hochschule für Musik, Theater und Medien Hannover
	Landesamt für Bergbau, Energie und Geologie
	Medizinische Hochschule Hannover
	Technische Informationsbibliothek
	Stiftung Tierärztliche Hochschule Hannover
Heide	Fachhochschule Westküste
Heidelberg	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	NEC Laboratories Europe GmbH
	Universität Heidelberg

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

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

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

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

DFN newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

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

DFN auf Mastodon
trötet & teilt spannende News rund um das Deutsche Forschungsnetz

DFN auf X
postet aktuelle Nachrichten zum Deutschen Forschungsnetz

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