DFN mitteilungen

Sein oder Nichtsein

die faszinierende Welt der Qubits

Neu im DFN-Vorstand

Odej Kao im Interview

Das Herzstück des SOC

neue Komponenten & Services

9 770177 689001

Impressum

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

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

ISSN 0177-6894

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

Fotonachweis
Titel: GlobalP/iStock
S. 5, Autorenbild 6: KOPF & KRAGEN Fotografie
Rückseite: Wallenrock/Shutterstock

Prof. Dr. Gerhard Peter
Vorsitzender der 81. DFN-Mitgliederversammlung, Altrektor der Hochschule Heilbronn und ehemaliger Leiter der DFN-Nutzergruppe Hochschulverwaltung

2020 und 2021 werden in die Geschichte als Corona-Jahre eingehen – mit vielen einschneidenden Veränderungen, die ich mir im Februar 2020 noch nicht hätte vorstellen können. Alle tragen Masken, dienstliche Reisen sind nahezu unmöglich. Wie viele andere Einrichtungen entschloss sich der DFN, die beiden Mitgliederversammlungen (MV) in 2020 online stattfinden zu lassen. Jetzt ist eine gute Gelegenheit, zurückzublicken, Bilanz zu ziehen und die Frage zu stellen, ob es bleibende Veränderungen geben soll.

Ich greife vor und kann zunächst feststellen, dass alle formalen Anforderungen an eine Mitgliederversammlung erfüllt wurden. Alle technischen Aufgabenstellungen wurden gelöst, Berichte wie Diskussionen fanden statt. Und auch die Wahl zum Verwaltungsrat verlief, dank der perfekten Vorbereitung durch die Geschäftsstelle, ohne irgendeinen Punkt der Beanstandung. Die Kandidatinnen und Kandidaten persönlich kennenzulernen wäre allerdings schöner gewesen. Interessanterweise blieb die Zahl der Teilnehmenden ungefähr gleich groß. Das Interesse am DFN ist offensichtlich unabhängig von der Veranstaltungsart. Wenn man es oberflächlich betrachtet, wurde nur der äußere Rahmen geändert und alles andere auf moderner Technik fortgeschrieben.

Die Frage muss deshalb gestellt werden, warum wir möglicherweise trotzdem nicht dauerhaft bei dieser Form bleiben wollen. Gleicht die Einsparung von Reise-, Übernachtungs-, Zeit- und Bewirtungskosten den Verlust an Qualität der Veranstaltung aus?

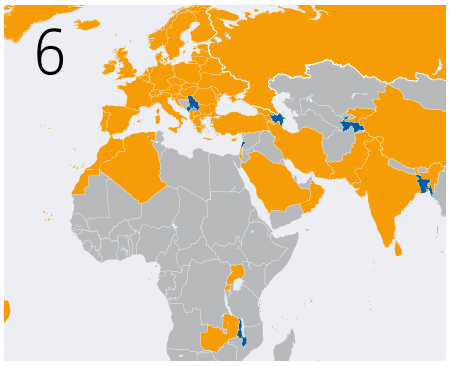
Was steht dem gegenüber? Der Austausch und die Fragen an Vorstand und Geschäftsstelle haben zwar stattgefunden, sind in der Anzahl aber erkennbar weniger geworden. Außerdem sind die Fragen, die in der großen Runde gestellt werden, an alle gerichtet. Die bilateralen Gespräche mit den Kolleginnen und Kollegen sowie den Beschäftigten des DFN, die üblicherweise in der Pause stattfinden, gibt es momentan nicht. Problemlösungen der anderen Einrichtungen zu erfragen und darüber zu diskutieren, ist in diesem Format nicht möglich – meiner Meinung nach ein wichtiges Merkmal der MV. Wie notwendig ist beim Vorabendtreffen in kulinarischer Runde die persönliche Kommunikation für die Entwicklung und Nutzung der Kommunikationsinfrastrukturen im Internet?

Die Antwort auf die Frage: *Es geht doch, warum nicht immer so?*, lautet:

Weil der persönliche Informationsaustausch fehlt,
weil wir von den Kolleginnen und Kollegen im direkten Austausch lernen und
weil Zwischentöne wichtig sind.

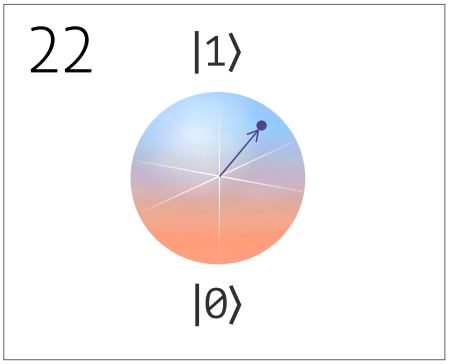
Herzlichst
Ihr Gerhard Peter

Inhalt



Vom Sternchen zur Galaxie – 10 Jahre eduGAIN
Für die internationale Zusammenarbeit unverzichtbar. Mit der Beliebtheit steigen jedoch auch die Herausforderungen.

Ideen fliegen sehen
Prof. Dr. Odej Kao im Gespräch: was den neuen Vorstandsvorsitzenden bewegt und wie er die Zukunft des DFN mitgestalten möchte.



II. Quantenrevolution – die Welt der Qubits
Heute Science-Fiction, übermorgen Alltag? Einblicke in die Quanten-technologie

Wissenschaftsnetz

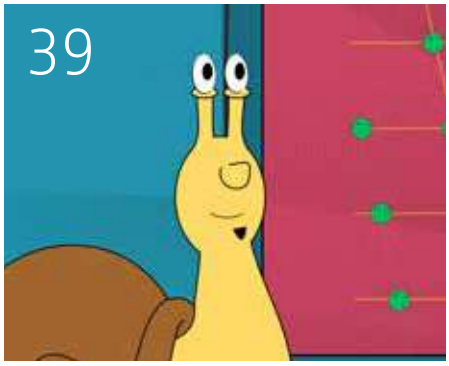
Interview

International

Forschung

Sicherheit

Campus



Von Schnecken und Raketen
Anschaulich erklärt: Herr Schnecke, Frau Rocketscientist und ein Inselverkäufer zeigen die wichtigsten Post-Quanten-Algorithmen.

Recht

DFN-Verein

Die Autoren dieser Ausgabe im Überblick

1 Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **2** Maimona Id, DFN-Verein (id@dfn.de); **3** Dr.-Ing. Martin Schellenberger, Fraunhofer-Institut für Integrierte Systeme und Bau-elementetechnologie, IISB (martin.schellenberger@iisb.fraunhofer.de); **4** Dr. Peter Kaufmann, DFN-Verein (kaufmann@dfn.de); **5** Dr.-Ing. Susanne Naegele-Jackson, Friedrich-Alexander-Universität Erlangen-Nürnberg (susanne.naegele-jackson@fau.de); **6** Dr. Reinhard Sell, DFN-CERT Services GmbH (sell@dfn-cert.de); **7** Stefan-Lukas Gazdag, genua GmbH (stefan-lukas_gazdag@genua.de); **8** Sophia Grundner-Culemann, LMU München (grundner-culemann@nm.ifi.lmu.de); **9** Dr. Tobias Guggemos, LMU München (guggemos@nm.ifi.lmu.de); **10** Tobias Heider, genua GmbH (tobias_heider@genua.de); **11** Dr. Daniel Loebenberger, Fraunhofer AISEC (daniel.loebenberger@aisec.fraunhofer.de); **12** Klaus Schmeh, Cryptovision (klaus.schmeh@cryptovision.com); **13** Uwe Jandt, Deutsches Elektronen-Synchrotron DESY (uwe.jandt@desy.de); **14** Christoph Scheid, Philipps-Universität Marburg (scheid@uni-marburg.de); **15** Maximilian Wellmann, Forschungsstelle Recht im DFN (wellmann@dfn.de); **16** Nicolas John, Forschungsstelle Recht im DFN (john@dfn.de)

eduGAIN 10th Anniversary

Vom Sternchen zur Galaxie

In den zehn Jahren seines Bestehens hat sich der Dienst eduGAIN zu einer globalen Authentifizierungs- und Autorisierungsinfrastruktur entwickelt, an der mittlerweile über 70 Föderationen teilnehmen. Insbesondere für internationale Forschungsverbünde und Communities hat er sich als unverzichtbare Infrastrukturkomponente etabliert und die föderationsübergreifende Zusammenarbeit überhaupt erst möglich macht.

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

PETER GIETZ, DAASI INTERNATIONAL GMBH

eduGAIN ist neben eduroam eine von der Forschung initiierte, weltweit funktionierende Infrastruktur. Die eduGAIN-Infrastruktur wird heute von den verschiedensten Communities für föderiertes Identitätsmanagement (FIM) genutzt. FIM4R (Federated Identity Management for Research), ein Zusammenschluss von Forschungsinfrastrukturen aus sehr unterschiedlichen Fachdomänen beispielsweise, trug anfangs wesentliche Anforderungen an eduGAIN zusammen und veröffentlichte sie. Durch dieses Engagement konnten im Rahmen von Horizont 2020 die Projekte AARC I und II ins Leben gerufen werden. Neben der Erstellung einer Blaupause für Forschungsinfrastrukturen führte dies zu vielen weiteren Aktivitäten im FIM-Bereich, zum Beispiel die bibliotheksgetriebene Initiative FIM4L (Federated Identity Management for Libraries). Diese Entwicklungen zeigen, wie sich um eduGAIN ein ganzes Ökosystem bildet, das für die zunehmende Verbreitung des Dienstes sorgt. Ich bin überzeugt davon, dass eduGAIN in den kommenden zehn Jahren genauso ubiquitär genutzt werden wird wie eduroam.

Bescheidene Anfänge

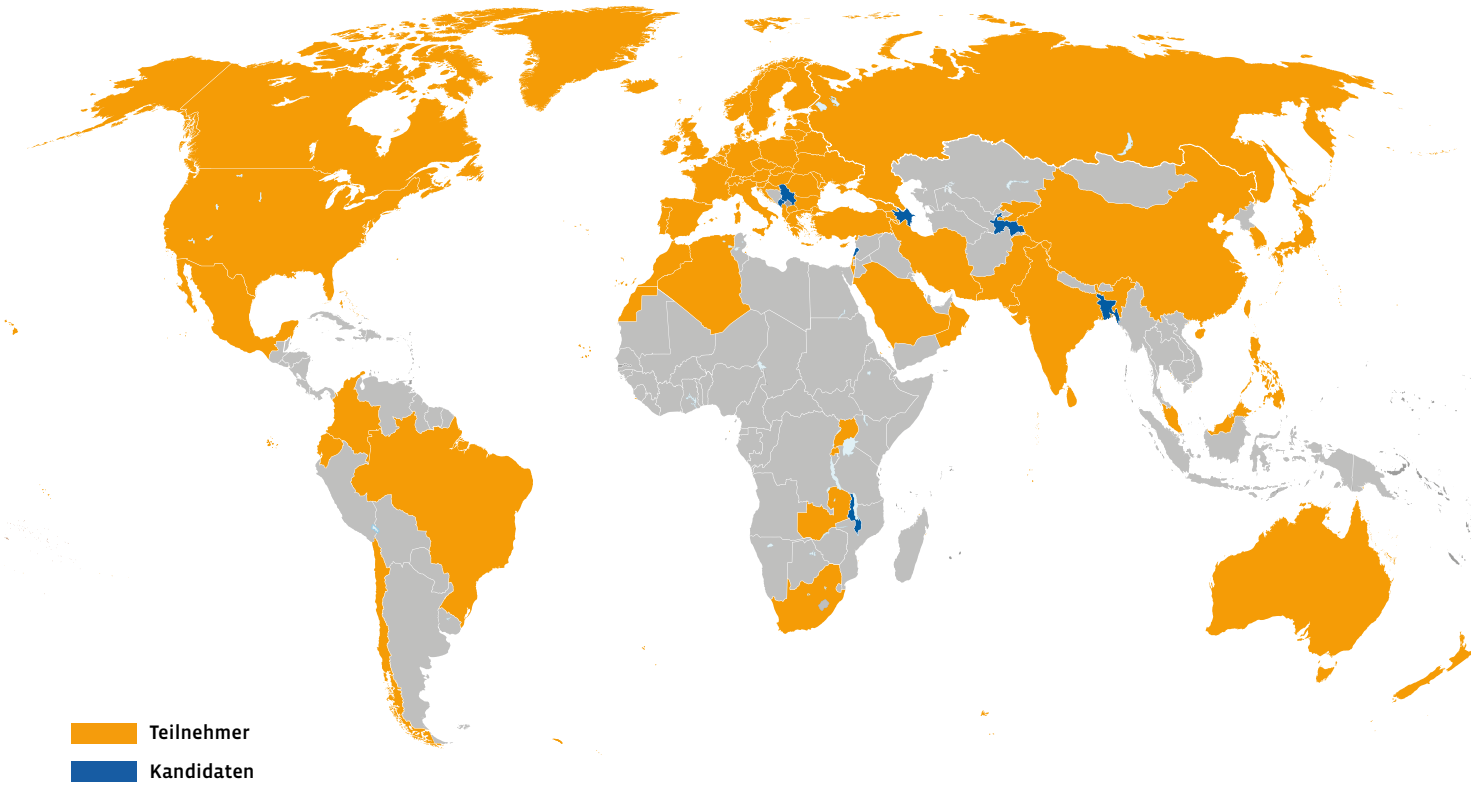
Als eduGAIN am 27. April 2011 im Rahmen des GÉANT2-Projekts offiziell in den Produktivbetrieb überführt wurde, ahnte wohl kaum jemand, dass sich dieser Dienst im Laufe der nächsten Jahre zu einem Erfolgsmodell entwickeln würde. Im Juni 2011 unterzeichneten RedIRIS (Spanien) und der DFN-Verein als erste Föderationsbetreiber die eduGAIN Policy Declaration. Doch ein regulärer, bilateraler Austausch der DFN-AAI-Föderationsmetadaten mit dem eduGAIN Metadata Distribution Service (MDS) erfolgte erst Anfang 2012. Als im Mai 2012 der Beitrag *DFN-AAI goes Europe!* in den DFN-Mitteilungen (Ausgabe 82) erschien, nahmen gerade einmal 14 Föderationen mit insgesamt 45 Entities (Identity und Service Provider) aktiv an eduGAIN teil. Es sollte noch einige Jahre dauern, bis über eduGAIN eine kritische Masse an Diensten (Service Provider) verfügbar war, die eine Teilnahme auch für Heimateinrichtungen (Identity Provider) attraktiv machte und andersherum – das übliche Henne-Ei-Problem.

Wachstum ist nicht alles

Die folgenden Jahre waren geprägt von kontinuierlichem Wachstum, sowohl was die Anzahl der teilnehmenden Föderationen als auch die über eduGAIN verfügbaren

eduGAIN TEILNEHMER (STAND 04/2021)

| 71 FÖDERATIONEN | 4200 IDP (davon 259 aus der DFN-AAI) | 3200 SP (davon 143 aus der DFN-AAI) |



Identity (IdP) und Service Provider (SP) angeht. In den Anfangsjahren galt generell das Opt-in-Prinzip, d. h., IdP- und SP-Betreiber mussten aktiv die Teilnahme am Metadatenaustausch mit eduGAIN veranlassen. Dieses Prinzip gilt auch heute noch für die Teilnehmer in der DFN-AAI. Andere Föderationen gingen dazu über, die Teilnahmemodalitäten auf Opt-out umzustellen, d. h., standardmäßig werden alle IdP (UK: auch alle nichtlokalen SP) an eduGAIN weitergereicht. Wer das nicht wünscht, muss entsprechende technische Maßnahmen treffen. Diese Policy-Änderung sorgte für einen deutlichen Anstieg vor allem der Anzahl der über eduGAIN verfügbaren IdP. Weiter befördert wurde das Wachstum durch die weltweit steigende Anzahl von Föderationen – ein Indiz für die zunehmende Bedeutung des föderierten Identity Managements im Rahmen von Authentifizierungs- und Autorisierungsinfrastrukturen für die Wissenschaft.

Mit dem stetig wachsenden Stellenwert von eduGAIN insbesondere für internationale Forschungsverbünde ergaben sich auch etliche Herausforderungen. Für diese wurden im Rahmen der GÉANT-Projekte gemeinsam mit den Forschungscommunities und REFEDS (Research and Education Federations) entsprechende Lösungen erarbeitet.

DR. MARCUS HARDT, STEINBUCH CENTRE FOR COMPUTING (SCC)

Im EU-Projekt AARC war der Interföderationsdienst eduGAIN eine wesentliche Grundlage für die Blueprint Architectures, mit denen wir im Projekt die Architektur für interoperables Identitätsmanagement in Forschungs-Communities und -infrastrukturen beschrieben haben. eduGAIN hat dabei wichtige Fragestellungen ins Spiel gebracht und den Rahmen geschaffen, in dem wesentliche Aspekte von Attributfreigabe, Konventionen und Standardisierung diskutiert und gelöst werden konnten. Die Organisation von föderiertem Identitätsmanagement ist heute ohne eduGAIN nicht mehr denkbar.

DIETER VAN UYTVANCK, CLARIN – EUROPEAN RESEARCH INFRASTRUCTURE FOR LANGUAGE RESOURCES AND TECHNOLOGY

Since its inception, CLARIN (Common Language Resources and Technology Infrastructure) always had a keen interest in the concept and implementation of eduGAIN, since it allows us to bridge the international gap between researchers and language resources that require authentication. Over the years, we saw eduGAIN growing from an experimental setup to a reliable infrastructure. It might not always be visible to researchers that need to access a data set hosted in another country, but it is most definitely a crucial element for research infrastructures like CLARIN. We are particularly thankful to DFN for helping us during all those years to keep our service provider metadata neatly synchronised with eduGAIN, and for the countless times we received useful advice and support.

Attributfreigabe

In einer föderationsübergreifenden AAI gilt ein gänzlich anderes Vertrauensniveau als innerhalb einer Föderation, in der ein Föderationsbetreiber als Trusted Third Party für das Vertrauen der Föderationsteilnehmer untereinander sorgt. Warum sollte ein IdP-Betreiber Attribute und damit personenbezogene Daten an einen unbekannten SP in einer anderen Föderation übertragen? Um diesem Problem zumindest innerhalb der EU und des europäischen Wirtschaftsraums zu begegnen, wurde der GÉANT Data Protection Code of Conduct for Service Provider in EU/EEA – kurz „CoCo“ – geschaffen. Die Umsetzung dieser vertrauensbildenden Selbstverpflichtungserklärung für Service Provider wird mit verschiedenen technischen Maßnahmen von eduGAIN- und Föderationsseite unterstützt. Aktuell wird an einer EU-DSGVO-konformen Umsetzung gearbeitet.

Incident Response

Mit zunehmender internationaler Vernetzung hat sich auch die Angriffsfläche für Identitätsdiebstahl an Heimateinrichtungen und Hacking von SP vergrößert. Um schnell und strukturiert auf Sicherheitsvorfälle reagieren zu können, wurde das Security Incident Response Trust Framework for Federated Identity (Sirtfi) etabliert. Manche SP-Betreiber wie das CERN kooperieren mittlerweile nur noch mit IdP, die Sirtfi unterstützen. Als Kontakt für Sicherheitsvorfälle mit Bezug zur DFN-AAI fungiert das Incident Response Team des DFN-CERT.

SANDER APWEILER, FEDERATED SYSTEMS AND DATA, JÜLICH SUPERCOMPUTING CENTRE (JSC)

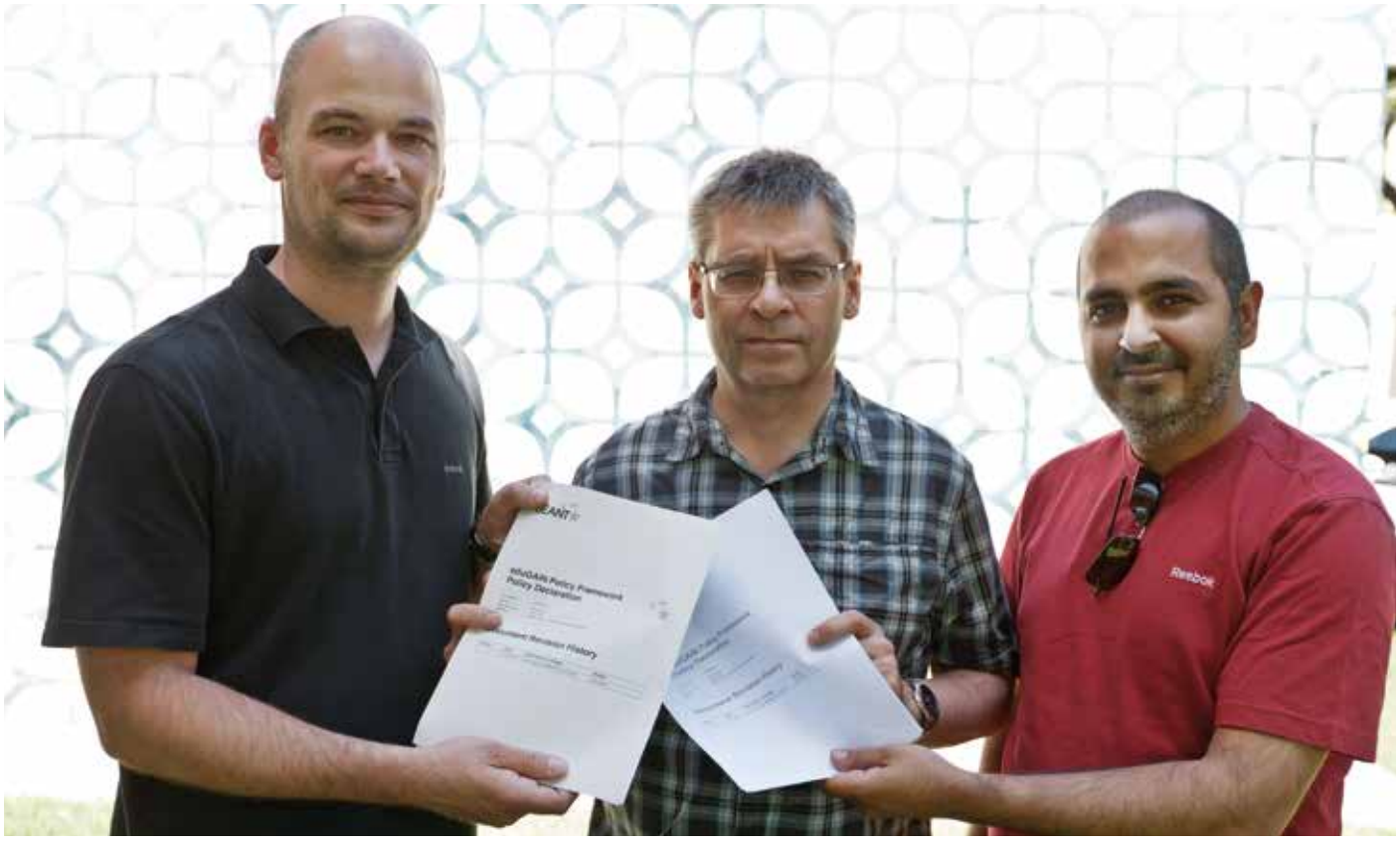
Im Rahmen der Helmholtz-AAI ermöglicht eduGAIN die problemlose technische Integration der Helmholtz-Zentren und ihrer Kooperationspartner. Ohne eduGAIN wäre die Anbindung der IdP der Zentren zwar noch möglich, aber die Einbindung aller Kooperationspartner mindestens schwierig. Für den Aufbau der EUDAT-e-Infrastruktur ist eine föderationsübergreifende AAI über eduGAIN eine wichtige Grundlage. Eine Anmeldung der Forscher bei EUDAT-Diensten unter Verwendung des Heimat-Accounts wäre ohne diesen Dienst nahezu unmöglich, da vor einer Verwendung zunächst die Heimateinrichtung eingebunden werden müsste. Somit ermöglicht eduGAIN nicht nur die Einrichtung von Diensten und Infrastrukturen, die vielen Forschenden zugänglich gemacht werden, sondern stärkt auch den Account an der Heimateinrichtung. Eine Vielzahl unterschiedlicher Konten bei diversen Diensten erstellen zu müssen, ist somit nicht mehr notwendig.

Monitoring

Es kommt hin und wieder vor, dass Föderationen fehlerhafte, nicht standardkonforme Metadaten ausliefern. Daher wurden automatisierte Prüfmechanismen entwickelt. Sie validieren die Metadaten, die von den teilnehmenden Föderationen an den eduGAIN MDS geliefert werden und sorgen ggf. dafür, dass die betreffenden Entities aus den von eduGAIN ausgelieferten Metadaten entfernt werden. Dies kann auch den gesamten Metadata-Feed einer Föderation betreffen.

Support

Wer beantwortet Fragen von Dienstanbietern, Heimateinrichtungen und anderen Nutzenden und verweist die Ratsuchenden zur zuständigen Föderation? Wer informiert Föderationsbetreiber über technische Probleme? Im eduGAIN Support Team kümmern sich AAI-Fachleute aus mehreren teilnehmenden Föderationen um Anfragen aller Art und benachrichtigen die Föderationsbetreiber über fehlerhafte Metadaten oder andere technische Probleme, die die Funktionalität von eduGAIN beinträchtigen könnten.



Die Köche der Ursuppe: Torsten Kersting (links) vom DFN-Verein und Ajay Daryanani (rechts), damals von RedIRIS, bei der Übergabe der eduGAIN-Erklärung an Tomasz Wolniewicz, Vertreter des eduGAIN Operations Teams und AAI-Koordinator des Poznan Supercomputing and Networking Center (PSNC) im Juni 2011.

Im Hier und Jetzt

Um den Bogen zur Gegenwart zu spannen, seien hier einige aktuelle Zahlen genannt. Der Anteil an Service Providern ist grundsätzlich kleiner als der der teilnehmenden Identity Provider, da nicht jeder AAI-fähige Dienst auch für eine internationale Nutzerschaft bestimmt ist. Anfang April 2021 nehmen 71 Föderationen mit ca. 4200 IdPs und ca. 3200 SPs an eduGAIN teil. Davon stammen 259 IdPs (von insges. 335) und 143 SPs (von insges. 609) aus der DFN-AAI.

Ein wichtiges Thema ist derzeit die Frage der Qualität des Betriebs von Identity- und Service-Providern sowie von Föderationen als Ganzem. Die kürzlich von einer REFEDS-Arbeitsgruppe erstellten Identity Federation Baseline Expectations könnten hier künftig als Richtlinie dienen. Weiterhin sind Sicherheit und der Umgang mit Sicherheitsvorfällen nach wie vor von großer Bedeutung. Ende 2020 wurde daher das eduGAIN Security Team ins Leben gerufen, das sich im eduGAIN-Kontext um Identitätsdiebstahl und sonstige Sicherheitsvorfälle kümmert. Zuvor übernahm diese Aufgabe das oben erwähnte eduGAIN Support Team. Kürzlich ist die eduGAIN Security Working Group gegründet worden, in der auch der DFN-Verein vertreten ist. Diese Arbeitsgruppe soll unter anderem das Bewusstsein für Fragen der Sicherheit in der eduGAIN Community schärfen, darauf hinwirken, dass das Sirtfi Framework breitere Unterstützung findet und Prozesse für den Umgang mit unterschiedlichen Arten von Sicherheitsproblemen definieren. Es wird also bestimmt nicht langweilig – auf die nächsten 10 Jahre! ◆

Kurzmeldungen

Auf einen Blick – Teilnehmerportal startet in den Pilotbetrieb

Foto: narith_2527/iStock

Ende März 2021 ist das neue Teilnehmerportal des DFN-Vereins in den Pilotbetrieb gestartet. Teilnehmer erhalten damit künftig einen kompakten Überblick zu den von ihnen genutzten DFN-Diensten und haben die Möglichkeit, Standardprozesse schnell und einfach abzuwickeln.

Das Teilnehmerportal stellt zunächst Daten und Informationen zum Kommunikationsdienst DFNInternet zur Verfügung. Zu einem späteren Zeitpunkt werden weitere Dienste des DFN-Vereins integriert. Für die Entwicklung des Webportals ist das Projekt- und Entwicklungsteam des DFN-CERT zuständig. Die Projektleitung verantwortet der Bereich Network and Communication Services in der DFN-Geschäftsstelle.

Nach Abschluss der Pilotphase soll voraussichtlich im Sommer 2021 das erste Release im Produktivbetrieb bereitstehen und für Teilnehmer am Dienst DFNInternet nutzbar sein. Diese können dann ihre Stammdaten sowie die Daten zu ihrem Rahmenvertrag und zur Dienstvereinbarung DFNInternet abrufen inklusive der technischen Parameter der DFNInternet-Dienste: Dazu gehören die vereinbarte Dienstkategorie, betriebliche Kontaktpersonen, die versorgten IP-Netzbereiche und Informationen zur Teilnehmeranbindung wie deren Übertragungskapazität, die verwendeten Schnittstellen und Installationsorte der Verbindungen zum X-WiN.

Geplant ist in den folgenden Releases, den Teilnehmern Interaktionen mit dem Portal zu ermöglichen. Kontaktinformationen zu Ansprechpersonen können dann selbstständig bearbeitet werden. Außerdem haben Teilnehmer die Option, über das Portal Upgrades und Downgrades für DFNInternet-Dienste zu beauftragen. Spätere Releases sollen Betriebsdaten zu DFN-Diensten enthalten. Ganz oben auf der Anforderungsliste steht die Bereitstellung von Messdaten zum übertragenen Datenvolumen, der Auslastung von Teilnehmeranbindungen sowie zur Verfügbarkeit von Diensten.

Für die Nutzung des Teilnehmerportals ist ein DFNInternet-Dienst auf der Basis eines Rahmenvertrages zur Teilnahme am Deutschen Forschungsnetz und der entsprechenden Dienstvereinbarung Voraussetzung. Dienste aus der Zeit vor 2005, die auf Basis von G-WiN-Anwenderverträgen geschlossen wurden, werden nicht unterstützt. Eine Umstellung auf die aktuellen Verträge ist jedoch mit geringem Aufwand möglich. Das Team von DFNInternet unterstützt Sie dabei gerne. ◆

Haben Sie Fragen zum Teilnehmerportal?
Dann melden Sie sich per E-Mail unter: **teilnehmerportal@dfn.de**

Mit dem X-WiN gut vernetzt: Zusätzliche Peerings sorgen für optimalen Datenaustausch

Ein schneller Datenaustausch und eine hohe Verfügbarkeit der Konnektivität – diese Ziele verfolgt der DFN-Verein nicht nur innerhalb des Wissenschaftsnetzes, sondern auch mit den Übergängen in andere für die DFN-Community relevante Teilnetze des Internets.

Im ersten Quartal dieses Jahres wurden sowohl Public Peerings (PPI, Public Peering Interconnection) als auch direkte Anbindungen an Zugangsprovider weiter ausgebaut und optimiert. Das bereits bestehende Private Peering (PNI) mit der 1&1 Versatel Deutschland GmbH konnte um eine georedundante Anbindung erweitert werden. Mit Vodafone Germany wurde eine direkte 100-Gbit/s-Anbindung am Standort Frankfurt am Main erfolgreich in Betrieb genommen. Private Peerings bestehen außerdem mit Liberty Global (UnityMedia) und Telefónica Deutschland (O_2).

Die aktuellen Optimierungen kommen insbesondere den Studierenden und Beschäftigen der DFN-Community zugute, die im Homeoffice arbeiten. ◆

Bye Bye ISDN – DFNFernsprechen vollständig auf VoIP umgerüstet

Und Tschüss: Der letzte ISDN-Anschluss ist gekappt. Das Migrationsteam von DFNFernsprechen freut sich, dass die Teilnehmeranschlüsse nun vollständig auf Voice-over-IP (VoIP) umgestellt sind. Mit viel Engagement und persönlicher Beratung sorgte das Team seit 2017 für den reibungslosen Ablauf der Migration. Damit ist die Sprachkommunikation im Wissenschaftsnetz X-WiN angekommen.

Mehr als 250 Einrichtungen nutzen die VoIP-basierten Anschlüsse von DFNFernsprechen, viele von ihnen VoIP-Centrex. Mit den mobilen und browserbasierten Anwendungen der virtuellen Telefonanlage ist eine sichere und stabile Echtzeitkommunikation möglich. Grund ist die doppelte Anbindung an das Wissenschaftsnetz, die eine hohe Verfügbarkeit gewährleistet.

Zum gesamten Portfolio berät Sie das Team von DFNFernsprechen: DFNFernsprechen@dfn.de ◆

Weitere Informationen finden Sie unter: **https://www.dfn.de/dienstleistungen/dfnfernsprechen/**

Vorbild DFN-AAI: DFN-Verein berät Projekt für deutschlandweite Schulföderation

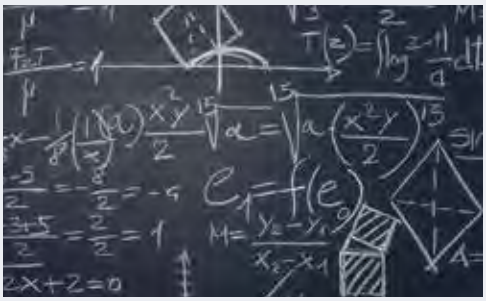


Foto: copperpipe/freepik

Wissen teilen, Erfahrungen weitergeben – der DFN-Verein berät das Medieninstitut der Länder FWU (Institut für Film und Bild in Wissenschaft und Unterricht gGmbH) zum Thema Authentifizierungs- und Autorisierungsinfrastruktur (AAI). Im Auftrag der Bundesländer hat das FWU im Februar das Projekt Vermittlungsdienst für das digitale Identitätsmanagement in Schulen (VIDIS) auf den Weg gebracht. Damit soll eine länderübergreifende Bildungsmedieninfrastruktur etabliert werden.

Ziel ist, Schülerinnen und Schüler sowie Lehrkräfte mit einer digitalen Identität auszustatten, die es ihnen ermöglicht, über Single Sign-on-Mechanismen auf digitale Inhalte wie Lehrmaterialien zuzugreifen – bildungspolitisch ist das ein Meilenstein.

Im Vorfeld des Projektstarts hatte der DFN-Verein insbesondere über die Schwerpunkte AAI-Standards und mögliche Föderationsmodelle informiert. Zukünftig erfolgt die Zusammenarbeit im Rahmen der VIDIS-Fachgruppe „Technik und Datenschutz“. ◆

Weitere Informationen finden Sie unter: **https://www.vidis.schule**

Ideen fliegen sehen

Seit Dezember 2020 ist Prof. Dr. Odej Kao Vorstandsvorsitzender des DFN-Vereins. Ob als Dozent, Wissenschaftler oder CIO, was er anpackt, macht er mit Leidenschaft und sehr erfolgreich dazu. Was die digitale Souveränität von Hochschulen für ihn bedeutet, warum ihm die Nachwuchsförderung ein Anliegen ist oder welche Erfahrungen er in der Pandemiezeit gemacht hat, und nicht zuletzt, warum er die Arbeit beim DFN-Verein als Privileg betrachtet, verrät der Informatiker im Gespräch.

Hat viel vor: Prof. Dr. Odej Kao freut sich auf die spannenden Aufgaben und Herausforderungen im DFN-Verein *Foto: ECDF/PR/Christian Kielmann*

Können Sie sich an Ihren ersten Kontakt mit dem DFN-Verein erinnern?
Sehr gut sogar. Das war 2003, ich hatte gerade die Leitung des Paderborn Center for Parallel Computing übernommen. Die ersten Sitzungen mit dem DFN fanden sogar noch in den alten Büros in Kreuzberg statt, in der Stresemannstraße. Noch enger wurde die Beziehung im Rahmen der D-Grid-Initiative. Als überregionales Zentrum für Hochleistungsrechnen mussten wir bundesweit erreichbar sein, damit unsere Partner bestmöglich an unsere Ressourcen rankommen. Der DFN-Verein war ein wichtiger Partner.

Seit 2017 sind Sie im Verwaltungsrat des DFN. Was schätzen Sie am Verein?
Man spürt die große Verantwortung. Stabile Netzwerke und Dienste sind heutzutage nicht mehr optional, sondern in der benötigten Qualität und Kapazität zwingend notwendig. Als Teilnehmer sind wir alle darauf angewiesen. Das ist unser gemeinsamer Nenner. Und da sehe ich den Verein als die bindende Komponente.

Etwas gehadert habe ich zu Beginn allerdings mit dem Tempo der Entscheidungsfindung. Wenn man sich aber die Struktur der Mitglieder anschaut und deren heterogene Interessen über die Jahre erlebt, versteht man, wie fragil die Herstellung einer gemeinsamen Linie verläuft. Ich staune immer wieder, was für ein Vertrauen der DFN genießt. Das ist ungewöhnlich.

Worauf freuen Sie sich in Ihrer Amtszeit?
Ich bin in der glücklichen Lage, dass die Entgeltordnung gerade verabschiedet wurde und zumindest die finanzielle Zukunft des DFN gesichert ist. Wir können uns nun auf die neuesten Herausforderungen konzentrieren, die die Digitalisie-

rung mit sich bringt. Dafür brauchen wir unter anderem neue Infrastrukturen. Das setzt implizit voraus, dass die Netzwerke mitwachsen. Das wird eine permanente Herausforderung für den DFN-Verein bleiben.

Spannend ist auch die Frage, ob wir ein nationales oder gar ein europäisches Identity Management (IdM) bekommen. Wir sind ein bedeutendes Wissenschaftsland und haben sehr viele mobile Forschende und Studierende, die an europäischen Kooperationen interessiert sind. Das Ziel ist, die Migration der IT-Umgebung zwischen Heimat- und Gasthochschule möglichst einfach zu gestalten. Hier sehe ich den DFN als nationalen Vertreter und auch als einen der Treiber. Es

> „Digitale Souveränität ist die Aufrechterhaltung der Handlungsfähigkeit der Hochschulen."

liegt nahe, dass wir mit unseren Partnern eine Art führende Rolle übernehmen und diese Entwicklung vorantreiben. Weitere Fragen sind, wie die 5G-Campusnetze die Hochschulen verändern werden oder was wir zur Umsetzung der digitalen Souveränität unserer Mitglieder und Teilnehmer beitragen können.

Was bedeutet denn digitale Souveränität und was können wir dazu beitragen?

Es gibt verschiedene Definitionen: Souveränität bedeutet zunächst Handlungsfähigkeit. Wenn beispielsweise Systeme komplett ausfallen, wenn bestimmte Länder entscheiden, dass die Auslieferung von Technologien nicht zulässig ist oder wenn es gegenüber bestimmten Systemen Bedenken zum Datenschutz gibt, möchte ich, dass wir handlungsfähig bleiben. Und dafür muss es alternative Möglichkeiten geben. Es wäre schön, wenn der DFN dafür Lösungen bieten könnte. Digitale Souveränität ist aus meiner Sicht die Aufrechterhaltung der Handlungsfähigkeit der Hochschulen.

Bedeutet das, dass wir als DFN-Verein Verantwortung abgeben?

Ganz im Gegenteil, wir würden mehr Verantwortung übernehmen. Im vergangenen März, infolge des ersten Lockdowns, wurden alle Hochschulen von heute auf morgen mit sehr harten Anforderungen konfrontiert. Die Hoffnungen, dass der DFN das abfangen kann, waren groß. Das hat nicht funktioniert, weil das Videokonferenzsystem niemals für diese Anforderungen konzipiert war. Letztendlich haben die Hochschulen ihre eigenen Lösungen geschaffen. Diese Überbrückungsphase war chaotisch. In meinen Augen ist der DFN-Verein auch ein Backup, wenn gar nichts mehr geht. Es muss eine Mindestfunktionalität geben, bis die Hochschulen, die betroffen sind, wieder auf eigenen Füßen stehen.

Digitaler Wandel – das erleben wir gerade sehr deutlich – bedeutet Aufbruch und Mut zur Veränderung. Welche mutigen Entscheidungen haben Sie in Ihrem Berufsleben bisher getroffen? Was war schwierig und was von Erfolg gekrönt?

Ich bin damals aus Mazedonien nach Deutschland gekommen, um Informatik zu studieren; quasi aus der dritten in die erste Welt – völlig ohne deutsche Sprachkenntnisse. Das war schwer und hat die Latte ziemlich hoch gelegt. Es war mitten im Winter in einer Kleinstadt, die Trennung von Freunden und Eltern machte mir zu schaffen und dazu die Ungewissheit, ob ich das Studium überhaupt bewältige – all das schlägt natürlich auf die Seele. Nach dem Sprachkurs, als das Semester losging, war es einfacher. Ich hatte meine Kommilitonen, einen geregelten Studienablauf und die ersten Erfolgserlebnisse. Es ging aufwärts.

Warum haben Sie sich ausgerechnet Deutschland ausgesucht?

Eigentlich habe ich mir das nicht ausgesucht. Ursprünglich wollte ich in den USA studieren. Dort wäre mein Einstieg deutlich einfacher gewesen, weil ich gut Englisch sprach. Meine Eltern lebten in den 70er-Jahren in Berlin, hier wurde auch meine Schwester geboren. Deutschland ist ihnen damals sehr stark in Erinnerung geblieben. Es hieß, Deutschland ist das beste Land der Welt, dort musst du hin. Ich konnte den Wunsch meiner Eltern nachvollziehen. Damals war es gerade in ärmeren Ländern wie Mazedonien nicht ohne Weiteres möglich, über den Atlantik zu reisen. So blieb ich zumindest in der Nähe. Das ist der Grund, warum ich jetzt hier bin.

Was haben Sie am meisten genossen im Studium?

Ich war noch nie so frei wie zu dieser Zeit. Ich konnte den ganzen Tag das tun, was mir leicht von der Hand ging, nämlich Mathematik und Informatik. Ich musste mir um nichts Sorgen machen. Ich hatte nichts. So gab es auch nichts, was ich verlieren konnte. Ich war auf dem Weg nach oben, also die beste Ausgangslage, die man sich vorstellen kann. Später gab es einige risikoreichere Entscheidungen. Zum Beispiel den Entschluss, auf eine Professur zu gehen oder eine tolle Stelle an der Uni Paderborn zu verlassen, um das tubIT aufzubauen. Diese Fragen stellten sich damals im Studium gar nicht. Und das fand ich extrem befreiend.

Warum ist es für den wissenschaftlichen Nachwuchs ein Risiko, eine Professur anzustreben?

Bei diesem Karriereschritt gibt es keine zuverlässigen Wege, das hängt von vielen Zufällen ab. Als junger Wissenschaftler investiere ich viel Zeit: Ich nehme die Promotion auf mich, eine lange Postdoc-Zeit und anschließend die Suche nach einem Ruf. Schnell besteht die Gefahr, zu alt zu sein. Oder es wird einem vorgeworfen, zu lange in einem Elfenbeinturm gearbeitet

zu haben und nicht mehr fit für die Praxis zu sein. Das sehe ich nach wie vor als Risiko. Es ist immer noch sehr undurchsichtig, wie Universitäten entscheiden, und die Karriere ist trotz aller exzellenten Vorqualifikationen keineswegs garantiert. Ich hatte Glück, auf so eine tolle Berufungskommission in Paderborn zu treffen, die nicht auf meine Historie, sondern auf mein Potenzial geschaut hat.

Sie setzen sich als Vorstandsvorsitzender des Einstein Center Digital Future (ECDF) sehr für die Nachwuchsförderung ein.
Über diese Entwicklung freue ich mich sehr. Ich bin dem Präsidenten der TU, Christian Thomsen, sehr dankbar, dass er das ECDF initiiert hat. Wir haben 50 jungen Menschen den Weg zu einer Professur geebnet, die sonst eventuell diese Chance nicht bekommen hätten. Vor vier Jahren haben wir begonnen, Unternehmen ins Boot zu holen, die für insgesamt 50 Professuren und eine Dauer von sechs Jahren die Finanzierung übernehmen. Das war harte Arbeit, so viele Unternehmen von einer Spende zu überzeugen. In der Regel sind das Juniorprofessuren, aber es sind auch einige W2- und W3-Professuren darunter. Einige der jungen Professorinnen und Professoren sind bereits auf Dauerstellen berufen worden. Für andere haben wir eine Perspektive am ECDF geschaffen. Darauf bin ich sehr stolz.

Neben der Leitung des Fachgebiets Verteilte Systeme und Betriebssysteme sind Sie an der TU Berlin als CIO außerdem für die IT-Strategie der Uni zuständig. Zuvor haben Sie das IT-Service-Center tubIT aufgebaut.
Ich bin Informatiker, ich weiß, wie Systeme funktionieren und wie man sie aufbaut. Das tägliche Management eines Rechenzentrums ist jedoch etwas völlig anderes. Personalführung, politische Raffinessen, Grundlagen des Finanzwesens, Umgang mit heterogenen Interessen und Lieferanten waren in meinem Hochschullehrer-Portfolio nicht ausgeprägt. Da war es ein Segen, Ulrike Gutheil, damals

Mit prominenter Unterstützung: Prof. Dr. Odej Kao (4. v. li.) und der Regierende Bürgermeister von Berlin Michael Müller (3. v. re.) eröffnen das ECDF *Foto: ECDF/PR/Kay Herschelmann*

Kanzlerin der TU Berlin, an meiner Seite zu haben. Ich habe viel von ihrer langjährigen Erfahrung profitiert und wir haben in dieser Phase viel miteinander für die Universität bewegen können. Das war eine wichtige Erfahrung.

Was ist als CIO nun anders?
Wenn Sie die operative Verantwortung dafür haben, dass die IT-Systeme nicht

> Wenn 40 000 Menschen möglicherweise nicht arbeiten können, ist das eine deutliche Belastung.

ausfallen und dadurch an einem Tag ca. 40 000 Menschen möglicherweise nicht arbeiten können, ist das schon eine deutliche Belastung. Da gehen morgens der erste und abends der letzte Blick auf das Handy, immer in der Hoffnung, dass alles in Ordnung ist. Als CIO muss ich deutlich weiter in die Zukunft schauen können. Ich muss aufpassen, dass ich wichtige Entwicklungen nicht verpasse. In der Informatik sind wir es gewohnt, dass es fast jeden Tag etwas Neues gibt. Aber nur wenig davon ist tatsächlich nachhaltig. Ich muss Augen und Ohren offenhalten und ein Gespür für die wichtigen Themen haben. Mir fällt es jedoch nach wie vor schwer, mich vom operativen Geschäft zu lösen.

Warum fällt Ihnen das schwer?
Na ja, wenn man als Informatiker Sachen baut, möchte man sie fliegen sehen. Das ist das Ziel. Meine Eltern sind beide Architekten und es ist schon ein tolles Gefühl, wenn man an einem Gebäude vorbeiläuft und sagen kann, das Haus hat meine Mutter entworfen. Mit einem neuen Dienst ist das ähnlich. Wenn der zum ersten Mal im Katalog auftaucht und genutzt wird, ist das ein echtes Erfolgserlebnis. Sich Innovationen nur auszudenken, die andere Leute dann umsetzen dürfen, das ist schwer – insbesondere, wenn man schon mal die Erfahrung gemacht hat, dass eine Idee, eine Wunschvorstellung zu etwas Realem geworden ist. Wie vor etwa acht Jahren bei der tubCloud. Wir hatten zu der Zeit schon sehr früh auf eine Cloudlösung gesetzt.

Die Covid-19-Pandemie hat insbesondere die Lehre und Forschung ganz schön durchgeschüttelt. Wie erleben Sie das als Dozent?

Mir tun die Studierenden sehr leid, weil sie ihre sozialen Kontakte nicht so ausleben können wie üblich. Ihre Sorgen werden viel zu wenig gehört. Die Zeit an der Uni gehört zu den schönsten im Leben, da geht gerade viel verloren.

Die digitale Lehre läuft zumindest bei meinen Kursen sehr gut. Ich nehme Vorlesungsvideos auf, die sich die Studierenden auf der Lernplattform jederzeit anschauen können. Zu Beginn habe ich etwa zehn Stunden gebraucht, um ein Zwei-Stunden-Video zu erstellen. Mittlerweile bin ich viel schneller. Das ist zwar viel mehr Arbeit als vorher, aber eine Arbeit, die sich lohnt. Die Nachbearbeitung der Videos hilft auch, um meine Lautstärke und Aussprache zu verbessern.

In den Videokonferenzen zur eigentlichen Vorlesungszeit kann ich mir nun viel Zeit für die komplexeren Inhalte nehmen und ausführlich auf Fragen der Studierenden eingehen. Diese können auch im Chat gestellt werden. Die Lehrevaluationen sind besser als jemals zuvor. Das hat mich schon gefreut und bestärkt, auf diesem Pfad auch in der Zukunft zu bleiben. Trotzdem vermisse ich die persönlichen Gespräche.

Wie läuft es bei den Prüfungen? Sind die Prüfungsergebnisse jetzt schlechter?

Nein, überhaupt nicht. Was die mündlichen Prüfungen angeht, sind die Studierenden sogar teilweise besser vorbereitet, da sie die Videos und somit meinen Unterricht parat haben. Ein großes Problem sehe ich bei den schriftlichen Prüfungen, rechtlich eine sehr komplexe Materie. Da werden alle Hochschulen ihre Erfahrungen in diesem komplizierten und neuen Bereich machen müssen. Gute Alternativen zu Open-Book-Klausuren, in denen sehr vieles erlaubt ist und dem anderen extremen Fall, den streng überwachten Prüfungen im privaten Bereich von Studierenden, sind schwer zu finden. Ich bin froh, dass wir an der TU sogenannte Portfolio-Prüfungen haben, bei denen viele Zwischenleistungen wie etwa Hausaufgaben und Vorträge benotet werden. Dadurch machen die Endprüfungen nur einen geringen Teil der Noten aus.

Haben Sie persönlich etwas aus der Pandemiezeit ziehen können?

Ich verzichte in Zukunft auf die überwiegende Zahl von Dienstreisen innerhalb Deutschlands, bei denen ich quasi am frühen Morgen hinfliege, nur um lediglich drei, vier Stunden an einer Sitzung teilzunehmen. Die Videokonferenzen sind jetzt gut eingeübt und eine sehr komfortable Lösung. Außerdem leisten wir damit einen Beitrag zum Klimaschutz – ein sehr wichtiges Thema, an dem niemand mehr vorbeigehen kann.

Sie erleben also eine Art Entschleunigung?

Nein, glücklicherweise das Gegenteil. Damit mir nicht langweilig wird, fülle ich momentan jede freie Minute mit Arbeit. Ich habe eine Menge zusätzliche Aktivitäten gestartet: die Organisation von großen Tagungen, Entwicklung von eigenen Produkten, neue Vorlesungen, viel mehr Paper schreiben und einiges mehr. Was teils auch nicht gesund ist, weil die Arbeit mein Leben extrem dominiert. Die schönen Sachen wie dreimal pro Woche zum Training zu gehen oder sich ab und zu mit Freunden zu treffen, fallen gerade leider weg. Meine Erkenntnis aus der Pandemie ist aber, dass ich auf vieles verzichten kann, ohne dass es mir richtig wehtut.

Sie beschäftigen sich im ECDF auch mit Digitalisierungsforschung. Wie wird sich unsere Gesellschaft verändern?

Die Digitalisierung werden wir schon mittelfristig hinbekommen. Wir müssen uns als Mitglieder der Gesellschaft überlegen, ob wir wirklich die beste Version von uns verkörpern. Milliarden von Menschen leiden derzeit. Wir haben im Prinzip die Lösungen, aber bekommen es nicht hin, beispielsweise ausreichend Impfstoff herzustellen. Warum kann Deutschland Milliarden für den Lockdown ausgeben, aber einer Firma als Entschädigung

> „Als Mitglieder der Gesellschaft müssen wir uns überlegen, ob wir wirklich die beste Version von uns verkörpern.“

nicht so viel Geld zahlen, dass diese als Geschenk an die Menschheit auf ihre Herstellungslizenzen verzichtet. Open Source sozusagen. Das geht mir nicht in den Kopf.

Noch einmal zurück zu der Frage, ob es etwas gibt, worauf Sie sich freuen in Ihrer Amtszeit?

Ich würde nicht direkt von Freude sprechen, sondern vielmehr von der Spannung und Aufregung, jetzt etwas auf dem Fundament meiner Vorgänger aufzubauen auf nationaler und europäischer Ebene. Da hat Hans Bungartz stellvertretend für die lange Liste meiner Vorgänger, Vorstände, Verwaltungsräte, Geschäftsstelle und DFN-Mitglieder exzellente Arbeit geleistet und mir ein toll bestelltes Feld hinterlassen. So eine Gelegenheit bekommt man im normalen Job eigentlich nicht geboten. Da ist man immer auf seine Universität oder Hochschule fokussiert, aber niemals auf den größeren Kontext. Und jetzt in einem größeren Kontext arbeiten zu dürfen, empfinde ich als Privileg.

Die Fragen stellte Maimona Id (DFN-Verein)

OCRE Open Clouds for Research Environments

Wenn „Cloud“ die Antwort ist – was war eigentlich die Frage?

Im Rahmen des Projekts OCRE, an dem der DFN-Verein gemeinsam mit GÉANT beteiligt ist, erhalten 15 innovative Forschungsprojekte insgesamt 1,175 Millionen Euro aus der Förderlinie OCRE Cloud Funding for Research. Zu den Glücklichen gehören auch Forschende des Fraunhofer-Instituts für Integrierte Systeme und Bauelementetechnologie IISB in Erlangen. Mit ihrem Schwerpunkt „Cognitive Power Electronics 4.0“ integrieren sie künstliche Intelligenz in leistungselektronische Systeme. Mit der Förderung wollen sie zeigen, wie kommerzielle Cloud-Dienste ihre Forschung effektiv voranbringen können.

Text: **Martin Schellenberger** (Fraunhofer-Institut für Integrierte Systeme und Bauelementetechnologie IISB)

Die Nutzung von Cloud-Diensten ist in weiten Teilen unserer Gesellschaft zur Selbstverständlichkeit geworden – ob im privaten Bereich mit dem Smartphone als wesentlichem Treiber oder im beruflichen Umfeld, wo insbesondere die Coronakrise neue Potenziale zur cloudbasierten Zusammenarbeit eröffnet hat. Im Forschungsbetrieb ist die Cloud häufig noch nicht im Alltag angekommen. Das kann unterschiedliche Gründe haben: sei es, weil Universitäten leistungsstarke eigene Rechenzentren haben und damit kein unmittelbarer Bedarf besteht, oder weil der Rechner (und damit die Daten und das eigene Know-how in Form von Algorithmen und Programmen) „woanders“ steht – fern der räumlichen und administrativen Eigenverantwortung. Und nicht zuletzt bedeutet die Nutzung von Cloud-Diensten mittelfristig auch, dass nicht mehr in allen Bereichen eigenes Know-how genutzt und gepflegt wird. Hier gilt es, die Vorteile einer personellen Entlastung gegen dem potenziellen Verlust von Wissen abzuwägen.

> Die Cloud kann die Antwort auf viele Herausforderungen in der Forschung sein.

Die Cloud kann die Antwort auf viele Herausforderungen in der Forschung sein. Sie wirft aber auch Fragen auf, wie und in welchem Umfang sie in der Forschung eingesetzt und angepasst werden kann. Umso wichtiger ist es, vor dem Einstieg in Cloud-Dienste genau zu überlegen, welche Ziele durch die Nutzung der Cloud erreicht werden sollen. Aus diesem Grund haben wir uns im Rahmen des Projekts Open Clouds for Research Environments (OCRE) auf die Ausschreibung „1st Open Call for Cloud Funding for Research“ beworben. Damit haben wir die Chance, Dienstleistungen und Know-how der Cloud-Anbieter zu testen und Antworten auf unsere Fragen bezüglich der Nutzung von (kommerziellen) Cloud-Diensten in der Forschung zu finden.

Daran forschen wir

Im Fraunhofer-Institut für Integrierte Systeme und Bauelementetechnologie IISB in Erlangen forschen und entwickeln wir in den Bereichen Leistungselektronik, Halbleitertechnologie und Materialentwicklung. Im Forschungsschwerpunkt „Cognitive Power Electronics 4.0“ integrieren wir künstliche Intelligenz in leistungselektronische Systeme, zum Beispiel in elektrische Motoren, komplette Antriebsstränge oder Batteriesysteme. Diese können wir an eigenen Prüfständen vollständig testen[1]. Im konkreten Anwendungsfall der intelligenten Antriebstechnik kombinieren wir leistungsfähige Umrichter, die Elektromotoren beispielsweise in Elektroautos oder Förderanlagen ansteuern, mit künstlicher Intelligenz. Dabei entwickeln wir edge- oder cloudbasierte KI-Methoden, um aus kleinsten Stromschwankungen im Elektromotor auf dessen Zustand und potenziell auftretende Fehler schließen und so beispielsweise den Verschleiß der Lager rechtzeitig erkennen (Abbildung 1) zu können. Wir haben die Auswertekette von der Datenaufnahme, -weiterleitung und -verarbeitung bis hin zur KI-gestützten Entscheidungsfindung erfolgreich aufgebaut[2] und die Machbarkeit am Prüfstand demonstriert.

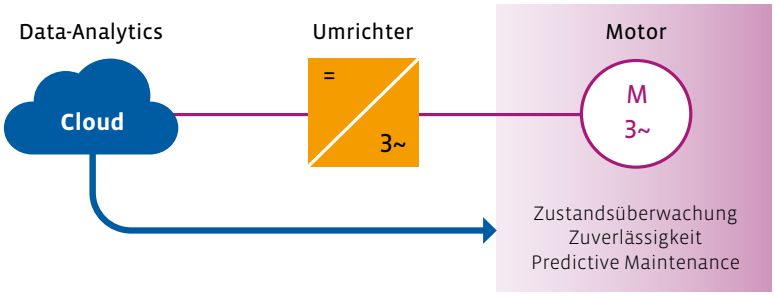


Abbildung 1: In der intelligenten Antriebstechnik werden Daten aus dem Antriebsumrichter genutzt, um mittels Methoden der künstlichen Intelligenz auf den Zustand des Elektromotors zu schließen

Verschleiß rechtzeitig erkennen: Aufnahme von elektrischen Daten eines Elektromotors am Prüfstand des Fraunhofer IISB *Foto: Kurt Fuchs / Fraunhofer IISB*

Die Entwicklung erfolgt derzeit ausschließlich unter Nutzung institutseigener Server, Datenbanken, Software und Workflows. Aufgrund der umfangreichen Daten und aufwendigen Berechnungen sowie der Entwicklung und Nutzung von KI-basierten Algorithmen käme hier folgerichtig die teilweise oder vollständige Nutzung von Cloud-Dienste infrage: sei es die flexible Nutzung von Speicher- und Rechenkapazitäten, die Entwicklung eigener Anwendungen in der Cloud mit den Werkzeugen des Cloud-Anbieters oder in geeigneten Fällen sogar die Nutzung fertiger Algorithmen und Softwarepakete des Cloud-Anbieters für die eigene Anwendung.

Ziele der Cloud-Nutzung

Im Rahmen des OCRE-Projekts erwarten wir folgenden konkreten Nutzen aus den Cloud-Diensten:

- **Fokus auf die eigene Kernkompetenz:** Als Rückgrat für unsere Datenverarbeitung und KI-Entwicklung können Cloud-Dienste uns dabei helfen, uns auf unsere Kernkompetenz zu konzentrieren. Das ist wichtig, um schnelle und substanzielle Forschungsergebnisse sowohl in öffentlich geförderten F&E-Projekten als auch in bilateralen Industrieprojekten mit hohem Technology-Readiness-Level zu erzielen.

- **Reduzierte Kosten und Aufwände:** Wir hoffen, dass die Kosten für institutsinterne Speicher- und Recheneinrichtungen substanziell sinken werden. Dies gilt es, kritisch zu prüfen, denn die tatsächlichen Kosten von Cloud-Diensten werden erst mit realen Anwendungsfällen sichtbar und nur eingeschränkt in Onlinebudgetrechnern abgebildet.

1 M. Schellenberger, B. Eckardt and V. Lorentz (2019), „So könnten leistungselektronische Schaltungen entscheiden“. Abgerufen am 1.4.2021 von https://www.all-electronics.de/so-koennten-leistungselektronische-schaltungen-entscheiden/

2 G. Roeder, X. Liu, M. Hofmann, M. Schellenberger, F. Hilpert and M. März, „Cognitive Power Electronics for Intelligent Drive Technology“, 10th International Electric Drives Production Conference (EDPC), Ludwigsburg, Germany, 2020, pp. 1–8, doi: 10.1109/EDPC51184.2020.9388182

- **Skalierbarkeit:**
Wir erwarten weniger Probleme bei der Übertragung und Speicherung großer Datenmengen, insbesondere nach erfolgreicher vollständiger Implementierung unseres Anwendungsfalls in der Cloud. Das würde den Rollout ähnlicher Lösungen auf weitere leistungselektronische Geräte erleichtern.

- **Dienstleistungsangebote:**
Wir möchten wissen, welche sicheren Marktplätze die Cloud-Betreiber anbieten und wie wir sie nutzen können, um unsere eigenen bewährten Algorithmen zur Verfügung zu stellen und neue Geschäftsmodelle mit Partnern zu testen.

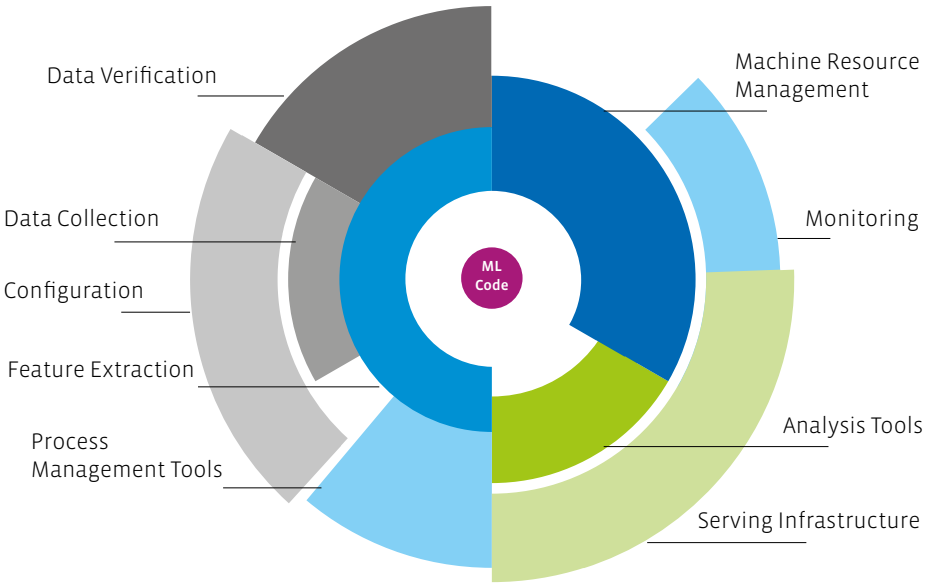


Abbildung 3: Die eigentlichen Machine-Learning-Algorithmen erfordern eine vergleichsweise riesige und komplexe Infrastruktur

Bisherige Erfahrungen mit der Cloud

Im Vorfeld unserer Bewerbung für das OCRE-Projekt konnten wir im Rahmen eines Hackathons erste Erfahrungen mit der Cloud sammeln. Von der Vielzahl an Cloud-Funktionen wollten wir vor allem ausprobieren, wie einfach sich unsere bestehenden lokalen Algorithmen tatsächlich mit den Werkzeugen der Cloud abbilden und auf virtuellen Maschinen ausführen lassen – die Aufgabenstellung bewegte sich also im Bereich „Platform as a Service“. Dabei zeigte sich, dass die Übertragung der Algorithmen schnell vonstattenging und wir unsere gewohnten Abläufe und Werkzeuge weiter verwenden konnten oder in ähnlicher Form in der Cloud wiederfanden. Das war für uns eine sehr positive Erfahrung, ebenso wie die Tatsache, dass die webbasierte Zusammenarbeit im Team gut funktionierte. Wir haben aber auch festgestellt, dass trotz guter Dokumentation der Cloud-Funktionalitäten der Einstieg ohne die im Hackathon gegebene Unterstützung des Cloud-Diensteanbieters erheblich länger gedauert hätte und uns manche fortgeschrittenen Funktionen und „Kniffe“ verborgen geblieben wären. Der Kostenaspekt lässt sich bei einer probeweisen Übertragung von Algorithmen kaum beurteilen – allerdings zeigte sich, dass die im Internet verfügbaren Kostenrechner der Cloud-Anbieter einerseits sehr komplex sind, andererseits aber so schwer zu konfigurieren, dass sie den eigenen Anwendungsfall nicht korrekt abbilden. Hier gilt es, die Kosten im tatsächlichen (Test-)Betrieb zu verfolgen. Dank der transparenten Werkzeuge ist das auch gut möglich.

> Das war für uns eine sehr positive Erfahrung.

Wenn „Cloud“ die Antwort ist – wie lauten eigentlich unsere Fragen?

Die geschilderten Gehversuche mit der Cloud betreffen nur einen kleinen Ausschnitt möglicher Cloud-Funktionalitäten, die wir nun im oben beschriebenen Anwendungsfall im OCRE-Projekt nutzen möchten: Wir benötigen zusätzlich eine skalierbare Infrastruktur, um erfasste Daten in einen sicheren Speicher zu übertragen (oft mehrere Gigabyte pro Tag und Gerät), KI-Algorithmen mithilfe dieser Daten zu trainieren und schließlich die Algorithmen auf Servern oder im Gerät vor Ort (Edge-Device) performant auszuführen.

Entscheidend ist nun, die richtige Balance zwischen der Investition in eigene und fremde Kompetenzen im Bereich der Dateninfrastruktur zu finden. Denn nur ein kleiner Teil tatsächlich implementierter KI-Systeme besteht aus den eigentlichen Machine-Learning-Algorithmen (Abbildung 3), während die erforderliche umgebende Infrastruktur vergleichsweise riesig und komplex ist[3]. Und wie bei vielen anwendungsorientierten Forschungseinrichtungen und Universitäten liegt unsere eigene Kompetenz vor allem im Domänenwissen, in der darauf aufbauenden Dateninterpretation und der Anpassung und Anwendung geeigneter KI-Algorithmen.

3 D. Sculley, G. Holt, et al., „Hidden technical debt in Machine learning systems“, Proceedings of the 28th International Conference on Neural Information Processing Systems - Volume 2 (NIPS‘15). MIT Press, Cambridge, MA, USA, 2503–2511.

FRAGENKATALOG FÜR DIE BEWERTUNG DER ZUR WAHL STEHENDEN CLOUD-DIENSTE

1. In Bezug auf die Nutzung zusätzlicher Speicher- und Rechenkapazitäten (oft bezeichnet als „IaaS“, Infrastructure as a Service):

- Ist die Leistungsfähigkeit der Datenhaltung in der Cloud ausreichend im Vergleich zur Nutzung lokaler Datenbanken?
- Welche (automatisierten) Möglichkeiten der Datenvorverarbeitung gibt es und wie leistungsfähig sind sie im Vergleich mit unseren selbst entwickelten Verfahren?
- Können wir von einer dateibasierten Datenübertragung zu einem (Echtzeit-)Streaming von Daten übergehen?
- Welche Kosten fallen im Vergleich zu unseren bisherigen, internen Lösungen an?
- Wie sicher und vertrauenswürdig ist die Cloud-Infrastruktur im Vergleich zu eigenen Lösungen?

2. In Bezug auf die Entwicklung eigener Anwendungen in der Cloud mit den Werkzeugen eines Cloud-Anbieters („PaaS“, Platform as a Service):

- Welche Werkzeuge stehen für die Datenverarbeitung sowie die Code- und Modellerstellung zur Verfügung und wie leistungsfähig sind sie?
- Wie einfach lassen sich existierende Codes und Modelle in die Werkzeuge des Cloud-Anbieters übertragen?
- Wie einfach lassen sich bereits eingespielte Abläufe aus den Bereichen Anforderungsdefinition, Datenerfassung und -bereinigung, Code-Entwicklung und –Test (oft lose unter dem Schlagwort „DevOps“ zusammengefasst) in die Cloud-Plattform übertragen? Welche Änderungen der eigenen Abläufe sind erforderlich?
- Welche Kosten fallen an, und ist ein Nutzen, z. B. im Hinblick auf Zeitersparnis, vereinheitlichte Abläufe oder verbesserter Qualität, sichtbar?

3. In Bezug auf die Nutzung fertiger Algorithmen oder Softwarepakete des Cloud-Anbieters für die eigene Anwendung („Saas“, Software as a Service):

- Wie leistungsfähig sind Algorithmen und KI-Modelle, die vom Anbieter zur Verfügung gestellt werden, wie gut sind sie dokumentiert und in welchem Umfang lassen sie sich anpassen und parametrieren?
- Wie effizient können Algorithmen und Modelle nicht nur in der Cloud, sondern auch vor Ort (Edge) genutzt werden?
- In welchem Maß sind andere Forschungspartner und Kunden bereit, sich auf die gemeinsame Entwicklung mit Cloudbasierten Diensten einzulassen?
- Ist ein hybrider Ansatz, z. B. der fallweise Übergang zu lokalen Lösungen („on-premise“) möglich?
- Welche Kosten fallen an und wie groß ist die Gefahr des „Vendor Lock-in“, wenn z. B. der Wechsel zu einem anderen Cloud-Anbieter aufgrund zu hoher Transaktionskosten unwirtschaftlich wird?

Für die strukturierte Bewertung der Cloud-Dienste – auch im Hinblick auf das bevorstehende Auswahlverfahren in OCRE – haben wir einen Fragenkatalog erstellt. Schwieriger zu bewerten ist jedoch, inwieweit durch die verstärkte Nutzung bestimmter Cloud-Dienste mittel- und langfristig die eigenen Kompetenzen geschwächt werden und ob das den durch die Cloud erzielten Benefit aufwiegt. Insbesondere für die Dienste vom Typ PaaS und SaaS erwarten wir hier spannende interne Diskussionen, welche Dienste als allgemein verfügbare „Commodities“ genutzt werden können und wo wir unser eigenes Know-how als Alleinstellungsmerkmal unabhängig von Cloud-Anbietern pflegen und ausbauen wollen.

Nächste Schritte

Im OCRE-Projekt werden wir im Rahmen des anstehenden Auswahlverfahrens zunächst einen Cloud-Anbieter auswählen und mit ihm die für unseren Anwendungsfall passende Edge-Cloud-Architektur entwickeln und umsetzen. Darauf folgt die schrittweise Übertragung unserer existierenden Entwicklungs- und Auswertekette für intelligente Antriebstechnik in die Cloud und wo nötig deren Anpassung. Nach der Auswertung der dabei gewonnenen Erfahrungen können wir schlussendlich entscheiden, ob „die Cloud“ überhaupt die richtige Antwort auf unsere Fragen ist und in welchem Umfang wir Cloud-Dienste für unsere Forschung künftig nutzen wollen. Fortsetzung folgt! ◆

Kurzmeldung

Meilenstein für BELLA: „Final Splice“ geglückt – Verlegung des Unterseekabels erfolgreich beendet

Grund, die Korken knallen zu lassen, gab es im EU-geförderten Projekt BELLA (Building the Europe Link with Latin America): Die Seeinstallation des 6 000 Kilometer langen transatlantischen Untersee-Glasfaserkabels, das einen direkten Datenaustausch zwischen Europa und Lateinamerika ermöglicht, konnte nun im Frühjahr 2021 nach vielen Jahren der Planung und Vorbereitung erfolgreich abgeschlossen werden.

2016 ging das Projekt an den Start: Die europäische Finanzierung wurde über Projekte und Serviceverträge mit drei Direktoraten der Europäischen Kommission (DG CONNECT, DG GROWTH, DG DEVCO) unter Dach und Fach gebracht, in denen z. T. auch lateinamerikanische Forschungsnetze als Partner eingebunden waren.

Am 2. August 2018 unterschrieben die beiden Dachorganisationen der europäischen und lateinamerikanischen Forschungsnetze, GÉANT und RedCLARA, den Vertrag mit EllaLink für das langfristige, uneingeschränkte Mitnutzungsrecht (Indefeasible right of use, IRU) an dem Unterseekabel – ein Drittel des verfügbaren Spektrums auf einem Faserpaar war somit für die nächsten 25 Jahre mit einer initialen Übertragungskapazität von 100 Gbps fest für Forschung und Wissenschaft reserviert.

Mit den darauffolgenden Vertragsabschlüssen mit den Firmen EllaLink und Alcatel Submarine Networks (ASN) 2019 stand den Bauarbeiten nichts mehr im Weg. Im nächsten Schritt legte das hydrografische Vermessungsschiff OGS Explora nach den Untersuchungen des Meeresbodens im Atlantischen Ozean die Route des Unterseekabels fest: Sie führt über den etwa 1 100 Kilometer von Brasilien entfernten Mittelatlantischen Rücken, ein gewaltiges Unterwassergebirge, das vom Arktischen Ozean bis zum Südzipfel Afrikas reicht und sich über rund 18 000 Kilometer erstreckt.

Nachdem das Unterseekabel Ende 2020 in Fortaleza gelandet war, wurde zu Beginn des Jahres 2021 der nächste BELLA-Meilenstein erreicht: Das Unterseekabel erreichte Europa in Sines. Dort wird derzeit auf rund 10 000 Quadratmeter Fläche die Kabellandestation Vasco da Gama gebaut, die die Basis für das Atlantik-Drehkreuz aus Unterseekabel und einem angeschlossenen Datenzentrum bilden soll. Weitere Landestationen auf Madeira und Portinho, Cabo Verde, folgten. Zusammen mit den

Ohne Umwege: direkter Datenaustausch zwischen Europa und Lateinamerika

Datenleitungen der verschiedenen Landrouten wird das BELLA-Kabel Datenzentren in São Paulo, Rio de Janeiro und Fortaleza sowie Lissabon, Madrid und Marseille miteinander verbinden. Derzeit nimmt der Datenverkehr nach Lateinamerika noch einen Umweg über Nordamerika. Mit der Seeroute kann die Latenzzeit der Datenübertragung um bis zu 60 Prozent verringert werden.

Der bisherige Höhepunkt im BELLA-Projekt: Anfang März 2021 fand mitten auf dem Atlantik an Bord des Kabellegerschiffs Île de Sein das finale Spleißen (Zusammenfügen) der Kabelenden von Sines in Portugal und Fortaleza in Brasilien statt. Damit steht die Verbindung in 4 500 Meter Tiefe, gemeinsam mit den Kabelsegmenten zu Land ist das Netz komplett. Im nächsten Schritt wird mit der Beleuchtung der optischen Fasern die Datenübertragung vorbereitet.

Voraussichtlich in der zweiten Jahreshälfte geht die Hochleistungsverbindung in Betrieb. Die Übertragungskapazität für die Forschungsnetze von zunächst 100 Gbps kann je nach Bedarf in den kommenden Jahren auch gesteigert werden. Von der niedrigen Latenzzeit und der sicheren Übertragung profitieren vor allem datenintensive Forschungsprojekte im Bereich der Astronomie und Satelliten-Erdbeobachtung. Als Mitglied im BELLA-Projektkonsortium vertritt der DFN-Verein in Deutschland die Interessen dieser Forschercommunity. ◆

Eine lange Reise neigt sich dem Ende und findet ihren Höhepunkt im finalen „Spleißen“ der Kabelenden von Sines in Portugal und Fortaleza in Brasilien
Fotos: EllaLink

Eine Auswahl an spannenden Videoclips zum Bau des Kabels sowie weitere Informationen finden Sie unter:
https://ella.link/news/videos/
https://bella-programme.redclara.net/index.php/en/

II. Quantenrevolution – die Welt der Qubits

Beamen, durch Wände gehen – In der Quantenwelt sind verrückte Dinge in den Bereich des Möglichen gerückt, aber noch sind wir in dieser Welt nicht zu Hause. Um die revolutionären Anwendungsmöglichkeiten der Quantentechnik zukünftig nutzen zu können, müssen wir sie erst einmal besser verstehen. Einen kurzen Einblick in die Welt der Qubits sowie einige grundlegende Mechanismen der Quantentechnik (ab Seite 27) wollen wir hier skizzieren. Wie Quantennetze aufgebaut sind und welchen Nutzen sie haben, erfahren Sie im nächsten Heft – Fortsetzung folgt!

Text: **Peter Kaufmann** (DFN-Verein), **Susanne Naegele-Jackson** (Friedrich-Alexander-Universität Erlangen-Nürnberg)

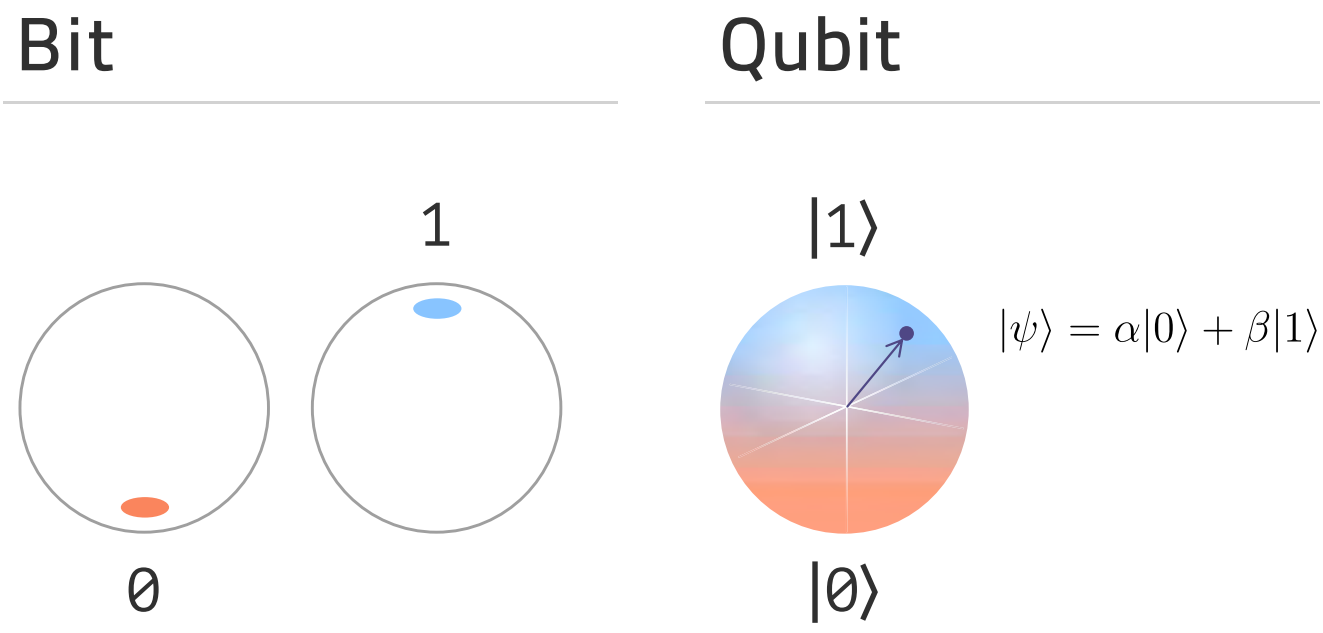


Illustration: Astibuag/Shutterstock

In der ersten Hälfte des 20. Jahrhunderts wurden die Grundlagen der modernen Physik, die Quantenphysik und die Relativitätstheorie entwickelt. Zwei zentrale Begriffe der Quantenphysik, die Unschärferelation und die diskontinuierliche Quantelung aller Prozesse und Eigenschaften, haben in der Zeit nach dem Zweiten Weltkrieg Eingang in fundamentale technische Entwicklungen gefunden. Die Ergebnisse der ersten Quantenrevolution, also die Atomtechnik (Waffen und Kraftwerke), die Festkörperphysik mit ihren bekanntesten Produkten, den Lasern und (Computer-)Chips sowie die Raumfahrt, sind aus unserem Alltag schon lange nicht mehr wegzudenken.

Eine zweite technische Quantenrevolution zeichnet sich nun seit der Jahrtausendwende ab. Sie findet Eingang in neue Computerarchitekturen (Quantencomputer), in neue Quantendatennetze und in neue Quantenmesssysteme (Quantensensortechnik). Der spektakulärste Erfolg der Quantensensortechnik zeigte sich bei der Entdeckung von Gravitationswellen im Jahr 2017.

Alle drei Bereiche der zweiten Quantengeneration haben längst die bloße Laborumgebung verlassen und werden in den nächsten Jahren zunehmend Eingang in die „Alltagstechnik“ finden. Davon werden auch die Datennetze betroffen sein.

Rechnen mit Qubits

Die Entwicklung von Konzepten zu Quantencomputern begann in den 90er-Jahren. Maßgeblich für deren Fähigkeiten ist die Verwendung der sogenannten Quantenbits oder auch Qubits (siehe Seite 27) zur Bewältigung von Rechenoperationen. Sie stellen extrem empfindliche Informationszustände dar. Alle technischen Entwicklungen haben das Ziel, möglichst viele Qubits für eine angemessene Zeit fehlerfrei aufrechterhalten zu können. Wir sprechen hier derzeit von etwa hundert Qubits, die Sekunden oder Minuten fehlerfrei aufrechterhalten werden sollen, schon hier werden die unterschiedlichen Dimensionen gegenüber der klassischen Datentechnik deutlich sichtbar.

Qubit-Fehler entstehen zum Beispiel durch Rauschen aufgrund externer elektrischer und magnetischer Felder, durch zu hohe Temperaturen oder durch magnetische Wechselwirkungen mit umgebenden Qubits (crosstalk).

Es gibt mehrere physikalisch-technische Varianten, um Qubits zu erzeugen und möglichst lange und fehlerfrei in ihrem Zustand zu halten. Google und IBM arbeiten mit supraleitenden Qubits, also mit stark gekühlten metallischen Leitern. In Europa wird bisher häufig auf Ionen-Qubits gesetzt, die in Ionenfallen durch elektromagnetische Felder stabilisiert werden. Darüber hinaus können Qubits auch durch orthogonale Polarisation von Photonen, durch das Manipulieren von Atomkernspins (Kernspinresonanz) und in Halbleiterstrukturen mit Elektronen erzeugt werden. Erst bei Quantencomputern mit mehr als 45 Qubits ergeben sich, Abschätzungen zufolge, Vorteile gegenüber klassischen Supercomputern.

In den letzten Jahren gab es beachtliche Fortschritte beim Bau von Quantencomputern:

- Google hat publikumswirksam im Jahre 2019 den Sycamore-Prozessor mit 53 Qubits präsentiert
- In einer Kooperation mit Google arbeitet das FZ Jülich an einem Quantencomputer mit 50–100 Qubits.
- Ein Quantencomputer von IBM-Q wird derzeit in Stuttgart aufgebaut und soll mit 20 Qubits arbeiten; derzeit testet IBM darüber hinaus einen Chip mit 50 supraleitenden Qubits.
- Im EU-Projekt AQTION wird an der Universität Innsbruck ein Quantencomputer entwickelt, der auf der Speicherung einzelner geladener Atome und deren Manipulation mit Laserlicht basiert. Verwendet wird aktuell ein Prozessor, der bis zu 50 Qubits unterstützt.

Verschlüsselungen neu denken

Die erkennbare Mächtigkeit der neuen Quantencomputer stellt vor allem die bisher verwendeten Sicherheitsstrukturen von Datennetzen vor neue Probleme. Zum Verständnis ist es nützlich, zwei unterschiedliche Ebenen zu betrachten, zum einen die gemeinsame Verwendung von geheimen Schlüsseln in Anwendungen (Nutzschlüssel) durch zwei beteiligte Kommunikationspartner (Sender: Alice; Empfänger: Bob) und zum anderen den anfänglich sicheren Transport dieser geheimen Nutzschlüssel von Alice zu Bob, der immer eine besondere Herausforderung darstellt.

Für den Bereich der oft bilateral verwendeten Nutzschlüssel werden entweder komplexe asymmetrische Schlüssel oder die überaus schwer zu knackenden symmetrischen Schlüssel verwendet. Beide Schlüsselarten werden unter dem Begriff der Post-Quantum-Cryptographie (PQC) bereits weiterentwickelt und können so sehr sicher gegen Angriffe durch Quantencomputer gemacht werden [ENISA].

Schwieriger sieht es zukünftig für den anfänglich sicheren Transport der Schlüsselinformationen aus. Konzeptionell haben sich dafür bisher die asymmetrischen Verschlüsselungen basierend auf der RSA-Methode als hervorragendes Werkzeug bewährt. Mit diesen ist es möglich, den Erstvorgang einer verschlüsselten Kommunikation höchst dialektisch gleichzeitig öffentlich (für die Verschlüsselung) und geheim (für die Entschlüsselung) in einer multilateralen offenen Umgebung zu gestalten. Die Sicherheit dieser Methode hängt jedoch von der Annahme ab, dass das prinzipiell mögliche „Knacken“ der asymmetrischen RSA-Schlüssel große Computerressourcen und viel Zeit benötigt und deshalb i. d. R. nicht praktikabel umgesetzt werden kann. Mit Quantencomputern und dem für sie

entwickelten Shor-Algorithmus wandelt sich diese Situation aber deutlich.

In Abbildung 1 sind Schlüssellänge und Zeitdauer für die Lösung verschiedener RSA-Algorithmen dargestellt. Während klassische Computer bei entsprechender Schlüssellänge sehr viele Jahre benötigen, lässt sich auch mit stark verlängerten Schlüssellängen nur (nicht skalierbare) „Zeit kaufen", bis der verlängerte asymmetrische RSA-Schlüssel mit der Kombination aus Shor-Algorithmus und Quantencomputer „zeitnah" gefunden werden kann.

Deutlich mehr Sicherheit versprechen asymmetrische PQC-Schlüssel, an deren Entwicklung intensiv gearbeitet wird. Das National Institute of Standards and Technology (NIST) hat dazu vor einigen Jahren einen Wettbewerb gestartet. Die PQC-Schlüssel werden jedoch auf der einen Seite einen recht hohen betrieblichen Zusatzaufwand erfordern und auf der anderen Seite steht deren erhoffte Sicherheit unter dem Vorbehalt, ob mit Quantencomputern nicht noch gänzlich neue mathematische Lösungsalgorithmen zur Entschlüsselung genutzt werden können (ähnlich dem Shor-Algorithmus für RSA-Schlüssel).

Grundlegend anders wird es daher erst mit der Verwendung sogenannter Quantenschlüssel für den anfänglich sicheren Transport der Nutzschlüssel, die dann auch weiter in den Anwendungen verwendet werden können. Mit Quantenschlüsseln wird das Sicherheitsproblem von der mathematischen Ebene in den Physikbereich verlagert und macht sie im Grundsatz unangreifbar (wenn man von der „Kleinigkeit" der technisch-industriellen Implementierungsfertigkeit absieht). Während die mathematischen Herausforderungen der asymmetrischen RSA-Schlüssel mit ausreichend Rechenkapazität (in Form von Quantencomputern) bewältigt werden können, sind im Gegensatz dazu die Quantengesetze, die den Quantenschlüsseln zugrunde liegen, durch nichts in der Welt auszuhebeln, auch nicht durch Quantencomputer. Eine erfolgreiche Implementierung von Quantensicherheitsstrukturen bietet also strukturell (d. h. als Alternative zu den bisherigen asymmetrischen RSA-Schlüsseln) eine Lösung für das anfänglich sichere Schlüsseltransportproblem.

> Quantengesetze, die den Quantenschlüsseln zugrunde liegen, sind durch nichts in der Welt auszuhebeln.

Physik ist der Schlüssel

Für Quantenverschlüsselungen und die dazugehörigen Quantennetze werden einige besondere Teilcheneigenschaften benutzt, die in bisherigen klassischen Datennetzen keine Rolle spielten. Dazu gehört zuallererst die Verwendung von **Qubits**, anstelle der klassischen Bits. Des Weiteren die sogenannte **Verschränkung**, also eine besonders „intensive Kopplung" zweier Qubits auf der Quantenebene. Diese macht die Informationsübertragung unangreifbar (oder genauer: niemals unbemerkt angreifbar). Und schließlich die sogenannte **Quantenteleportation**. Diese beschreibt einen besonderen Übertragungsmechanismus von Quanteninformationen, in welchem die ursprünglichen Informationsträger (Qubits) tatsächlich nicht selbst durch das Netz geschleust werden.

Für den gesamten Mechanismus der Quantenschlüsselübertragung wird allgemein der Begriff der „Quantum-Key-Distribution" (QKD) verwendet. Und wie es sich für ein vernünftiges Datennetz gehört, wird das Ganze auch durch spezifische Protokolle abgerundet, die QKD-Protokolle. Zu den ältesten und bekanntesten Protokollen gehört der BB84-Mechanismus (samt Nachfolgern). Auf die Einzelheiten dieser

Shor algorithm: prime number factorization in polynomial time

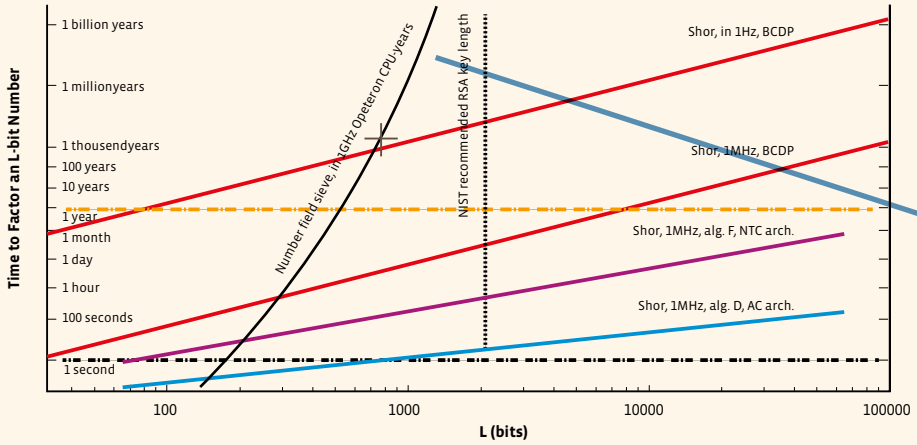


Figure: R. Van Meter and C. Horsman, "A blueprint for building a quantuam computer," Communications of the ACM, vol. 56, no. 10, pp. 84–93 (2013)

Abbildung 1: Im linken Bild ist für verschiedene Algorithmen (klassischer Rechner und Shor-Varianten auf Quantencomputern) der Zeitbedarf zur Auflösung eines RSA-Schlüssels mit der Bit-Länge L aufgetragen. Im rechten Bild ist die erwartete Qubit-Zahl der kommenden Quantencomputer abgeschätzt.

Protokolle wollen wir in kommenden Ausgaben näher eingehen.

Für die technisch-physikalische Umsetzung der Quantenkommunikation gibt es verschiedene Methoden, die auch die Teleportation und die Verschränkung unterschiedlich verwenden. Eine Methode wird „discrete-variable QKD“ (dv-QKD) genannt. Hier wird die diskrete Messung einzelner Photonen (ein Photon ist vorhanden: Ja/Nein) genutzt, um den Übertragungsvorgang zu implementieren. Die erforderliche Hardware muss daher einzelne Photonen messen und zählen können. Ein Problem sind die hohen Anforderungen an die Stabilität der Umwelt, um einen zu schnellen Zerfall (de-coherence) der Quantenzustände zu verhindern. Die dv-QKD-Methode verwendet zentral die Mechanismen der Teleportation und Verschränkung und erfordert für größere Reichweiten sogenannte Quanten-Repeater, die aber noch am Anfang ihrer technischen Entwicklung stehen. Für dv-QKD sind die theoretischen Grundlagen des Schutzes gegen Angriffe (Eavesdropper-Attacken) sehr gut gesichert.

„Moore‘s law for qubits“

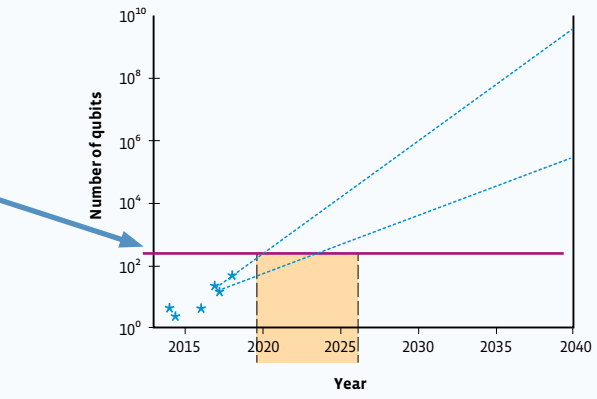


Figure: D. Aggarwal et al.: Quantum Attacks on Bitcoin, and How to Protect Against Them, Ledger, 2018, 3

Eine zweite Methode wird „continuous-variable QKD“ (cv-QKD) genannt. Hier wird ein kohärenter Vielteilchenansatz genutzt, der quantenstatistische Mechanismen zur Grundlage hat. Es werden „homodyne Detektoren“ zur Analyse der übertragenen elektromagnetischen Felder (ihrer Amplitude und Phase) genutzt. Die Ergebnisse zeigen kontinuierliche Werte (daher der Name). Allerdings ist der Formalismus bezüglich der Sicherheit gegen hochrangige Angriffe bisher weniger umfassend bewiesen.

Die hier getroffenen Aussagen bezüglich dv-QKD/cv-QKD können die technischen Aspekte nur umreißen, da in den Entwicklungslaboren eine große Dynamik bezüglich der theoretischen Grundlagen und der technischen Umsetzungen besteht.

Aktivitäten in der Quantenwelt

In vielen Ländern gibt es mittlerweile Initiativen zur Förderung von Quantentechnologie und -forschung, aber auch im Hinblick auf die Nachwuchsförderung passiert viel. Die Quantentechnologie kann nur vorangetrieben werden, wenn unterstützende Technologien und Zulieferungsindustrien Hand in Hand mit der Quantenforschung in Angriff genommen werden.

- In Deutschland startete das BMBF die Initiative QuNet [QUNET]. Die Initiative verfolgt das Ziel, zunächst ein Pilotnetzwerk für absolut abhörsichere Übertragungen aufzubauen. Mit einem solchen Netz könnten später alle Bundeseinrichtungen verbunden werden. Die erste Projektphase mit einem Budget von 12,8 Millionen Euro wurde bereits im Dezember 2020 abgeschlossen. Hier ging es in erster Linie darum, diverse Technologien zu untersuchen, ein Proof-of-Concept-Netz zunächst als hybride Lösung aufzubauen und die Anwendbarkeit zu testen. Zwei weitere Projektphasen von QuNet werden über die nächsten sieben Jahre fortgesetzt. Insgesamt stellt das BMBF in der derzeitigen Legislaturperiode 650 Millionen Euro für die Erforschung von Quantentechnologien zur Verfügung.

- Ein weiteres deutsches Quantenprojekt ist das Projekt „German Quantum Computer based on Superconducting Qubits“, kurz GeQCoS. Das Projekt hat im Februar 2021 begonnen und wird vom BMBF mit 14,5 Millionen Euro gefördert. Es hat zum Ziel, einen neuen Quantenprozessor basierend auf supraleitenden Qubits zu entwickeln.

- Die Entwicklung eines halbleiterbasierenden Quantenprozessors Made in Germany ist das Ziel des Projekts QUASAR. Es hat eine Laufzeit von vier Jahren (bis Januar 2025) und wird vom BMBF mit über 7,5 Millionen Euro finanziert.

- Ein weiteres neues Projekt (seit Februar 2021) ist DAQC – Digital-Analoge Quantencomputer. In dem Projekt wollen die teilnehmenden Einrichtungen einen digital-analogen Quantencomputer zusammen mit der dazugehörigen Kalibrier- und Steuertechnik herstellen. DAQC wird vom BMBF mit 12,4 Millionen Euro gefördert.

Sehr umfangreiche Quanteninitiativen wurden unter anderem auch in den USA und China ins Leben gerufen: Die USA starteten 2018 den National Quantum Initiative Act mit einer Laufzeit von zehn Jahren und einer Förderung von 1,2 Milliarden Dollar. Auch China verfolgt seit 2016 eine nationale Quantenstrategie, die auf eine Laufzeit von mindestens zehn Jahren ausgelegt ist

und ebenfalls auf eine Förderung in Milliardenhöhe zugreifen kann.

Aber auch viele europäische Länder haben inzwischen ihre eigenen Quanteninitiativen gestartet. So setzt Tschechien bereits seit 2016 auf eine nationale Quanteninitiative mit Fokus QKD und Quantum Communication und ist Teilnehmer an verschiedenen europäischen Projekten. Im Vereinigten Königreich gibt es das „UK National Quantum Technologies (UKNQT) Programme“ , das seit 2019 bereits in einer zweiten Phase für weitere fünf Jahre läuft. Polen verfolgt die Initiative NLPQT (National Laboratory for Photonics and Quantum Technologies) seit 2019 und betreibt Quantenforschung, vor allem in den Bereichen QKD, Uhren und Sensortechniken. Auch Österreich plant ab Mai 2021 ein neues Quanteninfrastrukturprojekt, das auf die kommenden fünf Jahre ausgelegt ist, nachdem eine erste österreichische Quanteninitiative von 2018 kurz vor dem Abschluss steht.

Das derzeit bedeutendste europäische Projekt ist das Quantum Flagship Program [FLAGSHIP], das 2019 ins Leben gerufen wurde und auf zehn Jahre ausgelegt ist. Die EU stellt dafür bis zu eine Milliarde Euro zur Verfügung.

> Die EU stellt dafür bis zu eine Milliarde Euro zur Verfügung.

Eine weitere europäische Initiative ist EuroQCI (European Quantum Communication Infrastructure); an diesem Programm sind mittlerweile 25 Länder (inklusive Deutschland) beteiligt. EuroQCI verfolgt vor allem das Ziel, eine europaweite Infrastruktur basierend auf hochsicheren Quantennetzen aufzubauen und den Austausch und die Entwicklung von Quantentechnologien und möglichen Standards gemeinsam voranzutreiben.

Auch in mehreren NRENs (z. B. CESNET und PIONIER/PSNC) und im GÉANT Projekt GN4 wird an hochsicherer Kommunikation mit Quantenschlüsselaustauschverfahren gearbeitet. GÉANT hat das Ziel, die betreffenden Informationen aufzuarbeiten, bereitzustellen und die Zusammenarbeit der NRENs im Bereich der Quantennetze zu fördern. Anfang 2021 ist dazu ein White Paper [GÉANT] veröffentlicht worden.

Ein Ausblick

Die moderne Quantentechnik wird insbesondere im Bereich von Rechnern und Datennetzen zu markanten Ergänzungen der klassischen Technik führen. Die entsprechenden Entwicklungen haben inzwischen den Sprung vom Labor zum Test- und Piloteinsatz geschafft.

Sie beinhalten eine technisch-wissenschaftliche Revolution und haben auch eine sehr hohe volkswirtschaftliche Bedeutung für Anwendungen im Bereich der Hochleistungsrechner und der Sicherheitsstrukturen, aber auch vieler Mess- bzw. Sensortechniken (Rohstofferkundung, Medizintechnik, Raumortung, Zeitmessungen usw.)

Zur Vorbereitung auf Anwendungen in Datennetzen bietet der DFN-Verein mit dem Wissenschaftsnetz und seinen „belastbaren“ Nutzerumgebungen ein hervorragendes Umfeld für frühzeitige Test- und Entwicklungsprojekte.

Ein wichtiger Bestandteil der Entwicklungsanforderungen ist dabei die Aus- und Fortbildung bezüglich dieser neuartigen technischen Umgebungen und die Sichtbarmachung der Möglichkeiten und Notwendigkeiten. Die Anforderungen an Quantennetze werden gegenwärtig vor allem durch Sicherheitsanwendungen, aber zukünftig sicherlich auch vermehrt durch Sensoranwendungen bestimmt. Da es naturgemäß noch kein fertiges Architekturkonzept für die neue Netztechnik gibt (im Rahmen der IRTF-QIRG wird intensiv daran gearbeitet), werden alle aktuell präsentierbaren technischen Umsetzungen nur Bausteine auf dem Weg zu einem Gesamtkonzept sein können. Auf den Aufbau von Quantennetzen sowie deren Nutzung für die QKD-Technik werden wir uns in einem weiteren Artikel konzentrieren.

PROJEKTTEILNEHMER

- **QuNet:** Fraunhofer-Institut für Angewandte Optik und Feinmechanik (IOF), Fraunhofer-Institut für Nachrichtentechnik, Heinrich-Hertz-Institut (HHI), Deutsches Zentrum für Luft- und Raumfahrt e. V., Max-Planck-Institut für die Physik des Lichts
- **GeQCoS:** Bayerische Akademie der Wissenschaften, Fraunhofer-Institut für Angewandte Festkörperphysik (IAF), Infineon Technologies AG, Karlsruher Institut für Technologie (KIT), Friedrich-Alexander-Universität Erlangen-Nürnberg, Forschungszentrum Jülich GmbH
- **Quasar:** Forschungszentrum Jülich GmbH, HQS Quantum Simulations GmbH, IHP GmbH, Fraunhofer-Institut für Angewandte Festkörperphysik (IAF), Fraunhofer-Institut für Photonische Mikrosysteme (IPMS), Infineon Technologies Dresden GmbH & Co. KG, Universität Konstanz, Universität Regensburg, Leibniz-Institut für Kristallzüchtung im Forschungsverbund Berlin e. V.
- **DAQC:** QM Germany GmbH, Infineon Technologies AG, Forschungszentrum Jülich GmbH, Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften, Freie Universität Berlin

Grundlegende Mechanismen für ein Quanteninternet

Qubits

Ein klassischer Rechner arbeitet binär mit den Bit-Zuständen {0,1}. Ein „Quanten-Bit“ (Qubit) existiert dagegen als beliebige Überlagerung (Superposition) der zwei binären Basismöglichkeiten (also als beliebige Kombination im zweidimensionalen Raum der Achsen $|0\rangle$ und $|1\rangle$):

$$\text{Qubit} = a\,|0\rangle + b\,|1\rangle$$

$|X\rangle$ bezeichnet einen Quantenzustand des Systems, hier die Binärzustande $|0\rangle$ oder $|1\rangle$. Die (komplexen) Koeffizienten a/b sind die Wahrscheinlichkeits-amplituden der Zustände.

Man kann grundsätzlich verschiedene physikalische Eigenschaften zur Erzeugung des Qubit-Raums verwenden, z. B. Elektronen-Spin, Photonen-Polarisierung oder atomare Energiezustände. Durch eine Messung „kollabiert“ die überlagerte quantenmechanische Qubit-Funktion **irreversibel** zu den klassischen Messergebnissen $|0\rangle$ oder $|1\rangle$. Das Ergebnis ist aber nicht deterministisch ableitbar – die Wahrscheinlichkeit für ein Messergebnis beträgt $|a|^2$ bzw. $|b|^2$, wobei $|a|^2 + |b|^2 = 1$.

Werden mehrere Qubits in einem Quantenzustand kombiniert, steigt der Zustandsraum exponentiell (2^n) an und alle möglichen Teilzustände überlagern sich zum Gesamtzustand. Beispiel: Mit n=zwei (Qubits) erhält man den vierdimensionalen Zustandsraum:

$$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

$|01\rangle$ bedeutet Qubit-1 ist im Zustand $|0\rangle$ und Qubit-2 ist im Zustand $|1\rangle$.

Mit anderen Worten: Der Zustandsraum eines klassischen Rechners umfasst 2^n **Elemente**, wobei n die Bitzahl ist, während der Zustandsraum eines Quantenrechners 2^n **Dimensionen** umfasst. Aus diesem Unterschied leitet sich die besondere „Rechenkraft“ eines Quantenrechners ab.

Verschränkung (Entanglement)

Teilchen (Elektronen, Photonen, Atome …) können auf viele Arten miteinander verkoppelt werden, mal eng oder mal weniger eng. Eine spezifische Art von Kopplung vollziehen Atome z. B. bei der Bildung von Kristallen. Bei solchen Kopplungen bleiben die beteiligten Teilchen als weiterhin unabhängige Teilchen bestehen.

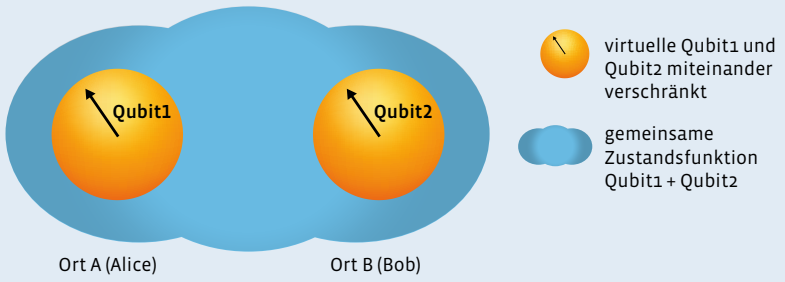


Abb. A: Zwei Teilchen (Qubits) in der Verschränkung als Bi-Teilchen

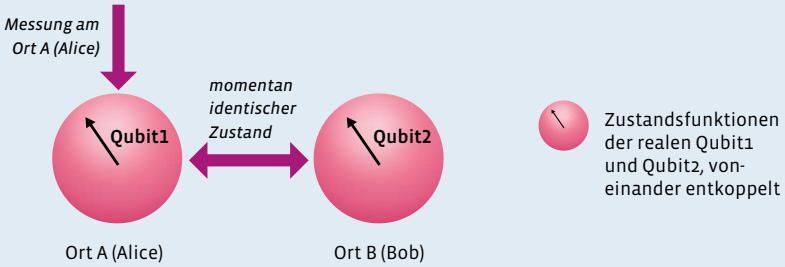


Abb. B: Zwei frei gewordene Teilchen (Qubits) nach der Messung am Qubit1

Abbildung 2: Verschränkung und Messung zweier Qubits

Die Verschränkung (Entanglement) ist dagegen eine besonders „intensive“ Art der Kopplung, bei der die ursprünglich unabhängigen Einzelteilchen in einen neuen gemeinsamen Zustand (beschrieben durch eine gemeinsame Quantenfunktion) übergehen. In diesem Zustand existieren sie nicht mehr voneinander getrennt, sie bilden stattdessen eine Art neues gemeinsames Teilchen: ein Bi-Elektron, ein Bi-Photon usw.

Außerdem kommt eine weitere Besonderheit ins Spiel. Wir alle sind es gewohnt, klassische Teilchen einem Ort im Raum zuordnen zu können. In der Quantenphysik wird dagegen jedes Teilchen durch eine Quantenfunktion beschrieben, die im Raum „verschmiert“ ist. Die üblichen Teilcheneigenschaften (Ladung, Drehimpuls …) gelten überall in dieser „verschmierten“ Quantenfunktion. Dies gilt auch für die oben erwähnten Bi-Teilchen. Die Distanz zwischen den Einzelteilchen im Bi-Teilchen spielt keine Rolle für die physikalische Eigenschaft der Verschränkung (für andere Aspekte schon).

Wie im Abschnitt „Qubits“ beschrieben, führt jede Messung zu einer Zerstörung des Quantenzustandes und zu einem ganz klassischen, festen („unverschmierten“) Messergebnis. Das gilt auch bei der Messung eines Bi-Teilchenzustandes. Allerdings mit der Besonderheit, dass das Bi-Teilchen bei der Messung in seine ursprünglichen Einzelteilchen zerfällt und diese Einzelteilchen in diesem Moment jeweils identische Eigenschaften besitzen, z. B. eine identische Polarisation.

Ist es also möglich, an Ort A eine Eigenschaft des dort aus dem Bi-Teilchen herauskommenden Teilchen-1 zu messen, so kennt man ganz genau die entsprechende Eigenschaft des Teilchen-2 am Ort B, egal wie weit beide voneinander entfernt sind. Diese momentane „scheinbare Fernwirkung“ steht übrigens nicht im Widerspruch zur Relativitätstheorie mit ihren Wirkungsbeschränkungen durch die Lichtgeschwindigkeit, da die Bi-Teilchenfunktion sich zuvor gemäß den Gesetzen der Relativitätstheorie mit höchstens Lichtgeschwindigkeit im Raum verteilt hat. Die Möglichkeit, verschränkte Teilchen mit ihren identischen „Ferneigenschaften“ zu benutzen, ist eine fundamentale Besonderheit in den Quantennetzen und kann für verschiedene Anwendungen genutzt werden. Es ist sogar möglich, mehr als zwei Teilchen zu einem gemeinsamen Multi-Teilchen zu verschränken.

Eine Eigenheit soll noch erwähnt werden, die besonders für Sicherheitsanwendungen (Verschlüsselungen) wichtig ist. Verschränkungen können nicht „geteilt“ werden, es kann kein „Dritter“ **unbemerkt** daran teilnehmen oder hineinschauen. Eine Verschränkung kann nämlich nicht eingesehen (d. h. gemessen) werden, ohne sie unwiderruflich zu zerstören (No-Cloning-Theorem) und damit das fremde Eindringen bekannt zu machen. Auch das ist anders als in „klassischen“ Verhältnissen, bei denen Datenbits unterwegs im Prinzip unbemerkt kopiert/abgezweigt werden können.

Bell-Paare

Ein **sehr vereinfachender Aspekt** der Quantenkommunikation ist, dass man häufig nicht beliebige verschränkte Quantenzustände aus dem vierdimensionalen Zustandsraum transportieren muss, sondern nur sogenannte Bell-Paare. Für die Bildung von Zwei-Qubit-Zuständen steht eigentlich der gesamte vierdimensionale Zustandsraum zur Verfügung, siehe auch Abschnitt Qubit:

$$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

Bell-Paare sind nun speziell verschränkte Zwei-Qubit-Zustände aus diesem gesamten Zustandsraum (mit unendlich vielen Zustandsmöglichkeiten), nämlich die vier quasi-symmetrischen Zustände:

$$|00\rangle + |11\rangle$$
$$|00\rangle - |11\rangle$$
$$|01\rangle + |10\rangle$$
$$|01\rangle - |10\rangle$$

(die Normierungsfaktoren a, b, c, d wurden zwecks Übersichtlichkeit weggelassen)

Jedes der vier obigen Bell-Paare kann darüber hinaus in jedes andere Bell-Paar transformiert werden; ein Bell-Paar steht also für alle vier Bell-Paare. Diese lokalen Transformationen zu den jeweils anderen Bell-Paaren können mittels einer Serie von Ein-Qubit-Gates erreicht werden. Eine Verteilung (inkl. Versendung der Bestandteile) von Bell-Paaren zwischen Quantennetz-Knoten ist wesentlich einfacher als die Verteilung beliebiger verschränkter Zwei-Qubit-Paarzustände.

Bell-Paare bilden außerdem die maximal verschränkte Zwei-Qubit-Untermenge der (unendlichen) Gesamtheit aller Zwei-Qubit-Zustände. Maximal verschränkt bedeutet, dass sie die stärksten nichtklassischen Korrelationen aller möglichen Zwei-Qubit-Zustände besitzen, was z. B. die Stabilität erhöht und die Fehleranfälligkeit reduziert.

Insgesamt stellen Bell-Paare daher ein herausgehobenes Werkzeug für die Quantenkommunikation dar, die insbesondere bei der Quantenteleportation im Zentrum stehen.

Quantenteleportation

Mit der Verteilung von Bell-Paaren ergibt sich die Möglichkeit, beliebige andere verschränkte Qubit-Zustände zu verteilen (quasi in huckepack). Der entsprechende Vorgang wird Quantenzustandsteleportation oder einfach Teleportation genannt. Die Teleportation nimmt einen unbekannten Quantenzustand C (ein Qubit C) vom Quellort Alice und erzeugt ihn identisch (und weiterhin unbekannt) am Zielort Bob. Am Quellort Alice existiert der Quantenzustand C dann nicht mehr, wodurch das No-Cloning-Theorem nicht verletzt wird. Was ist die Abfolge einer Teleportation?

a) Zuerst wird ein verschränktes Bell-Paar (A, B) zwischen Quellort Alice und Zielort Bob verteilt. Das verschränkte Bell-Paar

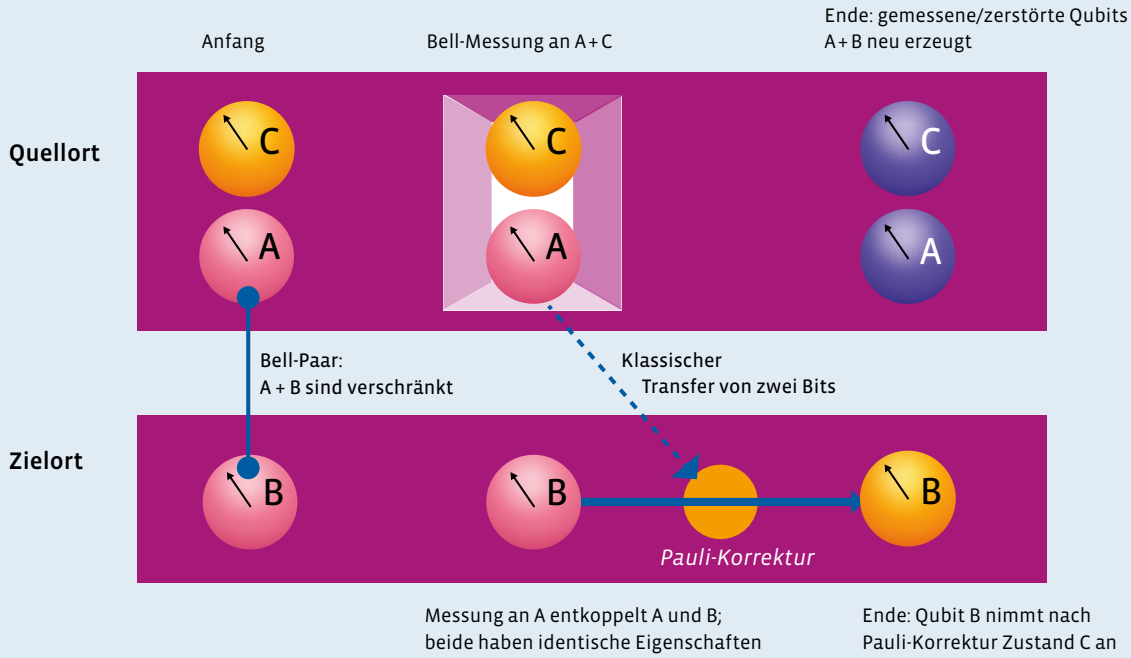


Abbildung 3: Quantenteleportation mit Bell-Paaren

bildet einen kohärenten Zweiteilchenzustand, in dem A und B nicht zu unterscheiden sind (siehe Abbildung 3).

b) Dann wird am Quellort Alice das unbekannte Qubit C mit dem dort befindlichen Qubit A des zuvor verteilten Bell-Paares verschränkt, was eine vorherige Messung des Qubits A am Quellort Alice beinhaltet. Die Summe dieser Operationen (Messung und Neuverschränkung) wird Bell-Messung genannt.

c) Damit sind die beiden verschränkten Qubits (A, B) des ursprünglichen Bell-Paares in unabhängige Zustände übergegangen, d. h. ihre Verschränkung ist beendet. Zuvor hat die Messung von A die beiden Qubits (A, B) aber in einen identischen Ergebniszustand gebracht. Man kann sagen, dass der bisherige gemeinsame Quantenzustand von (A, B) durch die Messung in ein identisches Doppelmessergebnis überführt worden ist (siehe Abschnitt „Verschränkung“).

d) Am Quellort Alice hat die Messung von A zusammen mit der Neuverschränkung (A, C) eine von vier möglichen Zustandsinformationen erbracht (zwei klassische Bits als Kombination von 0 und 1 zu: 00, 01, 10, 11), wobei durch den Messprozess beide ursprünglichen Qubits A + C zerstört worden sind. Über einen klassischen Datenkanal wird nun diese 2-Bit-Information über den Zustand (A, C) am Quellort Alice zum Zielort Bob geschickt. Aus der 2-Bit-Information und dem ehemals verschränkten Qubit B wird am Zielort Bob anschließend eine Transformationsfunktion (der Pauli-Operator führt die sogenannte Pauli-Korrektur durch) abgeleitet, die dieses Qubit B in den Zustand C (also den Zustand des Quellort Alice = Qubit C) überführt: B → C

Am Ende befindet sich der unbekannte Quantenzustand Qubit C vom Quellort Alice am Zielort Bob, ohne dass dieses Qubit C jemals selbst in das Netz hineingebracht und transportiert worden ist. Das Quantennetz musste nur Bell-Paare (also speziell verschränkte Teilchen) zwischen den Quantenknoten verteilen und ein zugehöriges klassisches Datennetz musste zusätzlich zwei klassische Bits transportieren. ◆

WEITERFÜHRENDE INFORMATIONEN

Für das gesamte Gebiet gibt es eine sehr große Anzahl wichtiger Arbeiten. Neben den folgenden (wenigen) Quellen verweisen wir vor allem auf die Webseite im WiN-Labor der Universität Erlangen (https://www.win-labor.dfn.de/), auf der weitere Informationen und Quellenangaben zur Verfügung stehen.

- [GÉANT]: https://www.geant.org/Resources/Documents/GN4-3_White-Paper_Quantum-Technologies-Status-Overview.pdf, Januar 2021
- [ENISA]: ENISA, Post-Quantum Cryptography, Editors: Smart, Lange, Februar 2021, (https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation)
- [FLAGSHIP]: https://qt.eu/about-quantum-flagship/
- [QUNET]: https://www.qunet-initiative.de/

Security Operations im DFN – die technische Basis

Prävention, Erkennung und Reaktion werden im neuen DFN-Dienst für Security Operations intensiv miteinander verzahnt. Das Herz des SOC-Systems bilden neue technische Komponenten und Services, die die bewährte CERT-Infrastruktur ergänzen. Auch ohne großen Installations- und Betriebsaufwand beim Teilnehmer können akute Bedrohungen der IT-Sicherheit so schneller erkannt werden.

Text: **Reinhard Sell** (DFN-CERT Services GmbH)

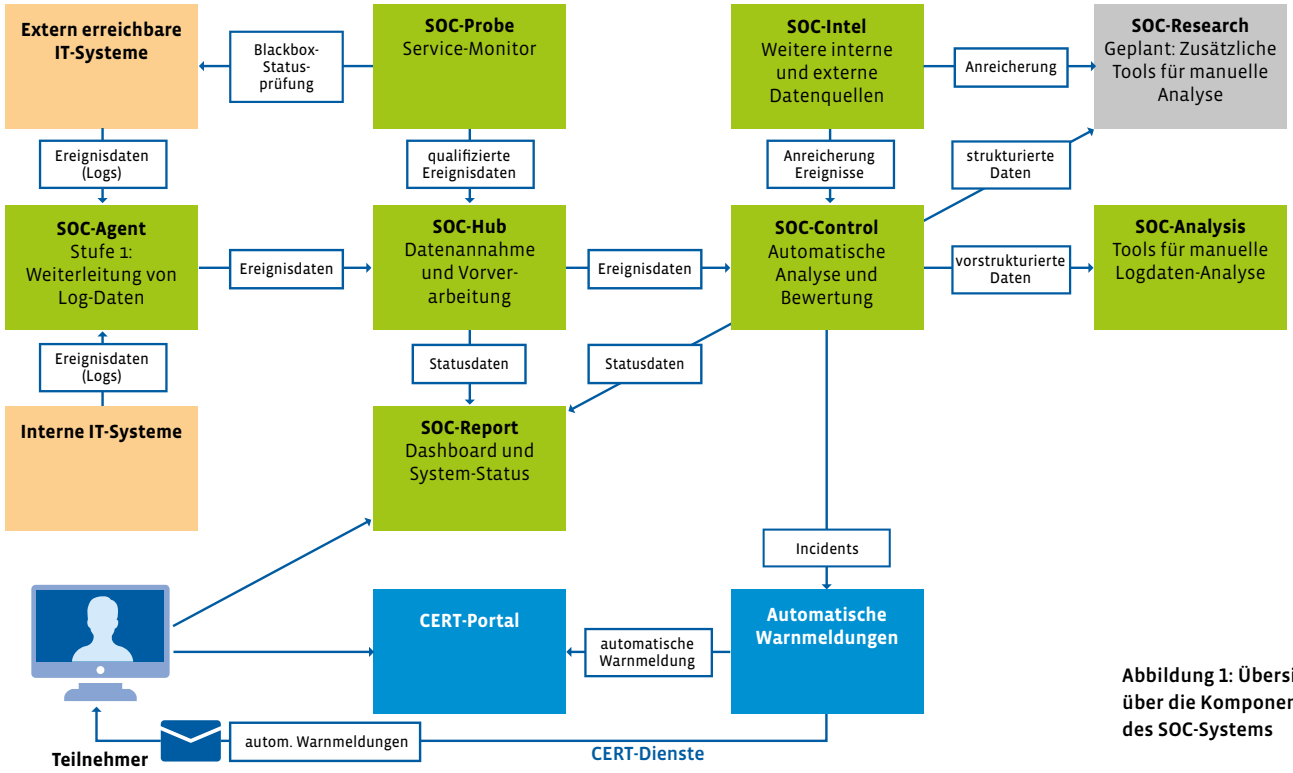


Abbildung 1: Übersicht über die Komponenten des SOC-Systems

Der neue DFN-Dienst für Security Operations wird vom DFN-Verein gemeinsam mit dem DFN-CERT entwickelt und betrieben und kann sich dabei auf viele bereits vorhandene und bewährte Systeme und Prozesse stützen. Insbesondere die Erfahrungen aus dem etablierten DFN-CERT-Dienst sowie der Incident Response-Bearbeitung am DFN-CERT spielen auch bei dem neuen Service eine zentrale Rolle. Darüber hinaus bauen die Security Operations auf der bereits vorhandenen Threat Intelligence-Infrastruktur auf wie die international vernetzte MISP-Community, eigene Honeypots und Darknet-Scanner oder die Netzwerküberwachung durch die NeMo-Systeme. Dazu kommen neue Komponenten zur passiven und aktiven Suche nach sicherheitsrelevanten Vorfällen wie ein System zur Analyse von Logdaten oder ein Monitoring für Services wie Webserver, DNS oder

E-Mail-Server. Um alle diese Systeme in geeigneter Weise zu integrieren, sind einige weitere Komponenten nötig, die den Kern des neuen SOC-Systems bilden.

Wichtige Kriterien

Für den Entwurf der Systemarchitektur waren folgende Eigenschaften relevant:

- Zuverlässige automatische Erkennung von sicherheitsrelevanten Vorfällen und automatische Weitergabe an die Teilnehmer bei gleichzeitig geringer Rate von False Positives
- Geringer Arbeitsaufwand für Teilnehmer durch weitgehende Weiterverwendung etablierter Meldekanäle sowie geringen Administrationsaufwand
- Gute Erweiterbarkeit, um regelmäßig weitere Erkennungsregeln hinzufügen bzw. bestehende Regeln optimieren zu können
- Flexible Struktur, um jederzeit zusätzliche Datenquellen oder Überwachungssysteme – auch mit neuen Protokollen und Formaten – integrieren zu können
- Umfassende Analysemöglichkeiten für die IT-Security-Experten des DFN-CERT, um neue IoC-Muster (Indicators of Compromise) entdecken zu können und daraus entsprechende Analyseregeln für die automatische Erkennung zu definieren
- Nach Möglichkeit Einsatz von (Open-Source-)Standardapplikationen: die eigene Entwicklung von proprietären Applikationen ist nur vorgesehen, wenn es wirklich notwendig ist

Automatische Ereignisverarbeitung

Die technische Plattform des SOC-Systems besteht aus verschiedenen Komponenten, die in Abbildung 1 schematisch dargestellt werden. Die Grafik zeigt insbesondere die Einbettung in die bestehende CERT-Infrastruktur. Zunächst werden die Komponenten beschrieben, die die automatische Verarbeitung der Ereignisdaten vornehmen, d. h. die nach IoC-Mustern suchen und ggf. automatische Warnmeldungen an die betroffenen Teilnehmer schicken.

Die Komponente SOC-Agent ist das einzige Teilsystem, das innerhalb der IT-Infrastruktur des Teilnehmers installiert und betrieben werden muss. Der SOC-Agent dient dazu, relevante Ereignisdaten im lokalen Netz des Teilnehmers zu erfassen und zur weiteren Verarbeitung an das zentrale SOC-System zu senden. Während der Pilotphase agiert der SOC-Agent noch rein passiv und leitet lediglich eine Auswahl vorhandener Logdateien an das SOC-System weiter.

In späteren Ausbaustufen werden weitere Funktionen den SOC-Agenten ergänzen, um einerseits eine Vorselektion und Vorverarbeitung der Ereignisdaten vorzunehmen und andererseits auch zusätzliche Systeme zur Netzwerküberwachung wie IDS oder Netflow-Sensorik zu integrieren. Soweit möglich, wird der SOC-Agent bereits selbst eine Analyse und Bewertung der Ereignisdaten vornehmen. Der Mehrwert eines zentralen SOC-Systems liegt aber gerade darin, dass lokale Ereignisdaten mit weiteren Datenquellen korreliert werden können, wodurch die Relevanz und Qualität der Bewertung erheblich verbessert werden.

> Der Mehrwert ist, dass lokale Ereignisdaten mit weiteren Datenquellen korreliert werden können.

Alle SOC-Agents der Teilnehmer schicken die relevanten Ereignisdaten an die Komponente SOC-Hub. Hier finden eine Normalisierung und die weitere Vorselektion der Daten statt. Insbesondere wird jedes Ereignis um Meta-Daten zur Quelle und zum Eingangskanal ergänzt, um jederzeit eine eindeutige Zuordnung zum Teilnehmersystem gewährleisten zu können.

Die eigentliche Analyse und Bewertung der Ereignisdaten werden anschließend von der Komponente SOC-Control vorgenommen. Dazu verwendet SOC-Control einen dynamischen Satz von Mustern und Regeln und greift insbesondere auf weitere externe und interne Datenquellen (SOC-Intel, s. u.) zu, um die Ereignisdaten mit weiterem Kontext anzureichern.

Sobald SOC-Control einen sicherheitsrelevanten Vorfall (Incident) erkannt hat, wird das entsprechende Ereignis über die etablierten CERT-Dienste als automatische Warnmeldung per E-Mail an den betroffenen Teilnehmer verschickt bzw. ist vom Teilnehmer über das CERT-Portal abrufbar. Darüber hinaus informiert das DFN-CERT bei einer Beteiligung Dritter im Rahmen seiner bestehenden Kanäle andere betroffene CERTs und ISP, um eine weitere Vorfallsbearbeitung zu ermöglichen.

Das, was in der Abbildung unter dem Begriff SOC-Intel zusammengefasst ist, besteht tatsächlich aus einer Vielzahl unterschiedlicher interner und externer Datenquellen. Alle diese Quellen werden vom SOC-System genutzt, sind aber nicht direkt Teil der SOC-Infrastruktur bzw. werden auch für andere Zwecke verwendet. Aufgrund der flexiblen Architektur können bei Bedarf weitere Datenquellen hinzugenommen werden, um das System zu erweitern.

Zu SOC-Intel gehören Systeme wie MISP, IP-Blocklisten, Daten über die Modellierung der DFN/X-WiN-Netzwerkstruktur oder Netflow-Daten der X-WiN-Kernrouter. Diese Datenquellen können zum einen zur Anreicherung der Ereignisdaten verwendet werden, um die Erkennung von Incidents zu verbessern oder überhaupt erst möglich zu machen. Zum anderen können einzelne Datenquellen aus SOC-Intel auch zur aktiven Erzeugung von Ereignisdaten verwendet werden, die dann ebenfalls in

die Analyse- und Bewertungsprozesse von SOC-Control einfließen. Dazu gehören die Daten aus der Netflow-Überwachung der X-WiN-Infrastruktur.

Mit SOC-Probe steht eine weitere aktive Komponente zur Verfügung, welche unabhängig von den Daten der SOC-Agent-Instanzen ist: Mit SOC-Probe können extern erreichbare Standardserver mit Protokollen wie https, DNS oder SMTP überwacht werden. Neben der reinen Erreichbarkeit des Services können in Zukunft auch wichtige Sicherheitsparameter überwacht (z. B. http-Header) oder das Defacement einer Website erkannt werden.

Manuelle Analyse und Lagebild

Den IT-Security-Experten bzw. SOC-Analysten des DFN-CERT stehen die Komponenten SOC-Analysis sowie die geplante Erweiterung SOC-Research für die manuelle Analyse der Ereignisdaten zur Verfügung. Diese Tools werden eingesetzt, um neue IoC-Muster zu entdecken und die entsprechenden Erkennungsmuster und Analyseregeln zu entwickeln und um neue, aktuelle Bedrohungen mithilfe der automatischen Prozesse erkennen zu können.

Den Teilnehmern steht über SOC-Report ein Dashboard zur Verfügung, über das jeder Teilnehmer den aktuellen Status des SOC-Systems in Bezug auf die eigene IT-Infrastruktur einsehen kann. Abbildung 2 zeigt einen Screenshot des SOC-Dashboards für einen fiktiven Teilnehmer. Hier ist u. a. die Rate der eingelieferten Ereignisse nach Anzahl und Größe sichtbar. Aber auch die Anzahl der jeweils erkannten Incidents oder der aktuelle Status der überwachten Standardserver sind hier abrufbar.

Zusätzlich wird für die Teilnehmer regelmäßig ein Dokument mit einem zusammenfassenden Lagebild erstellt, aus dem der aktuelle Status sowie die zeitliche Entwicklung hervorgehen. Perspektivisch sollen die durch SOC-Report bereitgestellten Informationen in das CERT-Portal integriert werden.

Incident-Erkennung

Wie beschrieben, kann das SOC-System ganz unterschiedliche Datenquellen und Ereignisarten nutzen, um regelbasiert nach sicherheitsrelevanten Vorfällen zu suchen. Die folgenden drei Use Cases zeigen beispielhaft, welche Datenquellen jeweils genutzt und wie die Incidents erkannt werden und außerdem, welche Reaktion erfolgt.

Use Case 1: Virenschleuder

Für diesen Fall werden die Logs von Mailservern bzw. Virenscannern genutzt, die von SOC-Agents eingeliefert wurden, um die Informationen zu geblockten E-Mails auszuwerten. Da die entsprechende E-Mail bereits geblockt wurde, muss der intendierte Empfänger nicht mehr durch das SOC gewarnt werden. Falls eine kompromittierte E-Mail aus dem Netz eines Teilnehmers versendet wird, informiert das SOC darüber, dass sich eventuell ein kompromittierter Rechner im betreffenden Netz befindet.

Datenquellen	Mail-Server- bzw. Virenscanner-Logs
	DFN-Teilnehmer-Datenbank für Zuordnung der IP-Adressen
Verfahren	Erkennen der Infektionsmeldung des Virenscanners an typischen Teilstrings in der Meldung
	Parsen der Meldung, um IP-Adresse des Senders zu ermitteln
	Prüfen, ob IP-Adresse zu einem Teilnehmer gehört
Ergebnis	Wenn Sender zu einem Teilnehmernetz gehört: automatische Warnmeldung über CERT-Dienste.
	Wenn Sender nicht zu einem Teilnehmernetz gehört: ggfs. Weiterleitung an zuständige externe CERTs.

Abbildung 2: DFN-SOC Dashboard

Use Case 2: Botnet-Client

Für diesen Use Case werden die Netflow-Daten der X-WiN-Kernrouter ausgewertet, die über SOC-Intel zur Verfügung stehen. Es wird geprüft, ob eine IP-Adresse aus dem Netzbereich eines Teilnehmers signifikant mit der IP-Adresse eines Command-and-Control-Servers eines Botnets kommuniziert hat. Dazu werden IP-Adressen und Kommunikationsparameter von bekannten CnC-Servern verwendet. Wenn eine entsprechende Kommunikation festgestellt wurde, wird ermittelt, zu welchem Teilnehmer die interne IP-Adresse gehört. Dieser wird dann darüber informiert, dass sich möglicherweise ein kompromittierter Rechner in seinem Netz befindet, der isoliert und kontrolliert werden sollte.

Datenquellen	Bekannte CnC-Server aus SOC-Intel
	Netflow-Daten der Kern-Router
	Liste bekannter, interner Scanner
Verfahren	Suche nach Zugriffen auf CnC-Server in Netflow-Daten
	Eliminierung von False Positives durch zusätzliche Selektionsschritte
	Eliminierung von bekannten, internen Scannern
Ergebnis	Automatische Warnmeldung an Teilnehmer über CERT-Dienste

Use Case 3: Gekaperter Webserver

Die Komponente SOC-Probe kommt hier zum Einsatz: Sie ruft regelmäßig eine Liste von vorgegebenen, extern erreichbaren Webservern auf und prüft, ob in der Antwortseite ein typisches Muster einer manipulierten Website sichtbar ist. Wenn ja, wird der Teilnehmer darüber informiert, dass der Webserver möglicherweise gekapert wurde.

Datenquellen	Liste von URLs der zu überwachenden Webserver
	Bekannte Muster von gekaperten Websites
Verfahren	Regelmäßiges Aufrufen der überwachten URLs
	Allgemeine Prüfung der Rückgabe
	Spezifische Prüfung der Rückgabe auf bekannte Angriffsmuster
Ergebnis	Automatische Warnmeldung an Teilnehmer über CERT-Dienste

Aktueller Stand und Ausblick

Das SOC-System ist mit den hier beschriebenen Komponenten und vergleichbaren Use Cases kürzlich in den Pilotbetrieb gegangen. Gemeinsam mit den ersten Teilnehmern sammelt das SOC-Team nun Erfahrungen mit dem neuen Dienst. Sukzessive werden weitere Teilnehmer an Bord genommen. Gleichzeitig wird das System erweitert und vor allem stetig um neue Use Cases ergänzt. Dadurch werden immer mehr sicherheitsrelevante Vorfälle automatisch erkannt und zuverlässige Warnungen generiert.

Insbesondere der SOC-Agent soll für den Regelbetrieb weitere Funktionen erhalten und in Form einer Virtual Appliance ausgeliefert werden, sodass der Installations- und Betriebsaufwand beim Teilnehmer so gering wie möglich ist. Darüber hinaus wird die Aufnahme weiterer Datentypen vorbereitet und die Architektur der zentralen Komponenten laufend dem Bedarf angepasst. ◆

Quantensichere IT: ein Blick in die Glaskugel

Mit der rasanten Entwicklung von Quantencomputern wachsen auch die Anforderungen an die Kommunikationssicherheit. Alle asymmetrischen kryptografischen Verfahren, die heute in Internetprotokollen Verwendung finden, laufen in naher Zukunft Gefahr, in relativ kurzer Zeit entschlüsselt zu werden. Die Migration zu quantenresistenten Verfahren ist dringend notwendig und muss jetzt schon für den Praxiseinsatz in der Breite vorbereitet werden.

Text: **Stefan-Lukas Gazdag** (genua GmbH), **Sophia Grundner-Culemann** (LMU München), **Tobias Guggemos** (LMU München), **Tobias Heider** (genua GmbH), **Daniel Loebenberger** (Fraunhofer AISEC)

Foto: vegefox.com/AdobeStock

Das heutige Internet wird von einer bereits kaum zu überbietenden Zahl an Protokollen und Anwendungen getragen, und dennoch werden es immer mehr. Während Internetgiganten aktuelle Trendtechnologien innerhalb weniger Monate zu De-facto-Standards etablieren, haben mühsam erarbeitete Protokolle wie IPv6 erst nach gut 20 Jahren Existenz an Praxisrelevanz gewonnen. Dabei hatten sich die Probleme, die IPv6 ursprünglich lösen sollte, teils schon fundamental geändert. Es herrscht also ein Durcheinander von Standards, das geprägt ist von Abhängigkeiten, Rück- und Abwärtskompatibilitäten, Workarounds und Best Practices. Gleichzeitig soll aber in und mit diesen Protokollen die Kommunikation abgesichert werden. Mithilfe von Kryptografie kann man beispielsweise den Datenverkehr abhörsicher gestalten. Das erhöht die Komplexität der Programme, vergrößert die zu sendenden Datenmengen und verlangsamt die Anwendungen; aufgrund mannigfaltiger Gefahren, z. B. durch Hacker oder auch staatliche Nachrichtendienste, kann aber auf diese Sicherheitskonzepte nicht verzichtet werden. Ganz im Gegenteil: An vielen Stellen müsste ein deutlich größeres Augenmerk auf die Verwendung von Kryptografie gelegt werden.

Quantencomputer – die neue Gefahr?

Mit der Covid-19-Pandemie ist der Bedarf an mobilen und vor allem sicheren Lösungen gestiegen, damit die Beschäftigten auch von zu Hause aus beispielsweise über Virtual Private Networks (VPNs) zuverlässig kommunizieren können. Gleichzeitig geraten immer mehr Firmen, aber auch Rechenzentren, in den Fokus von Angriffen. Währenddessen baut die amerikanische National Security Agency (NSA) ihre Datenspeicher in Utah offenbar immer weiter aus. Diese fassen mittlerweile schon Exabyte an Daten. Darauf gibt es verschiedene Hinweise, sagen Experten. Die NSA hält sich bedeckt. Nach dem Motto „store now, decrypt later“ ist höchstwahrscheinlich die Absicht, verschlüsselten Verkehr jetzt aufzuzeichnen und später zu brechen – mithilfe von Erkenntnissen und Entwicklungen, die jetzt noch in der Zukunft liegen. Das könnten Fortschritte in der Kryptanalyse sein, das Erkennen von Implementierungsfehlern oder künftige Supercomputer, die deutlich an Leistung zunehmen. Vielleicht wird sich aber auch eine neue Gefahr auftun: die sogenannten Quantencomputer.

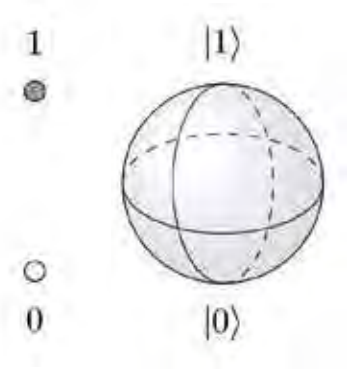


Abbildung 1: Ein klassisches Bit kann nur einen der beiden Zustände 0 oder 1 (links) annehmen. Ein Quantenbit (Qubit) hingegen kann sich in einer sogenannten Superposition befinden und jeden Zustand annehmen, der auf der Oberfläche der Bloch-Kugel liegt (rechts). Der Zustand kann z. B. solcherart sein, dass an diesem Qubit mit 65 Prozent Wahrscheinlichkeit eine 1 und mit 35 Prozent Wahrscheinlichkeit eine 0 beobachtet wird. Qubits können sich auch in einem „verschränkten“ Zustand befinden, sodass sie nur in bestimmten gemeinsamen Zuständen beobachtbar sind, egal wie weit sie voneinander entfernt sind. Mithilfe dieser Quanteneffekte können manche mathematischen Probleme mit einem Quantencomputer schneller gelöst werden.

Asymmetrische Verschlüsselungsverfahren

Die kryptografischen Verfahren haben verschiedene Ziele: Sie müssen einerseits für Vertraulichkeit sorgen: Wer unerlaubt den Datenverkehr mitliest, sollte möglichst lange die Klardaten nicht einsehen können. Andererseits müssen

> Wer unerlaubt den Datenverkehr mitliest, sollte möglichst lange die Klardaten nicht einsehen können.

die Integrität und Authentizität der versendeten Daten gewährleistet werden. Digitale Signaturen sollen dafür sorgen, dass die Daten nicht manipuliert werden und die Quelle der Daten verifizierbar ist. Um Vertraulichkeit zu erreichen, wird der Datenverkehr selbst meist mit schnellen, symmetrischen Verschlüsselungsverfahren wie dem Advanced Encryption Standard (AES) gesichert. Hierfür müssen alle Kommunikationsparteien das gleiche Passwort bzw. den gleichen Schlüssel nutzen. Um dieses gemeinsame Geheimnis vertrauenswürdig auszutauschen, ohne sich z. B. vorab persönlich treffen zu müssen, werden vergleichsweise langsame asymmetrische Verfahren genutzt. Damit kann ein gemeinsamer Schlüssel abgeleitet werden.

Die Sicherheit dieser Verfahren basiert auf der wohlbegründeten Hoffnung, dass Angreifende das genutzte Geheimnis nicht kennen und dadurch sehr viel Rechenaufwand benötigen, um das Verfahren zu knacken. Für ein symmetrisches Verfahren sollte z. B. ein Brute-Force-Angriff, also das sukzessive Ausprobieren möglicher Schlüssel, praktisch aussichtslos sein. Die wenigen in der Praxis etablierten asymmetrischen Verfahren beruhen auf schwierigen

mathematischen Problemen. So müssen für das beliebte Verschlüsselungsverfahren RSA (nach den Entdeckern Rivest, Shamir und Adleman) Zahlen faktorisiert oder für den Digitalen Signatur-Algorithmus (DSA) diskrete Logarithmen berechnet werden. Selbst mit heutigen Supercomputern ist der Aufwand viel zu hoch, um diese Verfahren zu brechen, sofern sie korrekt und mit ausreichend großen Schlüsseln genutzt werden.

Quantencomputer hingegen nutzen ein vollkommen anderes Rechenmodell. Damit könnten sie symmetrische Verfahren schwächen

> Diese radikale Bedrohung betrifft alle verbreiteten asymmetrischen Algorithmen.

und aktuell genutzte asymmetrische Verfahren relativ einfach brechen. Für einen Brute-Force-Angriff auf symmetrische Verfahren z. B. müsste man auf einem klassischen Computer im Schnitt die Hälfte aller möglichen Schlüssel testen. Bei N Schlüsseln sind das also N/2 Versuche. Bereits 1996 wurde jedoch von Lov Grover der nach ihm benannte „Grover-Algorithmus“ für Quantencomputer vorgestellt, welcher selbst im schlechtesten Fall nur die Quadratwurzel aus N Versuchen benötigt. Das würde die sogenannte Bit-Sicherheit etwa halbieren: 128-Bit-Schlüssel böten gegenüber einem Quantencomputer also nur noch eine Sicherheit von 64 Bit. Abhilfe schafft die Verdoppelung der Schlüssellänge. Diese Lösung ist zwar nicht besonders praktisch, aber technisch einfach umzusetzen: Statt beispielsweise den Advanced Encryption Standard (AES) mit 128-Bit-Schlüsseln zu verwenden, muss auf 256 Bit oder bei dem Hash-Verfahren, dem Secure Hash Algorithmus (SHA), von 256 Bit auf 512 Bit Ausgabelänge gewechselt werden.

Die Sicherheit von asymmetrischen Verfahren, die auf dem Faktorisierungs- oder dem Diskreten-Logarithmus-Problem beruhen, wird vom sogenannten „Shor-Algorithmus“ beeinträchtigt. Von Peter Shor im Jahr 1997 vorgestellt, bietet er auf einem Quantencomputer eine subexponentielle Beschleunigung beim Brechen der entsprechenden Verfahren. Egal wie lang die verwendeten Schlüssel sind, faktisch könnten sie binnen relativ kurzer Zeit berechnet werden. Diese radikale Bedrohung betrifft alle verbreiteten asymmetrischen Algorithmen wie RSA, Diffie-Hellman (DH), DSA oder deren Varianten ECDH, ECDSA, die auf elliptischen Kurven beruhen.

Quantensichere Kryptografie

Es ist also neue, quantensichere Kryptografie nötig, die auf anderen mathematischen Aufgabenstellungen beruht. Ein möglicher Kandidat sind die sogenannten Gitter (Abbildung 2): Auf dieser Grundlage wurden bereits effiziente Verschlüsselungs- und Signaturverfahren entwickelt. Zwar ist es bisher schwierig, geeignete Parameter zu finden, dennoch gelten sie als äußerst vielversprechend. Auch Verschlüsselungsverfahren auf der Basis fehlerkorrigierender Codes machen Hoffnung: Das Kryptosystem von Robert McEliece ist seit 1978 bekannt und damit in über 40 Jahren nie gebrochen worden. Bisher war es nicht praxisrelevant, weil der öffentliche Schlüssel, der den Kommunikationspartnern anfangs mitgeteilt werden muss, gut ein MB groß ist. Heutzutage findet das System aber besonders unter jenen Zuspruch, die für ihre Datensicherheit lieber auf altgediente Mathematik vertrauen.

Dem stehen jüngere Forschungsfelder wie das Gebiet der Isogenien auf supersingulären elliptischen Kurven entgegen (nicht zu verwechseln mit klassischer Kryptografie auf Basis elliptischer Kurven). An isogeniebasierter Kryptografie ist vor allem die geringe Schlüssellänge attraktiv, die jedoch mit erheblichem Rechenaufwand einhergeht. Auch die Eigenschaft der API-Kompatibilität mit dem bekannten, weitverbreiteten Diffie-Hellman-Schlüsselaustausch machen die entsprechenden Systeme interessant; daher werden sie, trotz bisher dünner Erkenntnisse über ihre Sicherheit, weiter als Alternative gehandelt. Bestens erforschte Sicherheit bieten die sogenannten hashbasierten Signaturen, die längst einsatzbereit sind. Sie sichern immerhin Integrität und Authentizität; Verschlüsselung (und da-

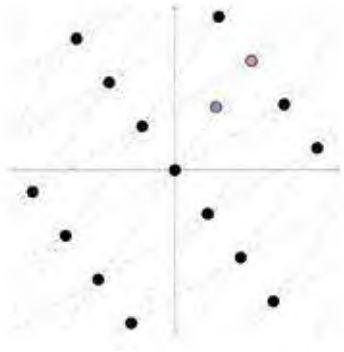


Abbildung 2: Das „Closest Vector-Problem“ beschreibt die Suche des am nächsten gelegenen Punktes eines Gitters (rot) zu einem beliebigen Punkt außerhalb des Gitters (violett). Im zweidimensionalen Fall ist das meist mit bloßem Auge erkennbar, wohingegen dies bei mehrdimensionalen Gittern auch rechnerisch sehr schwierig ist. Zur Verschlüsselung einer Nachricht wird diese auf einem Gitterpunkt abgebildet und anschließend zufällig auf eine Position außerhalb des Gitters verschoben. Der Empfänger kennt die genauen Eigenschaften zur Erstellung des Gitters und kann den ursprünglichen Punkt vergleichsweise einfach wiederherstellen. Für einen Angreifer, dem genau diese Informationen fehlen, ist dies faktisch unmöglich.

WARUM SIND KRYPTOGRAFISCHE VERFAHREN SICHER?

Typischerweise wird für kryptografische Verfahren eine Art Aufwandsschätzung genutzt. Es wird untersucht, wie viele Rechenschritte mit den besten bekannten Algorithmen für einen Angriff benötigt werden und ob dies für ein Verfahren überhaupt praktikabel möglich ist. Es lassen sich auch allgemeingültige bzw. generische Annahmen treffen. Erfüllt ein Verfahren bestimmte Anforderungen, so lassen sich Sicherheitseigenschaften ableiten. Nichtsdestotrotz erfolgen Angriffe unabhängig davon immer in der spezifischen Funktionsweise eines bestimmten Verfahrens.

Des Weiteren behilft man sich als Kryptologe mit sogenannten mathematischen Beweisen. Hier wird mithilfe mathematischer Modelle versucht, typischen Attacken eines unterschiedlich mächtigen Angreifers zu widerstehen. Es kann aber durchaus Angriffe geben, die in einem konkreten Modell nicht abgedeckt werden können. Außerdem werden die Implementierungen der Verfahren z. B. auf Seitenkanäle hin untersucht, da insbesondere die praktischen Umsetzungen einen deutlich leichteren Angriffsvektor bieten als die graue Theorie.

Die Sicherheit eines Verfahrens beruht also auf der akribischen Untersuchung vieler Krypto- und Programmierexperten, einer gehörigen Praxiserfahrung und der Fähigkeit, Angriffe möglichst gut einschätzen zu können. Aber es könnte immer das eine Genie geben, dass eines Tages eine Möglichkeit findet, ein bestimmtes Verfahren zu brechen.

mit Vertraulichkeit der Daten) ist damit konzeptionell allerdings nicht möglich.

Hybride Kryptoverfahren

Das langfristige Vertrauen in diese vergleichsweise unerforschten, neuen Verfahren ist allerdings noch nicht flächendeckend vorhanden. Deshalb sollen hybride Methoden die Sicherheit des Gesamtsystems auf mehrere Verfahren verteilen. Dazu werden klassische und neue kryptografische Verfahren parallel verwendet, um das Risiko zu minimieren, wenn eines der Verfahren mittels konventioneller Kryptanalyse oder durch einen Quantencomputer gebrochen wird oder andere Sicherheitsfälle auftreten. Um diese hybriden Verfahren zu ermöglichen, müssen sie in Protokollen und Software leicht auszutauschen sein – wir sprechen in diesem Kontext von Kryptoagilität. In der Realität allerdings setzen viele aktuelle Systeme auf wenige oder nur ein Verfahren, wie das oben erwähnte Diffie-Hellman-Verfahren beim Schlüsselaustausch. Dadurch entsteht ein weniger kompliziertes, aber auch starres System, in dem nicht einfach etwas auszutauschen ist. Das macht die Migration zu quantenresistenten Verfahren schwieriger, da ausschließlich die Datenstrukturen und Datengrößen nur dieses einen Verfahrens in Protokoll wie Implementierung Beachtung finden. Deshalb begann das National Institute of Standards and Technology (NIST) bereits vor einigen Jahren mit der Standardisierung neuer Verfahren, und auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt quantenresistente Algorithmen vor und rät zur Migration. Auch andere Standardisierungsgremien wie die Internet Engineering Task Force (IETF) bemühen sich bereits, gängige Kommunikationsprotokolle beispielsweise mit dem IKEv2-Schlüsselaustausch auf die neuen Anforderungen vorzubereiten. Bis zur Veröffentlichung von quantenresistenten Erweiterungen bzw. Anpassungen können aber noch Jahre vergehen. Vermutlich sind mehrere Zwischenschritte zur Migration besonders sicherheitskritischer Komponenten notwendig, welche wiederum andere Systeme dahinter schützen.

> Dazu werden klassische und neue kryptografische Verfahren parallel verwendet.

Erste Schritte auf dem Weg zu quantenresistenter IT

Zunächst muss im eigenen Unternehmen, Institut bzw. bei einem Produkt geklärt werden, in welchem Umfang Kryptografie verwendet wird und an welchen Stellen diese angepasst werden sollte, um Quantenresistenz zu gewährleisten. Hier sind Abhängigkeiten von anderen Produktherstellern oder Open-Source- Projekten leider vorprogrammiert, denn auch bei diesen sind Anpassungen durchzuführen. Wichtige Fragen sind, ob bei hohen Sicherheitsanforderungen umgehend Übergangslösungen geschaffen werden müssen oder ob bereits verwendete Kryptobibliotheken durch quantenresistente Alternativen ersetzt werden können. Im ersten Fall können sogenannte Pre-Shared Keys (PSK) eine Lösung bieten. Diese sind bereits in einigen Protokollstandards wie TLS oder IKEv2 verfügbar. Auf diese Art ist die aktuelle Kommunikation direkt gegen Quantencomputer gesichert, auch wenn das mit einem größeren Aufwand zur Schlüsselverwaltung einhergeht. Zu einem späteren Zeitpunkt kann dann auf praktikablere Standards umgestiegen werden. An diesen wird derzeit allerdings noch gearbeitet. Die Kernfra-

ge ist also, wie sicherheitskritisch ist ein System und wann – abhängig davon – soll die Migration erfolgen.

Eine Abschätzung, wann tatsächlich mit großen Quantencomputern zu rechnen ist, kommt einem Blick in die Glaskugel gleich. Für praxistaugliches Brechen von Kryptografie werden voraussichtlich mehrere Tausend sogenannter logischer Qubits benötigt. Hierfür werden vermutlich mehrere Millionen physikalischer Qubits auf dem Quantencomputer gebraucht. Dem stehen heute weniger als 100 (physikalische) Qubits gegenüber. Viele Behörden und Firmen gehen von der Arbeitshypothese aus, dass in etwa 15 Jahren überhaupt erst mit Maschinen zu rechnen ist, die Verfahren wie RSA mit 2048 Bit brechen können. Ein weiterer Blick ist auf die Angriffsziele und -vektoren zu richten. Aufgrund des immensen Bedarfs an Hardware und Energie sowie der einhergehenden Kosten dürfte es sich zunächst um staatliche Akteure handeln, die entsprechend hochrangige Ziele anvisieren werden – sei es wegen militärischer und politischer Interessen oder zur Wirtschaftsspionage.

Neue Standardlösungen sind notwendig

Derzeit ist auch nicht absehbar, wie schnell ein Quantencomputer ein erwünschtes Ergebnis liefert. Zu vermuten ist, dass verschlüsselte Daten innerhalb weniger Stunden oder Tage geknackt werden können. Ob ein solcher Rechner jemals effizient genug sein wird, um innerhalb von Sekunden(-bruchteilen) Signaturen zu fälschen und so einen Man-in-the-Middle-Angriff auf klassisch verschlüsselte Verbindungsaufbauten zu ermöglichen, ist unklar. Derzeit sind sich selbst Experten uneinig darüber, wie schwierig es ist, von einem Quantenrechner, der RSA-2048 brechen kann, zu einem Äquivalent zu gelangen, das RSA-4096 brechen kann. Ist es nur noch Ingenieurskunst, um von den vielen benötigten Qubits weiter hoch zu skalieren oder steigt der Aufwand derart, dass sogar mit einer Art „Schranke des Machbaren“ gerechnet werden muss? Die Antwort liegt leider noch in der Zukunft.

Die Erfahrung zeigt, dass es Jahre oder gar Jahrzehnte dauern kann, bis neue Technologien in der Breite eingesetzt werden. Die Fülle an unterschiedlichen Anforderungen machen allgemeingültige Empfehlungen oder Lösungen unmöglich. Schon deshalb müssen wir uns schon heute mit dem Thema beschäftigen. Dafür benötigen wir einen breiten Wissensaustausch von Experten aus der Krypto- und IT-Sicherheits-Community. Aber auch der Wissenstransfer in die Praxis mit Domänenexperten, beispielsweise Administratoren von kleineren und größeren Netzen sowie Soft- und Hardware-Entwicklern, muss gewährleistet werden. Nur mit ihrer Hilfe können neue Verfahren, Bibliotheken und Protokolle auf heterogenen Infrastrukturen mit großen Datenmengen getestet, ein Flickenteppich an „Insellösungen“ vermieden und das Ziel von wenigen Standardlösungen für viele Anwendungsfälle erreicht werden. Wir alle können die entsprechenden Behörden, Standardisierungsgremien und Communities mit unserem Input unterstützen, um die digitale Welt auf die Ära des Quantencomputers vorzubereiten. ◆

WEITERE INFORMATIONEN FINDEN SIE UNTER:

Handlungsempfehlungen des BSI zur „Migration zu Post-Quanten-Kryptografie“:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf

PQC Mailingliste der US-Behörde NIST:
https://csrc.nist.gov/projects/post-quantum-cryptography/email-list

Forschungsprojekt QuaSiModO (Quantensichere virtuelle private Netzwerke)
https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/quasimodo
https://pq-vpn.de/

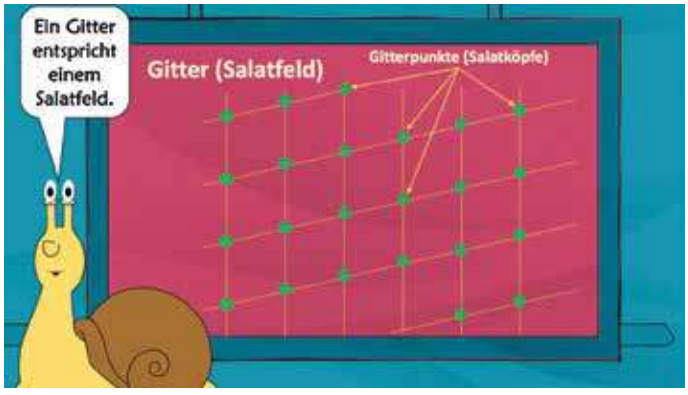
Von Schnecken und Raketen

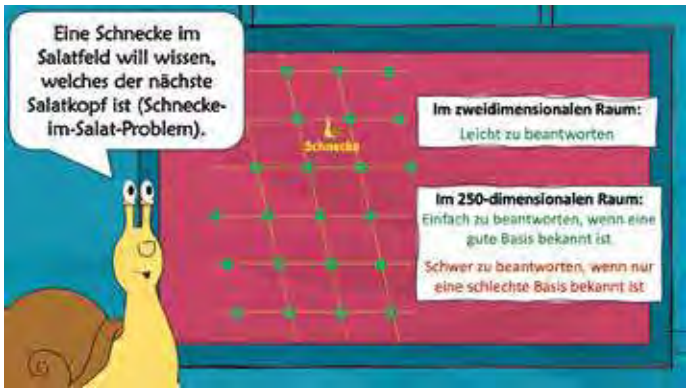
Wie lassen sich die Grundlagen der Post-Quanten-Kryptografie möglichst anschaulich erklären? Am besten mit einem Comic. In diesem erklären Herr Schnecke, Frau Rocketscientist und ein Inselverkäufer die wichtigsten Post-Quanten-Algorithmen.

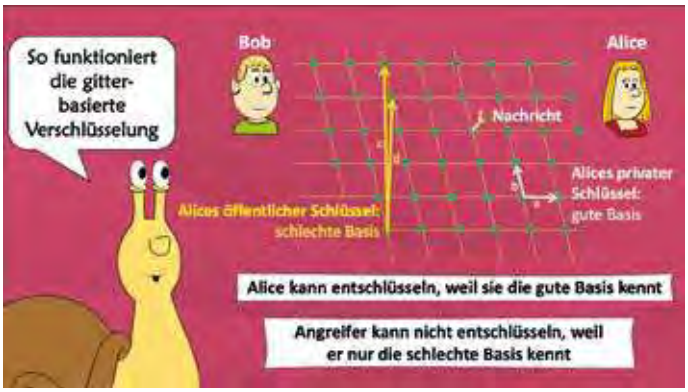
Text: **Klaus Schmeh** (cv cryptovision GmbH)

Unter dem Begriff Post-Quanten-Kryptografie werden asymmetrische Kryptoverfahren zusammengefasst, die nach aktuellem Stand der Forschung nicht mit einem Quantencomputer gebrochen werden können. Letztere sind zwar noch weit davon entfernt, praxistauglich zu sein, doch das kann sich ändern. Um auf die Ära der leistungsfähigen Quantencomputer vorbereitet zu sein, werden bereits jetzt Post-Quanten-Methoden erforscht und eingesetzt. Drei der wichtigsten werden im Folgenden vorgestellt: gitterbasierte, codebasierte und hashbasierte Verfahren.

Klaus Schmeh ist Kryptografieexperte und seit mehr als 16 Jahren für die cv cryptovision GmbH tätig. Er hat 16 Bücher, 25 Forschungsarbeiten, 300 Artikel und 1300 Blogbeiträge zum Thema verfasst und gilt damit als der meist veröffentlichte Autor auf diesem Gebiet. In seinem Blog schreibt der Informatiker über Verschlüsselungstechniken und das Knacken von Codes (www.schmeh.org).



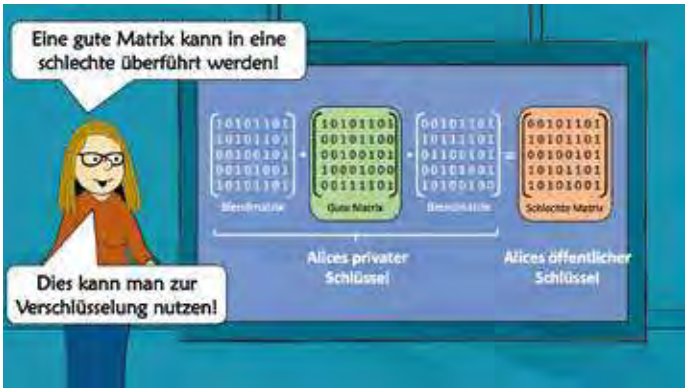

Eine Schnecke im Salatfeld will wissen, welches der nächste Salatkopf ist (Schnecke-im-Salat-Problem).
Schnecke
Im zweidimensionalen Raum:
Leicht zu beantworten
Im 250-dimensionalen Raum:
Einfach zu beantworten, wenn eine gute Basis bekannt ist.
Schwer zu beantworten, wenn nur eine schlechte Basis bekannt ist.

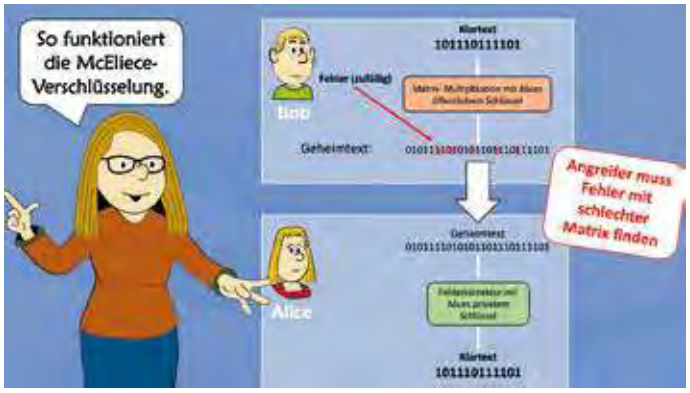

So funktioniert die gitterbasierte Verschlüsselung
Bob
Alice
Nachricht
Alices öffentlicher Schlüssel: schlechte Basis
Alices privater Schlüssel: gute Basis
Alice kann entschlüsseln, weil sie die gute Basis kennt
Angreifer kann nicht entschlüsseln, weil er nur die schlechte Basis kennt


Hallo Frau Rocketscientist, können Sie uns codebasierte Kryptografie erklären?
Gerne.
Gitter
Code

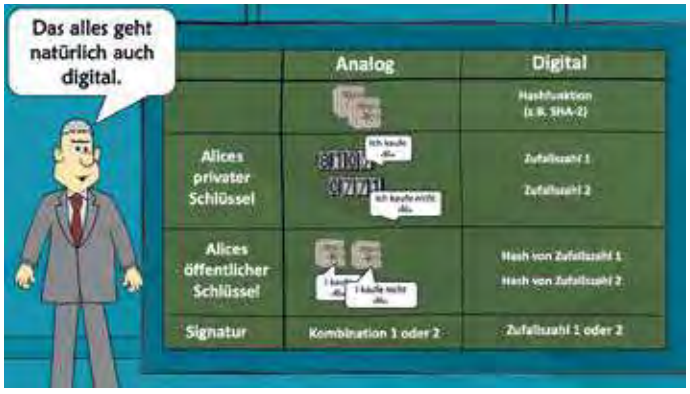

Eine Rakete funkt zur Erde.
ERROR
01010010110100110101010
Frage:
Wie kann man Übertragungsfehler vermeiden?
Antwort:
Durch lineare fehlerkorrigierende Codes (Matrix-Multiplikation)


10101
Matrix-Multiplikation
ERROR
Fehler-korrektur
Aufwendig
Inverse Matrix-Multiplikation
Die Fehlerkorrektur ist sehr aufwendig. Es gibt aber Ausnahmen, wenn man die Matrix richtig wählt („gute Matrix")!


Eine gute Matrix kann in eine schlechte überführt werden!
Alices privater Schlüssel
Alices öffentlicher Schlüssel
Dies kann man zur Verschlüsselung nutzen!


So funktioniert die McEliece-Verschlüsselung.
Bob
Alice
Angreifer muss Fehler mit schlechter Matrix finden


Unser nächster Gast ist ein Inselverkäufer. Er erklärt uns hashbasierte Kryptografie.
Gitter
Code
Hash
Gerne. Alice wollte mir neulich mitteilen, ob sie eine Südseeinsel kauft.



Da haben wir den Salat: gitterbasierte Verfahren

Ein Gitter (Lattice) entspricht einem Salatfeld, auf dem Salatköpfe in gleichen Abständen angeordnet sind. Ein Gitter kann mit einer guten Basis (aufeinander nahezu senkrecht stehende Vektoren) oder mit einer schlechten Basis (nahezu parallel stehende Vektoren) definiert werden. Zur Verschlüsselung wird eine Schnecke in das Salatfeld gesetzt. Sie hat das Ziel, den nächstgelegenen Salatkopf zu erreichen. Der Vektor zwischen Schnecke und Salatkopf ist die Nachricht. Im zweidimensionalen Raum ist es einfach, den nächsten Salatkopf zu erreichen und dadurch zu entschlüsseln. Im 250-dimensionalen Raum geht dies jedoch nur mit einer guten Basis. Eine solche hat aber nur der Empfänger (als privaten Schlüssel) zur Verfügung, während der Sender mit einer schlechten Basis (öffentlicher Schlüssel) arbeiten muss.

Aus Fehlern wird man klug: codebasierte Verfahren

Wenn eine Rakete zur Erde funkt, können Übertragungsfehler auftreten. Zum Glück gibt es leistungsfähige Prüfsummenverfahren (man spricht von „fehlerkorrigierenden Codes"), die falsche Bits korrigieren. Werden solche Codes auf mehrere Tausend Bits auf einmal angewendet, lassen sich zwar 100 Fehler und mehr korrigieren, doch der Korrekturvorgang wird extrem aufwendig. Dieses Prinzip kann zum Verschlüsseln genutzt werden: Der Sender einer Nachricht wendet auf diese einen fehlerkorrigierenden Code an. Dann fügt er Fehler ein. Aus der fehlerhaften Nachricht die ursprüngliche wiederherzustellen, ist nun sehr aufwendig – es sei denn, man hat eine geheime Zusatzinformation (diese bezieht sich auf eine Matrix, die in diesem Zusammenhang verwendet wird). Diese geheime Zusatzinformation (privater Schlüssel) hat jedoch nur der Empfänger.

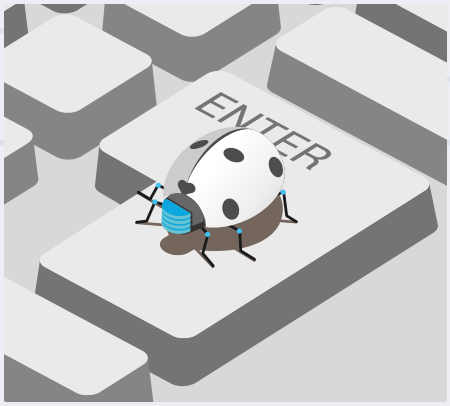
Reif für die Insel: hashbasierte Verfahren

Es gibt nur eine Information, die Alice von einer Südseeinsel an den Inselverkäufer in ihrer Heimat übermitteln will: „Ja, ich kaufe die Insel" oder „Nein, ich kaufe sie nicht". Damit beide nicht betrügen können, hinterlässt Alice bei ihrer Abreise zwei Tresore mit Kombinationsschloss. Der eine enthält die Ja-Nachricht, der andere die Nein-Nachricht – jeweils mit ihrer Unterschrift. Wenn Alice sich entschieden hat, schickt sie die Kombination für den passenden Tresor zurück – aber nur für diesen. Der Verkäufer hat Alices Zu- oder Absage nun schwarz auf weiß, inklusive Unterschrift. Ein solcher Ablauf lässt sich auch digital umsetzen. An die Stelle von Tresoren und Kombinationen treten dann eine Hashfunktion sowie gehashte Nachrichten.

Sicherheit aktuell

Operation Ladybird: wie aus Emotet Emotot wurde

Seit 2014 zählt die Schadsoftware „Emotet“ (damals noch unter dem Namen „Cridex“, „Bugat“ oder „Feodo“ bekannt) zu der wohl gefährlichsten und am weitesten verbreiteten Malware weltweit. Die Schäden, die durch Emotet und die nachgeladene Malware entstanden sind, gehen in die Millionen. Zehntausende Rechner weltweit waren infiziert und verbanden sich regelmäßig zu einem Botnetz – bestehend aus hunderten von Command-and-Control (C2)-Servern – um weitere Malware nachzuladen oder sich selbst zu aktualisieren und neue Schadfunktionalitäten auszurollen.



Tatsächlich handelte es sich jedoch nicht um ein einzelnes Emotet-Botnetz: Es existierten drei Botnetze quasi nebeneinander, die von den Emotet-Betreibern an unterschiedliche „Kundschaft“ verkauft oder vermietet wurden. Diese konnten mit den infizierten Rechnern weiteren Schaden anrichten und z. B. Ransomware in Firmennetzwerken verbreiten, um Dateien zu verschlüsseln und anschließend Lösegeld zu fordern.

Am 26. Januar 2021 gelang es endlich, Emotet quasi aus dem Nichts stillzulegen. Bei dieser Operation wurden in der Ukraine einige Handlanger (ob es sich wirklich um die Hauptakteure handelt, ist unklar) festgenommen. Viel wichtiger an diesem Takedown ist die Tatsache, dass es gelang, auch die komplette Infrastruktur, bestehend aus fast allen C2-Servern, zu beschlagnahmen.

Im Unterschied zu früheren Takedowns wurden die C2-Server jedoch nicht einfach abgeschaltet. Vielmehr ließen die verantwortlichen Strafverfolgungsbehörden die Server noch eine ganze Weile weiterlaufen und verbreiteten über die C2-Server „manipulierte“ Emotet-Varianten an infizierte Systeme. Diese manipulierte Version sorgt einerseits dafür, dass sich infizierte Systeme fortan nur noch mit Sinkholes verbinden: das sind Server, die von Strafverfolgungsbehörden kontrolliert werden. Ferner hat sich diese Emotet-Variante am 25. April 2021 von betroffenen Systemen selbst deinstalliert – ggf. bleibt aber andere Malware natürlich weiterhin auf den Systemen. Mit dieser neuartigen Vorgehensweise ist es die wohl größte Takedown-Operation in der Geschichte des Internets.

Die ganze Operation war in dieser Form nur möglich, weil unterschiedlichste öffentliche wie private Akteure aus vielen Ländern beteiligt waren: Strafverfolgungsbehörden, große Security-Firmen, CERTs, ISP, aber auch zahlreiche unabhängige Malware-Researcher, die alle ein Ziel hatten: die durch Emotet entstandenen Schäden zu minimieren. Und für dieses gemeinsame hehre Vorhaben wurde der „Firmenhut“ kurzzeitig abgelegt. Federführend war dabei eine Gruppe, die sich „Cryptolaemus“ nennt und deren Mitglieder in der Regel nicht namentlich genannt werden wollen. Auch Beschäftigte des DFN-CERT waren und sind – denn der Kampf geht an vielen anderen Stellen weiter – an dieser Gruppe beteiligt. Das dabei gewonnene Know-how konnte unmittelbar an DFN-Mitgliedseinrichtungen weitergegeben werden: So wurde z. B. regelmäßig in NeMo (Netzwerk Monitoring) nach Verbindungen zu C2-Servern gesucht und gewarnt.

Es ist nicht zu erwarten, dass die nicht festgenommenen Emotet-Akteure kurz- oder mittelfristig mit „Emotet 2.0“ wieder auftauchen werden. Aber frei nach dem Motto „Der König ist tot, es lebe der König“ sagte noch am Abend des Emotet-Takedowns ein Cryptolaemus-Mitglied in einer Telefonkonferenz: „We've won a battle, not the war …“

PS: Warum „Cryptolaemus“ und „Operation Ladybird“? Als Emotet 2014 zum ersten Mal auftauchte, wurde die Malware von der Firma Symantec „mealybug“ (deutsch: Schildlaus) genannt. Der natürliche biologische Feind der Schildlaus ist der Marienkäfer (englisch: ladybird, lateinisch: Cryptolaemus). Der Name der Takedown-Operation kann also als „Verneigung“ vor dem Cryptolaemus-Team verstanden werden. ◆

WEITERE INFORMATIONEN

https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

https://www.youtube.com/watch?v=L_O_2aGzfqs

https://www.youtube.com/watch?v=_BLOmClsSpc

https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html

Einführung von GÉANT TCS

Der DFN-Verein führt derzeit den Zertifikatdienst Trusted Certificate Service (TCS) ein. Dieser PKI-Dienst für europäische Forschungsnetze und deren Teilnehmer wird von GÉANT zur Verfügung gestellt. TCS wird über einen kommerziellen Anbieter realisiert und bietet, ähnlich wie das Sicherheitsniveau „Global“ der DFN-PKI, browserverankerte Server- und Nutzerzertifikate an. Der Dienst wird die DFN-PKI „Global“ zunächst ergänzen und nach einer gewissen Zeit ablösen.

TCS bietet unter anderem die folgenden Funktionen, die über das bisherige Angebot in der DFN-PKI hinausgehen:

- Unterstützung des ACME-Protokolls für das vollautomatisierbare Deployment von organisationsvalidierten Serverzertifikaten
- Ausstellung von Nutzerzertifikaten nach SAML-Authentifizierung über die DFN-AAI/eduGAIN ohne papierbasierte Antragsformulare
- EV-Zertifikate
- Adobe- und Microsoft-Dokumentensignatur-Zertifikate mit voreingestelltem Vertrauen (ggf. mit zusätzlichen Kosten verbunden)
- EV-Code-Signing-Zertifikate (ggf. mit zusätzlichen Kosten verbunden)

Hintergrund der TCS-Einführung ist eine starke Veränderung des PKI-Ökosystems: Die DFN-PKI „Global“ mit Browserverankerung wird seit langer Zeit erfolgreich von der DFN-PCA selbst betrieben. Allerdings gestalten die Root-Programme der Browser und Betriebssystemhersteller, die vertrauenswürdige Root-Zertifikate von den CAs dieser Welt verwalten und regulieren, die Bedingungen für alle Akteure seit einigen Jahren deutlich um.

Als Folge steigen die Risiken und der Aufwand zum Betrieb einer eigenen browserverankerten PKI kontinuierlich an. Die Spielräume zur technologischen Erneuerung und zur Anpassung an Bedürfnisse von Teilnehmern werden immer enger, und gleichzeitig steigen die Erwartungen an die Agilität der Prozesse und technischen Abläufe.

Um auf diese Entwicklung angemessen zu reagieren, wird der DFN-Verein künftig die Lösung von GÉANT nutzen. TCS wird bereits von über 30 europäischen Forschungsnetzen eingesetzt und bietet die notwendige Größe, um zum einen die steigenden Anforderungen der Root-Programme zu erfüllen und zum anderen notwendige Anpassungen an die Bedürfnisse der Anwender durchführen zu können.

TCS wird zurzeit bei den bestehenden Teilnehmern der DFN-PKI eingeführt. Für Standardnutzungsszenarien ist eine Migration zu TCS in einem relativ kurzen Zeitraum möglich.

In komplexen Anwendungsszenarien, in denen z. B. eigene IT-Systeme mit einer hohen Integration in die bestehenden Schnittstellen der DFN-PKI betrieben werden, muss gemeinsam eine Lösung erarbeitet werden. Diese kann aus einer Migration der technischen Systeme bestehen.

Aber auch eine Migration zu einer nicht mehr im Browser verankerten PKI ist denkbar. Derartige Spezial-PKIs unterliegen nicht den Bedingungen der Browser und Betriebssystemhersteller. Anwendungsfälle, die außerhalb von deren eng fokussierten Bedürfnissen liegen, können

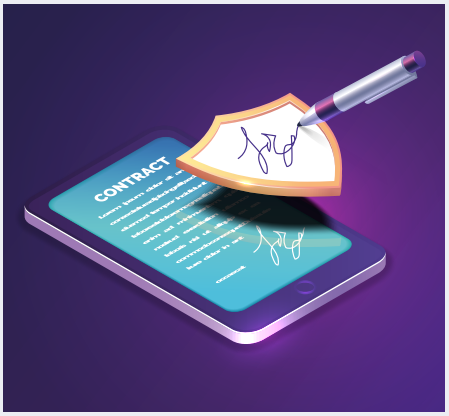


Illustration: upklyak/freepik

damit weiterhin unterstützt werden. Dieses Angebot wird der DFN-Verein bedarfsabhängig ausbauen. ◆

Weitere Informationen über den aktuellen Stand sind in den FAQ zu finden: **https://doku.tid.dfn.de/de:dfnpki:tcsfaq**

MITARBEIT AN DIESER AUSGABE SICHERHEIT AKTUELL:

Jürgen Brauckmann, Stefan Kelm (DFN-CERT)

KONTAKT

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

HIFIS: IT-Services für Helmholtz & Partner

Mit ihrem Inkubator *Information & Data Science* verfolgt die Helmholtz-Gemeinschaft Deutscher Forschungszentren das Ziel, die enormen Datenschätze und die vielfältige, dezentrale Expertise ihrer 18 Forschungszentren zusammenzuführen. Um eine nahtlose und leistungsfähige IT-Infrastruktur zu schaffen, wurde die Plattform *Helmholtz Federated IT Services (HIFIS)* etabliert. Mit einem Layer-3-VPN verbindet der DFN-Verein über sein Wissenschaftsnetz X-WiN die beteiligten Helmholtz-Zentren.

Text: **Uwe Jandt** (Deutsches Elektronen-Synchrotron DESY)

Illustration: Andy/iStock

Die Helmholtz-Gemeinschaft besteht aktuell aus 18 Forschungszentren mit einem sehr breit gefächerten wissenschaftlichen Profil. Vor einigen Jahren rief sie den Helmholtz-Inkubator Information & Data Science ins Leben. Sein Ziel ist es, die digitale Transformation domänen- und zentrenübergreifend zu unterstützen, die Zusammenarbeit der Helmholtz-Zentren zu intensivieren sowie Kompetenzen und Ressourcen zu bündeln. Dies geschieht auf zahlreichen Ebenen, sowohl im wissenschaftlichen Bereich mittels Plattformen wie z. B. der Helmholtz Imaging Platform (HIP), der Helmholtz Metadata Collaboration (HMC) oder der Helmholtz Artificial Intelligence Cooperation Unit (Helmholtz AI), als auch im Ausbildungsbereich mittels der Helmholtz Information & Data Science Academy (HIDA).

Ein weiterer Aspekt der Zusammenführung von verteilten Kapazitäten ist der Aufbau einer gemeinsamen Compute- und Cloud-Infrastruktur sowie die Vermittlung notwendiger Technologien und Kompetenzen zur optimalen Nutzung dieser Infrastruktur, vor allem für die wissenschaftliche Arbeit und Softwareentwicklung. Zuständig für den Aufbau und die Vermittlung gemeinschaftsweiter IT-Infrastrukturen ist die Plattform Helmholtz Federated IT Services (HIFIS), an der elf der 18 Helmholtz-Zentren direkt beteiligt sind.

Helmholtz VPN und AAI: einfacher und effizienter Zugriff auf IT-Services

Für den hürdenlosen und transparenten Datenaustausch zwischen schützenswerten Infrastrukturen mehrerer Partner in Helmholtz wird mit tatkräftiger Unterstützung des DFN-Vereins ein „Helmholtz Backbone“, Virtual Private Network (VPN), aufgebaut. Aktuell sind 15 Helmholtz-Zentren, auch außerhalb von HIFIS, an dem Vorhaben beteiligt und erste Pilotverbindungen bestehen zwischen sechs Zentren. Erste Szenarien für die Übertragung wissenschaftlicher Nutzdaten werden in Zusammenarbeit mit dem European XFEL erarbeitet.

Eine weitere Voraussetzung für den problemlosen Zugriff auf Cloud-Dienste ist der Aufbau der Helmholtz-weiten und darüber hinaus international zugänglichen Authentifizierungs- und Autorisierungsinfrastruktur (AAI). Die Helmholtz-AAI ermöglicht den Nutzenden angeschlossener Institutionen den direkten Zugriff auf unterstützte Dienste auf Basis der institutionseigenen Zugangsdaten. Damit wird die noch häufig anzutreffende Notwendigkeit vermieden, für jeden Nutzer eines Dienstes einen Account samt lästiger Passwörter anzulegen und zu verwalten. Zusätzlich ermöglicht diese Lösung die selektive Autorisierung der Nutzer für be-

DIE ANBINDUNG ÜBER DAS X-WiN DES DFN-VEREINS: VIRTUAL PRIVATE NETWORKS (VPNs):

Auf Wunsch etabliert der DFN-Verein für seine Teilnehmer maßgeschneiderte Virtual Private Networks (VPNs). Diese schaffen separate Kommunikationsumgebungen für die beteiligten Verkehre, die logisch vom übrigen Internet getrennt sind.

Für die Plattform HIFIS stellt der DFN-Verein über sein Wissenschaftsnetz X-WiN ein dediziertes Layer-3-VPN bereit. Ziel ist, die Bereitstellung einer flexiblen und erweiterbaren Netzwerkinfrastruktur, um dem zunehmenden Bedarf an Vernetzung und dem zunehmenden Datenvolumen in der Helmholtz-Gemeinschaft (Stichwort „Datenschatz“) zu entsprechen. Dafür werden die DFNInternet-Teilnehmeranbindungen der Zentren um einen Zugang zum HIFIS-VPN erweitert. Der DFN-Verein stellt je ein zusätzliches Sub-Interface (VLAN) an den beiden im Rahmen des jeweiligen DFNInternet-Dienstes bereitgestellten Schnittstellen zur Verfügung und bindet diese neuen Sub-Interfaces an das HIFIS-VPN an.

stimmte Dienste. Die Helmholtz-AAI ist eng mit der DFN-AAI verbunden. Dadurch und durch die Kompatibilität zum AARC Blueprint wird die direkte internationale Vernetzung der an die Helmholtz-AAI angeschlossenen Institutionen und Services – z. B. mit der European Open Science Cloud (EOSC), NFDI oder GAIA-X – ermöglicht.

Dank Single Sign-On (SSO) ist es möglich, mit einer einzigen Login-Prozedur mehrere Dienste zu nutzen und mehrere Dienste zu Meta-Services zusammenzuschalten. Typische Anwendungsbeispiele für Meta-Services sind die verteilte Speicherung großer Datenmengen und ihre Berechnung unter Nutzung verfügbarer Compute-Ressourcen an variablen Standorten. Eine weitere in Planung befindliche Nutzungsmöglichkeit ist die effiziente Lastverteilung, beispielsweise für Sync&Share-Dienste als föderierte Lösung.

Cloud Services für Helmholtz und Partner

Aufbauend auf der Helmholtz-AAI werden Cloud Services implementiert, von denen etliche bereits als Piloten über ein einheitliches Nutzerportal abrufbar sind. Diese werden seit etwa Mitte 2020 intensiv von Helmholtz-Forschungsgruppen sowie allen Inkubator-Plattformen genutzt. Von besonderer Dringlichkeit waren und sind vor allem kollaborative Dienste, basierend auf Softwares wie Gitlab, Nextcloud Office, OpenStack, Chat. Weitere Services sind Hochleistungsrechnen und beispielsweise der plan- und automatisierbare Datentransfer auf Basis des CERN FTS3, welche von HIFIS-Zentren bereits für europäische Verbundprojekte (WLCG, ESCAPE Data Lake) implementiert wurden. Auch speziellere Lösungen wie ein eigens für die Helmholtz-AI-Plattform maßgeschneidertes „Voucher“-System für Kurzzeitforschungsprojekte wurden von HIFIS maßgeblich entwickelt.

Der Zugriff auf die Services ist zwar in erster Linie für Mitglieder der Helmholtz-Gemeinschaft möglich, diese können jedoch jederzeit gemeinsame Projektgruppen initiieren und externe Partner zur Mitnutzung einladen. Diese als „Virtuelle Organisationen“ (VOs) implementierte Lösung ist Teil der Helmholtz-AAI und ermöglicht das flexible und gleichzeitig nachvollziehbare Management von Gruppen und verschachtelbaren Untergruppen über alle beteiligten Cloud Services hinweg.

Ausbildung, Community Building, Consulting

Die effiziente Nutzung verteilter Dienste für nichtlokale und teilweise domänenübergreifende Arbeitsgruppen ist offensichtlich nicht immer trivial umzusetzen. Für die Arbeit mit verteilten Cloud-Diensten bietet HIFIS darum im Rahmen der Aus- und Weiterbildung vielseitige Kurse und Veranstaltungen an – ebenso für Tools und Workflows in der wissenschaftlichen Softwareentwicklung (Research Software Engineering, RSE). Hierzu zählen Kurse für Programmiersprachen, aber auch Best Practices in der Softwareentwicklung und -veröffentlichung inklusive Lizenzierung und Transfer. Bei geeigneten übergreifenden Themen arbeitet HIFIS eng mit der Helmholtz Data Science Academy (HIDA) sowie weiteren Partnern (z. B. The Carpentries) zusammen.

Bei komplexen Fragen zu wissenschaftlichen Projekten mit IT-Bezug bietet HIFIS darüber hinaus einen Consulting-Service an. Dieser berät zum Aufsetzen und Durchführen von wissenschaftlichen IT-Projekten, zur Verbesserung vorhandener Lösungen und auch zu Fragen der langfristigen Weiterverwertung, z. B. hinsichtlich Lizenzierung. Das hierfür genutzte Ticketing-System ist unmittelbar an den HIFIS Helpdesk sowie die Helpdesks anderer Inkubator-Plattformen gekoppelt, sodass übergreifende Fragen im Verbund geklärt werden können.

Immer nah an der Wissenschaft: Surveys

Der Hauptauftrag von HIFIS besteht in der Unterstützung wissenschaftlicher Arbeit; so ist es naheliegend, Forschende regelmäßig zu ihrem Nutzungsverhalten zu befragen. Von besonderer Bedeutung ist dabei der „IT Knowledge Gap“. Dieser dreht sich um die zentrale Herausforderung, wie die Zielgruppe ihre Bedürfnisse in der wissenschaftlichen Arbeit adressieren kann, wenn ihr „Best Practices” und effiziente Arbeitsabläufe teilweise nicht geläufig sind. Zur Lösung dieser Herausforderung gibt es ver-

schiedene Ansätze: Zum einen sollen bereits existierende wissenschaftliche Arbeitsabläufe unter Nutzung von HIFIS-Diensten umfassend kommuniziert werden; zum anderen werden regelmäßig Helmholtz-weite Umfragen zu Nutzungsgewohnheiten und -bedingungen von IT-Services durchgeführt. Eine erste Umfrage im vergangenen Jahr brachte bereits wertvolle Ergebnisse, die in die Kursplanung für 2021 eingeflossen sind.

Wo geht es hin?

Alle Services von HIFIS werden den Helmholtz-Beschäftigten, und in vielen Fällen auch deren Kooperationspartnern, kostenlos zur Verfügung gestellt. Dies wird durch die dauerhafte Finanzierung von HIFIS als Inkubator-Plattform ermöglicht. Hierdurch leistet HIFIS einen erheblichen Beitrag zur Nachhaltigkeit der bereits vorhandenen Services sowie für die Etablierung echter „Helmholtz-Services".

Die HIFIS-Plattform hat jetzt knapp zwei Jahre Entwicklungszeit hinter sich: Nach einem etwas verzögerten Start 2019 haben alle HIFIS-Services 2020 enorm an Fahrt gewonnen – sicherlich auch beschleunigt durch die neuen Anforderungen der Pandemiesituation. Die weitere Roadmap beinhaltet komplexe Meta-Services und die intensivere Integration von vorhandenen Diensten, aber auch organisatorische Vertiefungen wie die Etablierung eines langfristigen Service-Managements und eines Helmholtz-Cloud-Rahmenvertrags. Es lohnt sich in jedem Fall, am HIFIS-Ball zu bleiben! ◆

WEITERFÜHRENDE INFORMATIONEN:

Positionspapier Digitale Dienste für die Wissenschaft – wohin geht die Reise?
https://zenodo.org/record/4301924#.YIki7KFCRPY
https://hifis.net
https://cloud.helmholtz.de

Das BigBlueButton-Cluster der Philipps-Universität Marburg

Illustration: krerksak/AdobeStock

In Zusammenarbeit mit dem Verbundprojekt *Digital gestütztes Lehren und Lernen in Hessen* hat das Hochschulrechenzentrum der Philipps-Universität Marburg eine browserbasierte Webkonferenzplattform auf Basis der Open-Source-Software BigBlueButton entwickelt – zur Unterstützung der Onlinelehre während der COVID-19-Pandemie. Die Webkonferenzräume sind in erster Linie für Seminare, Übungen sowie Projekttreffen vorgesehen. Geplant ist, die Plattform als Föderierten Dienst in der DFN-Cloud auch anderen Einrichtungen zur Verfügung zu stellen.

BIGBLUEBUTTON-CLUSTER PILOTTEILNAHME

Interessierte an der Pilotteilnahme des BigBlueButton-Clusters wenden sich bitte an das Hochschulrechenzentrum der Philipps-Universität Marburg.

Kontakt: Dr. Andreas Gabriel, gabriel@hrz.uni-marburg.de, 06421 28-23560.

Text: **Christoph Scheid** (Philipps-Universität Marburg)

Mit Beginn der Coronapandemie im Frühjahr 2020 und mit dem ersten Lockdown wurden quasi über Nacht diverse Lösungen für Webkonferenzen von den hessischen Hochschulen eingeführt. Auch an der Philipps-Universität Marburg stieg der Bedarf für browserbasierte Webkonferenzsysteme als Grundlage für die Kommunikation in größeren Gruppen, derzeit bis zu 200 Personen, und für die Unterstützung der Lehr- und Lernszenarien während der Pandemie. Neben der Nutzung eines kommerziellen, proprietären US-Dienstes suchte die Philipps-Universität nach einer selbst gehosteten, quelloffenen Lösung, die für eine große Zahl an Nutzenden tragfähig sein sollte. Die Wahl fiel auf BigBlueButton, das zahlreiche relevante Features für die Lehre bereithält: das Einrichten von Breakout-Räumen für Kleingruppenarbeit, eine Whiteboard-Funktion, Umfragewerkzeuge oder eine Screen-Reader-Funktionalität für hochgeladene Foliensätze. Für die eigenen Hochschulmitglieder wurde das System zudem in die Lernplattform Ilias integriert.

Leistungsfähige Infrastruktur

Vor dem Beginn des ersten Coronasemesters im Sommer 2020 war nur schwer abschätzbar, wie viel Netzwerkverkehr ein weitgehend auf digitaler Lehre basierendes Semester zu Stoßzeiten verursachen könnte und wie viel Leistung es den Videokonferenzservern abverlangen würde. Die Dienstqualität sollte jedoch keinesfalls an Skalierungsfragen der Infrastrukturen scheitern.

So wurde dezidierte Hardware bei einem externen, ISO-zertifizierten deutschen Hoster mit Breitbandanbindung angemietet

> Die Leistungsfähigkeit des Systems ist weit über den Bedarf der Philipps-Universität hinaus skalierbar.

und für die Installation des Konferenzsystems genutzt. Da mittlerweile knapp über die Hälfte der Endgeräte über das Internet Protocol Version 6 (IPv6) kommuniziert, wurde der Cluster gleichermaßen für IPv4 und IPv6 ausgelegt und konfiguriert.

Für Teilnehmende, deren eigene Anbindung oder Hardware nicht für Webkonferenzen ausgelegt ist, z. B. im Home-Office oder unterwegs, wurde zudem eine Möglichkeit zur telefonischen Einwahl in Konferenzräume geschaffen. Die Leistungsfähigkeit des Systems ist weit über den Bedarf der Philipps-Universität hinaus skalierbar.

Zentraler Einstieg mit dezentralen Credentials

Die Servicestelle des hessenweiten Verbundprojekts „Digital gestütztes Lehren und Lernen in Hessen“ kann seit Sommer 2020 den BigBlueButton-Cluster der Philipps-Universität nutzen. Als Einstiegspunkt dient eine eigene, von der Philipps-Universität unabhängige Benutzeroberfläche auf der Basis von Greenlight. Um Partnerhochschulen die Nutzung zu ermöglichen, bot sich die Authentifikations- und

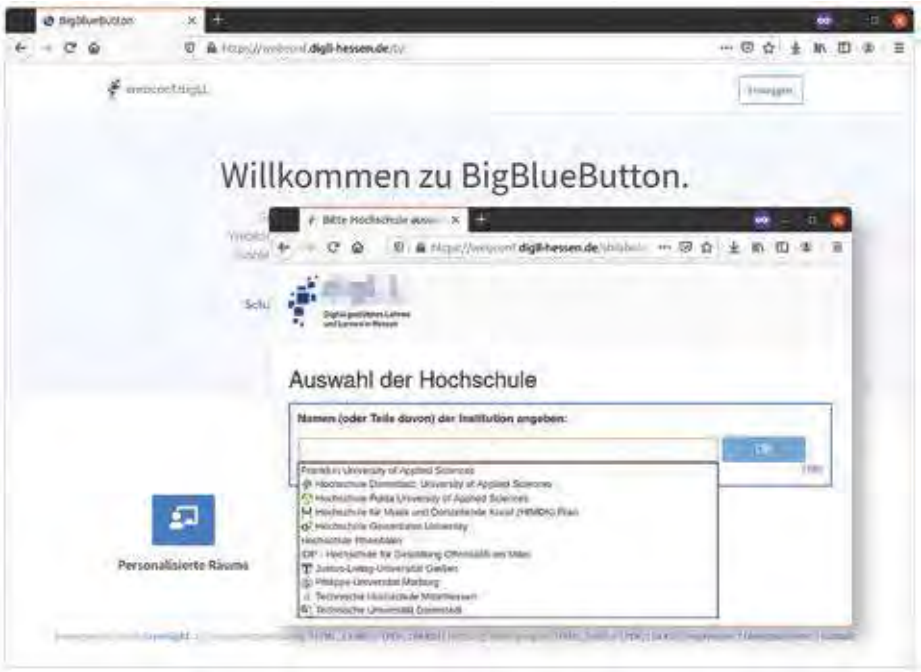


Abbildung 1: Auswahldialog per Embedded Discovery Service

Autorisierungsinfrastruktur des DFN-Vereins (DFN-AAI) an. Der Dienst wurde in der DFN-AAI als Shibboleth Service Provider registriert. Daher musste im Verbundprojekt keine eigene Nutzerdatenbank angelegt und geführt werden, um Identitäten und Berechtigungen zu prüfen. Vielmehr kann über den Identity Provider der jeweiligen Hochschule auf die existierende Benutzerdatenbank zurückgegriffen werden. Die Identity Management-Abteilungen der Hochschulen sorgen dabei je nach Verlässlichkeitsklasse (Basic bzw. Advanced) der DFN-AAI für die Übermittlung entsprechend aktueller Benutzerinformationen bei jedem Login.

In der Konfiguration des Service Providers wird eine Liste der Institutionen bzw. der Identity Provider gepflegt, deren Angehörige Zugriff auf den Dienst haben dürfen. Im zugehörigen Shibboleth Embedded Discovery Service wird aus dieser Liste eine Auswahl per Autovervollständigung oder Dropdown erstellt, aus der Nutzende beim Login die passende Hochschule auswählen können.

Zur Eingabe der Login-Daten (z. B. Username und Passwort) werden Nutzende dann direkt zum Identity Provider ihrer Institution weitergeleitet, der sie im Erfolgsfall an den Service Provider zurückleitet.

Datensparsamkeit

Der Service Provider legt fest, welche personenbezogenen Attribute zur sinnvollen Nutzung zwingend erforderlich sind, d. h. Name und E-Mail-Adresse sowie ein pseudonymer Identifier. Diese müssen seitens der IdP-Betreibenden beim Identity Provider entsprechend freigegeben und – mit Zustimmung der Nutzenden – beim Login übermittelt werden, damit eine vertrauensvolle Nutzung mit Klarnamen sowie eine Kontaktmöglichkeit bei Problemen besteht. Weitere Attribute werden nicht übermittelt.

Ausblick

Durch den Einsatz der leistungsfähigen DFN-AAI-Infrastruktur ist es möglich, auch bei begrenzten personellen Ressourcen Dienste zu betreiben und diese einer großen Gruppe von Nutzenden zur Verfügung zu stellen. Darum plant die Philipps-Universität Marburg, ihren BigBlueButton-Cluster interessierten Hochschulen und Forschungseinrichtungen als föderierten Dienst in der DFN-Cloud zur Verfügung zu stellen und sucht dafür Erprobungspartner. ◆

„VERBUNDPROJEKT DIGITALES LEHREN UND LERNEN IN HESSEN“

Das Projekt wurde am 1. Februar 2019 von elf hessischen Hochschulen gegründet, mittlerweile gehören ihm 13 Institutionen an. Ziel des Verbundes unter Federführung der Philipps-Universität Marburg ist es, Studierenden einen Zugang zu barrierefreien und qualitätsgesicherten digitalen Lehrinhalten und Lernformaten zu ermöglichen und Lehrende bei der Umsetzung digital gestützter Lehre zu beraten. Darüber hinaus soll Lehrenden ein (virtueller) Raum geboten werden, in dem sie sich in geschützter Umgebung über digital gestützte Lehre austauschen und innovative Konzepte erproben können. Dabei unterstützt das Projekt Lehrende sowohl bei der Erstellung von digitalen Lerninhalten als auch aus didaktischer, organisatorisch-technischer und rechtlicher Perspektive.

Kontakt:
Christoph Scheid,
scheid@uni-marburg.de,
Tel. 06421 28-25005,
Servicestelle „Digital gestütztes Lehren und Lernen in Hessen“,
Philipps-Universität Marburg,
Wilhelm-Röpke-Str. 4,
35032 Marburg

Framing – The Never Ending Story feat. EuGH

Der EuGH und die neuen Leitplanken zur Auslegung der öffentlichen Wiedergabe im Urheberrecht

Der Europäische Gerichtshof (EuGH) setzt den vorläufigen Schlusspunkt in der seit Jahren im Urheberrecht umstrittenen Frage des Framing. Höchste Zeit, Struktur in die rechtliche Gemengelage zu bringen und die Entscheidung mit Blick auf ihre Auswirkungen für Hochschulen und Forschungseinrichtungen darzustellen.

Text: **Maximilian Wellmann** (Forschungsstelle Recht im DFN)

Foto: chinaface/iStock

Anfang März dieses Jahres war es so weit. Nachdem der Bundesgerichtshof (BGH) im Jahr 2019 den zugrunde liegenden Rechtsstreit noch ausgesetzt hatte, machte sich der Europäische Gerichtshof (EuGH) nach den letzten drei wegweisenden Entscheidungen zum Urheberrecht[1] auf, den vorläufigen Schlusspunkt in der seit Jahren im Urheberrecht umstrittenen Frage des Framing zu setzen (EuGH, Urt. v. 9.3.2021 – C-392/19). Hierzu nimmt sich der EuGH die Auslegung des Art. 3 Abs. 1 der Informationsgesellschafts-Richtlinie (InfoSoc-RL) vor, die auf europäischer Ebene zahlreiche Verwertungsrechte des Urheberrechts harmonisiert. Höchste Zeit also, Struktur in die rechtliche Gemengelage rund um das Framing zu bringen und die Entscheidung des EuGH mit Blick auf ihre Auswirkungen für Hochschulen und Forschungseinrichtungen darzustellen.

I. Sachverhalt

Ausgangspunkt des jüngsten Urteils des EuGH ist der Streit zwischen der Verwertungsgesellschaft Bild-Kunst (VG Bild-Kunst) und der Stiftung Preußischer Kulturbesitz über eine Klausel in den

1 Siehe hierzu, Tiessen, Was das Gesetz nicht verbietet, verbietet der Anstand, DFN-Infobrief Recht 9/2019; vgl. Wellmann, Der BGH und sein letztes Wort zum Reformistischen Aufbruch, DFN-Infobrief Recht 6/2020.

Lizenzverträgen der VG Bild-Kunst, die die Stiftung Preußischer Kulturbesitz als Trägerin der Deutschen Digitalen Bibliothek dazu verpflichtet, technische Schutzmaßnahmen gegen das Framing Dritter vorzusehen. Bei der Deutschen Digitalen Bibliothek handelt es sich dabei um eine Onlineplattform, welche deutsche Kultur- und Wissenschaftseinrichtungen miteinander vernetzt. Die Plattform funktioniert dabei als „digitales Schaufenster". Auf ihr werden Vorschaubilder („Thumbnails") neben weiterführenden Informationen über die Werke angezeigt. Bei diesen Vorschaubildern handelt es sich um verkleinerte Versionen der Bilder in Originalgröße. Der Nutzer hat dabei die Möglichkeit, über die Digitale Bibliothek auf die Webseiten zu gelangen, auf denen die Werke in vollem Umfang öffentlich wiedergegeben werden.

Um die Vorschaubilder rechtmäßig darstellen zu können, erwirbt die Deutsche Digital Bibliothek regelmäßig über entgeltliche Lizenzverträge bestimmte Rechte an den Vorschaubildern von der VG Bild-Kunst. Diese machte den Erwerb der Lizenzen aber von dem Vorliegen einer Klausel abhängig, nach der sich die Stiftung Preußischer Kulturbesitz dazu verpflichtet, wirksame technische Maßnahmen gegen das Framing der im Portal der Deutschen Digitalen Bibliothek angezeigten Vorschaubilder durch Dritte anzuwenden.

II. Technische Einordnung des Framing

Nähert man sich der technischen Funktion des Framing, handelt es sich bei einem „Frame" (dt. Rahmen) um den Teilbereich einer Website, in dem Inhalte einer anderen Website enthalten sind. Ein paradigmatisches Beispiel stellt die Einbettung eines YouTube-Videos in eine Webseite dar. Der eingebettete Teil wird dabei als „Frame" bezeichnet. Übergeordnet funktioniert die Framing-Technik danach als Technik, nach der eine Webseite in mehrere Rahmen unterteilt wird und in einer dieser „Frames" mittels eines anklickbaren Internetlinks („Inline-Linking") die Inhalte einer anderen Website dargestellt werden.[2] Ziel dieser Framing-Technik ist es dabei, dass den Nutzern des Webauftritts die ursprüngliche Herkunft des eingebetteten „Frames" verborgen bleibt.

III. Urheberrechtliche Einordnung und Funktion von Verwertungsgesellschaften

Eine urheberrechtliche Dimension gewinnt das Framing durch den Umstand, dass eine unmittelbare Nutzungshandlung des Linksetzers in denjenigen Fällen angenommen wird, in denen er fremde Werke über seine Webseite den Nutzern zur Verfügung stellt und sie sich so zu eigen macht. Allerdings ist bisher nicht obergerichtlich geklärt, ob hieraus eine Verletzung des dem Urheber ausschließlich zustehenden Rechts zur öffentlichen Wiedergabe aus Art. 3 Abs. 1 InfoSoc-RL resultiert, das im deutschen Recht nicht explizit geregelt ist, systematisch aber dem § 19a Urheberrechtsgesetz (UrhG) (Recht zur öffentlichen Zugänglichmachung) zugeordnet wird.

Verwertungsgesellschaften, wie die VG Bild-Kunst, spielen im Kontext des Framing dahingehend eine Rolle, dass sie eine Intermediationsfunktion zwischen den Urhebern und den Nutzern gewährleisten. Die originäre Aufgabe von Verwertungsgesellschaften ist es, die Verwertungsreche bestimmter Urhebergruppen (Musikkünstler, Autoren etc.) kollektiv über Wahrnehmungsverträge zu bündeln, um dann über die ihnen gem. § 31 Abs. 3 UrhG übertragenen ausschließlichen Nutzungsrechte eine bestmögliche wirtschaftliche Verwertung der Werke und sonstigen Schutzgegenstände zu ermöglichen. Der Vorteil dieser Rechtebündelung liegt für die Nutzer in dem „one stop shop"-Prinzip, da Nutzer für die Einräumung von Nutzungsrechten nicht einzeln auf den jeweiligen Urheber zugehen müssen, sondern diese zentral bei der Verwertungsgesellschaft erwerben können. Die unterschiedlichen Verwertungsgesellschaften (VG Wort, VG Bild-Kunst etc.) unterliegen dabei nach deutschem Recht einem Kontrahierungszwang, das heißt, sie sind verpflichtet, jedermann auf Verlangen zu angemessenen Bedingungen eine Lizenz zur Nutzung der ihnen übertragenen Rechte einzuräumen. Dieser Kontrahierungszwang wird jedoch durch die deutsche Rechtsprechung ausnahmsweise dann abgelehnt, wenn die Verwertungsgesellschaft dem Verlangen auf Einräumung von Nutzungsrechten vorrangige berechtigte Interessen entgegenhalten kann. Solche berechtigten Interessen sollen nach der bisherigen Rechtsprechung des Bundesgerichtshofs (BGH) gerade dann bestehen, wenn das Framing durch einen Dritten eine öffentliche Wiedergabe des Werkes und somit eine urheberrechtlich relevante Nutzung darstellt und das Framing unter Umgehung von technischen Schutzmaßnahmen erfolgt, die der Rechtsinhaber getroffen oder einem Lizenznehmer auferlegt hat.

IV. Rechtsansicht der Parteien

Die Auferlegung technischer Schutzmaßnahmen schlägt auch den Bogen zurück zur zugrunde liegenden Entscheidung, in der dieses Vorgehen den maßgeblichen Streitgegenstand bildete. Konkret ging es um eine Lizenzabrede der VG Bild-Kunst, in der eine Klausel die Stiftung Preußischer Kulturbesitz als Trägerin der Deutschen Digitalen Bibliothek dazu zwang, wirksame technische Maßnahmen gegen das Framing Dritter anzuwenden. Danach müsse es Dritten unmöglich gemacht werden, das auf der Webseite des Berechtigten „geframte" Werk zu entnehmen und ihrerseits selbst als „Frame" auf ihre Webseite einzustellen. Die Stiftung Preußischer Kulturbesitz sah die streitgegenständli-

2 Siehe hierzu auch Strobel, Links, Links, Links und immer noch nicht der rechte Weg?, DFN-Infobrief Recht 11/2016.

che Klausel dabei schon aus urheberrechtlichen Erwägungen als unwirksam an, da es sich beim Framing schon nicht um eine rechtsverletzende öffentliche Wiedergabe vgl. § 19a UrhG handele. Wenn dies jedoch bereits nicht der Fall sei, könne sie auch über die Klausel nicht in Anspruch genommen werden, technische Schutzmaßnahmen gegen eine dann schon nicht rechtsverletzende Handlung vorzunehmen.

Vor dem Landgericht Berlin (LG Berlin) erhob sie deshalb Klage auf Feststellung einer Verpflichtung der VG Bild-Kunst, die Lizenzabrede auch ohne die entsprechende Klausel zu erteilen. Der Rechtsstreit gelangte bis zum BGH, der das Verfahren einstweilen aussetzte und dem EuGH im Rahmen des Vorabentscheidungsverfahren die grundlegende Frage vorgelegt hat, ob das Framing überhaupt als öffentliche Wiedergabe im Sinne von Art. 3 Abs. 1 InfoSoc-RL zu bewerten ist. Wäre dies der Fall, so würde diese Einordnung es der VG Bild-Kunst erlauben, die Stiftung Preußischer Kulturbesitz zur Durchführung wirksamer technischer Maßnahmen zu verpflichten.

Dass der EuGH letztlich zur Auslegung des Rechts zur öffentlichen Wiedergabe überhaupt angerufen werden kann, liegt dabei in der europäischen Überformung des Ausschließlichkeitsrechts aus Art. 3 Abs. 1 InfoSoc-RL begründet, die dem EuGH die Letztentscheidungskompetenz über die Auslegung des europäischen Rechts vermittelt.

V. Entscheidung des EuGH

In seiner nun ergangenen Entscheidung stellt der EuGH fest, dass, sofern der Rechtsinhaber (hier die VG Bild-Kunst) beschränkende Maßnahmen gegen Framing getroffen oder veranlasst hat, die Einbettung eines Werks in die Website eines Dritten (hier die Deutsche Digitale Bibliothek) im Wege der Framing-Technik eine Zugänglichmachung dieses Werks i. S. v. Art. 3 Abs. 1 InfoSoc-RL für ein neues Publikum darstellt. Dieses Ergebnis führt nachgelagert dazu, dass die VG Bild-Kunst die Stiftung Preußischer Kulturbesitz vertraglich wirksam dazu verpflichten kann, wirksame technische Schutzmaßnahmen gegen das Framing Dritter vorzusehen. Dies folgt dabei aus der verwertungsrechtlichen Relevanz des Framings, die der EuGH in seinem Urteil für diese Fälle festgestellt hat.

Arbeitet man den entscheidenden Kern des Urteils heraus, so ist aus dem Urteil abzuleiten, dass eine rechtsverletzende öffentliche Wiedergabe i. S. v. Art. 3 Abs. 1 InfoSoc-RL nur dann vorliegt, wenn der Zugang zu den Werken durch die VG Bild-Kunst beschränkt war oder sie dazu veranlasst hat, diesen zu beschränken. Da dies vorliegend der Fall war, lag ein Eingriff in das konstitutive Recht der „Zugänglichmachung des Werkes für ein neues Publikum“ vor, da die VG Bild-Kunst in diesen Fällen der freien öffentlichen Wiedergabe ihrer Werke nicht zugestimmt hatte. Diese Einordnung folgt nicht zuletzt aus dem verwertungsrechtlichen Beteiligungsgrundsatz, nach dem es dem Rechtsinhaber ohne die Einordnung als öffentliche Wiedergabe verwehrt bleibt, eine angemessene Vergütung für die Nutzung seiner Werke zu verlangen.

Unterliegt die Werknutzung im Rahmen des Framings allerdings keinen rechtsinhaberseitigen Beschränkungen, hat dieser von Anfang an die Wiedergabe seiner Werke gegenüber sämtlichen Internetnutzern erlaubt, sodass im Ergebnis keine öffentliche Wiedergabe durch die Framing-Technik vorliegt. Insofern zeigt sich die Quintessenz des EuGH-Urteils darin, dass sie den Rechtsinhabern einen differenzierenden Weg aufweist und es letztlich ihnen anheimstellt, ob sie wirksame technische Schutzmaßnahmen implementieren bzw. einem Dritten auferlegen, damit das Framing als Eingriff in das Recht auf öffentliche Wiedergabe zu beurteilen ist. In Fällen, in denen die Rechtsinhaber von solchen Maßnahmen oder Vorgaben absehen, ist das Framing durch Dritte weiterhin nicht als Eingriff in das Recht auf öffentliche Wiedergabe anzuerkennen.

VI. Fazit und Ausblick

Für die streitgegenständliche Klausel der VG Bild-Kunst bedeutet das Urteil, dass sie die Stiftung Preußischer Kulturbesitz wirksam dazu verpflichten kann, wirksame technische Schutzmaßnahmen gegen das Framing der im Portal der Deutschen Digitalen Bibliothek angezeigten Vorschaubilder durch Dritte anzuwenden. Die grundsätzlich nutzerfreundliche Rechtsprechung des EuGH schlägt somit einen bisher nicht gekannten Schlenker zugunsten der Rechtsinhaber.

Für Hochschulen und Forschungseinrichtungen ist mit dem Urteil des EuGH zu befürchten, dass sie in Zukunft durch die Verwertungsgesellschaften vertraglich verpflichtet werden können, eigene technische Schutzmaßnahmen gegen Dritte vorzusehen, damit Dritte auf der Hochschulwebseite „geframte Werk“ nicht ungehindert kopieren und auf ihrer eigenen Webseite „framen“ können. Insoweit ist durch das Urteil ein Mehraufwand zu erwarten, der die Hochschulen und Forschungseinrichtungen grundsätzlich dazu aufruft, sich Gedanken über technische Schutzmaßnahmen für Werke und sonstige Schutzgegenstände des Urheberrechts zu machen. Allzu viel Zeit sollten die Hochschulen und Forschungseinrichtungen jedoch nicht ins Land gehen lassen, ist doch zu vermuten, dass der BGH den Rechtsstreit noch 2021 abschließend entscheiden wird und die skizzierte Auslegung des EuGH zum Recht der öffentlichen Wiedergabe sich dann auch in der obergerichtlichen deutschen Rechtsprechung niederschlagen wird. Seien Sie also beruhigt, die „Never Ending Story“ des Framing wird schon bald fortgesetzt. ◆

TTDSG – Die Profis in spe

Zum aktuellen Stand des Gesetzgebungsverfahrens und dem Inhalt des Regierungsentwurfs des Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG)

Die Landschaft des Datenschutz- und Telekommunikationsrechts unterliegt, auch bedingt durch den technischen Fortschritt, einem stetigen Wandel. Nach dem Inkrafttreten der Datenschutz-Grundverordnung 2018 (DSGVO) ist der Erlass der lang erwarteten ePrivacy-Verordnung (ePrivacyVO) auf europäischer Ebene ins Stocken geraten. Wann es zu einer Einigung über diese kommen wird, ist derzeit ungewiss. In der Zwischenzeit bleibt aber auch der nationale Gesetzgeber nicht untätig. Zumindest auf nationaler Ebene soll der unübersichtliche Datenschutzdschungel etwas gelichtet werden. Ein Fall für TTDSG!

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

I. Entwicklung der Datenschutzgesetze

1. Datenschutzrichtlinie und ePrivacy-Richtlinie

Vor der Wirksamkeit der DSGVO bestimmten in Europa vor allem die Datenschutzrichtlinie[1] von 1995 und die sog. ePrivacy-Richtlinie[2] von 2002 das Telekommunikations- und Datenschutzrecht. Als europäische Richtlinien erlangten diese jedoch keine unmittelbare Rechtswirkung in den Mitgliedsstaaten, sondern mussten in nationales Recht umgesetzt werden. In Deutschland führte die Umsetzungspflicht sowohl zur Novellierung des Bundesdatenschutzgesetzes (BDSG) als auch des Telekommunikationsgesetzes (TKG). Parallel zu den Umsetzungen der Richtlinien wurde auch das nationale Datenschutzrecht 2007 weiter überarbeitet und so mit dem Erlass des Telemediengesetzes (TMG) drei verschiedene, bis dahin geltende Regelwerke[3] zusammengefasst, welche ebenfalls Bereiche des Telekommunikations- und Datenschutzrechts für Anbieter von Telekommunikationsdiensten (TK-Dienste) regelten.

2009 nahm der europäische Gesetzgeber mit der sog. Cookie-Richtlinie[4] Änderungen an der ePrivacy-Richtlinie vor, welche insbesondere die Nutzung von Cookies auf Webseiten betraf. Vor allem eine höhere Transparenz und Sicherheit für die Verbraucher stand im Fokus der Anpassungen. Der deutsche Gesetzgeber sah die erforderliche Umsetzung mit den Vorschriften des schon existierenden TMG als erfüllt an. Datenschützer kritisieren diese Ansicht als schwache Umsetzung, ihrer Meinung nach stelle die Cookie-Richtlinie strengere Anforderungen an die Einwilligung zur Datenverarbeitung bei Cookies auf Webseiten, als es das deutsche TMG vorschreibt.

Trotz der einheitlichen Vorgaben der Richtlinien entwickelten sich in Europa sehr unterschiedliche Prioritäten des Datenschutzrechts in den einzelnen Mitgliedsstaaten. Die Wahrnehmung der Umsetzungsspielräume der Richtlinien sorgte für stark voneinander abweichende Datenschutzniveaus in den Mitgliedsstaaten.

2. Einführung der DSGVO

Diese nationalen Unterschiede sollten mit der Einführung der DSGVO nach langen Verhandlungen harmonisiert werden. Als europäische Verordnung ist diese seit dem 25. Mai 2018 unmittelbar in allen Mitgliedsstaaten anwendbar und ersetzt die alte Datenschutzrichtlinie. Dennoch eröffnet die DSGVO mit verschiedenen Öffnungsklauseln den Mitgliedsstaaten weiterhin an vielen Stellen die Möglichkeit, von einzelnen Vorschriften im nationalen Recht abzuweichen und spezifische Aspekte (z. B. den Beschäftigtendatenschutz) selbst zu regeln. Daher wurde in Deutschland vor allem das BDSG mit Blick auf die Öffnungsklauseln neu gefasst, aber auch bereichsspezifische Regelungen und die Landesdatenschutzgesetze (LSDG) wurden an die DSGVO angepasst.

3. ePrivacy-Verordnung

In Erwägungsgrund 173 der DSGVO hat sich der europäische Gesetzgeber darüber hinaus verpflichtet, auch die ePrivacy-Richtlinie zu überprüfen, um einen einheitlichen Datenschutz zu gewährleisten. Hierfür hat-

1 Richtlinie 95/46/EG. 2 Richtlinie 2002/58/EG.
3 Das Teledienstgesetz (TDG), das Teledienstdatenschutzgesetz (TDDSG) und weitestgehend der Mediendienste-Staatsvertrag (MDStV).
4 Richtlinie 2009/136/EG.

Foto: Rutmer Visser /iStock

te die europäische Kommission schon 2017 einen Vorschlag der ePrivacyVO verabschiedet, doch der EU-Ministerrat konnte sich lange Zeit auf keine gemeinsame Position festlegen.[5] Erst im Februar 2021 konnten sich die Mitgliedsstaaten auf ein Mandat einigen, womit nun Verhandlungen mit dem europäischen Parlament und der Kommission im Rahmen der Trilog-Gespräche über den endgültigen Wortlaut der Verordnung aufgenommen werden können. Allerdings steht weiter in den Sternen, wann die Verordnung tatsächlich in Kraft treten wird.

4. TTDSG

Aufgrund dieser fehlenden Vereinheitlichung der Datenschutzvorschriften auf europäischer Ebene herrscht vor allem im Bereich der ePrivacy oftmals Rechtsunsicherheit in der Frage, wann Dienstanbieter elektronischer Kommunikationsdienste bestimmten Regeln unterliegen und welche Regeln in der Anwendung Vorrang haben. Entscheidungen des Europäischen Gerichtshofs (EuGH) wie „Gmail“[6] oder „Skype-Out“[7], welche sich um die Anwendbarkeit des TKG drehten, zeigen offenkundig diese Unsicherheiten. Insbesondere das TMG ist zu weiten Teilen aufgrund des Vorrangs der DSGVO nicht mehr anwendbar. Dennoch haben weiterhin Vorgaben der Cookie-Richtlinie im TMG Niederschlag gefunden und sind weiterhin anwendbar. Auch das TKG ist aufgrund verschiedener Öffnungsklauseln und anderer geregelter Teilbereiche, wie beispielsweise dem Fernmeldegeheimnis, trotz Geltung der DSGVO weiterhin anwendbar.

Aufgrund dieser Unsicherheiten in der Anwendung und Abgrenzung beabsichtigt der deutsche Gesetzgeber nun die Zusammenführung des TMG und TKG in das neue TTDSG. Ziel ist es, mehr Rechtsklarheit zu schaffen, erforderliche Anpassungen an die DSGVO vorzunehmen und die Schaffung einer nationalen Übergangsregelung bis zum Inkrafttreten der ePrivacyVO.

Nachdem Ende Juli 2020 ein Referentenentwurf geleakt wurde, hat die Bundesregierung den offiziellen Entwurf Mitte Januar 2021 veröffentlicht. Nach der Anhörung der Verbände durch das Bundesministerium für Wirtschaft und Energie beschloss und veröffentlichte das Bundeskabinett am 10. Februar 2021 den Regierungsentwurf[8]. Der Bundesrat gab im März 2021 zu diesem Entwurf eine Stellungnahme[9] ab. Ende März beriet der Bundestag in erster Lesung den Entwurf und leitete die Vorlage in den Ausschuss für Wirtschaft und Energie weiter.

5. EKEK-Richtlinie und TKG-Novelle

Parallel zu den oben genannten Richtlinien hat der europäische Gesetzgeber mit dem Europäischen Kodex für die elektronische Kommunikation[10] (EKEK-Richtlinie) weitere Anpassungen hinsichtlich der Regelungen von elektronischen Kommunikationsnetzen und -diensten vorgenommen. In Deutschland wird die Richtlinie mit einer erneuten Novelle des TKG umgesetzt, welche derzeit noch im Gesetzgebungsprozess steckt. Diese wird mit dem Telekommunikations-

5 Vertiefend hierzu: Uphues, Das Warten hat kein Ende, DFN-Infobrief Recht 3/2020.
6 EuGH, Urteil v. 13.06. 2019 – C-193/18; vertiefend hierzu s. Mörike, No Signal, DFN-Infobrief Recht 07/2019. 7 EuGH, Urteil v. 05.06.2019 – C-142/18.
8 BT Drs. 19/27441. 9 BR Drs. 163/21(B). 10 Richtlinie (EU) 2018/1972.

modernisierungsgesetz (TKMoG) stattfinden. Momentan befindet sich das TKMoG ebenfalls noch in der Gesetzgebungsphase, ein Referentenentwurf[11] wurde Ende 2020 beschlossen. Das kommende überarbeitete TKG (TKG-E) wird den Rahmen von Telekommunikationsdiensten regeln, wobei der Datenschutz und das Fernmeldegeheimnis dagegen gebündelt im TTDSG geregelt werden sollen. Auswirkungen der EKEK-Richtlinie auf das TTDSG ergeben sich vor allem im Anwendungsbereich des TTDSG.

II. Regelungsinhalte des TTDSG

Ziel des TTDSG ist die Behebung der bestehenden Rechtsunsicherheit im Datenschutzrecht durch das Nebeneinander von DSGVO, TKG und TMG. Hierdurch soll eine höhere Transparenz für Anwender und Betroffene im Datenschutzrecht geschaffen werden. Erreicht wird dies unter anderem durch die Überführung der Bestimmungen zum Datenschutz- und Fernmelderecht aus den §§ 88 ff. TKG und den Datenschutzbestimmungen für Telemedien aus §§ 11 ff. TMG.

Der Gesetzesentwurf ist in vier Teile aufgeteilt: Den Teil der „Allgemeinen Vorschriften", den Teil zum „Datenschutz und Schutz der Privatsphäre in der Telekommunikation", den Teil „Telemedienschutz, Endeinrichtung" und den Teil „Straf- und Bußgeldvorschriften und Aufsicht".

1. Anwendungsbereich

Der Anwendungsbereich des TTDSG soll neben der DSGVO nun auch sog. Over-the-top-Dienste (OTT) wie Messenger-Dienste explizit erfassen. OTT-Dienste sind Dienste, welche Kommunikationsinhalte von Nutzenden über das Internet übermitteln, ohne dass eine Kontrolle durch den Internetdienstleister möglich ist oder dieser für die Verbreitung eingebunden sein muss.

Die Eröffnung des Anwendungsbereichs geht auf die Umsetzung der EKEK-Richtlinie zurück, welche OTT-Dienste wie klassische TK-Dienste behandelt. Gemäß § 2 Abs. 1 TTDSG-E i. V. m. § 3 Nr. 24, 61 TKG-E fallen als „interpersonelle Telekommunikationsdienste" in den Anwendungsbereich des TTDSG auch webgestützte E-Mail-Dienste, Internettelefonie oder Kommunikationseinrichtungen in Onlinespieleplattformen.

2. Einwilligung bei Verwendung von Cookies

Inhaltliche Besonderheiten stellen insbesondere die Regelungen zum Einsatz von Cookies und vergleichbaren Technologien dar. § 24 TTDSG-E orientiert sich dabei eng am Wortlaut der ePrivacy-Richtlinie und umfasst nach Abs. 1 technologieneutral jegliche „Speicherung [oder Zugriff] von Informationen in der Endeinrichtung". Derzeit sind damit vor allem Cookies bei der Nutzung von Webseiten erfasst, aber auch schon in der Wirtschaft angedachte Techniken des „Browser Fingerprinting" werden von der Regelung erfasst.

Als Cookies werden kleine Textdateien bezeichnet, welche auf dem Computer des Nutzenden eines Onlinedienstes gespeichert werden. Durch sie können Webseitenbetreibende erkennen, wer ihre Seite gerade besucht und dadurch Präferenzen des Nutzenden wie beispielsweise die Log-in-Daten speichern, damit diese nicht bei jedem Besuch der Webseite erneut vorgenommen werden müssen. Auch der Inhalt eines Warenkorbs bei Onlineshops wird mithilfe von Cookies beim Nutzen des Shops gespeichert. Es ist durch Cookies allerdings auch möglich, dass Webseitenbetreibende anhand der gespeicherten Cookies erkennen können, welche Webseiten der Nutzende besucht hat und dadurch Interessen und Vorlieben des Nutzenden durch das umfangreiche Tracking erfahren. Diese Informationen werden vor allem in der Werbebranche für personalisierte Werbung genutzt. Zunehmend werden auch Trackingverfahren (z. B. das Browser Fingerprinting) entwickelt, die ohne eine Nutzung von Cookies auskommen.

§ 24 Abs. 1 TTDSG-E verlangt für die Speicherung oder den Zugriff auf Informationen wie Cookies stets eine Einwilligung des Nutzenden. Ausnahmen von diesem Einwilligungserfordernis gelten nur dann, wenn mithilfe dieser Daten eine Nachricht übertragen werden soll (§ 24 Abs. 2 Nr. 1 TTDSG-E) oder die Speicherung bzw. der Zugriff auf die Daten für die Nutzung des „vom Nutzer ausdrücklich gewünschten Telemedienendienstes" „unbedingt erforderlich" ist (§ 24 Abs. 2 Nr. 2 TTDSG-E).

Bemerkenswert ist bei dieser Regelung, dass der Anwendungsbereich nicht, wie im Rahmen der DSGVO, von einem Personenbezug abhängig gemacht wird. Dadurch soll der Nutzende unabhängig vom Vorliegen von personenbezogenen Daten bei jedem Eingriff geschützt werden. Außerdem stellt die Bundesregierung in den Erwägungen zu § 24 TTDSG-E klar, dass neben den klassischen Endgeräten auch sämtliche mit dem Internet verbundenen Geräte des Internet-of-things (IoT) unter den Anwendungsbereich des Einwilligungserfordernisses fallen sollen.

Die Regelung macht die Nutzung von Tools zur Webseitenoptimierung wie Analytics oder Reichweitenmessung weiterhin von der Einwilligung der Nutzenden abhängig. In der Praxis würde dies weiterhin für die bekannten unübersichtlichen Cookie-Banner sorgen, welche Nutzende oftmals gezielt verwirren sollen, um eine Einwilligung zu erreichen. Der Bundesrat hat in seiner Stellungnahme zum Regierungsentwurf daher vorgeschlagen, diese komplexen Banner zu verbieten. Er sieht vielmehr „eine einfache Gestaltung beispielsweise mithilfe von nur zwei Buttons (‚Einwilligen', ‚Ablehnen') [als] zielführend" an.[12] Doch ob eine solche Regelung im Hinblick auf die Vorgaben der ePrivacy-Richtlinie überhaupt zulässig ist, ist unklar. Eine Alternative hierzu könnte eine ebenfalls vom Bundesrat vorgeschlagene generelle Einwilligung (oder Ablehnung) von Cookies über die Browser-Einstellungen darstellen.

11 Abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/telekommunikationsmodernisierungsgesetz-referentenentwurf-20201612.pdf?__blob=publicationFile&v=8 (zuletzt abgerufen am 14.04.2021). 12 BR Drs. 163/21(B), S. 5.

3. Technische und organisatorische Vorkehrungen

§ 19 Abs. 2 TTDSG-E fällt mit seiner Regelung auf, dass Anbietende von Telemedien durch technische und organisatorische Vorkehrungen die Nutzung des Dienstes anonym oder unter Pseudonym ermöglichen sollen, soweit dies technisch möglich und zumutbar ist. Die Vorschrift basiert auf § 13 Abs. 5 und Abs. 6 TMG und wird in der Praxis kaum eine Rolle spielen, aufgrund von beispielweise Gerätekennungen wird eine Anonymisierung meist schon technisch unmöglich sein. Darüber hinaus läuft die anonyme oder pseudonymisierte Nutzung bei sozialen Netzwerken oder Messengerdiensten dem grundlegenden Zweck des Dienstes entgegen, denn das Geschäftsmodell solcher Plattformen zielt gerade auf die Identifizierbarkeit der Nutzenden ab.

Auch die Anzeigepflicht der Weitervermittlung auf eine andere Webseite gem. § 19 Abs. 3 TTDSG wird aufgrund der in der Praxis immer weiter verbreiteten Einbindung (Framing) von anderen Webseiten in die eigene Webpräsenz leerlaufen, da die Einbindung nicht als klassische Weiterleitung zu qualifizieren ist.

4. Fernmeldegeheimnis

Durch die Ausweitung des Anwendungsbereiches des TTDSG-E auf OTT-Dienste wird das Fernmeldegeheimnis in dem Entwurf gem. § 3 TTDSG-E nicht mehr nur für klassische TK-Dienste wie Telefon und SMS gelten, sondern nun auch für Messenger, Internettelefonie oder webbasierte E-Mail-Dienste, § 2 Abs. 1 TTDSG-E i. V. m. § 3 Nr. 24, 61 TKG-E. Als Konsequenz ist es Anbietenden von solchen TK-Diensten nicht gestattet, sich über das technisch erforderliche Maß hinaus Kenntnis vom Inhalt oder von den näheren Umständen der Kommunikation zu verschaffen, § 3 Abs. 3 S. 1 TTDSG-E. Eine Durchleuchtung von E-Mails zu Werbezwecken ist für Mailanbieter wie Google damit nicht mehr ohne Weiteres, wie beispielsweise einer Zustimmung des Nutzenden, möglich.

Im Übrigen soll das Fernmeldegeheimnis nicht der Wahrnehmung von Rechten der Erben eines Nutzenden entgegenstehen, § 4 TTDSG-E.[13]

5. Neue Aufsichtszuständigkeiten

Der Regierungsentwurf des TTDSG überträgt dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) einheitlich den Vollzug des 1. und 2. Teils des TTDSG, soweit personenbezogene Daten verarbeitet werden oder Anbietende von Telemedien § 24 TTDSG-E beachten müssen. Ursprünglich war der oder die BfDI nur für den Vollzug des TKG zuständig und für den Vollzug des TMG die Landesdatenschutzaufsichtsbehörden ermächtigt. Durch diese Anpassung werden die Verarbeitungen von personenbezogenen Daten und der Zugriff auf Endeinrichtungen von einer Aufsichtsbehörde einheitlich kontrolliert. Soweit in diesen Bereichen die Zuständigkeit des oder der BfDI nicht gegeben ist, bleibt die bisherige Aufsicht der Bundesnetzagentur (BNetzA) bestehen.

Hinsichtlich des 3. Teils des TTDSG-E fehlen ausdrückliche Zuteilungen der Aufsicht, insoweit dürfte die Aufsicht weiterhin bei den Landesdatenschutzbehörden liegen.

III. Fazit und Konsequenzen für Hochschulen

Die Einführung des TTDSG mag auf den ersten Blick einen positiven Eindruck machen, doch setzen zum Beispiel die Regelungen zur Verwendung von Cookies und ähnlichen Technologien lediglich die Situation fest, welche seit 2009 aufgrund der ePrivacy-Richtlinie und durch die Urteile des EuGH und BGH längst in der Praxis geformt worden ist. Digitalverbände kritisieren daher berechtigterweise, dass das Gesetz nicht die aktuellen Entwicklungen berücksichtige, sondern auf dem Stand der ePrivacy-Richtlinie von 2009 beruhe. Praktische Änderungen sind auf Grundlage des Regierungsentwurfs in der Verwendung von Cookies daher momentan nicht zu erwarten. Abzuwarten bleibt, welche Änderungen in der kommenden Zeit vorgenommen werden, bevor die endgültige Fassung des TTDSG in Kraft tritt. Gerade Forderungen wie die des Bundesrates zu einfachen Cookie-Bannern werden die Diskussionen weiterhin anfachen. Zu viel sollte aufgrund der engen Vorgaben der ePrivacy-Richtlinie allerdings nicht erwartet werden. Globale Browser-Einstellungen, wie ebenfalls vom Bundesrat vorgeschlagen, können eine Lösung darstellen, denn auch der europäische Gesetzgeber thematisiert schon diese Möglichkeit in Erwägungsgrund 66 der Cookie-Richtlinie. Mit dem vorgelegten Regierungsentwurf ist jedoch nicht mit einer umfassenden Lösung für den Einsatz von Cookies zu rechnen.

Dagegen stellt die Erweiterung des Anwendungsbereiches des TTDSG auf OTT-Dienste-Anbietende eine Klarstellung in der Praxis dar. Die noch 2019 von der Rechtsprechung des EuGH behandelte Problematik um die Einordnung von Skype-Out oder Gmail als Telekommunikationsdienstleister erledigt sich damit. Dadurch sind OTT-Dienste nun wie klassische TK-Dienste an das Fernmeldegeheimnis gebunden.

Auch auf Hochschulen und Forschungseinrichtungen wird das neue TTDSG Auswirkungen haben. Schon beim Betreiben einer öffentlichen Website sind die ggf. neuen Vorschriften zu Cookies umzusetzen. Auch im Falle eines öffentlichen Angebots eines OTT-Dienstes wie einem Messenger oder eines webbasierten E-Mail-Dienstes können Hochschulen an die Vorschriften des TTDSG gebunden sein. Inwieweit die Vorschriften dabei jeweils im Detail anzuwenden sind, muss nach Inkrafttreten des Gesetzes geprüft werden. Wie das TTDSG in seiner finalen Form aussehen wird, bleibt abzuwarten. Das finale Gesetz wird aufgrund der vielseitigen Wortbeiträge und der Vorschläge von Bundesrat, Datenschützern, Digitalverbänden und Wirtschaft sicherlich noch einige Änderungen im Vergleich zum jetzt vorliegenden Regierungsentwurf aufweisen. ◆

13 Zu der Ausgangsproblematik s. Strobel, Digitaler Nachlass – letzter Akt, DFN-Infobrief Recht 9/2018.

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.

Fliegen, wenn sonst keiner fliegt – das mussten René Jurk, IT-Sicherheitsbeauftragte des DFN-Vereins und Michael Röder, Dienstverantwortlicher für DFN-MailSupport, im Rahmen des …

… Vor-Ort-Audits der BSI-Zertifikate DFN-Mail-Support und RZ-Infrastruktur für Server- und Anwendungsbetrieb.

14. Januar 2021, 18 Uhr: Bei der Abfertigung am Flughafen BER ist – außer uns beiden und dem unabhängigen, vom BSI zertifizierten Auditor – nur eine Handvoll Menschen zu sehen. Ob es sich dabei um Passagiere oder Flughafenpersonal handelt, ist nicht genau auszumachen. Der neue Berliner Flughafen ist sehr weitläufig. Insgesamt haben wir den Eindruck, dass im Verhältnis „Reisende zu Personal“ die Reisenden deutlich in der Unterzahl sind. Das überrascht uns nicht, schließlich hat die Pandemie den Planeten fest im Griff.

Vor der Fahrt zum BER besuchen wir das Rechenzentrum der TU Berlin. Auch durch die Maske hindurch ist deutlich zu erkennen, wie zufrieden der Auditor mit dem Standort und den lokalen Gegebenheiten ist. Aber man spürt, dass sich die Gespräche anders gestalten – wenn auch das Votum unverändert gut ausfällt. Der Abstand, die Masken – jeder möchte sich richtig verhalten. Das führt dazu, dass die Situation etwas angespannt ist.

Denn schon unter Normalbedingungen ist ein gutes Vertrauensverhältnis in einer solchen Prüfsituation eine sehr wichtige Voraussetzung für alle Beteiligten.

Und warum befinden wir uns nun in einer Zeit, in der alle anderen im Homeoffice arbeiten, am Flughafen BER? Die Antwort ist naheliegend: Das Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz, mit dem der DFN-Verein seine Infrastruktur für den Dienst DFN-MailSupport zertifizieren lässt, besitzt eine begrenzte Gültigkeit von maximal drei Jahren. Zudem wurde der neue Informationsverbund RZ-Infrastruktur einschließlich seiner standardisierten Basisdienste zertifiziert. Die Ablauffrist ist wenig beeindruckt vom Pandemiegeschehen. Und um die dem Dienst zugrunde liegende Vertragslage weiterhin auf die Vorgaben des Zertifikats stützen zu können, ist ein Vor-Ort-Audit an ausgewählten Standorten unerlässlich. Es lässt sich nun einmal per Videokonferenz schlecht überprüfen, ob Wartungsintervalle von Feuerlöschern, Klimaanlagen und Netzersatzanlagen nachweisbar eingehalten, Zugangs- und Zutrittsbeschränkungen wirksam umgesetzt und Brandschutzbereiche mit entsprechenden Sicherheitstüren abgeschottet werden.

Fliegen im Dienste des DFN: Der Mund- und Nasenschutz ist momentan fester Bestandteil.

Schließlich gibt es Anforderungen an ein Zertifikat! Deren Umsetzung muss der Auditor mit Argusaugen überprüfen und dokumentieren.

Machen Sie sich keine Illusionen: Egal wie gut Sie sind, er findet eine Nachlässigkeit – das ist sein Job. So können sich teilnehmende Einrichtungen darauf verlassen, dass wir nichts übersehen.

Als wir um 19:20 Uhr in Stuttgart das Flugzeug verlassen, fällt uns ein nicht ganz unwichtiges Detail ein, mit dem wir uns vorher nicht auseinandergesetzt haben. Bei Reisen ins Ausland ist es klug, sich mit den lokalen Gegebenheiten vertraut zu machen. Innerhalb Deutschlands sind wir geneigt, bestimmte Umgebungsbedingungen vorauszusetzen. Zu Pandemiezeiten erscheint aber eine Strecke von 600 Kilometern schon wie eine Weltreise. Selbstverständlich wissen wir, dass auch in Baden-Württemberg keine Restaurants geöffnet sind und dass es Sicherheitsvorkehrungen gibt. Und so sind wir auf ein sparsames Sandwich aus dem Supermarkt vorbereitet. Was wir als Hamburger und Berliner nicht wissen: In Baden-Württemberg sind ab 19:00 Uhr infolge der Ausgangssperre sämtliche Geschäfte geschlossen. Aber auch dafür haben wir eine Lösung gefunden. Einschließlich des Vor-Ort-Audits und des Rückfluges verlaufen die nächsten Schritte routinemäßig.

Hat sich der Aufwand gelohnt? Ja – die Zertifikate liegen vor! Die Maske packen wir erst einmal zur Seite und gehen wieder zurück ins Homeoffice. Wer weiß, wie die Vor-Ort-Audits in drei Jahren ablaufen? Werden wir dann wieder genauso transparent und vertrauensvoll mit den Standorten zusammenarbeiten? Daran besteht überhaupt kein Zweifel, wir freuen uns darauf! ◆

DFN Live: Wissen teilen, Erfahrungen weitergeben

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

74. DFN-Betriebstagung

Am Dienstag und Mittwoch, 23. und 24. März 2021, traf sich die DFN-Community online zur 74. DFN-Betriebstagung (BT) und informierte sich über die neuen Entwicklungen rund um das Deutsche Forschungsnetz und seine Dienste. Rund 500 Teilnehmende zählte das gemeinsame Plenum, das über die Pexip-Plattform von DFNconf gestreamt wurde. Und auch die Fachforen von AAI über Sicherheit bis Multimedia, für die das Meeting-Tool Zoom genutzt wurde, waren mit bis zu 330 Gästen sehr gut besucht und boten viele spannende Themen wie beispielsweise IPv6. Dieses zog sich durch verschiedene Foren und wurde viel diskutiert. Neu bei der diesjährigen Frühjahrs-BT waren die liebevoll gestalteten Onlinepausenräume, in denen sich die Teilnehmenden als Avatare zwischen den Vorträgen und Foren austauschen konnten.

Treffpunkt gather.town: In den liebevoll gestalteten Pausenräumen machte es besonders viel Spaß, sich auszutauschen

TERMIN
Die 75. DFN-Betriebstagung findet am Dienstag und Mittwoch, **26.** und **27. Oktober 2021**, statt.

28. DFN-Konferenz „Sicherheit in vernetzten Systemen“

Für die 28. DFN-Konferenz „Sicherheit in vernetzten Systemen“, die vom 15. bis 18. März 2021 online stattfand, stellten unsere Kolleginnen und Kollegen vom DFN-CERT auch in diesem Jahr wieder ein spannendes und abwechslungsreiches Programm auf die Beine. Rund 300 Teilnehmende besuchten die Konferenz. In der Keynote berichtete der IT-Sicherheitsbeauftragte der Justus-Liebig-Universität Gießen, Matthias Stenke, über den Cyberangriff auf die Hochschule und die Hintergründe. Weitere Themen waren der Umgang mit dem Datenschutz-GAU und wie IT-Katastrophen aus technischer und juristischer Sicht gemeistert werden können sowie Phishing-Awareness mit Gamification. Das Tutorium „IPv6-Sicherheit“ im Anschluss erfreute sich ebenso großer Beliebtheit wie das Meet & Greet, das am Nachmittag zum Austausch einlud.

TERMIN
Die 29. DFN- Konferenz „Sicherheit in vernetzten Systemen“ findet am Donnerstag und Freitag, **3.** und **4. Februar 2022**, statt.

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

Bei der 81. Mitgliederversammlung am 2. Dezember 2020 wählten Vertreterinnen und Vertreter unter insgesamt 350 Mitgliedseinrichtungen einen neuen Verwaltungsrat. Als erste Amtshandlung ernannte der dreizehnköpfige erweiterte Vorstand im Anschluss Prof. Dr. Odej Kao von der Technischen Universität Berlin zum neuen Vorsitzenden. Auf das Herzlichste verabschiedet wurde Prof. Dr. Hans-Joachim Bungartz von der Technischen Universität München, der den Vorstand seit 2011 leitete. Nach zweimaliger Wiederwahl und somit insgesamt drei Wahlperioden konnte er gemäß der Satzung des Vereins nicht mehr gewählt werden.

Als stellvertretende Vorstandsvorsitzende wurden Dr. Rainer Bockholt, Direktor des Hochschulrechenzentrums der Rheinischen Friedrich-Wilhelms-Universität Bonn, und Christian Zens, Kanzler der Friedrich-Alexander-Universität Erlangen-Nürnberg, bestätigt. Auch sie sind dem Verein seit Längerem verbunden: Rainer Bockholt gehört seit 2009 dem DFN-Betriebsausschuss an und ist seit 2014 Mitglied des Verwaltungsrates sowie stellvertretender Vorstandsvorsitzender. Christian Zens ist seit 2017 stellvertretender Vorstandsvorsitzender. Zuvor gehörte er als Gast dem Verwaltungsrat an und vertrat dort die Belange deutscher Hochschulkanzlerinnen und -kanzler.

TERMIN
Die 82. Mitgliederversammlung findet am Dienstag, **8. Juni 2021**, statt.

15. Tagung der DFN-Nutzergruppe Hochschulverwaltung

edu.admin – Verwalten digital gestalten, so lautete das Motto der 15. Tagung der DFN-Nutzergruppe Hochschulverwaltung, die am 3. und 4. Mai 2021 zum ersten Mal online stattfand. Die Tagung organisierte die DFN-Nutzergruppe Hochschulverwaltung, unterstützt wurde sie dabei vom DFN-Verein. Vortragende aus Hochschulen, Forschung, Verwaltung und Wirtschaft beschäftigten sich mit hochaktuellen Themen aus den Bereichen Informationssicherheit, E-Government- und Onlinezugangsgesetz. Die Auswirkungen der COVID-19-Pandemie auf die Digitalisierung der Hochschulverwaltung hatten einen erkennbaren Einfluss auf die diesjährigen Schwerpunkte der Tagung: So ging es unter anderem um die Zukunft der Prüfungen, Cloud-Dienste und Awareness-Maßnahmen. Die erste Onlinetagung wurde sehr gut angenommen und war mit etwa 180 Teilnehmenden ebenso gut besucht wie die bisherigen Präsenzveranstaltungen.

In der 1991 gegründeten DFN-Nutzergruppe Hochschulverwaltung werden Entwicklungen der Informations-, Kommunikations- und Medientechnik in direkten Bezug zu Themen der Hochschuladministration gesetzt. Die Ergebnisse werden den Hochschulen alle zwei Jahre auf einer Tagung vorgestellt. Die Vortragsfolien finden Sie unter:
https://www.hochschulverwaltung.de/tagungen/2021-online/

TERMIN
Die 16. Tagung der DFN-Nutzergruppe Hochschulverwaltung findet vom **8.** bis **11. Mai 2022** in Wismar statt.

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

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

Überblick DFN-Verein

(Stand: 05/2021)

Fotos © jackijack/fotolia

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

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

Die Geschäftsstelle

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

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

Die Organe

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

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

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

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

Prof. Dr. Frank Jenko
(Technische Universität München)

Prof. Dr. Sabina Jeschke
(Deutsche Bahn AG)

Prof. Dr. Odej Kao
(Technische Universität Berlin)

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

Dr. Karl Molter
(Hochschule Trier)

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

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

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

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

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

Prof. Dr. Harald Ziegler
(Heinrich-Heine-Universität Düsseldorf)

Der Verwaltungsrat hat als ständige Gäste

eine Vertreterin der Hochschulrektorenkonferenz:
Prof. Dr. Monika Gross
(Beuth Hochschule für Technik Berlin)

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

einen Vertreter der Kultusministerkonferenz:
Jürgen Grothe
(SMWK Dresden)

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

den Vorsitzenden des ZKI:
Hartmut Hotzel
(Bauhaus-Universität Weimar)

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

Prof. Dr. Odej Kao
Vorsitz

Dr. Rainer Bockholt
Stellv. Vorsitzender

Christian Zens
Stellv. Vorsitzender

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

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

Die Mitgliedseinrichtungen

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

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

Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Hochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	FIZ Karlsruhe - Leibnitz-Institut für Informationsinfrastruktur
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe – Technik und Wirtschaft
	Karlshochschule International University
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Hochschule für angewandte Wissenschaften, Fachhochschule Kempten
Kiel	Christian-Albrechts-Universität zu Kiel
	Fachhochschule Kiel
	Institut für Weltwirtschaft an der Universität Kiel
	Helmholtz-Zentrum für Ozeanforschung Kiel (GEOMAR)
	ZBW – Deutsche Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft
Koblenz	Hochschule Koblenz
Köln	Deutsche Sporthochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Katholische Hochschule Nordrhein-Westfalen
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln gGmbH
	Technische Hochschule Köln
	Universität zu Köln
Konstanz	Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)
	Universität Konstanz
Köthen	Hochschule Anhalt
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e. V.
Landshut	Hochschule Landshut – Hochschule für angewandte Wissenschaften
Leipzig	Deutsche Telekom, Hochschule für Telekommunikation Leipzig
	Helmholtz-Zentrum für Umweltforschung – UFZ GmbH
	Hochschule für Grafik und Buchkunst Leipzig
	Hochschule für Musik und Theater „Felix Mendelssohn Bartholdy“
	Hochschule für Technik, Wirtschaft und Kultur Leipzig
	Leibniz-Institut für Troposphärenforschung e. V.
	Mitteldeutscher Rundfunk
	Universität Leipzig
Lemgo	Technische Hochschule Ostwestfalen-Lippe
Lübeck	Technische Hochschule Lübeck
	Universität zu Lübeck
Ludwigsburg	Evangelische Hochschule Ludwigsburg
Ludwigshafen	Hochschule für Wirtschaft und Gesellschaft Ludwigshafen
Lüneburg	Leuphana Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Leibniz-Institut für Neurobiologie Magdeburg
Mainz	Hochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Katholische Hochschule Mainz
	Universität Koblenz-Landau
Mannheim	Hochschule Mannheim
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	TÜV SÜD Energietechnik GmbH Baden-Württemberg
	Universität Mannheim
	ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung GmbH
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Philipps-Universität Marburg
Meißen	Hochschule Meißen (FH) und Fortbildungszentrum
Merseburg	Hochschule Merseburg (FH)
Mittweida	Hochschule Mittweida
Mülheim an der Ruhr	Hochschule Ruhr West
Müncheberg	Leibniz-Zentrum für Agrarlandschafts- u. Landnutzungsforschung e. V.
München	Bayerische Staatsbibliothek
	Hochschule für angewandte Wissenschaften München
	Hochschule für Philosophie München
	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e. V.
	Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt GmbH
	ifo Institut – Leibniz-Institut für Wirtschaftsforschung e. V.
	Katholische Stiftungshochschule München
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft
	Technische Universität München
	Universität der Bundeswehr München
Münster	Fachhochschule Münster
	Westfälische Wilhelms-Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neu-Ulm	Hochschule für Angewandte Wissenschaften, Fachhochschule Neu-Ulm
Nordhausen	Hochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
Nürtingen	Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen
Nuthetal	Deutsches Institut für Ernährungsforschung Potsdam-Rehbrücke
Oberwolfach	Mathematisches Forschungsinstitut Oberwolfach gGmbH
Offenbach/M.	Deutscher Wetterdienst (DWD)
Offenburg	Hochschule Offenburg
Oldenburg	Carl von Ossietzky Universität Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Bundesgesellschaft für Endlagerung mbH (BGE)
Pforzheim	Hochschule Pforzheim – Gestaltung, Technik, Wirtschaft und Recht

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

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

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

DFN newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

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