DFN mitteilungen

Abstand, bitte!

Die Folgen von COVID-19 für das X-WiN

Im Auge des Zyklons
Der Weg zum Krisenmanagement

Anpacken
Umweltschutz und Nachhaltigkeit in Rechenzentren

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: dfn-verein@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
© DFN-Verein 08/2020

Fotonachweis
Titelfoto: André Rumann / corpus delicti
Seite 6/7: baona / iStock
Seite 36/37: Supersmario / iStock
Umschlag Rückseite: André Rumann / corpus delicti

Der DFN-Vorstand (von links nach rechts):
Christian Zens (Stellv. Vorsitzender),
Prof. Dr. Hans-Joachim Bungartz (Vorsitzender),
Dr. Rainer Bockholt (Stellv. Vorsitzender).
Foto: Frank Homann

Liebe Leserinnen, liebe Leser,

die COVID-19-Pandemie hat uns alle vor besondere Herausforderungen in verschiedener Hinsicht gestellt, und der DFN-Verein war davon nicht ausgenommen. Bei allem Vertrauen in die Stärken der Gemeinschaft im Verein und in die Handlungsfähigkeit seiner Geschäftsstelle – wir als Vorstand waren uns sehr schnell des besonderen Fokus bewusst, in den der DFN-Verein innerhalb weniger Wochen gerückt war: Wird das Netz den teils drastisch gestiegenen Anforderungen gerecht? Vor welchen Herausforderungen werden unsere Dienste stehen, allen voran DFNconf? Mit welcher Erwartungshaltung werden die Mitglieder auf den Verein blicken? Keine einfachen Fragen, aber wir können mittlerweile ein ganz überwiegend positives Zwischenfazit ziehen: Der DFN-Verein hat in dieser ersten Welle von Veränderungen durch die Pandemie gezeigt, wie gut er aufgestellt ist.

Aber fraglos gibt es im Verein nun einiges zu besprechen. So stellt sich angesichts der inzwischen vorliegenden Erfahrungen mit onlinebasierter Lehre sowie den damit verbundenen technischen Anforderungen die offenkundige Frage, welche Rolle der DFN-Verein zukünftig bei diesem Thema für sich insgesamt und für Dienste wie DFNconf sieht. Ideen und Erwartungen in ganz verschiedene Richtungen stehen dazu schon im Raum und wollen abgewogen werden. Angesichts der großen Expertise im Verein – sei es bei den Mitgliedseinrichtungen, in den Ausschüssen, den Vereinsorganen, im Strategischen Beirat oder in der Geschäftsstelle – dürfen wir aber sehr zuversichtlich sein, dass uns auch diese Diskussionen wieder ein Stück weiterbringen werden. Und somit kann die COVID-19-Pandemie sogar als Impulsgeber verstanden werden, der Fragestellungen in den Vordergrund rückt, die manchmal vielleicht zu Unrecht im ständigen Wettstreit der Prioritäten hintangestellt wurden.

Doch nicht nur in der Lehre konnten Erfahrungen in Sachen „online“ gesammelt werden, der DFN-Verein erlebte in seiner 80. Mitgliederversammlung tatsächlich seine Online-Premiere. Dank akribischer Vorarbeit und dem engagierten Mitmachen aller lief es äußerst rund – auch wenn die persönlichen Begegnungen, der vielfältige Austausch und nicht zuletzt das Vorabendprogramm schon schmerzlich vermisst wurden. Unsere 80. Mitgliederversammlung hat aber auch in anderer Hinsicht quasi Geschichte geschrieben: Nach intensiven Diskussionen quer durch den Verein – auf allen Ebenen und allen Kanälen – hat sich der DFN-Verein eine neue Entgeltordnung gegeben; am Ende zwar nicht einmütig, aber mit einer überzeugenden Mehrheit auf Basis der gelebten Willensbildung in der Gemeinschaft. Ein solcher Kraftakt soll an dieser Stelle auch erwähnt werden, er kommt ja nicht alle Tage vor – was nun fürwahr ein Schreckensszenario wäre. Bei dieser Bewertung sind wir uns sicherlich alle einig.

Wir wünschen Ihnen eine informative und unterhaltsame Lektüre.

Der DFN-Vorstand


1


2


3


4


5


6


7


8


9


10


11


12


13

Unsere Autoren dieser Ausgabe im Überblick

1 Henry Kluge, DFN-Verein (kluge@dfn.de); **2** Dr. Stefan Piger, DFN-Verein (piger@dfn.de); **3** Maimona Id, DFN-Verein (id@dfn.de); **4** Dr. Leonie Schäfer, DFN-Verein (schaefer@dfn.de); **5** Dr. Jakob Tendel, DFN-Verein (tendel@dfn.de); **6** Burcu Ortakaya, TÜBİTAK ULAKBİM (burcu.ortakaya@tubitak.gov.tr); **7** Marina Köhn, Umweltbundesamt (marina.koehn@uba.de); **8** David Hausheer, OVGU Magdeburg und ETH Zürich (hausheer@ovgu.de); **9** Timo Malderle, Universität Bonn (malderle@informatik.uni-bonn.de); **10** Michael Meier, Universität Bonn, FKIE (mm@cs.uni-bonn.de); **11** Matthias Wübbeling, Universität Bonn, FKIE (wuebbel@cs.uni-bonn.de); **o. Abb.** Christine Kahl, DFN-CERT (kahl@dfn.de); **12** Owen Mc Grath, Forschungsstelle Recht im DFN (o.mcgrath@uni-muenster.de); **13** Marten Tiessen, Forschungsstelle Recht im DFN (tiessen@uni-muenster.de)

Inhalt


40
60
2
20
80
100
0

Wissenschaftsnetz

Auf den Kopf gestellt – was das X-WiN jetzt leisten kann
von Henry Kluge und Stefan Piger

Zusammenhalt in Krisenzeiten – DFNconf verbindet
Interview mit Christian Meyer

Auf den Kopf gestellt – was das X-WiN jetzt leisten kann

Als Mitte März die Kontaktverbote und Ausgangsbeschränkungen aufgrund der steigenden Zahl von Corona-Infektionen in Kraft traten, wechselten Studierende und Beschäftigte aus Forschung und Lehre weltweit vom Büro, Labor und Vorlesungssaal ins Homeoffice. Das tägliche Arbeiten wurde auf den Kopf gestellt, Prozesse mussten angepasst und Kommunikationswege neu gedacht werden. Von jetzt auf gleich musste die Digitalisierung ein großes Stück vorankommen, wodurch die IT und damit auch die Datennetze mehr denn je zur wichtigen Infrastruktur wurden und deren Verfügbarkeit und Leistungsfähigkeit in den Fokus der Öffentlichkeit rückten.

Text: **Henry Kluge, Stefan Piger** (DFN-Verein)

Foto: Torychemistry / Adobe Stock

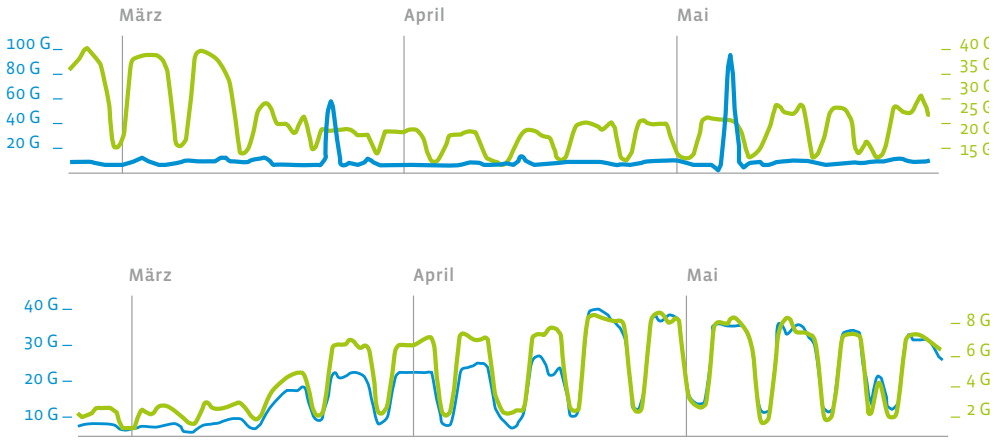


Abbildung 1: Verkehr mit Cloud Provider und Content Delivery Networks (exemplarisch oben Google) sowie mit Kabel- und DSL-Provider-Networks (exemplarisch unten DTAG), X-WiN ausgehend in blau, -eingehend in grün dargestellt

Der Übergang auf Homeoffice und digitale Lehre flößte auch vielen Teilnehmern am Dienst DFNInternet verständlicherweise Respekt ein. Befürchtungen, dass die Anbindungen der Einrichtungen an das Wissenschaftsnetz X-WiN dem erwarteten Anstieg des Verkehrsvolumens nicht gewachsen sein würden, erwiesen sich jedoch in den allermeisten Fällen als unnötig. Ein Grund hierfür war die Ende 2019 abgeschlossene Leistungssteigerung des Dienstes DFNInternet, die für die Teilnehmer erhebliche Erhöhungen ihrer Bandbreiten brachte. Dadurch waren die Anbindungen der Teilnehmer in der Regel so gut dimensioniert, dass sie ausreichende Übertragungskapazitäten für die nun gefragten Anwendungen zur Verfügung stellen konnten. Teilnehmern, die trotzdem ein Upgrade ihres Dienstes wünschten, wurde in der Regel zeitnah geholfen. Für mehr als 30 Einrichtungen konnte die DFN-Geschäftsstelle entsprechende Upgrades bis zum Semesterbeginn Mitte April realisieren.

Solides Fundament – Status des Wissenschaftsnetzes

Für das X-WiN stellte die veränderte Nutzung keine große Herausforderung dar, da parallel zur Leistungssteigerung von DFNInternet die Gesamtkapazität des X-WiN-Kernnetzes um 6.000 Gbit/s auf nahezu 10.000 Gbit/s erhöht wurde. Dadurch gab es auch hier zum Start des Sommersemesters keine Kapazitätsengpässe.

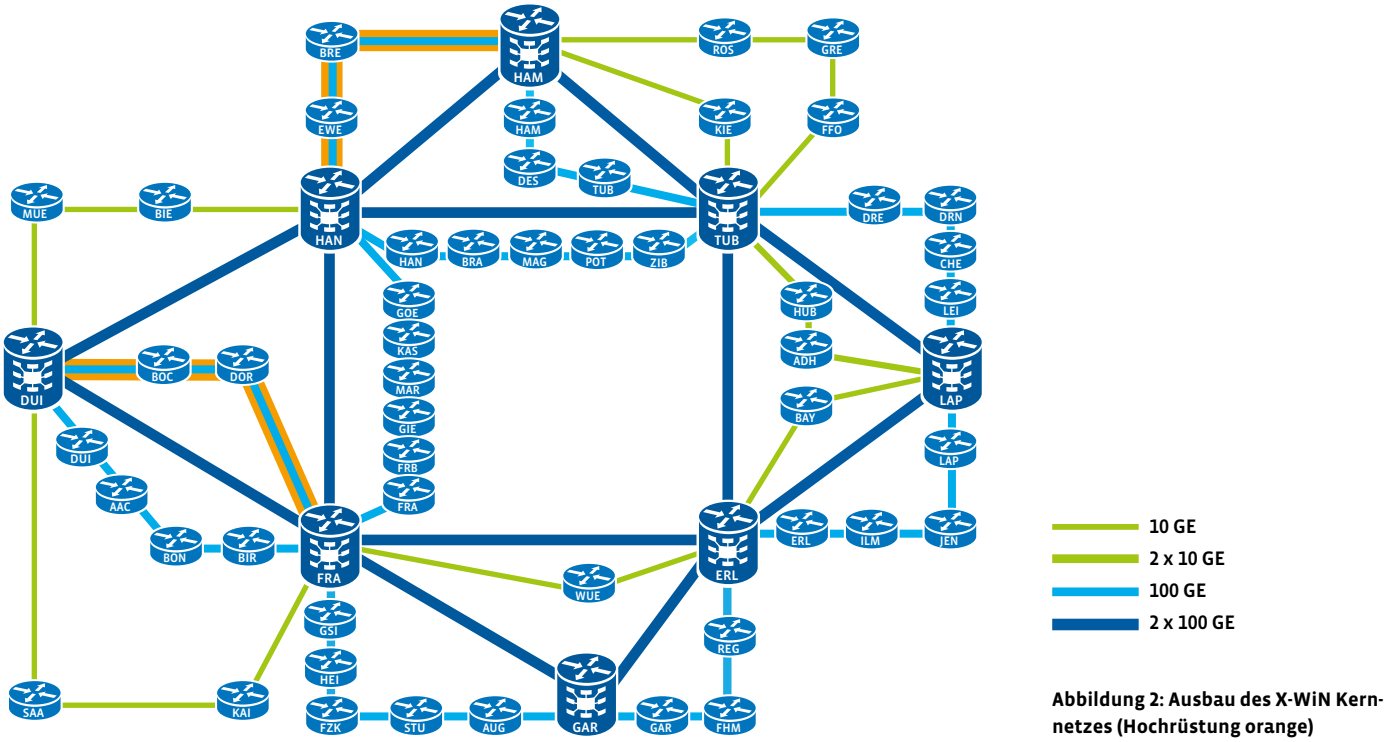


Abbildung 2: Ausbau des X-WiN Kernnetzes (Hochrüstung orange)

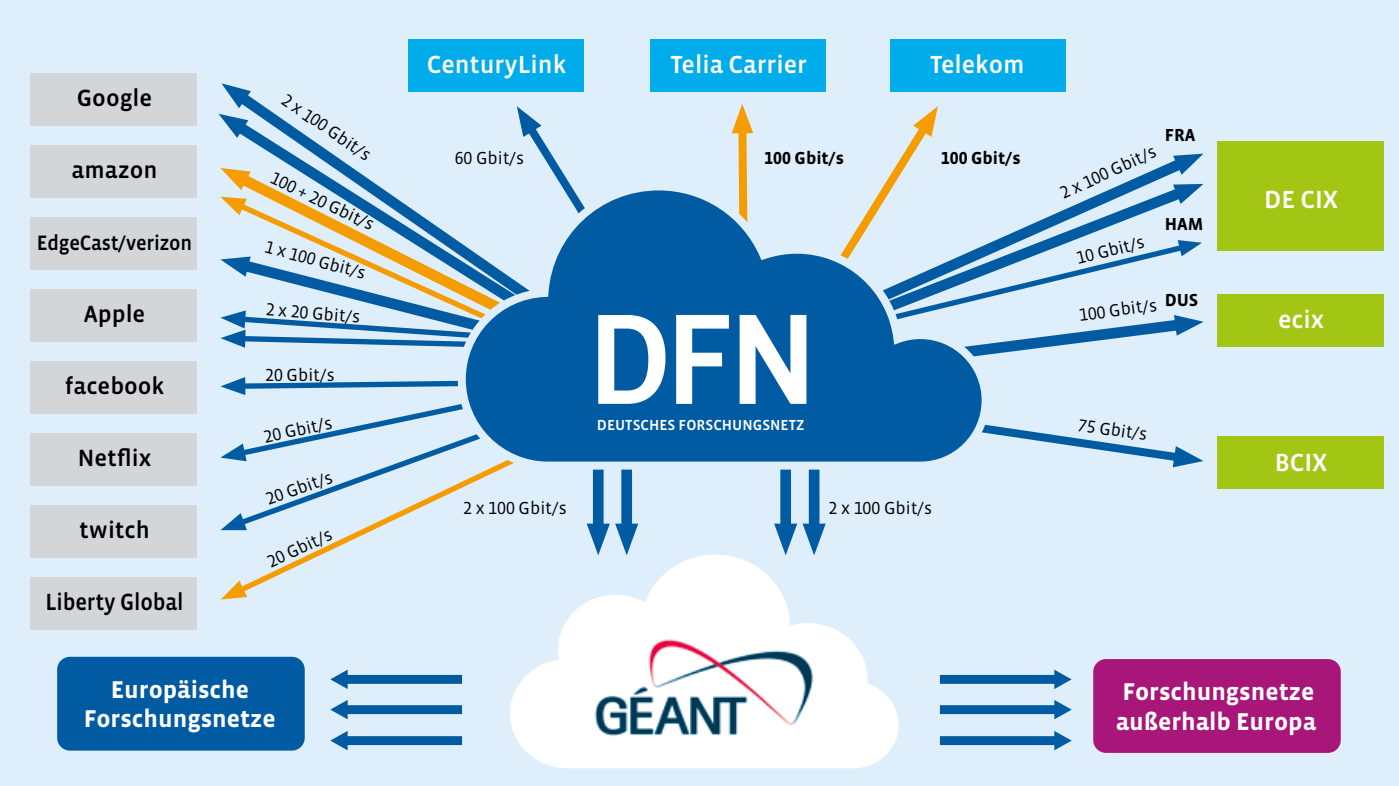


Abbildung 3: Außenanbindungen des X-WiN (Optimierungen orange)

Dies galt auch für die Übergänge des Wissenschaftsnetzes zu anderen Netzen sowie zu den beiden kommerziellen Global-Upstream-Providern. Interessant zu beobachten waren jedoch die Verlagerungen des Datenverkehrs mit Beginn des Sommersemesters. So blieben zwar die Verkehrsvolumina über die internationalen Wissenschaftsnetze relativ unverändert, der Datenverkehr zu den Content- und Cloud-Provider-Netzen nahm jedoch deutlich ab, während die Übertragungsraten in die kommerziellen Kabel- und DSL-Provider geradezu explodierten. Mitte April konnte in den Spitzenzeiten ein Wachstum der Übertragungsraten von über 300 Prozent gegenüber Anfang März verzeichnet werden. Begründet liegen diese Verschiebungen in der bereits beschriebenen neuen Situation. Der überwiegende Anteil der Nutzer verlagerte seinen Arbeitsort an den heimischen Schreibtisch und griff über kommerzielle Netze und das Wissenschaftsnetz auf Daten und Anwendungen in den Einrichtungen zu.

Herausfordernde Zeiten Peering im kommerziellen Internet

Nicht alle kommerziellen Netze und speziell deren Außenanbindungen (Peerings) waren auf diese Situation vorbereitet. Diese Erfahrung machten in den Wochen ab Mitte März zahlreiche Nutzer. Es kam zeitweise zu Engpässen zwischen kommerziellen Netzbetreibern, die auf dem Weg der Daten aus den Einrichtungen am Wissenschaftsnetz zu den heimischen Arbeitsplätzen, durchlaufen werden mussten. Das Network Operations Center (NOC) des DFN erhielt wiederholt Meldungen zu Konnektivitätsproblemen zwischen den Anschlüssen der Deutschen Telekom AG (DTAG) und den Einrichtungen am Wissenschaftsnetz. Diese Probleme konnten mit Messungen an DSL-Anschlüssen der DTAG auch nachvollzogen werden.

Diesbezügliche Beschwerden des DFN-Vereins bei den Upstream-Providern ergaben als Grund für diese Situation eine Überlast auf den Verbindungen zwischen dem Netz der DTAG und beiden Upstream-Providern des DFN-Vereins. Die beteiligten Parteien sahen sich außerstande, zeitnah, das heißt noch vor Start des Sommersemesters, Abhilfe zu schaffen und die Situation zu entschärfen. Für viele Nutzer im Homeoffice ist eine performante und stabile Erreichbarkeit des Wissenschaftsnetzes jedoch unabdingbar, um effizient arbeiten zu können. Um dies zu ermöglichen, musste der DFN-Verein schnell reagieren. Verhandlungen mit der DTAG über ein kostenneutrales direktes Private Peering wie bei solchen Konstellationen unter Internetservice- und Content-Providern üblich, waren leider nicht erfolgreich. Nach Abwägung aller Handlungsoptionen und Risiken wurde daraufhin ein kostenpflichtiger global Upstream bei der Deutschen Telekom AG beauftragt und am 16. April 2020, also noch vor Start des Sommersemesters, implementiert und auch unmit-

telbar in Betrieb genommen. Die Konnektivitätsprobleme konnten somit auf Initiative des DFN-Vereins erfolgreich behoben werden.

Mit Weitsicht – Optimierungen im Wissenschaftsnetz

Auch wenn sich das Kernnetz des X-WiN als durchweg gut gerüstet für die Herausforderungen der COVID-19-Pandemie erwies und es zu keinem Zeitpunkt zu Engpässen oder Überlastsituationen kam, erschien eine Hochrüstung einzelner Verbindungen im Kernnetz sinnvoll. Ursächlich für diese Entscheidung waren die kurzfristig beauftragten Upgrades von DFNInternet-Diensten. Um auch in Zukunft über genügend Kapazitätsreserven zu verfügen, wurden für die Kernnetz-Router an den Standorten Bremen, Oldenburg, Bochum und Dortmund neue Anbindungen mit 100 Gbit/s geplant und beauftragt. Diese Arbeiten können zeitnah durchgeführt werden, da bereits in der Frühphase der aktuellen Krise entsprechende Reserven an technischen Komponenten angelegt wurden.

Auch an den Außenanbindungen des X-WiN wurden seit Beginn der COVID-19-Krise weitere Optimierungen vorgenommen. So wurden seit Mitte März mit mehr als zehn Netzbetreibern neue Peerings vereinbart und in der Mehrzahl auch bereits realisiert. Darunter waren auch ein direktes Peering mit Liberty Global mit 20 Gbit/s, wodurch die Kunden von UnityMedia nun einen direkten Zugang zum X-WiN haben, und zwei georedundante Peerings mit Amazon mit je 100 Gbit/s. Schließlich wurde noch die Anbindung an einen der Global-Upstream-Provider auf 100 Gbit/s erhöht.

Gibt es Lehren aus der Krise?

Nach etwa drei Monaten im Krisenmodus und den so gemachten Erfahrungen, ist es Zeit für ein erstes Resümee. Festzuhalten ist, dass das Wissenschaftsnetz die geänderten Anforderungen bisher gut bewältigen konnte und sich die Leistungsfähigkeit und Verfügbarkeit der Kommunikationsdienste unverändert auf höchstem Niveau bewegen. Aber was sind die Gründe dafür und wo konnte der DFN-Verein auch noch etwas lernen?

Naturgemäß sind Weitverkehrsnetze mit der Ausdehnung und Komplexität des X-WiN träge Systeme, das heißt unvorhersehbare Entwicklungen und Krisen führen nur dann nicht zu Einschränkungen oder gar Katastrophen, wenn das System ausreichende Puffer enthält. Diese Puffer existieren im Wesentlichen in Form von im Normalbetrieb nicht genutzter Übertragungskapazität. Wichtig sind aber auch Reserven an technischen Komponenten, mit denen notwendige Kapazitäten an nicht vorhersehbarer Stelle nachgerüstet werden können sowie etablierte Prozesse, die für eine schnelle Inbetriebnahme dieser sorgen. Außerdem sollte die Abhängigkeit von Dritten minimiert werden. Das ist nur möglich, wenn die Funktionsherrschaft über die kritischen technischen Plattformen des Netzes und der Basisinfrastruktur gegeben ist.

Eine weitere Erkenntnis aus den letzten Wochen betrifft die Kommunikation mit den Teilnehmern und der interessierten Öffentlichkeit. Eine lebhafte, bilaterale Kommunikation mit einzelnen Teilnehmern wurde auch während der Krise geführt und gewann noch an Bedeutung. Durch die direkte Kommunikation war es möglich, die Teilnehmer schnell und individuell dabei zu unterstützen, die neuen Herausforderungen zu meistern. Zusätzlich schuf der DFN-Verein neue Kommunikationswege, um dem allgemein gestiegenen Informationsbedarf gerecht zu werden, denn die Verfügbarkeit und die Leistungsfähigkeit von Datennetzen rückte während der Krise immer weiter in den Fokus. Ein Ergebnis war die Etablierung eines News-Tickers auf der DFN-Webseite, der während des Höhepunktes der Pandemie tagesaktuelle Informationen zum Status der DFN-Dienste und der Infrastruktur bereitstellte. Der neue Kommunikationskanal stieß generell auf positives Feedback. Darüber hinaus wurden mit den Teilnehmern weitere Wünsche und Anregungen diskutiert, die die DFN-Geschäftsstelle gerne aufnimmt und weiterentwickelt, um die aktuellen Entwicklungen im Deutschen Forschungsnetz transparent und zielgerichtet zu vermitteln. ◆

Foto: onurdongel/iStock

Zusammenhalt in Krisenzeiten – DFNconf verbindet

Katastrophe oder Chance? Der Dienst, der im Deutschen Forschungsnetz (DFN) in Folge der COVID-19-Pandemie am härtesten auf die Probe gestellt wurde, ist der Videokonferenzdienst DFNconf. Über Nacht gingen die Nutzerzahlen durch die Decke und ein funktionierendes System stieß an seine Grenzen. Was es heißt, einen Dienst im Hauruckverfahren krisensicher zu gestalten, wie viele schlaflose Nächte das kostet – aber auch, wie stark eine Gemeinschaft in Krisenzeiten ist, erzählt unser Dienstverantwortlicher Christian Meyer im Interview.

Erprobter Krisenmanager: Christian Meyer behält auch während der COVID-19-Pandemie einen kühlen Kopf. *Foto: Maimona Id/DFN-Verein*

Wissenschaft und Lehre im Ausnahmezustand. Und ein Videokonferenzdienst, der in die Knie geht. Da kann man schon mal nervös werden, oder?

Auf jeden Fall. Wir standen alle ziemlich unter Strom. Mitte März wechselten unsere Einrichtungen – Universitäten, Hochschulen und Forschungsinstitutionen – deutschlandweit ad hoc in den Notbetrieb und schickten einen Großteil ihrer Beschäftigten zeitgleich ins Homeoffice. Dadurch gingen die Meeting- und Teilnehmerzahlen unseres Videokonferenzdienstes DFNconf über Nacht auf allen Plattformen durch die Decke – in Spitzenzeiten um das Zehnfache. Die Antwort auf Social Distancing war der Ansturm auf die virtuellen Meeting-Räume. Das führte zu dramatischen Engpässen beim Erstellen neuer Meetings sowie massiven Einschränkungen beim Verbindungsaufbau und der Dienstqualität. Ich kann mich noch genau an Sonntagnacht vom 15. auf den 16. März erinnern. Ich habe mich hin und her gewälzt und bei der Vorstellung, welche Auslastung zu Wochenbeginn auf uns wartet, kein Auge zubekommen.

Und da waren sogar noch Semesterferien.

Ganz genau. Verschärfend kam hinzu, dass das Sommersemester 2020 nicht ausfallen, wie verschiedentlich gefordert, sondern im Gegenteil digital stattfinden sollte. Unsere Einrichtungen standen nun vor der Herausforderung, digitale Vorlesungen und Prüfungsformate zu entwickeln, um die Lehre an den Hochschulen

so gut es geht aufrechtzuerhalten. Spätestens da war klar: Wir brauchen eine möglichst rasche, bundesweit einheitliche Lösung, um unsere Anwender in dieser überaus schwierigen und unübersichtlichen Situation zu unterstützen.

So standen wir vor einer doppelten Herausforderung: zum einen, unseren Dienst auf der technischen Plattform Pexip so schnell wie möglich auszubau-

„Das war ein regelrechter Wettlauf mit der Zeit."

en, um die steigenden Nutzerzahlen im Bereich Videokonferenz bewältigen zu können, und zum anderen, unseren Anwendern möglichst bis zum Semesterbeginn am 19. April Ideen hinsichtlich einer möglichen E-Learning-Plattform im DFNconf zu präsentieren. Jeden Tag gab es neue Hürden, die wir überwinden mussten. Das war ein regelrechter Wettlauf mit der Zeit.

Mit welchen Maßnahmen habt ihr die Pexip-Plattform stabilisiert?

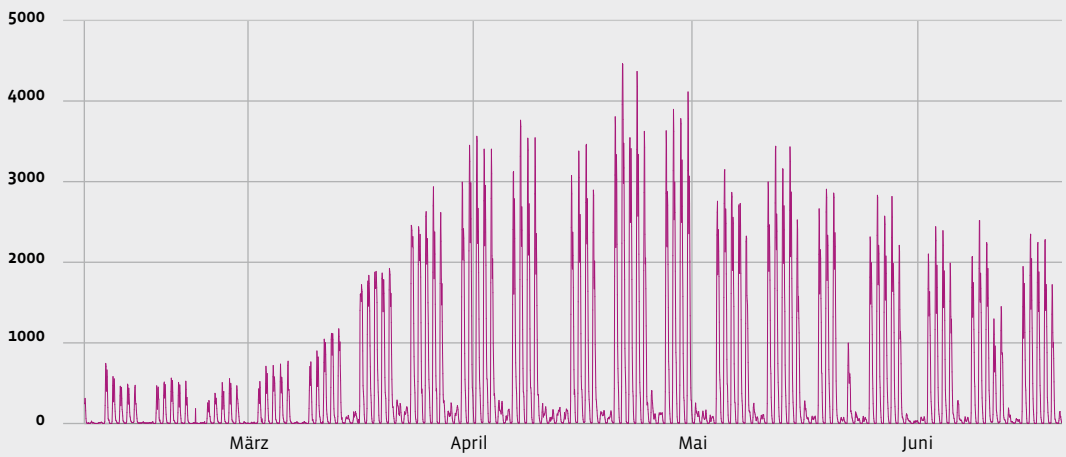
Das fing mit einer Reihe einfacher Sofortmaßnahmen an: Wir reduzierten die maximale Videoqualität von FullHD (1080p) auf zuletzt SD (448p), um mehr Meetings bewältigen zu können und empfahlen, diese möglichst außerhalb der Stoßzeiten durchzuführen, um die Infrastruktur zu entlasten und damit die Erreichbarkeit des Dienstes zu erhöhen. Außerdem rieten wir dazu, für Lehrveranstaltungen und Konferenzvorträge, die nicht zwingend Zwei-Wege-Kommunikation mit Audio und Video erfordern, das Streaming-Modul von DFNconf zu nutzen.

Um die Betriebsstabilität zu optimieren, konzentrierten wir uns vor allem darauf,

MEILENSTEINE DER TECHNOLOGIEWECHSEL

2000	Erste Planungen für einen Videokonferenzdienst
2002	Pilotdienst mit Multipoint Control Units (MCUs) von Radvision für Videokonferenzen
2003	DFNVC wird Regeldienst mit eigenem Entgelt. Ab 2006 im Dienst DFNInternet enthalten
2005	Verwaltungsrat erteilt Prüfungsauftrag für Webkonferenzdienst
2006	Wechsel von der Radvision-MCU zu MCUs von Codian (jetzt Cisco): Einführung von FullHD Videoqualität
	Pilotbetrieb „Macromedia Breeze", später „Adobe Connect" für Webmeetings
2007	nur noch Codian-MCUs
2018	Inbetriebnahme von Pexip als Nachfolgeplattform der abgekündigten Codian-Plattform: vereint Video- und Webkonferenztechnologie, DFNconf wird nun als Dienstbezeichnung für das Portfolio geführt

PEXIP: ANZAHL GLEICHZEITIG AKTIVER NUTZER

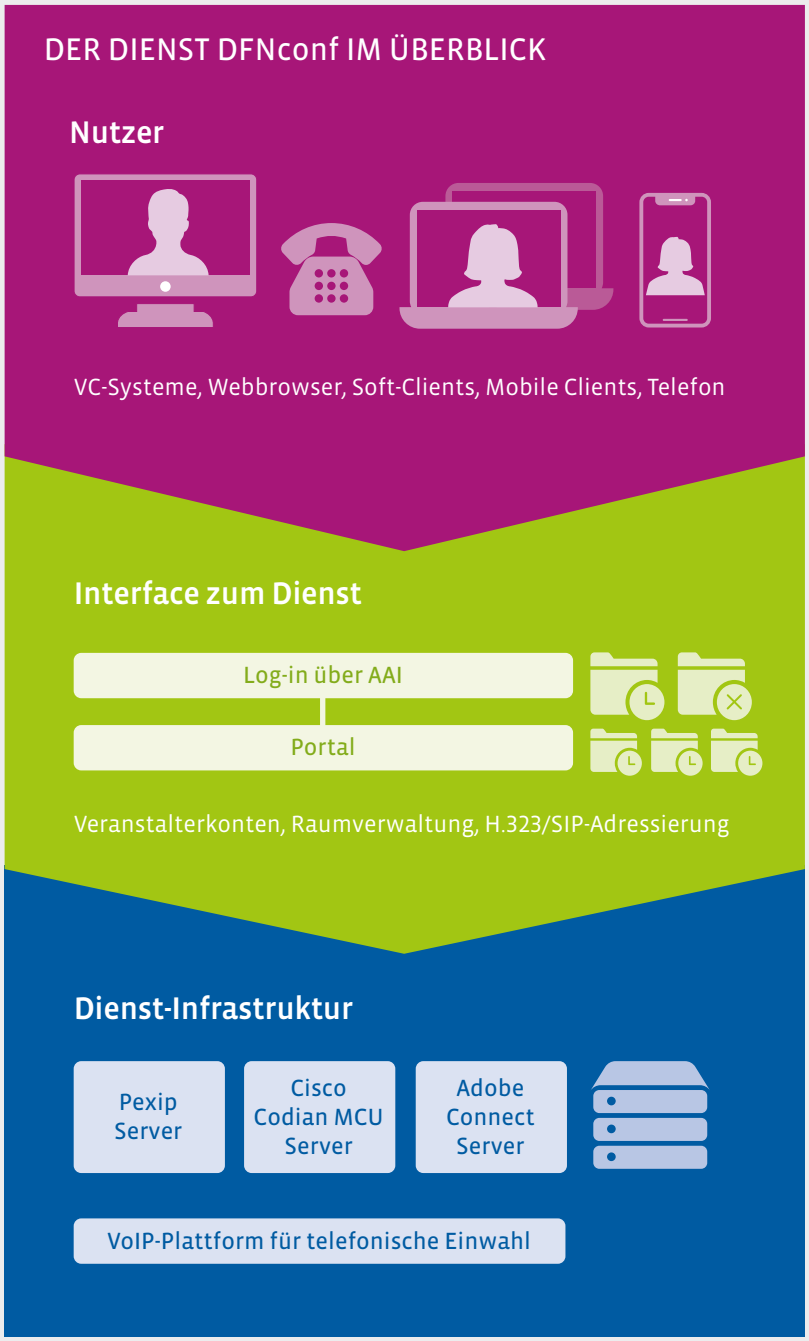


Im Februar:
Ø 400–500 gleichzeitige Nutzer mit 1.900 Nutzungsstunden Konferenzvolumen täglich

11.02.2020 (Sturmtief „Sabine"):
700 gleichzeitige Nutzer mit 2.400 Nutzungsstunden Konferenzvolumen täglich

21.04.2020 (Maximum in der COVID-19-Pandemie):
4.500 gleichzeitige Nutzer mit 26.600 Nutzungsstunden Konferenzvolumen täglich

**ein einstündiges Meeting mit drei Leuten erzeugt drei Nutzungsstunden Konferenzvolumen.*



weitere Kapazitäten zu schaffen. Hier ist uns von allen Seiten sehr große Hilfsbereitschaft entgegengebracht worden. Zum Beispiel vom Hersteller Pexip, der uns 2000 Video- und 1000 Audiolizenzen entgeltfrei zur Verfügung stellte. So konnten wir von je 400 auf insgesamt 5000 Video- und 3000 Audiolizenzen aufstocken.

Das ist schon sehr großzügig.

Es kommt noch besser: Ein großer Glücksfall und ein Beleg dafür, was die DFN-Gemeinschaft im Kern bedeutet, war das spontane Angebot einiger teilnehmender Einrichtungen, uns Anfang April kurzfristig Serverkapazitäten zur Verfügung zu stellen, um die Anzahl gleichzeitig stattfindender Meetings zu erhöhen. Dadurch haben wir innerhalb von zweieinhalb Wochen die Zahl der Konferenzknoten vervierfacht – auf insgesamt 53 Konferenzknoten an fünf Standorten. Diese Hilfsbereitschaft war wirklich enorm, an dieser Stelle noch einmal ein Riesendankeschön für die unkomplizierte Unterstützung.

Neben der Optimierung der Betriebsstabilität war es vor allem wichtig, unsere Anwender – sowohl die lokalen betrieblichen Ansprechpartner als auch die Endnutzer – zeitnah über unsere Maßnahmen zu informieren. Dass der Dienst nicht mehr wie gewohnt funktionierte, hat teils Ärger und Unverständnis erzeugt. Unsere Hotline war sehr stark

> „Dass der Dienst nicht mehr wie gewohnt funktionierte, hat teils Ärger und Unverständnis erzeugt.“

ausgelastet, es kam zu massiven Verzögerungen. Viele Endnutzer haben sich direkt an uns gewendet, ohne die Ansprechpartner in den lokalen Einrichtungen zu kontaktieren, wir hatten also auf einmal vermehrt mit First-Level-Support zu tun. Darum haben wir unter anderem unsere FAQ auf die aktuellen Erfordernisse abgestimmt und einen Newsticker zur COVID19-Pandemie ins Leben gerufen. Das Nutzervertrauen ist ein Stück verloren gegangen, das müssen wir wieder aufbauen. Gemeinsam haben wir versucht, so viel aus unserem Dienst rauszuholen, wie es nur geht. Und das ist uns, glaube ich, gut gelungen.

Erste Herausforderung gemeistert, kurz aufatmen und Haken dran. Was war nun mit dem Thema digitale Lehre? Warum hat euch das so viel Kopfzerbrechen bereitet?
Weil wir von diesem plötzlichen Bedarf unserer Anwende eine riesige Anzahl von E-Learning-Veranstaltungen mit mehreren Tausend Teilnehmern durchführen zu müssen, völlig überrascht wurden. So wie übrigens unsere Community auch. Dieser Bedarf hat sich trotz der schon lange anhaltenden Digitalisierungsbestrebungen in der Lehre erst durch die COVID19-Pandemie so verschärft. Das konnte niemand voraussehen. In seiner jetzigen Konstellation kann unser Dienst diese Nachfrage so kurzfristig nicht abdecken.

Was genau sind die Gründe dafür?
Da muss ich etwas ausholen: Der Dienst DFNconf besteht aus mehreren Modulen, die alle eine unterschiedliche Funktion erfüllen. So ergänzten wir den Dienst 2006 um die Plattform Adobe Connect, um einfache Webmeetings durchführen zu können. Diese ist außerdem in der Lage, Lern-Management-Systeme einzubinden. Als wir 2018 das Modul Pexip einführten, das sowohl Video- als auch Webkonferenzen vereint, wurde Adobe Connect mehr und mehr für E-Learning-Anwendungen genutzt. Dieses Modul basiert aber auf einer alten Webtechnologie, sie hat nach nunmehr 14 Jahren ausgedient und wurde vom Hersteller abgekündigt. Bereits seit 2017 beschäftigen wir uns intensiv damit, diese zu ersetzen.

Und warum kann die Pexip-Plattform kein E-Learning?
Na, ganz einfach darum, weil sie für ein völlig anderes Nutzungsszenario konzipiert wurde. Die Videoplattform „Pexip“ ist auf eine gleichmäßig steigende Anzahl von Besprechungen

„Ein Produkt, das wie die sprichwörtliche eierlegende Wollmilchsau funktioniert, gibt es nicht.“

mit maximal 23 gleichzeitigen Teilnehmern ausgerichtet und bietet darüber hinaus nur eine überschaubare Möglichkeit, interaktive Werkzeuge zu verwenden, dafür aber mit dem Fokus auf hoher Audio- und Videoqualität. Seit 2003 entwickeln wir unseren Videokonferenzdienst streng entlang der Bedarfe unserer Anwender: Pexip wurde explizit für die digitale „geschlossene Tür“ konzipiert. Das heißt, der damalige Auftrag unserer Anwender lautete: Wir wollen einen Videokonferenzdienst für Meetings mit hohem Schutz- und Sicherheitsbedarf: für Besprechungen mit vertraulichen Inhalten, beispielsweise zu unveröffentlichten Forschungsergebnissen oder für Bewerbungsgespräche. Und genau für diese Zielsetzung wird das DFNconf auch während der Corona-Krise gerne und viel genutzt. Das zeigen die nach wie vor hohen Auslastungszahlen auf der Pexip-Plattform. Dieser hohe Standard im Datenschutz führt jedoch zu Abstrichen in der Skalierbarkeit – sprich Einschränkungen in der Anzahl der Teilnehmer sowie im Umfang der Funktionen. Unterschiedliche Bedarfe verlangen immer noch unterschiedliche Tools. Ein Produkt, das wie die sprichwörtliche eierlegende Wollmilchsau funktioniert und solch ein breites Nutzungsspektrum abdecken kann, gibt es aus meiner Sicht nicht.

Zurück zum Problem digitales Sommersemester: An welche Lösung hattet ihr denn nun gedacht, um kurzfristig Abhilfe zu schaffen?
Als Ersatz für die Adobe-Connect-Plattform hatten wir uns bereits lange vor der COVID19-Pandemie damit beschäftigt, für unser Portfolio ein Tool zu finden, das sowohl Veranstaltungen mit einer großen Teilnehmerzahl als auch die Einbindung von Lernmanagementsystemen (LMS, z. B. Moodle) zulässt. Ende 2019 haben wir gemeinsam mit den europäischen Partnern im GÉANT-Verbund ein Proof-of-Concept für eine cloudbasierte hochskalierende Plattform für Videokonferenzen abgeschlossen, bei dem Zoom in allen Tests sehr gut abgeschnitten hat. Zoom hat sich dabei vor allem aufgrund des Funktionsumfanges und der Integrationsmöglichkeiten für Lehr- und Lernumgebungen bewährt und auch mit hoher Nutzerfreundlichkeit gepunktet. Aus diesem Grund ist der DFN-Verein im März

„Im März ist der DFN-Verein erneut auf die Firma Zoom zugegangen.“

erneut auf die Firma Zoom zugegangen, um die Möglichkeit für einen Rahmenvertrag zu prüfen. Ziel war es, eine Lizenzierung des Produktes für alle Teilnehmer im DFN zu erzielen. Leider konnten wir mit der Firma so kurzfristig zu keiner Übereinkunft kommen. Die Begründung war, dass sie wegen der unvorhergesehenen Krisensituation vom etablierten Geschäftsmodell, das aktuell keine Rahmenverträge vorsieht, erst mal nicht abweichen wollen. Jedoch hat uns Zoom für den Zeitraum nach der Bewältigung der Pandemie eine Perspektive für eine Einigung in Aussicht gestellt. Das wird sicher eine Herausforderung für alle Beteiligten, aber wir bleiben auf jeden Fall am Ball.

Was für ein Rückschlag. Wie sahen die Konsequenzen aus?
Dieses unbefriedigende Verhandlungsergebnis zu akzeptieren, ist mir sehr schwergefallen, zumal wir vor der Corona-Krise schon fast eine erste Einigung mit der Firma Zoom

erzielt hatten. Das war einfach nicht mein Anspruch. Wir wollten ja vermeiden, dass die ohnehin belasteten Einrichtungen unter den Druck geraten, eigene Betriebskonzepte aus dem Boden stampfen zu müssen und dadurch ein Wildwuchs an isolierten lokalen Lösungen entsteht. Und nun war eine schnelle Lösung leider nicht in Sicht.

Wir mussten letztendlich in den sauren Apfel beißen und unseren Teilnehmern empfehlen, unverzüglich in eigener Initiative lokale Lösungen für onlinebasierte Lehr- und Lernformate zu organisieren. Wir gaben außerdem den Rat, aufgrund der eingeschränkten Verhandlungsmöglichkeiten beim Preis mit den Anbietern kurze Vertragslaufzeiten von maximal einem Jahr abzuschließen. Im Bereich Wissenschaft und Lehre ist Open-Source-Software wie zum Beispiel BigBlueButton oder Jitsi weit verbreitet. Überwiegend sind die Anwender jedoch dazu übergegangen, Zoom zu nutzen. Das Produkt hat sich trotz Beanstandung der Datenschützer etabliert. Die Kritik ist bei der Firma angekommen, da erwarte ich eine Reihe von Verbesserungen.

Darüber hinaus haben wir eine Mailingliste ins Leben gerufen, um den gegenseitigen Erfahrungsaustausch hinsichtlich von E-Learning-Lösungen in unserer Community zu fördern und Feedback zu erhalten, wie groß der Bedarf ist und welche Lizenz- und Infrastrukturkosten zur Deckung diskutiert werden müssen. Mit den Ergebnissen können wir im DFNconf zielgerichtet eine E-Learning-Plattform aufbauen.

Was ist dein Fazit aus dieser Krise?

Im Nachhinein ist man ja immer klüger. Hätten wir im DFN-Verein besser vorbereitet sein können auf so eine Krise? Sind wir im Januar mit der Entscheidung, Pexip weiterzuentwickeln, den richtigen Weg gegangen? Und hätten wir schon viel früher, ohne von der COVID-19-Pandemie zu wissen, Zoom forcieren sollen? Ein echtes Dilemma!

„Das hat unser Team in Berlin und Stuttgart viele schlaflose Nächte gekostet."

Rückblickend muss ich sagen, wir haben, was die Krisenbewältigung angeht, vieles richtig gemacht – mit vereinten Kräften haben wir es innerhalb weniger Wochen geschafft, unseren Dienst schnell an die dringenden Erfordernisse anzupassen. Das hat unser Team in Berlin und Stuttgart viele schlaflose Nächte gekostet und war eine riesige Herausforderung, die uns auch nach Feierabend nicht losgelassen hat.

Würde ich mich wieder für eine standardkonforme Videoplattform mit hoher Datensicherheit und Videoqualität wie Pexip entscheiden? Ja. Aber mit dem Wissen von heute hätten wir sicherlich sehr viel eher auch eine hochskalierende Cloud-Lösung etabliert. Aber das konnten wir leider nicht voraussehen. In diesem Punkt waren unsere Anwender auf sich selbst gestellt – das fühlt sich nicht gut an und wirkt bei mir noch nach.

Aber hey, seit Jahren wird von der Digitalisierung der Hochschulen geredet, nun hat das Thema mit Turbogeschwindigkeit Fahrt aufgenommen. Das wird die Lehre nachhaltig verändern. Ein Nebeneffekt: IT-Bereiche und Rechenzentren erfahren jetzt viel mehr Anerkennung als zuvor und sind durch die Corona-Krise sichtbarer geworden. Gemeinsam mit unseren Anwendern sind wir gerade an einer sehr spannenden Entwicklung beteiligt und haben die Möglichkeit, neue Lösungen für Wissenschaft und Lehre mitzugestalten. Und darauf freue ich mich jetzt.

Das Gespräch führte Maimona Id

Starke Netze in Europa – DFN-Verein maßgeblich an EU-Projekten GN4-3 und GN4-3N beteiligt

Die Zusammenarbeit der Forschungsnetze auf europäischer Ebene ordnet sich seit Jahren rund um die GÉANT Association und die erfolgreich bewährten EU-Projekte der GN-Reihe. In den aktuellen Projekten GN4-3 und GN4-3N wird der strategische Ausbau der Forschungsnetzinfrastruktur in Europa weiter vorangetrieben. Beide begingen im Februar 2020 ihr einjähriges Projektjubiläum auf dem GÉANT-Symposium in Ljubljana.

Text: **Leonie Schäfer, Jakob Tendel** (DFN-Verein)

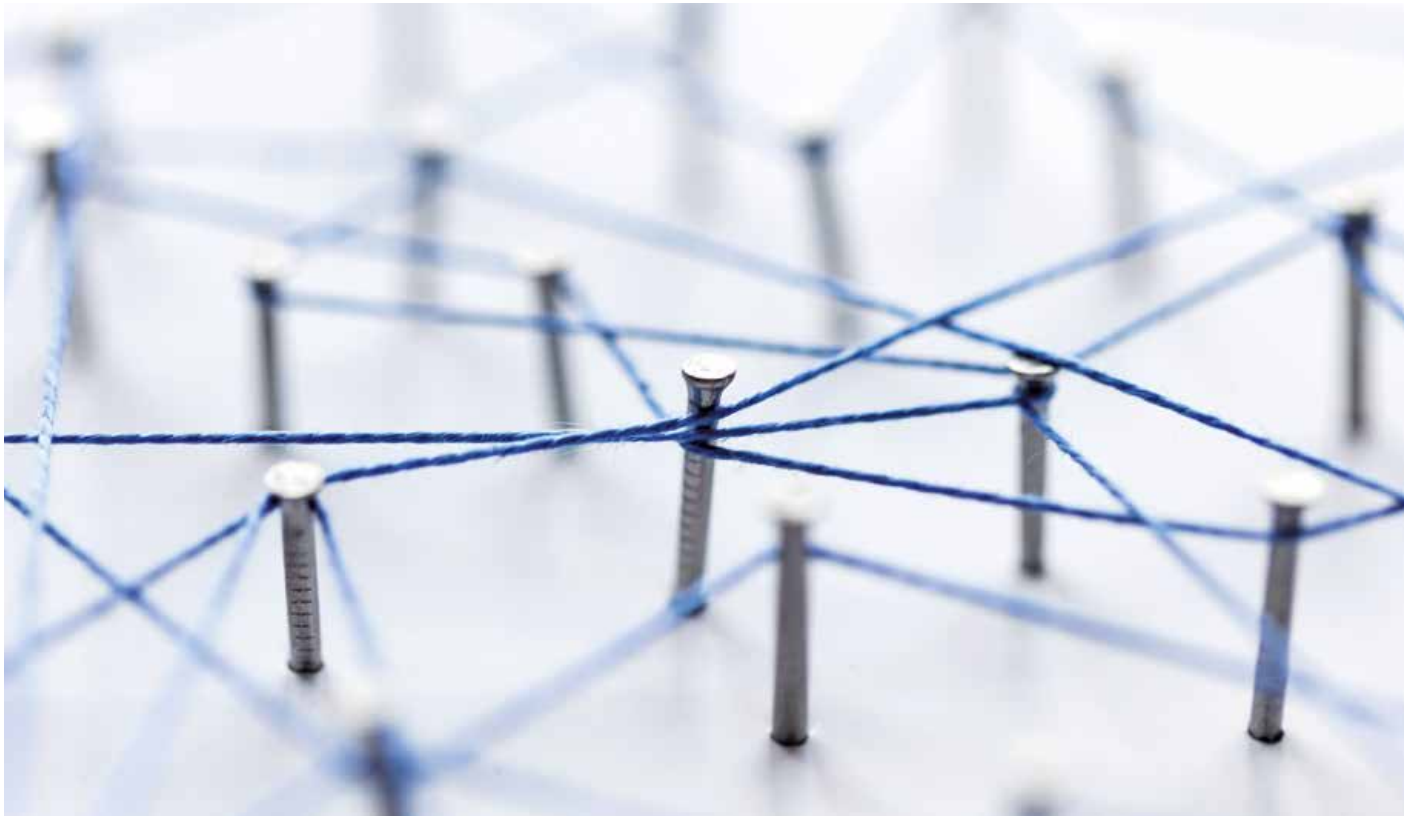


Foto: ink drop/Adobe Stock

Im Rahmen der EU-Projekte GN4-3 und GN4-3N trafen sich am 4. und 5. Februar 2020 über 250 Teilnehmerinnen und Teilnehmer zum GÉANT-Symposium in Ljubljana, Slowenien. Darunter waren auch Vertreter des DFN-Vereins sowie von Einrichtungen, die an unterschiedlichen Arbeitspaketen mitwirken und über die DFN-Beteiligung in GN4-3 gefördert werden. Ziel des Symposiums war, den aktuellen Stand der beiden Projekte zu diskutieren und die Projektinhalte an die hochdynamische Entwicklung im Bereich Netzwerke und Forschungsnetze in Europa anzupassen.

Andreas Veispak, Referatsleiter e-Infrastrukturen und Science Cloud bei der Europäischen Kommission, eröffnete das Symposium mit einem Plenarvortrag, in dem er die grundlegende Bedeutung von GÉANT für die Ziele der Kommission hervorhob. Insbesondere bezeichnete er das Projekt GN4-3N als wichtigen Schritt, um

> Die GÉANT-Community bildet eine Brücke

Europa in den nächsten 15 Jahren bei der Vernetzung der Wissenschaftsinfrastruktur in Führung zu bringen. Die GÉANT-Community bilde eine Brücke zwischen den Interessen der Forscher, der Mitgliedsländer und der EU Kommission, sagte Veispak. Neben zahlreichen Sitzungen rund um die Themen GÉANT-Netzwerk, Trust & Identity, Sicherheit, Cloud-Services und Community-Engagement gab es viele Diskussionen, die sich auch in den Kaffeepausen und beim Networking-Dinner fortsetzten.

Die Projekte im Überblick

Seit Anfang 2019 läuft die aktuelle und letzte Phase der EU-Projekte aus der „GN4" Reihe – dieses Mal mit zwei parallelen Projekten: GN4-3 und GN4-3N. Beide haben eine Laufzeit von 48 Monaten. GN4-3 zielt auf eine Weiterführung der Projekte GN4-1 und GN4-2 ab und befasst sich vor allem mit Forschung, Entwicklung und dem Betrieb des Forschungsnetzes.

GN4-3N dagegen ist ein neuer Projektansatz. Das Parallelprojekt befasst sich mit dem langfristigen Aufbau einer Basisinfrastruktur aus Glasfaserleitungen und optischen Systemen. Mit einem Zeithorizont von 15 Jahren werden langfristige Nutzungsrechte, die Indefeasible rights of use (IRU), an Glasfasern erworben. Ziel ist eine grundlegende Überarbeitung des GÉANT-Backbones im Hinblick auf Zuverlässigkeit, Reichweite und Anbindung der GÉANT-Partnerländer.

Herausforderungen für das Projekt GN4-3N bestehen in dem stark angestiegenen Datenvolumen im Forschungsbereich und den daraus resultierenden Anforderungen an Datenübertragungskapazitäten. Ein Beispiel hierfür ist der Aufbau des Radioteleskopverbunds „Square Kilometre Array" (SKA), das ganz neue Anforderungen an Netzwerke und Datentransfer zwischen Anlage und Forscher stellt.

Das Höchstleistungsrechnen entwickelt sich in den Exascale-Bereich mit seinen eigenen neuen Herausforderungen und einem weiter wachsenden Bedarf an weitverteilter Remote-Nutzung, die eine flächendeckende Verfügbarkeit von schnellen Netzen ohne Paketverlust noch wichtiger macht. Auch im Bereich Cybersecurity ergeben sich immer neue Anforderungen, die GN4-3 nun in einem eigenen Arbeitspaket behandelt.

GN4-3 unterstützt die Realisierung der sogenannten European Open Science Cloud (EOSC). Ziel ist die Bereitstellung von einfach und nahtlos zu nutzenden Diensten für Forscher und Lehrende durch europaweit integrierte und abgestimmte e-Infrastrukturen. Die in GN4-3 entwickelten und betriebenen Trust & Identity-Dienste sind hierbei essenziell für den Erfolg der integrierten e-Infrastrukturen.

Im Vergleich zu früheren GN4-Projekten wurden die Arbeitspakete dahingehend optimiert, das sie nun den kompletten Lebenszyklus eines Dienstes beinhalten

> Arbeitspakete beinhalten nun den kompletten Lebenszyklus eines Dienstes

– von der Konzeption über eine Versuchs- und Pilotphase bis hin zur Bereitstellung des Dienstes für die Forschungsnetze. Auf diese Weise wird auf ein besser vereinheitlichtes und kompatibles Diensteportfolio hingearbeitet und die Sicherheit und Interoperabilität der Dienste unterstützt. Innovationen werden in einem Inkubatorumfeld erprobt und für die Weiterentwicklung in größerem Maßstab ausgewählt.

Die Beteiligung des DFN-Vereins

Der DFN-Verein und seine Partner sind in fast allen Arbeitspaketen der beiden Projekte aktiv, insbesondere aber in den Bereichen Trust & Identity (AAI), Cybersecurity und Testbed-Entwicklung (GTS). Im Bereich Cybersecurity wird unter der Federführung des DFN-Vereins an der Bereitstellung eines Netzwerk-Monitoring-Systems (NeMo) zur Erkennung, Analyse und Abwehr von Netzwerkattacken für GÉANT gearbeitet. NeMo steht als Pilotprojekt kurz davor, von den GÉANT-Partnern erprobt zu werden und wird derzeit in das GÉANT-Netzwerk integriert.

DIE GN4-PROJEKTE:

Zur langfristigen Unterstützung aus dem Rahmenprogramm der Europäischen Union für Forschung und Innovation (Horizon 2020) hat die Europäische Kommission in 2015 einen Partnerschaftsrahmenvertrag mit GÉANT geschlossen (GÉANT-2020 Framework Partnership Agreement). Als dritte und letzte Phase unter dem Partnerschaftsrahmenvertrag erhalten die Projekte GN4-3 (Fördernummer 856726) und GN4-3N (Fördernummer 856728) insgesamt Mittel in Höhe von 128 Millionen Euro.

Nachgefragt bei Jule Ziegler, Leibniz-Rechenzentrum (LRZ), IT Security/Service Management. Als 3rd Party wird das LRZ über den DFN-Verein mit Projektmitteln in GN4-3 gefördert.

Jule Ziegler, LRZ, Foto: Alessandro Podo

Was ist aus deiner Sicht der größte Wert des Projekts?
Das ist die einzigartige Kollaboration im Projekt, nicht nur mit europäischen NRENs, sondern auch auf internationaler Ebene. Wertvoll sind außerdem die Diskussionen über forschungsrelevante Themen zur ständigen Verbesserung unserer Dienste sowie der Einbezug agiler Methoden, um auf verschiedenste Einflussfaktoren schnell reagieren zu können.

Wie erlebst du die Rolle des DFN-Vereins als Bindeglied zwischen Einrichtungen in Deutschland, dem Projekt (3rd Party) und der NREN-Community?
Im Projekt bin ich momentan im Trust & Identity-Bereich tätig. Bemerkenswert finde ich, dass der DFN hier seit Jahren stark vertreten ist, weil auch einige seiner teilnehmenden Einrichtungen als 3rd Partys aktiv im Projekt mitarbeiten. Das gibt es nicht überall. Es hat aber den Vorteil, dass die Bedürfnisse und Interessen des gesamten deutschen Forschungsnetzes in das Projekt und die Community einfließen können.

Welcher Mehrwert entsteht dadurch für die Hochschulen und Forschungseinrichtungen in Deutschland?
Dazu zählt beispielsweise der vereinfachte Zugriff auf föderationsübergreifende Dienste (eduGAIN) oder aber auch das gemeinsame Verständnis für Prozesse wie das Security Incident Handling. Nicht zu vergessen ist natürlich eduroam, was vermutlich jedem bekannt ist.

Im Trust & Identity-Arbeitspaket entwickelt sich der sogenannte Incubator Task besonders dynamisch. Hier geht es um die Erprobung von Technologien und die prototypische Entwicklung neuer Tools im Rahmen von jeweils sechsmonatigen Zyklen. Die aktuelle zweite Iteration des Inkubators mit sieben zum Teil auch für die DFN-AAI relevanten Projekten wird zum Jahresende abgeschlossen werden. Für den dritten Zyklus werden derzeit Projektvorschläge aus der Community gesammelt.

Der Netzdienst GÉANT Testbed Service (GTS) stellt ein virtuelles Netzwerk als Testumgebung bereit, in dem neu entwickelte Dienste gefahrlos und ohne Auswirkungen auf das aktuell laufende Netzwerk getestet werden können.

Im Arbeitspaket „User/Stakeholder Engagement“ engagiert sich der DFN-Verein bei den Themen EOSC und Partner Relations, insbesondere im Hinblick auf die Entwicklung eines Cloud-Geschäftsmodells für Forschungsnetze. Der DFN-Verein trägt im Arbeitspaket Online Services dazu bei, NRENs und ihre Einrichtungen beim Einsatz von digitalen Diensten auf Cloud Basis zu unterstützen. Hier werden Beschaffungsverfahren für europaweite Cloud-Ausschreibungen unterstützt bzw. durchgeführt, Rahmenverträge abgeschlossen, aber auch Informationsmaterialien und relevante Erfahrungswerte aus der Community für Einrichtungen zusammengestellt und geteilt.

Ausblick

Die Projekte GN4-3 und GN4-3N verfolgen wegweisende Ansätze für Neuentwicklungen und liegen derzeit hervorragend im Plan. In den kommenden Jahren werden sie einen wichtigen Beitrag zur bedarfsgerechten und nachhaltigen Verfügbarkeit der europäischen Forschungsnetzinfrastruktur und der Dienste liefern. ◆

Auf gute Zusammenarbeit – DFN-Verein startet Collaboration Programme mit ASNET-AM

Wissen teilen und Erfahrungen weitergeben – das ist das Ziel strategischer Zusammenarbeit innerhalb der NREN-Community. Mit ihrer Beteiligung und Unterstützung des *Collaboration Programme* innerhalb des Projekts EaPConnect leisten der DFN-Verein und seine Partner einen wichtigen Beitrag dazu.

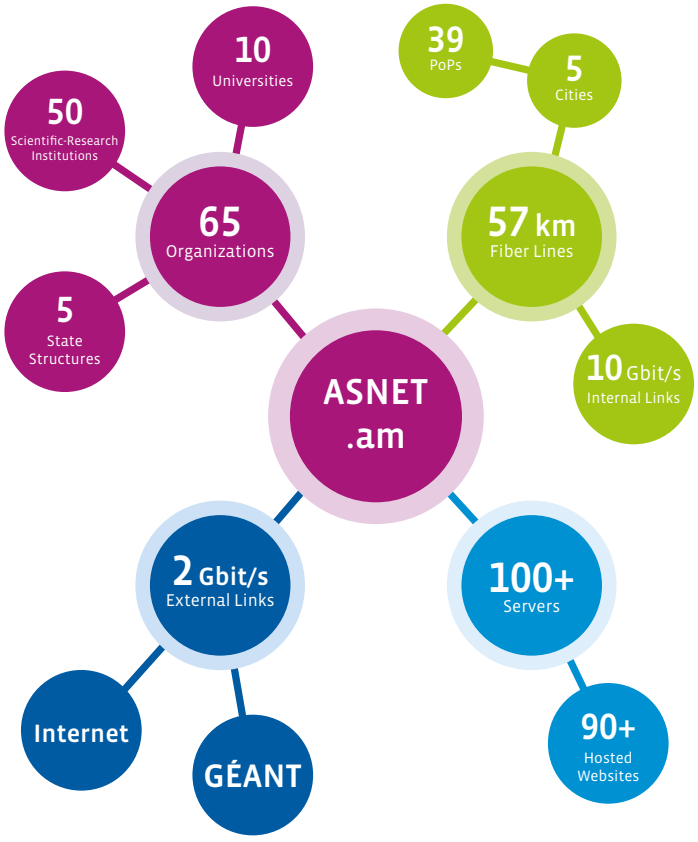
Text: **Leonie Schäfer** (DFN-Verein)

Berlin, Alexanderplatz: die Expertinnen und Experten beim Kick-off-Meeting auf dem Dach der DFN-Geschäftsstelle. *Foto: Nina Bark / DFN-Verein*

Mit einem Kick-off-Meeting in der Geschäftsstelle in Berlin startete der DFN-Verein im Januar dieses Jahres im Rahmen des EU-Projekts EaPConnect eine strategische Zusammenarbeit mit dem armenischen Nationalen Forschungsnetz (NREN) ASNET-AM (Academic Scientific Research Computer Network of Armenia). Ziel des Collaboration Programm ist es, eine Eins-zu-eins-Partnerschaft zwischen einem etablierten GÉANT-NREN und einem NREN der EaP-Region aufzubauen und den Wissensaustausch durch eine intensive Zusammenarbeit sowie persönliche Kontakte zu fördern.

Nach einer ersten Bestandsaufnahme der gemeinsamen Schwerpunkte Cybersecurity und AAI vereinbarten die Expertinnen und Experten beider NRENs aus den jeweiligen Bereichen Trust & Identity die weiteren Schritte der Zusammenarbeit. Ein wichtiges Ziel des armenischen Teams war es, ein Computer Emergency Response Team (CERT) für Armenien aufzubauen und akkreditieren zu lassen. Im AAI-Bereich lag der Schwerpunkt auf der eduroam-Adoption und der weiteren Verbreitung von eduGAIN.

ASNET-AM AUF EINEN BLICK



Mit etwa drei Millionen Einwohnern ist Armenien ein verhältnismäßig kleines Land im Kaukasus. Mit Georgien und Aserbaidschan als Nachbarn in der Region ist es Mitglied der Osteuropäischen Partnerschaft der EU (EaP). Obgleich landumschlossen und arm an Bodenschätzen, ist es bekannt für sein intellektuelles Kapital. Armenien ist ein innovationsorientiertes Land mit einer Reihe vielversprechender Start-ups im Hightech-Bereich. Durch die weltweite Diaspora der Armenier fließt viel Kapital zurück ins Land und begünstigt Start-ups und Kollaborationen mit Hightech-Firmen rund um den Globus. Die Bevölkerung ist weltoffen und der EU zugewandt, die Regierungsmannschaft ist jung und demokratisch orientiert – insgesamt also beste Startvoraussetzungen als Partnerland in Technologie und Forschung.

Nichtsdestotrotz hat auch Armenien mit den typischen Problemen der „Emerging Countries" zu kämpfen. Die IT-Infrastruktur des Landes bedarf – ebenso wie die Netzanbindung an das GÉANT-Backbone – der kontinuierlichen Optimierung. Dazu kommt, dass sich das Land geopolitisch als auch geologisch (Erdbeben) in einem Spannungsfeld befindet. Aus diesem Grund ist es wichtig, mithilfe einer strategischen Partnerschaft Land und Leuten eine Brücke zu bauen, die Anbindung an die Länder der EU zu stärken und die sogenannte digitale Kluft zu überwinden. Mit seiner Beteiligung und Unterstützung des *Collaboration Programme* innerhalb des Projekts EaPConnect sowie des im Juli gestarteten Folgeprojekts EaPConnect2 leistet der DFN-Verein dazu einen wichtigen Beitrag.

Erste Erfolge des *Collaboration Programme* konnten bereits Ende April mit der Zertifizierung des ASNET-AM-CERT verzeichnet werden. Inzwischen hat das Computer Emergency Response Team offiziell seinen seine Arbeit aufgenommen. Darüber hinaus erfolgt weiterhin eine kontinuierliche Betreuung vonseiten des DFN-Teams zu Fragen rund um eduroam, zudem steht der DFN-Verein bei der eduVPN-Implementation beratend zur Seite.

Kernstück des *Collaboration Programme* sind nicht nur der regelmäßige inhaltliche Austausch der Expertinnen und Experten per Videokonferenz, sondern auch persönliche Besuche im jeweiligen Partnerland zum Kennenlernen der Lage vor Ort. Aufgrund des Ausbruchs der COVID-19-Pandemie musste leider der Gegenbesuch des DFN-Teams in Armenien auf die zweite Hälfte des Jahres 2020 verschoben werden. In Planung ist außerdem ein Arbeitsbesuch eines ASNET-Experten für Cybersecurity in Berlin und in Hamburg beim DFN-CERT.

Im Rahmen von EaPConnect starteten zu Beginn des Jahres das ukrainische NREN URAN sowie das zypriotische NREN CYNET als Partner im *Collaboration Programme*. Der Schwerpunkt dieser Kooperation liegt auf dem Bereich Cybersecurity. In den Startlöchern stehen außerdem das aserbaidschanische NREN AzScienceNet und LITNET, das litauische NREN. Der Schwerpunkt dieser Kollaboration liegt im Bereich Trust & Identity und AAI. Das *Collaboration Programme* macht Schule und wird hoffentlich noch viele weitere erfolgreiche Partnerschaften zur Folge haben. ◆

Weitere Informationen zu ASNET-AM finden Sie hier:
https://asnet.am/?&lang=en

Informationen zum ASNET-AM-CERT finden Sie hier:
https://www.trusted-introducer.org/directory/teams/asnet-cert.html

ULAKBIM – The Academic Network between Anatolia and Europe

Starke Partner weltweit

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

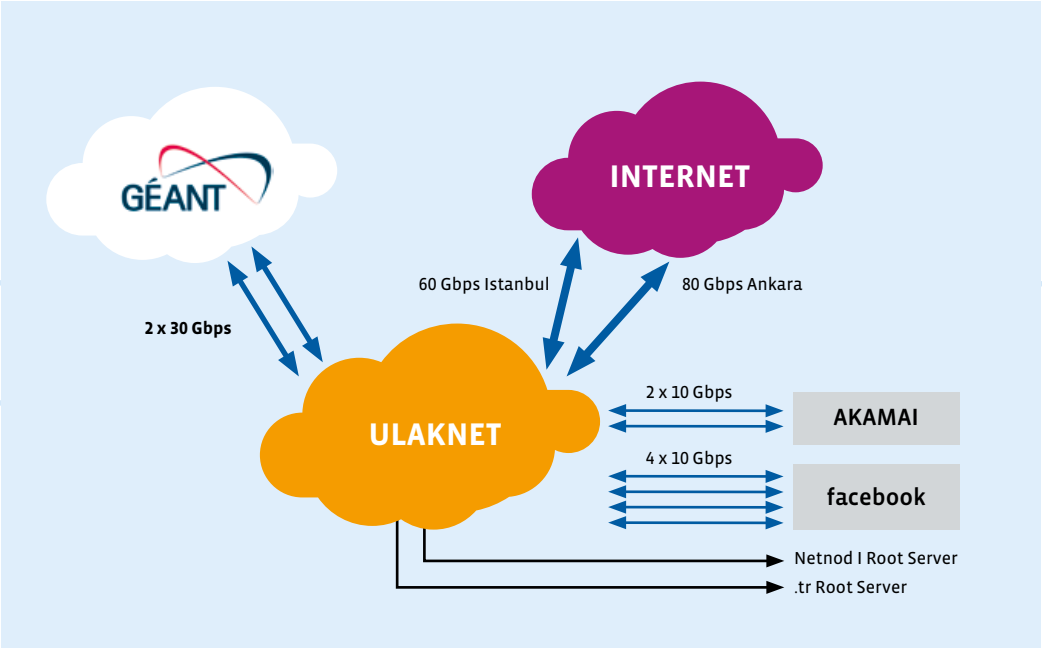
With 219 connected institutions, 150.000 academicians, more than 4.000.000 students and a considerable financial effort (21 Million Euro budget per year) the Turkish Academic Network and Information Centre (ULAKBIM) is an important player in the European NREN community and a strong partner of GÉANT Association for 18 years. It aims at operating the national academic network (ULAKNET) and providing IT facilities such as computer networks, high performance compute and storage solutions, data and cloud services, and library and information services, to meet the needs of the research community in Turkey and to increase the efficiency and productivity of their users.

Text: **Burcu Ortakaya** (TÜBİTAK ULAKBİM, Turkish Academic Network and Information Center)

In 1996 Turkish Academic Network and Information Centre (ULAKBIM)[1] was founded as an R&D Institute of TUBITAK (The Scientific and Technological Research Council of Turkey)[2]. ULAKBIM is responsible to provide and operate the national academic network (ULAKNET) and, computing and data infrastructure. Additionally, nationwide document supply services have been offered to the research and academia since the establishment of ULAKBIM. The open science and open access policies have been adopted both at current services and long-term planning.

Network Infrastructure:

ULAKNET backbone infrastructure is established among three regional Point of Presences (PoPs) located in Ankara, Istanbul, Izmir, and two metropolitan PoPs located in Konya and Eskisehir. The capacity of the backbone links



ULAKNET Connections

varies from 5 to 50 Gbps. Global Internet connection is provided through a local Internet Service Provider (ISP) over two links with a total capacity of 140 Gbps. Additionally, ULAKNET is hosting CDN cache servers (Akamai, Facebook), Netnod I Root DNS server, and .tr DNS servers. ULAKNET provides network services to about 150.000 academicians and more than 4.000.000 higher education students. Currently, 1147 units of 219 institutions are connected to the network.

ULAKNET is a part of GÉANT network since 2002. Present GÉANT connection is provided through a 30 Gbps main link over Budapest and a 30 Gbps backup link over Frankfurt.

Services:

TR eduroam Federation is a member of the European Confederation since 2007. The service is active in 127 institutions. The coverage area of eduroam includes about 1000 locations and more than 21.000 network access points. ULAKNET has TI accredited Computer Security Incident Response Team named ULAK-CSIRT since 2007. Turkish Identity Federation YETKİM is a member of eduGAIN since 2013.

ULAKNET-2: National Lightpath Project

After the revision of the Establishment Law in 2005, ULAKBIM obtained a right to build infrastructure for electronic communication between research and educational institutions. Then studies aiming to renovate the network and reduce connectivity cost by obtaining fiber infrastructure started. These studies have been strongly supported by the

TÜBİTAK ULAKBİM

Ministry of Development through the long-term national project ULAKNET-2

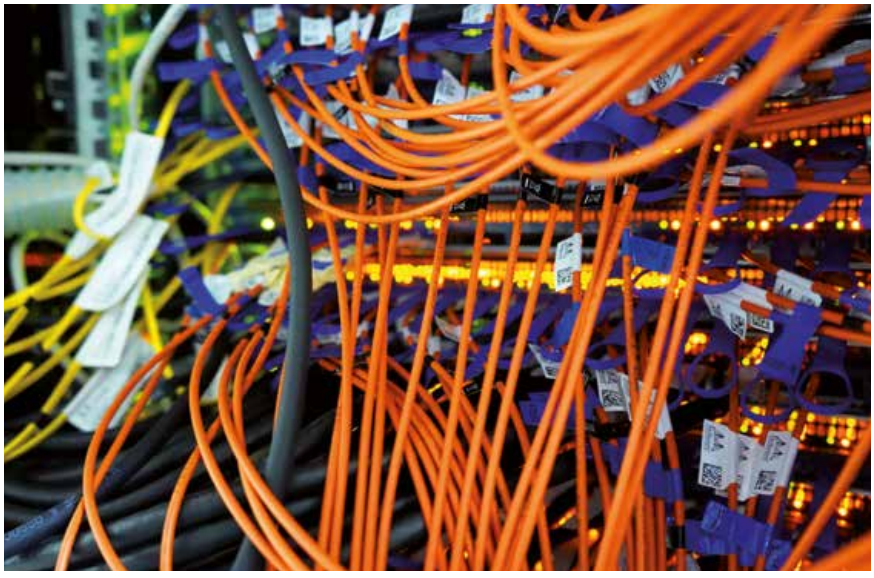


Foto: ULAKBIM

COVID-19 ACTIONS:

ULAK BULUT

On 13th March 2020, The Turkish Council of Higher Education announced that all universities will be closed on 16th March 2020, to avert the spread of COVID-19 virus. After this decision, the community was suddenly directed into an unplanned, distance education process for which many of the universities were not ready yet. This was a challenging process. The main problem was to provide a scaled online education system that can serve a high number of students. Many of the universities have started distance education after a short but busy preparation period as of March. ULAKNET, as NREN, worked hard to support universities and research institutions throughout this difficult process. From the first moment of the COVID-19 pandemic, all measures have been taken to ensure that services are not interrupted.

In this context, new 100Gbps and 10Gbps line cards have been put into service on the main backbone routers in order to meet capacity demands quickly. In one month, the link capacities of more than 80 units have increased by 60%. Additionally, urgent expansion and improvement work has been carried out for the Distance Education Infrastructure, which we serve to some universities and is running over the ULAKNET Cloud infrastructure. Besides, to meet the rapidly increasing video conferencing needs, a new pilot video conference service was commissioned by the Cloud team and offered for use of universities. The country-level web portal for COVID-19[3] was opened by TUBITAK and has been hosted by ULAK Cloud. This portal has been providing the needed support and collaboration to researchers.

As a result of all these efforts, although campuses are physically closed, the connection of students and academics has continued thanks to online education. We hope that this period will end soon and all universities can return to their in-class teaching activities.

which started in 2009. Till now more than 220 km fiber infrastructure has been built or leased and 38 units are connected to this fiber infrastructure.

Computing and Data:

High Performance Computing interest of ULAKBIM started in 2003 with a cluster of 128 desktop PCs funded as an institutional project, TR-Grid. This initial installation allowed researchers to use parallel computational execution capabilities, additionally, this starting point created significant awareness about grid initiatives, infrastructures, and EC funded project that can help to close the digital divide. The infrastructure has been expanded regularly through the national strategic and development budget. EC level projects participation also has provided support to infrastructure at the level of collaboration, policy, and new services as well as technologies. As of 2010, the infrastructure and initiative have renovated as TRUBA (Turkish National Science e-Infrastructure).

TRUBA: Turkish National Science e-Infrastructure

TRUBA[4] is a national center providing high performance, data-intensive and cloud computing infrastructure as well as scientific data warehouses. Currently, the infrastructure has 20K cores, 180 GPUs, and 12 PB distributed parallel file systems. The usage and community demands are continuously increasing and vary in different disciplines from computational sciences to agriculture and social sciences to more than 140 universities and research institutions.

TRUBA Türk Ulusal Bilim e-Altyapısı

Until today, TRUBA has evolved from a small cluster to national infrastructure, and has a collaborative background through participated European Commission project series; EUMedGrid, SEE-Grid, SEERA, EGEE, and EGI's. At present, EOSC partnership and EuroHPC[5] to pre-exascale Spanish consortium are closely followed to cover effectively the new way of making science. Regarding this new era – open science – TRUBA is aspiring to transform from a computing and data warehousing to a research support

RECOURCE	USAGE	VISION
→ 20k CPU cores & 180 GPUs → 12 PB storage → 2743 users	→ 15 thematic groups/VOs → 80 research projects → 155M CPUh/year	→ Collaboration to EC Projects → Sustainability & renovation – TRUBA 2023 Project

TRUBA Metrics (by March 2020)

center with FAIR data services, data policies for research. To realize these aspirations, TRUBA is moving to a new data center and modernizing its infrastructure to provide higher performance and more effective management. At the end of the day, the team behind the TRUBA infrastructure is excited as the first day and looking forward to accelerating research even further for every researcher in Turkey.

Open Science Perspective:

The Scientific and Technological Research Council of Turkey (TUBITAK) has prepared and adopted Open Science Policy as of March 2019[6]. This policy covers management, storage, archiving, curation, and digital preservation of the publications and the research data originated from the projects which have been carried out or supported by TUBITAK. As the research council of Turkey TUBITAK, provides research support mechanism varies from scholarships, awards, incentives to granted funds for researchers and research projects. The researcher, as a beneficiary, agrees to comply with the TUBITAK Open Science Policy and declares compliance with the policy in the project final report. In line with the global developments in the field of Open Science, publications and research data, produced by funded TUBITAK Projects and Research Institutions, has to be identified to increase re-usability.

ULAKBIM has taken the responsibility to support open science nationwide and carry on EOSC Governance Board membership to follow up open science at the European level. In addition to management of open science policy, TUBITAK ULAKBIM has been providing and developing the open platform to identify, share and re-use of publications and research data through the repository Aperta[7] and the search engine Harman[8]. Aperta is planned to be the main research data management platform nationwide. The "Harman" is the first and only OAI harvester in Turkey. Currently, there are 104 institutions and more than 1M records in the archive.

Foto: ULAKBIM

REFERENCES:

1. https://ulakbim.tubitak.gov.tr/en
2. https://www.tubitak.gov.tr/en
3. https://covid19.tubitak.gov.tr/
4. https://www.truba.gov.tr/
5. http://eurohpc.eu/
6. https://ulakbim.tubitak.gov.tr/en/haber/tubitak-open-science-policy-accepted
7. https://aperta.ulakbim.gov.tr/
8. https://arsiv.ulakbim.gov.tr/index

Umweltschutz und Nachhaltigkeit – Rechenzentren in der Verantwortung

Umweltverträgliche Maßnahmen und Informationstechnik (IT) sind teuer, so lautet die landläufige Meinung. Insbesondere für Rechenzentren und Informations- und Kommunikationstechnik stimmt das nicht. Ein ressourcenschonendes und klimaschutzfreundliches Rechenzentrum ist kostensparend. Es kommt auf die passenden Maßnahmen an und die richtigen Kenngrößen helfen, diese zu identifizieren. Gemeinsam mit verschiedenen Forschungseinrichtungen hat das Umweltbundesamt (UBA) das Kennzahlensystem Key Performance Indicators for Data Center Efficiency (KPI4DCE) entwickelt, mit dem die Energie- und Ressourceneffizienz eines Rechenzentrums erstmals ganzheitlich bewertet werden kann.

Text: **Marina Köhn**
(Umweltbundesamt, UBA, Beratungsstelle nachhaltige Informations- und Kommunikationstechnik, Green-IT)

Illustration: alexdndz/iStock

RELATIVE VERTEILUNG DER RESSOURCENINANSPRUCHNAHME AUF DIE RZ-TEILSYSTEME

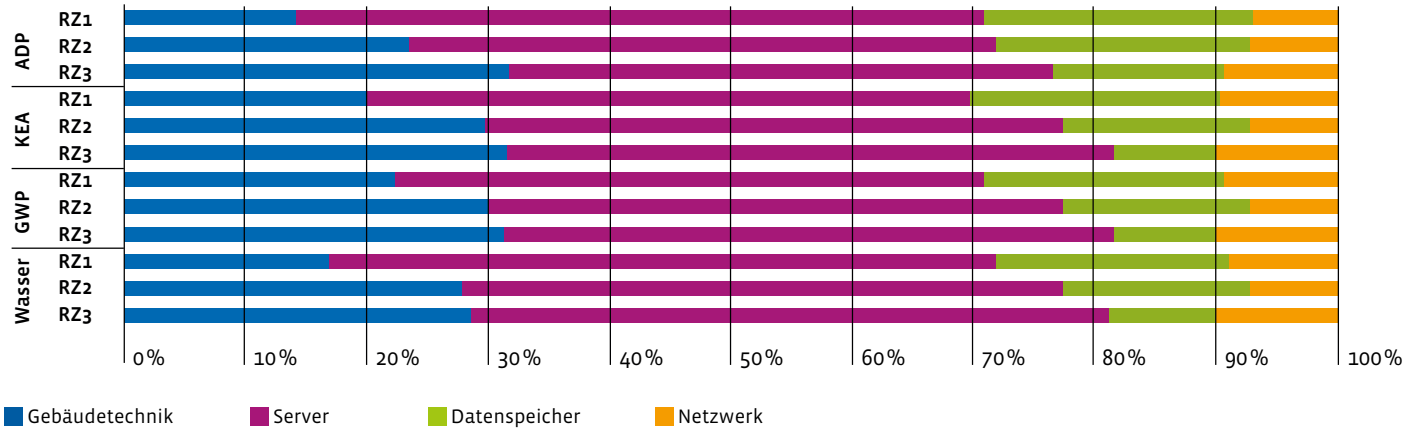


Abbildung 1: Ergebnisse der Kennzahlen KPI4DCE am Beispiel von drei Rechenzentren aus der Praxis

Rechenzentren sind Teil der digitalen Infrastruktur, wenn nicht sogar das Herz der Digitalisierung. Für unser modernes und vernetztes Leben spielen sie eine zentrale Rolle. Digitale Prozesse und vernetzte Technik werden immer stärker nachgefragt. Jeder, der in der Pandemie im Homeoffice weiterarbeiten konnte, weiß, wie essenziell Dienstleistungen der Rechenzentren sind.

Mit den digitalen Technologien ist die Hoffnung auf neue Lösungen für den Schutz des Klimas und der Umwelt verknüpft. Ob die Nettobilanz positiv für Klima- und Umweltschutz ausfällt, hängt nicht zuletzt davon ab, ob es gelingt, den Energieverbrauch der digitalen Infrastruktur zu senken und den Rohstoffbedarf auf ein Minimum zu reduzieren.

Bei einer Umfrage[1] der Firma Colt Data Centre Services unter 500 europäischen Betreibern von Rechenzentren gaben 63 Prozent an, dass ihnen Fehler bei der Kapazitätsplanung unterlaufen sind und sie mit höherer Leistungskapazität gerechnet haben. Das bedeutet, dass Fläche, abzuführende Wärme und Strombedarf für die entsprechende technische Ausstattung überdimensioniert sind und somit ein effizienter Betrieb kaum möglich ist. Eine in diesem Jahr veröffentlichte Studie[2] des amerikanischen Uptime Institute deckt weitere Defizite in den europäischen Rechenzentren auf. Sie führt unter anderem an, dass kaum strategische Entscheidungen für mehr Energieeffizienz getroffen werden und dass die Server überwiegend schlecht ausgelastet sind. Zusammengefasst könnte man meinen, dass das Energiesparen noch nicht in der DNA des Rechenzentrumsbetriebs verankert ist. Wie ist das möglich, wo doch bereits seit Jahren die Themen Nachhaltigkeit und Energieeffizienz diskutiert werden und junge Menschen weltweit jeden Freitag für mehr Klimaschutz auf die Straßen gehen? Die Antwort ist vielschichtig. An dieser Stelle werden einige wesentliche Aspekte beleuchtet.

Kennzahl ist nicht gleich Kennzahl

Um Energieeffizienzpotenziale zu erschließen und die Wirkung von Maßnahmen zu erkennen, werden Kennzahlen herangezogen. Die Power Usage Effectiveness (PUE)[3] ist die Kennzahl, die am häufigsten verwendet wird. Sie ist der Quotient aus dem jährlichen Gesamtenergiebedarf des Rechenzentrums und dem Energiebedarf der IT. Die PUE ist dann besonders gut, nämlich niedrig, wenn der Energiebedarf der Infrastrukturtechnik wie beispielsweise Klimatechnik, unterbrechungsfreie Stromversorgung (USV) usw. gering ist.

Die PUE hat einige Nachteile und Unsicherheiten. Ein Beispiel: Wenn inaktive Server abgeschaltet werden, braucht das Rechenzentrum de facto weniger Energie – doch die PUE steigt, verschlechtert sich also.

Der wesentliche Aspekt, warum die PUE nicht als Indikator für die Beurteilung der Energieeffizienz des Rechenzentrums geeignet ist, besteht darin, dass sie keine Aussagen über die Energieeffizienz der Kernaufgaben des Rechenzentrums treffen kann, nämlich die Rechen-, Speicher- und Übertragungsleistung. Die daher einseitige Orientierung auf die Energieeffizienzgewinne in der Infrastruktur der Rechenzentren führt dazu, dass die größten Energieverbräuche, die der IT-Komponenten, zum größten Teil außer Acht gelassen werden (vgl. Abbildung 1). Nicht die Kennzahl PUE ist das Problem, sondern sie als Maß zur Beurteilung der Energieeffizienz eines Rechenzentrums zu verwenden.

1 Das Whitepaper der Untersuchung: www.colt.net/resources/colt-european-organisations-feeling-the-four-forces-of-data-centre-disruption/

2 Uptime 2020: Beyond PUE: Tackling IT's wasted terawatts: uptimeinstitute.com/publications/asset/beyond-pue-tackling-its-wasted-terawatts

3 Die korrekte Interpretation des PUE (Power Usage Effectiveness) wird in der EN 50600-4-2 beschrieben

Mit den richtigen Kennzahlen die Potenziale erkennen

Das Umweltbundesamt hat gemeinsam mit verschiedenen Forschungseinrichtungen das Kennzahlensystem Key Performance Indicators for Data Center Efficiency (KPI4DCE)[4] entwickelt, mit dem die Energie- und Ressourceneffizienz eines Rechenzentrums erstmals ganzheitlich und richtungssicher bewertet werden kann. KPI4DCE umfasst den gesamten Lebenszyklus der Informationstechnik im Rechenzentrum und der technischen Versorgungsstruktur. Darüber hinaus wird die Leistung des Rechenzentrums, wie die Rechen-, Speicher- und Übertragungsleistung, ins Verhältnis zum Energie- und Rohstoffaufwand gesetzt.

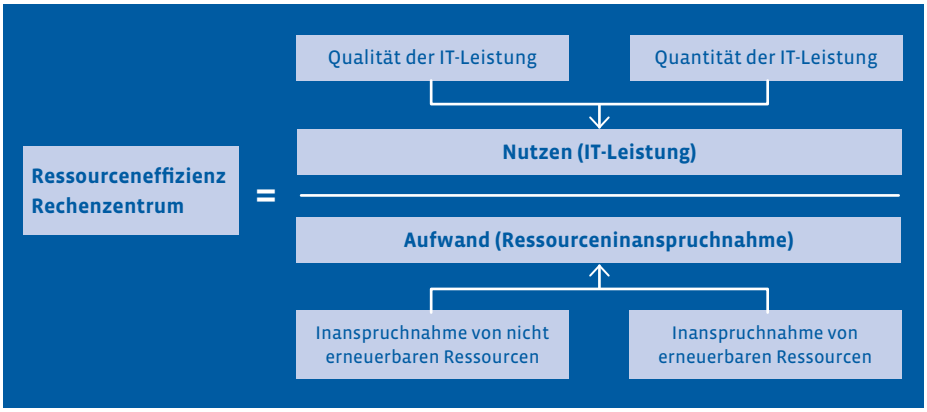
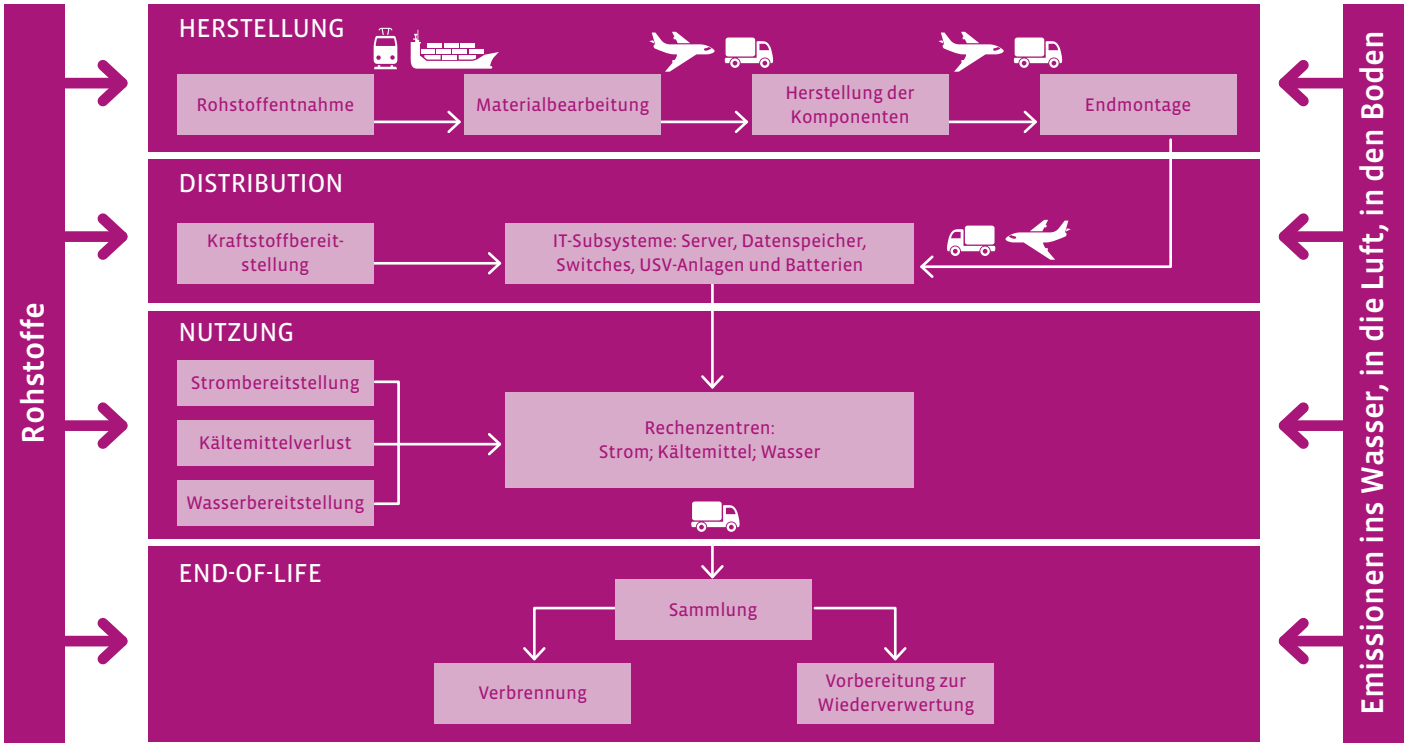


Abbildung 2: Die ganzheitliche Bewertung der Ressourceneffizienz eines Rechenzentrums erfordert die Berücksichtigung aller Teilbereiche.

Die Spezifikation der IT-Leistungsindikatoren stützt sich nicht zuletzt auf Benchmark-Daten der Standard Performance Evaluation Corporation (SPEC)[5] und weitere Leistungsindikatoren für Speichersysteme und Netzwerk. Diese Leistungsindikatoren werden ins Verhältnis zur Auslastung der Systeme gesetzt.

Für die Bewertung der Umweltaspekte stehen Wirkungsindikatoren aus der Ökobilanzierung zu Verfügung. Die Daten für die Berechnung der Wirkungsindikatoren kommen aus den Lebenszyklus-Datenbanken ProBas[6] und ecoinvent[7].

Abbildung 3: Methode der Ökobilanz für die Berechnung der verschiedenen Ressourcen und deren Inanspruchnahme über den gesamten Lebenszyklus



4 KPI4DCE UBA 2018: www.umweltbundesamt.de/en/publikationen/kennzahlen-indikatoren-fuer-die-beurteilung-der
5 https://www.spec.org/
6 Prozessorientierte Basisdaten für Umweltmanagementsysteme: www.probas.umweltbundesamt.de
7 Ecoinvent: https://www.ecoinvent.org/

Um die jeweiligen Ergebnisse zusammenzuführen, wurde das Berechnungswerkzeug KPI4DCE-Tool (Abbildung 3) entwickelt, das die Kennzahlen aus standardisierten Eingaben der Rechenzentrumsbetreiber automatisch berechnet.

und für den Entscheider nachvollziehbar dargestellt.

Auch für die Infrastrukturtechnik der Rechenzentren kann beispielsweise der Energieverbrauch für die Kühlung durch Wasser

Abbildung 4: Auszug aus dem Berechnungswerkzeug KPI4DCE

Mit dem KPI4DCE ist insbesondere der Trade-off zwischen Energie- und Materialeffizienz sichtbar. Ein möglichst kurzer Erneuerungszyklus von Servern ist von Vorteil für die Energieeffizienz im Betrieb, dem steht allerdings der energetische Aufwand bei der Herstellung und Entsorgung der Informationstechnik gegenüber. Vor allem aber lassen sich viele Rohstoffe elektronischer Komponenten noch nicht wirtschaftlich recyceln. Teilweise stehen noch keine Recyclingverfahren zur Verfügung und diese Rohstoffe sind somit nach der Nutzungsphase verloren. Unter dem Aspekt der Materialeffizienz ist daher eine möglichst lange Nutzung der Geräte anzustreben. Anhand der unterschiedlichen Wirkungsindikatoren des KPI4DCE wird insbesondere dieser Aspekt transparent

substituiert werden (Kühlturm vs. Trockenkühler). Auch der Einsatz bzw. der Austritt von klimaschädlichen Kältemitteln beeinflusst die ökologische Bilanz.

Expertenwissen gebündelt im Blauen Engel

Mit den richtigen Kennzahlen aus dem KPI4DCE kann die Energie- und Ressourceneffizienz des Rechenzentrums verlässlich ermittelt werden. Der nächste Schritt ist die Umsetzung der richtigen Maßnahmen. Bei deren Auswahl können die Kriterien des Umweltzeichens Blauer Engel helfen. Die Anforderungen des Blauen Engels an die Produkte und die Rechenzentren wurden mit Experten*innen aus der IT-Wirtschaft, den Verbänden und der Wissenschaft diskutiert und einvernehmlich festgelegt.

Der *Blaue Engel für den Energieeffizienten Rechenzentrumbetrieb* (DE-UZ 161)[8] zeichnet bereits seit 2012 besonders energieeffiziente Rechenzentren mit dem Umweltzeichen Blauer Engel aus. Damit wird ein interdisziplinärer Ansatz verfolgt, der alle Bereiche eines Rechenzentrums und seiner Infrastruktur umfasst. Dieser systembezogene Ansatz beinhaltet nicht nur die Energieeffizienz einzelner Komponenten, sondern das umweltbewusste Management des Rechenzentrums insgesamt. Unter den Ausgezeichneten befanden sich Rechenzentren aus der Wirtschaft, der Bundes- und Landesverwaltung und der Wissenschaft. Das Hauptziel des Umweltzeichens ist sehr einfach zusammengefasst: Rechenzentren sollen mit möglichst wenig Hardware – also möglichst wenig Servern und Speichertechnik – eine hohe Rechen- und Speicherleistung bei energieeffizienter Infrastruktur bereitstellen.

Darüber hinaus erwartet der Blaue Engel eine saubere Klimatisierung mit natürlichen Kältemitteln bzw. ohne den Einsatz von klimaschädlichen Kältemitteln auf Basis fluorierter Treibhausgase. Vor dem Hintergrund der EU-F-Gas-Verordnung[9] ist die Verfügbarkeit der klimaschädlichen Kältemittel deutlich eingeschränkt und wird in den nächsten Jahren weiter abnehmen. Wenn diese Kältemittel, die typischerweise auch zur Klimatisierung in den Rechenzentren eingesetzt werden, nicht mehr in dem Umfang verfügbar sind, dann hat das entsprechende Konsequenzen für die Ausfallsicherheit und damit Verfügbarkeit von Rechenzentren. Es ist daher aus Gründen der geforderten Hochverfügbarkeit von Rechenzentren dringend abzuraten, diese Art der Klimatisierungstechnik bei Neuplanung von Kälteanlagen zu beschaffen. Das Thema ist in einem Fachartikel des UBA ausführlich beschrieben, insbesondere die zur Verfügung stehenden alternativen Klimatisierungstechniken[10].

8 Blauer Engel Energieeffizienter Rechenzentrumsbetrieb: www.blauer-engel.de/de/produktwelt/elektrogeraete/rechenzentren

9 Fachartikel des UBA zur EU-F-Gas Verordnung (Verordnung (EU) Nr. 517/2014): https://www.umweltbundesamt.de/themen/klima-energie/fluorierte-treibhausgase-fckw/rechtliche-regelungen/eu-verordnung-ueber-fluorierte-treibhausgase?sprungmarke=VO5172014#VO5172014

10 Fachartikel des UBA Rechenzentrumsklimatisierung: https://www.umweltbundesamt.de/themen/klima-energie/fluorierte-treibhausgase-fckw/anwendungsbereiche-emissionsminderung/rechenzentrumsklimatisierung

Der Blaue Engel Klimaschonendes Co-Location-Rechenzentrum (DE-UZ-214)[11] ist für Betreiber von Co-Location-Rechenzentrumsbetreiber relevant. Die Bedeutung der Co-Location-Rechenzentren hat in den vergangenen Jahren deutlich zugenommen. Ihr Anteil an der Gesamtrechenzentrumsfläche lag 2017 bereits bei 32 Prozent. Vor diesem Hintergrund haben wir in diesem Jahr ein Umweltzeichen für das *Klimaschonende Co-Location-Rechenzentrum* eingeführt. Damit können solche Co-Location-Rechenzentren ausgezeichnet werden, deren Gebäudetechnik besonders energieeffizient betrieben wird und für die eine langfristige Strategie zur Erhöhung der Energie- und Ressourceneffizienz für die RZ-Infrastruktur vorliegt. Ebenso solche, die durch garantierte Mindeststandards und transparente Berichterstattung die Voraussetzung für Co-Location-Kunden schaffen, ihre Informationstechnik umweltverträglich zu betreiben.

Der Blaue Engel Server und Datenspeicherprodukte (DE-ZU-213)[12]*:* Der Bedarf an zentraler Verarbeitung und Speicherung von Daten steigt seit Jahren kontinuierlich und somit auch die Nachfrage nach Server- und Datenspeicherprodukten. Bei diesen Produkten hat die Nutzungsphase den größten Anteil an den Treibhausgasemissionen (CO_2) über den gesamten Lebenszyklus, bei Servern circa 80 Prozent und bei Datenspeicherprodukten etwa 90 Prozent des CO_2. Für die umfassende Bewertung der Umweltbelastungen ist es aber wichtig, diese sämtlich im Blick zu haben – auch die, die bei der Herstellung und Entsorgung entstehen. Dazu zählt vor allem der Rohstoffverbrauch. Eine lange Nutzung der Server und Speicherprodukte wirkt sich auf die Materialeffizienz somit positiv aus. Vor diesem Hintergrund ist das Ziel des Blauen Engels, den Energieverbrauch der Server und Datenspeicherprodukte insgesamt zu reduzieren und die Ressourceneffizienz zu steigern. Konkret bedeutet es, dass der Blaue Engel ambitionierte Mindestanforderungen an die Energieeffizienz von Servern, Datenspeicherprodukten und Netzteilen stellt und Vorgaben zur Materialeffizienz einfordert.

LEITFADEN FÜR DIE BESCHAFFUNG

Die Kriterien des Blauen Engels für Rechenzentren sind auch als Beschaffungsempfehlungen in Form eines Leitfadens für Beschaffer*innen aufbereitet worden. Mit diesem Leitfaden werden die öffentlichen Beschaffer*innen dabei unterstützt, umweltverträgliche Rechenzentrums-Hardware, Rechenzentrums-Infrastruktur sowie Rechenzentrums-Dienstleistungen auszuschreiben und zu beschaffen.

Bei weiteren Fragen wenden Sie sich an Marina Köhn, Beratungsstelle nachhaltige Informations- und Kommunikationstechnik (Green-IT) des Umweltbundesamt.

Leitfaden zur umweltfreundlichen öffentlichen Beschaffung – Produkte und Dienstleistungen in Rechenzentrum und Serverräumen, UBA 2015:

https://www.umweltbundesamt.de/sites/default/files/medien/376/publikationen/leitfaden_zur_umweltfreundlichen_oeffentlichen_beschaffung_-_produkte_und_dienstleistungen_fuer_rechenzentren_und_serverraeume.pdf

Übrigens …

Das größte Potenzial Energie einzusparen und wertvolle Rohstoffe zu schonen, liegt in der Art und Weise wie Server und Storage im Rechenzentrum betrieben werden. Zwischen 60 und 70 Prozent des Gesamtenergiebedarfs wird durch die Informationstechnik im Rechenzentrum verursacht. Das Effizienzpotenzial ist groß. Sowohl unsere Untersuchungen als auch zahlreiche internationale Studien kommen alle zum gleichen Ergebnis: Die Auslastung der Server muss dringend verbessert werden. Server, die keine Leistung verrichten, müssen heruntergefahren werden. Die Kapazitätsplanung muss besser an realen Bedarfen ausgerichtet werden um Überkapazitäten zu vermeiden, die einen effizienten Betrieb so gut wie unmöglich machen.

Zurück zur Eingangsthese des Artikels: Ein ressourcenschonendes und klimaschutzfreundliches Rechenzentrum ist deshalb gleichzeitig kostensparend, weil es bei gleicher Leistung weniger Server und Speichergeräte benötigt, die Klimatechnik und USV am tatsächlichen Bedarf ausgerichtet und modular an den tatsächlichen Bedarf anpassbar sind, die Abwärmenutzung bereits bei der Planung berücksichtigt wurde und der Ökostrom nicht wirklich viel teurer ist als konventioneller Strom. Also: Worauf warten wir noch? ◆

11 Vergabeunterlagen zum Umweltzeichen „Energieeffizienter Rechenzentrumsbetrieb“: www.blauer-engel.de/de/produktwelt/elektrogeraete/klimaschonende-colocation-rechenzentren

12 Vergabeunterlagen zum Umweltzeichen „Server und Datenspeicherprodukte“: www.blauer-engel.de/de/produktwelt/elektrogeraete/server-und-datenspeicherprodukte

Internet Testbed der nächsten Generation – SCIONLab jetzt mit DFN-GVS

SCION (Scalability, Control and Isolation on Next-Generation-Networks) ist eine neue, sichere Internetarchitektur, die eine hohe Verfügbarkeit selbst im Falle von möglichen Angriffen verspricht. Der Ansatz gewährleistet Transparenz über die Wahl der Pfade und erlaubt Multipath-Routing über mehrere Netzwerkdomänen hinweg. Dank dem globalen Forschungsnetzwerk SCIONLab werden innovative Forschungsexperimente an pfadbewussten Netzen und Inter-Domain-Multipath-Kommunikation nun erstmals in einem globalen Testbed ermöglicht. Auch der DFN-Verein betreibt im Rahmen der DFN-GVS-Testbed-Infrastruktur (General-Virtualization-Service) einen SCIONLab-Knoten und ermöglicht es damit seinen Benutzern, Hosts auf der DFN-GVS-Plattform direkt mit dem globalen SCIONLab-Netzwerk zu verbinden.

Text: **David Hausheer** (OVGU Magdeburg und ETH Zürich)

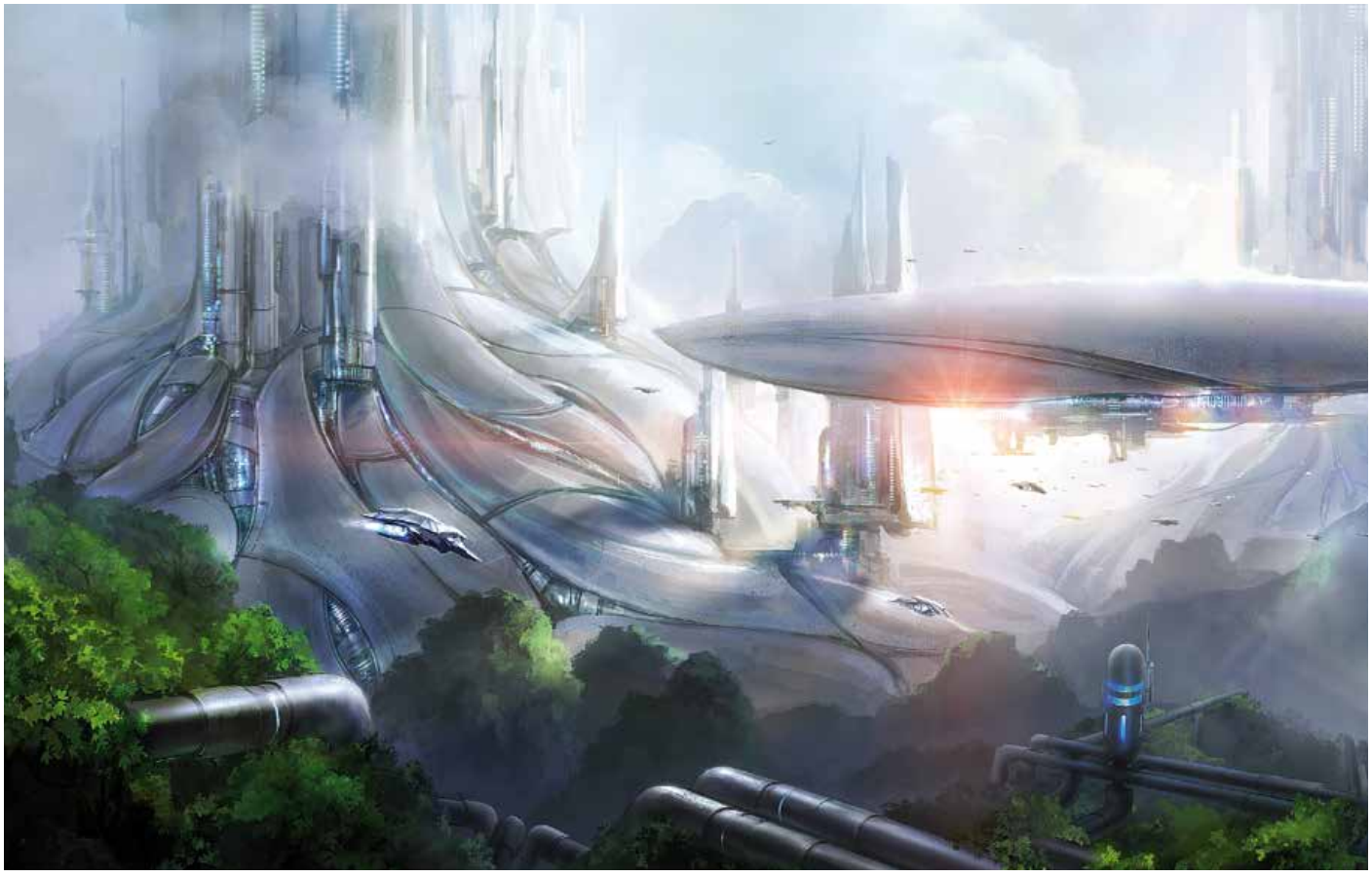


Illustration: liuzishan / Adobe Stock

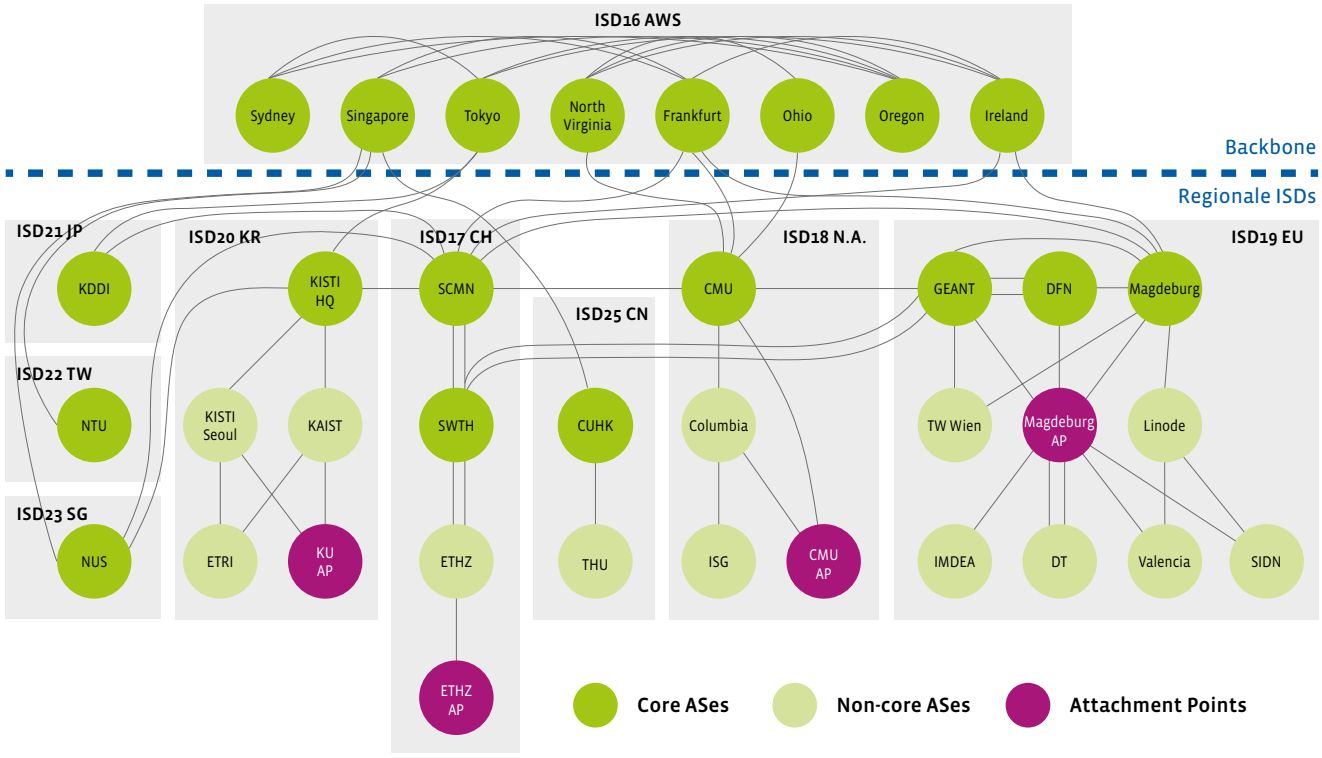


Abbildung 1: Die globale SCIONLab-Topologie

Netzwerk-Testbeds sind entscheidend für den wissenschaftlichen Fortschritt der Netzwerkforschung, durch sie ist es möglich, innovative Konzepte im Netzwerkbereich experimentell zu untersuchen. Die meisten verfügbaren Testbeds fokussieren allerdings hauptsächlich Experimente mit dem heutigen Internet. Mit dem Aufkommen neuer Netzwerkparadigmen und künftiger Internetarchitekturen bietet sich die Gelegenheit, die nächste Welle von Netzwerkanwendungen auszulösen. Insbesondere pfadbewusste Netze, Multipath-Kommunikation und netzwerkgestützte Sicherheitsmechanismen haben das Potenzial, die nächste Generation von Anwendungen voranzutreiben.

Mehr Transparenz durch pfadbewusste Netze

Pfadbewusste Netze ermöglichen es Endgeräten, Informationen über die zum Ziel führenden Netzwerkpfade vorzuhalten. So können sie den gewünschten Pfad aus einer Reihe von Pfaden, die das Netzwerk anbietet, auswählen. Diese Pfadauswahl stellt Anwendungen und Diensten spannende Eigenschaften wie die Pfadtransparenz, feingranulare Pfadkontrolle, schnelles Failover oder Routenoptimierung zu alternativen Pfaden sowie Geo-Fencing bereit. Diese Eigenschaften ermöglichen die Entwicklung neuer Transportprotokolle und fortgeschrittener Anwendungsfunktionen. Pfadbewusste Netze ermöglichen auch Multipath-Kommunikation: Falls das Endgerät mehrere Pfade vom Netzwerk erhält, kann es die Pfade paketweise auswählen. Die Multipath-Kommunikation erlaubt eine höhere Bandbreite oder niedrigere Latenz, eine verbesserte Zuverlässigkeit und eine effizientere Nutzung.

Fortgeschrittene Sicherheitsfunktionen, die in vielen pfadbewussten Netzwerkarchitekturen mit eingebaut sind, ermöglichen die Entwicklung neuer Anwendungen und Dienste. Diesen stellt das Netzwerk integrierte Mechanismen zur Vertrauensbildung und Schlüsselverteilung sowie die Abwehr von DDoS-Angriffen (Distributed Denial-of-Service) und Techniken zur Verbesserung der Privatsphäre bereit.

Um das volle Potenzial all dieser Möglichkeiten auszuschöpfen, müssen jedoch zuerst noch viele offene Forschungsfragen beantwortet werden: Welche Pfade und welche zusätzlichen Informationen sollen den Endgeräten angeboten werden? Wie soll die API-Schnittstelle zwischen Netzwerk-, Transport- und Anwendungsschicht aussehen? Wie arbeiten die verschiedenen Schichten zusammen, um die besten Pfade mit begrenztem Overhead auszuwählen? Welche Staukontrollalgorithmen sind geeignet, wenn Endgeräte die Pfade wechseln oder mehrere Pfade gleichzeitig benutzen?

Ein Testbed für innovative Netzwerkexperimente

SCIONLab ist ein globales Netzwerk-Testbed, das es Forschern ermöglicht, pfadbewusste Netzwerkarchitekturen zu erforschen und sie bei der Beantwortung dieser Fragen zu unterstützen. Basierend auf einer gut vernetzten Netzwerktopologie, die aus global verteilten Knoten besteht, ermöglicht SCIONLab innovative Netzwerkexperimente u. a. im Bereich Multipath-Kommunikation zwischen Domänen, pfadbewussten Netzen und Anwendungen sowie die Erforschung neuer Routing-Policies und neuer Ansätze zur DDoS-Abwehr.

Hinter dem SCIONLab-Ansatz verbirgt sich ein neuartiges Design für ein flexibles, skalierbares, erweiterbares und intuitives Testbed. Es basiert auf der SCION-Internetarchitektur und erbt damit deren Eigenschaften in Bezug auf Skalierbarkeit, Sicherheit und Effizienz. So verbessert SCION die Sicherheit auf verschiedenen Ebenen, z. B. durch Schutz vor bösartigen autonomen Systemen (AS) sowie durch Transparenz und Kontrolle über Pfade und Trustroots. Das Testbed ist seit 2016 in Betrieb und hat bereits verschiedene Forschungsprojekte unterstützt.

Die derzeitige Netzwerkinfrastruktur von SCIONLab (Abbildung 1) basiert auf 36 global verteilten AS. Jeder Knoten stellt dabei ein SCION-AS und jede Kante eine Netzwerkverbindung dar. SCION organisiert autonome Systeme in Isolationsdomänen (ISD), die untereinander verbunden sind, um globale Konnektivität zu gewährleisten. Eine ISD wird von einer Menge von AS (dem sogenannten ISD-Core) verwaltet, welche die Trustroots der ISD definieren, die Zertifikate für die AS in der ISD ausstellen und für die Konnektivität zwischen den ISD sorgen. Das DFN-SCION-AS ist eines dieser Core-AS für die Isolationsdomäne „EU“ im globalen SCIONLab-Netzwerk.

Benutzerzugang mit minimalem Aufwand

An der SCIONLab-Basisinfrastruktur hängen derzeit über 600 weitere sogenannte Benutzer AS, die sich über einen der Attachment Points verbunden haben, um am SCIONLab-Netzwerk teilzunehmen. Benutzer-AS sind vollwertige autonome Systeme, die von den Benutzern mit wenigen Mausklicks in kurzer Zeit erstellt werden können, um einen direkten, ungehinderten Zugang zum Inter-Domain-Routingsystem von SCION zu erhalten. Der zentrale Koordinierungsdienst, der SCIONLab-Koordinator, orchestriert die Infrastruktur und die Benutzer-AS, um eine nahtlose Vernetzung mit einer Vielzahl von Netzwerktopologien und Benutzerumgebungen zu unterstützen.

Um globale Konnektivität in SCIONLab zu erreichen, basieren die meisten Links derzeit auf einem IP-Overlay, welcher die Border Router zwischen benachbarten AS verbindet. Knoten, die hinter einem NAT-Gerät (Network-Address-Translation-Gerät) mit einer festen IP-Adresse liegen, können ebenfalls direkt verbunden werden, sofern der UDP-Zielport 50000 intern an den SCION-Border-Router weitergeleitet wird. Die Verbindung von Knoten mit dynamischen IP-Adressen wird über eine OpenVPN-Verbindung gewährleistet.

Illustration: NicoElNino/Adobe Stock

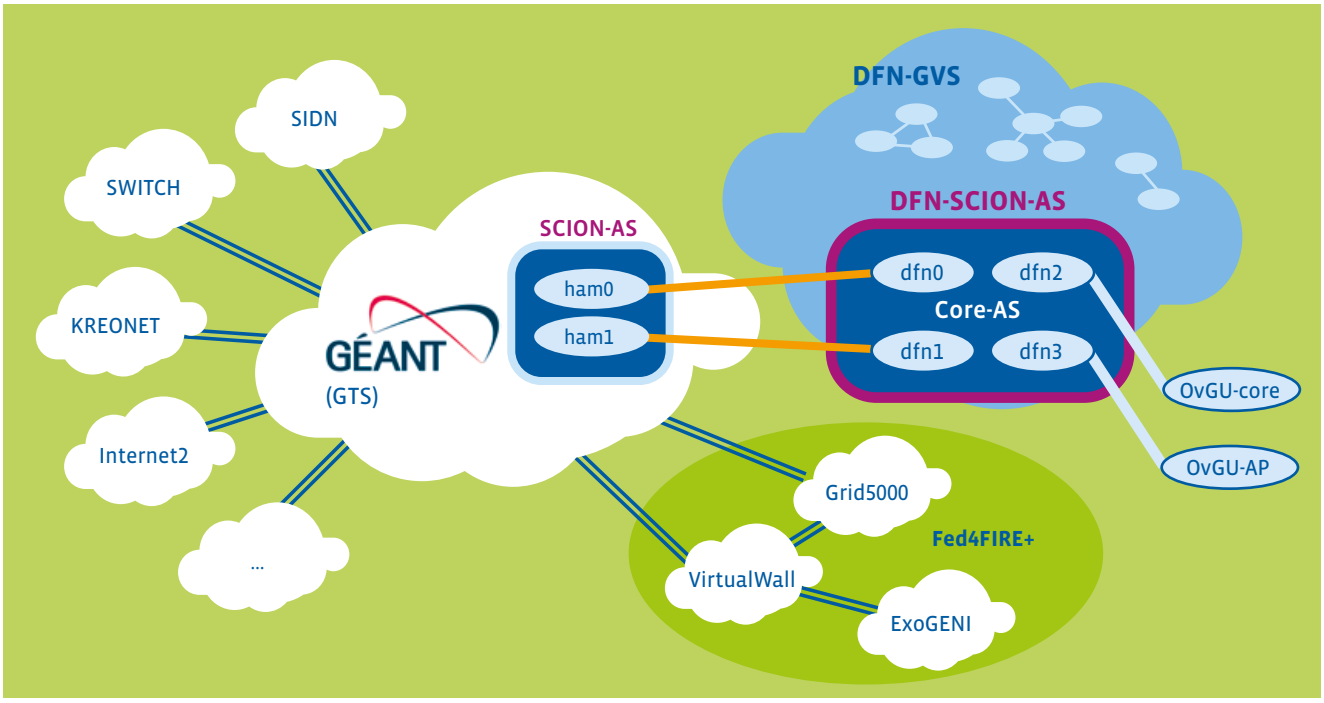


Abbildung 2: Übersicht DFN-GVS und DFN-SCION-AS

Jedes SCION-AS besteht aus einem Beacon-Service (BS), einem Zertifikatsdienst (Certificate Service-CS) und einem Pfaddienst (Path-Service-PS) sowie einem oder mehreren Border-Routern. Für Benutzer, die keine AS-Dienste betreiben wollen, wird auch die alleinige Installation eines SCION-Endgerätes unterstützt. Durch die Konfiguration des SCION-daemon (sciond) kann sich das Endgerät in ein bestehendes AS einklinken und mit den AS-Diensten kommunizieren, um Pfade und Zertifikatsinformationen zu erhalten.

Auf einem Endgerät kann eine Anwendung, die einen SCION-UDP- oder QUIC-Socket öffnet, die Auswahl eines Pfades aus einer Reihe von Pfaden treffen, die vom Netzwerk angeboten werden. Jeder SCION-Paket-Header enthält die Pfad-Informationen auf AS-Ebene. SCION-Border-Router leiten daher Pakete einfach an den nächsten Hop weiter, ohne dass eine Inter-Domain-Routingtabelle nachgeschlagen werden muss. Folglich können unterschiedliche Pfade mit einer feinen Granularität (pro Paket) eingesetzt werden.

AS-Ausführung auf heterogenen Systemen

Der SCIONLab-Koordinator (https://www.scionlab.org/) unterstützt derzeit verschiedene Möglichkeiten, um ein SCION-AS automatisiert aufzusetzen. Der einfachste Weg, um ein SCION-AS zu betreiben, ist innerhalb einer Virtuellen Maschine (VM). Dazu wird eine VM-Konfiguration vom Koordinator heruntergeladen, auf deren Grundlage ein vollwertiges SCIONLab-AS in einer Ubuntu-18.04-basierten VM mittels Virtualbox und Vagrant vollautomatisch installiert wird.

Alternativ können Benutzer die Installation eines SCIONLab-AS auf einem dedizierten Host einfach über vorkompilierte Softwarepakete vornehmen. Diese enthalten auch Anweisungen zur Konfiguration des AS. Derzeit unterstützt SCIONLab nur Debian-style-Pakete. Diese können auf einer Vielzahl von Linux-Systemen wie u. a. Debian oder Ubuntu installiert werden.

Für den speziellen Fall, dass der Benutzer die SCION-Dienste aus dem Quellcode kompilieren möchte, kann der Koordinator eine Konfiguration zurückgeben, die lediglich aus der Konfiguration der Dienste und einer Reihe von Supervisord-Dateien zum Starten und Stoppen der Dienste besteht.

Schließlich ist es auch möglich, SCION auf einem Android-Gerät zu installieren. Konkret ermöglicht es die SCION-App ein vollständiges SCIONLab-AS auf einem Android-Smartphone zu betreiben. Die Einrichtung des AS erfolgt in vollständig automatisierter Weise auf der Grundlage der AS-Konfiguration des Koordinators.

DFN-GVS stellt SCION-Core-AS zur Verfügung

Das DFN-SCION-AS ist physisch über mehrere Hosts auf der Infrastruktur des DFN-Pilotservice „General-Virtualization-

Service (GVS)“ im Regionalen Rechenzentrum Erlangen (RRZE) der Universität Erlangen-Nürnberg verteilt. Zwei dieser Hosts sind als SCION-Border-Router nativ über zwei dedizierte L2VLANs mit dem GÉANT Testbed Service (GTS) verbunden, in welchem wiederum das GÉANT-SCION-AS aufgesetzt ist. Gleichzeitig bietet das DFN-SCION-AS eine öffentliche IPv4-Schnittstelle, über welche beispielsweise das Core-AS und der Attachment Point an der OVGU Magdeburg verbunden sind. In Zukunft wird angestrebt, diese Verbindungen ebenfalls durch L2VLANs zu ersetzen und damit komplett BGP-frei (das heißt: unabhängig von BGP) zu gestalten.

Der DFN-GVS-Dienst ermöglicht es Nutzern, virtuelle Netze mit wenigen Mausklicks über ein Webportal selbst zu erzeugen. Der Ansatz basiert auf echtem Network Slicing der Hardware und eignet sich damit im Besonderen für Netzwerk-Forschungsexperimente wie SCION. Interessierte Forschungsgruppen können auf der DFN-GVS-Webseite (https://dfn-gvs.de/) einen Account beantragen, um damit Testbeds bestehend aus einem oder mehreren Hosts zu erstellen und diese untereinander zu verbinden. Jedes Projekt bekommt zudem ein Internet Access Gateway zugeteilt und 3GB+ Speicher zur freien Verfügung. Auch OpenFlow-Switches können für SDN-Tests einem Projekt zugeteilt werden. Internationale DFN-GVS-Netze können z. B. über Hamburg mit GÉANT-GTS erweitert werden.

Um Forschungsexperimente über SCIONLab durchzuführen, müssen die Hosts als ein (oder mehrere) SCION-AS konfiguriert werden. Dazu können sich Forscher auf der Webseite des SCIONLab-Koordinators registrieren und darüber SCION-Benutzer-AS erstellen und diese mit beliebigen SCIONLab Attachment Points verbinden. Auch im DFN-AS ist es geplant, einen entsprechenden Attachment Point anzubieten. Die erstellten SCION-AS-Konfigurationen können dann genutzt werden, um die Hosts im DFN-GVS-Testbed aufzusetzen und mit SCIONLab zu verbinden. Dank der lokalen Netzwerkanbindung können somit Experimente mit Bandbreiten im Gigabit-Bereich über das globale SCIONLab Testbed durchgeführt werden. Mittelfristig sollen sogar 10G-SCION-Verbindungen über das DFN-GVS ermöglicht werden.

Anbindung weiterer Testbeds

Im Rahmen eines „Fed4FIRE+“-Projektes, das innerhalb des EU-Programms Horizont 2020 gefördert wird, werden SCIONLab-AS derzeit auf weiteren Testbeds aufgesetzt. Dazu gehören VirtualWall, Grid5000 und ExoGeni. Während die ersten beiden Testbeds durch L2VLANs über GÉANT mit SCIONLab verbunden sind, läuft die Verbindung mit ExoGeni über das Internet2-Netz, das größte und schnellste Forschungs- und Bildungsnetz der USA, das über 300 Universitäten und Regierungsbehörden von Küste zu Küste versorgt. SCIONLab ermöglicht es, diese ansonsten voneinander weitgehend isolierten Testbeds über SCION mittels Inter-Domain-Multipath-Kommunikation zuverlässig miteinander zu verbinden und damit Testbed-übergreifende Forschungsexperimente durchzuführen, die insbesondere auch das DFN-GVS-Testbed mit einschließen können. Der SCION IP Gateway (SIG) ermöglicht es zudem, dass auch nicht-SCION-fähige Anwendungen über das SCIONLab-Netzwerk kommunizieren können.

Fazit

SCIONLab ist ein globales Testbed zur Erforschung und Entwicklung von Inter-Domain-Kommunikationsmechanismen der nächsten Generation. Es ermöglicht die Erstellung von eigenen, vollwertigen SCION-AS, die am globalen Inter-Domain-Routing teilnehmen können. Das SCIONLab Testbed bietet eine neuartige Infrastruktur, um innovative Forschungsarbeiten, z. B. an pfadbewussten und Multipath-fähigen Transportprotokollen, an globaler Schlüsselvereinbarung zur sicheren Kommunikation auf der Grundlage von Zertifikaten auf AS-Ebene, an Routing-Policies der nächsten Generation, an Traffic Engineering und an DDoS-Abwehrmechanismen zu unterstützen. Durch die Anbindung des DFN an das globale SCIONLab-Netzwerk über dedizierte L2VLANs kann das DFN-GVS-Testbed als Infrastruktur für Forschungsexperimente mit Bandbreiten im Gigabit-Bereich über SCION eingesetzt werden. ◆

WEITERFÜHRENDE LINKS

- SCION Internet Architektur: **https://www.scion-architecture.net/**
- SCIONLab Koordinator: **https://www.scionlab.org/**
- SCION Android App: **https://play.google.com/store/apps/details?id=org.scionlab.scion**
- SCIONLab Tutorial: **https://docs.scionlab.org/**
- General-Virtualization-Service des DFN: **https://dfn-gvs.de**

Sicherheit

Wer kennt mein Passwort?

Ein Frühwarndienst für Identitätsdatendiebstahl an Hochschulen

Text: **Timo Malderle** (Universität Bonn), **Michael Meier, Matthias Wübbeling** (Universität Bonn, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE)

Im Rahmen des Projekts „Effektive Information nach digitalem Identitätsdiebstahl“ (EIDI) werden öffentlich verfügbare Identitätsdaten-Leaks – durch Identitätsdatendiebstahl erbeutete Benutzerdaten eines Online-Dienstes – gesucht und verarbeitet, um möglichst viele Betroffene proaktiv zu warnen. Während der Projektlaufzeit konnten mehr als 20 Milliarden gestohlene Identitätsdaten gesammelt werden. Um diese große Menge an Identitätsdaten sicher und datenschutzkonform zu verarbeiten, müssen bereits von Projektbeginn an alle entwickelten Systeme datenschutzkonform gestaltet und implementiert werden. Warum Sie die analysierten Identitätsdaten überprüfen sollten, um Mitarbeiter und Studierende an Ihrer Hochschule zu unterstützen, erfahren Sie hier.

Foto: yipengge/iStock

Seit dem Identitätsdatendiebstahl im Frühjahr 2019, bei dem von etwa 1.000 Persönlichkeiten des öffentlichen Lebens, Politikern und Journalisten persönliche Daten gestohlen wurden, erfährt das sogenannte Doxxing insgesamt eine große öffentliche Aufmerksamkeit. Doxxing bezeichnet das digitale Zusammentragen und anschließende Veröffentlichen personenbezogener Daten, oft mit kriminellen Absichten gegenüber den Betroffenen. Viel häufiger sind Identitätsdaten-Leaks mit Zugangsdaten

und Kreditkartennummern von Nicht-Prominenten. Die große Zunahme von öffentlichen Identitätsdaten-Leaks liegt eventuell daran, dass die Anzahl der Benutzerkonten pro Verbraucher in den vergangenen Jahren kontinuierlich gestiegen ist. Aufgrund dieser Vielzahl von eigenen Benutzerkonten verwenden Verbraucher zur Authentifizierung bei unterschiedlichen Online-Diensten häufig dieselben Anmeldeinformationen wie E-Mail-Adressen oder Passwörter. Werden Anmeldeinformationen

durch Datendiebe erbeutet und anschließend verkauft oder veröffentlicht, besteht die Gefahr, dass eine Vielzahl der enthaltenen Benutzerkonten ad hoc gefährdet ist.

Identitätsdaten-Leaks enthalten oft nicht nur die Anmeldeinformationen von Benutzern, sondern auch persönliche Daten, etwa Postadressen, Telefonnummern aber auch Konto- oder Kreditkartennummern. Leaks werden von Kriminellen in Untergrundforen getauscht, verkauft oder sogar öffentlich zugänglich gemacht. Diese Leak-Daten können dann von Betrügern für Identitätsdiebstahl online wie offline, z. B. für Packstationen o. ä. genutzt werden. Durch eine Veröffentlichung von Leaks sind nicht nur professionelle Kriminelle sondern auch Laien und sogenannte Scriptkiddies in der Lage, Identitätsbetrug zu begehen.

Öffentlich verfügbare Leak-Daten bergen aber auch die Möglichkeit, Verbraucher frühzeitig zu warnen und so sogar Identitätsbetrug zu verhindern, da kritische Informationen wie Anmeldeinformationen von Betroffenen rechtzeitig geändert werden können.

Bestehende Leak-Informationsdienste

Zum Schutz von Identitäten und vor Identitätsdiebstahl gibt es unterschiedliche Projekte. Mit verschiedenen Ansätzen versuchen die Betreiber, den durch Identitätsdiebstahl entstehenden Schaden einzugrenzen. Einige Projekte beschäftigen sich dabei mit sogenannten Leak-Informationsdiensten. Diese bieten die Möglichkeit, die eigene Betroffenheit durch Identitätsdatendiebstahl zu überprüfen. Bekannte Dienste sind der Leakchecker der Universität Bonn, der HPI-Leak-Checker oder *Have I been pwned*. Es gibt auch kommerzielle Dienste, die gegen Bezahlung anbieten, die eigenen Identitäten zu überwachen.

Insbesondere das Angebot von *Have I been pwned*, als Dienst aus den USA, ist datenschutzrechtlich und ethisch bedenklich, weil bei diesem Dienst jede Person nicht nur ihre eigene, sondern beliebige E-Mail-Adressen auf Betroffenheit überprüfen kann und das Ergebnis der Überprüfung direkt angezeigt bekommt. Eine Authentifikation findet nicht statt. Somit kann im Grunde jeder erfahren, wessen Daten geleakt wurden und bei welchen Diensten eine dritte Person angemeldet ist. Der Leakchecker der Uni Bonn und der HPI-Leak-Checker versenden dagegen das Ergebnis per E-Mail an die überprüfte E-Mail-Adresse. Leider sind Leak-Informationsdienste wie die vorgestellten in der Gesellschaft nur wenig bekannt, sodass ein proaktiver Ansatz notwendig ist, um möglichst alle Verbraucher zu informieren.

Im Folgenden wird das Projekt „Effektive Information nach Digitalem Identitätsdiebstahl“ (EIDI) der Universität Bonn vorgestellt. Im Rahmen des Projekts werden öffentlich verfügbare Identitätsdaten-Leaks gesammelt und automatisiert analysiert. Um den Datenschutz zu gewährleisten, werden die Daten schon beim Einlesen in einem speziellen Verfahren pseudonymisiert und verschlüsselt. Anschließend können diese Daten nur dann verwendet werden, wenn ein Verarbeiter bereits zur Nutzung des Datensatzes berechtigt ist.

Leak-Sammlung und Analyse

Um einen Leak-Informationsdienst zu betreiben, müssen die Forscher der Universität Bonn zunächst gesammelte Identitätsdaten analysieren und die relevanten Merkmale der enthaltenen Identitäten extrahieren. Der Inhalt von Leak-Dateien unterscheidet sich dabei nicht nur in den enthaltenen Identitätsmerkmalen, sondern auch in den verwendeten Zeichen, mit denen die einzelnen Merkmale voneinander getrennt werden (dem Separator). Gängige Identitätsmerkmale in Leaks sind: E-Mail-Adresse, Passwort, Passwort-Hash, Benutzername, Name, Geburtsdatum, Anschrift, Kreditkartennummer, etc. Die meisten Identitätsdaten-Leaks enthalten pro Zeile genau den Datensatz einer Person, wodurch die Anzahl der Zeilen einer Datei häufig Aufschluss über den Umfang eines Leaks geben kann. Die im Rahmen von EIDI betrachteten Identitätsdaten-Leaks

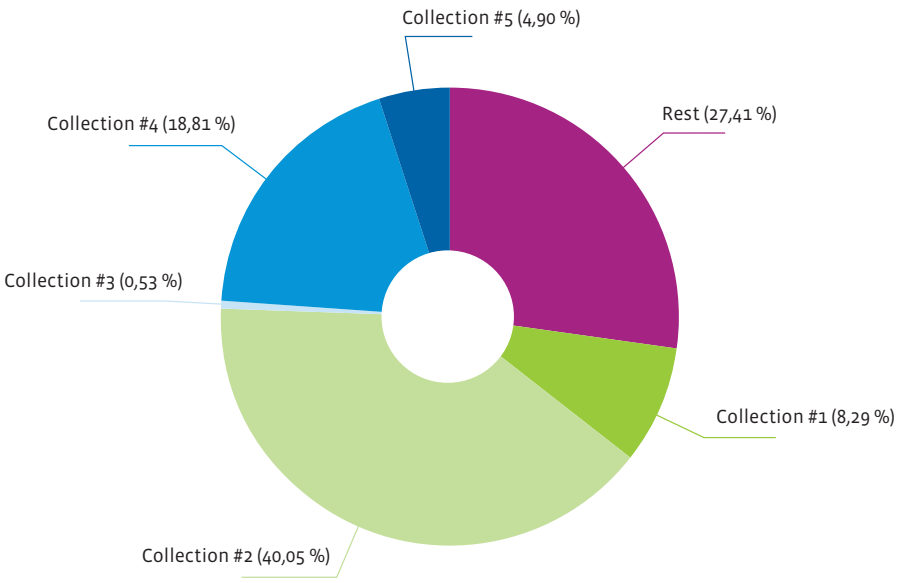


Abbildung 1: Größte Identitätsdaten-Leaks in 2019

enthielten mindestens zwei Identitätsmerkmale, so konnten einfache E-Mail-Spam-Listen ausgeschlossen werden. Die meisten vorkommenden Merkmalskombinationen sind: [E-Mail:Passwort], [E-Mail:Hash], [E-Mail:Hash:Passwort], [E-Mail:Benutzername:Hash:Salt]. Häufig gibt es auch vollständige Kopien von SQL-Datenbanken. Die in Leaks verwendeten Separatoren, in den vorherigen Beispielen der Doppelpunkt, variieren dabei deutlich, teilweise sogar innerhalb einer Datei. Gängige Separatoren sind: [;], [::], [--||--], [//], [tab], es gibt aber je nach Ersteller noch viele weitere Kombinationen.

In dem Forschungsprojekt der Universität Bonn werden nur öffentlich zugängliche Identitätsdaten-Leaks heruntergeladen und analysiert. Es werden keine Leaks von Kriminellen gekauft. Durch die adaptiven Verfahren beim Einlesen der Leak-Daten konnten mit mehr als 20 Milliarden Datensätzen deutlich mehr Informationen aus den Leak-Daten herausgearbeitet werden als bei den anderen genannten Leak-Informationsdiensten.

Die größten Leaksammlungen im Jahr 2019 waren Collection #1 bis Collection #5. Den Anteil dieser Leaks am Gesamtdatenbestand zeigt Abbildung 1. Aus diesen Sammlungen konnte der Parser – das ist die Software, die Identitätsdaten aus den Leak-Daten herausfiltert – aus mehr als 17,8 Milliarden Zeilen mehr als 14,5 Milliarden Identitätsdaten herausarbeiten, dies wäre mit einer manuellen Analyse kaum möglich gewesen. In Abbildung 2 sind die Top 10 der größten Leaks dargestellt, welche im EIDI-Projekt gesammelt wurden. Zu sehen ist, die Collections #1–#5 zwar in den Top 10 enthalten sind, dass es aber nicht die fünf größten Identitätsdaten-Leaks überhaupt sind.

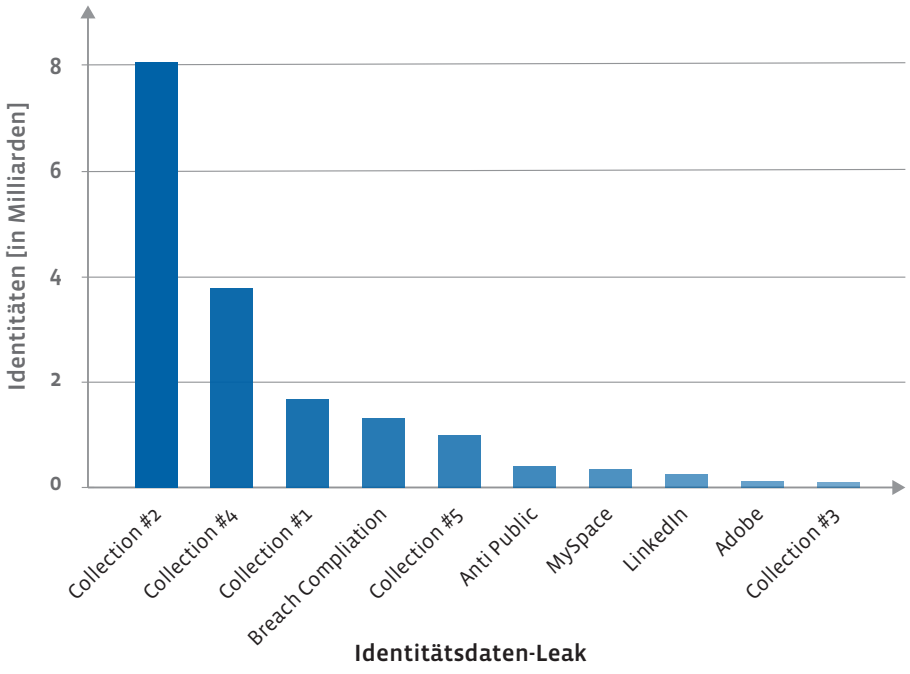


Abbildung 2: Größte Identitätsdaten-Leaks (insgesamt)

Aufbau eines Frühwarndienstes

Weil Leak-Informationsdienste aus Unkenntnis wenig genutzt werden, ist eine Dienstleistung notwendig, die betroffene Personen proaktiv kontaktiert. Es soll eine Warnung ausgesprochen werden, die im besten Fall zu einer schadenminimierenden Handlung des Benutzers führt.

Das Hauptproblem bei der Umsetzung ist, dass ein geeigneter Kommunikationskanal notwendig ist, um eine Warnung an betroffene Benutzer zu übermitteln. Ein trivialer Ansatz wäre, die in den Leaks enthaltene E-Mail-Adresse zu verwenden, um die Betroffenen zu kontaktieren. Allerdings scheint dieses Vorgehen nicht zielführend, da viele Betroffene eine E-Mail mit einem entsprechenden Warninhalt von einem für sie unbekannten Absender für Spam halten werden.

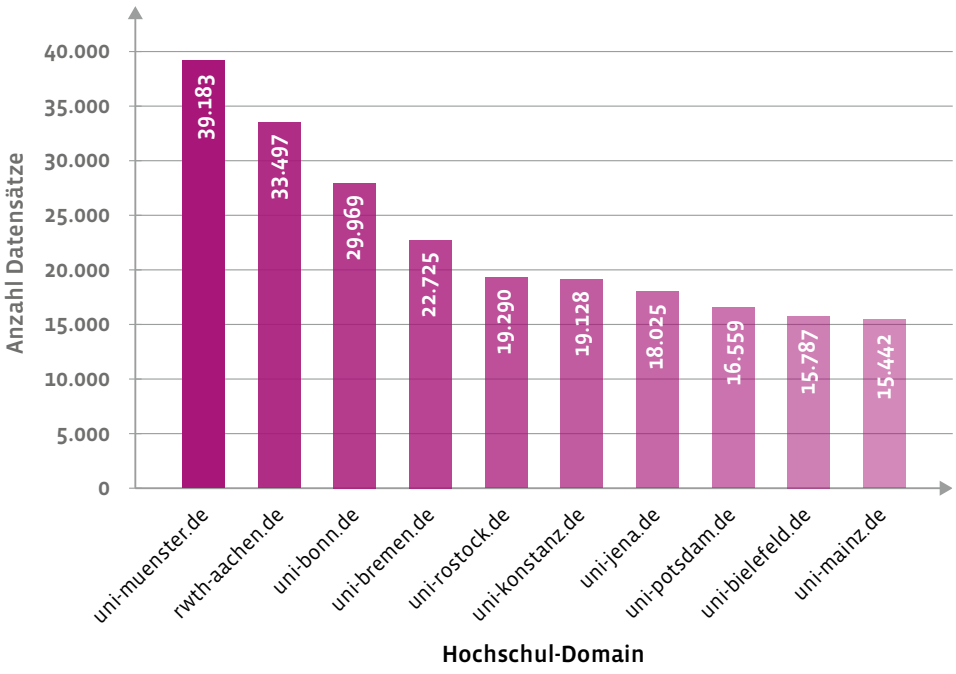


Abbildung 3: Top 10 betroffener Hochschuldomains

Eine bessere Lösung wäre, dass ein Benutzer von jemandem gewarnt wird, dem er mehr vertraut als einem unbekannten Absender. Dafür infrage kommen beispielsweise Dienstanbieter, denen ein Nutzer zur Erbringung einer Dienstleistung bereits Identitätsdaten bereitgestellt hat. Geeignet dafür sind im Grunde sämtliche Dienste, die Benutzerkonten verwalten: E-Mail-Anbieter, soziale Netzwerke, Web-Shops, Banken und viele mehr.

Hochschulen als Warnungsgeber

Auch Hochschulen bieten ihren Angestellten und Studierenden Benutzerkonten und E-Mail-Postfächer an. Deswegen sind auch Hochschulen in der Lage, eine Warnung gegenüber den Benutzern auszusprechen. Die Idee eines Frühwarndienstes ist, dass ein zentral betriebener Dienst eine Datenbank vorhält, die aktuelle Identitätsdaten-Leaks enthält. Dieser Dienst sendet die zur Warnung notwendigen Informationen an alle Kooperationspartner.

Der zentral verwaltete Frühwarndienst muss vor dem Austausch der Daten mit den Kooperationspartnern datenschutzrechtliche Aspekte beachten, da es sich umfassend um personenbezogene Daten handelt. Zum Schutz der Identitätsdaten und Personen dahinter, werden diese Daten ausschließlich pseudonymisiert gespeichert und ausgetauscht. Es muss festgelegt werden, welche Daten in einem übermittelten Datensatz enthalten sein müssen, damit sinnvoll gewarnt werden kann. Das wichtigste Attribut ist ein eindeutiges Identitätsmerkmal, das einen Identitätsdatensatz eindeutig einer Person zuordnet. Bei Hochschulen wird es sich dabei um einen Benutzernamen oder eine E-Mail-Adresse als Identitätsmerkmal handeln. Wenn es sich bei dem Identitätsmerkmal um einen Benutzernamen handelt, besteht dieser im Hochschulkontext in der Regel aus dem Alias der E-Mail-Adresse oder aus einer Matrikelnummer. Die Veröffentlichung einer einzelnen E-Mail-Adresse oder eines Benutzernamens alleine reicht zumeist nicht für einen Identitätsdiebstahl aus. Wenn jedoch das entschlüsselte Passwort zusammen mit der E-Mail-Adresse oder dem zugehörigen Benutzernamen einen Login erlaubt, handelt es sich um valide Identitätsdaten und eine umgehende Warnung des Betroffenen ist notwendig.

Identitätsdiebstahl an deutschen Hochschulen

Universitäten sind mögliche Partner für das EIDI-Projekt, weil sie Personen ein Identitätsmerkmal anbieten, mit dem sie sich auch bei weiteren Online-Diensten anmelden können. Studierende nutzen ihre universitären E-Mail-Adressen zwar hauptsächlich für studentische Zwecke, jedoch ist eine Verwendung für die Anmeldung bei Online-Shops, Karrierenetzwerken oder in Internetforen denkbar.

Im Rahmen des Projekts haben die Forscher der Universität Bonn die Hauptdomains der 429 deutschen Hochschulen betrachtet. Sie konnten so in der Leak-Datenbank des EIDI-Projekts insgesamt 676.091 betroffene Identitäten mit Hochschul-E-Mail-Adresse ermitteln. Die Top 10 der deutschen Hochschulen sind in Abbildung 3 mit der Anzahl an betroffenen Identitäten dargestellt.

Für die Domain uni-muenster.de konnten 39.183 Einträge identifiziert werden. Selbst Platz 10 der Liste, uni-mainz.de, ist immerhin noch mit 15.442 Einträgen in den EIDI-Datensätzen vertreten. Die Top 10 beinhalten 33,66 Prozent der von deutschen Hochschulen gefundenen Identitäten. Aus diesen Zahlen lässt sich schlussfolgern, dass auch Studierende und Mitarbeiter von Hochschulen umfangreich von Identitätsdiebstahl betroffen sind. Allerdings lassen sich vermutlich nicht sämtliche Login-Daten auch für einen erfolgreichen Login an der Universität nutzen. Es ist nicht unwahrscheinlich, dass bei mehreren Tausend geleakten Identitäten aber tatsächlich eine gewisse Anzahl valider Zugangsdaten enthalten ist.

Der Schaden, der durch Identitätsdiebstahl an einer Hochschule entstehen kann, ist abhängig von der Art des Angriffs. Im geringsten Fall nutzt ein Angreifer die Zugangsdaten nur zum Versand von Spam-

E-Mails. In einem schlimmeren Fall könnte ein Angreifer ein kompromittiertes Dozenten-Benutzerkonto missbrauchen, um falsche Noten einzutragen oder Zeugnisse auszustellen. Bei einem Angreifer mit kompromittiertem Studenten-Account könnte je nach Prozessstruktur ein Student unfreiwillig zu einer Klausur an- oder abgemeldet oder der Student sogar exmatrikuliert werden.

Integration des Warndienstes in der eigenen Infrastruktur

Um den vorgestellten Frühwarndienst zu nutzen, muss auf der Seite des Partners eine REST-Schnittstelle betrieben werden, an die dann der Frühwarndienst geeignete Identitätsdaten-Leaks versenden kann. Im Folgenden werden der Aufbau und die Funktionsweise der benötigten REST-Schnittstelle genauer beschrieben. Hauptsächlich benötigt die Schnittstelle zwei Anforderungen an die eigene Infrastruktur:

Anforderung 1 – gehashte E-Mail-Adressen

Da die Daten verschlüsselt vorliegen, müssen alle existierenden E-Mail-Adressen der Benutzer mit einem vorgegebenen Verfahren gehasht werden. Dieser Hash muss so abgespeichert werden, dass die Schnittstelle später wieder die Klartext-E-Mail-Adresse zuordnen kann. Idealerweise lässt sich der Hash direkt in der Benutzerdatenbank zu jedem Benutzereintrag mit abspeichern. Allerdings benötigt dann die Schnittstelle einen dauerhaft lesenden Zugriff auf die Benutzerdatenbank. Ob dies sinnvoll und möglich ist, hängt von der vorhandenen Infrastruktur ab.

Anforderung 2 – interne Authentifizierung ohne Rate-Limiting

Als zweite Anforderung wird ein Endpunkt in der eigenen Infrastruktur benötigt, welcher die entschlüsselten Login-Daten auf Validität überprüfen kann. Beispielsweise eignet sich dafür ein interner Zugang zum IMAP-Server, ein interner (Dummy-)Login-Dienst oder eine direkte Anbindung an Kerberos oder Active Directory.

Sind beide Anforderungen in der Hochschule umsetzbar, können diese in die REST-Schnittstelle integriert werden. Eine Definition der REST-Schnittstelle sowie eine Beispielanwendung für diese Schnittstelle sind vorhanden und werden bei Interesse an mögliche Partner herausgegeben. Wird diese Schnittstelle mit integrierter Infrastruktur betrieben, so kann der Frühwarndienst neue Leak-Daten zeitnah automatisiert an diese Schnittstelle übermitteln. In den Daten sind dann für jeden Datensatz ein Hash der E-Mail-Adresse sowie das verschlüsselte Passwort vorhanden.

Nach dem Empfang werden die gehashten E-Mail-Adressen aus dem Leak mit den gehashten E-Mail-Adressen aus der eigenen Benutzerdatenbank verglichen. Gibt es eine Übereinstimmung zwischen zwei Hashes, so kennt der Schnittstellenbetreiber auch die Klartext-E-Mail-Adresse. Diese Klartext-E-Mail-Adresse wird anschließend zum Entschlüsseln des Passworts genutzt. Danach wird überprüft, ob die E-Mail-Adresse und das Passwort einen erfolgreichen Login am eigenen System des Kooperationspartners zulassen. Sollte der betroffene Account kompromittiert sein, kann der Betroffene über einen geeigneten Kommunikationskanal gewarnt werden oder aber es werden spezielle sicherheitskritische Funktionen des Accounts deaktiviert. Natürlich kann auch der ganze Account zum Schutz der eigenen Infrastruktur und zum Schutz des Betroffenen vollständig gesperrt werden.

Fazit

Hochschulen agieren für ihre Beschäftigten und Studierenden als Betreiber von Online-Diensten und stellen Identitäten meist in Form von E-Mail-Adressen zur Verfügung. Der Artikel stellt das EIDI-Projekt vor, das Hochschulen als Partner des EIDI-Systems anbinden möchte, um durch eine geeignete Warnung der Betroffenen bestehende Bedrohungen minimieren zu können. Eine Anbindung an das EIDI-Projekt wird Hochschulen empfohlen, um Mitarbeiter und Studierende so gut es geht zu schützen. ◆

Weitere Informationen zum Leakchecker der Universität Bonn finden Sie hier:

https://leakchecker.uni-bonn.de/
https://itsec.cs.uni-bonn.de/eidi/
E-Mail: leakchecker@uni-bonn.de
Telefon: 0228/73 54210

Das Projekt EIDI wird gefördert vom Bundesministerium für Bildung und Forschung (BMBF) mit dem Förderkennzeichen 16KIS0696K.

Im Auge des Zyklons – DFN-Tutorium Crisis Management Exercise

Werden Sie eine Krise unbeschadet überstehen? Mit dieser Frage im Hinterkopf ließen sich am 25. Februar 2020 gut 80 Teilnehmerinnen und Teilnehmer der DFN-Sicherheitskonferenz in das erfundene Königraiche Guilder entführen. Im Rahmen des DFN-Tutoriums Crisis Management Exercise wurde eine Krisensimulationsübung durchgeführt, die speziell auf die Bedürfnisse der Nutzer an einem Forschungsnetz zugeschnitten war.

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

Foto: marrio31 / iStock

Eine Krise stellt die substanzielle Bedrohung einer Organisation dar, sie tritt überraschend auf, entwickelt sich schnell und erfordert eine unverzügliche Reaktion. Sie ist mit den üblichen Prozeduren, mit denen normalerweise auf potenziell schädliche Ereignisse und Vorfälle reagiert wird, nicht mehr zu beherrschen. Eine Krise ist zudem geprägt von Unsicherheit, wenigen oder zum Teil fehlerhaften Informationen sowie Druck von externen Interessengruppen und eventuell den Medien. Doch wie sich auf eine solche Situation vorbereiten, wie ihr begegnen? Die Antwort: Krisenmanagement.

Unter Krisenmanagement (engl. Crisis Management) versteht man die systematische Koordination der effektiven und rechtzeitigen Reaktion auf eine Krise. Ziel ist es, den Schaden in Bezug auf die strategischen Ziele, die Reputation und Handlungsfähigkeit der Organisation zu verhindern oder zu minimieren.

Eine Krise besteht aus vielen verschiedenen Herausforderungen. Um diese zu bewältigen, geht es im Krisenmanagement sowohl um die interne als auch die externe Kommunikation. Darüber hinaus spielen die Ermittlung und Priorisierung existierender Handlungsoptionen, eine klare Rollenverteilung sowie der Umgang mit dem jeder Krise innewohnenden Stress eine wichtige Rolle. Auch oder gerade weil jede Krise unterschiedlich ist und zu Verunsicherung führt, ist es notwendig und sinnvoll, sich auf mögliche Krisensituationen vorzubereiten.

Die Herausforderungen einer Krise bestehen unabhängig davon, ob es sich um eine Cyber-Krise oder um eine Krise außerhalb eines IT-Umfeldes handelt. Bei einer Cyber-Krise müssen jedoch der IT-Betrieb, das Incident Management und ggf. die Softwareentwicklung involviert und koordiniert werden. Im Falle einer Cyber-Attacke oder einer gravierenden IT-Panne müssen umgehend Maßnahmen getroffen werden, um die Vertraulichkeit und Integrität der Organisationsdaten sowie die zur Verarbeitung anvertrauten Daten Dritter zu schützen. Außerdem muss ein Informationsdiebstahl vermieden oder eingegrenzt werden und die Verfügbarkeit der IT-Dienste muss gesichert werden. Hierbei müssen sowohl Datenschutz als auch Informationssicherheit berücksichtigt werden. Dies gilt insbesondere, wenn der Vorfall durch einen Angriff ausgelöst wurde, welcher wiederum weitere spezielle Anforderungen an eine rechtlich und technisch richtige Spurensicherung stellt. Gerade die Spurensicherung kann in Konkurrenz zu anderen Zielen stehen, da beispielsweise das Einspielen eines Backups einen stabilen Zustand wiederherstellen kann, für eine forensische Analyse erforderliche Daten aber eventuell zerstört werden.

Je nach Ausrichtung der Organisation und damit der Wichtigkeit der IT-Systeme für den Geschäftszweck, ist die Erstellung spezieller Cyber-Krisenmanagementpläne ratsam.

Für die Cyber-Krisenmanagementpläne eines „National Research and Education Networks“ (NREN) sind Branchen-inhärente Besonderheiten zu beachten. Krisen, die einen Netzanbieter betreffen, haben wahrscheinlich einen Einfluss auf die Netzverfügbarkeit oder deren Vertrauenswürdigkeit und somit einen Einfluss auf die üblichen Kommunikationswege E-Mail und IP-Telefonie. Ein Krisenmanagementplan sollte daher Vorkehrungen für den Verlust dieser Medien treffen, um die Handlungsfähigkeit des Krisenmanagementteams zu gewährleisten. Durch die Beeinträchtigung des Netzwerks kann auch die Kommunikation mit den betroffenen Einrichtungen und Nutzern gestört sein, da zum Beispiel das Veröffentlichen einer Webseite nicht möglich ist. Auch diese Besonderheit muss gegebenenfalls bei der Planung berücksichtigt werden.

Der Weg zum Krisenmanagement

Als erster Schritt kann ein Plan mit vereinheitlichten Prozeduren und definierten Startpunkten aufgestellt und intern publiziert werden. Dieser Plan umfasst die Zusammensetzung eines Krisenmanagementteams, die jeweiligen Aufgaben und Verantwortlichkeiten im Team, aber auch die Kompetenzen der einzelnen Rollen. Außerdem sollten generelle Prozeduren beschrieben werden zum Beispiel für die Alarmierung und Eskalation sowie Prozesse für die Krisenkommunikation und die Koordination zum Zweck einer Entscheidungsfindung.

Im nächsten Schritt kann eine Liste möglicher Krisenszenarien auf Grundlage des eigenen Arbeitsumfelds erstellt werden. Krisensituationen zeichnen sich unter anderem dadurch aus, dass sie einen signifikanten Schaden für die Organisation zur Folge haben können und mit den üblichen Prozeduren nicht mehr steuerbar sind. Eine Auflistung möglicher Krisenszenarien vereinfacht es, eine Krise zu erkennen und hilft auch das Überraschungsmoment etwas zu reduzieren.

Im letzten Schritt können die entstandenen Krisenmanagementpläne durch Übungen getestet und die Beschäftigten im Umgang mit Krisen geschult werden.

Hier setzt das Tutorium Crisis Management Exercise an:
Während der Krisensimulation werden die Teilnehmerinnen und Teilnehmer des Tutoriums zu Beschäftigten des Forschungsnetzes des Königraiche Guilder (Guilder Kingdom Research & Education Network GuilREN).

Die Bildungsministerin des Königreichs, Helga Buttercup hat ein Projekt zur Digitalisierung initiiert: Erstmalig sollen alle Studierenden über ein zentrales Webportal statt per Brief die Informationen über ihre Zulassung erhalten. Alle 18 in Guilder existierenden und über GuilREN vernetzen Universitäten nehmen an diesem Projekt teil. Aufgrund einer erst kürzlich bekannt gewordenen Anforderung bzgl. der Einspruchsfrist muss der Tag zur Übermittlung der Zulassungsdaten vorverlegt werden. Während vier kleinere Universitäten

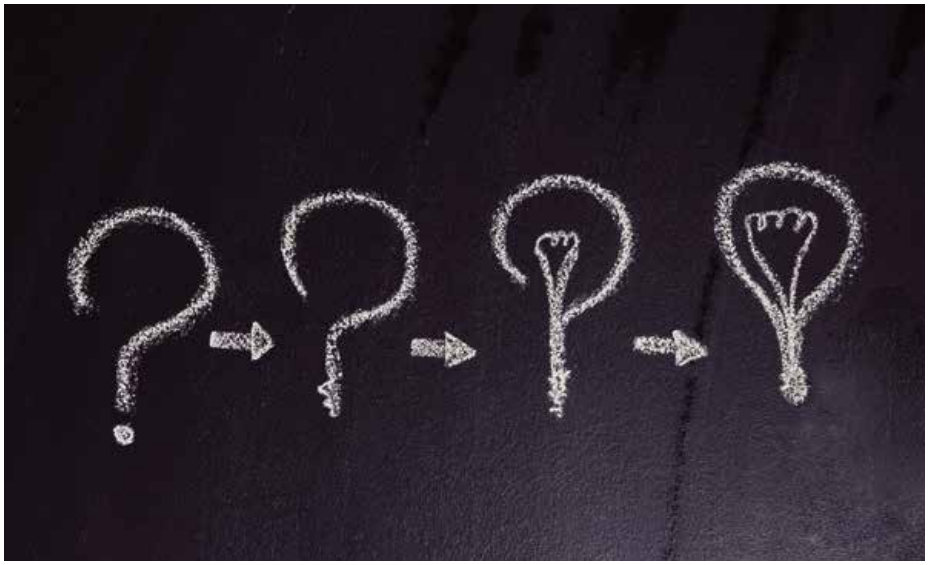


Foto: David-W-/photocase.de

ihre Daten bereits übermittelt haben, müssen die restlichen 14 Universitäten dies bis 11:00 Uhr am heutigen Tage tun …

An dieser Stelle verlieren die Universitäten ihre Netzwerkverbindung und die Teilnehmerinnen und Teilnehmer der Übung, aufgeteilt in Gruppen mit maximal zwölf Personen in vier Teams, versuchen den Schaden für GuilREN, für die angeschlossenen Universitäten und letztlich für die Ministerin Helga Buttercup zu minimieren.

Reale Voraussetzungen für eine optimale Stresssituation

Die vier Teams bestehen aus jeweils drei Personen und sind in die Bereiche NOC, CERT, Management und Communications unterteilt. Die Übung gliedert sich in eine Einführungsrunde und sechs jeweils 15-minütige Simulationsrunden. Während dieser Zeit versuchen die Übungsleiter, Charlie van Gnuchten (SURFnet – Forschungsnetz Niederlande) und Simon Jensen (Deic – Forschungsnetz Dänemark), die Teilnehmer in eine möglichst reale Stresssituation zu versetzen. So müssen die Teilnehmer innerhalb der 15-minütigen Simulationsrunden neu verfügbare Informationen sichten und filtern, die daraus gewonnenen Informationen mit den anderen Teams austauschen und eine nächste daraus resultierende Aktion planen. Nebenbei müssen außerdem von extern eingehende Anrufe beantwortet werden.

Um möglichst reale Bedingungen zu schaffen, greifen die beiden Leiter der Übung durchaus tief in die Trickkiste und lenken die Teilnehmer durch kleine Nachrichtenvideos, die bei der Problemlösung nicht weiterhelfen, ab. Außerdem übermitteln sie einzelnen Teams sehr viele, nicht notwendige Informationen und lassen technisch wichtige Details beim Kommunikationsteam auflaufen statt beim CERT oder NOC. Beherrscht wird der ganze Raum zudem von einer übergroßen Uhr, die gnadenlos die Sekunden herunterzählt und die Entscheidung über die nächste Handlung einfordert.

Crisis Management für die europäische Forschungsnetzcommunity

Auch wenn die Übung natürlich Spaß machen soll, so sollte sie den Teilnehmern vor allem bewusst machen, dass technische Expertise zwar sicherlich einen wichtigen Baustein zur Bewältigung einer Krise darstellt, dass aber die interne Kommunikation, eine im Einklang mit der eigenen Rolle stehende Priorisierung von Aufgaben sowie die Übernahme der Führungsverantwortung durch das Management unabdingbar sind, um eine Krise letztlich erfolgreich bewältigen zu können.

Entwickelt wurde die Übung im Rahmen des GÉANT-GN4-3-Projekts *Work Package 8 ‚Security'*. Sie wurde erstmalig im vergangenen Jahr bei dem Crisis-Management-Event CLAW 2019 durchgeführt. CLAW ist die Fortführung einer bereits zuvor durch GÉANT unterstützten Initiative zum Krisenmanagement in NRENs und hat mittlerweile das dritte Jahr in Folge stattgefunden. Die Krisenmanagementübung wurde unter besonderer Beachtung der Anforderungen von und für NRENs konzipiert, sie richtet sich dabei ausdrücklich nicht nur an IT-Experten, sondern auch an Beschäftigte aus dem Management und dem Bereich Kommunikation. Tatsächlich lautet die Empfehlung, Mitarbeiterinnen und Mitarbeiter aus jedem der an der Übung teilnehmenden Teams, also NOC, CERT, Management und Kommunikation zu einer Übung zu entsenden.

Die Anfänge von CLAW liegen in Crisis-Management-Aktivitäten, die SURFnet im Jahr 2016 mit zwei Projekten startete. Im darauffolgenden Jahr fand CLAW, basierend auf einem dieser Projekte für GÉANT, erstmals in Malaga statt und wenngleich die damalige Übung noch nicht so perfekt durchgeplant war wie die jüngst im Tutorium durchgeführte, so stand für alle Teilnehmerinnen und Teilnehmer hinterher fest: Davon brauchen wir mehr. Das ist wichtig.

So zieht CLAW jährlich etwa 100 Teilnehmerinnen und Teilnehmer von verschiedenen Forschungsnetzen an und versucht mit spezifischen Vorträgen und Trainings zusätzlich zu einer jeweils neuen Crisis-Management-Übung die Beteiligten anzuregen, das Thema in die eigene Organisation hineinzutragen, dort weiter zu verfolgen und zu hinterfragen.

Und auch wenn alle hoffen, ihn niemals zu benötigen, so ist es sicherlich gut, einen Krisenmanagementplan in der Schublade zu haben. ◆

Sicherheit aktuell

Reduzierung der Laufzeit von Serverzertifikaten

Der Trend die Laufzeit von Serverzertifikaten zu verkürzen wird fortgesetzt. Im nächsten Schritt wird ab 1. September 2020 die maximale Gültigkeitsdauer von den großen Softwareherstellern im Alleingang von 825 Tagen auf 398 Tage reduziert, nachdem eine entsprechende Standardisierung im Certification-Authority-Browser-Forum zuvor gescheitert war.

Der Hauptgrund für die immer weitere Verkürzung der Lebensdauer der Zertifikate ist aus Sicht der Browser- und Betriebssystemhersteller das Fehlen von funktionierenden Widerrufsmechanismen, mit denen ein Zertifikat zurückgezogen werden kann. Sperrlisten (CRLS) und das Online Certificate Status Protocol (OCSP) sind daher mittlerweile in einigen Browsern standardmäßig abgeschaltet, werden von der DFN-PKI aber natürlich weiterhin standardkonform bereitgestellt.

Wir möchten in diesem Zusammenhang auf die bestehenden Automatisierungsmöglichkeiten in der DFN-PKI per Web-Service-Schnittstelle (https://blog.pki.dfn.de/tag/soapclient-releases/) hinweisen. Bitte sprechen Sie uns vorab an, falls Sie automatisierte Workflows einrichten möchten – der Teufel steckt hier im Detail. Des Weiteren arbeiten wir an der Abschaffung des bisherigen Papierformulars für Serverzertifikate, wodurch der Aufwand bei der manuellen Beantragung von Serverzertifikaten reduziert wird. ◆

Illustration: Golden Sikorka/Adobe Stock

Illustration: Golden Sikorka/Adobe Stock

Video-Identifizierung durch den Teilnehmerservice

Die Ausstellung von Nutzerzertifikaten in der DFN-PKI setzt in der Regel die persönliche Anwesenheit des Antragstellers voraus. Aufgrund von Homeoffice-Regelungen und Social Distancing im Kontext der COVID-19-Pandemie war dies nicht mehr angemessen. Daher steht seit Ende April 2020 ein Verfahren zur Identifizierung über Video-Chat zur Verfügung, das jeder Teilnehmerservice der DFN-PKI selbst durchführen kann. Voraussetzung hierfür sind eine gründliche Durchsicht der Richtlinie zur Video-Identifizierung und eine einmalige Dokumentation der Selbstschulung. Als Zusatz zum normalen Antragsformular muss eine separate Checkliste zur Video-Identifizierung verwendet werden, um einen korrekten Ablauf sicherzustellen.

Alle Dokumente und die Checkliste, die zu dem Verfahren gehören, finden Teilnehmerservice-Mitarbeiterinnen und -Mitarbeiter an den teilnehmenden Einrichtungen unter https://www.pki.dfn.de/policies/videoident/. Falls Sie ein Zertifikat beantragen möchten, wenden Sie sich bitte an den lokalen Teilnehmerservice Ihrer Einrichtung. ◆

Änderungen im Common Vulnerability Scoring System (CVSS) von Version 2.0 auf 3.1

Ende Februar 2020 wurde das DFN-CERT-Portal auf die Softwareversion 1.4 aktualisiert. Damit wurde insbesondere eine Umstellung der Bewertung von Schwachstellenmeldungen gemäß Common Vulnerability Scoring System (CVSS) von Version 2.0 auf Version 3.1 vorgenommen.

Die konzeptionell größte Änderung der CVSS-Spezifikation zwischen Version 2.0 und 3.1 ist in der neu eingeführten Basismetrik „Scope" (kurz für Authorization Scope, etwa: Ermächtigungsrahmen) zu finden. Ganz allgemein ist ein Scope ein abgeschlossener Rahmen, in dem Rechenressourcen verwaltet werden. Ein Scope kann beispielsweise eine Webanwendung mit Benutzerverwaltung darstellen. Der Browser, mit dem eine solche Webanwendung aufgerufen wird, befindet sich in einem anderen Scope: dem Betriebssystem des Benutzers mit wieder eigener Rechteverwaltung. Wurde bei CVSSv2.0 der Einfluss (Vertraulichkeit, Integrität, Verfügbarkeit) einer Schwachstelle auf das gesamte System des Benutzers bewertet, wird seit Version 3.0 zwischen der verwundbaren Komponente und der betroffenen Komponente unterschieden. Liegen beide Komponenten in unterschiedlichen Scopes, beispielsweise Webanwendung als verwundbare Komponente und Browser als betroffene Komponente bei einem Cross-Site-Scripting (XSS)-Angriff, kann diese Information nun entsprechend berücksichtigt werden und der Scope wird als Changed (C) definiert.

- **Scope (S): Unchanged (U), Changed (C)**
  → Ist die verwundbare Komponente auch die einzig betroffene Komponente?

Unverändert erhalten Schwachstellen einen Score zwischen 0 und 10, für dessen Berechnung zusätzlich zum erläuterten Scope zwei weitere neue Ausnutzbarkeits-Metriken (Exploitability Metrics) eingeführt wurden:

- **User Interaction (UI): None (N), Required (R)**
  → Ist eine Benutzerinteraktion erforderlich, um die Schwachstelle auszunutzen?

Bisher wurde dieser Aspekt in der Access Complexity berücksichtigt.

- **Privileges Required (PR): None (N), Low (L), High (H)**
  → Welche Privilegien benötigt der Angreifer im Kontext der betroffenen Komponente?

Hier wird im Wesentlichen zwischen Benutzer- und Administratorrechten unterschieden. Dieser Parameter ersetzt den zuvor verwendeten Wert Authentication (AU).

Als zusätzlicher Angriffsvektor (Attack Vector, AV) kann jetzt auch physischer Zugriff angegeben werden:

- Physical (P)

Bei CVSSv2.0 fielen solche Angriffe in die Einstufung Local (L) des Zugriffsvektors (Access Vector, AV). Insgesamt orientiert sich der Attack Vector an der Frage, ob die verwundbare Komponente an den Netzwerkstack gebunden ist oder nicht bzw. ob für den antizipierten Angriff eine Netzwerkverbindung erforderlich ist. Ist die Bindung an den Netzwerkstack gegeben, kann der Angriff aus dem Netzwerk (N) oder aus dem benachbarten Netzwerk (Adjacent, A) erfolgen. Ist die Bindung an den Netzwerkstack nicht gegeben, kommen als Angriffsvektor Local (L) oder Physical (P) infrage.

Die Metriken zu Vertraulichkeit Confidentiality (C), Integrität Integrity (I) und Verfügbarkeit Availability (A) erhalten jetzt die Werte:

- None (N),
- Low (L),
- High (H)

Diese Werte sind auf die beeinträchtigte Komponente bezogen statt zuvor mit None (N), Partial (P) und Complete (C) auf das Gesamtsystem des Benutzers. Für das Ausspähen weniger, aber kritischer Informationen wird mit CVSSv3.1 beispielsweise der Einfluss auf die Vertraulichkeit auf „High" gesetzt, um der Kritikalität der ausgespähten Daten Rechnung zu tragen. Der entsprechende Wert „Complete" bei CVSSv2.0 entspräche dem Vollzugriff auf alle Daten des betroffenen Systems. Bisher musste in solchen Fällen der Einfluss auf die Vertraulichkeit lediglich mit „Partial" bewertet werden. ◆

WEITERE INFORMATIONEN

Weitere Informationen zu [CVSSv3.1][1] finden sich bei den Kollegen von FIRST im Common Vulnerability Scoring System v3.1: Specification Document. Die Entwicklung des CVSSs erfolgt durch eine [Special Interest Group (SIG)][2].

[1]: **https://www.first.org/cvss/v3.1/specification-document**
[2]: **https://www.first.org/cvss/**

Konfiguration von TLS-Servern

Es ist gute Praxis, jeden Dienst mit Transport Layer Security (TLS) zu sichern, um eine Verschlüsselung der Verbindung und eine Authentifizierung des Dienstes gegenüber dem Nutzer oder Client zu erreichen. Ungesicherte Web-Server, IMAP- oder SMTP-Zugänge oder Datenbankverbindungen entsprechen seit Längerem nicht mehr dem Stand der Technik.

Dabei ist die regelmäßige Anpassung der TLS-Konfiguration der Server notwendig, um die Sicherheit der Verbindungen dauerhaft zu gewährleisten. Diese Anpassung sollte in einer Organisation wie einem Rechenzentrum idealerweise als Prozess verankert werden, der zum Beispiel alle 18 Monate durchlaufen wird.

Nachdem im ersten Halbjahr 2020 große Browser-Hersteller Updates herausgebracht haben, mit denen der Support für die TLS Versionen 1.0 und 1.1 entfernt wurde, ist, sofern noch nicht geschehen, jetzt eine Überprüfung und gegebenenfalls Aktualisierung der TLS-Konfiguration sinnvoll. Sollten Server eingesetzt werden, die noch keine TLS Version 1.2 unterstützen, ist dringend ein Upgrade anzuraten. Grundsätzlich sollten alle Server-Betriebssysteme, die in 2020 noch Support haben, TLS 1.2 zur Verfügung stellen.

Es empfiehlt sich, insbesondere ältere Installationen mit Werkzeugen wie https://ssllabs.com/ssltest oder https://testssl.sh auf Konfigurationsmängel oder veraltete Parameter zu überprüfen. Generell sind folgende Maßnahmen sinnvoll, um eine sichere TLS-Konfiguration zu erreichen:

- TLS 1.0 und 1.1 abschalten
- Cipher Suites mit ECDHE bzw. DHE und GCM, evtl.zusätzlich CHACHA20-POLY1305, auswählen
- möglichst alle anderen Algorithmen abschalten

Hilfestellung für eine gute TLS-Konfiguration bietet der „Mozilla SSL Configurator“ https://ssl-config.mozilla.org/, bei dem man sich für die verschiedensten Server-Systeme Konfigurationen mit einem gewünschten Level „Modern“, Intermediate“ und „Old“ ausgeben lassen kann.

Die DFN-PKI hat auf ihren Servern die folgende Konfiguration aktiviert (hier für Apache):

```
SSLProtocol all -SSLv2
-SSLv3 -TLSv1 -TLSv1.1

SSLHonorCipherOrder On

SSLCipherSuite ‚EC-
DHE-RSA-AES256-GCM-
SHA384:DHE-RSA-AES256-
GCM-SHA384:ECDHE-RSA-
AES128-GCM-SHA256:DHE-
RSA-AES128-GCM-SHA256‘
```

Hierbei sind allerdings auch Kompatibilitätsaspekte zu betrachten. Zu einem so konfigurierten Server können beispielsweise die folgenden veralteten Clients keine Verbindung mehr aufnehmen: Safari <= 8, WinPhone 8.1, IE 8-10 auf Win7, Android <= 4.3, Java <= 7, Python <= 2.6.

Mit besonderer Vorsicht muss bei Spezial-Servern vorgegangen werden, die von Clients mit Custom-Software angesprochen werden. Custom-Software wird in vielen Fällen nicht regelmäßig aktualisiert, sodass sie unter Umständen noch nicht TLS-1.2-fähig ist. Dies kann entweder an fehlenden TLS-1.2-Funktionen des Basis-Systems liegen (wie zum Beispiel Python 2.6), oder aber an verwendeten Programmkonstrukten, die moderne TLS-Konfigurationen ausschließen. Es sind Beispiele für Software unter Java 8 bekannt, die aufgrund von unglücklich verwendeten Funktionsaufrufen nicht TLS 1.2-fähig sind. Auch Software unter Python 2.7 unterstützt nicht in jedem Fall automatisch TLS 1.2.

Es ist daher sinnvoll, eine Umstellung der TLS-Konfiguration eines Servers als Projekt zu behandeln. Eine genaue Betrachtung der Nutzer und Clients dieses Servers und sorgfältige Tests können in vielen Fällen erforderlich sein.

Dieser Aufwand mag hoch erscheinen und für Systeme, die doch eigentlich problemlos laufen, als unnötig empfunden werden, ist aber notwendig, da eine sichere TLS-Konfiguration zum Stand der Technik gehört. ◆

MITARBEIT AN DIESER AUSGABE DER SICHERHEIT AKTUELL:

Heike Ausserfeld, Jürgen Brauckmann, Ralf Gröper, Christine Kahl, Martin Waleczek

KONTAKT

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

Zuhause ist es doch nicht am schönsten?

Die vorübergehende Verweisung einer Beamtin ins Homeoffice entspricht einer amtsangemessenen Beschäftigung

Die Bedrohung durch das Coronavirus macht auch im öffentlichen Dienst die Arbeit aus dem heimischen Büro zur Notwendigkeit. In diesem Zusammenhang stellt sich insbesondere die Frage, welche Besonderheiten im Beamtenverhältnis im Gegensatz zur gewöhnlichen Angestelltensituation zu beachten sind und wie sehr die Rechtslage derzeit durch die akute Gefährdung beeinflusst wird.

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

Foto: peshkov/Adobe Stock

I. Sachverhalt

Mitte April dieses Jahres hat das Verwaltungsgericht Berlin (VG Berlin) einen Eilantrag abgelehnt, in welchem eine Angestellte des öffentlichen Dienstes bat, festzustellen, dass die Verlegung ihrer Tätigkeit ins Homeoffice, wie sie durch den Dienstherrn angeordnet wurde, keiner amtsangemessenen Beschäftigung entspricht und jeglicher Rechtsgrundlage entbehrt (VG Berlin vom 14.4.2020, 28 L 119.20). Die 60-Jährige war der Meinung, dass die Verlegung ins heimische Büro nur auf ihren Antrag erfolgen könne, nicht aber auf Anweisung des Dienstherrn. Dieser hat die Frau aufgrund ihrer größeren Gefährdung einer Infektion mit dem Coronavirus auf die Arbeit von zu Hause verwiesen. Mit 60 Jahren fällt sie in die von mehreren Stellen ausgewiesene Risikogruppe.

Problematisch war in den Augen der Angestellten vor allem auch die fehlende technische Infrastruktur (Dienstrechner, Diensthandy) im Homeoffice. Das VG Berlin stützt seine Entscheidung, den Eilantrag abzulehnen, auch darauf, dass der Zeitraum der Heimarbeit mit einer Befristung zum 17. April 2020 nur einen sehr beschränkten Zeitraum betrifft und die anfallenden Aufgaben trotz geringerer Mittel ausreichend bearbeitet werden können.

II. Amtsangemessene Beschäftigung

Schon grundgesetzlich in Art. 33 Abs. 5 Grundgesetz (GG) angeknüpft als hergebrachter Grundsatz des Berufsbeamtentums steht Beamten eine amtsangemessene Beschäftigung zu. Jegliche überwiesene Tätigkeit muss dem abstrakten Aufgabenbereich des statusrechtlichen Amtes entsprechen. Das bedeutet nicht, dass keinerlei Änderungen der Beschäftigungen hinzunehmen sind. Vielmehr ist im Einzelfall abzuwägen, inwiefern Beschäftigungsänderungen mit dem übertragenen Amt zu vereinbaren sind. Es muss ein sog. „amtsangemessener Tätigkeitsbereich“ verbleiben. Die Verlagerung der gewöhnlichen Tätigkeit, soweit möglich, in das Homeoffice stellt nach der Entscheidung des VG Berlin eine Verschiebung in einen amtsangemessenen Tätigkeitsbereich dar. Auch wenn nicht die gleiche Ausstattung im heimischen Büro bzw. Behelfsbüro vorhanden ist wie an der üblichen Arbeitsstätte, ist die Tätigkeit von zu Hause nach wie vor amtsangemessen. Das VG Berlin entschied ferner, dass selbst bei einer bloßen Rufbereitschaft im Homeoffice und keiner konkreten weiteren Aufgabenzuweisung für beschränkte Zeit keine amtsunangemessene Beschäftigung vorliegt.

III. Sonderfall Coronavirus

Im behandelten Fall ist der Sonderfaktor Coronavirus mit einzuberechnen. Die Bedrohung ist gerade auch für öffentliche Stellen akut und real. Besonders ältere Mitarbeiter und solche mit Vorerkrankung sind in dieser Zeit zu schützen. Die Verweisung der Beamten ins Homeoffice ist, soweit diese Möglichkeit auch nur in Ansätzen besteht, weniger eine Schikane als vielmehr eine Pflicht des Dienstherrn. Diesem ist eine Fürsorgepflicht gegenüber seinen Angestellten auferlegt.

> Dem Dienstherrn ist eine Fürsorgepflicht gegenüber Angestellten auferlegt

Auch wenn sich die Tätigkeit in der vorübergehenden Zeit der Verweisung ins Homeoffice auf eine Rufbereitschaft beschränken sollte, ist dies im vorliegenden Ausnahmefall gerechtfertigt.

Die so noch nicht dagewesene Bedrohung durch das Coronavirus führt nicht nur zur zwingenden Einhaltung der Fürsorgepflicht des Diensthabenden, sondern auch zu einem verschobenen Maßstab dessen, was Mitarbeiter zur Verhinderung einer Infektion hinzunehmen haben. Insbesondere auch im Lichte des Art. 2 Abs. 2 GG, welcher den Schutz der körperlichen Unversehrtheit ins Grundgesetz zementiert, wird die Pflicht des Staates, seine Bürger und eben auch Angestellten zu schützen, bewusst. Die Verweisung ins HomeoOffice im Normalfall könnte zu einer amtsunangemessenen Beschäftigung führen. Unter momentanen Umständen ist das aber nicht der Fall.

IV. Rechtliche Besonderheiten

Erst vor kurzer Zeit hat das Landesarbeitsgericht (LAG) Berlin-Brandenburg die einseitige Verweisung des Arbeitnehmers ins Homeoffice als nicht verpflichtend angesehen.[1] Für Beamte gilt in ihrem Sonderstatusverhältnis zum Staat allerdings nach dieser aktuellen Entscheidung etwas anderes. Das Verhältnis zwischen staatlichem Arbeitgeber und Beamten regelt in Deutschland gesondert das Beamtenrecht als Teil des öffentlichen Rechts. Es besteht eben gerade kein zivilrechtlich geregeltes vertragliches Arbeitsverhältnis auf Augenhöhe. Vielmehr ist das Beamtenrecht einseitig hoheitlich durch Gesetz geregelt. Dieses „besondere“ Arbeitsverhältnis ist auch der Grund dafür, dass über den vorliegenden Antrag das Verwaltungsgericht entschieden hat und nicht das Arbeitsgericht.

1 Urteil vom 10. Oktober 2018, Az: 17 Sa 562/18; zu dieser Entschei-dung ausführlich: Uphues, Ich werde ihm ein Angebot machen, das er ablehnen kann, DFN-Infobrief 02/2019.

Neben dem Beamtenrecht ist für die Heimarbeit auch das Datenschutzrecht von Bedeutung. Durch den zwangsläufigen Einsatz von Fernkommunikationsmitteln kommt es in dieser Situation mit sehr großer Wahrscheinlichkeit zu einer zusätzlichen Verarbeitung von personenbezogenen Daten sowohl durch den Diensthabenden als auch Dritte. Diese Verarbeitung bedarf sowohl einer Rechtsgrundlage als auch der Einhaltung der weiteren datenschutzrechtlichen Regeln. Die Grundsätze für die Verarbeitung personenbezogener Daten sind Art. 5 Datenschutz-Grundverordnung (DSGVO) zu entnehmen.

Eine weitere Besonderheit ergibt sich für Beamte im Homeoffice aus versicherungsrechtlicher Sicht. Im Gegensatz zu herkömmlichen Angestellten ist ein Beamter nicht durch die gesetzliche Unfallversicherung abgesichert, sondern genießt beamtenrechtliche Fürsorge. Regelungen hierzu finden sich im Beamtenversorgungsgesetz (BeamtVG). Im Beamtenrecht gilt grundsätzlich das Dienstgebäude als unfallfürsorgerechtlich geschützter Risikobereich des Dienstherrn. Ist dem Beamten die Heimarbeit

> Erfolgt die Arbeit im Home-Office aufgrund einer Dienstanweisung, ist ein Unfall als Dienstunfall zu sehen

freigestellt und verlässt er diesen geschützten Bereich ohne direkte Anweisung, ist ein Unfall regelmäßig nicht als Dienstunfall zu werten. Hierfür müsste der Unfall seine wesentliche Ursache in einer dienstlichen Verrichtung finden. Erfolgt die Arbeit des Beamten allerdings aufgrund einer eindeutigen Dienstanweisung aus dem Homeoffice und es ereignet sich in diesem Zuge ein Unfall, ist dieser wohl in aller Regel als Dienstunfall zu sehen und eine entsprechende fürsorgerechtliche Absicherung gegeben. Ein herkömmlicher Arbeitnehmer ist regelmäßig schon dann versichert, wenn der Unfall an einem Ort erfolgt, der auch wesentlich den Betriebszwecken dient. Dies trifft auf das Homeoffice zu, unabhängig von einer direkten Anweisung von zu Hause aus zu arbeiten.

V. Fazit und Konsequenzen für die Praxis in wissenschaftlichen Einrichtungen

Auch im staatlichen Hochschul- und Forschungsbetrieb werden zurzeit nach Möglichkeit alle Stellen im heimischen Büro fortgeführt. Das Zurückweisen des Eilantrages durch das VG Berlin zeigt, dass die Anweisung von Vorgesetzen an ihre angestellten Beamten die Arbeit im Homeoffice fortzuführen nicht nur der Fürsorgepflicht entspricht, sondern, insofern es sich nur um einen vorübergehenden Zustand handelt, mit einer amtsangemessenen Beschäftigung zu vereinbaren ist. Für die Zukunft wird vor allem auch die zeitliche Komponente interessant. Die vorliegende Entscheidung stützt sich unter anderem darauf, dass die Verweisung ins Homeoffice nur für wenige Wochen gilt und damit eine geringe Belastung darstellt. Zurzeit ist aber noch nicht klar absehbar, wann die Heimarbeit ohne großes Risiko wieder aufgehoben werden kann. Es wird früher oder später zu entscheiden sein, wann ein Zeitraum im Homeoffice nicht mehr einer amtsangemessenen Beschäftigung entspricht. Die Entwicklungen und zukünftigen gerichtlichen Einstufungen sind abzuwarten. ◆

Ausgeknipst!

Ende des Schutzes für Reproduktionsfotografien durch Art. 14 DSM-RL

Mit der Reform des europäischen Urheberrechts wurde das Ende des Schutzes von Reproduktionsfotografien gemeinfreier Werke eingeläutet. Der Wegfall dieses zuletzt sehr umstrittenen Schutzes ist ein Gewinn für den freien Wissensaustausch. Auch für Hochschulen, die Sammlungen gemeinfreier Werke haben, bringt die Veränderung überwiegend Vorteile. Der Beitrag soll erklären, warum es den Reproduktionsschutz gemeinfreier Werke überhaupt gab, warum er abgeschafft wurde und welche Bedeutung diese Änderung für Hochschulen und Wissenschaft hat.

Text: **Marten Tiessen** (Forschungsstelle Recht im DFN)

Foto maxexphoto / iStock

I. Das Leistungsschutzrecht nach § 72 UrhG

Während bereits der Lichtbildschutz immer mehr die Frage nach seiner Zeitgemäßheit aufwirft, stellt insbesondere der bislang mitumfasste Schutz von Reproduktionsfotografien gemeinfreier Werke ein rechtliches Kuriosum dar. Um das zu verstehen, sollen zunächst kurz die wichtigsten Aspekte des Lichtbildschutzes erläutert werden.

§ 72 UrhG stellt Lichtbilder und Erzeugnisse, die ähnlich wie Lichtbilder hergestellt werden unter den Schutz eines sogenannten Leistungsschutzrechts. In den Anwendungsbereich fallen in erster Linie Fotografien, aber auch durch andere Techniken entstandene Bilder, wie medizinische Röntgenbilder, gehören dazu. Leistungsschutzrechte unterscheiden sich vom Urheberrecht darin, dass sie keine persönlichen geistigen Schöpfungen schützen, sondern Leistungen von ausübenden Künstlern oder Leistungen auf organisatorisch-technischem Gebiet. Unter den zweiten Punkt fallen z. B. Leistungen von Filmherstellern, Tonträgerherstellern, Veranstaltern und Presseverlegern. Leistungsschutzrechte schützen hier nicht das kreative Schaffen, sondern unternehmerische Investitionen, die im Zusammenhang mit der Vermittlung von fremden Werken an die Öffentlichkeit stehen. Der Lichtbildschutz nimmt unter den Leistungsschutzrechten eine Sonderrolle ein. Zwar zählt er zu den Leistungsschutzrechten, vom Schutzumfang ist er allerdings dem Urheberrecht viel näher. Auch schützt er weder eine besondere technische Leistung, noch eine außergewöhnliche persönliche Fertigkeit. Sein Zweck ist hingegen, den Fotografen vor Abgrenzungsschwierigkeiten zu dem urheberrechtlichen Lichtbildwerkschutz zu bewahren. Denn eigentlich ist für Fotografien bereits ein eigener urheberrechtlicher Schutz vorgesehen. Die Voraussetzung dafür ist aber – wie übrigens bei allen Werken –, dass sie das Maß an Individualität einer geistigen persönlichen Schöpfung nach § 2 Abs. 2 UrhG erreichen. Diese Schöpfungshöhe, die das Werk von simplen Alltagserzeugnissen abgrenzen soll, erreichen viele Fotografien nicht. Das ist wenig verwunderlich, wenn man allein an die unzähligen Schnappschüsse denkt, die täglich mit Handykameras geschossen werden.

Illustration: SiberianPhotographer/Adobe Stock

Wann allerdings die Schöpfungshöhe erreicht ist und welche Merkmale ein Foto dafür aufweisen muss, lässt sich nicht pauschal beantworten, sondern muss bei jedem Bild einzeln beurteilt werden. Um diese Abgrenzungsschwierigkeiten nicht dem Fotografen aufzubürden, entschied sich der Gesetzgeber dafür, die einfacheren Lichtbilder ebenfalls unter Schutz zu stellen. Der sich daraus ergebende Leistungsschutz von Lichtbildern orientiert sich nach § 72 Abs. 1 UrhG inhaltlich weitestgehend an dem Schutz für Lichtbildwerke. Der einzige wesentliche Unterschied ist die Schutzdauer, die bei urheberrechtlichen Werken 70 Jahre nach dem Tod des Urhebers endet und bei Lichtbildern 50 Jahre nach dem Erscheinen des Lichtbildes erlischt.

II. Reproduktionsfotografie

Unter diesen Lichtbildschutz fallen bisher auch die sogenannten Reproduktionsfotografien, die ein Werk möglichst originalgetreu wiedergeben. Sie sind von rein technischen Reproduktionen, die keinen Lichtbildschutz genießen, zu unterscheiden. Während die technische Reproduktion eine reine Vervielfältigung eines Originalwerkes darstellt, setzt eine geschützte fotografische Reproduktion voraus, dass der Fotograf zumindest ein Mindestmaß an Gestaltungsspielraum nutzt. Der soll bereits gegeben sein, wenn er eine andere Werkart, wie z. B. ein Gemälde, zu einer Fotografie transformiert. Die gestalterische Leistung kann auch in der Berücksichtigung der besonderen Lichtverhältnisse oder in anderen technischen Schwierigkeiten gesehen werden. Wie groß dieser Gestaltungsspielraum sein muss und wann er im Einzelfall ausgenutzt sein soll, wurde bislang in der Rechtswissenschaft uneinheitlich bewertet. Ein Lichtbild von einem Lichtbild soll zumindest nicht mehr dem Schutz unterfallen, da es dann zu einer unendlichen Verlängerung der Schutzfrist des ursprünglichen Bildes kommen könnte.

> Ein Lichtbild von einem Lichtbild soll zumindest nicht mehr dem Schutz unterfallen

Ein ähnliches Problem ergibt sich jedoch auch bei dem Schutz von Reproduktionsfotografien gemeinfreier Werke. Gemeinfrei sind ehemals urheberrechtlich geschützte Werke, bei denen inzwischen die Schutzfrist abgelaufen ist und somit das ursprüngliche Schutzinteresse des Urhebers hinter dem Zugangsinteresse der Allgemeinheit zurücktritt. Nimmt man den Schutz von Reproduktionsfotografien dieser Werke an, verlängert sich zwar nicht die

Schutzdauer des Ursprungswerkes, aber die nahezu identische fotografische Replik ist dann geschützt. Das ist besonders gravierend, wenn die Allgemeinheit keinen Zugang zum Originalwerk hat, sondern nur zu den Reproduktionsfotografien. Denn wer den Zugang zu dem Werk kontrolliert, kann auch kontrollieren, welche Fotografien davon angefertigt werden, und somit letztlich bestimmen, wie mit den Vervielfältigungen umzugehen ist. Die Gemeinfreiheit, die der Allgemeinheit die Werknutzung nach Ablauf der Schutzfrist ermöglichen soll, wird dadurch untermi-

> Ein Auslöser des Rechtsstreits war der Upload von Reproduktionsfotografien

niert. Einrichtungen, die gemeinfreie Werke ausstellen, haben dagegen ein Interesse am Fortbestand des Schutzes. Sie hoffen auf höhere Besucherzahlen durch den begrenzten Umlauf der Exponatsabbildungen und können die geschützten Motive über Postkarten und Ausstellungskataloge wirtschaftlich verwerten.

Dieser Widerspruch der unterschiedlichen Interessen wurde besonders deutlich, als die Reiss-Engelhorn-Museen in Stuttgart einen ehrenamtlichen Mitarbeiter von Wikimedia Commons verklagten.[1] Die Plattform Wikimedia Commons ist eine freie Datenbank von Bildern und anderen Medien, die mit dem Internetlexikon Wikipedia verknüpft ist und von jedermann kostenlos genutzt werden kann. Ein Auslöser des Rechtstreits war unter anderem, dass der Beklagte die in einem Museumskatalog enthaltenen Reproduktionsfotografien gemeinfreier Ausstellungsstücke auf die Plattform hochgeladen hatte. Dadurch sah sich das Museum in seinen Bildrechten verletzt. Der Streit wurde Ende 2018 schließlich durch den BGH, der Reproduktionsfotografien von gemeinfreien Werken den Lichtbildschutz zusprach, zugunsten der Museen entschieden (Urt. v. 20.12.2018 – I ZR 104/17). Bei diesem Ergebnis sollte es allerdings nicht lange bleiben.

III. Art. 14 DSM-RL

Im letzten Jahr kam es durch die europäische Reform zu erheblichen Veränderungen im Urheberrecht.[2] Davon ist auch der Lichtbildschutz für Reproduktionsfotografien betroffen. Nach Art. 14 DSM-RL sollen zukünftig Vervielfältigungen von Werken der bildenden Kunst nach Ablauf ihrer Schutzfrist weder urheberrechtlich noch durch verwandte Schutzrechte geschützt sein, es sei denn sie stellen eine eigene geistige Schöpfung dar. Als solches vervielfältigendes Material kommen auch Laufbilder in Betracht, also Filmsequenzen, die nicht die Voraussetzungen eines Werkes erfüllen. Allerdings wird der Hauptanwendungsfall die Reproduktion durch Lichtbilder sein. Andere Vervielfältigungsmethoden wie z. B. 3D-Druck wären zwar theoretisch von der Richtlinie umfasst, ihnen kommt aber nach deutschem Urheberrecht schon jetzt kein eigener Schutz zu.

Mit der Einführung von Art. 14 DSM-RL endete somit der noch wenige Monate vorher höchstrichterlich bestätigte Schutz der Reproduktionsfotografien. Allerdings mit einer Einschränkung: Art. 14 DSM-RL stellt nur die Reproduktionen von gemeinfreien Werken der bildenden Kunst frei. Auch wenn die Richtlinie selbst den Begriff der „bildenden Kunst“ nicht näher definiert, sind nach gängigem Verständnis darunter nicht nur klassische Werke, wie Gemälde, Grafiken und Plastiken, sondern ebenso Werke der angewandten Kunst und Bauwerke zu verstehen. Nach Erwägungsgrund 53 der DSM-RL sollen gerade im Bereich der bildenden Kunst die originalgetreuen Vervielfältigungen gemeinfreier Werke zum Zugang zur Kultur und ihrer Förderung und zum Zugang zum kulturellen Erbe beitragen. Wie unter anderem das Beispiel mit Wikimedia Commons zeigt, kommt es gerade in diesem Bereich zu den größten Einschränkungen der Gemeinfreiheit. Die Reform soll gemäß Erwägungsgrund 53 zusätzlich dabei helfen, die nationale Gesetzgebung in den Mitgliedstaaten in Hinblick auf Reproduktionsfotografien zu vereinheitlichen. Hier gab es bislang erhebliche Unterschiede, welche auch europaweiten Digitalisierungsvorhaben im Wege standen.

Art. 14 DSM-RL enthält allerdings kein Zugangsrecht zu Vervielfältigungen oder zum Originalwerk. Die Nutzung von Reproduktionsfotografien gemeinfreier Werke setzt voraus, dass solche überhaupt schon erschaffen wurden oder dass es zumindest die Möglichkeit gibt, selbst Reproduktionsfotografien anzufertigen. Letzteres kann aber derjenige, dem das Werk gehört oder bei dem es ausgestellt ist, nach wie vor unterbinden. Wie der BGH in seinem Urteil ausgeführt hat, kann ein Fotografieverbot wirksam in die allgemeinen Geschäftsbedingungen des Besuchervertrages einbezogen werden. Darüber hinaus ist fraglich, ob dem Eigentümer ein Recht am Bild der eigenen Sache zusteht. Dies ließ der BGH bislang offen.

Wie jede europäische Richtlinie findet auch die DSM-RL nicht direkt Anwendung, sondern muss erst in nationales Gesetz umge-

1 Siehe hierzu Tiessen, Kunst und Kopie, DFN-Infobrief Recht 1/2018 und Tiessen, Kunst unter Verschluss, DFN-Infobrief Recht 3/2019.

2 Zu den anderen wichtigen Änderungen durch die europäische Urheberrechtsreform siehe auch Gielen, Die neue urheberrechtliche Schranke zu Text- und Data-Mining, DFN-Infobrief Recht 12 / 2019; Gielen, First Rule: You Do Not Talk About Uploadfilter!, DFN-Infobrief Recht 1/2020; Tiessen, Vergriffen heißt nicht vergessen, DFN-Infobrief Recht 1/2020.

setzt werden. Zu der notwendigen Änderung des Urheberrechtsgesetzes hat der deutsche Gesetzgeber ab Inkrafttreten der Richtlinie zwei Jahre Zeit. Die Frist endet am 7. Juni 2021.

IV. Praxishinweise für Hochschulen und Forschungseinrichtungen

Viele Hochschulen sind im Besitz von umfangreichen Sammlungen ehemals urheberrechtlich geschützter Werke. Darunter befinden sich auch Sammlungen von Werken der bildenden Kunst. Inzwischen besteht ein Interesse daran, diese Werke nicht nur vor Ort zur Verfügung zu stellen, sondern sie auch digital nutzbar zu machen. Dafür ist es notwendig, dass Reproduktionsfotografien dieser Werke angefertigt werden. Wie bei anderen Schutzgegenständen des Urheberrechts mussten sich die Hochschulen dazu die Rechte an diesen Fotografien sichern. Denn das Recht am Lichtbild steht nicht automatisch der Hochschule zu, sondern nach § 72 Abs. 2 UrhG demjenigen, der es aufgenommen hat. Diese Rechteklärung ist zukünftig für Reproduktionsfotografien gemeinfreier Werke obsolet. Unklar ist hingegen noch, ob der einmal entstandene Lichtbildschutz einer Reproduktionsfotografie entfällt, sobald das abgelichtete Werk gemeinfrei wird.

Viele Hochschulen sind im Besitz von umfangreichen Sammlungen ehemals urheberrechtlich geschützter Werke

Neben der Rechteklärung vereinfacht die Neuregelung zudem das wissenschaftliche Arbeiten. Bislang ist die Abbildung von Reproduktionsfotografien gemeinfreier Werke in wissenschaftlichen Arbeiten nur möglich, wenn sie entweder im Rahmen eines Zitats nach § 51 UrhG verwendet wird oder aber die Rechte des Lichtbildners vorher eingeholt wurden. Da die Rechteeinräumung in der Regel zu kostspielig und aufwendig ist, bleibt nur die Möglichkeit des Zitats. Dafür muss die Verwendung aber den Zitatzweck erfüllen. Das setzt eine inhaltliche Auseinandersetzung mit dem Werk voraus. Die Reform ermöglicht es, Reproduktionsfotografien gemeinfreier Werke auch lediglich als Anschauungsmaterial in wissenschaftliche Arbeiten einzubinden.

Auch weiterhin können Einrichtungen Besuchern das Fotografieren von bildender Kunst verbieten, da sich das Verbotsrecht nicht aus dem Urheberrecht bzw. Lichtbildschutz ableitet, sondern aus dem Eigentumsrecht bzw. Hausrecht. Für das Verbot können noch durchaus andere Gründe sprechen als der Schutz vor an sich zulässigen Vervielfältigungen, wie z. B. die mit dem Einsatz von Blitzlicht verbundene Schädigung der Werke oder der durch das Fotografieren beeinträchtigte Werkgenuss Dritter. Unabhängig von den Gründen darf die Einrichtung über die Nutzung ihrer Räumlichkeiten frei entscheiden. ◆

DFN unterwegs

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

Dr. Ralf Gröper ist als Bereichsleiter verantwortlich für die Security sowie Trust & Identity Services des DFN-Vereins. Zuletzt besuchte er…

…den GÉANT-SOC-Workshop in Amsterdam am 5. und 6. Dezember 2019.
Die Bereitstellung von Security Operations (SecOps) und eines Security Operations Centers (SOC) beschäftigt derzeit viele europäische Forschungsnetze (NRENs). So gibt es auch im gemeinsamen EU-Projekt GN4-3 einen Task zum Thema SOC-Tools. Bei dem Workshop ging es unter anderem um Tools wie MISP und Apache NiFi, Erfahrungsberichte aus unterschiedlichen Ländern und intensive Diskussionen zum weiteren Vorgehen. Ein besonderes Highlight der sehr gut besuchten Veranstaltung war neben den neuesten Nachrichten von GÉANT und den NRENs, der informelle offene Erfahrungsaustausch, der nur aufgrund des großen Vertrauens zwischen den europäischen NRENs und deren Mitarbeiterinnen und Mitarbeitern möglich ist. Die Kooperation über GÉANT sowie gemeinsame große Veranstaltungen wie die TNC-Konferenz tragen dazu bei, dass nicht jedes Rad in jedem Land neu erfunden werden muss, sondern gemeinsam Lösungen erarbeitet werden. Der DFN nutzt diese Erkenntnisse und die Expertise des DFN-CERT derzeit, um einen eigenen SecOps-Dienst für die Teilnehmer am Deutschen Forschungsnetz vorzubereiten. Dies wird dabei helfen, dass Wissenschaftseinrichtungen in Deutschland auch zukünftig gemeinsam mit dem DFN den Gefahren für die Informationssicherheit adäquat begegnen können. ◆

Dr. Stefan Piger hat beim DFN-Verein den Hut auf für den Bereich Network and Communication Services. Begeistert war er vom…

…LHCOPN/LHCONE-Workshop am 13. und 14. Januar 2020 am CERN in Genf,
wo sich 74 Teilnehmerinnen und Teilnehmer von 47 wissenschaftlichen Institutionen und acht NRENs (National Research and Education Networks) bei schönstem Winterwetter trafen, um über die Zukunft der Verteilung und Verarbeitung der Daten des Large Hadron Collider (LHC) zu diskutieren. Im Grunde genommen ging es um die ewige Frage, wie man die gigantischen Datenmengen, die am CERN, genauer durch die Detektoren des LHC, erzeugt werden zu den Datenzentren bekommt, wo sie verarbeitet werden und zu den Wissenschaftlern, die sie analysieren wollen.

Diese Frage beschäftigt die Beteiligten an den LHC-Experimenten und den weltweiten Forschungsnetzen seit den frühen Planungstagen des LHC. Im Ergebnis entstan-

den auf Basis der NRENs über die Jahre eigene Netzinfrastrukturen für die weltweite Hochenergiephysik. So wurden mit dem LHC Optical Private Network (LHCOPN) direkte Wellenlängenverbindungen zwischen dem CERN und den nationalen Tier-1-Datenzentren errichtet und mit dem LHC Open Network Environment (LHCONE) entstand ein weltweites virtuelles Layer-3-Netz, an das mittlerweile über 100 Einrichten angebunden sind.

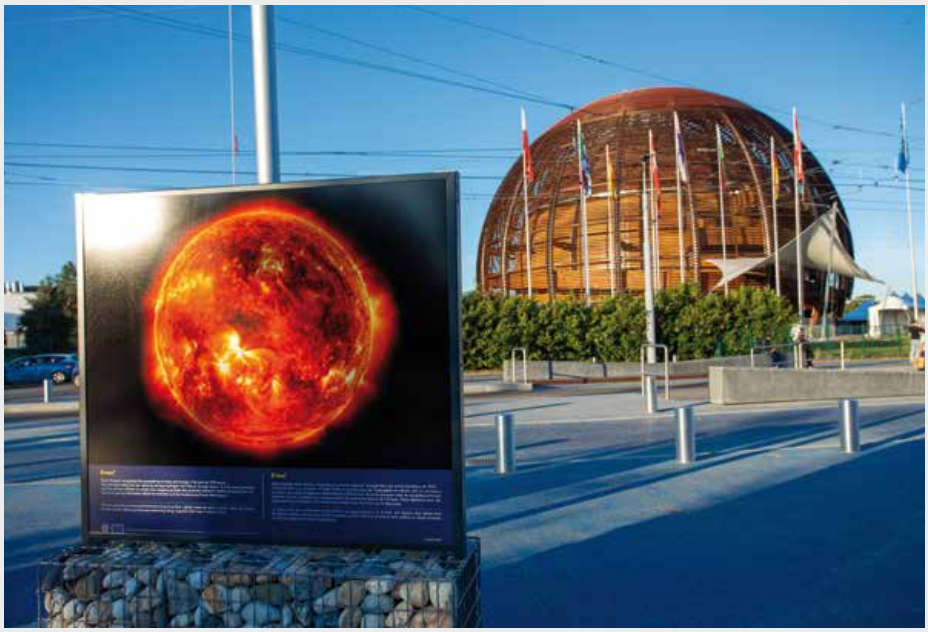
Der erste Tag des Workshops war ganz den Berichten und Ausblicken der LHC-Experimente gewidmet. Deren Erfahrungen in Bezug auf Speicher-, Rechen- und Netzinfrastrukturen scheinen bisher positiv zu sein. Als Netzverantwortlicher konnte man sich über Aussagen freuen wie „ALICE (A Large Ion Collider Experiment) is happy with LHC OPN/One and in general with the network performance during Run 2 – always one step ahead of/above the needs" oder auch „Networking is and has been one of the rock-solid highly reliable building blocks of ATLAS computing successes".

Was sind nun die Herausforderungen, vor denen diese Community steht? Sie kommen einem seltsam bekannt vor: eine starke Erhöhung der Datenmengen (HL-LHC wird ungefähr die zehnfache Datenmenge pro Jahr gegenüber heute produzieren), gleichzeitig aber weitgehend statische Budgets und eine Verlangsamung von Moore's Law (es geht hier um die Komplexität integrierter Schaltkreise), wodurch die Kosten pro Einheit an nutzbarer Rechenleistung nicht mehr in dem Maße zurückgehen wie man es über Jahrzehnte gewohnt war.

Der zweite Workshop-Tag war daher den Ansätzen gewidmet, wie man diesen und weiteren Herausforderungen begegnen könnte. Bei der Verteilung der Daten planen die CERN-Verantwortlichen auf dem Campus den Einsatz von kohärenten Optiken und für den Transport zu den Tier-1-Zentren mit 400 Gbit/s pro Wellenlänge. Bei der Prozessierung der Daten denkt man an die verstärkte Nutzung von Spezial-Hardware wie GPUs oder FPGAs, um die Effizienz zu verbessern. Künftig will man verstärkt Software-Entwicklungen Community-übergreifend vorantreiben, HPC-Infrastrukturen gemeinsam nutzen oder auch gleich in der Cloud rechnen.

Als Vertreter eines Forschungsnetzes hört man bei solchen Plänen sehr aufmerksam zu. Gerade die Nutzung von HPC-Ressourcen, die über keine eigenen Speicherressourcen verfügen, erzeugt potenziell interessante Herausforderungen bei der Dimensionierung der Netze. In diesem Anwendungsfall müssen die zu verarbeitenden Daten vor jeder Berechnung von den Datenzentren der LHC-Community in die HPC-Zentren und die Ergebnisse der Berechnungen wieder zurücktransferiert werden. Während des Workshops kamen erste Forderungen auf nach Übertragungskapazitäten im Bereich von Terabit/s.

Als Fazit bleibt zu sagen, dass es für die Forschungsnetze wie den DFN-Verein extrem wertvoll ist, so frühzeitig an diesen Diskussionen beteiligt zu werden. Wenn ein Wunsch frei wäre, dann der, dass andere Communities diesem Beispiel folgen. Wir kommen gern! ◆



Das Forschungszentrum Cern in Genf. *Foto:*

DFN Live: Wissen teilen, Erfahrungen weitergeben – jetzt erst recht!

Der DFN-Verein lebt von der Expertise und Erfahrung seiner Mitglieder und Teilnehmer am Deutschen Forschungsnetz. Mit zahlreichen Veranstaltungen, Tutorien, Tagungen und Workshops bietet der DFN-Verein ein Forum für einen lebendigen Dialog und Wissenstransfer. Gerade in COVID-19-Zeiten erhält der Austausch innerhalb der Netz-Community – egal ob digital oder physisch – eine besondere Bedeutung.

Mitgliederversammlung:

An der ersten virtuellen Mitgliederversammlung – insgesamt die 80. in der Geschichte des DFN-Vereins – nahmen am Dienstag, 16. Juni 2020, 115 Mitgliedsvertreter aus ganz Deutschland teil. Veranstaltungsort war nicht wie üblich Berlin, sondern die Videokonferenzplattform Zoom. Durch die Verwendung von Zoom war es möglich, diese große Anzahl von Teilnehmerinnen und Teilnehmern zuzulassen, ohne die Diskussionskultur der Veranstaltung zu verlieren. Ein reines Streaming hätte das nicht bieten können.

Es gab einige spannende Themen auf der Tagesordnung. Dazu gehörte die derzeitige Situation rund um die COVID-19-Pandemie und deren Auswirkungen auf das Deutsche Forschungsnetz. Dabei standen die aktuellen Entwicklungen im X-WiN und im Videokonferenzdienst DFNconf, über die die jeweiligen Bereichsverantwortlichen ausführlich berichteten, im Fokus. Doch es stand noch ein anderes wichtiges Thema auf der Tagesordnung: So wurde nach einer zweijährigen Vorbereitungsphase und vielen intensiven Diskussionen

Aufgabenteilung: Backstage managt Dr. Ralf Gröper das Technische, während Prof. Dr. Gerhard Peter als Vorsitzender der 80. Mitgliederversammlung die Online-Veranstaltung eröffnet. *Foto: Nina Bark/DFN-Verein*

die Einführung eines neuen Entgeltmodells beschlossen. Das Modell präzisiert und ergänzt die Regelungen für die Umlage der Kosten für Netz und Dienste auf die teilnehmenden Einrichtungen. Die neue Entgeltordnung wird mit Beginn des 01.01.2022 wirksam.

Weitere Themen waren unter anderem die Entwicklungen im europäischen und internationalen Umfeld sowie die Projekte, an denen der Verein beteiligt ist. Ferner stellte der Vorstand im Hinblick auf die Neuwahl des Verwaltungsrates im Dezember 2020 seine Liste der Kandidatinnen und Kandidaten vor.

TERMIN

Die 81. Mitgliederversammlung findet am **Mittwoch, 2. Dezember 2020**, statt. Ob digital oder physisch in Bonn, darüber informieren wir die Mitgliedsvertreter rechtzeitig über unsere Kommunikationskanäle.

Betriebstagung

Zweimal im Jahr treffen sich Mitarbeiterinnen und Mitarbeiter der am Wissenschaftsnetz X-WiN teilnehmenden Institutionen, Vertreter der Mitgliedsorganisationen sowie andere an den Fachthemen des DFN-Vereins Interessierte zur zweitägigen Betriebstagung, um sich fachlich weiterzubilden und Erfahrungen auszutauschen. In den Foren, unter anderem Sicherheit, AAI, IP über WiN, Multimedia oder Clouddienste, werden die Teilnehmerinnen und Teilnehmer über neue Entwicklungen informiert und diskutieren Fragen, die sich aus dem Einsatz von DFN-Diensten ergeben.

TERMIN

Die 73. DFN-Betriebstagung findet am **Dienstag und Mittwoch, 15. und 16. September 2020**, als Videokonferenz statt.

DFN-Konferenz „Datenschutz“

Seit 2012 veranstaltet das DFN-CERT im Auftrag des DFN-Vereins jährlich die DFN-Konferenz „Datenschutz“. Ziel sind unter anderem die Beratung und der Austausch der für die Einhaltung und die praktische Umsetzung des Datenschutzes Verantwortlichen in Forschungs- und Bildungsinstitutionen sowie Behörden. Zugleich bietet die Veranstaltung die Möglichkeit, Anforderungen mit Vertretern der Datenschutzaufsichtsbehörden und eingeladenen Experten aus der Datenschutzpraxis zu diskutieren. Am 5. und 6. Dezember 2019 fand in Berlin die 8. DFN-Konferenz „Datenschutz“ statt. Zu den vielfältigen Themen zählte auch dieses Mal die DSGVO, besucht wurde die Konferenz von 144 Teilnehmerinnen und Teilnehmern.

TERMIN

Den voraussichtlichen Termin für die 9. DFN-Konferenz „Datenschutz“ teilen wir Ihnen rechtzeitig über unsere Kommunikationskanäle mit.

DFN-Konferenz „Sicherheit in vernetzten Systemen“

Im Auftrag des DFN-Vereins veranstaltet das DFN-CERT jedes Jahr die Konferenz „Sicherheit in vernetzten Systemen“ im Grand Elysée Hotel Hamburg. Diese im Sicherheitsbereich etablierte Veranstaltung beinhaltet Beiträge und Diskussionen zu unterschiedlichen Aspekten der Informationssicherheit. Mit ihrer explizit technischen und wissenschaftlichen Ausrichtung und durchschnittlich 350 Teilnehmerinnen und Teilnehmern hat sich die DFN-Konferenz zu einer der größten deutschen Sicherheitstagungen entwickelt.

Am 24. und 25. Februar 2020 fand die 27. DFN-Konferenz „Sicherheit in vernetzten Systemen“ statt. Mit 360 Teilnehmerinnen und Teilnehmern war diese Veranstaltung die bisher bestbesuchte (Vorjahr 330).

Die Themen waren breit gefächert und spiegelten so die große Zielgruppe der Konferenz wider. Zunehmend in den Fokus geraten neben eher technisch orientierten Vorträgen die Themen zur Governance von Informationssicherheit. Dabei spielen neben der Compliance zu gesetzlichen Rahmenbedingungen (diesmal: IT-Sicherheitsgesetz) die Einführung und der Betrieb von Informationssicherheitsmanagementsystemen (ISMS) eine zentrale Rolle.

Im Anschluss an die Konferenz fand das Tutorium „Crisis Management Exercise“ statt. Hierbei wurde eine Krisensimulationsübung durchgeführt, während der die Teilnehmerinnen und Teilnehmer in verschiedenen Rollen eine nachgestellte Krisensituation bewältigen mussten und so die damit einhergehende Stresssituation am eigenen Leib erfahren durften – natürlich mit dem Ziel, im Ernstfall an der eigenen Einrichtung möglichst ruhig und besonnen reagieren zu können (Bericht S. 43).

Dr. Klaus-Peter Kossakowski, Geschäftsführer der DFN-CERT Services GmbH, eröffnet die Sicherheitskonferenz. *Foto: Silke Meyer/DFN-Verein*

TERMIN

Die 28. DFN- Konferenz „Sicherheit in vernetzten Systemen“ findet am **1. und 2. Februar 2021** statt. Ob online oder physisch in Hamburg, darüber informieren wir Sie rechtzeitig über unsere Kommunikationskanäle.

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: 08/2020)

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 verwirklicht insbesondere 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
D-10178 Berlin
Telefon: +49 (0)30 884299-0

Standort Stuttgart
DFN-Verein e. V.
Lindenspürstraße 32
D-70176 Stuttgart
Telefon: +49 (0)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 12. Wahlperiode sind Mitglieder des Verwaltungsrates:

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

Prof. Dr. Hans-Joachim Bungartz
(Technische Universität München)

Prof. Dr. Gabi Dreo Rodosek
(Universität der Bundeswehr München)

Prof. Dr. Rainer W. Gerling
(Max-Planck-Gesellschaft München)

Dr.-Ing. habil. Carlos Härtel
(Selbstständiger Unternehmensberater)

Prof. Dr. Odej Kao
(Technische Universität Berlin)

Prof. Dr.-Ing. Ulrich Lang
(Universität zu Köln)

Prof. Dr. Joachim Mnich
(Deutsches Elektronen-Synchrotron Hamburg)

Dr. Karl Molter
(Hochschule Trier)

Dr.-Ing. Christa Radloff
(Universität Rostock)

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. Hans-Joachim Bungartz
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 Mitgliedereinrichtungen

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 Institut 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
	Konrad-Zuse-Zentrum für Informationstechnik (ZIB)
	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)
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
	BundesminIsterium für Umwelt, Naturschutz u. 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 i.G.
	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
	Kirchlische Hochschule Wuppertal/Bethel
Würzburg	Hochschule für angewandte Wissenschaften – Fachhochschule Würzburg-Schweinfurt
	Julius-Maximilians-Universität 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 Informationsrechtes

DFN newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

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