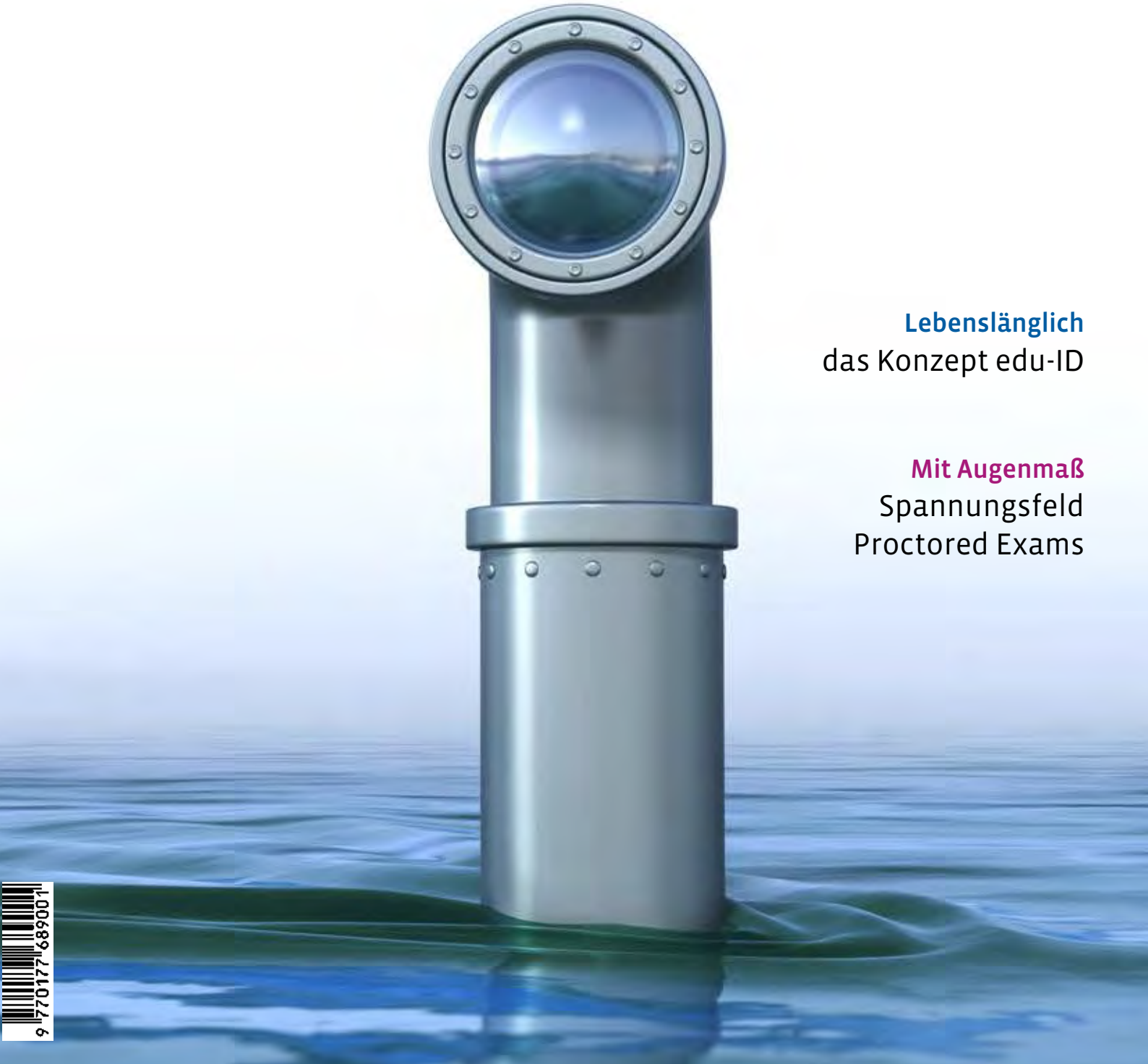
Deutsches Forschungsnetz | DFN Mitteilungen Ausgabe 98 | Dezember 2020 | www.dfn.de

DFN mitteilungen

Erkennung & Reaktion

neuer DFN-Dienst Security Operations



Lebenslänglich
das Konzept edu-ID

Mit Augenmaß
Spannungsfeld
Proctored Exams

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

Fotonachweis
Titelillustration: iLexx / iStock
Seite 6/7: Bet_Noire / iStock
Seite 34/35: magicbones / photocase.de

Dr.-Ing. Christa Radloff
Langjähriges Mitglied des DFN-Verwaltungsrates, ehemalige Leiterin des IT- und Medienzentrums der Universität Rostock
Foto: Frank Homann

Liebe Leserinnen und Leser,

den DFN-Verein kenne ich seit dem Beitritt der neuen Bundesländer. Mit dem erweiterten Wissenschaftsnetz ERWIN wurde 1991 schnell eine Infrastruktur geschaffen, die für unsere Hochschulen eine Verbindung zur gesamtdeutschen Wissenschaft ermöglichte und eine nicht hoch genug anzurechnende Unterstützung darstellte. Heute betreibt der DFN-Verein mit dem X-WiN ein exzellentes Wissenschaftsnetz mit hervorragenden Außenanbindungen. Darüber hinaus steht uns eine Vielzahl von Diensten zur Verfügung, die für uns zum großen Teil existenziell wichtig sind. In den rund 30 Jahren konnte ich den DFN-Verein in verschiedenen Rollen als Vertreterin meiner Universität und als Mitglied im Verwaltungsrat und im Betriebsausschuss miterleben. Dabei ist mir keine Periode in Erinnerung, in der nicht neue Herausforderungen bewältigt werden mussten oder neue Ideen diskutiert wurden. Seit seiner Gründung 1984 hat der Verein mehrfach seine besondere Fähigkeit unter Beweis gestellt, Gemeinschaft zu bilden und die häufig auch unterschiedlichen Interessen seiner Mitglieder zu bündeln. Dabei ging es nicht immer einmütig zu, aber die Diskussionen waren stets konstruktiv und lösungsorientiert.

Der erfolgreiche Weg des DFN-Vereins fußt seit jeher auf dem breiten Mandat seiner Mitglieder. Und so konnte im Sommer nach einer zweijährigen Diskussion auf allen Ebenen eine neue Entgeltordnung verabschiedet werden. Bei diesem Thema ist es nicht leicht, Partikularinteressen hintenanzustellen. Deshalb war es besonders hilfreich, sich zuvor auf Prinzipien zu einigen, die sich aus der Verfasstheit und dem Selbstverständnis des DFN-Vereins ergeben. Mit der verabschiedeten Entgeltordnung haben wir letztendlich eine Lösung, die die alten Schwachstellen beseitigt und viele besondere Situationen weitestgehend berücksichtigt. Ein Großteil der Prinzipien gilt nicht nur für das Thema Entgelt – das Besinnen auf Grundprinzipien des Vereins kann in konfliktreichen Situationen sicher wertvoll sein.

Angesichts der Pandemie beschäftigt uns in hohem Maße die Absicherung der digitalen Lehre, insbesondere die Bereitstellung eines technisch funktionierenden und datenschutzrechtlich abgesicherten Konferenzdienstes. Jede Einrichtung arbeitet für sich an diesem Problem und es liegt auf der Hand, dass eine Bündelung der Aktivitäten äußerst hilfreich wäre. Dabei besteht eine gewisse Hoffnung und Erwartungshaltung, dass der DFN-Verein hierbei eine wichtige Rolle übernehmen kann. Angesichts der drängenden Zeit ist ein langwieriges Abwägen hierbei leider nicht möglich. Bei der Bewältigung der Aufgaben kann der Verein auf die große Expertise seiner Mitgliedseinrichtungen, auf die engagierte Arbeit in den Vereinsorganen und Ausschüssen sowie auf die Kompetenz der Mitarbeitenden der Geschäftsstelle zurückgreifen. Und so bin ich zuversichtlich, dass in der Gemeinschaft auch diese Herausforderung gemeistert und ein für alle Seiten gutes Ergebnis erzielt werden kann.

Herzlichst
Ihre Christa Radloff

Unsere Autoren dieser Ausgabe im Überblick

1 Stefan Anders, DFN-Verein (anders@dfn.de); **2** Henry Kluge, DFN-Verein (kluge@dfn.de); **3** Michael Röder, DFN-Verein (roeder@dfn.de); **4** Thorsten Michels, TU Kaiserslautern (michels@rhrk.uni-kl.de); **5** Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **6** Frank Schreiterer, Uni Bamberg (frank.schreiterer@uni-bamberg.de); **7** Jens Link, IT-Consulting (jenslink@quux.de); **8** Frank Schulze, TU Dresden (frank.schulze@tu-dresden.de); **9** Nils Szuka, FernUniversität in Hagen (nils.szuka@fernuni-hagen.de); **10** Maimona Id, DFN-Verein, (id@dfn.de); **11** Dr. Jakob Tendel, DFN-Verein (tendel@dfn.de); **12** Nelson Simões, Rede Nacional de Ensino e Pesquisa, RNP (nelson.simoes@rnp.br); **13** Dr. Ralf Gröper, DFN-Verein (groeper@dfn.de); **14** Ralf Paffrath, DFN-Verein (paffrath@dfn.de); **15** Jan-Frederik Rieckers, DFN-Verein (rieckers@dfn.de); **16** Thomas Schmid, DFN-Verein (schmid@dfn.de); **17** Martin Waleczek, DFN-CERT Services GmbH (waleczek@dfn-cert.de); **18** Steffen Uphues, Forschungsstelle Recht im DFN (steffen.uphues@uni-muenster.de); **19** Nico Gielen, Forschungsstelle Recht im DFN (nico.gielen@uni-muenster.de)

Inhalt

Wissenschaftsnetz

Campus

International

Sicherheit

Recht

DFN-Verein

Wissenschaftsnetz

DANE & DNSSEC – ein schlagkräftiges Team

Es gibt keine Möglichkeit, DANE (DNS-based Authentication of Named Entities) ohne DNSSEC (Domain Name System Security Extensions) sicher umzusetzen. Um zu verstehen, woraus sich der Mehrwert von DANE ergibt, ist deshalb auch ein grundsätzliches Verständnis von DNS und DNSSEC notwendig. Aber wie kommt man über DNS und DNSSEC schließlich zur Aktivierung von DANE?

Text: **Stefan Anders, Henry Kluge, Michael Röder** (DFN-Verein)

Foto: BrianAJackson / iStock

Das Domain Name System (DNS) ist ein elementarer Bestandteil aller Kommunikation in digitalen Netzwerkinfrastrukturen. In Computernetzwerken werden Geräte mithilfe von eindeutigen Zahlenkolonnen adressiert. Menschen arbeiten aber besser mit wortbasierten Adressierungen, also Namen. DNS ist die Schnittstelle, die den vom Menschen vergebenen Namen einer Maschine in die maschinenlesbare Form übersetzt.

Wozu überhaupt DNSSEC?

Der Übersetzungsvorgang vom DNS-Protokoll ist kompromittierbar: Was passiert, wenn der Nutzer zum Beispiel beim Onlinebanking eine Maschine seiner Bank ansprechen möchte und unbemerkt auf ein gehacktes System umgeleitet wird, das

> Was passiert, wenn der Nutzer unbemerkt auf ein gehacktes System umgeleitet wird?

sich optisch nicht von dem seiner Bank unterscheidet? So funktioniert ein gängiges Verfahren von Trickbetrügern, den Man-In-The-Middle-Attacken (MitM), die mithilfe von Trojanern in der Lage sind, auf dem Client-PC eigene DNS-Einträge zu hinterlassen. Sie sorgen dafür, dass der regelmäßig und automatisch stattfindende Selbstaktualisierungsmechanismus des DNS-Protokolls unterwandert wird. Deshalb werden Verfahren entwickelt, die diesen Übersetzungsvorgang absichern.

In den letzten beiden Jahren gerieten im DNS-Umfeld Verfahren wie DNS over HTTP (DoH) oder DNS over TLS (DoT) verstärkt in den Fokus. Diese zielen in erster Linie auf die Sicherstellung der Vertraulichkeit auf der „letzten Meile" zum Anwender ab. Das schon lange verfügbare DNSSEC-Protokoll (DNS Security Extensions) ist aber deshalb jedoch noch lange nicht obsolet. Hier liegt der Schwerpunkt auf der Integrität und Authentizität der DNS-Daten (Resource Records). Diese werden durch das Signieren der einzelnen Records mit bewährten kryptografischen Methoden hergestellt. Die erzeugten Signaturen können dann entlang einer sogenannten Chain of Trust bis zur Wurzel der DNS-Hierarchie validiert werden. Der mit Abstand am häufigsten genutzte Anwendungsfall für DNSSEC ist im Moment die zusätzliche Absicherung von sicherheitskritischen Resource Records im Rahmen des DANE-Verfahrens. Durch dieses Verfahren wird eine zusätzliche Überprüfung des für eine TLS-Verbindung (Transport Layer Security) genutzten Zertifikats auf seine korrekte Zuordnung zur genutzten DNS-Domain ermöglicht.

Hier wird deutlich, warum DNSSEC und DANE natürlich Themen sind, die über individuelle Interessen einzelner Einrichtungen hinaus auch für die Infrastruktur der Dienstelandschaft des DFN-Vereins von Bedeutung sind. Insbesondere für die Teilnehmer am DFN-Dienst DFN-MailSupport ist die Absicherung der Transportwege auf Basis von DANE zwischen zwei Mail-Gateways mit einem spürbaren Mehrwert verbunden. Nachdem DFN-MailSupport bereits seit mehreren Monaten DANE für ausgehende E-Mails anbietet, folgt nun die Absicherung via DANE auch für den eingehenden Mailverkehr.

Was können DNSSEC und DANE gemeinsam leisten?

Mail-Gateways haben die Aufgabe, der E-Mail den richtigen Weg zu weisen, damit sie auch tatsächlich dort ankommt, wo sie soll. Es gibt verschiedene Möglichkeiten sicherzustellen, dass die Daten, die zwischen Mail-Gateways hin- und her gesendet werden, nicht unterwegs von unberechtigten Dritten mitgelesen oder verändert werden können. Eine Möglichkeit hierfür ist, den Datentransport zu verschlüsseln. Das sendende und das empfangende Gateway handeln dabei ein gemeinsames Geheimnis aus und verwenden dieses als Schlüssel – sodass nur diese beiden in der Lage sind, den transportierten Inhalt zu ver- und entschlüsseln.

Im Internet existieren sehr viele Mail-Gateways – und die meisten von ihnen kommen potenziell dafür infrage, per E-Mail mit einer Einrichtung im Wissenschaftsnetz im Kontakt zu stehen. Bei der Vielzahl an Gateways und Betreibern ist es aber kaum möglich, einheitliche Verschlüsselungsstandards zu erzwingen. Wenn inkompatible Übertragungsstandards aufeinanderprallen, kommt als kleinster gemeinsamer Nenner eben doch wieder der unverschlüsselte Transport zum Einsatz.

Die Architektur hinter DFN-MailSupport bietet mit DANE nun für dieses Problem eine Lösung. Wenn sich beide Mail-Gateways

> Die Architektur hinter DFN-MailSupport bietet mit DANE nun für dieses Problem eine Lösung

auf die Verwendung von DANE geeinigt haben, ist ein Fallback auf unverschlüsseltes Senden per SMTP (Simple Mail Transfer Protocol) nicht mehr möglich, denn die gängigen Implementierungen von DANE lassen das schlicht nicht zu. SMTP-Server-Implementierungen die DANE unterstützen, sind zum Beispiel: postfix, powerMTA, halon, exim und seit neuestem sendmail.

Ein neues Feature für DFN-MailSupport

Der Dienst DFN-MailSupport ist so konzipiert, dass der DFN-Verein vorgelagerte Empfänger-Mail-Gateways betreibt. Für eine teilnehmende Einrichtung A nimmt der DFN-Verein also initial jede eingehende E-Mail entgegen, die an die Mail-Adresse einer Person gesendet wurde, die in der Einrichtung A ein Postfach besitzt. Anschließend werden im Rahmen der Diensterbringung schadhafte und unerwünschte E-Mails aussortiert. Die verbleibenden E-Mails werden an die Mail-Gateways von Einrichtung A weitergeleitet (Abb. 1, S. 14).

Auch die von den Teilnehmern ausgehenden E-Mails können über den DFN-MailSupport geleitet werden. Bei Spam- und Phishingausbrüchen infolge kompromittierter PCs innerhalb von Einrichtung A können damit die Kommunikationspartner geschützt werden.

Der DANE-Check wird stets vom sendenden Gateway ausgeführt, wie in Abbildung 2 dargestellt. Hierbei wird geprüft, ob die MX-Records der Empfängerdomain sowie

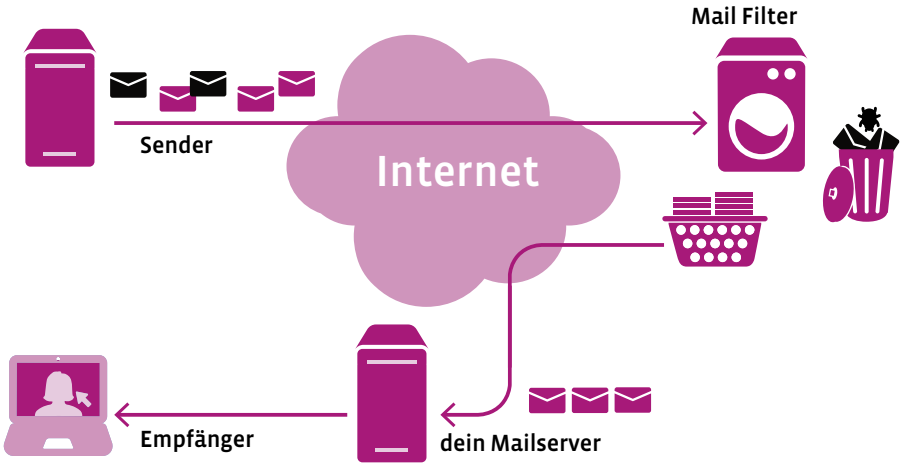


Abbildung 1: DFN-MailSupport

die A-Records der zugehörigen Mailserver DNSSEC-geschützt und darüber hinaus zu den A-Records passende TLSA-Records konfiguriert sind. Die TLSA-Records enthalten eine prüfbare Eigenschaft des Mailserver-Zertifikats, üblicherweise eine Checksumme. Mit dieser wird das vom Empfänger-Mailserver im SMTP-Protokoll angebotene Zertifikat überprüft. Hiermit ist es möglich, MitM-Angriffe zu erkennen, da ein Angreifer dank DNSSEC die Checksumme nicht manipulieren kann.

Solche MitM-Attacken durch gefälschte Zertifikate sorgten in den vergangenen Jahren bei einigen CA-Betreibern („Certificate-Authority") für schwerwiegende Sicherheitsvorfälle. Bei der Anwendung von DANE wird die Sicherstellung der Vertrauensbasis auf die Betreiber der Root-Name-Server (IANA) und den Betreiber der Top-Level-Domain (z. B. DENIC) reduziert – ohne DANE sind dafür etwa 100 CA-Betreiber innerhalb der weltweiten PKI verantwortlich. Mit DANE existieren also erheblich weniger Einfallstore für die Bösewichte dieser Welt.

Da bislang nur ein Bruchteil der Domains im DNS auch DNSSEC-signiert sind, erfolgt bei fehlenden Voraussetzungen (DNSSEC, TLSA-Records) seitens des Empfängers ein Rückfall auf die Übertragung der E-Mail mit unverifizierter Verschlüsselung oder sogar auf den gänzlich unverschlüsselten Transport. Dies wird auch opportunistic DANE genannt.

Innerhalb einer geschlossenen Nutzergruppe, in der alle Teilnehmer ihr DNSSEC und DANE korrekt aufgesetzt haben, kann der DANE-Check auch erzwungen werden, das sogenannte mandatory DANE. Die E-Mail wird hierbei nur dann übertragen, wenn alle Voraussetzungen erfüllt sind und alle Prüfungen bestanden wurden. Wissen Absender und Empfänger um diese Konfiguration, so können sich beide auf Authentizität und Vertraulichkeit ihrer Kommunikation verlassen. DFN-MailSupport unterstützt solche Nutzergruppen mit entsprechenden Optionen in der Konfiguration.

Das eigentliche Aktivieren von DANE ist technisch kein besonders großer Aufwand – weder beim Versender noch beim Empfänger. Die Konfiguration ist überschaubar und kann beispielsweise als Ersatz für das sogenannte Certificate Pinning dienen. Da die kryptografische Verifizierung der Gegenstelle vom DNS-Resolver übernommen wird, werden keine zusätzlichen PKI-signierten Zertifikate mehr benötigt. Es genügen selbstsignierte Zertifikate.

> Das eigentliche Aktivieren von DANE ist technisch kein besonders großer Aufwand

Langer Weg bis zur Umsetzung

Es hat in der Vergangenheit bereits einige Versuche gegeben, die Zone „dfn.de" mit DNSSEC signieren zu lassen. Gleichzeitig kursierten in regelmäßigen Abständen Meldungen durch die einschlägigen Nachrichtenkanäle, in denen namhafte DNS-Provider teils populäre Ausfälle infolge eines Problems innerhalb ihrer Signierungskette hinnehmen mussten.

Jedoch sank die Anzahl der sichtbaren Ausfälle zuletzt, während die Qualität der Dokumentation und von Toolchain spürbar gestiegen ist. War DNSSEC also anfangs spannend und zog deshalb die Blicke auf sich, dann war es in diesem Stadium auch ebenso fehleranfällig, weil die Softwareentwicklung noch nicht die notwendige Produktionsreife erreicht hatte. Das ist mittlerweile längst nicht mehr der Fall.

Die Tatsache, dass Ausfälle teils sehr sichtbar passiert sind, zeigt aber auch, dass DNSSEC einen hohen Betreuungsaufwand generiert – zumindest so lange, bis die automatischen Prozesse zuverlässig funktionieren. In den Fehlerberichten wurde deutlich, dass eine einzige defekte Signatur zur Unterbrechung der Validierungskette führen kann. Dann sind alle Dienste innerhalb der signierten Zone davon beeinträchtigt. Das DNS-Protokoll bietet zwar weniger Sicherheit, ist aber dafür auch weniger anfällig für solche Single Points of Failure. Ein Fehler in der Zone „dfn.de" würde eine signifikante Beeinträchtigung weiterer Dienste, wie der DFN-AAI oder DFNconf, bedeuten. Ein hoher Grad an Automatisierung und ein umfangreiches Monitoring der Betriebsparameter können bei der Vermeidung von Ausfällen von entscheidender Bedeutung sein.

Folglich mussten die Betriebskonzepte überarbeitet und absehbare Fehlverhalten und Fehlertoleranzen in der Betriebsumgebung berücksichtigt und beobachtet

werden. Notfallkonzepte wurden angepasst und die Dokumentation erweitert – damit im Problemfall unmittelbar eine Reaktion möglich ist. Im Rahmen eines Pilotbetriebes konnten Qualität und Zuverlässigkeit sichergestellt werden. Dabei sind auch unerwünschte Artefakte bemerkt und behoben worden, die im theoretischen Modell noch nicht sichtbar waren.

Durch die COVID-19-Pandemie war die Beteiligung an der Pilotphase geringer als erwartet, trotzdem konnten alle Tests erfolgreich absolviert werden. Die Sicherstellung der Betriebssicherheit war eher ein sekundäres Ziel der Pilotphase. Primär galt es herauszufinden, ob simulierte Kompromittierungsversuche auch tatsächlich die richtigen Reaktionen hervorrufen. Für den Testzeitraum wurde eine bislang ungenutzte Domain verwendet, über die DFN-MailSupport-Teilnehmer nichtproduktiven Mailverkehr generiert haben. In dieser Zone liefen dann zum Beispiel Signaturen aus, wurden plötzlich ungültig oder Teile der Validierungskette waren für einen eingeschränkten Zeitraum nicht erreichbar. Sobald einer dieser bewusst herbeigeführten Ausfälle eintrat, wurde überprüft, ob er mit den antizipierten Effekten einherging und ob die Notfallpläne die richtigen Schlüsse zuließen beziehungsweise anschließend auch die notwendigen Maßnahmen zur Instandsetzung bereithielten. Gleichzeitig war es an den Teilnehmern zu beobachten, ob ihre eigene Schnittstelle adäquat reagiert. Mit dem Ende der Pilotphase wurde deutlich: Die Mechanismen funktionieren, die Umgebung ist bereit für den professionellen Betrieb.

Wir möchten uns an dieser Stelle ausdrücklich bei den engagierten Testern während der Pilotphase bedanken! Sie haben einen großen Anteil daran, dass wir pünktlich in die Produktivphase starten können.

Während der gesamten Umsetzungsphase war das Thema Know-how-Transfer in diversen Schattierungen präsent. Die Themen DNSSEC und DANE sind so eng miteinander verzahnt, dass es naheliegend war, den DNS-Betrieb in die Hand des Teams zu legen, das auch für die Erbringung von DFN-MailSupport zuständig ist. Ein weiterer bedeutender Know-how-Transfer fand zwischen dem Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften und dem DFN-Verein statt. Das LRZ unterstützte den DFN-Verein mit seinen umfangreichen Erfahrungen im Kontext von DNSSEC und DANE. Herzlichen Dank an dieser Stelle! Mithilfe externer und interner Workshops konnte das gesammelte Know-how weiter vertieft und im Team verankert werden.

Im Ergebnis war die Arbeit im Projekt neben einer sehr technischen Komponente ebenfalls stark von organisatorischen Einflüssen geprägt. Planungen, Erkenntnisse und Ergebnisse sorgten für kontinuierliches Wachstum der internen Dokumentation. Der dadurch gestiegene Aufwand zeigt sich gegenüber den Teilnehmern zwar einerseits durch einen langen Weg bis zum Abschluss des Projekts – andererseits steigen dadurch aber auch unmittelbar und nachhaltig die Betriebssicherheit des Dienstes und der Schutz der sensiblen Informationen, die zehntausende Endanwender dem Dienst DFN-MailSupport täglich anvertrauen. ◆

WEITERE INFORMATIONEN ZUM THEMA FINDEN SIE HIER:

Kein X für ein U – mehr Sicherheit fürs Domain Name System!, Henry Kluge
https://www.dfn.de/fileadmin/5Presse/DFNMitteilungen/DFN_Mitteilungen_88.pdf

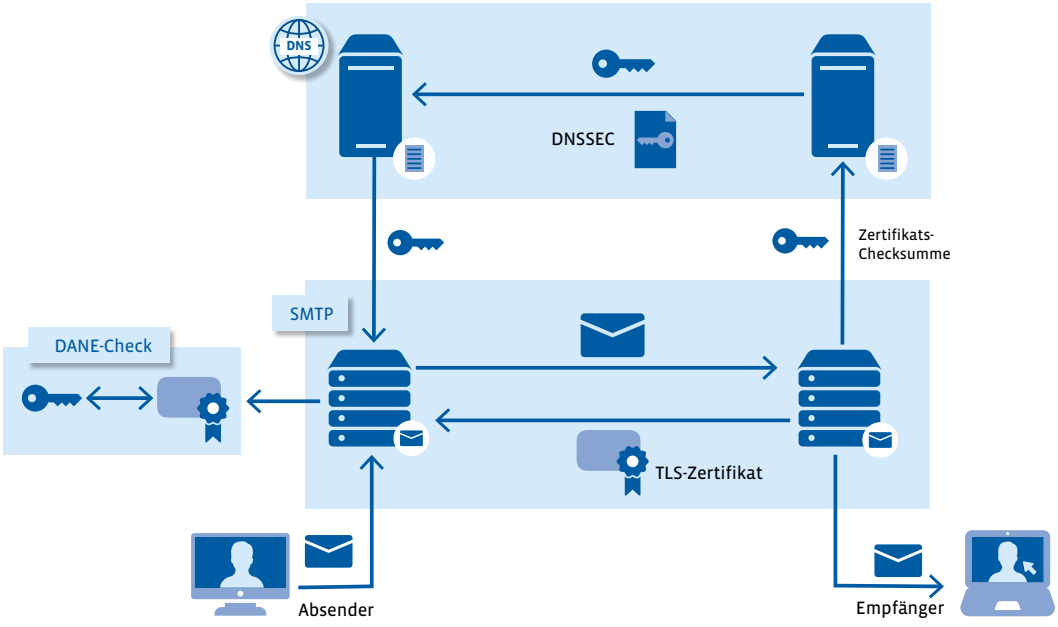


Abbildung 2: Wie funktionieren DNSSEC, DANE?

edu-ID – sei Du selbst. Immer.

Seit März 2019 beschäftigt sich eine ZKI-Arbeitsgruppe mit dem Konzept einer edu-ID. Hierbei handelt es sich um eine nutzerzentrische, einrichtungsunabhängige und lebenslang gültige digitale Identität für den Forschungs- und Bildungsbereich in Deutschland. Dieses Konzept orientiert sich in vielerlei Hinsicht am Schweizer Modell der SWITCH edu-ID.

Text: **Thorsten Michels** (TU Kaiserslautern), **Wolfgang Pempe** (DFN-Verein), **Frank Schreiterer** (Uni Bamberg)

Am Tropf der Heimateinrichtung

Im AAI- und Föderationskontext ist es üblicherweise die jeweilige Heimateinrichtung, die für ihre Angehörigen die digitale Identität zur Verfügung stellt und diese verwaltet. Ändert sich nun im Laufe der akademischen Vita die Affiliation, das heißt die Zugehörigkeit zu einer Einrichtung, wird die bisherige digitale Identität durch eine neue ersetzt. Mit der bisherigen Identität erlöschen somit alle damit verbunden Berechtigungen, Rollen und Verknüpfungen zu anderen Identitäten. In manchen Fällen genügt hierfür bereits der Übergang vom Studierenden- in den Mitarbeitendenstatus innerhalb derselben Einrichtung. Eine Unterbrechung oder das Ende eines akademischen Lebenslaufs führt in dieser Hinsicht zu einem völligen Identitätsverlust.

Viele der oben erwähnten Berechtigungen beziehen sich in aller Regel auf den Zugriff auf hochschul- beziehungsweise einrichtungsinterne Ressourcen und Dienste. Es existieren jedoch Szenarien, in denen ein unterbrechungsfreier Zugriff auf bestimmte Inhalte und Dienste auch nach dem Aus-

Foto: Pogonici / iStock

scheiden aus einer bestimmten Einrichtung möglich oder sogar unabhängig von einer

> Beispiele hierfür sind der langfristige Zugriff auf Leistungsnachweise …

bestimmten Affiliation sein sollte. Als Beispiele hierfür seien der langfristige Zugriff auf Leistungsnachweise, Speicherdienste oder Inhalte, die über Nationallizenzen verfügbar sind, genannt. Der unterbrechungsfreie und langfristige Zugriff auf Ressourcen wird auch im Rahmen der kommenden Nationalen Forschungsdateninfrastruktur (NFDI) eine wichtige Rolle spielen.

Ein weiterer Punkt, der eine ausschließlich von der Heimateinrichtung verwaltete Identität im AAI-Kontext problematisch macht, ist die Freigabe von Attributen, die zur Nutzung bestimmter Dienste vor allem im Bereich E-Research erforderlich sind. In diesem Modell ist die Nutzerin beziehungsweise der Nutzer von der Attributfreigabe seitens der für den Betrieb des Identity Providers zuständigen Stelle abhängig.

Die Community reagiert

Unter anderem um den oben genannten Punkten zu begegnen, die auch beim lebenslangen Lernen eine zentrale Rolle spielen, verfolgt die Schweizer Föderation SWITCHaai, seit 2010 das Konzept einer sogenannten edu-ID (https://www.switch.ch/edu-id/). Hierbei handelt es sich um eine lebenslang gültige digitale Identität, bei der die Nutzerin oder der Nutzer im Zentrum steht, nicht die jeweilige Heimateinrichtung. Nachdem die SWITCH edu-ID Ende 2016 in den Produktivbetrieb ging, stellte sich die Community der DFN-AAI und des ZKI die Frage, ob sich ein solches Modell auch auf den deutschen Forschungs- und Bildungsbereich nutzbringend anwenden lassen würde. Daher beschäftigt sich seit März 2019 eine ZKI-Arbeitsgruppe mit den folgenden Fragen: In welchen Anwendungsfällen (Use Cases) würde ein edu-ID System existierende Prozesse oder Infrastrukturmaßnahmen erleichtern oder gar überflüssig machen?

- Welche Szenarien wären mit einer edu-ID erst sinnvoll umsetzbar/möglich?
- In welchen Fällen würde ein edu-ID-System zu einer (Qualitäts-)Verbesserung bestehender Verhältnisse beitragen?
- Was müsste ein edu-ID-System in solchen Fällen leisten?

Und natürlich geht es auch um die Frage, welche Aspekte und Komponenten des Schweizer Modells für ein edu-ID-System im Rahmen der DFN-AAI nachnutzbar wären.

Neben Angehörigen der Hochschul-, Forschungs- und Bibliotheks-Communities beteiligen sich an der Arbeitsgruppe auch Mitglieder des DFN-AAI-Teams sowie Vertreter des DFN-CERT und verschiedener Dienstleister aus dem Bereich Trust & Identity.

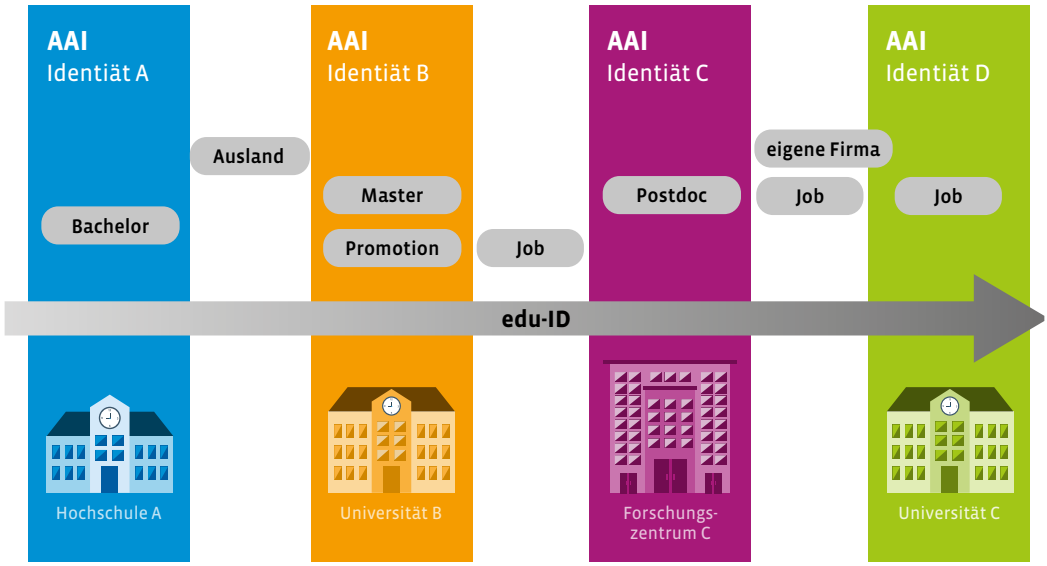
Ergebnisse und Fragen

Im Rahmen ihrer Arbeit konnte die Arbeitsgruppe zahlreiche Anwendungsfälle identifizieren, in denen ein edu-ID-System einen erkennbaren Mehrwert bringen würde. Die Ergebnisse gehen deutlich über die eingangs erwähnten Use Cases, wie des unterbrechungsfreien Zugriffs auf bestimmte Ressourcen, hinaus. Während die oben genannten Vorteile eines edu-ID-Systems primär die Nutzerinnen und Nutzer betreffen, besteht seitens der Hochschul-Community ein großes Interesse, Onboarding-Verfahren aller Art mithilfe eines edu-ID-Systems zu vereinheitlichen und zu vereinfachen. Eine bereits bestehende und zumindest in Teilen verifizierte digitale Identität erleichtert die Registrierung neuer Nutzender erheblich. Insbesondere für den Bereich Studienplatzbewerbung und Immatrikulation bestehen diesbezüglich große Hoffnungen. Nicht minder groß sind jedoch die damit verknüpften Anforderungen an die Verlässlichkeit der mit den edu-ID-Identitäten verknüpften Nutzerdaten. Hier steht die Anforderung im Raum, zumindest die über eine staatliche, elektronische Identifikation (eID) verfügbaren Daten anhand des neuen Personalausweises (nPA), eines elektronischen Aufenthaltstitels oder anderer eIDAS-konformer, elektronisch lesbarer Ausweisdokumente zu verifizieren. Eine solche Prüfung sollte bereits vor dem Onboarding erfolgen, idealerweise im Rahmen der Registrierung im edu-ID-System. Das hierfür erforderliche Prozedere zu definieren und einen Weg zu finden, die damit verbundenen Kosten zu decken, sind nur zwei der vielen Anforderungen an ein zukünftiges Betriebskonzept – es bleibt also noch viel zu tun. Allerdings wird die Zukunft zeigen, ob nicht zumindest die Use Cases Studienplatzbewerbung und Immatrikulation im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) seitens öffentlicher Stellen bedient werden, die ohne ein edu-ID-System auskommen.

Ein weiterer Anwendungsfall, der vor allem aus den Bibliotheken und den Forschungs-Communities kommt, ist das Account-Linking, also die Möglichkeit, die edu-ID-Identität über den edu-ID-Account mit weiteren Identitäten und Identifiern zu verknüpfen, zum Beispiel ORCID (https://orcid.org). Eng damit zusammen hängt auch die Anforderung analog zum Schweizer Modell, die mit den weiteren Identitäten verbundenen Nutzerdaten am edu-ID-Account zu aggregieren. Dies betrifft insbesondere die AAI-relevanten Attribute aus den Einrichtungen, denen die Nutzerin oder der Nutzer aktuell angehört. Beim Zugriff auf bestimmte Dienste kann also der Nutzende entscheiden, mit welcher Identität bzw. in welcher Rolle er den betreffenden Dienst nutzen möchte, sofern mehrere Affiliationen existieren.

Daneben spielt der Identity Provider des edu-ID-Systems eine wichtige Rolle als Gast- bzw. Homeless IdP, also als Authentifizierungsquelle für Personen, die aktuell keiner Einrichtung angehören, die mit einem Identity Provider an der DFN-AAI oder einer anderen Föderation teilnimmt. Bislang betreiben Forschungs-Communities und

EINE LEBENSLANGE DIGITALE IDENTITÄT …



Bibliotheksplattformen zu diesem Zweck jeweils eigene IdP-Instanzen. Dieser nicht nur technische Mehraufwand würde mit einem edu-ID-System also entfallen.

Nutzerzentrische Identität

Es liegt in der Natur dieses Modells, dass die Pflege eines edu-ID-Accounts nur seitens der Person erfolgen kann, der er gehört. Selbiges gilt für die Einrichtung eines solchen Accounts bzw. die Registrierung im edu-ID-System. Das Konzept sieht vor, dass die Account-Inhaberinnen und -Inhaber die aktive Kontrolle über alle Transaktionen und Verknüpfungen haben und somit volle Souveränität über ihre Daten genießen. Dies betrifft wie oben erwähnt die Freigabe und Übertragung von Nutzerdaten an AAI-Dienste, aber auch die Verknüpfung des Accounts mit weiteren Identitäten und die Aggregation von Nutzerdaten aus anderen Quellen wie zum Beispiel dem Nutzerverzeichnis der jeweiligen Heimateinrichtungen, genauso wie die Löschung des Accounts. Das edu-ID-System muss über entsprechende Infrastrukturkomponenten verfügen, die solche Maßnahmen ermöglichen und unterstützen. Selbstverständlich ist die betreffende Person verpflichtet, die von ihr selbst bereitgestellten Nutzerdaten aktuell zu halten und ggf. über geeignete Prozeduren und Mittel verifizieren zu lassen.

> Ein weiterer Anwendungsfall ist das Account-Linking

Wie geht es weiter?

Dieser Beitrag reflektiert lediglich einige Zwischenergebnisse, die die oben genannte Arbeitsgruppe bislang erzielt hat. Noch sind viele Fragen offen und Themen unberührt. So wird sich die Gruppe in ihrer weiteren Arbeit unter anderem mit dem Thema Levels of Assurance, also der Verlässlichkeit von Nutzerdaten, befassen: Welches Attribut wurde mit welchem Verfahren verifiziert? In manchen Fällen spielt auch das Datum der letzten Verifizierung oder Identitätsprüfung eine Rolle. Genügt die leichtgewichtige Schweizer Lösung den hiesigen Ansprüchen oder benötigen wir ein ausdifferenziertes, kontrolliertes Vokabular?

Weitere wichtige Themen sind Deprovisionierung – gemeint ist das Löschen und Stilllegen von Accounts – sowie Dublettenerkennung und -vermeidung. Auch der mögliche Einsatz und die Registrierung eines zweiten Faktors für die Authentisierung am edu-ID-System ist ein wichtiges Thema. Daneben gilt es, auch den internationalen Kontext im Auge zu behalten, um eine Interoperabilität zu edu-ID-Systemen in anderen Föderationen zu gewährleisten.

Letztendlich gilt es, ein umfassendes Betriebskonzept zu erarbeiten, das nicht nur die technischen Aspekte eines edu-ID-Systems, sondern auch die Finanzierung des Betriebs sowie rechtliche Rahmenbedingungen berücksichtigt. Eine ganz entscheidende Rolle wird hierbei auch dem Thema Datenschutz zukommen. Sobald auf konzeptioneller Ebene die wichtigsten Details geklärt sind, muss ein Datenschutzgutachten eingeholt werden. Es gibt also noch einiges zu tun.

Die bisherigen Ergebnisse der Arbeitsgruppe sind im DFN-AAI Wiki unter https://doku.tid.dfn.de/de:aai:eduid:start dokumentiert. Wer die Arbeit der Gruppe verfolgen oder sich auch an den Diskussionen beteiligen möchte, findet dort den Link zur Subskription der edu-ID-Mailingliste. ◆

Kurzmeldungen

Flex-Grid – Der nächste Schritt zum Terabit-Netz

Im Oktober 2020 startete ein Umsetzungsprojekt mit dem Ziel, das Wissenschaftsnetz X-WiN für zukünftige Anforderungen jenseits aktueller Bandbreitenbedarfe vorzubereiten. In der aktuellen Ausbaustufe ermöglicht die Optische Plattform des X-WiN Übertragungsraten von bis zu 200 Gbit/s je Verbindung, dafür kommt eine feste spektrale Breite von 50 GHz je Verbindung zum Einsatz. In der aktuellen technischen Implementierung können bis zu 88 Verbindungen je Glasfaserstrecke übertragen werden. Genutzt werden diese Verbindungen für das IP-Kernnetz sowie die Anbindungen von Teilnehmern und externen Netzen.

Durch den Einsatz der Flex-Grid-Technologie werden die Voraussetzungen geschaffen, um Verbindungen mit Übertragungsraten jenseits von 400 Gbit/s sowie mit optimierter Reichweite realisieren zu können. In Netzen auf Basis der Flex-Grid-Technologie wird das bisher starre 50 GHz Raster für optische Kanäle durch eine flexible Zuteilung des Spektrums in 12,5 GHz Schritten ersetzt. Dies ermöglicht eine bedarfsgerechte Allokation von optischer Bandbreite für die einzelnen Verbindungen, sodass die gewünschte Übertragungsrate über die geforderte Distanz zwischen den Endpunkten der Verbindung erreicht werden kann.

Um diese Vorteile nutzen zu können, muss die Optische Plattform in einem ersten Schritt mit Flex-Grid-fähigen ROADM (Rekonfigurierbare Optische Add-Drop-Multiplexer) ausgestattet werden. Beginnend mit einer Pilotinstallation im November 2020 werden im Laufe des Jahres 2021 weitere 19 der insgesamt 65 Kernnetzknoten mit der Technik bestückt und die notwendigen Soft- und Firmware-Upgrades durchgeführt. Mit Abschluss dieses Projekts ist der Weg zur bedarfsgerechten Einführung von 400 Gbit/s Technik auch auf der IP-Plattform bereitet. ◆

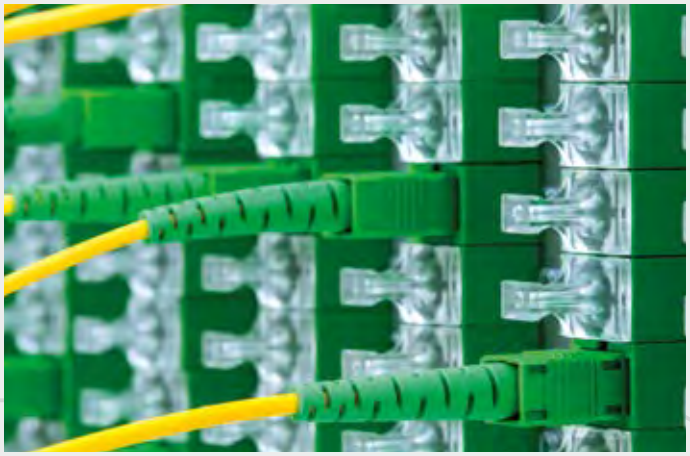


Foto: FactoryTh / iStock

Überholspur für Echtzeitverkehr

Nach einer Pilotphase im Sommer wurde Anfang Oktober 2020 eine Bandbreitengarantie für Echtzeitdatenverkehr auf allen Teilnehmeranbindungen an das Wissenschaftsnetz eingeführt. Diese stellt in Überlastsituationen sicher, dass IP-Pakete, die spezifisch markiert sind (IP Precedence 5), weiterhin mit einem garantierten Mindestanteil von zehn Prozent der Anschlussbandbreite übertragen werden. Liegt kein Echtzeitverkehr an, erhält der übrige Verkehr weiterhin die komplette Bandbreite des Anschlusses.

Die Maßnahme wurde ergriffen, um der Sprach- und Videokommunikation zu jedem Zeitpunkt ausreichend Übertragungskapazitäten bereitzustellen. Gerade unter den aktuellen Bedingungen mit dem vermehrten Einsatz von Onlinelehre und Homeoffice ist die störungsfreie Echtzeitkommunikation über das Wissenschaftsnetz von großer Bedeutung. Nutznießer ist aber auch der Dienst DFNFernsprechen, dessen Anschlüsse mit der Abkündigung von ISDN nun vollständig auf Voice-over-IP migriert werden.

Die entsprechende Markierung der Datenpakete erfolgt auf den jeweiligen Endsystemen und kann somit durch den Teilnehmer eigenständig vorgenommen werden. Diese Maßnahme kann natürlich nicht die Probleme einer ständigen Überbuchung der Anbindung nachhaltig lösen, jedoch in kritischen Situationen die Benutzbarkeit von Voice-over-IP oder Videoconferencing aufrechterhalten. Für Teilnehmer, die keinen Echtzeitverkehr über ihre Anschlüsse führen, hat der Mechanismus keine negativen Auswirkungen. Teilnehmer, die auf die Priorisierung dennoch verzichten wollen, können diese per Opt-out abwählen. Dazu wenden Sie sich bitte an das DFN-NOC unter noc@noc.dfn.de. ◆

Meine Suppe ess ich nicht – IPv6-Faktencheck

Jens Link (IT-Consulting) befasst sich bereits seit 2007 mit dem Thema IPv6, er hat in dieser Zeit zahlreiche Vorträge und Schulungen zu dem Thema gehalten und an einigen IPv6-Projekten mitgearbeitet. Zuletzt berichtete er auf der DFN-Betriebstagung im September 2020 über das Thema. Neben IPv6 liegen seine Schwerpunkte im Bereich Linux und Netzwerk.

Foto: PolaRocket/photocase.de

IPv6 ist die neueste Version des Internet-Protokolls, das Geräte über das Internet identifiziert, damit diese lokalisiert werden können. Das Protokoll ist seit 1998 in Arbeit, um neue Kapazitäten für die immer knapper werdenden IPv4-Adressen zu schaffen. Trotz seiner Effizienz- und Sicherheitsvorteile setzt sich IPv6 jedoch nur langsam durch. Seine persönlichen Erfahrungen, was die möglichen Gründe, Fake News und Ausreden bei der Umsetzung von IPv6 betrifft, teilt unser Autor in einem Faktencheck.

Text: **Jens Link** (IT-Consulting)

Viele werden jetzt schon aufgehört haben zu lesen. Ein Artikel zu IPv6. Nicht schon wieder. Können uns diese „Spinner“, die uns seit mehr als zehn Jahren erzählen, dass IPv6 wichtig ist, nicht endlich mal in Ruhe lassen? IPv6 macht doch keiner!

Wir haben doch noch genug IPv4-Adressen! Diese und andere Aussagen schaue ich mir hier einmal genauer an.

Zu unterscheiden sind drei Kategorien von Personen im IPv6-Kontext:

- Gegner – Das brauchen wir nicht! Nicht vor meiner Rente!
- Interessierte – Klingt interessant aber … und
- Macher, also Leute die IPv6 wirklich nutzen.

Eventuell liefert der Artikel ja den Interessierten und zum Teil auch den Machern einige Argumente (mehr), IPv6 zu implementieren. Das ist eigentlich nicht schwer und muss nicht viel Arbeit machen. Das Schwierigste ist, erst mal anzufangen.

Falls noch Gegner mitlesen, hier ein Tipp: unter https://ipv6excuses.com/ findet sich immer eine passende Ausrede.

IPv6 und der Autor

Am 6. Juni 2012 war der World IPv6 Launch Day, der Tag, an dem einige große Content-Anbieter IPv6 eingeschaltet haben. Am 5. Juni 2012 habe ich quasi mein erstes großes IPv6-Projekt abgeschlossen. Es ging darum, ein größeres Webportal IPv6-fähig zu machen. Alle von außen erreichbaren Dienste (WWW, DNS, SMTP) waren nach drei Monaten auch per IPv6 aus dem Internet erreichbar. Und das Ganze, ohne dass auch nur eine Person Vollzeit daran gearbeitet hat. Wie geht das? Es wurde miteinander geredet, die Administratoren kannten ihre Infrastruktur, die Entwickler ihren Code. Wurde ein Teil der Infrastruktur beziehungsweise des Codes angefasst, wurde gleich nach der IPv6-Fähigkeit geschaut. Keiner hat sich quergestellt, alle haben mitgemacht.

Dieses Projekt ist einer der Gründe, warum ich mich immer etwas schwer tue zu verstehen, was an IPv6 so kompliziert sein soll. Gab es Probleme? Ja, natürlich gab es die. Aber relativ wenige. Und damals hat das maximal ein Prozent der Nutzer mitbekommen. Heute sieht das ganz anders aus. Manche Fehler sind gar nicht offen als solche erkennbar und fallen erst dann auf, wenn mal jemand ganz genau hinschaut. Ein Beispiel hierfür sind Webserver in einem IPv6-fähigen Netz mit entsprechend konfigurierten Servern und den passenden DNS-Einträgen. Allerdings fehlen die entsprechenden Firewall-Regeln. Das Ganze fällt nicht auf, weil Webbrowser einen Mechanismus namens Happy Eyeballs haben, um solche Probleme zu umgehen. Der Browser fällt einfach auf IPv4 zurück und der Nutzer bekommt davon nichts mit.

Es gibt aber noch ein anderes Problem bei der Umstellung auf IPv6. Das (externe) Monitoring ist umfangreicher und wird daher oft nicht ausreichend umgesetzt. Dienste müssen überwacht werden, und wenn diese mit IPv6 und IPv4 betrieben werden, müssen auch beide Protokolle überwacht werden.

Die Gründe und die Ausreden

„Wir haben doch noch genug IPv4-Adressen."

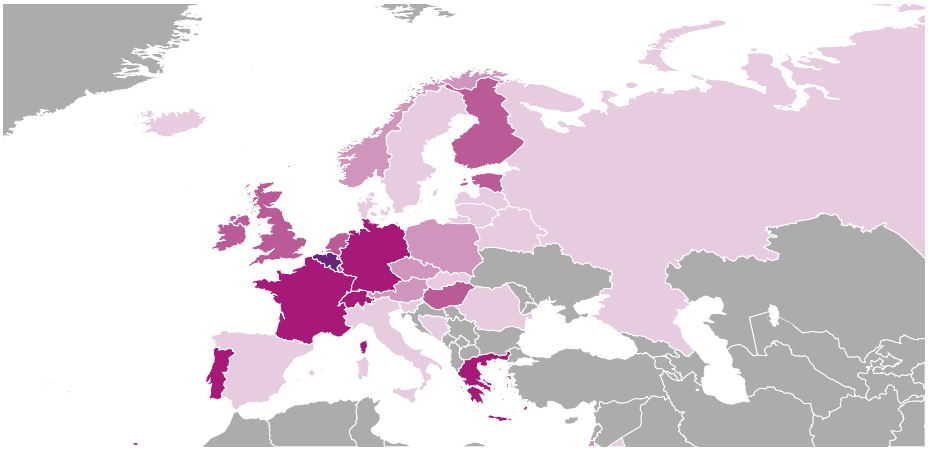
Widmen wir uns den üblichen Ausreden. „Wir haben noch genug IPv4-Adressen" ist die beliebteste Ausrede, egal ob bei Firmen, Behörden oder Hochschulen. Es mag ja sein, dass der Einzelne selbst genug Adressen hat, aber was ist mit dem Rest der Welt? Und wollen wir uns wirklich erst mit dem Problem fehlender Adressen beschäftigen, wenn keine mehr vorhanden sind?

Werfen wir einen Blick ins Internet: Die Internet Assigned Numbers Authority (IANA) hat 2012 ihre letzten /8er Netze an die fünf regionalen Internet Registries (RIRs) verteilt. Die RIRs, zum Beispiel das für Europa zuständige RIPE, haben ab diesem Zeitpunkt nur noch ein /22er Netz pro Mitglied vergeben. Das ist nun seit Ende 2019 auch vorbei, jetzt gibt es maximal nur noch Reste. Zwar existieren noch freie Adressen, aber diese kosten Geld. Der Preis pro Adresse liegt derzeit bei 22 Dollar und es braucht mindestens ein /24 Netz, also 256 Adressen, um diese zu bekommen. Bei größeren Netzen sind die Preise pro Adresse etwas günstiger.

Es gibt Firmen und Institutionen, bei denen sind neben den öffentlichen Adressen auch die privaten RFC1918-Adressen knapp. Diese wurden von der IANA für die Nutzung in internen Netzen reserviert und werden nicht im Internet geroutet. Ist dies der Fall, kommen einige Firmen auf die Idee, Netzwerkadressübersetzung, englisch Network Address Translation (NAT), oder sogar mehrfach NAT, zu nutzen. Andere verwenden irgendwelche reservierten Adressbereiche, 44.0.0.0/8 ist hier ein gutes Beispiel. Dieser Bereich wurde ursprünglich für den Amateurfunk reserviert, 2019 sind Teile davon an Amazon verkauft worden. Manche Firmen kaufen aber auch einfach zusätzliche öffentliche Adressen. Nur wenige führen gleich IPv6 ein. Erstaunlicherweise sind dies aber meist keine IT-Firmen. Projektanfragen zu IPv6 kommen unter anderem aus der Automobilbranche und von Versicherungen.

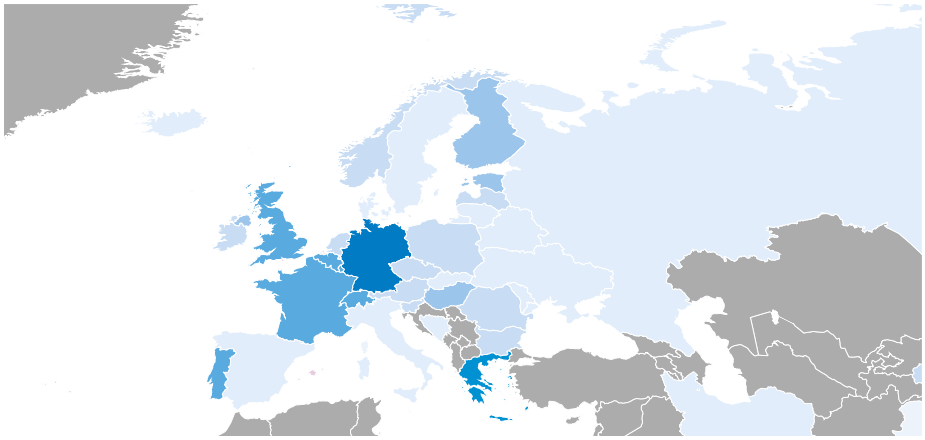
Auch vielen Zugangsprovidern gehen mittlerweile die Adressen aus. Bei einigen gibt es echtes Dual-Stack (DS), das heißt IPv4 und IPv6, bei anderen DS-Lite, dabei gibt es IPv6 und IPv4 per NAT vom Provider. Bei wieder anderen gibt es kein IPv6 sondern nur geNATetes IPv4. Die Nutzer merken davon in der Regel nichts, solange der Provider sein NAT-System nicht zu sehr überbucht, was auch immer mal wieder vorkommt, da die Hardware teuer ist und ausgenutzt werden muss. Nur bei bestimmten Spielen, VPN-Verbindungen und SIP kommt es immer wieder zu Problemen. In einem Vorgespräch zu einem IPv6-Projekt bei einer Versicherung hieß es: „Uns ist egal, wo wir mit IPv6 anfangen, aber die VPN-Gateways sind als erstes dran". Ein Großteil der VPN-Probleme entstand durch das NAT beim Provider.

ANBIETER GOOGLE



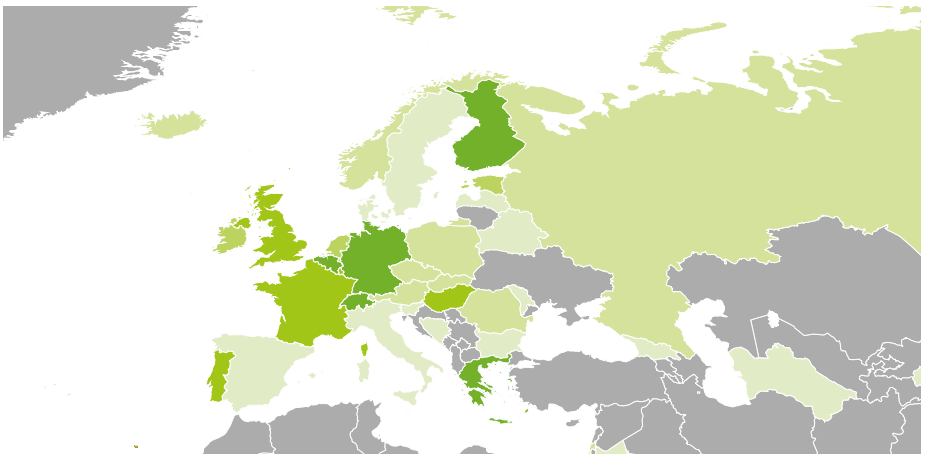
Anteil der IPv6-Zugriffe 1–10 % 11–20 % 21–30 % 31–40 % > 41 % Quelle: Google 10/2020

ANBIETER AKAMAI



Anteil der IPv6-Zugriffe 1–10 % 11–20 % 21–30 % 31–40 % > 41 % Quelle: Akamai 10/2020

ANBIETER FACEBOOK



Anteil der IPv6-Zugriffe 1–10 % 11–20 % 21–30 % 31–40 % > 41 % Quelle: Facebook 10/2020

Wieder andere, vor allem im Mobilfunkumfeld, machen gleich IPv6 only mit entsprechenden NAT-Mechanismen um in die IPv4-Welt zu kommen. T-Mobile US macht das seit Jahren so, T-Mobile Deutschland testet es gerade und ist sogar schon dabei es für bestimmte Endgeräte auszurollen. Apple und auch Facebook messen übrigens in Mobilfunknetzen eine bessere Performance per IPv6. Wer also VPNs und Dienste im Internet betreibt, sollte sich dringend mit IPv6 beschäftigen. Viele Nutzer werden es einem danken und wahrscheinlich wird auch weniger über schlechte Qualität gemeckert.

„IPv6 macht doch keiner."

Wie wir im vorangehenden Abschnitt gesehen haben, stimmt die Aussage zumindest für die meisten Zugangsanbieter nicht. Sie stimmt aber im Hochschulumfeld. Auch sind nur wenige Firmenwebseiten per IPv6 erreichbar. Eines der größten Ärgernisse aller IPv6 only-User ist hierbei wohl GitHub. GitHub dürfte, neben Stack Exchange, eine der am häufigsten genutzten Webseiten für Entwickler und Admins sein. Gerade hier ist es immer wieder problematisch, ein Repository auf einen IPv6 only-Host zu klonen. Wenn die eine Seite nur IPv4 und die andere Seite nur IPv6 kann, muss irgendwo eine Übersetzung stattfinden. Und das bedeutet zusätzliche Arbeit.

Einige große Anbieter wie Google, Facebook und Akamai haben aber seit langem IPv6 aktiv und veröffentlichen auch Statistiken dazu. Bei allen drei Anbietern kommen rund 50 Prozent der Zugriffe über IPv6 aus Deutschland.

Das Argument, dass am DE-CIX nur ein Bruchteil des Traffics IPv6 ist, stimmt teilweise. Jedoch ist zu beachten, dass längst nicht der gesamte Traffic über einen öffentlichen Internet Exchange geht. Außerdem ist es fraglich, wo diese Information herkommt. Der DE-CIX hat dazu seit Jahren keine Statistiken mehr veröffentlicht.

„IPv6 wird noch nicht richtig unterstützt."
Auch das stimmt leider, zumindest teilweise. Es ist jedoch möglich beim Einkauf von Hard- und Software die Augen aufzuhalten und die IPv6-Kompatibilität entsprechend in die Anforderungen mit aufzunehmen. Zumindest auf Bundesebene muss auf neu beschaffter Hard- und Software auch IPv6 only laufen können, in einigen Bundesländern gibt es ähnliche Vorschriften.

„Unsere Hard-/Software kann aber kein IPv6."
Ja, das kann ein Problem sein. Entweder ist die Hardware sehr alt oder beim Einkauf wurde nicht aufgepasst. Als Beispiel führt eine Hochschule das Firewall-Service-Modul (FWSM) von Cisco an. Dieses Modul läuft bereits seit März 2013 ohne Support, sollte also längst ersetzt worden sein. Aber ja, es gibt auch immer noch aktuelle Produkte, die kein IPv6 unterstützen. Daher ist es wichtig, dies beim Einkauf zu berücksichtigen und auch entsprechend zu testen. Außerdem ist es wichtig, den Herstellern mitzuteilen, warum ihr Produkt gegebenenfalls nicht genommen wurde.

Mögliche Folgen für IPv6-Verweigerer

Wird das Thema IPv6 verweigert, kann es unter Umständen zu komischen Seiteneffekten kommen. Trotzdem wird der Rat oder die Anforderung IPv6 abzuschalten, um eventuellen Problemen vorzubeugen, immer noch oft gegeben. Was man nicht kennt, braucht man nicht. Hier hilft es, mal zu schauen, was ein bekannter Hersteller dazu sagt:

„Internet Protocol version 6 (IPv6) is a mandatory part of Windows Vista and Windows Server 2008 and newer versions. We do not recommend that you disable IPv6 or its components. If you do, some Windows components may not function."

Ein anderes Beispiel ist das Netzwerk selbst. Wird IPv6 auf Netzwerkkomponenten bewusst deaktiviert, ist man noch lange nicht auf der vermeintlich sicheren Seite. Wenn, wie von Microsoft empfohlen, auf den PCs weiterhin IPv6 aktiviert bleibt, kann dieses relativ einfach missbraucht werden. So kann mit „Script-Kiddie"-Tools der IPv6-Verkehr gezielt umgeleitet, ausgespäht und manipuliert werden. Eine konkrete Umsetzung existiert mit „fake route" aus dem THC-Toolkit. Hier reicht der einfache Befehl, um IPv6-Router-Advertisements ins Netz zu injizieren:

```
fake_router6 wlp3s0 2001:db8:de-
ad:beef::/64 2001:db8::53 \
fe80::3884:aabb:fffe:ccdd
```

Mit diesem Befehl werden auf einem Interface (wlp3s0) ein Prefix (2001:db8:dead:beef::/64), ein DNS-Resolver (2001:db8::53) und ein Default-Gateway (fe80::3884:aabb:fffe:ccdd) announced.

Jeder moderne WLAN Controller beziehungsweise Switch sollte über entsprechende Mechanismen verfügen, um dies zu verhindern. Aber dazu muss man sich ja erst einmal ernsthaft mit IPv6 beschäftigen. Durch das Starten des Kommandos in einem nicht entsprechend gesicherten Netz spielt man selbst Router und zieht sämtlichen IPv6-Traffic zu sich, auch viel DNS-Traffic sollte einen erreichen. Alleine schon dadurch kann viel Schaden angerichtet werden.

Zum Schluss

Ja, IPv6 macht Arbeit. Es bietet aber auch die Möglichkeit, sich von Altlasten zu befreien, seine Infrastruktur aufzuräumen und gegebenenfalls neu aufzubauen. „Wir haben doch keine Zeit, uns mit IPv6 zu beschäftigen" ist die letzte Aussage, auf die ich eingehen möchte. Eventuell ist eine zu knappe Zeit ein Zeichen unzureichender Prozesse und fehlender Automatisierung. ◆

WEITERE INFORMATIONEN:

https://tools.ietf.org/html/rfc1918 fake_route
aus dem THC-Toolkit unter
https://github.com/vanhauser-thc/thc-ipv6

Herausforderung Onlineprüfung

An den meisten Universitäten und Hochschulen waren bisher Präsenzprüfungen das Mittel der Wahl, um den Nachweis für Studienleistungen zu erbringen. Seit dem Pandemie-Sommer experimentieren viele Einrichtungen nun mit Onlineprüfungen. Bis diese etabliert sind, müssen jedoch noch verschiedene Aspekte bedacht und geprüft werden.

Text: **Frank Schulze** (TU Dresden), **Nils Szuka** (FernUniversität in Hagen)

Foto: 06photo / iStock

Bedingt durch die Entwicklung der vergangenen Monate stellte sich zum Ende des Sommersemesters 2020 an vielen deutschen Hochschulen die Frage, wie mit den Prüfungen des vermittelten Lehrstoffes umzugehen wäre. Zwar waren Präsenzprüfungen am Ende prinzipiell möglich, erforderten aber einen enorm erhöhten Bedarf an Räumen, Beschäftigten und Zeit. Um die vorhandenen Ressourcen so effektiv wie möglich einzusetzen, aber trotzdem für die Studierenden kein verlorenes Semester entstehen zu lassen, kam schnell der Gedanke an Onlineprüfungen auf. Jedoch waren diese bis dahin an fast keiner deutschen Lehreinrichtung vorgesehen. Präsenzprüfungen waren bis dato annähernd überall das Mittel der Wahl.

Bei den Überlegungen zur Durchführung von Onlineprüfungen tauchen ganz neue relevante Punkte auf, die bisher wenig im Fokus standen. Dabei müssen Fragen des Persönlichkeitsrechts, des Datenschutzes, des Einsatzes von Informations- und Medientechnik und der organisatorischen Abläufe für alle Seiten zufriedenstellend und vor allem rechtssicher beantwortet werden. Darüber hinaus ist es wichtig, Lehrende wie auch Studierende gleichermaßen in diesem Prozess mitzunehmen.

Die verschiedenen Fachrichtungen haben unterschiedliche Anforderungen an die Erbringung einer Studienleistung. Nicht jede Disziplin kann Multiple-Choice-Tests nutzen, manche Studiengänge sind mündlich kaum prüfbar und wieder andere, wie beispielsweise künstlerische Fächer, benötigen Skizzen oder Zeichnungen. Daraus resultiert eine Reihe von verschiedenen Prüfungsordnungen und Ablaufplänen.

Onlineprüfungen sind einerseits mithilfe eines Videokonferenztools als mündliche und schriftliche Leistungsabfrage und

andererseits auch ohne Einsatz audiovisueller Medientechnik als rein schriftliche Klausur mit beschränktem Zeitbudget denkbar. In diesem Artikel soll nur auf digitale Prüfungen mit paralleler Verwendung eines Videokonferenztools eingegangen werden.

Datenschutz und Prüfungsrecht

Das geltende Datenschutzrecht stellt derzeit eine der wesentlichen Herausforderungen für die Umsetzung von Onlineprüfungen dar. Aufgrund der Komplexität der Datenschutz-Grundverordnung (DSGVO) und ihrer verschiedenen Ausgestaltungsmöglichkeiten sind allgemeingültige Aussagen nur schwer zu treffen. Die Tendenzen der konkreten Festlegungen in den einzelnen Bundesländern sind jedoch vergleichbar, sodass die praktischen Unterschiede letztlich gering sind.

Hinzu kommt, dass nach ständiger Rechtsprechung des Bundesverfassungsgerichts in Prüfungssachen dem Gebot der Chancengleichheit[1] im Lichte des Art. 12 Abs. 1 GG besondere Bedeutung zuzumessen ist. In diesem Zusammenhang wird derzeit diskutiert, ob unter anderem die Nutzung von Software zur Kontrolle und Überwachung der Umgebungsbedingungen (sogenanntes Proctoring) bei Onlineprüfungen angezeigt sei. Deren zulässige Intensität ist aber umstritten. Die Diskussion wird zusätzlich durch die Frage der Freiwilligkeit bzw. der Möglichkeit einer datenschutzrechtlichen Einwilligung verkompliziert.

Gerade die Nutzung der IT-Technik schafft eine Reihe von neuen Möglichkeiten eines Täuschungsmanövers bei gleichzeitiger verringerter Kontrollmöglichkeit des Aufsichtspersonals. Ein erstes „Gutachten zur datenschutzrechtlichen Zulässigkeit von Überwachungsfunktionen bei Online-Klausuren“ des Projektes „Rechtsinformationsstelle Digitale Hochschule NRW“ (Leitung Prof. Dr. Thomas Hoeren)[2] kommt zur Schlussfolgerung, dass eine eingangs- und verdachtsbezogene Kontrolle der Prüfungsumgebung und die generelle Kontrolle der Leistungserbringung zulässig seien. Das schließt aber nicht den technisch durchaus denkbaren Einsatz von Tools ein, die Tastatur, Mausbewegungen, aktives Fenster und eine Reihe weiterer digitaler Kontrollen ermöglichen. Der Einsatz eines virtuellen Hintergrunds verhindert die Sichtkontrolle durch die Aufsichtsperson und ist ebenfalls problematisch. Des Weiteren erlangt der Prüfling keinerlei Informationen darüber, wie lange und mit welcher Intensität er während der Sitzung gemustert wird. Gegenüber den mehr allgemeinen Blicken in Prüfungsräumen sind

> Der Prüfling erhält keinerlei Informationen darüber, mit welcher Intensität er gemustert wird

hier wesentlich detailgetreuere Bilder möglich. Digitale Aufzeichnungen der Online-Prüfung sind nach derzeitiger Rechtslage hochproblematisch und unzulässig. Es gilt, den Eingriff in die Privatsphäre zu berücksichtigen, die einerseits durch die Übertragung des persönlichen Umfeldes geschieht und andererseits durch die digitalisierte Verarbeitung der notwendigerweise übertragenen Medien, welche natürlich Bild und Ton darstellen, aber auch die Prüfungsleistung selbst. Die Durchführung von Onlineprüfungen stellt damit einen nicht unerheblichen Eingriff in die Privatsphäre der Studierenden dar.

Die Autoren des Gutachtens stellen fest, dass vor der Durchführung von Onlineprüfungen datenschutzkonforme Szenarien zu entwickeln und durchzuführen sind. Diese Szenarien seien mit der Freiheit von Forschung und Lehre sowie den prüfungsrechtlichen Fragen in Konkordanz zu bringen. Im Sommersemester 2020 lag hier, bedingt durch die Pandemie eine Zeitnot vor, da die deutsche Wissenschaftslandschaft inhaltlich nur unzureichend auf das Thema vorbereitet war.

Häufig haben sich die Prüfenden in ihrer Not mit „Einwilligungserklärungen“ der Prüflinge beholfen. Auch diese bieten aber rechtlichen Zündstoff. Sie müssen zwingend freiwillig sein und dürfen keine Nachteile bei Verweigerung nach sich ziehen. Folglich können sie von den Studierenden jederzeit (auch während der Prüfung) zurückgezogen werden, was wiederum ganz neue Probleme schafft. Diese Fragestellungen werden in den kommenden Monaten weiterhin Gegenstand lebhafter Diskussionen bleiben.

Technische Voraussetzungen und Anforderungen an die Videokonferenzsoftware

Die Anforderungen an die IT-Infrastruktur sind sowohl für die Bildungsstätte als auch für den Prüfling zu beachten. Die Einrichtung muss mindestens die notwendige Software (wie z. B. das Lernmanagementsystem, das Videokonferenztool und weitere relevante Programme) zur Verfügung stellen. Hier kann es schon zu ersten Problemen durch die unterschiedliche private Ausstattung mit Hardware kommen. Es sollten deshalb Mindestanforderungen definiert werden und Leihgeräte in ausreichender Zahl zur Verfügung stehen.

Aufseiten der Studierenden müssen eine ausreichend dimensionierte Internetanbindung, eine frei bewegliche Webcam, Audioequipment, eventuell ein Scanner und notwendige Software vorhanden sein.

1 BVerfG, Beschl. v. 25.06.1974 – 1 BvL 11/3, BVerfGE 37, 342, 353 f.

2 https://www.itm.nrw/wp-content/uploads/RiDHnrw_11.06.20_Gutachten-zur-datenschutzrechtlichen-Zulässigkeit-von-Überwachungsfunktionen-bei-Online-Klausuren.pdf

Eine zentrale Rolle in der Onlineprüfung nimmt die audiovisuelle Übertragungssoftware ein. Sie muss die Fernaufsicht mit einer störungsfreien und zuverlässigen Kommunikation ermöglichen. Gleichzeitig darf die Bedienung dieses Tools nicht im Vordergrund der Prüfung stehen, sondern es muss als normales Arbeitsmittel Verwendung finden, damit die eigentliche Leistungserbringung nicht beeinträchtigt wird.

Im Gegensatz zu den Empfehlungen für die üblichen Videokonferenzen am Rechner sollte aus Gründen der Kontrolle kein Headset verwendet werden. Damit ist die Gefahr des Echos durch einzelne Teilnehmer sehr hoch. Unter Umständen führt das sogar zu einer technisch bedingten Störung der Kommunikation. Hier liegt ein Dilemma vor, was sich nur durch teure, hochwertige Technik (wie z. B. Echocanceller) lösen ließe, die aber keinesfalls vorausgesetzt werden kann und darf.

Die Verwendung des Audiokanals während der Prüfung ist generell als problematisch

> Die Verwendung des Audio-Kanals während der Prüfung ist generell problematisch

anzusehen, da Videokonferenzsysteme keinen Modus kennen, der die gezielte Ansprache nur eines Teilnehmers ermöglicht, ohne dass es alle hören.

Ähnliche Probleme ergeben sich ebenfalls bei Nutzung des Chatkanals. Er muss einen Modus bieten, der oftmals als „privat" bezeichnet wird. Damit können Chatnachrichten direkt an nur eine Person gerichtet werden und erreichen nicht alle Prüflinge. Eine solche Möglichkeit muss genau wie beim Audio ausgeschlossen werden.

Da Onlineprüfungen oftmals aus Gründen der Effektivität für Gruppen mit hoher Teilnehmerzahl durchgeführt werden, ergibt sich ein weiteres Problem. Die wenigsten Videokonferenzsysteme am Markt lassen einen Modus zu, bei dem zwar die Aufsicht alle Teilnehmenden sieht, aber diese sich untereinander nicht. Wenn jeder jeden sehen kann, kann es durch die Vielzahl an bewegten Bildern leicht zu einer Ablenkung kommen. Andererseits gibt es wenig praktische Erfahrungen damit, wie viele Bilder eine Aufsichtsperson sinnvoll auf einem Bildschirm parallel verfolgen kann.

Um Einblicke in die Privatsphäre zu verhindern, sollten die Studierenden private Gegenstände, wie z. B. Fotos wegräumen oder für die Zeit der Klausur abdecken. Idealerweise stehen Tutorials oder einführende Veranstaltungen als Anleitungen zur Verfügung, und die Studierenden haben die Möglichkeit, die technischen Prozeduren vorab in einem Testraum auszuprobieren.

Erfahrungen der Fernuni Hagen

Die FernUniversität in Hagen bietet seit Jahren die Möglichkeit von Fernprüfungen an. Trotzdem ergaben sich auch für die dortigen Kolleginnen und Kollegen im Sommersemester 2020 ganz neue Herausforderungen.

An der Einrichtung wurden im Bereich Rechtswissenschaften insgesamt etwa 3.000 Onlineklausuren durchgeführt, was etwa 80 Prozent aller Prüfungen entspricht. Die institutionelle Akzeptanz war genauso vorhanden wie jene aufseiten der Studierenden. Deren größte Befürchtung war, dass die Noten dieses Semesters später durch die Wirtschaft als Notabschluss bewertet werden könnten und nicht dieselbe Wertigkeit in der Wahrnehmung hätten.

Bei den Dozierenden war die Akzeptanz gespalten, es ging hier von Ablehnung bis hin zu vollständiger begeisterter Mitarbeit an den neuen Möglichkeiten. Besonders das Problem der Identitätskontrolle und Chancengleichheit wurde kontrovers diskutiert. Als sehr positiv wurde hingegen die deutlich erleichterte Kontrolle der Arbeiten angesehen, da unleserliche Handschriften wegfielen und die Antworten parallel aufgabenweise korrigiert werden konnten.

Die Erkenntnisse des Frühjahrs flossen in die Vorbereitung der Onlineprüfungen im Herbst 2020 ein. Die stichprobenartigen Kontrollen der Identitäten und Prüfungsabläufe schafften einen gewissen Erkennungsdruck und wirkten positiv auf die Verhinderung von Täuschungsversuchen. Die Erfahrung zeigt, dass der virtuelle Testraum zu Beginn der Prüfung unbedingt geschlossen werden muss, da sonst eine erhebliche Anzahl von Studierenden diesen als echten Prüfungsraum ansieht und sich somit in den falschen virtuellen Raum begibt.

Fazit

Die dargelegten Fakten und Erfahrungen zum Thema Onlineklausuren zeigen deutlich, dass noch eine Menge Klärungsbedarf auf verschiedenen Gebieten gefordert ist. Obwohl eine Umsetzung technisch schnell handhabbar scheint, treten demgegenüber viele organisatorische und datenschutzrechtliche Fragen auf. Die Folgen der Entscheidung „Privacy Shields" des EUGH[3] sind noch nicht vollständig überschaubar und werden die künftigen Entwicklungen weiter beeinflussen. Auch die Bereiche der Barrierefreiheit, des Nachteilsausgleichs sowie der Verhinderung von Täuschungsmanövern müssen noch einmal lösungsorientiert bearbeitet werden. Die konsensorientierte Lösung dieser Einwände ist zeitintensiv und verlangt die Einbeziehung verschiedener Fachbereiche sowie Gremien und nicht zuletzt der Studierenden. Da diese offenbar keine Berührungsängste gegenüber den neuen Technologien und Abläufen haben, wird eine Entwicklung dieser Prüfungsform zu einem gleichwertigen Werkzeug des Nachweises von Studienleistungen unumgänglich sein. Trotzdem gilt es zu beachten: Je technisch voraussetzungsreicher die Prüfung wird, desto mehr kann es zur Ungleichbehandlung kommen. ◆

3 EuGH Entscheidung vom 16.07.2020 – Az.: C-311/18

Die Reifeprüfung

Nach einem Ausnahmesemester im Sommer stehen Universitäten und Hochschulen in Deutschland im Wintersemester erneut vor massiven Herausforderungen in puncto Lehre und Prüfungswesen. Mit dem Pilotprojekt Fernprüfungen hat die Technische Universität München (TUM) früh ein Experiment gewagt. Ein wichtiger Baustein sind die Proctored Exams, automatisiert beaufsichtigte Onlineprüfungen. Welche Erfahrungen sie damit gemacht haben, erzählen Mediendidaktiker Dr. Matthias Baume und die Studierenden Maximilian Frank und Lorenz Bayerlein.

Treffpunkt Videokonferenz Dr. Matthias Baume (unten rechts), Maximilian Frank (unten links) und Lorenz Bayerlein (oben links) im Gespräch mit Maimona Id (oben rechts) vom DFN-Verein.

Für die einen Totalüberwachung und ein klares Misstrauensvotum, für die anderen der Rettungsanker in Pandemiezeiten. An Proctored Exams scheiden sich die Geister. Können Sie das nachvollziehen?

Matthias Baume: Auf jeden Fall. Als Mediendidaktiker betrachte ich das Thema genauso kritisch – schon von Berufswegen. Wir reden schwerpunktmäßig über die beaufsichtigten Fernprüfungsformate – automatisiertes, AI-gestütztes oder menschliches Proctoring –, aber es gibt viele verschiedene Arten von Fernprüfungen: von der mündlichen ZOOM-Prüfung mit Videoaufsicht bis hin zur unbeaufsichtigten Uploadprüfung unter Zeitdruck.

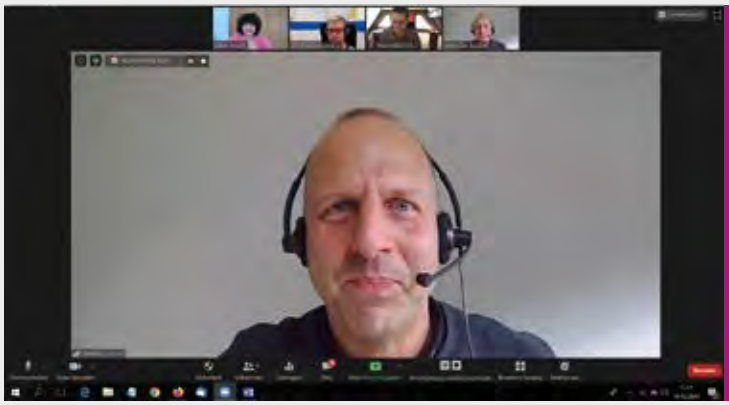
Der Begriff Onlineprüfung hat eine gewisse Unschärfe. Darum müssen wir das Thema differenziert betrachten, aber ohne Schwarz-Weiß-Malerei. An erster Stelle stehen für mich die Fragen: Wie können wir die unterschiedlichen Prüfungsformate sinnvoll einsetzen? Wo bieten sie einen Mehrwert?

Sie beschäftigen sich mit der Thematik ja nicht erst seit dem Ausbruch der COVID-19-Pandemie.

Matthias Baume: Zum Glück. Die COVID-19-Pandemie hat die Hochschulen im Sommersemester vor erhebliche Herausforderungen gestellt – insbesondere das Prüfungswesen. Prüfungen sind nach wie vor ein notwendiger Beleg für den Studienfortschritt.

Seit knapp zwei Jahren arbeite ich im Rahmen der Förderlinie „Internationalisierung 2.0“ des Freistaats Bayern am Projekt Fernprüfungen, das insgesamt auf vier Jahre ausgelegt ist. Wir hatten eigentlich erst in ein bis zwei Jahren unseren Rollout geplant. Doch als Anfang des Jahres die COVID-19-Pandemie ausbrach, haben uns die Ereignisse praktisch überrollt, das ganze Thema wurde stark gepusht. Aus Neugierde hatten wir bereits verschiedene Piloten gemacht, was uns die zügige Umsetzung in den Realbetrieb erleichtert hat. Trotzdem war noch einiges an Vorbereitungsaufwand hineinzustecken, wie z. B. Prozessabläufe aufzusetzen oder die Expertise der Dozierenden schulen. Mir sind derzeit nicht viele deutsche Hochschulen bekannt, die im Sommer Fernprüfungen in der Breite durchgeführt haben. Dafür braucht es nämlich einen gehörigen Vorlauf.

> „Unter strengen Infektionsschutzbedingungen ist es teilweise fast unmöglich Präsenzprüfungen vor Ort zu gewährleisten“



Dr. Matthias Baume studierte Pädagogik, Psychologie, Biologie und Mediendidaktik an der Universität Erlangen-Nürnberg. Er war als Projektleiter der zentralen Lernplattform Moodle an der TUM tätig, sowie als stellvertretender Leiter von ProLehre I Medien und Didaktik an der TMU. Aktuell leitet er das strategische Projekt „Fernprüfungen“.

Welchen Mehrwert genau bieten die Proctored Exams?
Matthias Baume: Wir haben an der TUM teils mehr als tausend Teilnehmende pro Prüfung. Unter strengen Infektionsschutzbedingungen ist es mit einem irgendwie überschaubaren Aufwand fast unmöglich, Präsenzprüfungen vor Ort zu gewährleisten, selbst im Audimax nicht. Man bräuchte glatt die doppelte bis dreifache Anzahl an Räumen und bedeutend mehr Personal für die Beaufsichtigung.

Einer der größten Vorteile der Proctored Exams ist die Möglichkeit, unter vergleichbaren Rahmenbedingungen eine beaufsichtigte Prüfung zu Hause oder außerhalb des Hörsaals durchzuführen. Das heißt, den Prüfling sicher zu authentifizieren und zu beaufsichtigen, damit Gerechtigkeit und Chancengleichheit für alle Studierenden gewahrt bleiben.

Der Mehrwert besteht zusätzlich ganz klar im Skalierungseffekt. Der ist generell bei elektronischen Prüfungsformaten entscheidend, weil ich mit deutlich geringeren Ressourcen eine große Kohorte prüfen kann. Zudem benötigen die Studierenden keine spezielle technische Ausstattung.

Maximilian Frank: Die TUM hat sehr viele ausländische Studierende, die aufgrund der Reisebeschränkungen während der Pandemie nicht einreisen können. Es ist jedoch wichtig, dass sie am Prüfungsbetrieb teilhaben können. In dieser Sondersituation ist die E-Prüfung ein probates Mittel, um den Studienfortschritt nicht zu gefährden. Die Studierenden müssen nicht warten, bis sie wieder an einer Präsenzprüfung teilnehmen können. Dadurch wird eine Chancengleichheit zu den Kommilitoninnen und Kommilitonen hergestellt, die vor Ort sind und eine Präsenzprüfung wählen können. Für uns Studierende war lange Zeit gar nicht klar, wie Lehre stattfinden soll und ob Prüfungen überhaupt möglich sind. Da bestand bei allen Beteiligten eine ganz große Verunsicherung, die auch sicherlich mit Ängsten einherging, was neue Prüfungsformate angeht.

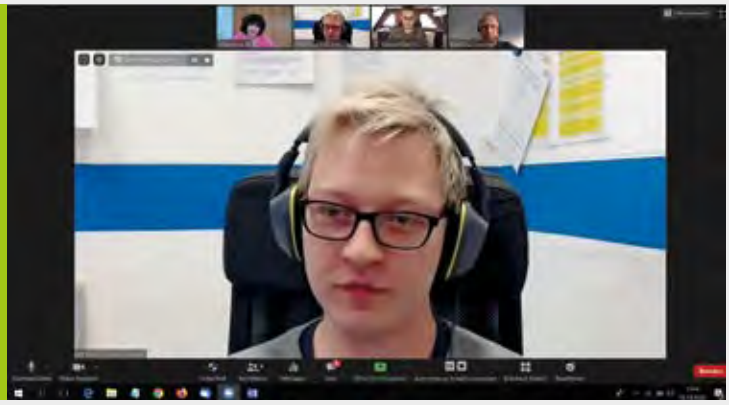
Welche Ängste waren das konkret?
Matthias Baume: Ich glaube gar nicht mal, dass die Ängste überwiegend eine konkrete Grundlage hatten. Es ist die diffuse Angst vor der Überwachung und vor einer technischen Lösung, die am Ende vielleicht das Prüfungsergebnis beeinflusst. Das ist ein komisches Gefühl, wenn man sich selbst in der Kamera sieht und quasi zum Aufzeichnungsgegenstand wird. Das ging mir definitiv genauso, als ich die verschiedenen Tools getestet habe.

> „Entscheidet ein Algorithmus völlig autonom, ob geschummelt wurde?“

Maximilian Frank: Wenn ich mich an der Nase kratze oder konzentriert in eine Ecke gucke, wertet der Algorithmus das schon als Täuschungsversuch? Und wie wirkt sich das auf meine Noten aus? Das sind Ängste, die definitiv bestanden und die ich auch nachvollziehen kann.

Wie haben Sie das erlebt, Herr Bayerlein? Sie haben ja nun Erfahrung aus erster Hand.
Lorenz Bayerlein: Ich hatte im Fach Politik eine Proctorio-Prüfung – allerdings an der Hochschule vor Ort im Hörsaal, weil

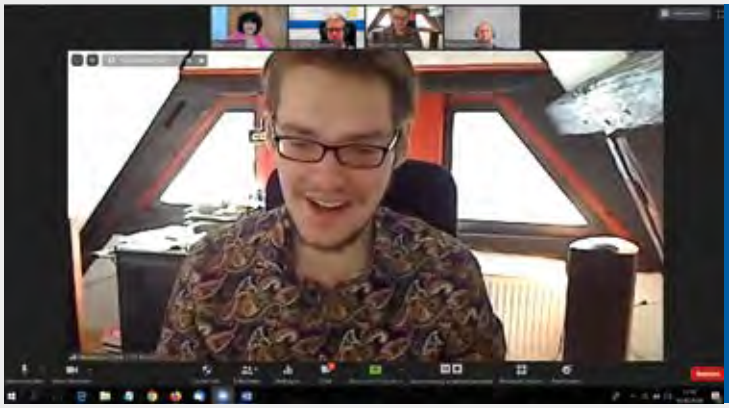
Lorenz Bayerlein studiert im Master „Mechatronik und Robotik“ an der Fakultät Maschinenwesen der TUM und ist Vertreter der Studierenden in der Fakultät.



ich Chrome nicht auf meinem Linux-Rechner installieren wollte. Wir hatten die Möglichkeit, die Prüfung von zu Hause, vom PC-Pool an der Uni oder in Präsenz zu schreiben. Da wurden zwar

„Eine Sache der Wahl“

lediglich Tastatur- und Mausbewegung aufgezeichnet, trotzdem fühlte ich mich überwacht. Das unbekannte Format sorgte für eine gewisse Anspannung und Aufregung, die ich zuvor so nicht gekannt habe. Für mich war das schon eine Mehrbelastung, verglichen mit der normalen Präsenzprüfung. Ein Nachteil war auch, dass die Kommunikation mit dem Aufsichtspersonal nicht möglich war, wenn z. B. eine Frage unklar formuliert war.



Maximilian Frank absolviert derzeit den Masterstudiengang Human Factors in Engineering an der TUM und ist Sprecher der LAK Bayern, dem Zusammenschluss der bayerischen Studierendenvertretungen auf Landesebene.

Zum Verständnis: Präsenz- und Proctored-Prüfungen fanden gleichzeitig statt, oder wie darf ich mir das vorstellen?

Matthias Baume: Die erfolgreiche Einführung neuer Formate steht und fällt mit der Akzeptanz. Ein ganz zentraler Punkt unseres Konzepts ist darum, dass die Studierenden frei wählen können zwischen Präsenzprüfung im Hörsaal und einer Fernprüfung mit automatisierter Beaufsichtigung. Ich habe sehr lange nach einem Tool gesucht, das mehrgleisige hybride Prüfungsvarianten mit flexiblen Aufsichtswerkzeugen erlaubt. Das Tool von Proctorio arbeitet wie eine Art Werkzeugkasten mit verschiedensten Optionen, was Beaufsichtigung und Sperrfunktionen betrifft. Wir nutzen den gleichen Prüfungstyp, nämlich die identische elektronische Prüfung und auch dieselbe Software. Aber bei der einen Variante zu Hause schalten wir die automatisierte Beaufsichtigung dazu, bei der Variante im Hörsaal wird der Rechner zwar abgesichert, damit ein Surfen im Internet nicht möglich ist, aber die restlichen Tools zur Beaufsichtigung werden abgeschaltet. Das Szenario ist bei beiden Varianten praktisch identisch, aber es kommen verschiedene Tools zum Einsatz. Einmal werden die Studierenden automatisiert beaufsichtigt und einmal durch die menschliche Aufsicht wie bei einer klassischen Prüfung.

Was haben Sie im Vorfeld noch getan, um Akzeptanz zu erreichen?

Matthias Baume: Damit Studierende und insbesondere Dozierende ihre Bedenken abbauen und Vertrauen in das Format fassen, ist sehr viel Kommunikation auf allen Kanälen notwendig. Wir haben sehr viel Arbeit in Infomaterial, Onlineveranstaltungen sowie in die individuelle Betreuung der Prüfungsverantwortlichen gesteckt.

Und auch der Datenschutz ist ein wichtiges Thema. Die Information beispielsweise, dass die Datenspeicherung auf deutschen Servern in Frankfurt liegt, ist für unsere Anwender essenziell.

Wichtig und auch rechtlich zwingend notwendig sind die Demoprüfungen zum Ausprobieren. Trotz vereinzelter, massiver Kritik im Vorfeld – so massiv, dass wir nicht wussten, ob wir einige Prüfungen überhaupt durchführen können – haben sich 85 Prozent der Studierenden, die die Demo- und Testprüfungen absolvierten, freiwillig für die Prüfung zu Hause entschieden. Das hat uns gezeigt, wie wichtig diese vorherige Erfahrung ist, damit die Studierenden mit einer gewissen Sicherheit in die eigentliche Prüfung gehen können.

Welche Möglichkeiten der Beaufsichtigung gibt es denn insgesamt?

Matthias Baume: Oh, da gibt es so einiges: von der Gesichts- und Stimmerkennung, dem Fingerknochenscan und der Tippanalyse bis hin zur Plagiatserkennung. An der TUM kommt aber nur ein Teil davon zum Einsatz.

Ein wichtiger Aspekt bei den beaufsichtigten Fernprüfungen ist natürlich die Kamera, in erster Linie für die Authentifizierung der Teilnehmenden und natürlich um die Chancengleichheit zu wahren, denn im Hörsaal gibt es ja auch eine Aufsicht, die Betrugsversuche unterbinden soll. Diese hat sogar mehr Einblicke als eine Kamera. Natürlich gibt es Tools mit 360-Grad-Kameras auf dem Markt, die nahezu eine Rundumüberwachung aus allen Winkeln erlauben. Genauso gibt es auch Dozierende, die gerne zwei oder drei Kameras mehr hätten. Aber das ist immer eine Abwägung, die letztendlich zulasten der Akzeptanz geht. Und aus Datenschutzgründen ist das überhaupt nicht möglich! Bevor wir die ersten Prüfungen gemacht haben, gab es zwar schon eine Anpassung der allgemeinen Studi-

enordnung der TUM, was aber gefehlt hat, war ein fundierter Rechtsrahmen, damit sich das Thema nicht in der Grauzone bewegt. Diesen gibt es nun. Da haben das Staatsministerium für Wissenschaft und Kunst und der Landesdatenschutzbeauftragte Prof. Petri gute Arbeit geleistet.

Durch unsere Vorerfahrungen mit den Formaten konnten wir von der TUM zwar verschiedene Argumente beitragen, aber es war sicherlich ein Ringen und Abwägen vonseiten des Ministeriums, die Rechtsverordnung am Ende passend auszugestalten.

Apropos Rechtsrahmen, Herr Frank: Die Landes-ASten-Konferenz (LAK) Bayern, deren Sprecher Sie sind, hat an der Bayerischen Fernprüfungserprobungsverordnung (BayFEV) kräftig mitgefeilt. Wie kommt es, dass sich andere Hochschulen aus rechtlichen Gründen klar gegen beaufsichtigte Fernprüfungen entschieden haben?

Maximilian Frank: Das liegt unter anderem daran, dass andere Hochschulen wenig bis gar keine Erfahrungen mit Fernprüfungen in dem Maße wie die TUM oder die Hochschule München hatten. So ein Konzept stampft man nicht mal eben aus dem Boden. Und wenn es in dem entsprechenden Bundesland dann noch nicht einmal einen rechtlichen Rahmen gibt, würde ich als Hochschulverantwortlicher den Aufwand auch nicht riskieren. Einige Hochschulen haben das Problem gelöst, indem sie Prüfungen auf das kommende Semester verschoben haben. In Bayern wurde zum Beispiel dafür die individuelle Regelstudienzeit verlängert, damit den Studierenden aufgrund verschobener oder entfallener Prüfungen keine Nachteile entstehen.

„Rechtsverordnung aus Maß und Mitte“

Wir sind relativ weit in Bayern. Obwohl die BayFEV erst am 16. September, also am Ende des Sommersemesters, erlassen wurde, gilt sie rückwirkend für das gesamte Semester. Damit schafft sie eine Rechtssicherheit für die bisher aufgesetzten Prozesse.

Was sind die wichtigsten Punkte in der Verordnung?

Maximilian Frank: Die Verordnung regelt sehr detailliert den Ablauf elektronischer Prüfungen und schafft verlässliche Mindeststandards. Das betrifft auch die starke Stellung des Datenschutzes. Technisch gesehen gibt es fast unbegrenzte Möglichkeiten der Überwachung, doch zu welchem Preis? Die Verordnung hält fest, dass ein Raumscan, wie ihn fast alle Anbieter im Portfolio haben, nicht zulässig ist (§ 6 Absatz 1 Satz 2 BayFEV). Wir haben uns daran orientiert, welches Maß an Kontrolle im Hörsaal üblich ist. Das sollte im digitalen Raum nicht anders ein. Im Hörsaal steht ja auch nicht hinter jedem Studierenden eine Aufsicht. Ein weiteres wichtiges Anliegen ist, dass die Studierenden ein Wahlrecht haben und nicht zu einer Fernprüfung verpflichtet werden können. Zum Thema Wahlrecht gibt es in der Verordnung einen eigenen Paragrafen (§ 8 BayFEV). Sogar die Möglichkeit, Probeklausuren zu absolvieren, ist in der Verordnung festgeschrieben – ein wichtiger Punkt, um Vertrauen in das Format zu schaffen. Die Verordnung gilt erst einmal für vier Jahre und enthält eine Klausel zur Evaluation, um nachzubessern. Als LAK Bayern haben wir im Rahmen der Verbändeanhörung auch Stellung zu der Verordnung genommen und freuen uns, dass viele für die Studierenden wichtige Punkte übernommen wurden. Die Verordnung ist die richtige Mischung aus Maß und Mitte und kann mit den darin enthaltenen Qualitätskriterien für andere Hochschulen als Orientierungshilfe dienen. Wir sind daher sehr zufrieden mit dem Ergebnis.

Und Sie, Herr Bayerlein? Was ist Ihr Resümee zum vergangenen Sommersemester?

Lorenz Bayerlein: Ich bin froh, dass mir das Semester nicht verloren gegangen ist. Unsere Hochschule hat keinen Aufwand gescheut, um uns faire Prüfungen und Lehre zu ermöglichen. Allein dafür stelle ich ihr sehr gute Noten aus.

Das letzte Wort haben Sie, Herr Baume.

Matthias Baume: Wir haben in den zurückliegenden Monaten gelernt, dass nichts selbstverständlich ist, aber auch, dass wir gemeinsam Lösungen erarbeiten können. Demzufolge, was mir Kolleginnen und Kollegen sowie unsere Rechtsabteilung rückmelden, werden die Fernprüfungen überwiegend recht positiv wahrgenommen. Studierende, die derzeit in Südamerika oder Asien sind, haben geschrieben, dass sie wahnsinnig dankbar sind, dass sie Prüfungen ablegen konnten. Das motiviert mich für die kommende Arbeit. Selbst wenn sich die Coronasituation hoffentlich wieder entschärft, könnte ich mir vorstellen, dass die Proctored Exams in puncto Familienfreundlichkeit und Internationalisierung künftig eine gute Alternative zu den Präsenzprüfungen sind. Wir sammeln derzeit immer mehr Erfahrungen mit dem Format und werden es kontinuierlich verbessern. Ich bin sehr gespannt, welche Entwicklungen noch auf uns warten.

Die Fragen stellte Maimona Id

Die Verordnung zur Erprobung elektronischer Fernprüfungen an den Hochschulen in Bayern (Bayerische Fernprüfungserprobungsverordnung – BayFEV) können Sie nachlesen unter: **https://www.stmwk.bayern.de/download/20638_BayFEV-mit-Begr%C3%BCndung-final_kurz.pdf**

OCRE: Frischzellenkur für die DFN-Cloud

Durch sein Engagement auf internationaler Ebene rund um die Cloud-Aktivitäten im GÉANT-Umfeld sorgt der DFN-Verein dafür, dass praktisch und beschaffungsrechtlich sicher umsetzbare Rahmenvereinbarungen für kommerzielle Public Cloud-Dienste für die Einrichtungen der deutschen Hochschul- und Forschungscommunity verfügbar sind. Im Rahmen des Projekts Open Clouds for Research Environments (OCRE) wird durch eine neue Vergabe nicht nur die Kontinuität der bestehenden Angebote erhalten, sondern es kommen zusätzliche attraktive Cloud-Plattformen zu optimierten Konditionen dazu.

Text: **Jakob Tendel** (DFN-Verein)

Foto: LaCozza/Adobe Stock

Digitale Dienste aus einer Cloud werden von den meisten Menschen bereits regelmäßig verwendet, zum Beispiel in Webanwendungen und mobilen Apps. Auch Hochschulen und Forschungsinstitute setzen in ihren IT-Lösungen vermehrt und zentral organisiert auf Cloud-Services für Teile der IT-Infrastruktur und als Plattform für

> Dieses Vergabeverfahren hat sich eindeutig bewährt

agile Forschung und Lehre. Seit 2017 hält der DFN-Verein über die externen Dienste der DFN-Cloud ein leistungsfähiges Angebot von Public-Cloud-Diensten vom Typ „Infrastructure-as-a-Service“ aus der europaweiten „GÉANT IaaS“-Vergabe bereit. Dieses Vergabeverfahren, in dessen Rahmen die Forschungsnetze für die Beschaffung zuständig sind, hat sich eindeutig bewährt. Die Rahmenvereinbarungen enden jedoch am 31. Dezember 2020. Deshalb findet derzeit im Projekt OCRE (Open Clouds for Research Environments) ein Nachfolgeverfahren nach dem gleichen Ansatz statt – ebenfalls unter der Koordination von GÉANT und mit Beteiligung des DFN-Vereins. OCRE verfolgt aber eine breitere Zielsetzung mit mehr als einem Vergabeverfahren und zusätzlich einem Programm zur finanziellen Förderung von Cloud-Nutzung in der Forschung. Der DFN-Verein informiert die Einrichtungen in Deutschland über die Ergebnisse der aktuellen Ausschreibung und unterstützt sie bei der Beschaffung und bedarfsgerechten Umsetzung der Serviceangebote.

Clouds in Hochschulen und Forschungsinstituten

Die Nutzung von IT-Ressourcen nach dem Cloud Computing-Prinzip ist schon jetzt an Einrichtungen allgegenwärtig. Auch der Aufbau von internen Private-Clouds oder das Teilen von Ressourcen in Community-Clouds hat eine längere Tradition. Die Einbindung von kommerziellen

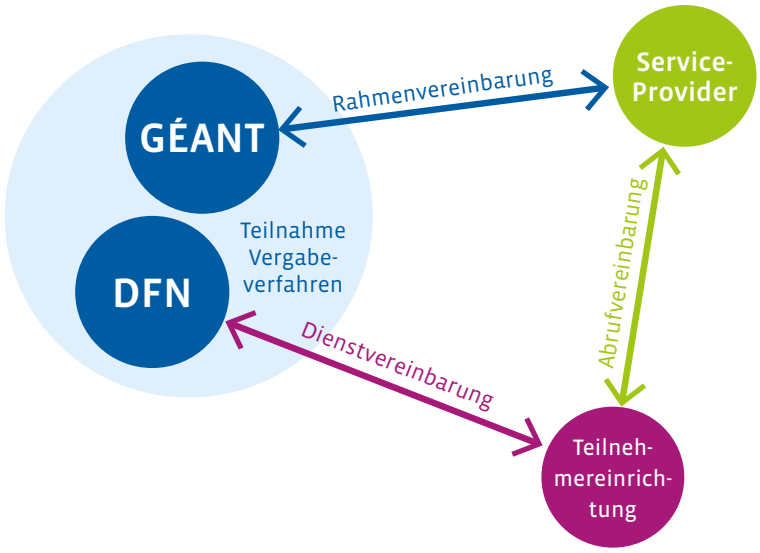


Abbildung 1: Beziehungsdiagramm bei der Realisierung der externen Dienste

Public Cloud-Angeboten birgt zwar vielfältige Chancen rund um Agilität und innovative IT-Anwendungen, aber auch Herausforderungen beim Datenschutz, bei der Beschaffung oder zum Beispiel bei der internen Abrechnung. Dabei unterscheiden sich die verschiedenen Zielgruppen innerhalb einer Einrichtung wie das Rechenzentrum, die Verwaltung, die Lehre oder die Forschung in ihren Traditionen und Erfahrungen im Umgang mit IT. Dazu kommt, dass diese sehr unterschiedliche Bedarfe, aber auch Hemmnisse bezüglich Cloud-Nutzung haben. Während beispielsweise das Thema Datenschutz in externen IT-Diensten für Anwendungen mit Personal- oder Studierendendaten berechtigterweise als noch nicht abschließend geklärt gilt, kann eine pragmatische Nutzung von Clouds im Wissenschaftsbetrieb abseits personenbezogener Daten bereits heute mit überschaubaren rechtlichen Risiken in Angriff genommen werden. Moderne Cloud-Plattformen bieten eine Funktionsvielfalt und Leistungsfähigkeit, die für jedes Vorhaben bedarfsgerecht zu konfigurierende IT-Umgebungen sehr individuell ermöglichen und so zu einer Produktivitätssteigerung im Wissenschaftsbetrieb beitragen können.

Das OCRE-Projekt

Das von der Europäischen Kommission im Rahmenprogramm Horizon 2020 geförderte Projekt OCRE tritt seit Projektbeginn Anfang 2019 unter anderem die Nachfolge des GÉANT-Cloud-Vergabeverfahrens „2016 IaaS“ an, jedoch getrennt

> Ein Ziel ist es, andere Konditionen der Cloud-Services zu optimieren

für Infrastruktur-Clouds und Satellitenfernerkundung. Als OCRE-Projektkoordinator hat sich GÉANT mit den Konsortialpartnern CERN, RHEA Group und Trust-IT zusammengetan, um deren Erfahrungen in der Anwendung und Bereitstellung von Cloud Services im Hochschul- und Forschungsbereich miteinzubringen. Ein Ziel der OCRE-Vergabeverfahren ist es, neben der Erfüllung der Ausschreibungspflicht im Interesse der Einrichtungen auch andere Konditionen der Cloud-Services zu optimieren. Diese umfassen unter anderem Rabatte, Befreiung von Datentransfer-

gebühren, einrichtungsfreundliche Lizensierung und Abrechnungsmodelle.

Das „IaaS+"-Vergabeverfahren

Das erste OCRE-Vergabeverfahren für neue Cloud Computing-Services richtet sich an Dienste vom Typ „Infrastructure-as-a-Service" (IaaS). In diesem „IaaS+"-Vergabeverfahren werden erneut Compute & Storage-Dienste ausgeschrieben, die jedoch nun neben einer serverbasierten VM-Architektur (IaaS) auch äquivalente Serverless-Dienste vom Typ Platform-as-a-Service (PaaS) inklusive Spezialanwendungen wie beschleunigtes Machine Learning abdecken. Unterstützende, herstellereigene Software Services (SaaS) aus dem jeweiligen Plattform-Marketplace sind ausdrücklich mit eingeschlossen, reine SaaS-Angebote für Dokumentbearbeitung, Kollaboration oder Ähnliches von Drittanbietern aber nicht.

Kriterien

Die Ausschreibung definiert einen Satz Minimalkriterien, die jedes Gebot erfüllen muss. Zusätzlich gibt es einen Satz Bewertungskriterien, die nach einem Punkteschema benotet werden. Dieses wird bei der Vergabe zur Auswahl des meistgeeigneten Anbieters pro Plattform pro Land verwendet und steht Einrichtungen zur Unterstützung ihres Abrufverfahrens zur Verfügung.

Minimalkriterien:

- Identity Management: SAML2/ OIDC-Unterstützung
- Egress-Gebühren: Erlass von Datentransfergebühren
- Mitnutzung: Cloud-Ressourcen für externe Partner von Forschungsverbünden mitnutzbar
- Lizenzen: Bring Your Own License (BYOL): Umfang der Unterstützung für Nutzung existierender Lizenzen in der Cloud-Umgebung

Zusätzliche Bewertungskriterien:

- Onboarding, Beratung und Tech-Support
- Infomaterial und -veranstaltungen
- Exit Support
- Kosten: diverse Kategorien von Preisnachlässen
- Nachhaltigkeit, CO_2-Fußabdruck

Auswahlverfahren für Einrichtungen

Für Einrichtungen, die einen Bedarf an Cloud Services haben und vor der Auswahl eines Anbieters stehen, empfiehlt OCRE folgenden beschaffungsrechtlich korrekten Ablauf:

1. Abgleich des Bedarfs mit den Dienstangeboten
2. bei einem alternativlosen Angebot einer Plattform -> **Direktabruf**
3. bei mehreren in Frage kommenden Plattformen -> **geleiteter Direktabruf** „Schreibtisch Miniwettbewerb": eine Anleitung hierfür stellt der DFN-Verein bereit
4. bei keinem ausreichenden Angebot-> per **Miniwettbewerb** nachgebesserte Angebote einholen, daraufhin Direktabrufprozedur anwenden

Timeline des Vergabeverfahrens

Ab 2021 werden die neuen Rahmenvereinbarungen in den externen Diensten der DFN-Cloud verfügbar sein. Diese haben eine Gültigkeitsdauer von vier Jahren. Abrufvereinbarungen können eine Gültigkeitsdauer haben, die darüber hinausgeht.

Verfügbare Dienstangebote

Eine Information über die unter OCRE-IaaS+ verfügbaren Dienstangebote kann erst nach Abschluss des Vergabeverfahrens und der Veröffentlichung der Rahmenvereinbarungen kommuniziert werden.

Integration in die DFN-Cloud

Die Vertragsgestaltung sieht eine Konstellation aus der Rahmenvereinbarung (Framework Agreement) zwischen GÉANT und dem Anbieter und aus der subsidiären Abrufvereinbarung (Call-off Agreement) zwischen Einrichtung und Anbieter vor. Der DFN-Verein koordiniert diesen Vorgang in seiner Rolle als Vermittler im Rahmen der externen Dienste der DFN-Cloud. Nach dem Abschluss einer Abrufvereinbarung beendet eine Einrichtung die restliche Beschaffung bilateral mit dem Anbieter – unter den Konditionen des Rahmenvertrags. ◆

Eine Übersicht über die aktuell in der DFN-Cloud verfügbaren Dienste erhalten Sie unter **https://www.dfn.de/dfn-cloud/**

Brazil-Germany Connection: Long-Term Partnership

The relations between the Brazilian and German research networks go back a long way. Just one year after DFN-Verein was founded, a delegation of network researchers visited the Berlin office to learn about German network design. Since then, there have been many joint collaborations, such as the BELLA project (Building the Europe Link with Latin America). Successful cooperation between the NRENS has never been more important.

Text: **Nelson Simões** (Director General of RNP)

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.

The first article[1] written and illustrated about Brazil is by Hans Staden, marksman and adventurer from Hessen, published in 1557 in Marburg. It was a success in several languages. Its report, imaginative though factual, filled with an acute sense of observation, caused an enormous impact at the time.

Almost three hundred years later, Spix, zoologist, and Von Martius, botanist, had to attend to a wedding in Rio de Janeiro. Science was part of the bridal price for the future empress of Brazil, Maria Leopoldina, archduchess of Austria, to be wedded to Emperor Pedro I. Here they remained for two years exploring the Brazilian biomes and, in 1820, published "Travels in Brazil". For 66 years, the Brazilian, Austrian and Bavarian crowns sponsored the compilation of Flora Brasiliensis [2]: a pioneering study on biodiversity which catalogued 22,767 species, thousands previously unknown – by the way, we toast the 200th anniversary of this famous and yet incredible scientific joint venture! Almost two hundred years later, a certain captain named Lahm, accompanied by other top marksmen, in the semifinals of the soccer World Cup… Well, actually, we don't have enough space to talk about our historical bonds.

1 https://archive.org/details/staden/mode/2up
2 https://www.biodiversitylibrary.org/item/9629#page/1/mode/1up

Because Germany is currently Brazil's fourth largest commercial partner, there are numerous interests and cooperation on very diverse and traditional subjects such as biodiversity, climate, energy, telecommunications, health, and among others, obviously, research networks.

Cooperation also between academic networks

Exchange between the academic communities also has been going on for a long time. For instance, the study on traffic viability for the submarine cable between Brazil and Europe performed in 2011, showed out that our greatest traffic volume was with Germany. Long before that, in June 1985, in order to create the Brazilian academic network, a group of network researchers paid a visit to the Deutsches Forschungsnetz (DFN) installations. Out of this visit, a national initiative based on the DFN design started being outlined. During the pre-internet era, we were initially supported to explore ancient technologies for electronic mail (X.400).

Learn about RNP

Created by the academic community in September 1989, the National Education and Research Network (RNP) was the precursor of the internet in Brazil, operating the first national backbone in 1992 and assisting its dissemination to society. Challenged to drive the progress of science and education in the country through information and communication technologies, the institution evolved over the years, leading several new initiatives. Learn more about some of them.

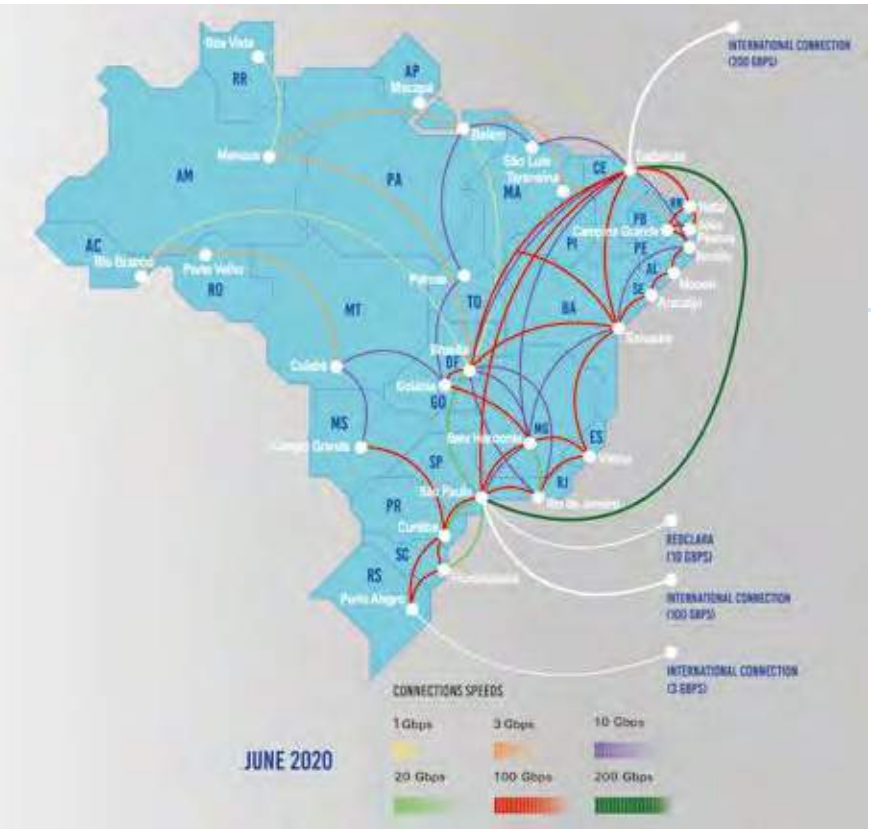


Figure 1: Benefit for millions of users: RNP System connects all 26 states and the Federal District

RNP System

The RNP System is responsible for the digital services platform for education, research and innovation in the country. Its base is supported by a high-performance network infrastructure, available throughout Brazil, interconnected with community networks in dozens of cities and a service portfolio for students, teachers and researchers.

The RNP System is available in all 26 states and the Federal District, through Presence Points in the states, connecting 1,529 campi [3] of higher education institutions and research units in the country. And what does that represent? Over four million users benefiting from an infrastructure of advanced networks for communication and experimentation, integrating higher education, research institutes, teaching hospitals, innovation environments and museums.

Services and collaborative networks

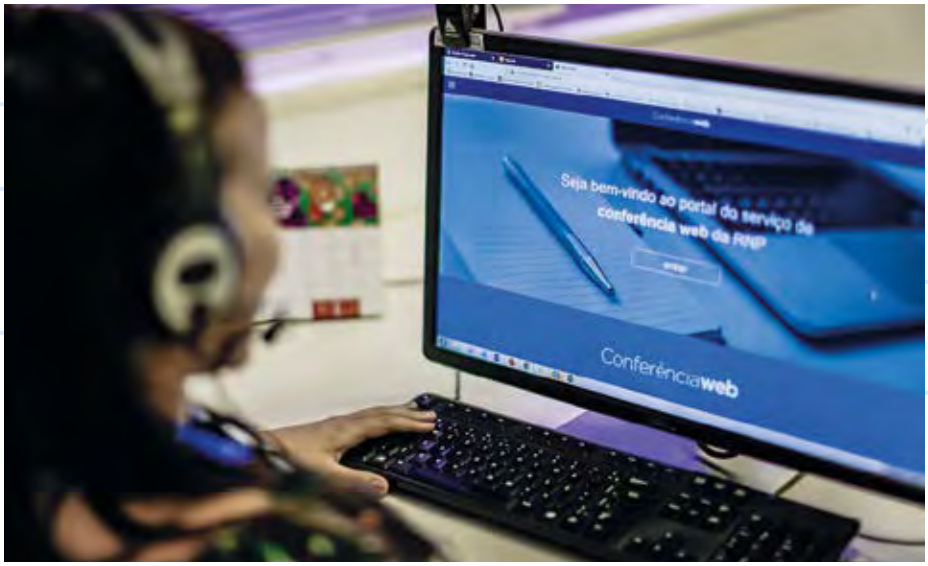
RNP also provides collaborative networks for specialists. An example of that is the Telemedicine University Network (Rute), which seeks to support improvement of existing telemedicine projects[4] and stimulates emergence of future interinstitutional projects through its work groups, who promote regular video sessions for debates, case discussions, classes, research projects and remote evaluations.

This year, with the COVID-19 pandemic, the COVID19 BR[5] group was created which promoted a unique experience for various professionals not only in

3 https://viaipe.rnp.br/?&aglomerado=0#@-12.404388944669792,-52.16308593749999,5z

4 https://www.rnp.br/en/news/incor-teleuti-supports-hospitals-public-network-combat-pandemic

5 https://www.rnp.br/en/news/sig-covid19-br-concludes-40-sessions-more-2-thousand-registered-participations



Communication in pandemic times: RNP expanded their video collaborative services.
Foto: APphoto Images, Antonio Pinheiro

Brazil, but also China, Italy, and others, with exchange of information on the disease, sessions on impactful themes such as health of native populations, vaccines, lab testing, as well as dentistry, nursing and physiotherapy support for patients.

"A collaborative network of specialists like Rute generates innovation, knowledge, permanent training and stimulates research. For this reason, academic networks and Rute are so important for Telehealth", comments Luiz Ary Messina, Rute's national coordinator.

During this pandemic period, one of the RNP's greatest challenges was to expand video collaborative services[6] for the education and research community to hold meetings, thesis and dissertation defenses, not to mention distance learning. In order to meet this rising demand, there was an extraordinary effort from the whole staff, along with the sharing of the computer infrastructure among several RNP System customers.

Brazil's continental size makes it difficult to improve the RNP System user experience in all locations. A successful alternative has been the Community Networks[7] Education and Research program. Together, universities and other customer organizations jointly implement and maintain high-speed network solutions. These networks in the country's metropolitan areas, and especially in inland cities with a high density of campuses are scalable and sustainable over the long term. The impact on education, research groups and establishment of highly qualified professionals in these cities is very relevant, not to mention the savings attained.

International Collaboration

The development of international partnerships is part of the RNP's purpose. For this reason, there have always been various collaborative projects with other countries.

RedCLARA

RNP was the founder of the Latin American Cooperation of Advanced Networks (CLARA)[8], our regional research network, through which we integrate ourselves with our Latin American neighbors and Géant's European network. This network, on the other hand, was created driven by the visions of the European Commission, national research networks and Géant, who were organized through the ALICE (Latin America Interconnected to Europe) Project, in 2003.

Figure 2: EllaLink – the first direct connection between Latin America and Europe

6 https://www.rnp.br/en/news/web-conference-rd-notification-service
7 https://www.rnp.br/en/news/institutionalized-and-developed-redecomeps-receive-certificate-rnp
8 https://www.redclara.net/index.php/en/

BELLA Project

RNP also participates in the BELLA (Building the European Link to Latin America) Project's consortium, an initiative which, by May 2021, will allow for the first modern direct connection between Latin America and Europe. A submarine system with exclusive and ample capacity to meet the needs of education and research communities of both regions for the next 25 years. Bella will benefit several areas that need this technology, such as those of the Earth observation (Copernicus) [9] and astronomy.

"BELLA is a very important cooperation project of academic networks from Europe and Latin America, led by Géant and RedCLARA, in which RNP and DFN are also part", comments Eduardo Grizendi, Director of Engineering and Operations.

"Chile is one of the countries with the driest climate in the world, thus making its sky very clear for optical observations. That is why Europeans, as well as Japanese and Americans have invested in observatories in the country which continuously generate a large amount of data", clarifies Michael Stanton, Network Scientist at RNP.

Africa Connection

The AARCLight Project[10] is a cooperation program with the United States, which implemented a direct connection between Brazil and Angola, being the first south-south intercontinental connection for research purposes between America and Africa.

Subsequently, the partnership with the research network in South Africa, SANREN/TENET, allowed this high direct connectivity to expand to the South and East of Africa (Ubuntunet Alliance networks). This direct connection will strengthen our traditional cooperation with Morenet, Mozambique's academic network. Thus, Europe, America and Africa are very close to having a direct integration between their education and research communities, thanks to the intense cooperation of their national and regional networks.

R&D in Cooperation with Europe

RNP manages R&D projects between research groups in Brazil and Europe, as a result of joint projects on subjects agreed upon between the Brazilian Science, Technology & Innovation Ministry and the European Commission. Some of these projects have had the participation of German researchers such as Futebol [11], infrastructure for research and 5G-Range[12] in 5G access to isolated areas. Other cooperations between Brazil and Germany, such as Cherenkov Telescope Array, CTA[13], are part of the support we provide to e-science. We have also collaborated to develop and integrate, together with other research networks, monitoring facilities such as Perfsonar[14] and the use of dynamic end-to-end circuits (Meican)[15].

"Participating in the research collaboration with other academic networks and institutions allows RNP to keep itself at the forefront of technology and provide advanced services to Brazilian scientists", explains Iara Machado, Director of Research, Development and Innovation.

For the coming years

The pandemic revealed the limitations we have and required reinvention of our plans. Our challenges have been increased to support and sustain the innovative use of technology in education and research, safely integrating, not only the campus, but our students' and teachers' homes. Simplifying and humanizing remote work. We have discovered that there are competencies we need to develop. "We have learned and developed solutions collaboratively. Successful cooperation with the other research networks has become even further important. Sometimes, it's the personal contribution of a leader, the integration of specialists, a common production process, an experiment, an idea. It has been like this for several years, and this is the common thread wire for the future", concluded Nelson Simões, RNP's Director General. ◆

9 https://www.rnp.br/en/news/copernicus-technology-allied-earth-observation
10 https://www.rnp.br/en/news/digital-academic-route-connects-usa-brazil-and-south-africa-now-activated
11 http://www.ict-futebol.org.br/
12 http://5g-range.eu/
13 https://www.cta-observatory.org/
14 https://www.rnp.br/en/servicos/experimentos-avancados/eciencia/monipe
15 https://ieeexplore.ieee.org/document/8002814

Sicherheit

Security Operations im DFN – ein neuer Dienst entsteht

In der Informationssicherheit hat in den vergangenen Jahren ein Paradigmenwechsel stattgefunden. Neben der reinen Prävention, das heißt der bestmöglichen Absicherung von IT-Systemen, sind Detektion und Reaktion in den Fokus gerückt. Eine Kompromittierung muss jederzeit als potenziell möglich angesehen werden. Daher müssen entsprechende Maßnahmen ergriffen werden, um einen definierten Betriebszustand auch in diesem Fall sicherstellen zu können. Die DFN-Dienste mit Sicherheitsbezug sollen daher in den kommenden Jahren sukzessive erweitert werden. Dazu sollen die Dienstleistungskategorien Prävention, Erkennung und Reaktion des DFN-Vereins intensiver miteinander verzahnt werden und neue Werkzeuge zum Einsatz kommen, um insbesondere die Bereiche Erkennung und Reaktion zu stärken. Ergebnis wird ein neuer DFN-Dienst für Security Operations (SecOps) sein.

Text: **Ralf Gröper** (DFN-Verein)

Foto: noblige / iStock

Nur durch gemeinsame Anstrengungen wird es gelingen, eine nachhaltige und finanzierbare Verteidigung gegen die zunehmend komplexeren Cyberangriffe auf Wissenschaftseinrichtungen aufzubauen und damit den Verlust von Daten oder den Ausfall von IT-Infrastrukturen zu verhindern. Sicherheitsvorfälle zeitnah zu erkennen und dies als Ausgangspunkt für eine angemessene Reaktion zu nutzen, ist eine Aufgabe, die effizient nur von einer Gruppe von Sicherheitsexperten zentral wahrgenommen werden kann. Know-how aufbauen, Personal bereitstellen und geeignete Hard- und Software einkaufen, das alles wäre in Eigenregie von einzelnen Einrichtungen deutlich aufwendiger und für viele gar nicht zu leisten. Diese Aufgaben sollen in einem neuen Dienst gebündelt werden. Dafür werden in der Vorbereitung vor allem die Erfahrungen des DFN-CERT genutzt.

Es gilt, die hierfür notwendige technische Infrastruktur aufzubauen und zu betreiben, sowie ein Team von Analysten zu bilden, die diese Infrastruktur nutzen, um die in der Infobox beschriebenen Mehrwerte zu erreichen. Dieses Team wird in Form eines Security Operations Centers (SOC) realisiert.

Für die eigene Infrastruktur des DFN-Vereins sowie die der Teilnehmer sollen durch den neuen Dienst folgende Mehrwerte geschaffen werden:

- Live-Erkennung von Angriffen auf IT-Infrastrukturen durch fortwährende Analyse von Log- und anderen Daten auf Basis bekannter Angriffsmuster (sogenannte Indicators of Compromise, IoCs)
- Analyse der gesammelten Daten und Suche nach bisher unbekannten Bedrohungsmustern, um diese dann automatisiert erkennen zu können (Erstellung eigener IoCs, allgemeiner: Aufbau eigener Threat Intelligence)
- Regelmäßige Bereitstellung von Lagebildern zur aktuellen Bedrohungslage

Aktueller Stand

Über den bestehenden Dienst DFN-CERT können Teilnehmer auf aktuelle Schwachstellen von verbreiteten Softwaresystemen zugreifen, Informationen zu erkannten Vorfällen, die direkt ihre Einrichtung betreffen, erhalten und ihr eigenes Netz in einer Außenansicht auf aus dem Internet erreichbare Ports scannen. Dazu können über das DFN-CERT-Portal automatische Warnmeldungen, Schwachstellenmeldungen und der Netzwerkprüfer eingerichtet und konfiguriert werden.

Durch ein Filtersystem können die Meldungen aus diesen Diensten nach Meldungstyp sortiert und nach Schweregrad und Netzbereich gefiltert werden. Danach werden sie direkt den zuständigen Verantwortlichen in der betroffenen Einrichtung zugestellt. Darüber hinaus ist im Dienst DFN-CERT die Incident Response, also die Unterstützung bei Sicherheitsvorfällen durch die Experten des Incident Response-Teams, enthalten.

Durch die Einführung der SecOps im DFN und durch den Betrieb einer technischen Plattform zur Erkennung von Cyberangriffen sollen die Qualität der Meldungen und der Nutzen für die Teilnehmer deutlich erhöht werden. Der wesentliche Mehrwert, also die Identifizierung von Angriffen, ergibt sich jedoch nur, wenn Anomalien im Netzwerk oder sicherheitsrelevante Ereignisse in der eigenen Infrastruktur erfasst und ausgewertet werden. Daher sind einige neue Komponenten im Portfolio der sicherheitsbezogenen DFN-Dienste notwendig, die dann im neuen Dienst gebündelt werden.

Neue Dienstkomponenten

Die SecOps im DFN zeichnen sich zukünftig durch die im Folgenden beschriebenen Komponenten aus.

Threat Intelligence

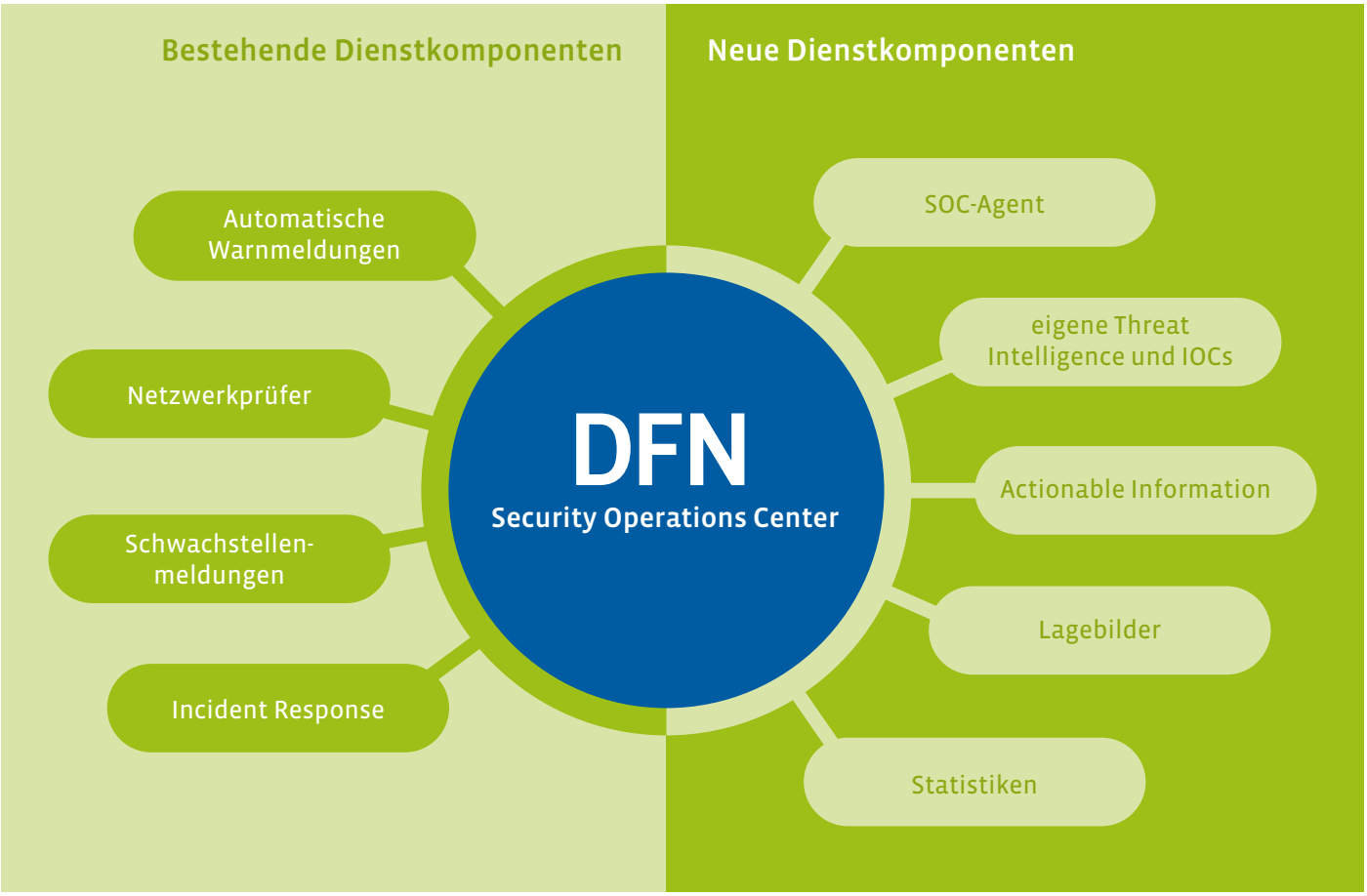
Die erfolgreiche Abwehr von Cyberangriffen ist nur möglich, wenn in die Auswertung kontinuierlich Informationen über neue Angriffsmethoden, Schwachstellen oder IoCs einfließen. Es ist offensichtlich, dass die Gewinnung dieser Informationen, in Summe auch als Threat Intelligence bezeichnet, nur mit hohem Aufwand und hinreichend technischen und personellen Ressourcen möglich ist. Daher bieten auch kommerzielle und nichtkommerzielle Sicherheitsdienstleister Threat Intelligence Feeds mit den entsprechenden technischen und/oder strategischen Informationen an. Die eigene Erzeugung von Threat Intelligence aus dem Wissenschaftsnetz mit der Einbindung der Hochschulen, Forschungseinrichtungen und den forschungsnahen Unternehmen hat jedoch einen entscheidenden Vorteil: Mit einer zentralen Auswertung und Informationsgewinnung

durch Analysten des DFN-CERT, die seit über 20 Jahren vertrauensvoll mit den DFN-Teilnehmern zusammenarbeiten und deren Anforderungen und Bedürfnisse genau kennen, kann dies wesentlich zielgruppenspezifischer und effizienter realisiert werden, als es einem externen Sicherheitsdienstleister möglich wäre.

Warnmeldungen über erkannte Sicherheitsvorfälle

Der bestehende Dienst DFN-CERT informiert die Teilnehmer über kompromittierte IT-Systeme, die außerhalb des eigenen Netzwerks auffällig geworden sind. In den meisten Fällen kann daher von einem bereits in der Vergangenheit erfolgreichen Angriff ausgegangen werden. Soll aber die Ausbreitung von Schadsoftware, wie zum Beispiel Emotet verhindert oder APT-Angriffe (Advanced Persistent Threats – also zielgerichtete Angriffe durch gut ausgestattete Angreifer) detektiert werden, so ist das nur möglich, wenn sicherheitsrelevante Ereignisse in der zu schützenden Infrastruktur selbst erfasst und ausgewertet werden. Probate Informationsquellen sind beispielsweise Syslog-Server und, soweit vorhanden, Intrusion Detection Systeme (IDS) oder Honeypots. Durch deren Einbindung kann die Erkennung von Angriffen deutlich verbessert werden: zum einen durch die unmittelbare Nähe und damit der direkten Relevanz der ausgewerteten Daten für die zu schützenden Systeme, zum anderen aber auch dadurch, dass bereits Angriffsversuche detektiert werden können. Der bisherige Ansatz war in der Regel nur in der Lage, die Auswirkungen von bereits erfolgreichen Angriffen, wie der Infizierung mit einer Malware, zu erkennen.

Die aus dem Dienst DFN-CERT bekannten Automatischen Warnmeldungen bleiben das zentrale Instrument zur Alarmierung von Teilnehmern, wenn in ihrer IT-Infrastruktur Auffälligkeiten mit Bezug zur Cybersicherheit erkannt werden. Sie werden allerdings durch die SecOps zu einem deutlich mächtigeren Werkzeug mit positiven Auswirkungen sowohl auf die Quantität als auch auf die Qualität der Warnungen.



Die Quantität könnte sich zunächst aufgrund der größeren Datenbasis durch die erweiterte Erkennung vor Ort erhöhen, da nicht nur wie bisher von außen erkennbare Sicherheitsvorfälle (wie die Versuche von bereits aktiver Malware, sich weiter zu verbreiten) gemeldet werden können, sondern bereits die Versuche, Systeme zu kompromittieren, erkannt und gemeldet werden. Im Idealfall führt dies allerdings nicht zu einer tatsächlichen Erhöhung der reinen Anzahl der Meldungen, sondern durch die frühere Erkennung von Angriffen werden die bisher bekannten Meldungen zu beispielsweise Bots zurückgehen, da eine Kompromittierung und damit Weiterverbreitungsversuche von Schadsoftware gar nicht oder zumindest signifikant reduziert auftreten.

Die Qualität der Meldungen erhöht sich, da der Erkennung selbst gewonnene und damit für den akademischen und forschenden Sektor besonders relevante Threat Intelligence zugrunde liegt und die ausgewerteten Rohdaten direkt von den geschützten Systemen kommen. Es muss nicht mehr im gleichen Umfang wie bisher aus von außen sichtbaren Effekten auf eine Kompromittierung indirekt zurückgeschlossen werden. Die Erkennung von APTs und anderen zielgerichteten Bedrohungen wird durch SecOps zudem überhaupt erst ermöglicht.

Des Weiteren erhöht sich die Qualität der Warnmeldungen durch die Hinzunahme weiterer „Actionable Informations“, welche konkrete Handlungsempfehlungen beinhalten. Diese unterstützen die Verantwortlichen der teilnehmenden Einrichtungen bei der Reaktion auf gemeldete Bedrohungen mit der umfassenden Expertise des DFN-CERT. Die weiterführende manuelle Vorfallsbearbeitung mit den Experten des DFN-CERT Incident Response-Teams steht im Rahmen des etablierten Dienstes DFN-CERT selbstverständlich weiterhin ergänzend zur Verfügung.

Statistiken

Statistiken, Kennzahlen und aktuelle Entwicklungen sollen übersichtlich dargestellt werden. Die Informationen werden direkt aus den Systemen zur Angriffserkennung und der Analyse gewonnen und automatisch für die Teilnehmer am neuen Dienst aufbereitet. Mögliche statistische Auswertungen und Kennzahlen sind beispielsweise die Anzahl mit Spam oder Malware verseuchter E-Mails, Art und Verteilung der automatischen Warnmeldungen oder die Anzahl und Art erkannter Angriffe in der zeitlichen Entwicklung.

Dies dient primär der Übersicht über aktuelles Infektions- und Angriffsgeschehen für technisch orientiertes Personal in den Einrichtungen. Die Statistiken bilden also ein mittleres Abstraktionsniveau ab, zwischen konkreten Warnmeldungen und abstrakten Lagebildern.

Lagebilder

Mit der Ausweitung der SecOps kann die Gefährdungslage der Informationssicherheit im Deutschen Forschungsnetz und den angeschlossenen Einrichtungen umfassender als bisher bewertet werden. Durch die kontinuierliche Erfassung von Cyber-Angriffen und deren Ursachen werden Erkenntnisse gewonnen, die in regelmäßigen Lageberichten zusammengefasst und bereitgestellt werden. Die Lagebilder beinhalten Informationen, um strategische Entscheidungen im Rahmen einer Risikoanalyse treffen zu können. Aus den Angriffszielen, -methoden und -mitteln lassen sich Trends und Tendenzen erkennen, die für eine erfolgreiche Abwehr genutzt werden können. Neben der Zusammenfassung der Gefährdungslage werden besonders relevante Angriffsmethoden und von den Angreifern benutzte Werkzeuge beschrieben. RZ-Leiter, CIOs und Informationssicherheitsbeauftragte erhalten dadurch eine wichtige Grundlage für ein erfolgreiches Risikomanagement.

Zeitplan

Der Ausbau der SecOps im DFN erfolgt schrittweise, um mit den gegebenen Ressourcen zunächst einen sinnvollen Einstieg in dieses komplexe Thema umzusetzen und den Dienst dann iterativ bedarfsgerecht auszubauen. In einem internen Pilotbetrieb wurden im Sommer 2020 diverse Systeme aus den Diensten DFN-MailSupport und DFN-AAI erfolgreich angeschlossen.

ZEITPLAN

2020

Pilotphase – ab November 2020:

In der Pilotphase werden zunächst in Workshops die Anforderungen der zukünftigen Teilnehmer mit der bereits aufgebauten SecOps-Infrastruktur beim DFN-Verein abschließend abgeglichen. Die Ergebnisse dieser Workshops beeinflussen dann die weitere Roadmap für den Ausbau, wie in Phase I und II dargelegt. Anschließend wird schrittweise die SOC-Sensorik für die Überwachung bei den ersten Pilotteilnehmern ausgerollt. Der SOC-Agent, der diese Sensorik vor Ort bereitstellt, wird in geeigneter Form zur Inbetriebnahme in der Infrastruktur des Teilnehmers zur Verfügung gestellt, zum Beispiel als Virtuelles Disk Image (VDI) oder als Docker / OCI-Container. Primäre Zielsetzung dieser Phase ist die Verbesserung der Qualität der DFN-Dienste und der Aufbau der technologischen Plattform.

2021

Produktionsphase Niveau I – ab Mitte 2021:

Auf Grundlage einer stabilen technologischen Plattform, einer gefestigten Organisationsstruktur und entsprechender personeller Ressourcen wird der Dienst allen interessierten Teilnehmern im DFN zur Verfügung gestellt. Der SOC-Agent wird weiterhin als VDI oder als Docker / OCI-Container ausgeliefert. Die Dienstqualität wird sukzessive durch die Implementierung weiterer Analysesysteme gesteigert.

2022

Produktionsphase Niveau II – ab Mitte 2022:

In dieser Phase soll ein erweiterter SOC-Agent bereitgestellt werden, der derzeit als Appliance angedacht ist. Neben dem reinen Einsammeln und der Vorverarbeitung der Logdaten kann der SOC-Agent durch den langfristigen weiteren Ausbau der Fähigkeiten der SecOps zusätzliche Dienste anbieten, beispielsweise in Form von erweiterter Sensorik und Scannern. Infrage kommen hier Komponenten wie aktive Schwachstellenscanner, Honeypots oder dedizierte Intrusion Detection-Systeme.

Durch den Einsatz von Sensorik und Scannern wird die Dienstqualität deutlich ansteigen. Durch eine flächendeckende Sensorik wird die aktuelle Bedrohungslage besser erfasst und es kann schneller auf relevante Ereignisse reagiert werden. Werkzeuge zum Netzwerk-Discovery und zum Auffinden von Schwachstellen dürften für eine große Anzahl von Einrichtungen sehr hilfreich sein, die derartige Werkzeuge nicht selbst betreiben können. Ebenso sollen erweiterte Analysesysteme zum Einsatz kommen und die Threat Intelligence-Aktivitäten ausgeweitet werden.

Zusammenfassung

Der DFN-Verein baut in Kooperation mit dem DFN-CERT mit den Security Operations im DFN einen neuen Dienst für die Teilnehmer am Deutschen Forschungsnetz auf, der, den sich im Wandel befindlichen und steigenden Herausforderungen von Wissenschaftseinrichtungen im Hinblick auf Fragen der Informationssicherheit Rechnung trägt. Die proaktive Erkennung von Angriffsversuchen möglichst vor der erfolgreichen Kompromittierung sowie die adäquate Reaktion auf derartige Ereignisse spielen hier eine wesentliche Rolle. Um im risikobasierten Ansatz bei der Bewertung von Informationssicherheitsaspekten fundierte Entscheidungen über die Behandlung von Risiken treffen zu können, müssen diejenigen, die diese Entscheidungen treffen und verantworten, über geeignete Informationen verfügen. Auch dieser Anforderung wird der DFN-Verein Rechnung tragen durch die Bereitstellung von einrichtungsspezifischen Statistiken mittlerer Abstraktion sowie von Lageberichten zur übergeordneten Situation auf hohem Abstraktionsniveau.

Der Aufbau der hierfür notwendigen technischen Infrastruktur und der entsprechenden Organisationseinheit DFN-SOC läuft derzeit auf Hochtouren. Teilnehmer sind herzlich eingeladen, am externen Pilotbetrieb teilzunehmen und können unter sicherheit@dfn.de weitere Informationen erhalten. Im Laufe des Jahres 2021 wird dann der Dienst in den Produktionsbetrieb gehen und interessierte Teilnehmer werden ihn beim DFN-Verein ergänzend zu ihrem DFNInternet-Anschluss nutzen können. ◆

eduroam – ein sicherer Dienst

eduroam bietet seinen Nutzenden eine ortsunabhängige und sichere Einwahl in die weltweiten Forschungsnetze und hat sich in den vergangenen Jahren zu einem weltumspannenden Dienst in der akademischen Welt entwickelt. Ob in Nairobi, Sydney, New York oder Berlin, die Welt wird für die Forschungsnetz-Community dank föderierter Infrastrukturen wie eduroam ein ganzes Stück kleiner. Doch wie sicher ist diese Infrastruktur? Wie sicher sind die einzelnen Komponenten? Und ist die Sicherheit in eduroam überhaupt messbar?

Text: **Ralf Paffrath, Jan-Frederik Rieckers** (DFN-Verein)

Foto: alengo / iStock

Sicherheit in eduroam – ein Moving Target

Der DFN-Verein betreibt und verwaltet eduroam bereits seit dem Start des Dienstes im Jahre 2004 mit größter Sorgfalt und orientiert sich dabei nicht nur an den internationalen Entwicklungen. Am Dienst teilnehmende Einrichtungen haben die Möglichkeit über die DFN-AAI und eduGAIN Zugang zu einem im Rahmen von GÉANT entwickelten, international verfügbaren Konfigurationsassistenten zu erhalten. Der Zugang wird von Administrierenden benötigt, um sichere Konfigurationsprofile für ihre eduroam-Nutzenden zu hinterlegen. Der Konfigurationsassistent ist besonders wichtig, da er für gängige Authentisierungsverfahren wie EAP-(T)TLS und PEAP die Komplexität bei der Konfiguration der Clients reduzieren kann.

2018 stellte der DFN-Verein, weltweit als einziges nationales Forschungsnetz, die eduroam-Infrastruktur komplett auf RADIUS over TLS (RFC6614), auch bekannt unter dem Namen RadSec, um und erhöhte so die Sicherheit, Robustheit und Flexibilität des Dienstes. Die Idee war unter anderem, eine Möglichkeit zu schaffen, den RADIUS-Server der Einrichtung nach innen, in den geschützten Netzbereich zu ziehen und den RadSec-Client/Server in die demilitarisierte Zone (DMZ) zu stellen. Mit dem RadSec-Protokoll werden die Autorisierungsanfragen im X-WiN über einen TCP-Port mit dem TLS-Protokoll abgesichert übertragen. Auch bei der Initiative „eduroam off campus“ (eoc) kommt das RadSec-Protokoll zum Einsatz. Organisationen können, ohne selbst den Dienst zu nutzen, ihre Netzanschlüsse eduroam-Nutzenden zur Verfügung stellen.

Sicheres Backend, unsicheres Frontend?

Mit dem Konfigurationsassistenten, der die sichere Konfiguration auf den Endgeräten erleichtert, und der RadSec-Infrastruktur, die die eduroam-Infrastruktur absichert, bietet der DFN-Verein seinen Anwendern eine weltweit einzigartige Sicherheitsinfrastruktur. Aber wie sicher sind die Endgeräte der Nutzenden und die RADIUS-Server in den Einrichtungen? Schließlich und letztendlich entscheiden beide Komponenten, wie sicher die Authentisierung tatsächlich ist.

> Während des Handshakes werden essentielle Parameter der Verschlüsselung ausgehandelt

Zum Einsatz kommt, sowohl bei EAP-(T)TLS als auch bei EAP-PEAP das altbekannte Sicherheitsprotokoll TLS. Hier wird im initialen Handshake zwischen Client und Server eine verschlüsselte Verbindung aufgebaut, über die dann im nächsten Schritt die Zugangsdaten übermittelt werden. Während des Handshakes werden essenzielle Parameter der Verschlüsselung ausgehandelt, die Einfluss auf die Sicherheit der Verbindung haben. Der Handshake findet vor Beginn der eigentlichen Verschlüsselung statt und kann deshalb beobachtet und analysiert werden.

An der Universität Bremen wurde ein Analysewerkzeug für EAP-TLS-Handshakes entwickelt und in Zusammenarbeit mit der DFN-Geschäftsstelle in Berlin im Rahmen eines Testlaufs auf Föderationsebene eingesetzt. Dieses Werkzeug analysiert die vom Client angebotenen TLS-Versionen, Verschlüsselungsmethoden und Erweiterungen sowie die dann vom Server ausgewählten Parameter. Über diese Analyse ist es somit möglich, Probleme auf Client- und auf Serverseite zu erkennen.

Der technische Aufbau

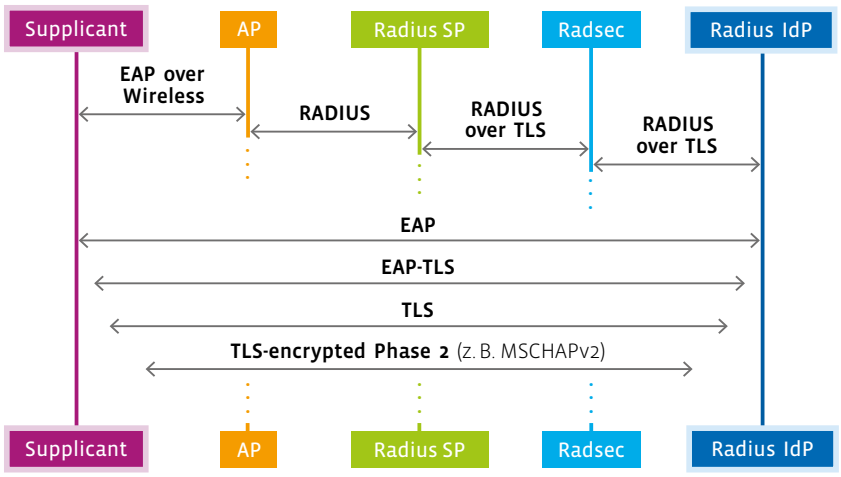
Das Analysewerkzeug unterstützt aktuell zwei verschiedene Datenquellen. Zum einen kann die RADIUS-Kommunikation zwischen den Controllern und dem lokalen RADIUS-Server analysiert werden. Hierfür schneidet das Werkzeug den gesamten UDP-Verkehr auf dem RADIUS-Standard-Port 1812 mit. Die zweite Möglichkeit des Mitschnitts besteht in einer für diesen Zweck entwickelten Schnittstelle in RadSec-Proxy. Hier wird, nachdem RadSec-Proxy die RADIUS-Pakete über das RadSec-Protokoll empfangen und entschlüsselt hat, eine Kopie des Datenverkehrs an das Analysewerkzeug ausgeleitet. Das Werkzeug analysiert die EAP-Kommunikation und sammelt Informationen über den TLS-Handshake. Die Daten werden dann als JSON in Elasticsearch gespeichert. Als Identifizierungsmerkmal dient hier ein Hash aus der äußeren Identität (anonymer Username) und der Calling-Station-ID (MAC-Adresse des Clients). Über dieses Pseudonym werden Authentifizierungen desselben Clients in der Regel nur einmal in der Datenbank abgespeichert.

Über Elasticsearch sind dann Analysen mit den gesammelten Daten möglich, um Sicherheitsprobleme zu erkennen. Für die visuelle Unterstützung der Analyse wird Kibana, eine Visualisierungssoftware für Elasticsearch-Daten, eingesetzt.

Sicherheits-Beobachtungen

Die erste Beobachtung betrifft die eingesetzte Version des Protokolls. Das TLS-Protokoll existiert in verschiedenen Versionen. Jede neue Version hat bekannte Probleme der vorigen Version adressiert und behoben. Die aktuelle Version von TLS, die für EAP-TLS eingesetzt werden kann, ist TLSv1.2. Auch wenn im Web TLSv1.3 gerade ausgerollt wird, kann TLSv1.3 für EAP-TLS noch nicht eingesetzt werden, da hier der Standardisierungsprozess der IETF noch nicht abgeschlossen ist. Ein kleiner Teil der Clients fragt bereits jetzt TLSv1.3 an, ob die Implementierung hier allerdings mit der Spezifikation kompatibel ist, lässt sich noch nicht abschätzen. Die überwiegende Mehrheit der Clients (rund 96,6 Prozent) unterstützt die aktuell für EAP-TLS beste TLS-Version 1.2. Lediglich 3,1 Prozent der Clients fragen die veraltete TLS-Version

ZUSAMMENSPIEL DER PROTOKOLLE BEI EAP-TLS

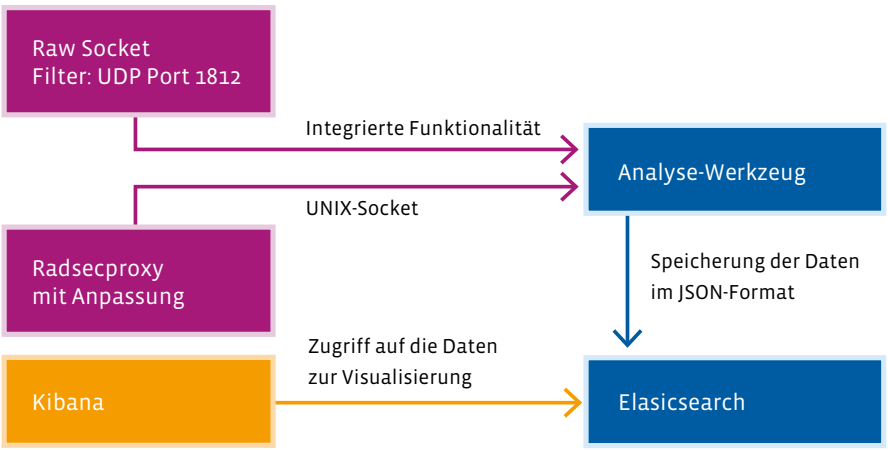


TLSv1.0 an. Die serverseitige Unterstützung für TLSv1.2 ist im Gegensatz dazu nicht so hoch. Hier zeigt die Analyse, dass lediglich 74,4 Prozent (global) beziehungsweise 83,4 Prozent (nur .de) der beobachteten Realms auch TLSv1.2 unterstützen. Ohne TLSv1.2 können bestimmte Sicherheitsmechanismen von TLS, wie zum Beispiel die Nutzung von stärkeren Hash-Funktionen wie SHA-2 statt SHA-1 für die Authentisierung der Parameter für den Schlüsselaustausch, nicht genutzt werden.

Der für die Sicherheit der Verschlüsselung zentrale Teil ist die Aushandlung der konkreten Verschlüsselungsverfahren. Hier bietet der Client eine Anzahl an Verfahren an, aus denen der Server dann eine passende auswählt. In den meisten Fällen wird Diffie-Hellman über elliptische Kurven für den Schlüsselaustausch und AES-256 oder AES-128 für die Verschlüsselung der Daten genutzt. Doch längst nicht alle Clients und Realms nutzen standardmäßig starke Verschlüsselungen. Die Analyse hat gezeigt, dass etwa ein Fünftel aller Clients das inzwischen als gebrochen geltende Verschlüsselungsverfahren RC4 anbietet und es in seltenen Fällen sogar von einzelnen Servern ausgewählt wird. In weiteren wenigen Fällen wird das immer noch ausreichend sichere, aber veraltete Verfahren 3DES ausgehandelt. Ältere Android-Versionen bieten sogar noch Verschlüsselungsverfahren auf dem EXPORT-Level, also mit einer Verschlüsselungsstärke von maximal 56 Bit, an. Zu sehen ist allerdings auch die Aushandlung der neueren Verschlüsselungsmethode CHACHA20, die auf Endgeräten ohne Hardware-Unterstützung für AES effizienter berechnet werden kann.

Ein weiterer Punkt der ausgehandelten Verschlüsselungsmethode ist die (Perfect) Forward Secrecy. Gängiger Standard ist hier ein Austausch des Sitzungsschlüssels über das Diffie-Hellman-Verfahren. Nach Aushandlung des Schlüssels werden die zufälligen privaten Diffie-Hellman-Parameter verworfen, sodass nachträglich keine Rekonstruktion des Sitzungsschlüssels möglich ist. Wird für den Schlüsselaustausch nicht Diffie-Hellman genutzt, dann kann aufgezeichnete Kommunikation bei Bekanntwerden des privaten Schlüssels des Zertifikats nachträglich entschlüsselt werden. Hier sehen wir einen Anteil von rund 15 Prozent aller Realms, die Verschlüsselungen ohne Forward Secrecy aushandeln, davon etwa die Hälfte ausschließlich.

ZUSAMMENSPIEL DER SOFTWARE



Neben ausgehandelter Verschlüsselung und der TLS-Version gibt es noch einige Erweiterungen von TLS, die die Sicherheit erhöhen. Eine dieser Erweiterungen ist EXTENDED_MASTER_SECRET. Ohne die Verwendung dieser Erweiterung ist, unter gewissen Umständen, ein Middleperson-Angriff möglich, bei dem die Verbindung vom Client zur Middleperson und von der Middleperson zum Server dasselbe Master-Secret benutzen. Aus dem Master-Secret werden vor allem die symmetrischen Schlüssel für die Verschlüsselung abgeleitet, aber im EAP-TLS-Kontext auch weitere Parameter wie zum Beispiel die Schlüssel für die folgende WLAN-Verschlüsselung oder Parameter für den MSCHAPv2-

Algorithmus. Clientseitig wird diese 2015 spezifizierte Erweiterung lediglich von zwei Prozent der Clients nicht unterstützt. Serverseitig ist der Support wesentlich geringer. Hier haben wir bei mehr als zwei Dritteln der Realms keine Unterstützung für diese Erweiterung beobachtet.

Viele Daten – was jetzt?

Die gesammelten Daten können nun genutzt werden, um den aktuellen Stand der Sicherheit in eduroam zu beurteilen. Insbesondere die Analyseergebnisse der Clients können einen Indikator bieten, wann veraltete TLS-Versionen oder unsichere Verschlüsselungsverfahren abgeschaltet werden können.

Sehr positiv auffallend ist, dass der überwiegende Teil der beobachteten Clients die aktuelle TLS-Version sowie aktuelle Verschlüsselungsmethoden unterstützt. Die gefundenen Probleme wegen fehlender Unterstützung für aktuelle Verfahren treten nur in geringer Häufigkeit auf und betreffen meist auch nur vereinzelte Geräte. Leider zeigt die Analyse aber auch, dass die Unterstützung für gebrochene oder veraltete Verfahren in den Geräten zum Teil noch lange verbleibt. Hier haben die Hersteller ein augenscheinlich gut funktionierendes System, auch ältere Geräte in Sachen Verschlüsselung auf den aktuellen Stand zu bringen. Ältere Verfahren verbleiben aber, um die Kompatibilität mit möglichst vielen Systemen sicherzustellen.

Dies wirft eine wichtige Frage auf: Weshalb ist die Unterstützung der neueren TLS-Versionen, aktueller Verschlüsselung und Protokollerweiterungen clientseitig viel weiter verbreitet als serverseitig? Den Resultaten der Analyse zufolge liegt der Flaschenhals der Verschlüsselung sehr klar auf Seite der Server.

Ein Grund hierfür könnte veraltete Serversoftware sein. Die vermutlich meistgenutzte Software, FreeRADIUS, setzt auf OpenSSL für die Umsetzung von TLS. Hier wird die aktuell auf dem System vorhandene OpenSSL-Bibliothek verwendet. Debian 8 (Jessie, schon End of Life erreicht) oder Ubuntu 16.04 (Xenial, LTS, EoL 2024) liefern OpenSSL in der älteren Version 1.0.1t bzw. 1.0.2g mit. Der Support für einige Sicherheitsmechanismen wie EXTENDED_MASTER_SECRET oder Verschlüsselungen wie CHACHA20 wurde erst in der OpenSSL-Version 1.1.0 eingeführt. Es ist also zu vermuten, dass an vielen Hochschulen ältere Betriebssystem- und Softwareversionen für RADIUS eingesetzt werden.

Alles kaputt – oder doch nicht?

Wie geht es jetzt also weiter? Ist der eduroam-Dienst unsicher? Die gute Nachricht vorweg: Die gefundenen Sicherheitsprobleme sind keine kritischen Lücken. Auch wenn die Analyse einen großflächigen Einsatz von älterer Software offenbart, entsteht hierdurch nicht zwangsläufig ein großes Risiko. Fast alle lokalen Clients unterstützen aktuelle Verschlüsselungsalgorithmen, besitzen allerdings immer noch eine breite Unterstützung für veraltete Verfahren. Insbesondere zeigt die Analyse, dass die Kompatibilität der Serversoftware mit neuen Verfahren sehr viel langsamer aktualisiert wird, als die der Clients.

> Die gefundenen Sicherheitsprobleme sind keine kritischen Lücken

Bereits jetzt befindet sich der DFN-Verein im Austausch mit weiteren Akteuren der eduroam-Infrastruktur. Die Ergebnisse dieser Forschung werden auch in internationalen Gremien vorgestellt und sollen so zur Verbesserung der Sicherheit dieses weltweiten Verbunds beitragen.

Der DFN-Verein wird Handlungsempfehlungen zur Konfiguration von RADIUS-Servern erarbeiten und in enger Zusammenarbeit mit den teilnehmenden Einrichtungen kontinuierlich daran arbeiten, das Sicherheitsniveau zu erhalten und auszubauen. ◆

Der DFN-Verein betreibt und verwaltet eduroam bereits seit dem Start des Dienstes im Jahre 2004

Routing? – aber sicher!

Die ersten Nutzer von dem, was heute als Internet bezeichnet wird, waren akademische Einrichtungen, die (idealerweise) geprägt sind von einem Geist der Offenheit, der Kooperation und des gegenseitigen Vertrauens. Auch mit der Entwicklung des World Wide Web und trotz der damit einhergehenden Kommerzialisierung des Internets hat sich dieser Geist bewahrt: Das Internet wird noch heute von vielen als gemeinsames Projekt aller Beteiligten angesehen. Der Geist des gegenseitigen Vertrauens hat nun leider auch seine Schattenseiten: Es wird zu wenig kontrolliert. Es werden Fehler gemacht, Router falsch konfiguriert, und Kriminelle missbrauchen das Vertrauen für ihre eigenen Zwecke. Mit der RPKI besitzen Netzbetreiber ein Werkzeug, um hier für mehr Sicherheit zu sorgen.

Text: **Thomas Schmid** (DFN-Verein)

Foto: Orbon Alija / iStock

Blick in die Historie

Durch den gemeinschaftlichen Nutzen haben die Betreiber von Netzen ein Interesse daran, das Internet als Ganzes „am Laufen“ zu halten. Am Laufen wird es unter anderem dadurch gehalten, indem dafür gesorgt wird, dass man sich gegenseitig gut erreicht. So ist es gängige Praxis, dass die Netzbetreiber sich über sogenannte Peerings an privaten Peering-Punkten oder an Internet Exchange Points (IXP) kostenneutral verbinden und gegenseitig die eigenen Netze und die ihrer Kunden annoncieren. Dadurch werden die Wege im Internet kurz und performant gehalten und unnötige Umwege des Verkehrs über teure oder schlechte Verbindungen umgangen. Ist ein Peering technisch nicht möglich, kommerziell nicht sinnvoll oder aus anderen Gründen nicht gewünscht, wird der Verkehr an einen Upstream-Provider

> Immer wieder annoncieren Netzbetreiber von Autonomous Systems versehentlich fremde Netze

geschickt und es wird ein entsprechendes Entgelt dafür gezahlt, seine Daten mit der restlichen Welt auszutauschen.

Doch immer wieder annoncieren Netzbetreiber von Autonomous Systems versehentlich fremde Netze oder gar die globale Routingtabelle als Subnetze, was zu großräumigen Ausfällen des Internets führt.

In den letzten Jahren nehmen aber auch Angriffe zu, deren Ziel es ist, Adressräume zu kapern, um den Verkehr umzuleiten und sich damit Zugang zu Kreditkarteninformationen, Passwörtern oder ähnlichem zu verschaffen oder Bitcoin-Transaktionen zu manipulieren. Nicht zuletzt geschuldet durch den Umstand, dass neue IPv4-Adressen inzwischen nicht mehr über die regulären Vergabestellen, den Internet Registries, verfügbar sind und teuer auf dem freien Markt gekauft werden müssen, werden auch hier bereits vergebene Adressräume gekapert und missbräuchlich weltweit annonciert.

Die Angriffe können prinzipiell auf zwei Arten erfolgen: ein IP-Netz wird als Ganzes gekapert und von anderer Stelle weltweit annonciert oder Teilbereiche eines größeren IP-Netzes werden annonciert und somit umgeleitet. Im ersten Fall wird ein Umrouting in dem Teil des Internets erreicht, der dem Angreifer am nächsten ist. Der letzte Fall führt aufgrund dessen, wie das Routing funktioniert immer dazu, dass der gesamte Verkehr zu diesem Subnetz dann zu dem Angreifer umgeleitet wird (longest prefix match).

RPKI PROBLEMSTELLUNG

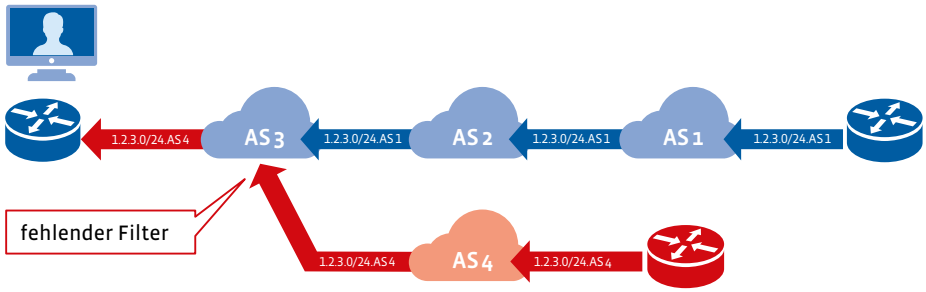


Abbildung 1: Das globale Routing hat ein Sicherheitsproblem

All dies ist möglich, da das Internet in seiner ursprünglichen Form nur über schwache Mechanismen verfügt, solchen Missbrauch zu verhindern. Zunächst sollte sich jeder Provider verpflichten, von seinen Kunden nur Netze anzunehmen, die dem dem Kunden zugewiesenen Adressraum entsprechen und auch nur diese Netze an seine Kunden, Peering-Partner und Upstreams zu annoncieren. Bereits dieser Schritt ist nicht immer gegeben und so kam es zum Beispiel allein im Sommer dieses Jahres zu drei Zwischenfällen bei großen globalen Internet-Service-Providern (sogenannten Tier-1-Providern). In deren Netzen waren Filter zu ihren Kunden nicht implementiert und so wurden große Teile des Internetverkehrs in die falschen Wege geleitet.

Im nächsten Schritt sollte jeder Netzbetreiber, der mit einem anderen ein Peering un-

> Datenbankeinträge stellen nicht immer eine zuverlässige Informationsquelle dar

terhält, von diesem auch nur Netze akzeptieren, die dem benachbarten Netzbetreiber und dessen Kunden zugeordnet sind. Diese Zuordnung erfolgt in der Regel in von Regional Internet Registries (RIRs) gehosteten Datenbanken (Internet Routing Registries, IRR) oder in gegenseitiger Absprache. In den IRRs ist idealerweise in einem sogenannten Route-Objekt die Zuordnung {Quell-AS, Präfix, Präfixlänge} hinterlegt und kann für Routing-Filter referenziert werden.

Leider stellen diese Datenbankeinträge nicht immer eine zuverlässige Informationsquelle dar. Die Vollständigkeit ist nicht gegeben, Einträge können veraltet sein, Legacy-Adressen haben nur einen historischen informellen Charakter und werden ohne Sponsoring LIR nur schwach oder gar nicht von den Registries auf Korrektheit geprüft. Aber auch Einträge können

durch gefälschte Dokumente erschlichen werden oder in krimineller Absicht angelegt werden.

Hinzu kommt, dass eine vollständige Prüfung anhand von Listen schon aufgrund der großen Zahl von Routen (circa eine Million) nicht skaliert und dadurch die Router überfordern würde.

Somit existieren zwar Möglichkeiten, das bestehende Routing zu überprüfen, aber diese reichen bei weitem nicht aus, um Missbrauch zu verhindern.

Dieser Missstand wurde erkannt und so wurde im Rahmen der IETF 2006 eine Working Group gegründet, die sich mit dem Thema Secure Interdomain Routing (sidr) befasst.

Auftritt Ressource Public Key Infrastructure

2012 wurde in der Internet Engineering Task Force (IETF) entschieden, die Absicherung des Routings im Rahmen einer hierarchischen Public Key Infrastructure, einer sogenannten Ressource Public Key Infrastructure (RPKI) umzusetzen. Somit kann der Halter eines IP-Adressraums die Korrektheit der Kombination aus Quell-AS, Präfixes und Präfixlänge dokumentieren und zertifizieren. Dies erfolgt über sogenannte Route Origin Authorisation (ROA)-Objekte (RFC6483), die durch den legitimen Halter des Adressbereiches signiert werden. Somit sind Routen gegenüber einem Validator automatisch invalide, wenn das Quell-AS oder die Präfixlänge nicht mit dem hinterlegten ROA-Objekt übereinstimmen.

> Ein Validator erkennt ungültige Routen

In der Praxis gibt es fünf Wurzel-CAs, welche sich aus den fünf RIRs RIPE, LACNIC, AFRINIC, APNIC und ARIN zusammensetzen. Local Internet Registries (LIRs) wie der DFN-Verein bilden Sub-CAs und können dann mithilfe ihres Schlüsselpaares eigenständig ROA-Objekte anlegen und signieren.

Möglich ist dies jedoch nur, wenn der DFN-Verein gegenüber der Wurzel-CA RIPE den Nachweis führen kann, dass er die Autorisierung der Einrichtungen für das Anlegen von ROAs besitzt. Diese ergibt sich automatisch, wenn der Adressraum von RIPE selbst an den DFN-Verein übergeben wurde. Für Einrichtungen, die über einen eigenen Adressraum verfügen, geht dies nur, wenn die Einrichtung den DFN als sogenannten Sponsoring LIR hierfür autorisiert hat. Ein Großteil der Einrichtungen am DFN verfügt über einen eigenen Adressraum, den sie in der Regel zu einer Zeit von der IANA erhalten haben, in der noch keine RIRs existierten. Für die Autorisierung dieser Netze ist der Abschluss einer entsprechenden Vereinbarung notwendig. Zwar ist dies schon durch viele Einrichtungen erfolgt, jedoch gibt es noch eine große Anzahl von am X-WiN angeschlossenen Universitäten und Forschungseinrichtungen, für die dies noch nicht geschehen ist. Für diese Einrichtungen kann der DFN-Verein keine ROA-Objekte anlegen und zertifizieren und somit das Routing für diese Netze nicht absichern.

Validierung im X-WiN

Aktuell existieren mehrere unabhängige Open-Source-Implementierungen von Software zur Validierung von ROAs. Im X-WiN werden zwei Server mit zwei verschiedenen Implementierungen der Validierungssoftware betrieben. Über diese können die Router die Gültigkeit der von den Peerings und Upstreams gelernten Routen überprüfen. Diese Validatoren beziehen von den

RPKI

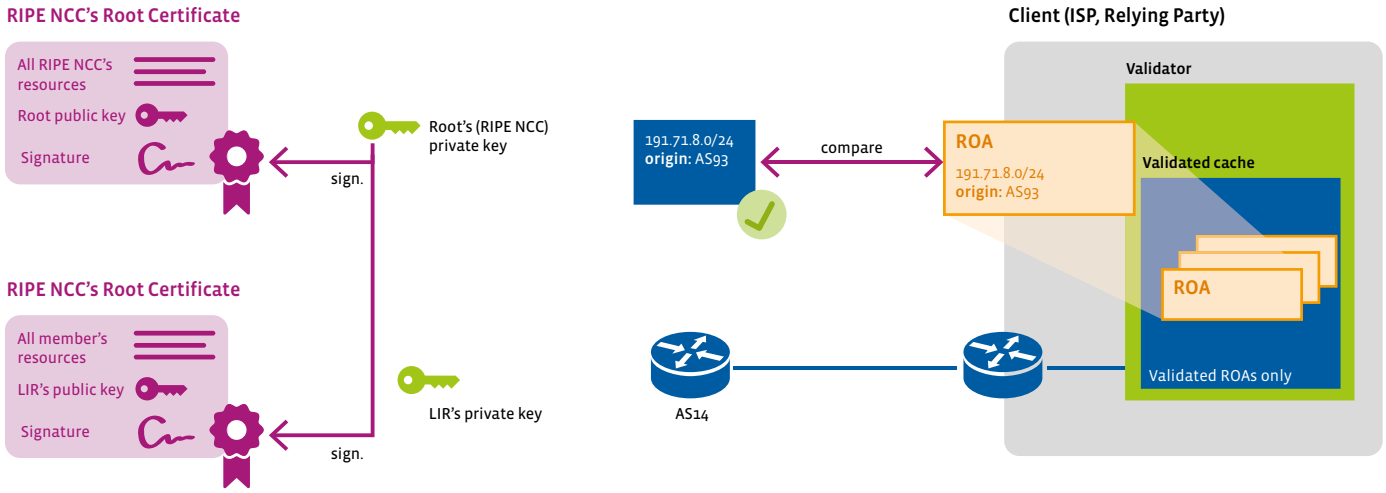


Abbildung 2: Vertrauenswürdiger als eine reine Datenbankabfrage

VALIDATOR UND ROUTER

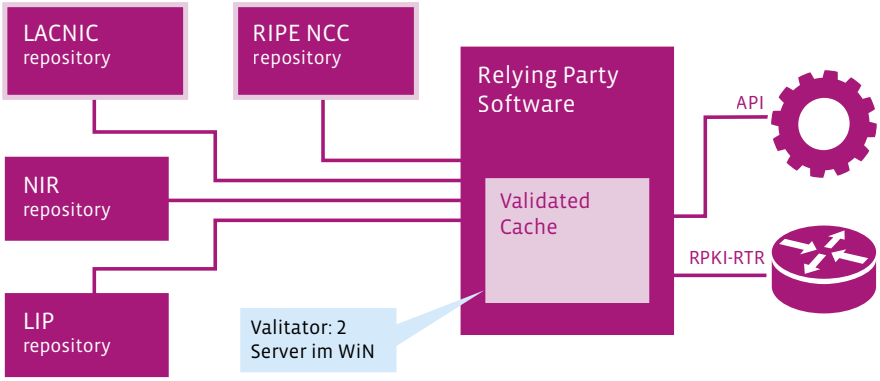


Abbildung 3: ROA-Veröffentlichung, Datenbeschaffung, -validierung und -verarbeitung

Wurzel-CAs und den Trust-Anchors (TAs) die ROA-Objekte und deren Zertifikate und entlasten somit den Router von kryptografischen Aufgaben. Eine Abfrage der Validatoren kann drei mögliche Ergebnisse liefern: valid, invalid und unknown. Netzbetreiber können dann selbst entscheiden, welche Aktionen für die Routen aus diesen Ergebnissen abgeleitet werden. Mögliche Aktionen sind im Wesentlichen „ablehnen", „schlechter gewichten" oder „nichts tun". Sinnvollerweise werden invalide Routen natürlich abgelehnt.

An einem normalen Tag beobachtet das DFN-NOC immerhin mehrere Tausend invalide Routen. In den meisten Fällen handelt es sich um offensichtliche Fehlkonfigurationen in den Quell-AS, die durch andere valide Routen abgedeckt sind. Doch sind auch immer wieder invalide Routen dabei, die nach der Aktivierung der RPKI-Filter auch nicht mehr erreicht werden können und möglicherweise in krimineller Absicht annonciert werden.

Fertig? Nein…

Die Kombination RPKI+ROAs sorgt bereits für eine erhebliche Verbesserung der Sicherheit im globalen Routing, doch es gibt noch Lücken. Sobald ein Angreifer die volle Kombination aus Quell-AS, Präfix und Präfix-Länge fälschen kann, ist er in der Lage, die Validatoren zu überlisten und sein Announcement ‚an den Mann' zu bringen. In der Praxis ist ein solches Fälschen des Quell-AS jedoch sehr viel schwieriger zu erreichen als das Annoncieren eines Netzes unter einer falschen AS-Nummer.

Um diese Lücke zu schließen, ist ein zusätzlicher Mechanismus, die AS-Path-Validation (BGPsec, RFC 8205) notwendig. Die notwendigen Standards existieren bereits, doch ist bisher eine Umsetzung in der Fläche noch nicht erfolgt. Zu hoch sind derzeit noch die kryptografischen Anforderungen an die Router, die doch inerster Linie Pakete weiterleiten sollen. Auch ist die überwiegende Anzahl an invaliden Announcements auf Fehlkonfigurationen zurückzuführen, die immer mit einer ungültigen Quell-AS-Nummer einhergehen. So ist man mit der RPKI bereits gegen die allermeisten beabsichtigten oder unbeabsichtigten Angriffe im Routing gewappnet. ◆

WEITERE INFORMATIONEN:

Mit Einführung der RPKI konnte der DFN-Verein der Initiative „Mutually Agreed Norms for Routing Security" (MANRS) beitreten.
MANRS wurde von einer Gruppe einzelner Network Operators gegründet und will mit Unterstützung der ISOC für mehr Sicherheit im globalen Routing sorgen.

WICHTIGE LINKS ZU ROUTING-VORFÄLLEN

Route leaks:
https://radar.qrator.net/blog#year2020

Bankdaten:
https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/

Crypto hijacks:
https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit
https://www.wired.com/2014/08/isp-bitcoin-theft/
https://techbeacon.com/security/bgp-hijack-steals-aws-ip-range-cryptocurrency-theft-ensues

Phishing: you win again

Having an online existence has never been more rewarding. Almost daily someone wins the million dollar jackpot of a lottery and wants to share it with you, you get links to the best prices at the local/online stock exchange/pharmacy and your IT department or bank kindly remind you to change your expired password by clicking on a complicated link (again), that has been shortened for your convenience. Everyone wants to help you. But do they really?

Text: **Martin Waleczek** (DFN-CERT)

First contact

Phishing is the act of sending out millions of identical promises to unsuspecting online users and working hard to monetise the few actual responses. With this approach to social engineering victims are nudged to handing out sensitive personal information like login passwords or financial data freely by means of official looking web forms or even lured into providing access to sensitive resources of company networks by elaborate psychological manipulation.

The phishing experience usually starts with a more or less suspicious email that contains a link to an external website or an unsolicited attachment. The phishing campaign itself may have started weeks or even months before when the attacker made the decision about

which peer group, industry, company or person should be their next target. Such decisions are conscious ones and one has to keep in mind, that phishing campaigns

> The phishing campaign itself may have started weeks or even months before

don't just happen. Someone decided to harvest someone else's personal data or use their computing ressources for their own personal gain.

The effort put into those campaigns can vary widely. Since there are pre-constructed phishing kits available, everyone with access to some kilobytes of webspace and the ability to send promotional emails can set up their own landing page and collect credentials with relative ease. But reaching specific user groups or aiming at high-profile accounts of targeted associations requires significant reconnaissance in order to customise the campaign accordingly.

The various breaches and data leaks of the recent years provide attackers with billions of valid email addresses (i. e. possible recipients) for their first contact. There are datasets for specific industries sold or even publicly available in the darker corners of the web. So whenever a new pandemic shows up the attacker can just grab their folder of contacts in health care, start a new campaign and hope that at least some users are overwhelmed with the recent developments and thereby neglect their online hygiene long enough for the attacker to get their foot in the door.

The same event can be utilised for a campaign targeting users unacquainted with the new videoconferencing solution or online tool that their employer would like them to use in order to work from home. As could be expected, the COVID-19 pandemic brought several such campaigns with it. Fake notifications for missed online meetings were among those attempts targeting users while establishing their home-offices.

For the first contact attackers will take advantage of any social, cultural or environmental development that presents itself and see how much human curiosity or sense of duty can be exploited. Most of the time the campaigns aren't even highly current, but just slightly adapted to the target audience. If some user falls for the email in their inbox that tells them to reset their password in an online form or log in to the company's new online portal with their current credentials, the campaign's first milestone, the first contact, is reached. The link provided in the email leads to a spoofed webpage that resembles the expected log-in page well enough not to raise any suspicion. The slick design of common web portals like the standard login pages of the Outlook Web App, Dropbox or Paypal certainly helps here.

Some campaigns just stop after the first contact. There is not much harm done and the harvested credentials will find their way to some shady database and may end up being sold as part of a collection that is used as a precursor for more advanced phishing or malspam campaigns that require credible sender addresses. Harvested financial data such as bank account or credit card details may be sold individually and is only rarely used by the attacker themselves.

Customised campaigns

Some threat actors use more sophisticated emails and web pages for their phishing campaigns. In the academic environment there is often a multitude of login pages for different services offered by parts of the institution: imagine libraries, e-learning platforms, content management systems (CMS) and various other services. For a targeted campaign the attacker will check the existing environment and adapt the

Illustration: user8545944 / freepik

campaign content. Looking for students' credentials? Your quota is full. Interested

> In the academic environment there is often a multitude of login pages for different services

in administrative contacts for the CMS? You didn't change your password in years. Looking for research papers? A fellow scientist asks, if you have access to a paper in their field that you can reach by clicking a (specially prepared) link to your own library.

The success of targeted campaigns relies on not raising suspicion (unspecific campaigns just rely on mass mailing and statistics). The member of a university that does not heavily use Microsoft's products is not likely to fall for a fake Outlook Web App landing page, so the campaign is adapted accordingly. Speaking the local language helps as well as providing a local sender address, e. g. of the local IT department.

Email addresses (more specifically the ‚From:' part of the email header) can often be easily spoofed since the Simple Mail Transfer Protocol (SMTP) does not require the checks necessary to identify spoofed addresses by default. If spoofing protections are in place, the attacker can use an address from a familiar institution instead. Today's scientific operations rely on interdisciplinary as well as cross-university projects and communication among scientists across borders is encouraged, so an incoming request from another scientist will rarely raise suspicions at a first glance.

The boldest attackers will try to use the local infrastructure to stay under the radar. If the first contact campaign or a breach yields valid email or user credentials, those can be used to send even more convincing emails, look for additional targets in connected online address books or even use the content of past emails in a new

Figure 1: Can You spot the difference? Luckily, sometimes only little effort is put into imitating login pages for phishing campaigns.

campaign disguised as a follow up on the earlier conversation.

The content of the email aims at convincing the reader to click on a provided link. Consequently, the matter has to be rel-

> The boldest attackers will try to use the local infrastructure to stay under the radar

evant to the recipient, which may require additional reconnaissance regarding the local e-learning platform, CMS or whichever service is most promising. For example, e-Learning platforms tend to send notifications to upcoming events, a CMS might provide weekly or monthly statistics and, as a fallback, every postmaster will warn their users in case their mailbox is reaching capacity.

If the attacker's email seems plausible in general there is one last obstacle for the attacker: the URL for the fake log-in page. Due to the combined effort of security researchers and browser vendors users are getting better at recognising fraudulent URLs, so some hint to the institution or some recognisable keywords (webmail, library, ..) are expected by the attentive user. Again there are different levels of sophistication when constructing those URLs. Registering full domains for this purpose is rarely an option, since this involves the submission of personal details most of the time and is quite expensive for a campaign that only runs for some days. There is a plethora of services that offer the registration of free subdomains for little or no money, so often the domains of companies like weebly.com or 000webhost.com show up in phishing campaigns, prefixed by almost non-random subdomains like ‚portalit00', ‚itservdesksuprt' or ‚mailboxstoragenotify-node645'. All of which were part of recent campaigns targeting universities.

If those subdomains are not convincing enough, more sophisticated campaigns will use the long or short form of the name of target institutions as a subdomain. Those URLs are frequently used in campaigns where a non-standard log-in form is expected by the user, for example because of a target university's special corporate identity. The special log-in page of the target can be rebuilt by skilled web programmers or simply saved to a single file with an appropriate browser extension. There is only little programming knowledge necessary to be able to direct entered credentials to a local text file or database, which can be collected later. Often the user is redirected to the expected log-in page afterwards and sometimes even logged in automatically with the credentials initially provided.

With HTTPS usage passing 90 % last year and the padlock in browsers' address bars becoming synonymous for online security there is an optional icing on the campaign cake: a decent campaign needs a valid certificate for the subdomain used. This has been a problem in the past when the authorities responsible for signing those digital certificates made their fortune, but has become far less of a hassle with the advent of free X.509 certificates for Transport Layer Security (TLS) in recent years. The attacker can just register an arbitrary subdomain at a free hoster and create a fitting certificate with the help of Let's Encrypt's free service in less than a minute. Let's Encrypt issued their billionth certificate in February 2020.

Recently a group known for targeting the academic sector even started using some target's infrastructure for the construction of non-suspicious links. Some universities offer services like URL shorteners for their constituency, so the campaign went ahead and just used those short URLs with a trustworthy domain to hide and redirect to their own just a little less trustworthy subdomains of free hosters, thereby avoiding most email filters looking for suspicious URLs. The campaign even used the names of real people working at different universities as senders, so that a quick online search for the person might just lead to the conclusion that there is an individual who used to work at university X and now works at my institution in IT and just wants to tell me that my mailbox is full. What a nice person. The link looks fine. I click.

Help!

Nowadays even sophisticated phishing campaigns with authentic landing pages and convincing stories can be set up easily by attackers with different motivations and varying technical background. There are phishing kits readily available that can be customised to a specific target if needed and even trained professionals can have trouble identifying sophisticated scams.

This article has been published as part of the European Cyber Security Month 2020.

This is an initiative launched by ENISA, EC DG CONNECT and a variety of partners, to raise cyber security awareness in Europe. During October 2020, GÉANT as European umbrella organization shared weekly practical tips, case studies and articles on a different cyber security topic, four in total: social engineering, phishing, password security and ransomware. Many research networks have participated in the campaign.

With the tagline "Become a Cyber Hero" they aimed to encourage end-users to arm themselves against digital threats and feel empowered to protect themselves and their organisations. They also wanted to prove that with the right knowledge and information everybody can become a cyber hero!

But the international CERT community has its own arsenal when it comes to identifying new threats and countering the attackers' efforts. New phishing campaigns are often identified by automatic analysis of incoming emails and the information is shared rapidly among the CERTS of National Research and Education Networks (NRENs) around the globe so that local action can be triggered almost instantly.

This includes the identification and if necessary the deactivation of compromised accounts in order to stop ongoing campaigns, but it starts beforehand with extensive training of the user base. It is vital to raise awareness to the techniques used in malicious campaigns and help the average user to identify suspicious activity. Users are encouraged to report such events even after the act of submitting personal

> the actors behind established campaigns know their cat-and-mouse game quite well

data, clicking on links or opening attachments. No professional will ever blame You for reporting Your own mishaps, because every bit of information helps to fight the larger threat.

Unfortunately, the actors behind established campaigns know their cat-and-

mouse game quite well and will happily switch to the next compromised user account in line, if the one used for the current batch of phishing emails is shut down. So identifying a campaign before it speeds up is key.

This is why NRENs monitor content storing websites (pastebins) and forums in the darker parts of the web for published user credentials. Every such data point can act as a precursor for a new phishing campaign, so account owners are notified and urged to change their password when their email address shows up in a new collection of usernames and passwords. There is a lot to be gained by the simple act of using a password manager to store unique passwords for each service used. On the one hand, this avoids techniques such as credential stuffing, where a malicious actor takes a collection of credentials and feeds those to a third party internet service. Users who tend to reuse their passwords will just end up having multiple compromised accounts with different services. On the other hand, once a password unique to a certain service shows up in a collection of credentials in the dark web, this is a strong indicator, that the service has been compromised. This information can help other users of the service to protect their data before it is misused by a malicious third party.

Monitoring can help identifying new phishing campaigns at earlier stages. Since tailored subdomains are used for targeted campaigns, analysts can deploy tools like urlscan.io to identify newly registered subdomains of typical keywords and wildcards (think ‚uni*.weebly.com‘) in the scan engine. Similarly, the Certificate Transparency Log (CTL) can be used to identify newly issued certificates for subdomains that suspiciously resemble possible phishing targets. Great effort is put into the identification of those candidate domains and information is shared freely among the community by those who identify future threats in order to enable the affected parties to file their take-down notice with their respective hosters. Most of those hosters respond quickly to requests like this and active campaigns can be stopped timely.

> Since tailored subdomains are used for targeted campaigns, analysts can deploy tools to identify newly registered subdomains

Help us!

Unfortunately, all these efforts won‘t prevent your inbox from receiving phishing mails daily, but this knowledge might support you in identifying online scams. There is a very basic set of rules that should be honoured:

Don‘t click on links in emails.
Don‘t open unsolicited attachments.

That‘s it, you‘re safe now. Most of the phishing scams today involve malicious attachments, since harvesting, revising and reselling personal data requires so much more time and effort than just waiting for someone to open an attachment and setting up an electronic wallet to collect ransom for the soon to be encrypted files. Actually, there is a whole industry now offering ransomware-as-a-service including software development and even tech support for victims who have trouble using cryptocurrencies, because it just works so well. Don‘t open unsolicited attachments.

Links in emails are harder to ignore since we are used to the streamlined processes of online shops or services that start with a single click on an offer or friendly reminder in your mail or webmail client. If the events after the click closely match your expectations of what should happen, your safeguards are lowered and maybe not every visited URL will be checked to the last character. In some browsers the address bar will show the domain only instead of the full address of the visited page, which is considered a security feature, but really hampers the quick identification of sophisticated fraud. Visit log-in pages from bookmarks. Don‘t click on links in emails.

If you still do click on the link and enter your login data and shortly after recognise that a mistake was made, stay calm and try to contain the damage. Go to the website in question directly, log in with the now compromised credentials if still possible and change them immediately.

And please share your experience with your local peers and security contacts. They may be able to help you stay on top of the events and your mishap may be the reason why the new sophisticated phishing campaign stops before it really gains momentum. ◆

Sicherheit aktuell

Security Operations: Erste Dienstkomponenten im Pilotbetrieb

Im Verlauf des Sommers wurden diverse Komponenten der DFN-MailSupport- und der DFN-AAI-Infrastruktur im Pilotbetrieb an die derzeit in Aufbau befindlichen Security Operations (siehe Artikel in dieser Ausgabe) angeschlossen. Hierfür werden die Syslog-Daten ausgewählter Server bzw. virtueller Maschinen laufend gesammelt und vom DFN-SOC am DFN-CERT auf Sicherheitsaspekte hin analysiert. Die aktuelle Phase dient in erster Linie dazu, Erfahrungen zu sammeln und die geplanten Prozesse anhand realer Systeme zu validieren. Die Einbindung weiterer Systeme aus anderen Diensten wie dem DFNconf sowie die Bereitstellung der Security Operations als produktiven neuen Dienst für Teilnehmer am DFN sind derzeit in Vorbereitung und werden im Laufe des kommenden Jahres eingeführt. ◆

Illustration: microone

Trainingsreihe „Operational Network Security“

Das Thema IT-Sicherheit ist in aller Munde, verfügbare Aus- und Weiterbildungen richten sich jedoch häufig an Beschäftigte im Bereich Sicherheit und weniger an Mitarbeiterinnen und Mitarbeiter in der System- und Netzwerkadministration. Im Rahmen des GN4-3-Projektes entwickelte das DFN-CERT eine Trainingsreihe zum Thema „Operational Network Security“, die sich primär an System- bzw. Netzwerkadministratorinnen und -administratoren richtet, aber auch für technisch Interessierte aus anderen Bereichen einen Mehrwert bietet. Aufgrund der aktuellen Pandemiesituation wird der Kurs in Form von Webinaren durchgeführt, die insgesamt vier Module bilden. Diese finden bis Februar 2021 statt. Die Trainings bauen nicht aufeinander auf und können daher auch einzeln besucht werden. Alle Webinare werden aufgezeichnet und mit den Kursmaterialien dauerhaft für Interessierte, die nicht an den Live-Terminen teilnehmen können, zum Download bereitgestellt. Detaillierte Informationen zu den Webinaren sowie den Link zu den Aufzeichnungen finden Sie unter: https://learning.geant.org/operational-network-security-new-for-2020-virtual-learning-with-experts/ ◆

MITARBEIT AN DIESER AUSGABE SICHERHEIT AKTUELL:

Heike Ausserfeld, Dr. Ralf Gröper, Wolfgang Pempe, (DFN-Verein)

KONTAKT

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

Der Prüfling – allein zu Haus

Zur datenschutzrechtlichen Rechtmäßigkeit von Maßnahmen im Zuge von Home-Klausuren

Als Folge der Coronapandemie erleben die öffentlichen Hochschulen zurzeit ein größtenteils digital gestaltetes Semester. Eine ganz besondere Herausforderung ist in diesem Zusammenhang die Gestaltung des Prüfungsablaufs. Je nach Bundesland bestehen Möglichkeiten, Präsenzprüfungen abzuhalten. Vielerorts wird es jedoch gerade in überlaufenen Studiengängen nicht möglich sein, die Klausuren in gewohntem Ablauf schreiben zu lassen. In diesem Zuge kam die Idee von Home-Klausuren auf die Liste alternativer Wahlmöglichkeiten. Dieser Beitrag soll nach einer kurzen Einführung der Frage nachgehen, ob die Anfertigung von Home-Klausuren und die damit einhergehende Überwachung der Prüflinge datenschutzrechtlich möglich ist.

Text: **Steffen Uphues** (Forschungsstelle Recht im DFN)

I. Einführung

Unter dem Begriff der Home-Klausur im Sinne dieses Beitrags ist die Durchführung einer schriftlichen Prüfungssituation zu verstehen. Den Prüflingen steht ein begrenzter Zeitraum zur Verfügung und die Klausur soll ohne Hilfsmittel angefertigt werden. Dabei ist der prüfungsrechtliche Grundsatz der Chancengleichheit zu beachten. Dieser ergibt sich aus Art. 3 Grundgesetz (GG) und besagt, dass die Prüfung den Wissensstand der einzelnen Studenten in einen Vergleich setzen soll. Mögliche Täuschungen über den wahren Wissensstand, etwa durch sogenannte Spickzettel oder Absprachen mit Kommilitonen während der Prüfungszeit, sollen ausgeschlossen werden. Im analogen Bereich erfolgt eine Kontrolle etwa durch: Abgabe von Smartphones bei der Aufsicht; Gänge von Aufsichtspersonen durch die Reihen, um etwaige Spickzettel ausfindig zu machen und Gespräche zwischen Studenten zu unterbinden; Kontrolle von Toilettengängen.

Um den prüfungsrechtlichen Gleichheitsgrundsatz auch im digitalen Bereich zu wahren, sind bestimmte Überwachungsmöglichkeiten der räumlichen Umgebung des Studenten im „Homeoffice“ denkbar. Ein prominentes Beispiel hierfür ist die Bucerius Law School in Hamburg. Dort soll es im Rahmen einer Home-Klausur dazu gekommen sein, dass noch während der Bearbeitungszeit eine Lösungsskizze der Klausur im Internet auftauchte. Die private Hochschule sah hierin einen Täuschungsversuch und ging dazu über, die Prüflinge per Video zu überwachen. Im Folgenden soll bewertet werden, ob ein solches Vorgehen auch für öffentliche Hochschulen eine gangbare Option darstellt. Hierfür sind zunächst die Maßnahmen in den Blick zu nehmen, die zur Überprüfung der Prüflinge angewendet werden können. Vor Beginn der Klausur ist eine Identifikationskontrolle durch die Aufsichtsperson via Videokonferenz durchzuführen. Ebenso sollte ein 360-Grad-Raumscan erfolgen. Hierdurch soll die Möglichkeit minimiert werden, dass Prüflinge auf an die Wand geheftete Notizen oder ähnliches zurückgreifen können. Während der Klausur kann eine Reihe von technischen Werkzeugen auf dem Rechner der Prüflinge genutzt werden. Diese können unterschiedlichen Zwecken dienen: Dem Verhindern eines zweiten Bildschirms; dem Schließen geöffneter Tabs und dem Unterbinden vom Öffnen neuer Tabs; der Deaktivierung der Zwischenablage; der zwingenden Anzeige im Vollbildmodus; der Deaktivierung der Druckfunktion. Daneben erfolgt während der Anfertigung der Klausur eine Video- und Audioüberwachung durch Aufsichtspersonen. Schnell wird klar: Im Rahmen von Home-Klausuren werden in erheblichem Umfang personenbezogene Daten verarbeitet. Durch die Maßnahmen erfolgt ein Eingriff in das Recht auf informationelle Selbstbestimmung der Prüflinge. Dieses Recht gewährt es jeder Person, selbst darüber zu bestimmen, ob und in welchem Umfang sie ihre personenbezogenen Daten zugänglich machen möchte. Gerade durch eine Videoüberwachung verliert der Prüfling einiges an Privatsphäre. Viele Studenten haben nur ein Zimmer in einer Wohngemeinschaft. Dieses stellt ihren persönlichen Rückzugsort dar, von dem sie andere ausschließen können. Gerade

> Noch während der Bearbeitungszeit tauchte eine Lösungsskizze der Klausur im Internet auf

diese Räumlichkeit muss nun im Rahmen einer Videoüberwachung anderen offenbart werden. Insofern stellt sich die Frage, inwiefern ein solcher Eingriff seitens der Hochschulen datenschutzrechtlich zu rechtfertigen ist.

II. Rechtmäßigkeit der Datenverarbeitungen im Rahmen von Home-Klausuren

Eine Verarbeitung personenbezogener Daten bedarf einer im Gesetz verankerten Erlaubnisgrundlage. Dieses Grundprinzip des Verbots mit Erlaubnisvorbehalt ist in Art. 6 Abs. 1 Datenschutz-Grundverordnung (DSGVO) normiert. Hiernach kommt für die Rechtfertigung einer Datenverarbeitung eine Einwilligung nach lit. a oder aber eine gesetzliche Erlaubnisgrundlage nach lit. b–f in Betracht. Für Datenverarbeitungen öffentlicher Hochschulen sind zwei mögliche Erlaubnisgrundlagen zu prüfen: zum einen die Einwilligung nach lit. a und zum anderen die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe nach lit. e.

1. Datenverarbeitung aufgrund einer Einwilligung

Eine Datenverarbeitung ist nach Art. 6 Abs. 1 lit. a DSGVO rechtmäßig, wenn die betroffene Person im Vorfeld über die Zwecke der Datenverarbeitung informiert wurde und eingewilligt hat. Diese Einwilligung muss insbesondere freiwillig erteilt werden, wie Art. 4 Nr. 11 DSGVO unmissverständlich formuliert.

Dem Merkmal der Freiwilligkeit kommt im Verhältnis zwischen öffentlicher Hochschule und Student eine besondere Bedeutung zu. Erwägungsgrund 42 S. 5 DSGVO fordert für ein freiwilliges Handeln, dass die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“. Speziell zum Machtgefälle zwischen öffentlichen Stellen und Bürgern äußert sich Erwägungsgrund 43 S. 1 DSGVO. Hiernach bestehe zwischen Behörde

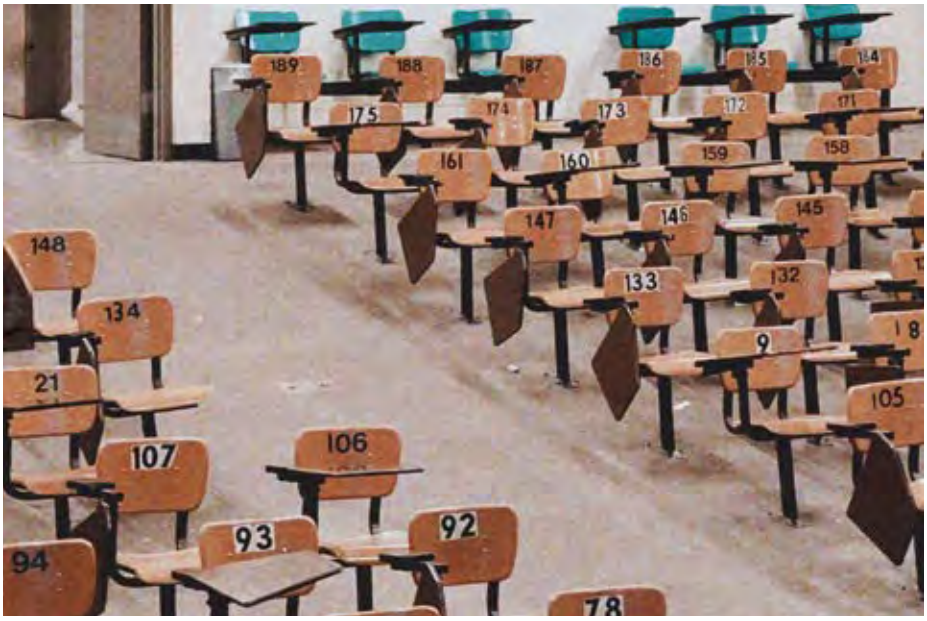


Foto: Elijah Beaton on Unsplash

und Bürger ein derartiges Ungleichgewicht, dass grundsätzlich anzunehmen ist, eine Einwilligung könne nicht freiwillig abgegeben werden. Zwar können Prüflinge im Regelbetrieb ebenfalls nicht über die Bedingungen bestimmen, unter welchen sie ihre Prüfung ablegen. Auch bei Präsenzklausuren stehen sie durchgängig unter Aufsicht. Jedoch kommt es dort eben nicht zu einem Eingriff in die räumliche Privatsphäre.

In den meisten Fällen besteht die Möglichkeit, Home-Klausuren zu verweigern bzw. sich schlichtweg nicht zu diesen anzumelden. Sofern die Studenten die Prüfungsleistung erst zu einem späteren Zeitpunkt ablegen dürften, könnte dies ihren Studienabschluss verzögern. Insofern würde sich aus dem Verweigern der Einwilligung ein mittelbarer Nachteil für die Studenten ergeben. Mit Blick hierauf sind Präsenzklausuren als Alternative zu beachten. Für diejenigen, die keine Home-Klausur schreiben möchten, kann ein solches Präsenzangebot geschaffen werden. Besteht die Möglichkeit, die Prüfung unter Aufsicht und unter Einhaltung aller infektionsbedingten Sicherheitsmaßnahmen abzulegen, so ist dies den Studenten zuzumuten. Das Verweigern der Einwilligung würde die Studenten in diesem Fall aufgrund des Alternativangebots nicht benachteiligen.

Eine Rechtfertigung der Datenverarbeitung aufgrund einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO erscheint nach den vorangegangenen Ausführungen unter Umständen möglich. Jedoch zeigen die angesprochenen Problemfelder, dass erhebliche Bedenken in datenschutzrechtlicher Hinsicht bestehen.

Sofern die Hochschule als Verantwortlicher der Datenverarbeitung auf eine Einwilligung zurückgreifen möchte, ist die Möglichkeit des Widerrufs nach Art. 7 Abs. 3 S. 1 DSGVO zu beachten. Hiernach kann eine betroffene Person die von ihr erteilte Einwilligung jederzeit widerrufen. Eine bis dahin erfolgte Datenverarbeitung bleibt in ihrer Rechtmäßigkeit zwar unberührt. Jedoch ist die Datenverarbeitung im Fortlauf nicht mehr durch die Einwilligung gerechtfertigt. Daneben besteht nach Art. 17 Abs. 1 lit. b DSGVO für die betroffene Person das Recht, den Verantwortlichen zur Löschung der personenbezogenen Daten zu veranlassen, sofern diesem keine anderweitige Erlaubnisgrundlage zur Verfügung steht. Dies steht im Widerspruch zu der Dokumentationspflicht der Hochschulen, die im Rahmen von Prüfungsleistungen besteht. Der Grundsatz des effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG erfordert, dass einem Prüfling die

behördliche und gerichtliche Überprüfung der Bewertung einer von ihm erbrachten Prüfungsleistung zusteht. Insofern sind die Hochschulen bis zu einem gewissen Grad und einer gewissen Zeit verpflichtet, die Dokumentation des Prüfungsablaufs aufzubewahren. Ein Widerspruch zum Recht auf Löschung nach Art. 17 Abs. 1 lit. b DSGVO entsteht hierdurch jedoch nicht. Denn in Art. 17 Abs. 3 lit. b DSGVO ist normiert, dass die Löschpflicht aus Abs. 1 für den Verantwortlichen nicht besteht, soweit die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung erfolgt. Die in den Prüfungsordnungen festgelegten Dokumentationspflichten dürften als eine solche rechtliche Verpflichtung einzuordnen sein.

2. Datenverarbeitung aufgrund gesetzlicher Erlaubnisgrundlagen

Als weitere Erlaubnisgrundlage für die Datenverarbeitung kommt Art. 6 Abs. 1 lit. e DSGVO in Betracht. Hiernach ist eine Datenverarbeitung gerechtfertigt, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Es handelt sich bei lit. e um eine sogenannte Scharniernorm. Die Norm selbst bietet also nicht unmittelbar die Rechtsgrundlage für eine Datenverarbeitung. Es muss vielmehr eine gesondert normierte Rechtsgrundlage bestehen, die die Aufgabenwahrnehmung näher ausgestaltet. Diese Rechtsgrundlage kann nach Art. 6 Abs. 3 DSGVO durch Unionsrecht, aber auch durch das Recht der einzelnen Mitgliedstaaten geschaffen werden.

Hieraus ergibt sich, dass die nationalen Gesetzgeber in Deutschland eigenständig Regelungen für öffentliche Stellen wie etwa Hochschulen erlassen können. In diesem Zusammenhang sind insbesondere die landesrechtlichen Datenschutz- und Hochschulgesetze maßgeblich. Insofern ist es wichtig, dass sich jede Hochschule an den für sie geltenden landesrechtlichen Regelungen orientiert. Als Ausprägung des föderalistischen Systems können sich deutschlandweit erhebliche Unterschiede in der rechtlichen Bewertung ergeben. Dieser Beitrag kann somit keine pauschale Antwort liefern, ob öffentlichen Hochschulen eine taugliche Rechtsgrundlage im Sinne von Art. 6 Abs. 1 lit. e DSGVO zur Verfügung steht. Zwei Beispiele können jedoch dabei helfen, die Auswirkungen der unterschiedlichen Regelungen zu verdeutlichen:

In § 17 Abs. 1 S. 1 des Niedersächsischen Hochschulgesetzes (NHG) ist normiert, dass Hochschulen personenbezogene Daten von Studenten unter anderem dann verarbeiten dürfen, wenn diese Datenverarbeitung für die Teilnahme an Prüfungen erforderlich ist und entsprechende Hochschulordnungen hierzu existieren. Die Datenverarbeitung im Rahmen von Home-Klausuren könnte hiernach über die Scharniernorm des Art. 6 Abs. 1 lit. e DSGVO gerechtfertigt sein. Allerdings könnte hier auch argumentiert werden, dass im Normtext die Verwendung einer Videoaufsicht zumindest anklingen muss. In diesem Zusammenhang ist auch die Ansicht der jeweiligen Landesdatenschutzbehörde zu beachten. In Nordrhein-Westfalen besteht keine vergleichbare Regelung. § 8 Abs. 5 des Hochschulgesetzes NRW (HG NRW) äußert sich lediglich allgemein dahingehend, dass die Verarbeitung personenbezogener Daten unter Beachtung der allgemeinen datenschutzrechtlichen Vorschriften stattfindet. § 82a HG NRW hat dem Wissenschaftsministerium die Möglichkeit gegeben, eine Corona-Epidemie-Hochschulverordnung zu erlassen. Der darin befindliche § 6 gibt die Verantwortung zur Schaffung einer datenschutzrechtlichen Erlaubnisgrundlage an die einzelnen Hochschulen weiter, indem diese die Befugnis erhalten, durch ihre Rektorate den Prüfungsbetrieb regeln zu lassen. Insofern muss auch ein Blick darauf geworfen werden, wie sich die jeweilige Hochschule positioniert.

III. Fazit für öffentliche Hochschulen

Auch in der momentanen Ausnahmesituation haben die Hochschulen das Datenschutzrecht zu beachten und die dort normierten Grundsätze und Regelungen zu wahren. Im Umgang mit der Privatsphäre der Studenten ist eine gesteigerte Sensibilität erforderlich. Dies gilt mit Blick auf eine Einwilligung gerade hinsichtlich der Freiwilligkeit – etwaige Nachteile im Falle einer Verweigerung sollten minimiert werden. Die Möglichkeit des Widerrufs stellt für die Datenverarbeitung dagegen keine Risiken dar. Zwar resultiert hieraus grundsätzlich ein Recht auf Löschung der personenbezogenen Daten. Die Hochschulen dürfen die Daten jedoch solange aufbewahren wie es zur Ermöglichung von Überprüfungsansprüchen seitens der Prüflinge erforderlich ist.

Bei der Frage, ob eine gesetzliche Erlaubnisgrundlage über Art. 6 Abs. 1 lit. e DSGVO heranzuziehen ist, muss stets das jeweilige Landesrecht beachtet werden. Wenn eine Datenverarbeitung im Rahmen von Prüfungen nicht in die Regelungen mitaufgenommen wurde, liegt im Zweifel keine hinreichend konkrete Anknüpfungsnorm vor.

Anders als für öffentliche Hochschulen bieten sich für private Hochschulen noch weitere mögliche Erlaubnisgrundlagen. So kommen im Verhältnis einer privaten Hochschule zu ihren Studierenden auch eine Datenverarbeitung aufgrund vertraglicher Verpflichtungen nach Art. 6 Abs. 1 lit. b DSGVO sowie berechtigte Interessen der Hochschulen nach Art. 6 Abs. 1 lit. f DSGVO in Betracht. ◆

ANMERKUNG:

In einer früheren Version dieses Artikels wurde nicht näher auf die Möglichkeit kurzfristiger Gesetzesänderungen zur Schaffung einer Rechtsgrundlage im Sinne von Art. 6 Abs. 1 lit. e DSGVO eingegangen. Dies wurde nachträglich zur Verdeutlichung geändert.

Am Anfang war alle Software frei

Rechtliche Fallstricke im Umgang mit freier und Open-Source-Software

Die Pandemie und die damit einhergehenden Restriktionen stellen hohe Anforderungen an die Digitalisierung an Hochschulen und Forschungseinrichtungen. Der richtige Einsatz von Software ist damit von zentraler Bedeutung, um die anstehenden Herausforderungen zu bewältigen. Ein besonderes Augenmerk liegt dabei auf Videokonferenzdiensten, mithilfe derer eine digitale Lehre ermöglicht wird. Da hierbei zunehmend auch auf freie und Open-Source-Software zurückgegriffen wird, soll dies den Anlass für eine Erläuterung und rechtliche Einordnung geben.

Text: **Nico Gielen** (Forschungsstelle Recht im DFN)

Foto: clu/iStock

I. Historischer Hintergrund

Bis 1970 haben Computerhersteller ihre Software noch kostenlos, mitsamt Quellcode und stets zusammen mit der Hardware ausgeliefert. Dieser freie Umgang mit Software begünstigte die Entstehung einer Hackerkultur an akademischen Universitäten, im Rahmen derer Programmierer die Software veränderten und untereinander austauschten. Dann aber wurde das Konzept einer Softwarelizenz eingeführt, um fortan die Softwarenutzung rechtlich zu beschränken, ein neues Marktsegment zu etablieren und dieses im gleichen Zuge gewinnbringend zu erschließen. Software wurde nicht mehr zwingend mit der Hardware zusammen und erst recht nicht mit dem Quelltext ausgeliefert. Vielmehr wurde sie nur in maschinenlesbarer Form vertrieben und zudem als Geschäftsgeheimnis klassifiziert. Veränderungen der Software waren fortan rechtlich und praktisch unmöglich. Die ursprünglich freie Software wurde somit proprietär.

Daraufhin zerfiel auch die akademische Hackerszene. Dessen prominentes Mitglied Richard Stallman kündigte daraufhin seinen Arbeitsvertrag am MIT und widmete sich nunmehr einer Gegenbewegung. Er gründete 1985 die Free Software Foundation, deren Hauptaufgabe die Unterstützung des GNU-Projektes war. GNU ist dabei eine Abkürzung für „GNU's not Unix" und spielt damit auf das Betriebssystem Unix an, das ursprünglich Arbeitsmittel der Hackergemeinde war, dann aber proprietär wurde und ihr damit die Arbeitsgrundlage entzog – mithin ein perfektes Feindbild. Im Rahmen dieses GNU-Projektes wurden fortan diverse Maßnahmen ergriffen, die allesamt darauf gerichtet waren, freie Software zu fördern.

Aus dieser an der Ostküste der USA gegründeten Bewegung spaltete sich jedoch bald darauf an der Westküste eine Gruppe ab. Die im Silicon Valley tätigen Softwareentwickler planten 1998 eine regelrechte Marketingkampagne. Denn sie fürchteten, der

> Sie fürchteten, der Aktivismus des Free Software Movements würde Wirtschaftsvertreter abschrecken

Aktivismus des Free Software Movements würde Wirtschaftsvertreter abschrecken und damit das an sich begrüßenswerte Ansinnen der Bewegung gefährden. Daher tadelten sie den Begriff „Free Software" als verwirrend und sprachen sich für einen terminologischen Richtungswechsel aus. Daraufhin wurde der Begriff „Open Source" vorgeschlagen, der sich prompt durchsetzte und ein eigenes Open Source Movement lostrat.

Obgleich sich die inhaltlichen Anforderungen an freie und Open-Source-Software im Einzelnen unterscheiden mögen, sind sie zu

> Das Free Software Movement verband mit freier Software auch eine soziale und freiheitliche Dimension

weiten Teilen deckungsgleich. Der Hauptunterschied zwischen den beiden Bewegungen ist vielmehr ideologischer Natur. Das Free Software Movement verband mit freier Software auch eine soziale und freiheitliche Dimension und war damit eng an die politischen Vorstellungen von Stallman geknüpft. Hingegen liegt Open Source eine andere Philosophie zugrunde. Eric S. Raymond, der das Aushängeschild des Open Source Movements werden sollte, verglich Open Source mit einem Basar, auf dem die Öffentlichkeit jede Entwicklung einsehen und an ihr mitwirken kann. Neben diesem kollaborativen Element ist Open Source aber auch weniger politisch aufgeladen, sondern verfolgt vielmehr einen pragmatischen Ansatz.

II. Definitionsansätze

Wie bereits anklang, bestand Verwirrung hinsichtlich des Begriffs der freien Software. Oftmals wurde sie mit kostenloser Software gleichgesetzt, woraufhin Aktivisten sich genötigt sahen den Slogan „Free as in Freedom, Not Free as in Free Beer!" zu skandieren. Die offizielle Definition von freier Software wurde von Stallman entwickelt und als „The Four Essential Freedoms of Free Software" getauft. Eine Software ist in diesem Sinne frei, wenn sie keinerlei Nutzungsbeschränkungen unterliegt, wenn sie studiert und verändert werden kann, wozu der Quellcode einsehbar sein muss, und wenn Kopien des Originals sowie von veränderten Versionen verbreitet werden dürfen.

Wann eine Software hingegen Open Source ist, bestimmt sich nach der durch die Open-Source-Initiative erlassenen Definition.[1] Zunächst wird klargestellt, dass der Begriff nicht gleichbedeutend ist mit einem Zugriff auf den Quellcode. Vielmehr sind zehn Kriterien zu beachten. Dazu gehört, dass die Software unentgeltlich vervielfältigt, bearbeitet und verbreitet werden darf, dass der Quelltext einsehbar ist und dass eine Verbreitung modifizierter Versionen nur unter denselben Lizenzbedingungen erfolgen darf wie unter denen des Originals. Des Weiteren darf die Software niemanden diskriminieren und die Nutzung der Software darf nicht an einen bestimmten Verwendungszweck oder ein bestimmtes Produkt gebunden werden. Schließlich darf die

1 Siehe unter www.opensource.org/osd.

Nutzung anderer Software nicht beeinträchtigt werden und die Nutzung der Software muss technologieneutral gestaltet sein.

Aufgrund der großen Überschneidung der beiden Definitionsansätze und zur Umgehung dieses Namensstreits wurde mit Free and Open Source Software (FOSS) ein Sammelbegriff geschaffen. Dieser kann zum einen zur proprietären Software abgegrenzt werden. Allerdings wird an den dargestellten Bedingungen auch klar, dass FOSS nicht uneingeschränkt genutzt werden kann. Deswegen ist sie zum anderen zur Public Domain-Software abzugrenzen. Ein häufiges Missverständnis bei FOSS besteht auch darin, dass angenommen wird, sie dürfe keinesfalls entgeltlich vertrieben werden. Zentral ist jedoch nur, dass für die Nutzung der Software keine Gebühr anfallen darf. Dies bedeutet nicht, dass für den Verkauf einer bestimmten Programmkopie im Einzelfall nicht doch ein Preis verlangt werden darf. Des Weiteren ist auch eine kommerzielle Nutzung von FOSS nicht prinzipiell ausgeschlossen.

III. Rechtliche Einordnung

Software beschäftigt nicht nur Programmierer, sondern auch Urheberrechtler. Allerdings gehen diese FOSS aus der entgegenstehenden Perspektive an. § 69c Urheberrechtsgesetz (UrhG) macht deutlich, dass der Urheber einer Software bestimmte Rechte innehat, wodurch die Nutzung der Software anderen Personen zu einem großen Teil verboten wird. Insbesondere dürfen sie Software ohne eine Erlaubnis des Urhebers nicht vervielfältigen, bearbeiten oder verbreiten. Damit widerspricht das Urheberrecht in einem zentralen Punkt der FOSS, die voraussetzt, dass solche Verbote gerade nicht bestehen.

> Software beschäftigt nicht nur Programmierer, sondern auch Urheberrechtler

1. Lizenzvereinbarung

Das Mittel zur Lösung dieses Konflikts ist die Lizenz. Das UrhG nennt sie in § 31 UrhG zwar Nutzungsrecht, ein inhaltlicher Unterschied geht damit aber nicht einher. Die Lizenz ist eine Vereinbarung zwischen dem Urheber der Software und einem Softwarenutzer. Diese wird oftmals dem Quelltext des Programms vorangestellt. Der Nutzer, der sodann eine Vervielfältigung oder eine Verbreitung vornimmt, zeigt sich dadurch mit der Lizenz einverstanden. Das Zustandekommen der Lizenzvereinbarung bedarf also keines direkten Kontakts zwischen Nutzer und Urheber. Mithilfe dieser Vereinbarung kann der Urheber allerdings nicht auf sein gesamtes Urheberrecht verzichten. Der Grund dafür liegt in der kontinentaleuropäischen Auffassung, dass Urheberrecht nicht nur ein wirtschaftliches Verwertungsrecht ist, sondern damit untrennbar auch eine persönlichkeitsrechtliche und damit im Kern unverzichtbare Verbindung zwischen Urheber und dem Werk einhergeht. Abseits dieses Kernbereichs darf ein Urheber aber über seine eigenen Verbotsrechte verfügen. Er kann damit insbesondere anderen Personen erlauben, seine Software zu vervielfältigen, zu bearbeiten und zu verbreiten.

Der Gesetzgeber hat mit § 32 Abs. 3 S. 3 UrhG auch eine Ausnahme von dem Grundsatz geschaffen, dass der Urheber angemessen zu vergüten ist, wenn er die Nutzung seines Werkes erlaubt. Ohne diese sog. Linux-Klausel wäre es mit dem deutschen Urheberrecht nicht vereinbar, dass FOSS unentgeltlich vertrieben wird.

2. Mustertexte

Der Urheber der Software kann mit dem jeweiligen Nutzer eine individuelle Vereinbarung aushandeln. Er kann aber auch – und dies ist der Regelfall – auf eine vorformulierte Vereinbarung zurückgreifen. Dabei kann zwischen allgemeinen und auf bestimmte Bereiche zugeschnittene Lizenzen differenziert werden. Beispielweise sind die GNU Lesser General Public License auf die Programmierung von Programmbibliotheken und die GNU Free Documentation License auf die Weitergabe von Softwaredokumentationen zugeschnitten. Breiter Verwendung erfreuen sich auch Creative Commons-Lizenzen, die für die Lizenzierung von Bildern, Texten und Musik verwendet werden.

Die am häufigsten verwendete Lizenz ist die GNU General Public License (GPL).[2] Sie wurde 1989 von Richard Stallman verfasst und stellt die wohl bekannteste Errungenschaft des oben erwähnten GNU-Projektes dar. Mittlerweile wurde die GPL noch zweimal aktualisiert. Auch in der dritten Version finden sich zwar unwirksame Bestimmungen, da die Lizenz nicht auf das deutsche Recht zugeschnitten ist. Ein Beispiel hierfür ist der zu weitgehende Haftungsausschluss. Im Grundsatz jedoch handelt es sich bei der GPL um eine auch nach deutschem Urheberrecht wirksame Lizenz.

Im Besonderen zeichnet sie aus, dass sie auf dem Prinzip des Copyleft gründet – ein Wortspiel als Gegenüberstellung zum Copyright. Dieses erfordert, dass jegliche Modifikationen der Ursprungssoftware auch der Ursprungslizenz unterworfen werden müssen. Damit unterscheidet sie sich in einem zentralen Punkt von anderen Lizenzen wie etwa der Lizenz der Berkeley Software Distribution (BSD). Die einer BSD-Lizenz unterworfene Software, die also nicht dem Copyleft unterliegt, kann damit auch als Vorlage für proprietäre Software dienen.

2 Weitere Beispiele bei Mörike, Der Preis der Freiheit – Zu den Rechten und Pflichten bei der Nutzung „Freier Software“, DFN-Infobrief Recht 04/2017, S. 2 f.

IV. Folge eines Verstoßes

Wenn die in der jeweiligen Lizenz aufgelisteten Bedingungen nicht erfüllt werden, kann das Nutzungsrecht erlöschen. Dadurch ist die Softwarenutzung wieder verboten und der Nutzer urheberrechtlichen Ansprüchen ausgesetzt. Hierzu zählen die Ansprüche auf Ersatz etwaiger Abmahnungskosten (§ 97a Abs. 3 S. 1 UrhG), Unterlassung (§ 97 Abs. 1 S. 1 UrhG) und Schadensersatz (§ 97 Abs. 2 S. 1 UrhG).

Dazu ein Beispiel aus dem Jahr 2016: In diesem Fall hatte eine Hochschule eine unter der GPL angebotene Software bezogen und wiederum auf ihrer Webseite zum Download angeboten. Da sie aber weder den Lizenztext noch den Quellcode zur Verfügung stellte, verstieß sie gegen die GPL und das Nutzungsrecht entfiel. Die Entgegnung der Hochschule, sie habe die Software ihrerseits von einer Seite geladen, die diese Bedingungen nicht erfüllte, ließ das Gericht nicht durchgreifen. Vielmehr treffe die Hochschule eine Prüfpflicht, der sie in diesem Fall nicht nachgekommen sei. Schließlich verurteilte das Landgericht (LG) Bochum die Hochschule wegen Urheberrechtsverletzung einerseits zum Ersatz der Abmahnungskosten und zur Unterlassung, wobei hervorgehoben werden kann, dass bereits der einmalige Verstoß eine für den Unterlassungsanspruch erforderliche Wiederholungsgefahr indizieren soll. Überraschenderweise verurteilte das LG Bochum die Hochschule auch zur Zahlung eines Schadensersatzes (Urteil vom 3.3.2016, Az. I-8 O 294/15).[3]

> Schließlich verurteilte das Landgericht (LG) Bochum die Hochschule wegen Urheberrechtsverletzung

Nicht zuletzt wegen dieser Überraschung wurde Berufung eingelegt, wodurch das Urteil des LG Bochum vom Oberlandesgericht (OLG) Hamm überprüft wurde (Urteil vom 13.6.2017, Az. 4 U 72/16). Dieses schloss sich dem LG Bochum grundsätzlich an, widersprach jedoch in Bezug auf den Schadensersatz. Es verwies darauf, dass für unter einer GPL vertriebenen Software eben kein Entgelt verlangt werden darf. Daher habe die Nutzung der Software durch die Hochschule keinen objektiven Wert. Mit anderen Worten bestehe kein Schaden, der von der Hochschule ersetzt werden könnte. Da gegen das Urteil des OLG Hamm keine Revision eingelegt wurde, ist ungewiss, ob diese Rechtsansicht auch vor dem Bundesgerichtshof Bestand haben wird.

V. Empfehlungen und Fazit

Bereits an den genannten Gerichtsentscheidungen wird deutlich, dass sich auch Hochschulen tunlichst an die Lizenzbedingungen halten sollten, da sie sich ansonsten urheberrechtlichen Ansprüchen aussetzen können. Um die Lizenzbedingungen einzuhalten, ist ein aufmerksames Studium des Lizenztextes unabdingbare Voraussetzung. Im Regelfall wird dieser einen Hinweis auf die Ursprungsquelle der Software erfordern. Darüber hinaus können jedoch auch noch andere Voraussetzungen bestehen, wie die Offenlegung des Lizenztextes und des Quellcodes.

Eine weitere Problematik besteht darin, dass dem vermeintlichen Lizenzgeber unter Umständen die Berechtigung zur Weitergabe der Software fehlt. Daher sind Lizenznehmer dazu angehalten, diese Berechtigung zu überprüfen. Für den Umfang dieser Prüfpflicht gibt es keine starren Vorgaben und sie ist auch stets vom Einzelfall abhängig. Gleichwohl dürfte nur selten das blinde Vertrauen auf die Zusicherung des Softwarelieferanten ausreichen, er sei zur Weitergabe der Software befugt. Zwar dürfte die Annahme naheliegen, dass die Anforderungen an die Prüfpflicht sinken, wenn die Software seit längerer Zeit verfügbar ist und durch anerkannte Distributoren bereits weit verbreitet wurde. Bestehen aber weiterhin Zweifel, sollte gleichwohl sachkundiger Rat eingeholt werden.

Sollte es trotz aller Vorsichtsmaßnahmen zu einer Abmahnung kommen, sollte in einem ersten Schritt überprüft werden, ob der Anspruchsteller wirklich Rechteinhaber ist oder dies nur vorgibt zu sein. Wenn die Berechtigung des Anspruchstellers feststeht, sollte die Urheberrechtsverletzung unverzüglich unterbunden werden. Zudem kann die Abgabe einer strafbewehrten Unterlassungserklärung sinnvoll sein, da durch eine solche die für einen Unterlassungsanspruch erforderliche Wiederholungsgefahr entfällt und damit einem teuren Gerichtsverfahren vorgebeugt werden kann.[4]

Diese Überlegungen sollen gleichwohl nicht zu der Annahme verleiten, dass Hochschulen und Forschungseinrichtungen Abstand von FOSS nehmen sollten. Da bei proprietärer Software nicht minder große Herausforderungen bestehen, sollten sie im Gegenteil FOSS mehr in den Fokus nehmen. Dadurch können sie Kosten einsparen und zugleich eine transparente Softwareentwicklung fördern. ◆

3 Ausführlicher Klein, Die Grenzen der Freiheit – Landgericht Bochum verurteilt Hochschule zur Zahlung von Schadensersatz wegen Verstoßes gegen die Bedingungen der General Public License, DFN-Infobrief Recht 07/2016, S. 2 ff.

4 Hierzu auch Ochsenfeld, Freie Gefahrenquelle – Landgericht Halle zur Reichweiter der Wiederholungsgefahr bei der Verletzung der sogenannten General Public License (GPL), DFN-Infobrief Recht, Jahresband 2015, S. 150 ff.

Gemeinsames Votum: die neue Entgeltordnung ab 2022

Die Mitglieder haben entschieden: Mit der Entgeltanpassung zum 1. Januar 2020 und der neuen Entgeltordnung ab dem 1. Januar 2022 hat sich der DFN-Verein weiterhin wirtschaftlich stabil und zukunftsfähig aufgestellt. Vorangegangen war ein drei Jahre dauernder, ausführlicher und produktiver Willensbildungsprozess. Aus den intensiven Diskursen in allen Vereinsorganen und Ausschüssen mit diversen Feedback-Zyklen in der gesamten Mitgliedschaft resultierten insgesamt neun Prinzipien, die das Fundament der neuen Entgeltordnung bilden. So ist es gelungen, sie unter anderem fair, solidarisch und bedarfsgerecht zu gestalten.

Prinzipien der neuen DFN-Entgeltordnung

1. Kostendeckend: Sie muss zur mittelfristigen Deckung der Kosten für Betrieb und Weiterentwicklung von Netz und Diensten führen.

2. Nachvollziehbar: Sie soll auf interpretationsfreien Sachverhalten aufbauen und möglichst einfach zu verstehen sein.

3. Einfach: Sie soll sowohl für die teilnehmenden Einrichtungen als auch für den DFN-Verein einfach und mit möglichst geringem Aufwand anwendbar sein.

4. Bedarfsgerecht: Sie soll allen Einrichtungen eine bedarfsgerechte Teilnahme am Netz und den Diensten ermöglichen.

5. Fair: Alle teilnehmenden Einrichtungen sollen von den Vorteilen des gemeinsamen Handelns im DFN-Verein profitieren (Win-Win) und die Verteilung der Vorteile dabei als angemessen wahrnehmen. Darum soll die Höhe der Kostenbeteiligung einer Einrichtung in einem angemessenen Verhältnis zu ihrer Nutzung von Netz und Diensten stehen.

6. Solidarisch: Sie soll allen Einrichtungen möglichst einheitliche Bedingungen zur Teilnahme am Netz und den Diensten bieten. So sollen die Einrichtungen z. B. nicht wegen ihrer Verfasstheit (z. B. ob Hochschule, Forschungseinrichtung, Behörde oder gewerbliche Wirtschaft) oder wegen ihres Standortes bevorzugt oder benachteiligt werden.

7. Vertretbar: Sie soll für alle Einrichtungen gegenüber ihren Aufsichtsgremien und Mittelgebern überzeugend vertretbar sein (u. a. im Hinblick auf eine „Marktsituation“).

8. Strategisch: Sie soll die Zusammenarbeit in der Wissenschaft befördern, indem ein abgestimmtes Portfolio von laufend weiterentwickelten Diensten eine weite Verbreitung findet.

9. Robust: Sie soll Auslegungen von Regelungen vermeiden, mit denen eine Teilnahme am Netz oder den Diensten unter Missachtung dieser grundlegenden Prinzipien begründet werden könnte („Nachhaltigkeit und Zukunftsfähigkeit“ des Entgeltmodells).

Bei Fragen zur neuen Entgeltordnung können Sie uns unter folgender E-Mail-Adresse erreichen:
dfninternet@dfn.de

DIE ECKPUNKTE DER NEUEN ENTGELTORDNUNG:

Neues ermöglichen: Neben dem bekannten Regelanschluss und Clusteranschluss werden zukünftig auch ein Dienstpaket ohne Anschluss und ein Versorgeranschluss angeboten.

Dienstpaket ohne Anschluss: Dienste und Netzanschluss werden entbündelt

- Die Staffelung der Kategorien orientiert sich am Ist-Stand der Teilnehmer beim Regelanschluss.
- Die teilnehmenden Einrichtungen können die Kategorie nicht frei wählen – sie wird nach der jeweiligen Anzahl ihrer Nutzenden festgesetzt.
- Das Entgelt beträgt 27 % vom Regelanschluss.

Versorgeranschluss: Gemeinsam einen Anschluss nutzen

- Die beauftragte Bandbreite können die teilnehmenden Einrichtungen gemeinsam nutzen.
- Der Versorgeranschluss hat die gleichen Kategorien wie der Regelanschluss.
- Das Entgelt pro Kategorie ist geringer (degressiv 85 % – 74 % vom Regelanschluss).
- Jede teilnehmende Einrichtung muss ergänzend das „Dienst-Paket ohne Anschluss“ beauftragen.

Bewährtes anpassen: Regel- und Clusteranschluss werden überarbeitet

- Sie werden um eine neue kleinste Kategorie 01 ergänzt.
- Die Nummerierung der Kategorien wird „glattgezogen“ (von 01 bis 13).
- Pro Einrichtung wird eine Mindestkategorie festgesetzt („Dienstpaket ohne Anschluss“ – 2 Kategorien).

Weitergabe von Diensten: Der Handlungsspielraum für die Teilnehmer wird erweitert

- Das Verbot zur Weitergabe an Dritte wird gelockert.
- Die Versorgung von Gästen wird präzisiert (z. B. bei Messkampagnen an Forschungsgroßgeräten).

Altes beenden: Portanschlüsse und Mitnutzung werden mit einer Übergangszeit beendet

- Die neuen Regeln zur Weitergabe machen die heutige Mitnutzung obsolet.
- Heutige Teilnehmer werden unterstützt, um in ein alternatives Nutzungsmodell zu wechseln.

Schwarze Null: Die Maßnahmen sind so gestaltet, dass sie als Ganzes die Einnahmen des DFN-Vereins möglichst unverändert lassen sollen.

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. Leonie Schäfer ist für den DFN-Verein viel international auf Reisen. Nicht persönlich unterwegs und dennoch in weiter Ferne befand sie sich …

… in dem Webinar „NRENs Business Models“. Auftraggeber war WACREN, die Dachorganisation der westafrikanischen Forschungsnetze. Das Webinar ist Teil der e-Academy von WACREN; Co-Organisatoren sind der DFN-Verein und das französische Forschungsnetz RENATER.

In Westafrika dominieren einige wenige Internet-Provider die lückenhafte e-Infrastruktur der Region. Das Konzept eines Forschungsnetzes als Netzwerkanbieter und Dienstleister für Forschung und Lehre ist wenig verbreitet. WACREN bietet mit seiner e-Academy Starthilfe für neue Forschungsnetze in der Region und unterstützt sie bei ihrer Positionierung.

Das Ziel des Webinars „NRENs Business Models“ war es, die Bestandteile eines Businessplans zu erläutern, dessen Relevanz aufzuzeigen und passende Methoden und Werkzeuge vorzustellen. Dabei konnten die Teilnehmerinnen und Teilnehmer von den Erfahrungen anderer Forschungsnetze profitieren.

So wurden zum Beispiel im ersten Teil des Webinars Strategien zur Positionierung im Hinblick auf potenzielle Geldgeber sowie Universitäten und Forschungseinrichtungen als Kunden vorgestellt. Hierzu erläuterte George Konnis, der Direktor des zypriotischen Forschungsnetzes CYNET, seine Herangehensweise. CYNET ist mit nur vier Mitarbeitern ein eher kleines Forschungsnetz mit einer langen Geschichte, das vor einigen Jahren neu positioniert und aufgebaut wurde. In dieser Ausgangssituation und den damit verbundenen Herausforderungen finden sich die westafrikanischen Forschungsnetze gut wieder.

Der zweite Teil des Webinars fokussierte den Einsatz von Werkzeugen bei der Erstellung eines Businessplans. Für die zwei noch folgenden Webinar-Teile liegt der Schwerpunkt auf der Realisierung eines Businessplans durch die teilnehmenden NRENs. Unter anderem sind Einzelberatungen, sowie im Laufe des nächsten Jahres auch ein Besuch vor Ort geplant. ◆

Michael Röder ist Leiter des Bereichs IT-Services und für Themen rund um die DFN-Cloud mitverantwortlich. Im Rahmen des aktuellen europäischen Vergabeverfahrens für kommerzielle Public Cloud-Dienste nahm er an einer Reihe von …

… OCRE-Workshops teil, die nicht, wie ursprünglich geplant, in Dublin stattfanden, sondern online.

Januar 2020: Das Projekt Open Clouds for Research Environments (OCRE) schreitet voran. Es geht darum, eine Ausschreibung durchzuführen, die den gesamten Kontinent umspannt. Mit der unmittelbar bevorstehenden Eröffnung des Verfahrens beginnt die Uhr zu ticken: Es müssen Fristen genannt und eingehalten werden, um allen Anforderungen und Beteiligten gerecht zu werden. Das GÉANT-Procurement-Team ist sich schnell einig: Spätestens nach der Sommerpause steht ein großer Haufen Arbeit an. Um diesen optimal bewältigen zu können, wird im August 2020 ein Kick-off als Präsenzmeeting erforderlich sein. Im Team befinden sich Kolleginnen und Kollegen aus Norwegen, Deutschland, den Niederlanden, Großbritannien und Irland. Es wird ein gemeinsamer, mehrtägiger Workshop in Dublin geplant.

Dann kommt der März 2020 und bringt mit der COVID-19-Pandemie diverse Veränderungen, die für uns alle mittlerweile zum Alltag gehören. OCRE ist in dieser Phase kaum davon betroffen. Aber in Bezug auf die geplanten Dienstreisen für den Workshop in Dublin wachsen die Bedenken. Das bereitet Sorgenfalten im Team, denn der Zeitplan des gesamten Verfahrens ist knapp kalkuliert und eine Verzögerung der Auswertungsphase praktisch nicht wieder wettzumachen. Droht das Projekt zu scheitern? In den kommenden Tagen und Wochen wird schnell klar, dass 2020 Dienstreisen keine Option sein werden. Das Team beginnt, den Irland-Workshop in diverse VC-Sessions umzugestalten und stellt Tools zusammen, die für echtzeitfähige und ortsunabhängige Kollaboration besonders geeignet sind.

August 2020: Die Aufwärmphase in den VC-Sessions dauert etwas länger als üblich, dafür sind die Meetings im weiteren Verlauf so produktiv und angenehm wie eh und je – beinahe so, als säße man im selben Raum. Das Team hat den Vorteil, dass es mittlerweile seit circa sechs Jahren in nahezu unveränderter Konstellation zusammenarbeitet. Man kennt und schätzt sich – hat sich aber vorher noch nie im privaten Arbeitszimmer besucht. Und so ist es nicht selten, dass Hunde in Mikros bellen, Katzen durch den Bildschirm spazieren oder die Post an der Tür klingelt – Homeoffice eben! Das lockert die Diskussionen angenehm auf und verleiht ihnen einen zusätzlichen individuellen Touch. Danach geht es auf fachlicher und professioneller Ebene zügig weiter.

Der geplante Workshop in Dublin musste online stattfinden. *Foto: David-W-/photocase.de*

Das Resümee im September 2020: Es ist ein angenehmes und nicht weniger effizientes Arbeiten, als wir es im Januar geplant hatten. Alle Arbeiten liegen weiterhin im Zeitplan. Und das liegt auch maßgeblich an den Kollaborationstools. Es ist hilfreich und auch witzig, wenn Änderungen beinahe zeitgleich im Spreadsheet eintreffen, obwohl die Kolleginnen und Kollegen mehrere hundert Meilen entfernt am Schreibtisch sitzen.

Aber eine Sache fehlt, auch darüber sind sich alle im Team einig: Wenn wir einen Wunsch frei hätten, dann ginge der wohl für ein gemeinsames Abendessen drauf – ohne Webcams! ◆

DFN Live: Wissen teilen, Erfahrungen weitergeben

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

Erfolgreiche Onlinepremiere der 73. DFN-Betriebstagung

Ist Emotet dem Coronavirus zum Opfer gefallen? Was sagt der Datenschutz zu Home-Klausuren? Und wie sieht der Weg zu IPv6 jetzt aus? Die Onlineveranstaltung der 73. DFN-Betriebstagung, die am 15. und 16. September 2020 stattfand, wartete mit vielen spannenden Themen auf. Trotz oder vielleicht gerade wegen der „stürmischen Zeiten" – so auch der Titel des Vortrags von Dr. Thomas Hildmann (TU Berlin) im Cloudforum – wollten sich viele Teilnehmerinnen und Teilnehmer über die neuen Entwicklungen rund um das Deutsche Forschungsnetz und seine Dienste informieren. Denn natürlich spielte auch der Austausch der Erfahrungen und der gemeinsamen Herausforderungen während der COVID-19-Pandemie eine Rolle.

Gelungene digitale Premiere: Gewohnt souverän moderierte DFN-Kollege Michael Röder die Betriebstagung, dieses Mal online. *Foto: Nina Bark*

Bis zu 317 Teilnehmerinnen und Teilnehmer nahmen am gemeinsamen Plenum teil, das über die Pexip-Plattform von DFNconf gestreamt wurde. Und auch die Fachforen von AAI über Rechtsfragen bis VoIP, die in Zoom übertragen wurden, waren gut besucht. Die Chatfunktion in den einzelnen Foren sorgte für einen regen Austausch und auch der eine oder andere humorvolle Chatkommentar hob die Stimmung. Auch wenn keine Onlineveranstaltung die intensiven und herzlichen Diskussionen beim gemeinsamen Feierabendbier ersetzen

kann, so war die digitale Premiere der DFN-BT doch eine gelungene Alternative, die von der Community – den Feedbacks nach zu ordnen – sehr gut angenommen wurde.

TERMIN

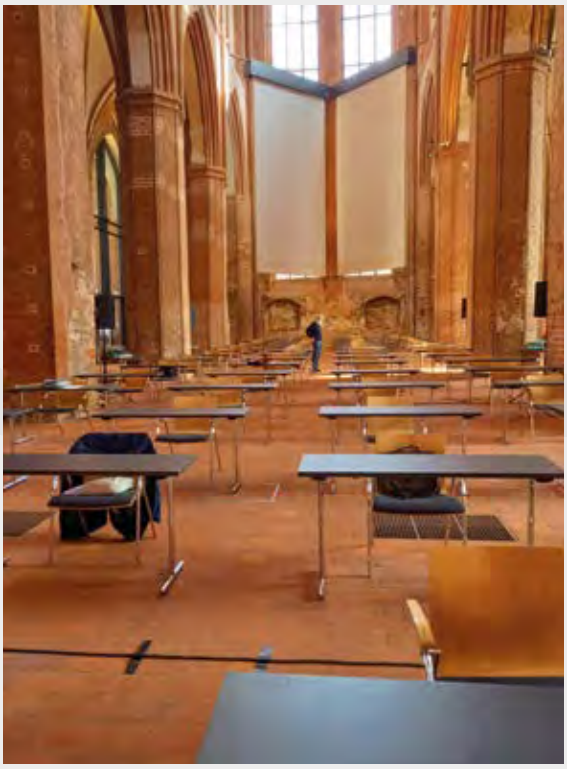
Die 74. Betriebstagung findet am **23. und 24. März 2021** statt.

15. Tagung der DFN-Nutzergruppe Hochschulverwaltung

„edu.kette – über den Umgang mit der Digitalisierung“: Das ist das Motto für die nächste Tagung der DFN-Nutzergruppe Hochschulverwaltung, die nach derzeitiger Planung vom 3. bis 5. Mai 2021 stattfinden wird.

Organisiert wird die Tagung vom DFN-Verein in Zusammenarbeit mit der Hochschule Wismar. Vortragende aus Forschung, Verwaltung und Wirtschaft beschäftigen sich mit hochaktuellen Themen aus den Bereichen Informationssicherheit, E-Government- und Onlinezugangsgesetz. Auch die Auswirkungen der COVID-19-Pandemie auf die Digitalisierung der Verwaltung werden ein Thema sein.

In der 1991 gegründeten DFN-Nutzergruppe Hochschulverwaltung werden bundesweit Informationen aus der Informations-, Kommunikations- und Medientechnik in direkten Bezug zu Themen der Hochschuladministration gesetzt. Die Ergebnisse werden den Hochschulen alle zwei Jahre auf einer Tagung vorgestellt.



Tagungsort St.-Georgen-Kirche zu Wismar, Foto: Meike Quaas

TERMIN

Die 15. Tagung DFN-Nutzergruppe Hochschulverwaltung findet voraussichtlich vom **3. bis 5. Mai 2021** statt.

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

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

Überblick DFN-Verein

(Stand: 11/2020)

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
(Climeworks AG)

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 Mitgliedseinrichtungen

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Technische Hochschule Aschaffenburg
Augsburg	Hochschule für angewandte Wissenschaften, Fachhochschule Augsburg
	Universität Augsburg
Bad Homburg	NTT Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	Berlin-Brandenburgische Akademie der Wissenschaften
	Berliner Institut für Gesundheitsforschung/Berlin 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 für Informationssicherheit gGmbH
	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn Rhein-Sieg
Schenefeld	European X-Ray Free-Electron Laser Facility GmbH
Schmalkalden	Hochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Siegen	Universität Siegen
Sigmaringen	Hochschule Albstadt-Sigmaringen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Hochschule Stralsund
Stuttgart	Cisco Systems GmbH
	Duale Hochschule Baden-Württemberg
	Hochschule der Medien Stuttgart
	Hochschule für Technik Stuttgart
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte Tautenburg
Trier	Hochschule Trier
	Universität Trier
Tübingen	Eberhard Karls Universität Tübingen
	Leibniz-Institut für Wissensmedien
Ulm	Technische Hochschule Ulm
	Universität Ulm
Vechta	Universität Vechta
	Private Hochschule für Wirtschaft und Technik gGmbH
Wadern	Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH (LZI)
Weimar	Bauhaus-Universität Weimar
	Hochschule für Musik FRANZ LISZT Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz
Weßling	T-Systems Information Services GmbH
Wiesbaden	Hochschule RheinMain
	Statistisches Bundesamt
Wildau	Technische Hochschule Wildau
Wilhelmshaven	Jade Hochschule Wilhelmshaven / Oldenburg / Elsfleth
Wismar	Hochschule Wismar
Witten	Private Universität Witten / Herdecke gGmbH
Wolfenbüttel	Ostfalia Hochschule für angewandte Wissenschaften
	Herzog August Bibliothek
Worms	Hochschule Worms
Wuppertal	Bergische Universität Wuppertal
	Kirchlische Hochschule Wuppertal/Bethel
Würzburg	Hochschule für angewandte Wissenschaften – Fachhochschule Würzburg-Schweinfurt
	Julius-Maximilians-Universität Würzburg
	Universitätsklinikum Würzburg
Zittau	Hochschule Zittau / Görlitz
Zwickau	Westsächsische Hochschule Zwickau

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

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

DFN newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

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