Deutsches Forschungsnetz | DFN Mitteilungen Ausgabe 88 | Mai 2015
www.dfn.de

DFN

Mitteilungen

In fünf Schritten in die DFN-Cloud

X-WiN – GÉANT – SINET:
Globales VPN für deutsch-japanische Weltraum-Mission

DFN-NeMo:
Erkennung und Bearbeitung von DDoS-Angriffen im X-WiN

9 770177 689001

Nachruf

Der Verein zur Förderung eines Deutschen Forschungsnetzes e. V. trauert um seinen langjährigen Vorstandsvorsitzenden

Prof. Dr.-Ing. Eike Jessen
28. August 1933 bis 18. März 2015

Als eine treibende programmatische Kraft, Gründungsvorstand und langjähriger Vorstandsvorsitzender des DFN-Vereins hat sich Eike Jessen herausragend um den Aufbau des Deutschen Forschungsnetzes und die Einführung und Verbreitung der rechnergestützten Datenkommunikation in Deutschland verdient gemacht.

Eike Jessen wurde als hervorragender und international anerkannter Wissenschaftler im Bereich der Informatik und insbesondere der Datennetze weit über das Forschungs- und Wissenschaftsumfeld hinaus geachtet und gehört. Mehr als drei Jahrzehnte lang hat er die Entwicklung des Deutsches Forschungsnetzes maßgeblich mitgeprägt und sich dadurch größte Verdienste für die Wissenschaft erworben.

Durch eine Vielzahl von Ehrenämtern in der Wissenschaft, als Träger des Bundesverdienstkreuzes am Bande und als Fellow der Gesellschaft für Informatik hat sich Eike Jessen bis ins letzte Lebensjahr hinein für das Deutsche Forschungsnetz engagiert und die Vision des DFN in Wissenschaft, Wirtschaft und Politik vertreten und vorangetrieben.

Unser tief empfundenes Mitgefühl gilt seiner Familie, seinen Freunden und Wegbegleitern.

Lieber Herr Jessen, herzlichen Dank für alles – Sie werden uns fehlen.

Prof. Dr. Hans-Joachim Bungartz
im Namen der Mitglieder und der Mitarbeiterinnen und Mitarbeiter des DFN-Vereins

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 - 70
Mail: dfn-verein@dfn.de
Web: www.dfn.de

ISSN 0177-6894

Redaktion: Kai Hoelzner (kh)
Gestaltung: Labor3 | www.labor3.com
Druck: Bloch&Co, Berlin

Fotonachweis:
Titelfoto © infinity / fotolia
Seite 8/9 © chungking / fotolia
Seite 10 © R9_RoNaLdO / iStock
Seite 36/37 © Nine Ok / gettyimages

Bob Day
Executive Director, Janet;
interim CEO, GÉANT Association

The recent merger of DANTE and TERENA into the new GÉANT Association (described in the last edition of DFN-Mitteilungen) was a major chapter in the continuing history of increased collaboration amongst Europe's NRENs. Apart from producing a more coherent organisation and removing duplication, it offers new opportunities to harness to much better effect our collective expertise and innovation in the service of European research and education.

So what will be the next challenges to take up? They will be many and varied, but it is clear that the research community across very many disciplines is approaching a profound shift in the way it conducts its business. The widespread availability of unprecedented amounts of data, alongside the storage and computational facilities to exploit these, will mean that ever more data-intensive research will be conducted, with mining of this data supplementing or even in some disciplines replacing more traditional experimental techniques.

The physical infrastructure to support this, including the high-performance networks needed to connect researchers, data and processing, already exist in the form of national networks such as X-WiN and my own NREN, Janet, alongside GÉANT to interconnect them across Europe and to the wider world. There are many challenges to be surmounted in sustaining this infrastructure in the present economic climate, but the technological aspects of these are well understood and largely tractable.

Newer, and more challenging, are the issues around management of the datasets involved. Storing them and making them accessible in a form that can be relied upon by other researchers is one aspect of this. Another, equally important, is managing access to the data. Increasingly, such datasets are sensitive, either because they have a commercial value or because their use raises societal issues of privacy and ethical use of the data, particularly where large previously unconnected datasets are combined. Failure to address these issues poses a very real risk that the full value to humankind is not realised. There have already been examples where poor handling of the aspects of privacy and ethics has led to this unfortunate outcome.

Europe's NRENs are uniquely positioned to contribute. We have unprecedented achievements in services such as eduroam and edugain, where highly scalable, reliable and trusted authentication and authorisation are critical. Janet is currently engaged in a major project with the UK's health informatics research community applying these technologies to medically sensitive data, alongside introducing services to allow for secure transfer of such data across the network. As GÉANT now goes forward I confidently expect the next chapter to be one where Europe's NRENs provide the basis for the true exploitation of the "data tsunami" – or the "data bonanza" as one scientist a few years ago described it to me!


1


2


3


4


5


6


7


8


9


10


11


12


13


14


15

Unsere Autoren dieser Ausgabe im Überblick

1 Michael Röder, DFN-Verein (roeder@dfn.de); **2** Dr. Thomas Hildmann, Technische Universität Berlin (thomas.hildmann@tu-berlin.de); **3** Prof. Dr.-Ing. Stefan Schwarz, Universität der Bundeswehr München (Stefan.Schwarz@unibw.de); **4** Benedikt Wegmann, GWDG (benedikt.wegmann@gwdg.de); **5** Gisela Maiß, DFN-Verein (maiss@dfn.de); **6** Jochen Schönfelder, DFN-CERT Services GmbH (schoenfelder@dfn-cert.de); **7** Henry Kluge, DFN-Verein (kluge@dfn.de); **8** Christian Meyer, DFN-Verein (cmeyer@dfn.de); **9** Dr. Jakob Tendel, DFN-Verein (tendel@dfn.de); **10** Dr. Leonie Schäfer, DFN-Verein (schaefer@dfn.de); **11** Thorsten Hindermann, GWDG (thorsten.hindermann@gwdg.de); **12** Dr. Ralf Gröper, DFN-Verein (groeper@dfn.de); **13** Jürgen Brauckmann, DFN-CERT Services GmbH (brauckmann@dfn-cert.de); **14** Kevin Kuta, Forschungsstelle Recht im DFN (kuta@dfn.de); **15** Philipp Roos, Forschungsstelle Recht im DFN (recht@dfn.de)

Inhalt

Wissenschaftsnetz

In fünf Schritten in die DFN-Cloud
von Michael Röder 10

Cloudspeicher auf Basis von ownCloud Enterprise
von Thomas Hildmann 15

TeamDrive: Sync&Share an der Universität der Bundeswehr München
von Stefan Schwarz 16

GWDG Cloud Share
von Thorsten Hindermann 16

DFN-NeMo: Erkennung von DDoS-Angriffen
von Gisela Maiß, Jochen Schönfelder 18

Kein X für ein U – mehr Sicherheit fürs Domain Name System!
von Henry Kluge 22

DFNFernsprechen: Kurznachrichten über SMS-Gateway versenden
von Christian Meyer 29

Kurzmeldungen 30

International

Globales VPN für deutsch-japanische Weltraum-Mission
von Jakob Tendel 32

GÉANT in HORIZON 2020
von Leonie Schäfer 34

Kurzmeldungen 35

Sicherheit

Sicherer E-Mail-Verkehr im DFN – von der Beantragung bis zur Nutzung von Zertifikaten
von Thorsten Hindermann 38

Sicherheit aktuell
von Ralf Gröper, Jürgen Brauckmann 42

Recht

Lifestyle contra Sicherheit
von Kevin Kuta 43

Freies Wissen für alle?
von Philipp Roos 49

DFN-Verein

Übersicht über die Mitgliedseinrichtungen und Organe des DFN-Vereins 54

Wissenschaftsnetz

In fünf Schritten in die DFN-Cloud
von Michael Röder

Cloudspeicher auf Basis von ownCloud Enterprise
von Thomas Hildmann

TeamDrive: Sync&Share an der Universität der Bundeswehr München
von Stefan Schwarz

GWDG Cloud Share
von Thorsten Hindermann

DFN-NeMo: Erkennung von DDoS-Angriffen
von Gisela Maiß, Jochen Schönfelder

Kein X für ein U – mehr Sicherheit fürs Domain Name System!
von Henry Kluge

DFNFernsprechen: Kurznachrichten über SMS-Gateway versenden
von Christian Meyer

Kurzmeldungen

In fünf Schritten in die DFN-Cloud

Viele wissenschaftliche Einrichtungen haben große Erfahrung mit der Bereitstellung von Cloud-Diensten. Mit der DFN-Cloud schafft der DFN-Verein einen Rahmen, in dem diese Cloud-Dienste von allen Teilnehmern am DFN-Verbund genutzt werden können. In entsprechenden Forschungsvorhaben bringt der DFN-Verein Anbieter und Nutzer zusammen, um die DFN-Cloud zu nutzen, zu erproben und weiterzuentwickeln.

Text: **Michael Röder** (DFN-Verein)

Eine Cloud für die Wissenschaft

Mit der Einführung föderierter Dienste eröffnet der DFN-Verein seinen Anwendern die Möglichkeit, sich neben der Inanspruchnahme der zentralen Dienste im DFN künftig auch gegenseitig Dienste zur Verfügung zu stellen. Der DFN-Verein schafft dafür einen Rahmen, innerhalb dessen Cloud-Dienste von allen Teilnehmern am DFN-Verbund sowohl angeboten als auch genutzt werden können. Ziel ist nicht allein die Nutzung der DFN-Cloud – das Augenmerk liegt vor allem auf der Erprobung und Weiterentwicklung von Diensten in der Community.

Die DFN-Cloud startet mit Dienstprofilen aus dem Sync&Share-Umfeld. Dabei handelt es sich um Dienste, die zur Dateiablage und -synchronisierung über verschiedene Endgeräte entstanden sind. Damit kann der Endnutzer zentral gespeicherte Daten per Freigabe einem definierten Empfängerkreis zugänglich machen und gezielt Rechte zur Bearbeitung der Inhalte vergeben. In der Vergangenheit wurden gemeinsam bearbeitete Daten und Dokumente vielfach als Anhang von E-Mails oder über ungesicherte FTP-Verbindungen ausgetauscht. Der Synchronisierungsprozess im Anschluss an die Bearbeitung passierte manuell. Ein Sync&Share-Dienst verfügt im Gegensatz dazu über einen lokalen Client, der die Kollaboration vereinfacht, indem er den Datenbestand bei bestehender Netzwerkverbindung automatisch aktualisiert, sobald eine Veränderung vorgenommen wurde. Außerdem besteht die Möglichkeit, die eigenen Dokumente über den Browser zu nutzen und zu editieren – völlig unabhängig von Bearbeitungsort und Betriebssystem.

Mit einem breit im DFN-Verein abgestimmten Konzept über die Organisation und die administrative Abwicklung beim Anbieten und Nutzen bisher nur lokal oder regional verfügbarer Cloud-Services ermöglicht die DFN-Cloud ab sofort eine wissenschaftskonforme Bereitstellung und Nutzung dieser Form der Zusammenarbeit im gesamten Wissenschaftsnetz.

Schon heute stehen in der DFN-Cloud mit GWDG Cloud Share, der TU Berlin ownCloud und UNIBW Sync&Share erste für die Zwecke von Forschung und Lehre maßgeschneiderte Cloud-Services bereit. Weitere Cloud-Dienste sollen in den kommenden Jahren folgen.

DFN-Cloud verbindet Anbieter und Nutzer von Diensten

Die Teilnahme an der DFN-Cloud ist auf zwei unterschiedliche Arten möglich: Entweder bietet ein Teilnehmer einen Dienst in der DFN-Cloud an und tritt in der Folge als Forschungspartner auf – oder der Teilnehmer nutzt einen Cloud-Dienst und wird dadurch als Erprobungspartner aktiv. Dabei schließen sich beide Rollen gegenseitig nicht aus, denn die DFN-Cloud selbst ist kein expliziter Dienst. Sie bildet vielmehr das Dach für eine Vielzahl darunter vereinter Dienste und ist dadurch vergleichbar mit bereits bekannten Diensten im DFN: Um beispielsweise DFNInternet oder DFNFernsprechen nutzen zu können, muss der Rahmenvertrag über die Teilnahme am Deutschen Forschungsnetz anerkannt werden. Aus diesem Grund kann eine Einrichtung einen Dienst nutzen, während sie gleichzeitig einen anderen selbst anbietet.

In der Rolle des administrativen Partners und Organisators steht der DFN-Verein allen Teilnehmern in der DFN-Cloud zur Verfügung.

Erprobungs- oder Forschungsrahmenvertrag?

Wer an der DFN-Cloud teilnehmen möchte, muss dafür zunächst einen Vertrag mit dem DFN-Verein abschließen. Hierbei existieren unterschiedliche Verträge, je nachdem ob eine Einrichtung Cloud-Dienste nutzen oder anbieten will. Einrichtungen, die einen Cloud-Dienst nutzen wollen, setzen sich über cloud@dfn.de mit dem DFN-Verein in Verbindung und erfragen den Erprobungsrahmenvertrag. Möchte eine Einrichtung selbst einen Dienst in der DFN-Cloud anbieten, erhält sie auf demselben Weg den Forschungsrahmenvertrag. Einrichtungen, die sowohl Dienste nutzen als auch anbieten wollen, schließen beide Verträge ab.

Am Ende dieses Schrittes sind neben den allgemeinen Rechten und Pflichten auch grundsätzliche Fragen wie z. B. die Laufzeit geregelt. Damit sind die Voraussetzungen abgeschlossen, um an der DFN-Cloud teilzunehmen – ohne dass bereits Details einzelner Dienste betroffen wären.

Auswahl des passenden Cloud-Dienstes

Im nächsten Schritt soll bei der Nutzung der DFN-Cloud der passende Dienst gefunden werden. Da jeder Anbieter eines Cloud-Services ein eigenes Betriebsmodell für seinen Dienst entwickelt hat, können sich die verschiedenen Dienste in der DFN-Cloud sowohl im Entgeltmodell als auch in Fragen der Verschlüsselungstechnologie, der Lizenzpolitik oder der Einflussnahme auf die Entwicklung der Software voneinander unterscheiden.

Eine Übersicht sämtlicher Dienste in der DFN-Cloud ist auf der Webseite des DFN-Vereins unter
https://www.dfn.de/dfn-cloud/
verfügbar.

Um interessierte Einrichtungen bei der Entscheidung zu unterstützen, sind hier die Basisfunktionen der jeweiligen Services in Kurzporträits dargestellt und konkrete Informationen über das

jeweilige Entgeltmodell abgebildet. Technische Details können zielgerichtet vom Ansprechpartner abgerufen werden, der durch den Forschungspartner hier hinterlegt wurde.

Eine Kurzvorstellung der ersten Dienste in der DFN-Cloud durch ihre Anbieter findet sich ebenfalls in dieser Ausgabe der DFN- Mitteilungen.

Unentgeltliche Probenutzung

Selbstverständlich können nicht alle Facetten eines umfangreichen Dienstes in wenigen Worten abgebildet werden. Die DFN-Cloud ist daher so konzipiert, dass die Dienste zunächst für einen gewissen Zeitraum kostenneutral erprobt werden können, bevor sich ein Teilnehmer für eine dauerhafte Nutzung eines Dienstes entscheidet.

Diese Probenutzung kann ohne Zutun des DFN-Vereins durchgeführt werden. Im Sinne der gemeinsamen Weiterentwicklung der DFN-Cloud ist der DFN-Verein jedoch interessiert daran zu erfahren, welche Beweggründe zur Auswahl eines Dienstes der DFN-Cloud geführt haben.

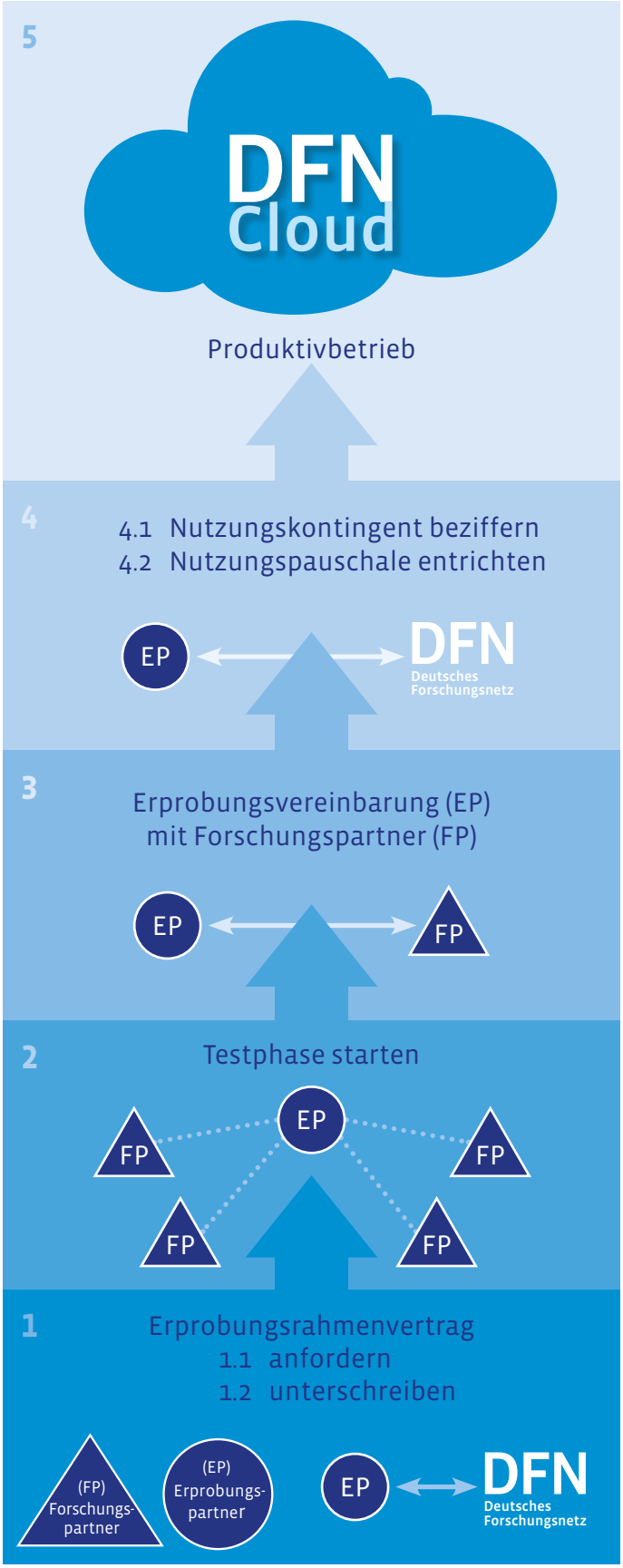
Hat sich ein potentieller Anwender auf der Grundlage dieser Erprobung für die Nutzung eines bestimmten Dienstes entschieden, ist der dritte Schritt geschafft.

Erprobungsvereinbarung mit dem Anbieter

Im dritten Schritt stimmen sich Anwender und Anbieter des Cloud-Dienstes darüber ab, auf welcher Basis der Dienst schließlich an die tatsächlichen Endnutzer – nämlich die Mitarbeiter und Studenten des Erprobungspartners – weitergereicht wird. Das Ergebnis wird in der sogenannten „Erprobungsvereinbarung“ festgehalten.

Die Erprobungsvereinbarung hilft dabei, das rechtlich-technische Verhältnis zwischen Anwender und Anbieter zu regulieren. Konkret betrifft das beispielsweise Fragen der Haftung und des Datenschutzes. Aber auch Details zur Laufzeit der Vereinbarung und das Format der Daten bei Herausgabe können darin verankert werden.

Bei der Gestaltung der Erprobungsvereinbarung haben beide Seiten weitgehend freie Hand. Der DFN-Verein bietet allerdings Formulierungsvorschläge an, die im bilateralen Verhältnis zwischen Anbieter und Anwender bearbeitet werden können – solange das Ergebnis nicht im Widerspruch zu den Rechten und Pflichten steht, die dem Anwender durch Anerkennung des Erprobungsrahmenvertrages und dem Anbieter durch Unterzeichnung des Forschungsrahmenvertrages zugesichert werden.



Für den Weg in die DFN-Cloud sind fünf Schritte erforderlich.

Anmeldung beim DFN-Verein

Der vierte Schritt besteht darin, beim DFN-Verein die Nutzung eines konkreten Dienstes anzumelden. Dadurch werden im Wesentlichen der Mitwirkungsbeginn und das Nutzungskontingent festgelegt. Der Anwender muss bei der Anmeldung für einen Dienst nach bestem Wissen abschätzen, in welchem Umfang er nach seiner eigenen Einschätzung den Cloud-Dienst im Mittel über das Kalenderjahr nutzen wird. Der Anwender verpflichtet sich, die künftige Nutzung des Dienstes möglichst gewissenhaft und nicht zum Nachteil eines Dienstanbieters einzuschätzen. Der DFN-Verein berät die Einrichtungen hierbei und stellt den Partnern seine Erfahrung bei der Gestaltung solcher Entgeltmodelle zur Verfügung.

Nach der Anmeldung steht es dem Anwender frei, den Cloud-Dienst nach seinen Bedarfen zu nutzen. Überschreitet er sein Nutzungskontingent, so muss er es jedoch im fünften und letzten Schritt für das Folgejahr entsprechend anpassen.

Kostenumlage der DFN-Cloud

Die Kosten für die DFN-Cloud werden den Anbietern der Cloud-Dienste vom DFN-Verein erstattet. Zur Deckung dieser Kosten zieht der DFN-Verein die Anwender anteilig entsprechend ihren Anmeldungen und der veröffentlichten Kostenumlage für die DFN-Cloud heran.

Somit trägt der DFN-Verein die Verantwortung, auf mittlere Sicht eine kostendeckende Finanzierung der DFN-Cloud sicherzustellen.

Der Ausgleich von Planungsabweichungen und Schwankungen bei der Nutzungsintensität erfolgt durch Anwendung des Fair-Use-Modells jeweils in der nächsten Nutzungsperiode, in der die Entgelte auf der Basis der Vorjahresverbrauche festgelegt werden. Jeweils bis zum 1. November eines Jahres melden die Nutzer dem DFN-Verein ein aktualisiertes Nutzungskontingent pro Cloud-Dienst, auf dessen Grundlage das Jahresentgelt für das Folgejahr bestimmt wird.

DFN-Cloud als Motor für künftige Dienste

Ziel der DFN-Cloud ist nicht nur, den Anwendern im Wissenschaftsnetz dezentrale Dienste in der DFN-Cloud zur Verfügung zu stellen, sondern die Funktionen, Prozesse und Bedingungen föderierter Dienste unter aktiver Mitwirkung aller Beteiligten zu erforschen. Das rege Interesse der Anwender an der DFN-Cloud spiegelt den Bedarf an wissenschaftskonformen Cloud-Diensten wider. Zugleich zeigt es die Potentiale, die ein Aufsetzen von Diensten für einen größeren Kreis von Anwendern hinsichtlich einer Economy of Scale für die Anbieter hat.

Dem DFN-Verein ist es gelungen, mit der DFN-Cloud einen Rahmen zu schaffen, innerhalb dessen sich Einrichtungen rechtssicher und zu vernünftigen Konditionen gegenseitig Dienste erbringen können. Damit hat die DFN-Cloud die Chance, ein Motor für die Ausweitung bestehender und die Entwicklung neuer Dienstinhalte zu werden. ◆

Foto © Gio_1978/fotolia

Cloudspeicher auf Basis von ownCloud Enterprise

Text: **Dr. Thomas Hildmann** (Technische Universität Berlin)

Plattformunabhängige Cloud-Lösung

Der DFN-Verein organisiert unter dem Stichwort „DFN-Cloud“ eine Cloud für die Wissenschaft. Die in diesem Rahmen angebotenen Cloud-Dienste können von allen Mitgliedern des DFN-Verbunds genutzt, erprobt und weiterentwickelt werden. Die TU Berlin bietet im Rahmen der DFN-Cloud den Dienst: „Cloudspeicher auf Basis von ownCloud Enterprise“ mit Hilfe des Speicherdienstes „ownCloud“ an und stellt einen ortsunabhängigen Speicherbereich für Daten zur Verfügung.

ownCloud synchronisiert persönliche Daten auf mehreren Endgeräten. Clients stehen aktuell für Windows, Linux, OS X, iOS und Android zur Verfügung. Die Dateien sind ferner über ein Webinterface oder über WebDAV zugreifbar. Über verschiedene Plugins kann die Funktionalität (z. B. über eine Fotogalerie, einen Editor, einen Kalender usw.) erweitert werden. ownCloud ist eine quelloffene Alternative zu den bekannten Cloud-Speicherdiensten wie z. B. Dropbox.

Blick in den Maschinenraum

Der Dienst wird 24/7 zur Verfügung gestellt. Updates der ownCloud-Server-Version erfordern eine Downtime von gewöhnlich wenigen Minuten. Der Dienst wird über ein Cluster mit mehreren Webfrontends, ein Datenbankcluster und ein mehrfach redundantes Speichersystem über zwei Rechenzentrumsstandorte verteilt angeboten. Ferner findet eine zusätzliche Sicherung über eine Tape-Library in unserer Lampertz-Zelle statt. Die tubIT-Administratoren werden vom ownCloud-Support-Team unterstützt.

Standard-Verfügbarkeit

Bei der Standard-Verfügbarkeit werden die Daten in der ownCloud jeweils nur auf einem der beiden Rechenzentren der TU Berlin gespeichert. Steht eines der Rechenzentren temporär nicht zur Verfügung (z. B. wegen Wartungsarbeiten, die die Abschaltung eines RZ nötig machen, wegen Ausfall der Leitungen zum RZ o.ä.), kann somit auch der Dienst für den Erprobungspartner ausfallen.

Premium-Verfügbarkeit

Bei der Premium-Verfügbarkeit werden die Daten auf beiden Rechenzentren gespiegelt. Bei Ausfall eines kompletten RZ kann der Dienst (evtl. mit reduzierter Performanz) weiter erbracht werden.

Quelloffene Linux-Lösung

Die Entscheidung zugunsten der Linux-basierten quelloffenen ownCloud basiert auf einer Evaluation, die die tubIT im Jahr 2012 durchgeführt hat. Vor allem galt es, schon zuvor bekannt gewordene Sicherheits- und Rechtsprobleme bei der Nutzung von Cloud-Diensten zu lösen. Dabei standen Wartbarkeit, Skalierbarkeit und vor allem die Bedienschnittstelle und damit der Supportaufwand im Vordergrund der Evaluation. Die Marktanalyse erbrachte zum damaligen Zeitpunkt keine interessanten Outsourcing-Möglichkeiten. Hingegen zeigten einige getestete Produkte hohes Potential auch für die Integration und Weiterentwicklung des Dienstes, weshalb die TU Berlin sich entschlossen hat, den Dienst selbst aufzusetzen.

Technische Universität Berlin

Da die TU Berlin in vielen Bereichen seit Langem mit anderen Hochschulen zusammengearbeitet hat und aus eigener Erfahrung bei der Suche nach geeigneten Dienstanbietern wusste, dass es hier eine Marktlücke gibt, beteiligte sie sich von Beginn an an der Mitgestaltung der DFN-Cloud mit dem Ziel, den Dienst für andere Hochschulen anzubieten.

Economy of Scale

Die Bereitstellung des Dienstes für eine größere Anzahl von Nutzern erhöht in der Regel den Administrationsaufwand nur unwesentlich. Hingegen ist es möglich, bestimmte Infrastruktur in größerem Maßstab für den Einzelnen sehr viel günstiger anzuschaffen. Insofern ist es auch im Interesse der TU Berlin, etwaige Hardware- und Supportkosten mit anderen Hochschulen zu teilen.

Sicherheit

An Stelle der in ownCloud implementierten serverseitigen Verschlüsselung werden derzeit verschiedene Lösungen von Drittherstellern auf ihre Eignung im Zusammenspiel mit ownCloud getestet. Eine Client-seitige Verschlüsselung würde nicht nur den Schutz gegen Ausspähen erhöhen, sie hätte ferner keinen Einfluss auf die Auslastung der Infrastruktur.

Flexibel für Nutzerwünsche

Neben der Tatsache, dass die Daten der tubCloud sowie der über die DFN-Cloud angeschlossenen Instanzen ausschließlich in den beiden Datacenter-Standorten der TU Berlin gespeichert werden, steht auch die Flexibilität des Dienstes in Richtung Anpassung an Nutzerwünsche und Integration in die vorhandene Infrastruktur im Vordergrund. Die Vereinbarung zur Auftragsdatenverarbeitung und das Sicherheitskonzept wurden bereits intern wie auch extern positiv bewertet. ownCloud bietet viele Schnittstellen, die für die Integration im Hochschulumfeld benötigt werden. Ferner hat ownCloud eine große Community, die das Produkt weiterentwickelt, gekoppelt mit einem vertrauenswürdigen Team, das diese Entwicklungen in unserem Sinne kanalisiert. ◆

TeamDrive: Sync&Share an der Universität der Bundeswehr München

Text: **Prof. Dr.-Ing. Stefan Schwarz** (Universität der Bundeswehr München)

Gehäufte Nachfragen sicherheitsbewusster Anwender und die Analyse des aktiven Nutzungsverhaltens filebasierter Clouddienste haben an der Universität der Bundeswehr München (UniBw M) im Jahr 2013 dazu geführt, ein hochschulinternes Angebot zur Bereitstellung von Sync&Share-Diensten zu projektieren. Nur dadurch kann einerseits den im Hinblick auf Sicherheit und Datenschutz bereits sensibilisierten Anwendern als auch der Gruppe der weniger arglosen Nutzer ein langfristig sicheres Verfahren zur zentralen Ablage und gemeinsamen Nutzung von nahezu allen Arten von Daten angeboten werden.

Die Initiative des DFN-Vereins zu einem föderierten Dienst für Sync&Share wurde von der Universität der Bundeswehr München von Beginn an unterstützt und eine Integration der Föderation war eine Grundvoraussetzung in der Auswahl möglicher Produkte. Nur dadurch ist auch gewährleistet, dass Kooperationen zwischen Einrichtungen im Bereich von Lehre und Forschung auch durch die gemeinsame Bereitstellung von Dokumenten sinnvoll unterstützt werden.

Primäres Ziel war stets eine ausreichende Berücksichtigung des Datenschutzes. Daten und Dokumente sollten zwingend so geschützt werden, dass eine unberechtigte Kenntnisnahme oder

der Bundeswehr Universität München

Manipulation (Vertraulichkeit und Integrität) außerhalb des Nutzerarbeitsplatzes wirksam verhindert werden kann. Dazu zählt auch der Schutz der zuständigen Administratoren vor dem bloßen Verdacht. Aus den Erfahrungen im Nutzerverhalten der Anwender zeigt sich, dass insbesondere datenschutzrelevante Dokumente bevorzugt mit anderen Anwendern geteilt werden (Bewerbungen/Berufungsverfahren, Prüfungen, Notenlisten, Sitzungsprotokolle etc.). Ein wesentliches Kriterium dazu ist auch die Speicherung und Verarbeitung der Daten an einem klar definierten Ort, was zusätzliches Vertrauen der Anwender schafft.

Nach einer Marktanalyse vorwiegend unter Nutzung bereits einschlägiger (Fraunhofer SIT, DFN) Studien fiel die Entscheidung ganz eindeutig zu Gunsten des Produkts TeamDrive (TeamDrive GmbH, Hamburg) aus. Danach wurde das Produkt über eine sechsmonatige Testphase intensiv (auch durch externe Einrichtungen) getestet, vor allem wurde dabei auch die Handhabung des Datenschutzes über verschiedene Nutzungsszenarien (insbesondere sicheres Schlüsselmanagement) geprüft, was direkte Änderungen in der Grundkonfiguration veranlasste. Bereits zu diesem Zeitpunkt war durch die Authentifizierung und Autorisierung über Shibboleth die Integration in die DFN-AAI sichergestellt. Als Resultat wurde der Dienst TeamDrive nahezu zeitgleich mit der Registrierung als Erprobungspartner des DFN im Juni 2014 gestartet. ◆

GWDG Cloud Share

Text: **Benedikt Wegmann** (GWDG – Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen)

Die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) betreibt für ihre Nutzer seit 2012 den Dienst „GWDG Cloud Share“. Am Anfang des Projektes stand die Anfrage der Max-Planck-Gesellschaft MPG, eine Alternative zu dem verbreiteten Dienst »Dropbox« anzubieten. Forschungsdaten sollten komfortabel verwaltet und verteilt werden können, ohne die Hoheit über die eigenen Daten zu verlieren, welche in einem Rechenzentrum der Deutschen Forschungsgemeinschaft verbleiben sollten, statt einem internationalen Cloud-Anbieter anvertraut zu werden.

GWDG Cloud Share steht seit Beginn der DFN-Cloud als Angebot zur Verfügung. Durch ein modernes Betriebskonzept und ein gutes Angebot des Herstellers PowerFolder kann die GWDG den Dienst für Interessenten mit minimalem Aufwand und geringen Kosten anbieten. Das neue Angebot eignet sich mit einem flexiblen Preismodell sowohl für kleinere bis mittlere Teams oder Abteilungen als auch mit einem stark ermäßigten Preismodell für ganze Einrichtungen. Interessenten steht der Dienst für drei Monate zur kostenfreien Evaluierung zur Verfügung.

Der Dienst wird von der GWDG in ihrem modernen, ISO-zertifizierten Rechenzentrum mit hoher zugesicherter Verfügbarkeit in der eigenen Servervirtualisierung und mit eigenem Storage betrieben. Verwaltet wird GWDG Cloud Share durch ein zentrales Konfigurationsmanagement. Durch dieses Konzept wird ein leicht skalierbarer Betrieb mit geringem administrativem Mehraufwand erreicht, der schnell eine größere Zahl neuer Benutzer aufnehmen kann.

Im Vergleich zu Clients anderer verbreiteter Dienste erlaubt der Client von GWDG Cloud Share ein flexibleres Verwalten unterschiedlicher Ordner des Benutzers in individuellen Pfaden. Dadurch müssen Nutzer die Organisation ihrer Daten nicht ändern und es können relevante Verzeichnisse einfach unter die Verwaltung von GWDG Cloud Share gestellt werden.

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Um Nutzern einen flexiblen Zugriff auf ihre Daten zu ermöglichen, bietet der Dienst eine moderne Web-Oberfläche, Clients für die gängigsten Desktop-Betriebssysteme ebenso wie für Android- und iOS-Oberflächen sowie eine API für Benutzer und Unterstützung für WebDAV.

Die GWDG hat als einer der ersten Anbieter von Cloud-Services in der DFN-Community seit 2012 Erfahrung im Betrieb des Dienstes, entwickelt das Betriebskonzept eigenständig weiter und unterstützt den Hersteller in der Weiterentwicklung des Produktes für den breiten Einsatz im Hochschulrechenzentrum. ◆

DFN-NeMo: Erkennung von DDoS-Angriffen

Für den sicheren Betrieb des DFNInternet-Dienstes auf dem X-WiN zählt die Beobachtung und Analyse des Netzverhaltens – das Netzwerk-Monitoring – zu den wesentlichen Aufgaben. Zur Abwehr von Angriffen auf die Infrastruktur müssen geeignete Methoden entwickelt und eingesetzt werden, die die Erkennung von DDoS (Distributed Denial of Service) Angriffen ermöglichen. Aufgrund der Analyse eines Angriffs und der erkannten Netzwerk-Anomalien soll das Netz so angepasst werden, dass der Angriff weitestgehend eingedämmt werden kann.

Text: **Gisela Maiß** (DFN-Verein)**, Jochen Schönfelder** (DFN-CERT Services GmbH)

Foto © johny schorle / photocase.de

In den letzten Jahren wurde eine Entwicklung gestartet, die genau diese Anomalien-Erkennung im Datenverkehr über das X-WiN zum Ziel hat. Sie soll zur Alarmierung und Unterstützung bei der Vorfallsbearbeitung dienen und setzt mit ihren Methoden und Lösungen gezielt die betrieblichen Anforderungen der beteiligten Gruppen um.

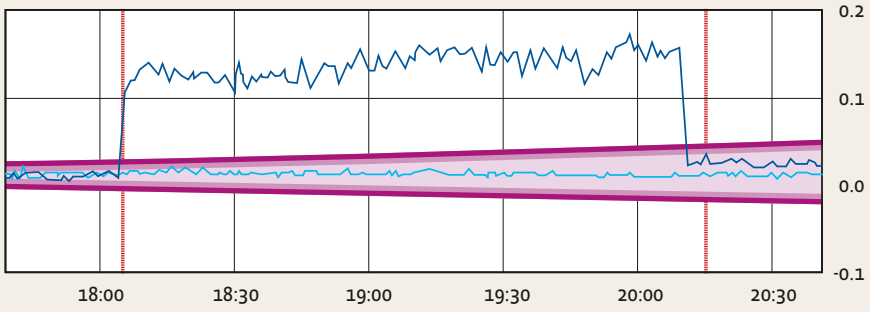
Um Anwendungen wie die Erkennung von DDoS-Angriffen im Betrieb des X-WiN verankern zu können, ist es neben der Entwicklung nötig, die vorhandenen Geschäftsprozesse zu analysieren und weiterzuentwickeln. Dabei kommt der Berücksichtigung der nachhaltigen Nutzung sowie der Gewährleistung von Datenschutz und Datensicherheit bei der Auswertung der Verkehrsdaten ein hoher Stellenwert zu.

1. Hintergrund der Entwicklung von DFN-NeMo

Der Bedarf für das Netzwerkmonitoring-Tool DFN-NeMo entstand aus der täglichen Arbeit der Mitarbeiter vom DFN-NOC und dem Incident Response Team (IRT) des DFN-CERT. Diese wurden in ihrer täglichen Arbeit mit Netzwerkanomalien konfrontiert, für die ein Analysewerkzeug benötigt wurde.

Eine typische Ursache solcher Anomalien sind kurzfristige Überlastsituationen der betroffenen Infrastruktur durch Datenströme mit extrem hohem Verkehrsaufkommen. Hierbei kann es sich um Angriffe auf Komponenten des X-WiN, auf Anwender im X-WiN oder auch um Angriffe handeln, die von Anwendern selbst ausgehen. Aber nicht alle Angriffe verursachen anhand von Überlast erkennbare Anomalien und nicht alle erkannten Anomalien im Überlastbereich werden durch Angriffe verursacht. Daher sind ein genaues Monitoring und die Analyse des Datenverkehrs im X-WiN in der jeweiligen Situation für eine Bewertung des Vorgangs dringend erforderlich.

DFN-NeMo wird im Auftrag des DFN-Vereins von einem Team des DFN-CERT entwickelt. Nach ersten Vorarbeiten im Jahr 2010 wurde 2011 mit der Entwicklung begonnen. Seit 2013 wird die Software „produktionsnah“ beim DFN-NOC eingesetzt.



dunkelblau: Paketanzahl von Verbindungen im Aufbau im Verhältnis zur Paketanzahl der aktuell bestehenden Verbindungen
hellblau: das Verhältnis in der Vergangenheit
Anmerkung: Das Verlassen des Korridors führt zu einem Alarm.

Abb. 1: Beispiel eines Alarms auf einer Leitung, ausgelöst durch die Abweichung von statistischen Schwellwerten

2. Struktur der DDoS-Anwendung

DFN-NeMo kann als ein System aus Arbeitsprozessen und -schritten beschrieben werden, die auf Betriebsdaten im X-WiN zugreifen und diese im Sinne definierter interner Dienste verarbeiten. So sind als Grundlage zur Modellierung des X-WiN aktuelle Informationen erforderlich, die die Netztopologie abbilden. Mit diesen Informationen werden den Routern, Leitungen, Autonomen Systemen (AS) und IP-Adressbereichen des X-WiN Kenndaten zugeordnet. Die eigentliche Messung von Daten ist nicht Bestandteil der DFN-NeMo-Entwicklung, sondern wird an anderer Stelle bereitgestellt. Bei den verarbeiteten Daten handelt es sich um Statusinformationen der Router in Form von SNMP-Daten sowie um gesampelte Netflow-Daten, die als Verbindungsinformationen auf den Routern gemessen werden. Diese Rohdaten werden maximal sieben Tage gespeichert und danach gelöscht. Sie dienen als Datenbasis für eine Analyse im Angriffsfall. Ein Monitoring von Inhalten der Kommunikation erfolgt zu keinem Zeitpunkt.

Die Arbeitsschritte, die als Unterstützung der darauf aufbauenden Geschäftsprozesse entwickelt wurden, gliedern sich in Messung, Erkennung, Alarmierung, Analyse und Aktion. In der Erkennungskomponente nimmt DFN-NeMo die notwendigen Daten entgegen, verarbeitet sie vor und gleicht sie mit den Daten der Netzwerkmodellierung ab. Sobald bekannte statistische oder zeitabhängig zu erwartende Schwellwerte überschritten werden, erfolgt eine Alarmierung (Abb. 1). Es werden keine IP-Adressen beobachtet, sondern die Auswertung erfolgt lediglich aus gewonnenen Kennzahlen aus den Rohdaten wie z. B. UDP-Paketraten, Volumendaten über TCP oder Paketraten von Verbindungen mit gesetztem TCP-SYN-Flag.

Alarmierungen erfolgen aus unterschiedlichen Gründen und werden durch die Erkennung von Überlastsituationen entweder am Punkt der Messung oder an entfernteren Orten der Netztopologie erkannt. Es können statistische Schwellwerte überschritten werden, Abweichungen von trainierten Kennzahlen auftreten, das Verkehrsverhalten kann von gelernten Modellen abweichen und auch eine extreme Überlast oder ein Ausfall des Messsystems selbst kann zu einer Alarmierung führen. Eine Übersichtskarte zeigt grob die Situation im Netz für einen ausgewählten Zeitraum an (Abb. 2).

DFN-NeMo liefert mit der Alarmierung eine Reihe notwendiger Informationen zur Planung und Durchführung einer zeitnahen Re-

Abb. 2: Netzwerk-Topologiekarte: Schematische Darstellung des X-WiN-Backbones. Die Strichbreite kennzeichnet die Paketrate, die Farben geben die Anzahl der Alarme in den letzten Stunden an.

aktion. Diese Informationen ermöglichen eine sachgerechte Bewertung der Alarme. Die Alarme können mit anderen Alarmen korreliert werden und es kann eine erste Einschätzung des Schadpotentials vorgenommen werden. Es gibt die Möglichkeit, Angriffe durch die Topologie des X-WiN zurückzuverfolgen. Die entwickelten Werkzeuge, die auch Funktionen wie Reporting, Dokumentationen und ggf. Archivierungen enthalten, bieten die Möglichkeit, auch den Anfragen und Hinweisen von Anwendern im X-WiN oder anderen CERTs nachzugehen.

3. Netzwerkanalyse NEA

Im Rahmen des DDoS-Projekts wurde eine weitere Entwicklung unter dem Namen Netzwerkanalyse (NEA) angestoßen. Diese soll zur Darstellung und Recherche der Kommunikationsbeziehungen zwischen DFN-Anwendern und externen Netzen bzw. Autonomen Systemen (AS) sowie zwischen DFN-Anwendern untereinander dienen. Hierbei stehen nicht einzelne Verbindungen im Fokus, sondern die Volumenmessungen der Verkehrsströme zwischen den Standorten, was auch dem Gedanken des Datenschutzes Rechnung tragen soll. Ziel von NEA ist die Unterstützung der Verkehrsplanung innerhalb des X-WiNs als auch zu den externen Kommunikationspartnern.

Eine Rückverfolgung einzelner Kommunikationsbeziehungen oder gar ein Zugriff auf die Rohdaten ist innerhalb von NEA nicht möglich. Abb. 3 gibt einen Überblick über die Struktur von DFN-NeMo und NEA.

Eingabedaten für NEA sind die bereits innerhalb von DFN-NeMo genutzten Netflow-Daten sowie zusätzlich BGP-Daten der Router und aktuelle Daten der Netztopologie.

Wie auch in der DDoS-Anwendung werden die darzustellenden Daten anhand von Objekten gespeichert und visualisiert. Wegen der unterschiedlichen Zielsetzung werden hier jedoch ausschließlich Autonome Systeme modelliert. Diese sind in der Lage, sowohl die AS interner DFN-Anwender als auch die AS externer Organisationen abzubilden. Im Rahmen der Messung von NEA kann das in einem Netflow enthaltene Quell- oder Ziel-AS und auch jedes AS, das auf dem BGP-Pfad dazwischenliegt, erreicht werden. Somit sind auch alle Peering-Partner modellierbar.

Interne DFN-Anwender, die über ein privates oder öffentliches AS verfügen, sowie die Peering-Partner des DFN-Vereins werden hierbei automatisch anhand der aktuellen Netzwerkdokumentation modelliert. Alle weiteren Objekte müssen manuell angelegt werden und können vom Zeitpunkt des Modellierens an betrachtet werden. Eine Nachberechnung von Verkehrsströmen vor dem Zeitpunkt der Modellierung ist nicht möglich.

Bisher wurden knapp 700 Objekte automatisch bzw. manuell angelegt. NEA befindet sich zurzeit noch in der Entwicklung. Ähnlich wie bei der DDoS-Anwendung werden die berechneten Kenngrößen in Zeitscheiben gespeichert. Für kurze Zeiträume bietet NEA eine Auflösung von 5 Minuten an. Länger zurückliegende Daten werden konfigurierbar ausgedünnt. Eine Echtzeitfähigkeit ist für NEA nicht erforderlich, dementsprechend stellt eine größere oder schwankende Latenz kein Problem dar.

4. Datenschutzaspekte

Es ist selbstverständlich, dass die Einhaltung des Datenschutzes bei der Arbeit mit den benötigten Daten höchste Priorität hat. Deshalb haben schon im Vorfeld Gespräche mit Juristen stattgefunden und es wurde bereits während der Konzeptionsphase auf datenschutzrechtliche Randbedingungen geachtet. Unstrittig ist, dass der DFN-Verein sein eigenes Netz zum Zwecke der Störungserkennung nach TKG Telekommunikationsgesetz § 100 Abs. 1 überwachen darf.

Bei den verwendeten Daten in DFN-NeMo handelt es sich um Verbindungsdaten, die IP-Adressen und Ports von Quelle und Ziel, nicht jedoch Paketinhalte enthalten. Diese werden nach 7 Tagen gelöscht. Darüber hinaus kann bei der Verarbeitung in DFN-NeMo nur in den Arbeitsschritten zur Angriffsanalyse und Angriffsabwehr darauf zugegriffen werden, sodass im Normalzustand kein manueller Zugriff auf diese Daten erfolgt. Bei den gewonnenen Kennzahlen aus den Netflows, die aktuell 90 Tage aufgehoben werden, erfolgt keine Speicherung der IP-Adressen. Die Volumendaten der Router in Form der SNMP-Daten enthalten ebenfalls keine IP-Adressen und auch die Modelldaten des Netzes sind nicht datenschutzrelevant. Noch in der Entwicklung sind im Zusammenhang mit den geplanten Arbeitsabläufen genaue Anweisungen an die Analysten und eine sorgfältige Berichts- und Dokumentationsform der Systemnutzung.

5. Ausblick

DFN-NeMo hat sich bereits in der Pilotphase als ein sehr hilfreiches Werkzeug erwiesen. Es wird zurzeit in die internen Betriebsprozesse der DFN-Geschäftsstelle integriert. Für einen Einsatz unter aktiver Einbeziehung aller Anwender sind zuvor jedoch noch Rahmenbedingungen zu klären. Im produktiven Einsatz wird unter anderem die Weitergabe von Informationen an die Anwender erforderlich sein. Hier ist ein äußerst sorgfältiges Vorgehen, gerade auch bezogen auf Haftungsfragen, geboten, was eine Anpassung der Dienstvereinbarung DFNInternet erforderlich machen wird.

Derzeit besteht keine Möglichkeit, dass ein Anwender sein eigenes Netz über DFN-NeMo überwachen kann, da es in der Anwendung keine Trennung der Daten entsprechend einer Mandantenfähigkeit gibt. Somit sind auch keine auf bestimmte Netzbereiche eingeschränkte Sichten möglich. Langfristig könnte die Entwicklung jedoch in einen neuen DFN-Dienst mit separater Dienstvereinbarung und einem Vertrag zur Auftragsdatenverarbeitung einfließen.

Darüber hinaus ist der Einsatz von DFN-NeMo auch im GÉANT-Umfeld denkbar. Erste Kontakte wurden hierzu bereits aufgenommen und stießen auf großes Interesse. ◆

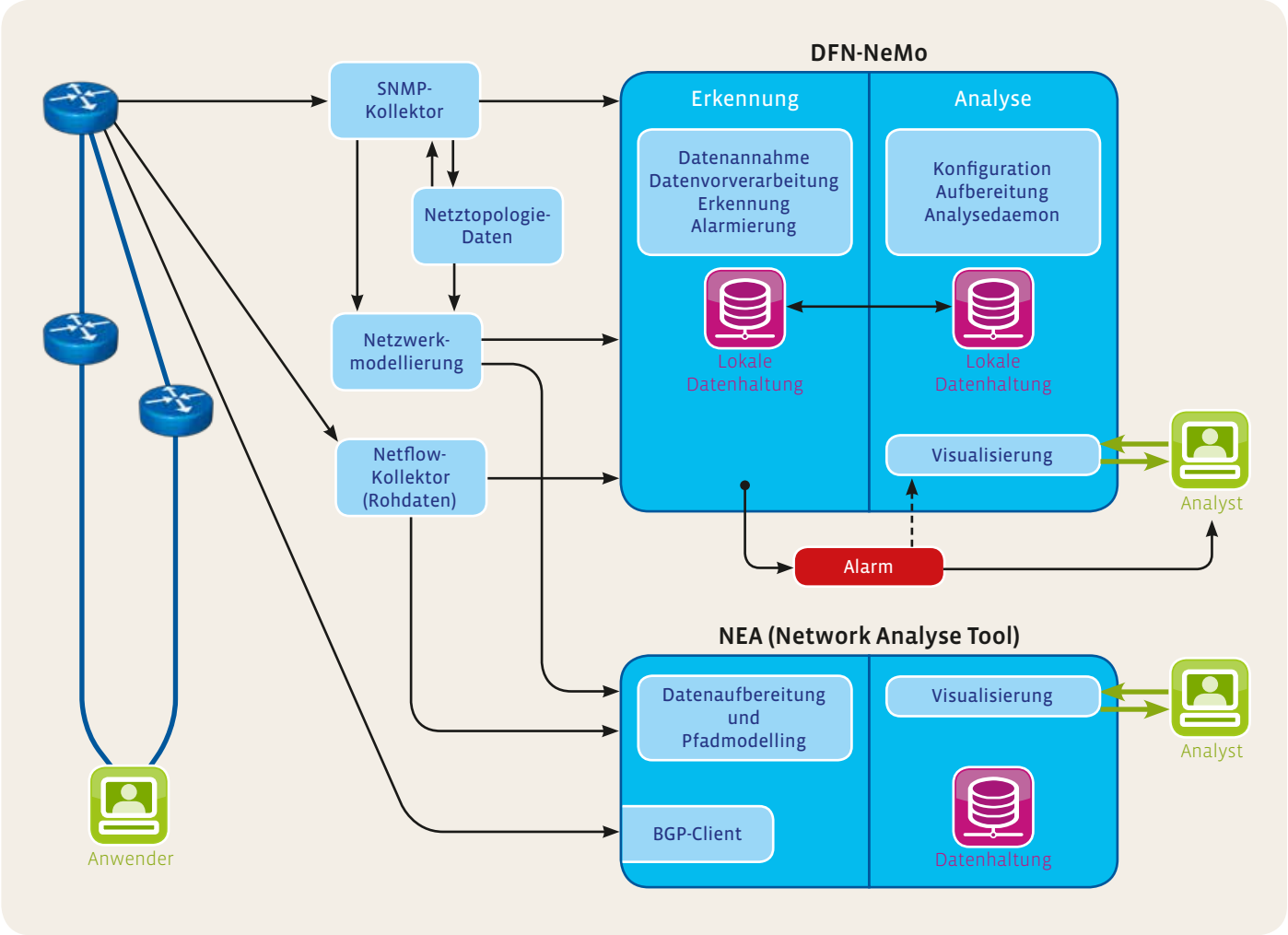


Abb. 3: Strukturbild von DFN-NeMo und NEA

Kein X für ein U – mehr Sicherheit fürs Domain Name System!

Eines der häufigsten Ziele für Angriffe auf das Internet ist heute das Domain Name System (DNS). Angriffe auf das DNS treffen Kommunikationsinfrastrukturen an ihrer empfindlichsten Stelle, nämlich im inneren Kern. Attraktiv wird das DNS für Angriffe vor allem dadurch, dass es dezentral organisiert ist.

Text: **Henry Kluge** (DFN-Verein)

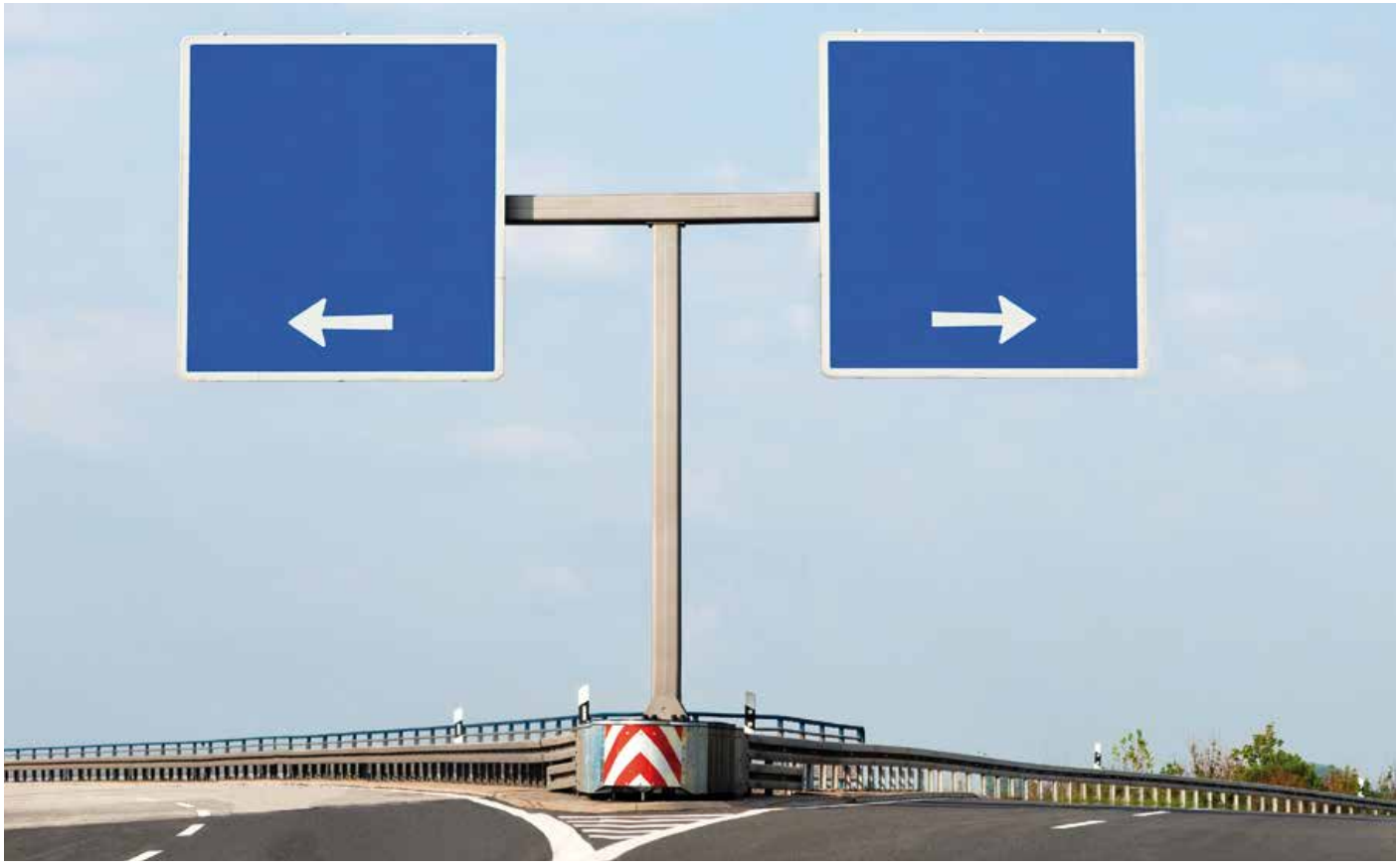


Foto © Sandor Jackal / fotolia

Einleitung

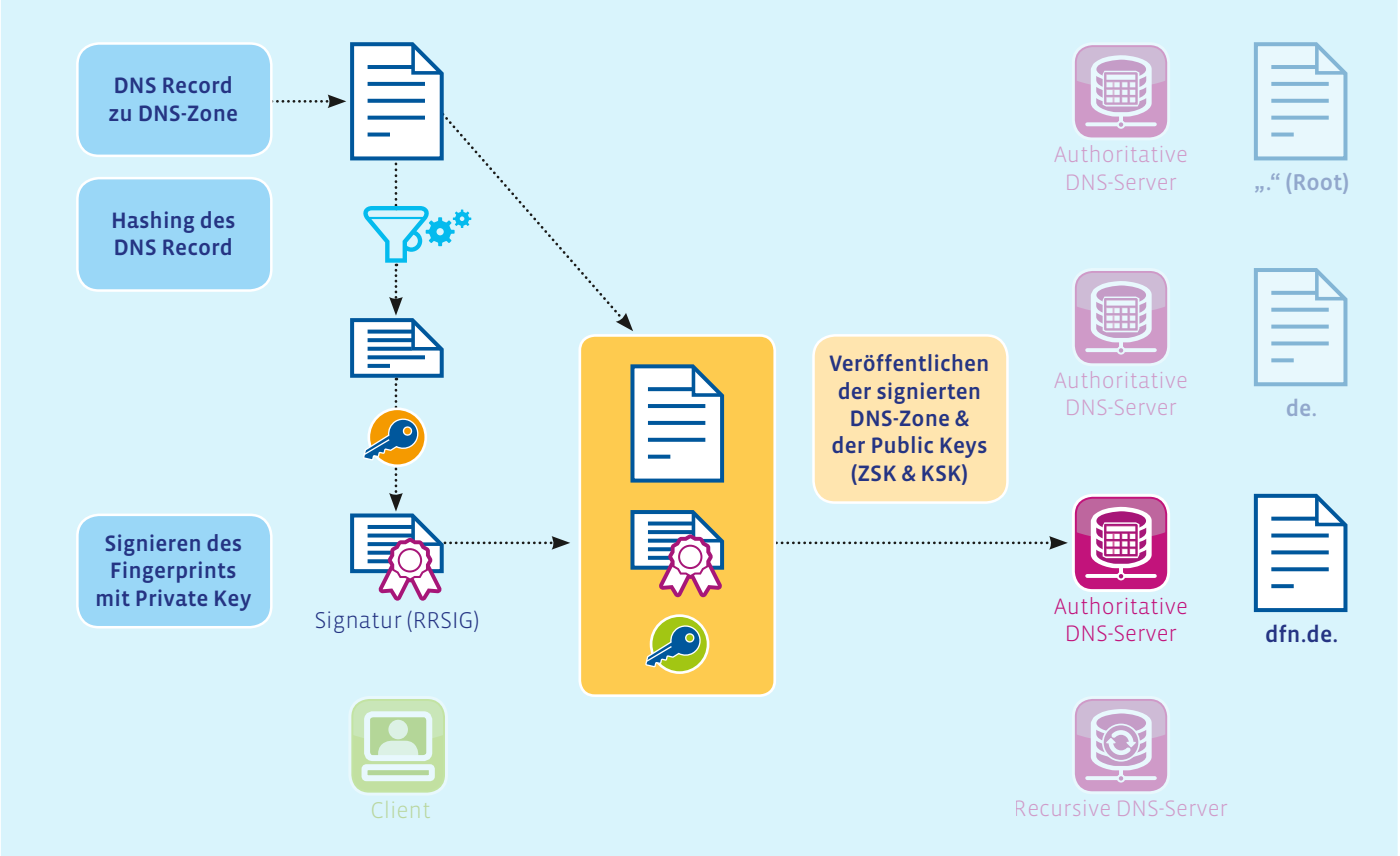
Jede Einrichtung im Deutschen Forschungsnetz verwaltet ihrem Namensraum eigenverantwortlich und muss ihn gegen Angriffe schützen. Besonders sensibel ist das DNS vor allem, weil eine Manipulation des ‚Adressbuchs' DNS nicht nur die angegriffene Einrichtung, sondern potentiell auch andere Anwender im Netz schädigen kann. Unterlassungen bei Schutz und Pflege des DNS sind also potentiell schädlich für die Gemeinschaft. Wenngleich heute eine Reihe von Werkzeugen für DNS-Security (DNSSEC) bereitsteht, stellt DNSSEC für die Einrichtungen nach wie vor eine betriebliche Herausforderung dar.

Ob beim Aufrufen von Webseiten oder dem Versenden von E-Mails, immer ist eine Umsetzung von logischen, durch Menschen lesbaren Namen in für den Transport der Datenpakete genutzte Adressen notwendig. Zum Beispiel muss der im Web-Browser eingegebene Name „www.dfn.de" vom DNS-Server in eine IP-Adresse übersetzt werden, hier die „194.95.248.240" als IPv4 bzw. die „2001:638:d:c101:acdc:1979:3:1008" als IPv6. Erst aufgelöst können Datenströme von Netzwerkkomponenten wie Routern verarbeitet werden. Hierzu wird eine Infrastruktur genutzt, die im Prinzip eine über das ganze Internet verteilte, hierarchische Datenbank darstellt und über standardisierte Schnittstellen und Netzwerkprotokolle abfragbar ist.

Seit seiner Einführung im Jahr 1983 wurde das DNS-Protokoll ständig optimiert und um neue Funktionen erweitert [DNS RFC]. Gerade in den letzten Jahren ist zu beobachten, dass immer mehr sicherheitskritische Informationen im DNS verfügbar gemacht werden bzw. dass sich andere Protokolle und Verfahren mit einem Sicherheitsfokus zumindest teilweise auf DNS-Funktionen abstützen (z. B. DANE/TLSA, SSHFP). Hier kommt jedoch eine Schwäche des „Ur"-DNS zum Vorschein: Bei der Definition der ersten RFC wurden keine Maßnahmen zur Sicherung der gespeicherten und übertragenen Daten vorgesehen. Aus damaliger Sicht ist die Wahl eines „Keep It Simple"-Ansatzes zwar nachvollziehbar, allerdings stellt eine derartige Offenheit bei der heutigen Bedrohungslage im Internet ein Problem dar. Typische Angriffsszenarien in diesem Zusammenhang sind „DNS-Spoofing" oder „Cache-Poisoning", bei denen gefälschte oder zusätzliche Informationen den DNS-Clients oder -Servern untergeschoben werden. Dadurch ist es zum Beispiel möglich, den Datenverkehr vom Nutzer unbemerkt auf manipulierte Webseiten umzulenken und Schadsoftware auf die Clients zu laden.

Schon in den 1990er-Jahren wurden erste Anstrengungen unternommen, die so-

Abbildung 1: Signieren der DNS Resource Records



genannten „Securitiy Extensions“ für das DNS-Protokoll (DNSSEC) zu definieren, um den Angriffen auf das Protokoll zu begegnen. Jedoch stellte sich schnell heraus, dass dieser erste Ansatz nicht implementierbar war. Somit bedurfte es einer kompletten Überarbeitung der Standards, bevor im Jahr 2005 eine in diversen RFCs beschriebene grundsätzliche DNSSEC-Architektur verfügbar war. Die mit diesen Erweiterungen verbundene Erhöhung der Komplexität und der Einsatz von anderen Verfahren, die einen Teil der Angriffe abwehren konnten, verzögerten jedoch eine Einführung von DNSSEC auf breiter Front. Mittlerweile sind allerdings sowohl handhabbare DNSSEC-Softwareimplementierungen als auch umfassende Erfahrungen aus der täglichen Praxis verfügbar, sodass einer Nutzung von DNSSEC prinzipiell nichts entgegensteht. Wo aber liegen nun die Herausforderungen, die eine Einführung dieses Verfahrens erschweren? Bevor auf diese Fragestellung eingegangen wird, ist ein kurzer Abriss der grundsätzlichen Funktionalitäten von DNSSEC hilfreich.

Funktion des DNSSEC-Protokolls

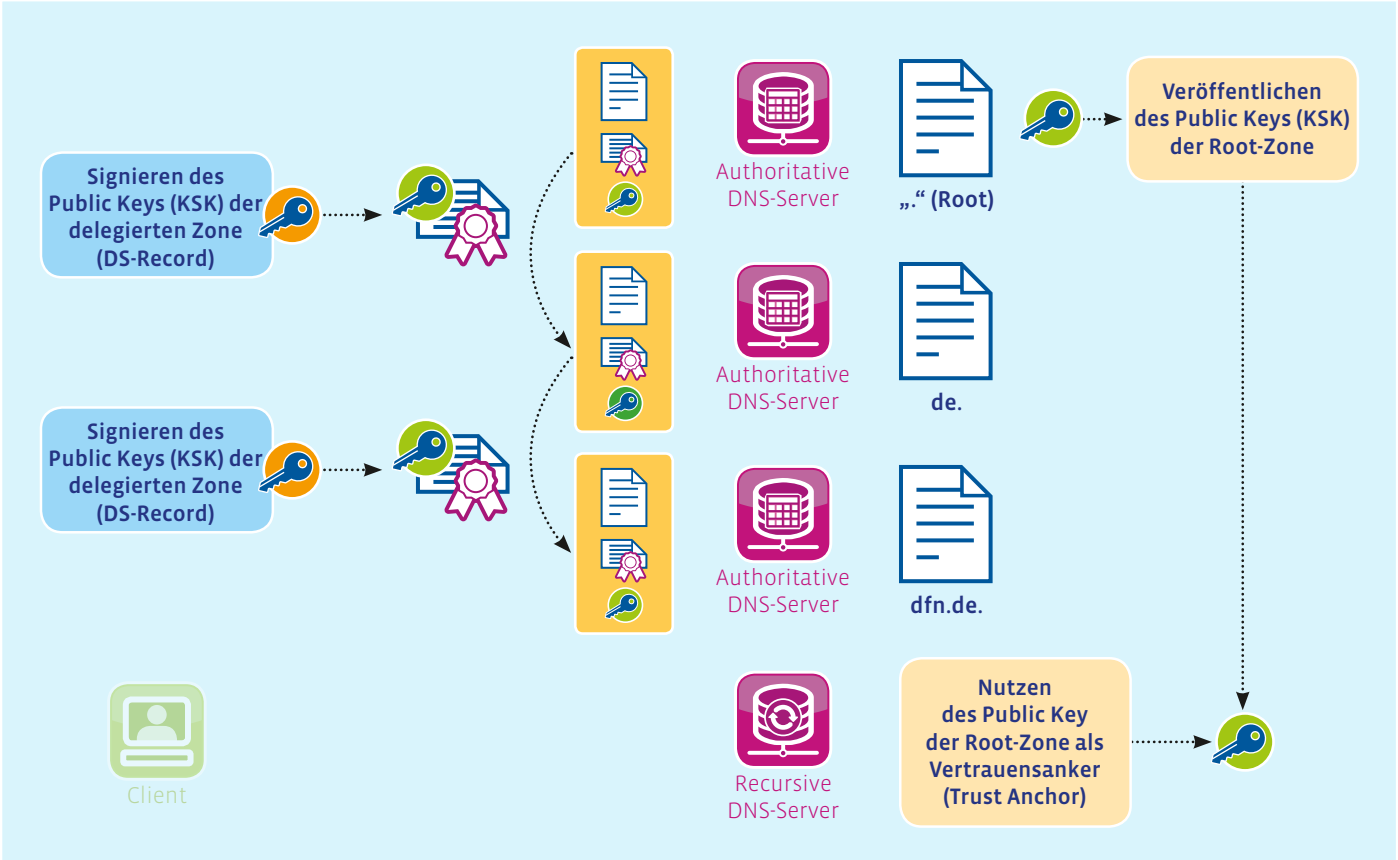
Im DNS werden öffentliche Informationen verarbeitet. Deshalb liegt beim DNSSEC-Protokoll der Fokus nicht auf dem Schutz der Vertraulichkeit, sondern auf der Sicherstellung der Authentizität und Integrität der abgefragten Daten. Das heißt, auch wenn der Begriff „Security“ etwas anderes suggeriert, dass die zu schützenden Datensätze (Resource Records/RR) „nur“ signiert und nicht verschlüsselt werden. Hierbei werden bewährte kryptographische Verfahren wie RSA oder SHA-1/2 genutzt.

In Abbildung 1 ist das Signieren einer DNS-Zone schematisch dargestellt. Hierbei wird zuerst von jedem Resource Record (RR) ein Hash erzeugt, der im Anschluss mit dem privaten Zone Signing Key (ZSK) signiert wird. Die Resource Records werden zusammen mit den zugehörigen Signaturen (RRSIG-Record) und dem öffentlichen Teil des ZSK auf dem autoritativen Server veröffentlicht. Die Gültigkeitsdauer der Signaturen (typischerweise 30 Tage) und die Angaben zum verwendeten Algorithmus werden hier ebenfalls gespeichert.

Mit diesen Informationen ist es prinzipiell möglich, die Gültigkeit eines übermittelten DNS-Eintrages zu überprüfen. Hierfür benötigt man jedoch ein übergreifendes Vertrauensmodell, um nicht für jeden einzelnen DNS-Server den Vertrauensstatus separat prüfen und lokal speichern zu müssen.

Zur Umsetzung dieser Vertrauenskette (Chain of Trust) wird, wie in Abbildung 2

Abbildung 2: Chain of Trust



dargestellt, die bereits vorhandene Hierarchie des Domain Name Systems genutzt. Die Vertrauensbeziehung setzt auf dem Prinzip der Delegation von Zonen auf und ergänzt dieses um die Verknüpfung mit den sogenannten Key Signing Keys (KSK) der delegierten Zone. Somit benötigt ein validierender rekursiver DNS-Server (Resolver) im Standardfall nur den öffentlichen Schlüssel der obersten Ebene (Public KSK der Root-Zone).

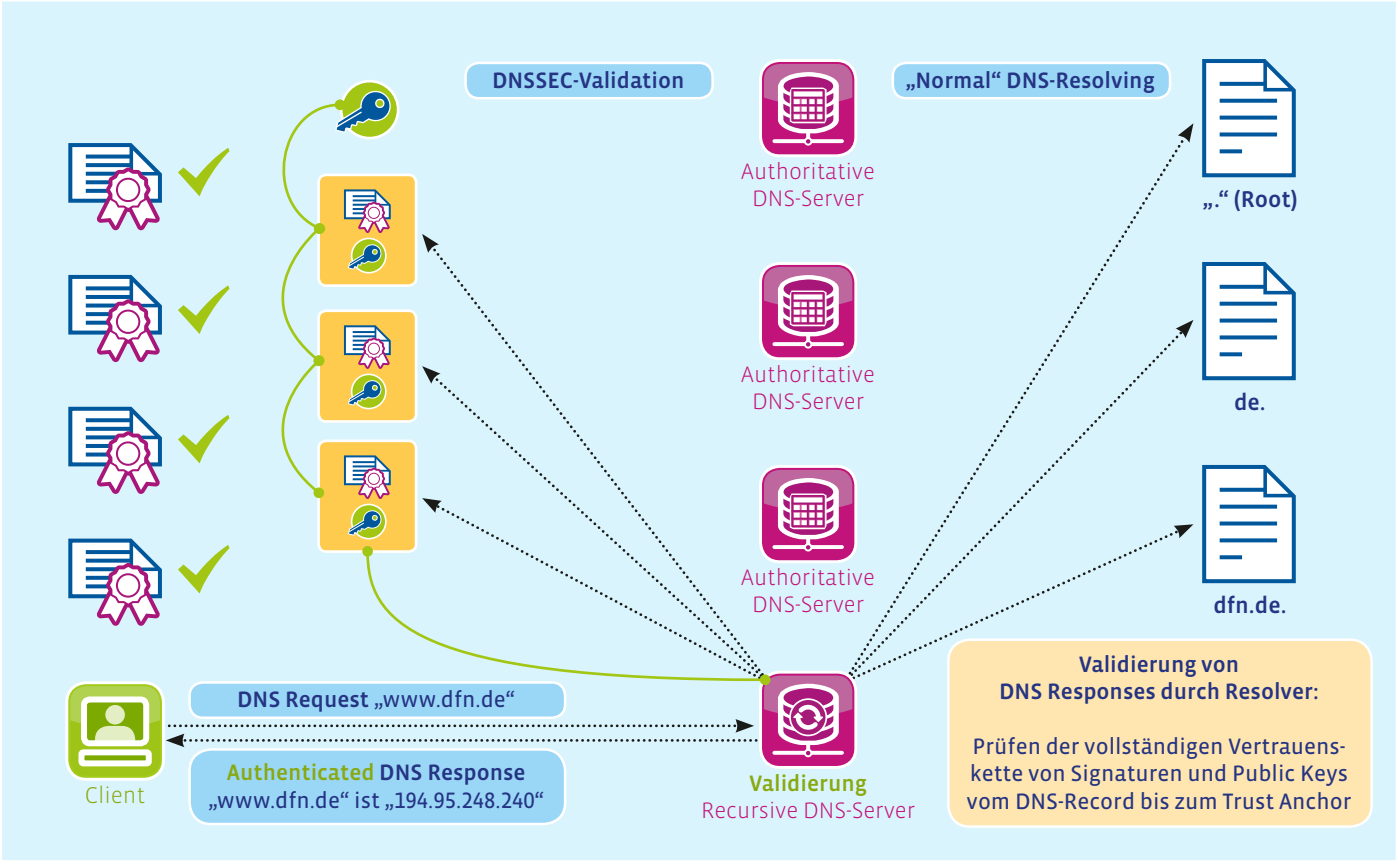
Die Validierung der DNS-Antwortpakete stellt nun sicher, dass die übermittelten Resource Records vom zuständigen DNS-Server stammen und auf dem Transportweg nicht manipuliert wurden (siehe Abbildung 3). Hierzu wird vom Resolver die Übermittlung der Signaturen und Public Keys per DO-Flag (DNSSEC OK) angefordert. Auf Grundlage dieser Informationen wird geprüft, ob eine Vertrauenskette aus Public Keys und deren Signaturen bis zum Vertrauensanker herstellbar ist. Ist dies der Fall, wird die Antwort per AD-Flag (Authenticated Data) als geprüft gekennzeichnet. Schlägt diese Prüfung fehl, wird dem anfragenden Client eine Fehlermeldung (SERVFAIL) zurückgesendet.

Herausforderung Technik & Funktion

Bei der Einführung von DNSSEC sind im ersten Schritt diverse technische bzw. funktionale Rahmenbedingungen zu klären. Diese haben oftmals auch Auswirkungen auf sicherheitsspezifische Aspekte, insbesondere auf die Verfügbarkeit des DNS-Services. In den folgenden Ausführungen wird der Fokus auf eine Auswahl von Herausforderungen aus diesem Bereich gelegt. Durch die Einbindung der Signaturen werden DNSSEC-Antwortpakete deutlich größer als die ursprünglich als Normalwert üblichen maximal 512 Byte. Aus diesem Grund wurde die Einführung eines Extension Mechanismus für DNS (EDNS0) notwendig, der u. a. die UDP-Paketlängenproblematik auf Protokollebene löste. Leider gab und gibt es noch immer Hersteller oder Administratoren von Netzwerkkomponenten, die eine Übertragung von größeren DNS-UDP-Paketen oder DNS-TCP-Paketen blockieren. Hierdurch kann es zu schwer nachvollziehbaren Fehlersituationen kommen, die abhängig von Typ und Größe der DNS-Abfrage sind. Deshalb ist es dringend geboten, Firewalls, Loadbalancer und andere Middle-Boxes, die sich in eigener Hoheit befinden, auf diese Funktionalität zu prüfen und gegebenenfalls die Konfiguration anzupassen.

Eine weitere Besonderheit, die DNSSEC mit sich bringt, ist die Notwendigkeit, auch das Nichtvorhandensein von Domainnamen authentisch nachzuweisen. Hierfür

Abbildung 3: DNSSEC-Validierung



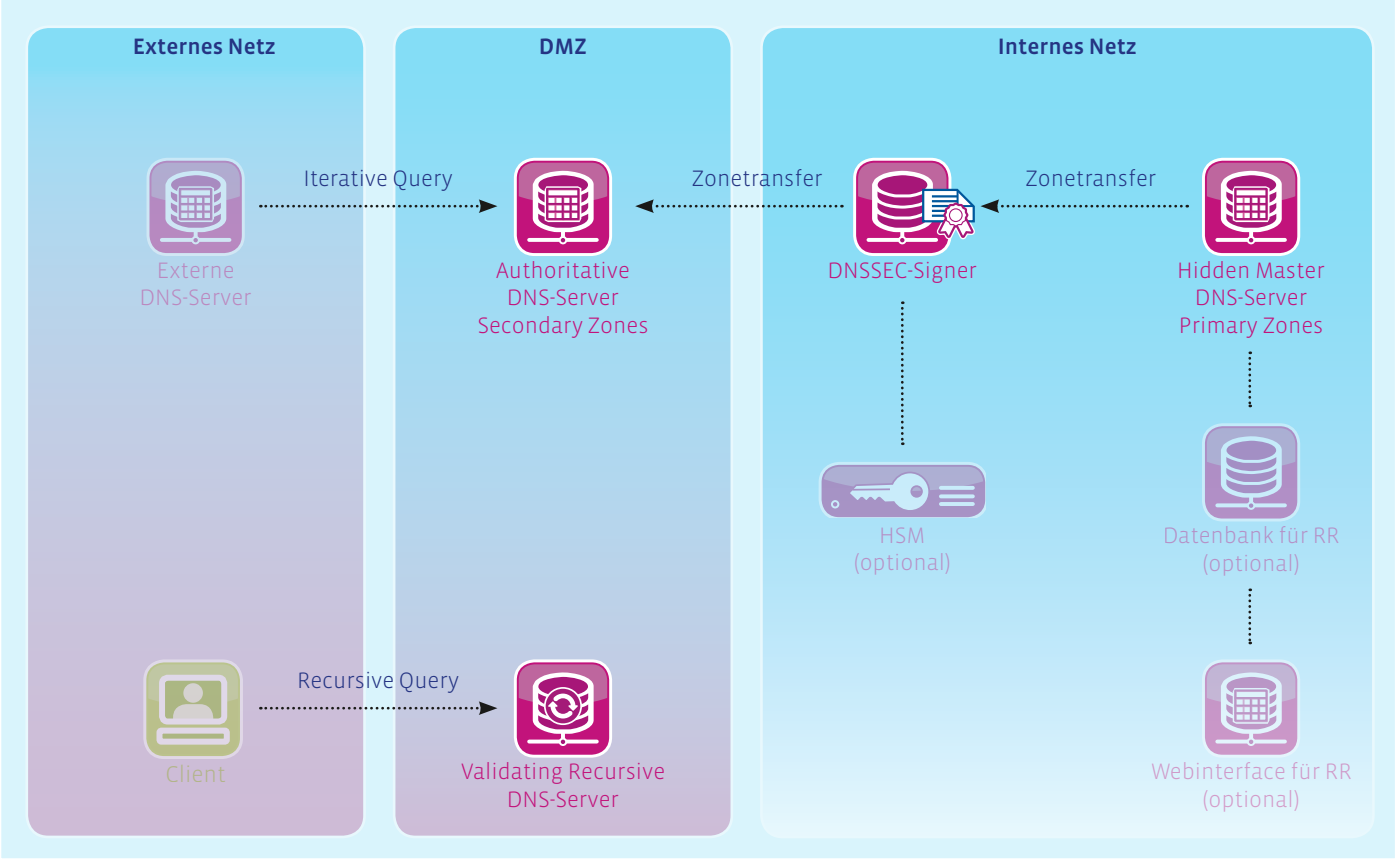


Abbildung 4: Beispiel Deployment DNSSEC

wurde initial der Resource Record NSEC (Next SECure) eingeführt, der über einen Verweis auf den nächsten gültigen Eintrag im Zonenfile eine ringförmige Verkettung herstellt und somit die „Lücken" zwischen den Einträgen füllt. Somit kann an einen anfragenden Client eine signierte NXDOMAIN- bzw. NODATA-Antwort gesendet werden. Nachteil dieser Methode ist, dass die NSEC-Einträge in Klartext gespeichert vorliegen und somit ein sehr einfaches Auslesen der kompletten Domaininhalte möglich ist (sog. Zone-Walking). Als Abhilfe wurde der RR-Typ NSEC3 definiert, bei dem die Informationen mittels eines Hashs geschützt werden. Dieses hat allerdings den Nachteil, dass für die Erstellung und Validierung dieser Einträge ein wesentlich höherer Rechenaufwand nötig ist. Je nach Nutzungszweck der Domain und Schutzbedarf der einzelnen Domaininformationen (Hostnamen, Service-Records etc.) muss hier entschieden werden, ob das Risiko eines potentiellen Zone-Walks tragbar ist.

Eine weitere Risikobewertung ist für den Umgang mit der „letzten Meile" der DNS-Kommunikation notwendig. Da die DNS-Clients der meist genutzten Betriebssysteme standardmäßig keine DNSSEC-Validierung unterstützen, wird diese Funktion von einem separaten DNS-Server erbracht. Dieser kann sich in eigener administrativer Hoheit befinden oder z. B. vom Netzprovider angeboten werden. Mit dieser Betriebsweise ist verbunden, dass auf der Netzwerkstrecke zwischen Client und Server potentiell eine Manipulation der DNS-Antwortpakete möglich ist. Bei besonders sicherheitskritischen Systemen und Anwendungsservern ist es deshalb dringend zu empfehlen, die Validierung der DNSSEC-Daten lokal vorzunehmen. Hierfür sind mittlerweile Implementierungen wie „Unbound" von NLnet Labs verfügbar. Betriebssysteme wie Windows Server 2012 unterstützen die DNSSEC-Validierung direkt (siehe auch [DNSSEC Resolver]).

Zwar ist der Schutz vor Angriffen kein spezifisches DNSSEC-Thema, dennoch ist auch hierauf besonderes Augenmerk zu richten, da es sich bei DNS-Servern um kritische Infrastrukturkomponenten handelt. Aus diesem Grund ist es empfehlenswert, eine eventuell bereits vorhandene Installation unter diesem Aspekt zu überprüfen. Schwerpunkt sollte auf einer klaren Definition der einzelnen Funktionen und wenn möglich deren Trennung liegen. Somit kann man z. B. die eigentliche Pflege der Zonen- bzw. Domaindaten auf einen Hidden Master Server konzentrieren und diesen in einer Sicherheitszone platzieren, die eine nur sehr eingeschränkte Kommu-

nikation zulässt. Ebenso kann die Signatur der DNS-Daten auf einer separaten Serverinstanz erfolgen, die ebenfalls nicht direkt von externen DNS-Systemen erreichbar ist. Für einen solchen DNSSEC-Signer existieren sowohl kommerzielle Produkte (z. B. Infoblox, BlueCat) als auch Open-Source-Lösungen (z. B. ISC Bind mit Inline Signing oder OpenDNSSEC).

Auch die Aufteilung der Authoritativen- und der Resolver-Funktion auf der Serverseite bekommt mit DNSSEC eine besondere Bedeutung. Resultierend aus dem DNSSEC-Vertrauensmodell, ist es nicht erlaubt, dass eine DNSSEC-Validierung eines Resource Records auf einer Serverinstanz erfolgt, die autoritativ für diesen Eintrag zuständig ist. Somit ist hier eine Implementierung dieser beiden Funktionen auf unterschiedliche Serverinstanzen notwendig, die aber auch aus anderen Gründen Sinn ergibt. Zum Beispiel kann der Zugriff auf die einzelnen Systeme bzw. Funktionen wesentlich zielgerichteter gesteuert werden. Wobei im speziellen Fall insbesondere die Einschränkung der Erreichbarkeit des rekursiven Resolvers relevant ist. Ein Schutz vor Angriffen wie z. B. Amplification-Attacks, kann nun auf einem vorgelagerten Perimeter (Paketfilter oder Firewall) erfolgen und muss nicht direkt auf dem Server durch z. B. Views definiert werden (siehe Abbildung 4).

Herausforderung Betrieb & Prozesse

Neben den rein technischen und funktionalen Aspekten bei der Einführung von DNSSEC treten die betrieblichen und organisatorischen Anforderungen oftmals in den Hintergrund. Die frühzeitige Auseinandersetzung mit diesen Themen und die Anpassung bzw. Definition von Prozessen sind allerdings essentiell für einen erfolgreichen DNSSEC-Betrieb. Sicherlich können die konkreten Maßnahmen je nach Umgebung spezifisch und durchaus unterschiedlich sein, jedoch gibt es einige allgemeingültige Eckpunkte, die hier beachtet werden sollten.

Mit der Nutzung und Verarbeitung von kryptographischem Material (Public/Private Keys und Hashes für Signatur oder Resource Records) nehmen die notwendigen Prozesse und Prüfaufgaben einen mit der „klassischen" PKI vergleichbaren Stellenwert ein. Dies gilt insbesondere, wenn neben der Namensauflösung weitere Funktionen über DNS implementiert werden sollen, beispielsweise mittels DANE oder SSHFP. In diesen Fällen wird über DNS die Zugehörigkeit eines öffentlichen Schlüssels zu einer Entität garantiert, was exakt der Aufgabe einer CA bei der Ausstellung von X.509-Zertifikaten entspricht. Somit ist es insbesondere notwendig, dass Hinzufügen, Ändern und Löschen von Einträgen nachvollziehbar zu dokumentieren. Dazu gehört der Nachweis darüber, wer, was, wann und warum an Zonen- oder Konfigurationsdateien geändert hat. An dieser Stelle muss nicht alles neu erfunden werden, da im Regelfall etablierte PKI-Verfahren nachgenutzt werden können. Jedoch ist eine Adaption auf die spezifischen DNSSEC-Belange erforderlich.

Besonders das Management der für die Signatur verwendeten Schlüssel stellt einen zentralen und im DNS-Umfeld neuen Prozess dar. Hierbei ist zwischen dem regelmäßigen Schlüsselwechsel (Key-Rollover) für den Zone Signing Key (ZSK) und dem Key Signing Key (KSK) zu unterscheiden. Der Aufwand und die Komplexität beim ZSK-Key-Rollover sind vergleichsweise gering, da er nur lokale Auswirkungen hat und in den aktuellen Nameserver- bzw. DNSSEC-Implementierungen vollständig automatisierbar ist. Beim Wechsel des KSK hingegen ist in jedem Fall eine Interaktion mit der delegierenden Instanz notwendig, denn es muss eine abgesicherte Übertragung des neuen Public Keys bzw. dessen Hashs zur Erstellung des Delegation Signer Eintrages (DS) erfolgen. Die DNS-Registries und -Registrare bieten mittlerweile nahezu durchgehend Schnittstellen zur DS-Administration an [DNSSEC DS Support]. Ziel ist es, auch hier einen möglichst vollautomatischen Prozess zu etablieren, für den bereits die technischen Eckwerte standardisiert sind (siehe auch [Auto DS]).

Im Kontext der Schlüsselnutzung muss sichergestellt werden, dass der Schutzbedarf

Foto © Janine Wittig/photocase.de

der verwendeten Private Keys über ihren gesamten Lebenszyklus erfüllt wird. Hier können bereits etablierte Verfahren adaptiert werden und eventuell vorhandene Hard- und Software nachgenutzt werden. Besonders relevant ist in diesem Zusammenhang die sichere Erzeugung und Speicherung der Schlüssel. Je nach ermitteltem Schutzbedarf kann dies lokal auf dem DNS-Server umgesetzt werden oder auch den Einsatz eines Hardware Security Moduls (HSM) erfordern. Der Vorteil der Nutzung eines HSM liegt neben der Realisierbarkeit eines höheren Schutzniveaus auch in einer höheren Performance bei der Erzeugung von Schlüsseln und Signaturen. Bei der Entwicklung der OpenDNSSEC war und ist die Unterstützung von HSM über die PKCS#11-Schnittstelle ein integraler Bestandteil, sodass hier eine valide Basis unterstützter Produkte zur Auswahl steht [OpenDNSSEC HSM].

Das Monitoring der automatisierten Prozesse und deren Ergebnisse ist im Rahmen eines DNSSEC-Betriebs von außerordentlich hoher Bedeutung. Neben der Überwachung der relevanten Performanceparameter sollte auch die externe Sicht auf den Dienst berücksichtigt werden, d. h. regelmäßig geprüft werden, dass ausgewählte Resource Records über externe Resolver auflösbar und validierbar sind. Für diesen Zweck stehen z. B. unter [DNSSEC Tools] diverse Werkzeuge zur Verfügung, die für die konkrete Umgebung anpassbar sind. An diesem Beispiel wird deutlich, dass es wichtig ist, bereits vor der produktiven Nutzung von DNSSEC die genutzten Managementwerkzeuge anzupassen bzw. zu erweitern. Aber nicht nur die Arbeitsmittel müssen „DNSSEC-fit“ gemacht werden, sondern auch alle am IT-Betrieb beteiligten Mitarbeiter müssen mit den neuen Funktionen des Protokolls und den Möglichkeiten der Fehlersuche und -beseitigung vertraut gemacht werden.

Fazit

Nach einer durch verschiedenste Ursachen begründeten zähen Startphase für DNSSEC ist spätestens seit dem letzten Jahr eine weltweit sichtbare Zunahme an signierten Zonen zu verzeichnen. Dies hängt zum einen mit der immer besseren und stabileren Unterstützung durch Open-Source-Lösungen und kommerzielle Produkte zusammen, die die Administration erleichtern. Der Haupttreiber ist aber sicherlich der zunehmende Einsatz von DANE/TLSA im E-Mail-Umfeld, der eine Nutzung von DNSSEC zwingend erfordert. Da sich mit hoher Wahrscheinlichkeit weitere ähnliche Verfahren und Protokolle auf DNSSEC abstützen werden, wird es für Betreiber von DNS-Infrastruktur immer wichtiger, sich mit diesem Thema auseinanderzusetzen. Hierbei ist neben den rein funktionalen und technischen Fragestellungen ein mindestens ebenso großer Wert auf die Anpassung und ggf. Definition von Betriebsprozessen und -werkzeugen zu legen.

Am Ende gilt aber wie immer: „It Has To Work!“ [RFC Network Truth] ◆

Ausblick

Zurzeit konsolidiert der DFN-Verein die von ihm betriebene DNS-Infrastruktur. In diesem Rahmen erfolgt auch eine Evaluierung einer konkreten DNSSEC-Umsetzung für das X-WIN mit folgenden Schwerpunkten:

- Evaluierung der Trennung der Funktionen DNS-Service und Signatur-Erzeugung
- Auswahl der SW-Plattform für DNSSEC (bind, PowerDNS, OpenDNSSEC ...)
- DNSSEC-Signatur für die Domain dfn.de
- Unterstützung von DNSSEC für alle Secondary-Zonen
- Anpassung der Betriebsprozesse
- Definition der Außenschnittstellen für DS-Austausch
- Integration von DNSSEC-Validierung in bestehende Systeme und Prozesse

Links & Quellen

[DNS RFC] DNS related RFCs – http://www.statdns.com/rfc/

[DNSSEC Resolver] – Deploying DNSSEC, Validation on recursive caching name servers – https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_Deploying_DNSSEC_v20.pdf

[DNSSEC DS Support] Registrars that support end user DNSSEC management – https://www.icann.org/resources/pages/deployment-2012-02-25-en

[Auto DS] RFC 7344-Automating DNSSEC Delegation Trust Maintenance – https://tools.ietf.org/html/rfc7344

[DNSSEC Tools] – Internet Society, DNSSEC Tools – http://www.internetsociety.org/deploy360/dnssec/tools/

[OpenDNSSEC HSM] – List of HSM Vendors – https://wiki.opendnssec.org/display/DOCREF/HSM

[RFC Network Truth] – RFC 1925 The Twelve Networking Truths – https://tools.ietf.org/html/rfc1925

DFNFernsprechen: Kurznachrichten über SMS-Gateway versenden

Durch eine europaweite Ausschreibung des DFN-Fernsprechdienstes konnten dessen bestehende Dienstmodule optimiert und neue Dienstmodule integriert werden. Dazu gehört unter anderem das SMS-Gateway. Kernfunktion dieses Dienstes ist die Versendung von E-Mail-Textnachrichten als SMS über Mobilfunknetze an einen Mobilfunkempfänger.

Text: **Christian Meyer** (DFN-Verein)

Neuer Dienst für DFNFernsprechen

Viele Einrichtungen nutzen Textkurznachrichten in Form von SMS-Nachrichten für die Abwicklung ihrer Arbeitsprozesse. An erster Stelle sind hier Bibliotheken zu nennen, die Nutzer über fällige Medien oder abgelaufene Leihfristen informieren müssen. Auch im Campus-Management, also in verschiedenen Bereichen der Hochschulverwaltung und in unterschiedlichen Aufgabenfeldern der Administration des studentischen Ausbildungszyklus, wird durch die Integration alternativer Informationswege wie SMS-Kurznachrichten ein Mehrwert geschaffen, zum Beispiel können Studenten kurzfristig über Lehrplanänderungen, Raumänderungen oder über Unterrichtsmaterialien und Prüfungsergebnisse informiert werden. Auch die Sicherheit bei der Anmeldung an verschiedensten Nutzerportalen kann mit dem Einsatz von SMS-Nachrichten mittels Zwei-Faktor-Authentifizierung erhöht werden, indem das SMS-Gateway zur Übersendung von einmalig gültigen Passcodes verwendet wird. Nicht zuletzt ist der Einsatz von SMS-Benachrichtigungen auch in der IT-Überwachung ein Weg, um Reaktionszeiten der Administratoren und somit Ausfallzeiten essentieller IT-Systeme zu minimieren, etwa durch automatisierte Benachrichtigungen der zuständigen Rufbereitschaft über Systemalarme oder Havarien.

SMS per E-Mail versenden

Teilnehmende Einrichtungen können Nutzer per Mobilfunk-SMS erreichen, indem die gewünschte Textnachricht per E-Mail an das SMS-Gateway geschickt wird. Das SMS-Gateway nimmt SMTP-konforme E-Mails über eine zentrale E-Mail-Adresse entgegen. Zur Sicherstellung der Nutzungsberechtigung kann das SMS-Gateway anhand einer Positivliste von IP-Adressen sicherstellen, dass nur E-Mails von E-Mail-Servern weitergeleitet werden, die in dieser Liste verzeichnet sind. Im DNS konfigurierte SPF-Datensätze (Sender-Policy-Framework-Datensätze) können ebenso zur Festlegung der Nutzungsberechtigung und zur Verhinderung von Absenderfälschungen verwendet werden. Die Mobilfunkrufnummer des Empfängers einer SMS wird aus der Betreffzeile der E-Mail entnommen. Sollen mehrere Empfänger die gleiche Nachricht erhalten, kann die Betreffzeile mehrere mit Komma getrennte Zielrufnummern enthalten. Eine SMS kann maximal 160 Zeichen lang sein (durch die sogenannte GSM-7-bit-Kodierung), längere Nachrichten werden dann automatisch aufgeteilt. So können bis zu 612 Zeichen (aufgeteilt in 4 SMS-Nachrichten) übertragen werden. Das SMS-Gateway stellt empfangene, vorgabenkonforme E-Mails im SMS-Format über das Mobilfunknetz der Empfängerrufnummern zu, nimmt Quittungs- und Fehlermeldungen aus den Mobilfunknetzen entgegen und leitet diese Meldungen an den E-Mail-Absender zurück. Bei der Einrichtung des Dienstes wird festgelegt, welche Absenderadresse dem SMS-Empfänger angezeigt werden soll. Je eingerichteter E-Mail-Adresse kann dabei eine bis zu 11 Zeichen umfassende alphanumerische Identifizierung gewählt werden.

Sonderfunktionen

Der direkte Zugriff auf das SMS-Gateway ist auch ohne den Weg über eine E-Mail-Infrastruktur möglich. An erster Stelle steht dafür eine Programmierschnittstelle (API) zur Verfügung, die in schon bestehende Anwendungen und Programme integriert werden kann. Dieser API-Zugriff auf das SMS-Gateway erlaubt es, individuell angepasste und automatisierte Kurznachrichten direkt aus einem System einer Einrichtung zu versenden, zum Beispiel aus einem Monitoring-System für Infrastrukturkomponenten. Die technische Realisierung erfolgt primär über eine REST-Schnittstelle, es kann aber auch auf eine SOAP-API sowie eine FormPost-API zugegriffen werden. Zur Implementierung werden Software Development Kits (SDK) für eine Vielzahl von Programmierumgebungen bereitgestellt, um die Integration so einfach wie möglich zu gestalten.

Zur Adressierung eines großen Empfängerkreises mit personalisierten Textnachrichten bietet der Dienst SMS-Gateway auch die Möglichkeit, über ein Webinterface auf entsprechend vorbereitete Werkzeuge zuzugreifen. In wenigen intuitiven Arbeitsschritten kann eine aufbereitete Datei, in der alle Empfängerinformationen sowie der entsprechende Nachrichteninhalt abgelegt sind, über das System verarbeitet werden. Dafür können auch schon vorhandene Vorlagen genutzt werden. ◆

Kurzmeldungen

Prof. Dr. Hans-Joachim Bungartz als Vorstandsvorsitzender des DFN-Vereins bestätigt

Auf der 69. Mitgliederversammlung des DFN-Vereins, die am 03. Dezember 2014 im Wissenschaftszentrum in Bonn zusammenkam, wählten die Vertreter der Mitgliedseinrichtungen des DFN-Vereins einen neuen Verwaltungsrat. Das dreizehnköpfige Gremium trat unmittelbar nach Abschluss der Mitgliederversammlung zusammen und bestimmte aus seinen Reihen den Vorstand für den DFN-Verein für die bis 2017 dauernde XI. Wahlperiode. Hierbei wurde Prof. Dr. Hans-Joachim Bungartz (TU München) als Vorsitzender des DFN-Vereins bestätigt. Als Stellvertreter wurden Prof. Dr. Ulrike Gutheil (TU Berlin) sowie Dr. Rainer Bockholt (Universität Bonn) gewählt.

Dem Verwaltungsrat des DFN-Vereins gehören außer den drei Vorstandsmitgliedern auch Prof. Dr. Gabi Dreo Rodosek (Universität der Bundeswehr München), Prof. Dr. Rainer W. Gerling (Max-Planck-Gesellschaft), Dir. und Prof. Dr. Siegfried Hackel (Physikalisch-Technische Bundesanstalt), Dr.-Ing. habil. Carlos Härtel (General Electric), Prof. Dr.-Ing. Ulrich Lang (Universität zu Köln), Prof. Dr. Joachim Mnich (DESY), Prof. Dr. Peter Schirmbacher (Humboldt-Universität zu Berlin), Prof. Dr. Horst Stenzel (Fachhochschule Köln), Prof. Dr.-Ing. Ramin Yahyapour (Universität Göttingen und GWDG) sowie Dr. Harald Ziegler (Universität Jena) an.

Detaillierte Informationen über den Verwaltungsrat des DFN-Vereins finden sich unter: http://www.dfn.de/verein/vr/. ◆

Foto © joel-t/iStock.

Neue Teilnehmeranbindungen zum DFN

Der DFN-Verein hat im April 2015 ein Vergabeverfahren für die Teilnehmeranbindungen an das X-WiN gestartet. Mit den Teilnehmeranbindungen werden die Teilnehmer des Wissenschaftsnetzes, die nicht direkt an einem Kernnetzknoten lokalisiert sind, an das Wissenschaftsnetz angebunden.

Mit dem Vergabeverfahren verfolgt der DFN-Verein mehrere Zwecke: Zunächst soll der Handlungsspielraum geschaffen werden, der für zukünftige Steigerung der Leistung des Wissenschaftsnetzes benötigt wird. Darüber hinaus ist das Vergabeverfahren so gestaltet, dass ein Wettbewerb um die Erschließung von Standorten befördert wird, die heute noch nicht mit adäquaten Bandbreiten zu erreichen sind. Außerdem sollen die Voraussetzungen geschaffen werden, um die betrieblichen Prozesse für den gesamten Lifecycle von Teilnehmeranbindungen von der Beauftragung, der Inbetriebnahme, der Entstörung, dem Change-Management bis hin zur Außerbetriebnahme weiter zu verbessern. Das Verfahren wird in diesem Jahr abgeschlossen. ◆

SuperCore auf acht Standorte erweitert

Der bisherige SuperCore des X-WiN, der zwischen Hannover, Berlin, Frankfurt und Erlangen aufgespannt ist, wird bis voraussichtlich Ende des Jahres um vier weitere Standorte in Hamburg, Essen, Leipzig und Garching erweitert. Der bisherige SuperCore wird hierbei auf eine Kapazität von 200 Gbit/s aufgerüstet, die neu hinzukommenden Standorte verfügen zunächst über 100-Gbit/s-Anbindungen in den SuperCore. Der erweiterte SuperCore steigert nicht nur die Übertragungskapazitäten im Netz, sondern dient zugleich der Optimierung der Verkehrsflüsse im Wissenschaftsnetz. ◆

Online-Vortragsreihe zum Einsatz von Adobe Connect in der Lehre gestartet

Universitäten und andere öffentliche Einrichtungen, die Adobe Connect in Forschung, Lehre und Kooperation einsetzen, haben sich seit 2009 in einer DACH Nutzergruppe für Deutschland, Österreich und die Schweiz organisiert. Hier werden Erfahrungen ausgetauscht, Probleme diskutiert und gemeinsame Lösungen für den Einsatz der Software erarbeitet. Darüber hinaus tritt die DACH Nutzergruppe als Interessengemeinschaft gegenüber Adobe auf.

Die Arbeitsgruppe Didaktik in der DACH Nutzergruppe bietet seit März 2015 eine Online-Vortragsreihe zum Einsatz der Webkonferenz-Software Adobe Connect in der Hochschullehre an. Zweimal pro Monat stellen Teilnehmende der Nutzergruppe Themen wie z. B. Grundfunktionen, Einsatzszenarien und spezielle Features vor. Ein Vortrag dauert jeweils eine halbe Stunde.

Die Vortragsreihe richtet sich an alle, die am Einsatz von Adobe Connect in der Hochschullehre interessiert sind. Angesprochen sind sowohl Einsteiger als auch Fortgeschrittene. Eine Anmeldung ist nicht notwendig.

Die Vorträge finden in einem Online-Meetingraum des DFN-Vereins statt: https://webconf.vc.dfn.de/dachadobeconnect/. Eine Viertelstunde vor Beginn ist der Raum geöffnet. Für die Teilnahme ist ein Browser (z. B. Firefox, Internet Explorer) erforderlich. Außerdem sollte die Möglichkeit vorhanden sein, den Ton zu hören (Lautsprecher, Headset).

Die einzelnen Online-Vorträge werden aufgezeichnet und anschließend anonymisiert öffentlich zur Verfügung gestellt. Weitere Informationen unter
http://blogs.fu-berlin.de/dachadobeconnect/ ◆

Globales VPN für deutsch-japanische Weltraum-Mission

Die Europäische Weltraumorganisation ESA unterhält am Standort in Darmstadt ihr Raumflugkontrollzentrum „European Space Operations Center – ESOC", von wo aus jüngst die historischen Erfolge der Kometensonde ROSETTA geleitet wurden. Neben eigenständigen Missionen betreibt die ESA auch Kooperationen mit internationalen Partner-Organisationen, so auch mit der japanischen Weltraumerforschungsbehörde „Japan Aerospace Exploration Agency – JAXA".

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

Aktuell ging es um die Zusammenarbeit bei zwei Weltraumsonden-Missionen, der Asteroidensonde Hayabusa2 und des Merkur-Orbiters BepiColombo. Hayabusa2 ist eine japanische Entwicklung, die jedoch die bodengestützte Antennen-Infrastruktur der ESA zum Datenempfang mitnutzen sollen. Ihr Ziel ist der erdnahe Asteroid „1999 JU3". Nach der Ankunft am Asteroiden wird Hayabusa2 zunächst die Oberfläche des Himmelskörpers vermessen. In einem zweiten Schritt sollen dann der Asteroidenlander MASCOT (Mobile Asteroid Surface Scout) der federführend vom Deutschen Zentrum für Luft- und Raumfahrt (DLR) in Kooperation mit der französischen Raumfahrtagentur CNES und der japanischen Raumfahrtbehörde JAXA entwickelt wurde, sowie zwei Landungsroboter zum Einsatz kommen. Die Daten, die Hayabusa2 und MASCOT auf dem Asteroiden sammeln, werden an eine global verteilte Infrastruktur von Richtfunk-Antennen auf der Erde geschickt und über einen Verbund der Forschungsnetze zusammengeführt.

In ähnlicher Weise kommuniziert die Merkur-Mission BepiColombo mit der Erde. Die nach dem 1984 verstorbenen italienischen Mathematiker Giuseppe Colombo benannte Mission hat das Ziel, das Magnetfeld und die geologische Zusammensetzung und Geschichte des sonnennächsten Planeten zu untersuchen. Hierzu führt die Sonde zwei unabhängige Sensorplattformen – je eine in Europa und Japan entwickelt – mit sich, die gemeinsam auf einer Transferstufe zum Merkur gebracht und in engerer Zusammenarbeit von ESOC und JAXA betrieben werden sollen.

Bei Missionen, die in großer Entfernung von der Erde stattfinden, müssen leistungsstarke Richtfunk-Antennen am Erdboden für die Kommunikation genutzt werden, die jedoch nur an wenigen Standorten existieren. Idealerweise sollten sogar mehrere um den Erdball verteilte Antennen zum Einsatz kommen, damit sich durchgehend eine auf der der Sonde zugewandten Seite der Erde befindet.

Im Rahmen der Planungen für den Betrieb mit den verteilten Bodenstationen trat das ESOC Anfang 2014 an den DFN-Verein heran, um Möglichkeiten des Datenaustauschs zwischen den Partnereinrichtungen über die Wissenschaftsnetze zu untersuchen. Es bestand Bedarf am Transport von Datenströmen mit Telemetrie der Sonden zwischen den Antennen-Stationen und den Kontrollzentren sowie VoIP-Sprachkommunikation zwischen den Kontrollzentren. Zuvor wurden für solche Anwendungen dedizierte Direktleitungen verwendet. Da jedoch durch den Einsatz mehrerer Direktleitungen über solch große Entfernungen erhebliche Kosten entstehen, wurde nach geeigneten Alternativen gesucht. Die Datenströme sind bereits digital und lassen sich problemlos auf IP-basierten Netzwerken transportieren. Die anfallenden Datenraten im Bereich 1 Mbit/s sind verschwindend klein im Vergleich zu anderen Anwendungen in den Wissenschaftsnetzen. Die Herausforderung in diesem Projekt lag von Anfang an in der Sicherstellung einer VoIP-tauglichen Latenz und einer minimalen Paketverlustrate auf der knapp 19.000 km langen Strecke (one way), sowie in der Koordination der diversen unterwegs involvierten Netzbetreiber. Gleichzeitig ist solch ein international sichtbares Projekt auch erneut eine gute Gelegenheit, die Flexibilität und Zuverlässigkeit von Best-Effort-IP-Diensten auf den internationalen Wissenschaftsnetzen zu demonstrieren. Hauptpartner dabei sind der DFN-Verein, die europäische Organisation der Wissenschaftsnetze GÉANT und das japanische Wissenschaftsnetz SINET.

Für die Ende 2014 gestartete Hayabusa2-Mission wurde ein Layer-2 VPN zwischen dem ESOC in Darmstadt und dem JAXA-ISAS In-

stitut im japanischen Sagamihara geschaltet, das im Regelbetrieb zum Einsatz kommt. Außerdem dient es als Backup für die in missionskritischen Phasen parallel zum VPN genutzte Direktleitung. Für die 2016 anstehende „BepiColombo"-Mission soll zur Ausfallsicherheit eine zweite, physisch und logisch unabhängige Verbindung eingerichtet werden, die jederzeit einen identischen Datenstrom transportieren und dem Endanwender jederzeit zwei live umschaltbare Datenquellen zur Verfügung stellen kann. Damit soll eine erhöhte Zuverlässigkeit und Vertrauenswürdigkeit der neuen Übertragungsmethode realisiert werden.

Aufgrund der geographischen Lage Deutschlands und Japans waren die zur Verfügung stehenden Verbindungen in West- und Ost-Richtung ähnlich lang, weshalb zunächst je eine in westlicher und eine in östlicher Richtung geplant waren. Bei der Identifizierung und Koordination geeigneter internationaler Partner konnte – insbesondere auf der westlichen Route via USA – auf bereits bestehende Vereinbarungen zurückgegriffen werden. Damit konnte die erste Route von Darmstadt über das X-WiN, das GÉANT, den New Yorker Exchange-Point MANLAN und den dort befindlichen SINET Peering-Point nach Japan relativ problemlos definiert und implementiert werden. Zum Einsatz kommt ein Layer-2 VPN, welches vom DFN-Verein am GÉANT-Knoten in Frankfurt a. M. übergeben und von dort mit übersetzter VLAN ID über einen MPLS-(Multiprotocol Label Switching)-Circuit durch die Partner-Netze nach Japan geleitet wird. Die zweite Verbindung wird dann mit einer eigenen VLAN ID voll redundant über die zweite Zugangsleitung des ESOC-Standortes in Darmstadt und den zweiten DFN-GÉANT Zugang in Berlin an GÉANT übergeben. Nachdem sich die ursprünglich angedachte Ost-Verbindung verzögert hatte, wird nun zunächst eine physisch getrennte zweite West-Verbindung via USA implementiert, bis in 2016 die geplante direkte Anbindung von SINET an GÉANT in Europa in Betrieb genommen wird.

Die erste West-Verbindung steht seit Sommer 2014 zur Verfügung und konnte ausgiebig und mit sehr zufriedenstellendem Ergebnis vom ESOC getestet werden. Zum aktuellen Zeitpunkt, kurz vor der Indienststellung der zweiten Verbindung, kann man ein vorläufig positives Fazit ziehen. Die grundlegende Best-Effort-IP-Technik der internationalen Wissenschaftsnetze hat sich ein weiteres Mal bewährt und erfüllt die Anforderungen zur Zufriedenheit der Anwender in Japan und Deutschland. Die Komplexität dieses Vorhabens entspringt hauptsächlich der Anzahl der Partner und der Einzel-Abschnitte der Gesamtstrecke, welche erheblichen Kommunikationsaufwand und eine gründliche Vorbereitung des Projekts erforderte. Da nun aber die grundlegenden Fragen positiv beantwortet werden konnten und die Kommunikationswege erprobt sind, steht einer erfolgreichen Implementation der voll redundanten Lösung nichts mehr im Weg. ◆

Foto © Akihiro Ikeshita/JAXA

Figure of imagination of "HAYABUSA2" to explore asteroid 1999JU3

GÉANT in HORIZON 2020

Ein Framework Partnership Agreement sichert für die kommenden sieben Jahre die Zusammenarbeit zwischen der Europäischen Kommission und GÉANT.

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

Seit vielen Jahren engagiert sich die Europäische Kommission für den europäischen Forschungs-Backbone GÉANT. So wurden von der Kommission in den vergangenen Jahren erhebliche Mittel zum Ausbau des Netzes und dessen technologischer Erneuerung bereitgestellt. Für das 8. Rahmenprogramm der Europäischen Kommission mit Namen „HORIZON 2020“ (H2020) wird nun erstmals ein Framework Partnership Agreement (FPA) zwischen der EU-Kommission und GÉANT vereinbart. Hierbei handelt es sich um einen Rahmenvertrag mit der Europäischen Kommission, welcher für den Zeitraum 2015 bis 2022 die Modalitäten der Zusammenarbeit sowie die längerfristigen strategischen Ziele festlegt.

Die Europäische Kommission und die nationalen Forschungs- und Bildungsnetze in Europa verfolgen ein gemeinsames Ziel: für den europäischen Forschungsraum ein stabiles Umfeld zu schaffen, in welchem GÉANT als offener Raum für Wissen, Innovation und Wachstum genutzt werden kann. Dieses Ziel, die Schaffung eines sogenannten „European Communication Commons“, wurde bereits 2011 in dem Bericht „Knowledge without Borders“ der GÉANT Expert Group (GEG) besonders hervorgehoben. Die Forderung der Experten lautet, dass Wissenschaftler überall in Europa ein Anrecht auf Zugang und Nutzung von Datennetzen und anderen IT-Infrastrukturen haben müssen. Der Report betont nachdrücklich die Bedeutung einer bestmöglich ausgestalteten digitalen Infrastruktur als Voraussetzung dafür, dass Europa auch künftig in der Informationsgesellschaft an der Spitze von Wissenschaft und Forschung steht.

Vor mehr als zwanzig Jahren gegründet, nimmt der europäische Forschungs-Backbone GÉANT im Verbund mit einer Vielzahl nationaler Forschungsnetze in Europa eine herausragende Stellung in der globalen Vernetzung ein. Sowohl im Hinblick auf die Leistungsfähigkeit der Infrastruktur als auch im Hinblick auf die Anzahl der angeschlossenen Einrichtungen und der damit versorgten Nutzer ist GÉANT mit seinem Verbund von nationalen Forschungsnetzen weltweit führend. Insbesondere die internationale Koordinierung von Netzinfrastrukturen oder die Synchronisierung von Diensten wie den vom DFN-Verein mitentwickelten Trust-and-Identity Services oder auch eduroam eröffnen weitreichende Möglichkeiten für eine netzgestützte Wissenschaft. Der DFN-Verein beteiligt sich im Rahmen des FPA an Specific Grant Agreements, den sogenannten SGAs. SGAs sind Teilprojekte über eine bestimmte Laufzeit mit dem Ziel des Ausbaus der Netzinfrastrukturen und der Förderung von Partnerschaften mit internationalen Forschungsnetzen. Im Rahmen der SGAs trägt der DFN zur Weiterentwicklung von Mess- und Monitoring-Tools (PerfSONAR, CMon) bei. Gemeinsam mit anderen Partnernetzen entwickelt der DFN-Verein Technologie für die Trust-and-Identity Services „eduGAIN“ und „eduPKI“.

Ziel der Partnerschaft mit der Europäischen Kommission ist es, GÉANT technologisch weiter voranzutreiben und die Potentiale des Netzes für die Wissenschaft langfristig zu steigern. Dies ist jedoch nur mit einer stabilen Finanzierung auf europäischer und nationaler Ebene möglich. Das Engagement der Europäischen Kommission für GÉANT lenkt das Augenmerk der Mitgliedstaaten auf die wichtige Rolle der nationalen Netze. Auch bietet die Nutzung der europäischen Strukturfonds eine Möglichkeit, Herausforderungen wie die digitale Kluft zwischen den EU-Mitgliedstaaten zu überwinden.

Das FPA definiert sechs Themenfelder, die als entscheidend zur Erreichung der Ziele angesehen und an denen sich zukünftige SGAs orientieren werden. Diese sind (A) die Weiterentwicklung des Netzwerks vorantreiben, (B) die Wissensgesellschaft unterstützen, (C) Sicherheit, Vertrauen und Identität bieten, (D) ein Collaboratives EcoSystem für GÉANT bereitstellen, (E) das Bildungskapital innerhalb der GÉANT-Partnerschaft fördern und (F) die langfristige Finanzierung der GÉANT-Infrastruktur sicherstellen.

Die im Laufe der Jahre von den GÉANT-Partnern entwickelten technischen Innovationen und Kostenteilungs-Prinzipien haben sich bei der Bereitstellung von Dienstleistungen für die F&E-Gemeinschaft bewährt. Bereits heute dient GÉANT der europäischen Wissensgesellschaft durch seine offene, innovative und vertrauenswürdige Informations-Infrastruktur. GÉANT bietet sichere und effiziente Hochgeschwindigkeitsverbindungen und zuverlässige Dienste und Services z. B. im Bereich Identity Inter-Federation und Ressourcen-Virtualisierung. Von großer Bedeutung ist auch die Abstimmung mit anderen europäischen e-Infrastruktur-Anbietern wie der Supercomputing-Initiative PRACE oder der Grid-Initiative EGI sowie der Identity Federation. Ziel ist es, grenzüberschreitende Dienste und Nutzungsszenarien zu etablieren und langfristig die Schaffung eines europaweiten „digitalen Kontinuums“ von Diensten für alle Anwender aus Forschung und Bildung überall in Europa zu ermöglichen. ◆

Kurzmeldungen

Seekabel als ORIENTplus-Nachfolger

Nach Ende des europäisch-chinesischen Vernetzungsprojektes ORIENTplus im Dezember vergangenen Jahres wurde zur Fortführung der Konnektivität zwischen GÉANT und den chinesischen Forschungsnetzen im Dezember 2014 ein gemeinsames Ausschreibungsverfahren der europäischen und chinesischen Partner gestartet.

Der Zuschlag wurde im Februar 2015 für eine 10-Gigabit/s-Verbindung über ein Seekabel mit einer Vertragslaufzeit von zehn Jahren erteilt. Aufgrund der Länge der Verbindung erhöht sich die Einweg-Latenz gegenüber der bisherigen, rein landgestützten Verbindung von ca. 90 ms auf 140 ms. Demgegenüber sinken die jährlichen Kosten erheblich. Mit dem Seekabel bieten sich außerdem perspektivische Optionen für die direkte Anbindung weiterer Forschungsnetze in Indien oder im Mittleren Osten. Darüber hinaus enthält die Vereinbarung Optionen für ein Upgrade auf 100-Gigabit/s und eine redundante landgestützte Verbindung. ◆

Spezialschiff zur Seekabelverlegung, *Foto © Erich Westendarp/pixelio*

Förderung globaler Netzprojekte

Der DFN und elf weitere nationale Forschungsnetze aus Europa, Nord- und Südamerika sowie Australien und Neuseeland haben sich zur Unterstützung der aktuellen, zwei Jahre währenden Runde des Projekts „Enlighten Your Research Global" zusammengeschlossen. „EYR Global" verfolgt das Ziel, den unterschätzten Wert fortschrittlicher Netzwerk- und Kommunikations-Dienste für internationale Forschungsaktivitäten zu demonstrieren. Trotz zahlreicher Forschungsprojekte mit verteilter Infrastruktur und internationalen Partnern, wird die effiziente Nutzung von Netzwerkressourcen oft nicht ausreichend im Projektplan betrachtet und budgetiert.

Daher werden nun im Rahmen eines Ende April beginnenden zweistufigen Auswahlverfahrens geeignete Einrichtungen aus verschiedenen Disziplinen gesucht, welche dann während der zwei Jahre durch die EYR-Global-Partner bei der Erstellung und Umsetzung eines IKT-Plans unter Nutzung der bereitgestellten Ressourcen unterstützt werden.

Weitere Informationen finden sich auf der Projekt-Homepage unter https://www.enlightenyourresearch.net/ ◆

Erster Vorstand der GÉANT Association gewählt

Die Mitgliederversammlung der GÉANT Association hat auf ihrem Treffen am 11. Dezember 2014 in Zagreb aus einem Kreis von fünfzehn nominierten Kandidaten einen neuen Vorstand gewählt. Vorstandsvorsitzender der GÉANT Association wird für die kommenden beiden Jahre Pierre Bruyère vom belgischen Belnet sein. Zu den Mitgliedern des Vorstandes gehören neben Bruyère der DFN-Geschäftsführer Christian Grimm, Sabine Jaume-Rajaonia vom französischen Forschungsnetz RENATER, Ivan Mari vom kroatischen CARNet, der Niederländer Erwin Bleumink von SURFnet, Marco Bonač vom slowenischen ARNES sowie Alberto Pérez vom spanischen RedIRIS. Zwei weitere Mitglieder des Vorstandes werden satzungsgemäß nicht aus dem Kreis der nationalen Forschungsnetze berufen. Als Nicht-NREN-Vertreter wurden Dorte Olesen aus Dänemark und David Foster vom CERN in den Vorstand der GÉANT Association gewählt.

Nach der Zusammenführung von TERENA und DANTE zur GÉANT Association im Oktober letzten Jahres ist somit erstmals ein gemeinsam gewählter Vorstand im Amt. ◆

Sicherheit

Sicherer E-Mail-Verkehr im DFN – von der Beantragung bis zur Nutzung von Zertifikaten
von Thorsten Hindermann

Sicherheit aktuell
von Ralf Gröper, Jürgen Brauckmann

Sicherer E-Mail-Verkehr im DFN – von der Beantragung bis zur Nutzung von Zertifikaten

Wer bereits ein Zertifikat der DFN-PKI besitzt und erfolgreich nutzt, findet's meist gar nicht mehr kompliziert. Lebt man erst einmal „verschlüsselt", versteht man nicht mehr, warum sich alle Welt so schwer damit tut, ein Zertifikat zu nutzen. Tatsächlich ist der Weg zum Zertifikat viel kürzer als man denkt. Der vorliegende Artikel erklärt, wie man in wenigen Schritten zu seinem „Schlüssel" kommt.

Text: **Thorsten Hindermann** (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen – GWDG)

Foto © carlitos/photocase.de

Der Weg zum eigenen Zertifikat

Die zwei Hauptbegriffe, die im Zusammenhang mit dem Umgang von E-Mail-Verschlüsselung fallen, sind X.509-Zertifikate und Public Key Infrastructure, kurz ‚PKI' genannt.

Die PKI ist ein hierarchisch organisierter Aufbau von Zertifikatsautoritäten, engl. Certification Authority (kurz „CA"), die die Echtheit von verwendeten Schlüsseln garantiert. Das Prinzip der CA ist, sämtliche ausgestellten Schlüssel über Zwischenstationen bei einer jeweils nächsthöheren Instanz abzusichern, so dass alle Zertifikate einer PKI mit einem zentralen Wurzelzertifikat validiert sind. Eine solche Kette von Zertifikaten wird Validierungspfad oder Zertifizierungspfad genannt und bildet die Grundlage einer PKI.

Die Zertifikate wiederum sind eine digitale Repräsentation von Benutzern, Diensten, Netzwerkgeräten oder Computern, die durch eine CA ausgestellt werden. Sie funktionieren nach einem einfachen Prinzip: Mit Hilfe eines asymmetrischen Kryptosystems können Nachrichten in einem Netzwerk digital signiert und verschlüsselt werden. In diesen asymmetrischen Kryptosystemen benötigt der Nutzer für eine verschlüsselte Übermittlung den öffentlichen Schlüssel (Public Key) des Empfängers. Dieser kann z. B. per E-Mail versendet oder von einer Webseite heruntergeladen werden. Wird eine Mail mit dem öffentlichen Schlüssel des Empfängers codiert, kann diese anschließend nur noch mit dem zum öffentlichen Schlüssel passenden privaten Schlüssel des Empfängers entziffert werden.

Es ist essentiell, dass hierbei tatsächlich der Schlüssel des Empfängers verwendet wird und nicht die Fälschung eines Betrügers. Und dafür bedarf es der oben beschriebenen Instanzenkette, die sämtliche Schlüssel innerhalb einer PKI an einer gemeinsamen Wurzel validiert.

Zur Logik des Verfahrens gehört, dass der private Schlüssel und der im Zertifikat enthaltene öffentliche Schlüssel fest aneinander gebunden sind. Ein öffentlicher Schlüssel funktioniert nur mit dem zugehörigen privaten Schlüssel und umgekehrt. Trotzdem ist es nicht möglich, vom öffentlichen auf den privaten Schlüssel zu schließen, er kann also gefahrlos veröffentlicht werden. Der private Schlüssel muss allerdings unter allen Umständen geheim gehalten werden.

Zertifikate beantragen

Die Beantragung eines Zertifikats erfolgt grundsätzlich schriftlich und persönlich. Wer ein Zertifikat benötigt, muss hierfür einen Antrag ausfüllen und mit seinem Personalausweis seine tatsächliche Identität bei seiner Zertifizierungsstelle nachweisen. Es ist also notwendig, zunächst herauszufinden, wer in einer Einrichtung für den Antrag zuständig ist. Dies kann in der Regel über das Rechenzentrum bzw. die IT-Abteilung in Erfahrung gebracht werden. Dort wird auch der pro Einrichtung personalisierte Link auf die Antragswebseiten der DFN-PKI bereitgestellt.

Der Antrag für ein Zertifikat wird nicht aus dem Web heruntergeladen, sondern dynamisch während des Beantragungsprozesses generiert. In jahrelanger Praxis hat es sich bewährt, hierfür Mozilla Firefox zu verwenden, da dieser Browser die für Laien komfortabelste Verwaltung von Zertifikaten und Schlüsseln bietet.

Der eigentliche Antrag wird durch einen Klick auf die Schaltfläche „Nutzerzertifikat" in der Menüleiste des Registerreiters „Zertifikate" in Firefox generiert. Hier werden die Basisdaten für das spätere Zertifikat angegeben: Name, E-Mail-Adresse und ggf. die Abteilung, wenn dies von der Einrichtung gefordert wird. Schließlich muss noch eine PIN festgelegt und eingegeben werden. Diese kann später bei verschiedenen Gelegenheiten gebraucht werden, etwa beim Import des Zertifikats in Browser, aber auch, wenn Anwender ihr Zertifikate sperren möchten.

Beim Antrag muss sich der Nutzer entscheiden, ob sein Zertifikat veröffentlicht werden und für Kommunikationspartner auffindbar sein soll. Dies empfiehlt sich in fast allen Fällen, da verschlüsselter Mailverkehr nur mit veröffentlichten Zertifikaten möglich ist.

Ist der Antrag ausgefüllt, werden sämtliche Informationen in einer Übersichtsseite zur Prüfung zusammengefasst und können noch einmal korrigiert oder abschließend bestätigt werden. Bereits mit Betätigung der Schaltfläche „Bestätigen" wird der private Schlüssel im Browser des Nutzers generiert und automatisch im Firefox-Zertifikatspeicher abgelegt. Der Zertifikatspeicher arbeitet dabei unabhängig vom verwendeten Betriebssystem. Erst jetzt wird der schriftliche Zertifikatantrag, die so genannte „certificate signing request (CSR)" bei der Zertifizierungs-Abteilung (meist im Rechenzentrum angesiedelt) gestellt. Das vom Browser generierte Antrags-PDF muss heruntergeladen, ausgedruckt und vom Zertifikatnehmer eigenhändig unterschrieben werden.

Mit diesem Formular wird die persönliche Identifizierung als Teilnehmer der DFN-PKI vorgenommen. Mittels des Personalausweises des Zertifikatnehmers bestätigt der Teilnehmerservice-Mitarbeiter die Authentizität des Antragstellers und die Richtigkeit der Angaben auf seinem Antrag. Kurze Zeit später erhält der Zertifikatnehmer eine Bestätigungsmail, die ihn über die Ausstellung des Zertifikats unterrichtet. Um die Zertifizierung endgültig abzuschließen, muss der Zertifikatnehmer eine Bestätigungs-URL in dieser Mail anklicken. Hier empfiehlt sich einmal mehr die Verwendung von Firefox als Browser: Ist auf dem System des Zertifikatnehmers Firefox der Standardbrowser, genügt ein Klick auf diesen Link. Nutzt er standardmäßig einen anderen Browser, muss die URL kopiert und in

die Adresszeile des Firefox eingefügt werden. Nun werden im Firefox der private und signierte öffentliche Schlüssel zusammengeführt und beide ergeben zusammen das Zertifikat. Ist dieser Vorgang erfolgreich abgeschlossen, wird ein entsprechender Hinweis präsentiert.

Sicherung von Zertfikaten

Es empfiehlt sich für den Nutzer dringend, umgehend eine Sicherungskopie des Zertifikats anzufertigen. Zertifikate werden bei Verlust niemals nacherstellt. Ist das Zertifikat durch Verlust des Rechners oder Verlust der Software verloren, muss ein Neues beschafft werden.

Die Sicherung von Zertifikaten ist nicht nur im Hinblick auf einen möglichen Verlust von Daten oder Hardware sinnvoll, sondern hat noch einen weiteren praktischen Aspekt, der nicht unterschätzt werden sollte: Zertifikate sind nur begrenzt gültig und müssen von Zeit zu Zeit erneuert werden. Ein persönliches Zertifikat für die E-Mail-Verschlüsselung hat z.B. eine Laufzeit von drei Jahren. Im Laufe der Zeit sammeln sich daher einige alte Zertifikate an. E-Mails, die in früheren Jahren mit abgelaufenen Zertifikaten verschlüsselt worden sind, können nur mit dem ursprünglichen Zertifikat wieder entschlüsselt werden, selbst wenn zu diesem Zeitpunkt das Zertifikat sein Ablaufdatum überschritten hat. Deshalb ist die Sicherung und Aufbewahrung ein wichtiger Schritt. Zu bedenken ist auch, dass bei einem Rechnerwechsel am besten alle alten und das aktuelle Zertifikat in die entsprechenden Zertifikatspeicher importiert werden.

Auch hier ist Firefox wieder der Browser der Wahl: Im Einstellungsdialog „Extras“ findet sich ein Zahnrad-Symbol mit der Unterschrift „Erweitert“. Auf der mehrfach geteilten Schaltfläche darunter findet sich der Schalter für „Zertifikate“. Dort erscheint ein Dialog mit einer mehrfach geteilten Schaltfläche bzw. einem Registerreiter. Unter „Ihre Zertifikate“ lässt sich das aktuelle Zertifikat sichern. Da die Sicherungsdatei verschlüsselt wird, wird hier nach einem Kennwort gefragt. Der Grund dafür ist, dass diese Datei sowohl den privaten als auch den öffentlichen Schlüssel enthält. Gerade wegen des privaten Schlüssels ist es wichtig, dass diese Datei entsprechend gesichert ist.

Installation und Verteilung von Zertifikaten

Nachdem ein Zertifikat erfolgreich beantragt und mit dem privatem Schlüssel gesichert wurde, müssen die beiden noch zu ihrem eigentlichen Einsatzort, dem E-Mail-Programm, gebracht werden. Das E-Mail-Programm verwendet den privaten Schlüssel zum Signieren von E-Mails und den öffentlichen Schlüssel zum Entschlüsseln von erhaltenen verschlüsselten E-Mails. Darüber hinaus soll das eigene Zertifikat von Personen, die eine verschlüsselte E-Mail an den Zertifikatinhaber schicken möchten, gefunden werden. Zertifikate bestehen, wie schon erwähnt, aus zwei Teilen: dem privaten und dem öffentlichen Schlüssel. Während der private Schlüssel gut geschützt beim Zertifikatnehmer verbleibt, kann und darf der öffentliche Schlüssel verbreitet werden.

Grundsätzlich gibt es zwei Möglichkeiten, seinen öffentlichen Schlüssel zu verteilen. Man kann hierfür eine zentrale Ablage verwenden oder ihn per E-Mail an potentielle Kommunikationspartner versenden, etwa, in dem man seinen öffentlichen Schlüssel standardmäßig an alle Mails anhängt, die man versendet.

Wenn man eine signierte E-Mail verschickt, ist der eigene Schlüssel übrigens automatisch Bestandteil der E-Mail und der Empfänger ist automatisch nach Empfang in der Lage, verschlüsselt zu antworten.

Eine zentrale Möglichkeit zur Verbreitung des Zertifikats ist der Public-Key-Server des DFN-Vereins. Wird bei der Beantragung des Zertifikats ein Haken bei „Veröffentlichung des Zertifikats“ gesetzt, wird der öffentliche Schlüssel nach dem Ausstellen des Zertifikats durch den DFN-Verein automatisch dort abgelegt. Damit E- Mail-Programme bei der Mailverschlüsselung dort nach dem öffentlichen Schlüssel eines Empfängers suchen können, muss das E-Mail-Programm jedoch zuvor dafür eingerichtet werden.

In den Konfigurationsmenüs der E-Mail-Programme müssen dabei folgende Werte eingestellt werden:

- Port: 389
- Servername: ldap.pca.dfn.de
- Basispunkt: O=DFN-Verein,C=DE.

Wo genau diese Konfigurationsdaten eingetragen werden müssen, ist abhängig vom jeweiligen Programm/Betriebssystem. Meist findet sich ein Schalter oder Reiter, der mit LDAP bezeichnet ist. Konkrete Informationen finden sich in den Konfigurationsanleitungen (siehe Infokasten).

Signieren und Verschlüsseln mit X.509-Zertifikat

Zertifikate haben zweierlei Funktion: Mit ihnen können E-Mails digital unterschrieben (signiert) oder aber verschlüsselt werden. Nicht selten wird beides zugleich getan. Beim einfachen Signieren einer Mail wird diese aber noch nicht verschlüsselt! Sinn der Signatur ist lediglich, die Mail gegen ein nachträgliches Ändern zu schützen und die Identität des Absenders zweifelsfrei sicherzustellen. Unabhängig von den verwendeten Browsern und Betriebssystemen ist das Funktionsprinzip dabei immer gleich. Ohne dass der Nutzer hiervon Kenntnis haben muss, laufen im E-Mail-Programm eine Reihe von Prozessen ab.

Signiert der Nutzer seine E-Mail, erzeugt das E-Mail-Programm eine Prüfsumme (engl. message digest), die aus dem Text

der E-Mail generiert wird, ähnlich einer Quersumme oder einer Prüfziffer auf einer EC-Karte. Diese Prüfsumme wird mit dem privaten Schlüssel des Absenders verschlüsselt. Anschließend wird die E-Mail mitsamt der verschlüsselten Prüfsumme an den Empfänger geschickt. Dieser entschlüsselt die Prüfsumme unter Verwendung des mitgesendeten öffentlichen Schlüssels des Signaturzertifikats vom Absender. Die E-Mail-Anwendung des Empfängers stellt dieselbe Berechnung zur Ermittlung der Prüfsumme über die empfangene E-Mail an. Beide Prüfsummen werden verglichen. Sind sie identisch, ist die E-Mail unterwegs nicht verändert worden. Sollten sich die beiden Prüfsummen unterscheiden, gibt das E-Mail-Programm eine entsprechende Warnung an den Empfänger aus. Ist auch die Absenderadresse der E-Mail mit der im Signaturzertifikat genannten Adresse identisch, herrscht auch Sicherheit bezüglich der Identität des Absenders.

Beim Verschlüsseln einer E-Mail verwendet das E-Mail-Programm des Absenders den öffentlichen Schlüssel des Empfängers, den es zuvor per Mail erhalten hat oder aus einem zentralen Verzeichnis, z. B. aus dem oben beschriebenen DFN LDAP-Server erfährt. Mit diesem öffentlichen Schlüssel wird nun die E-Mail chiffriert.

Der Empfänger erhält also eine mit seinem eigenen öffentlichen Schlüssel codierte Nachricht, die nur mit seinem privaten Schlüssel wieder lesbar gemacht werden kann. Damit ist der digitale Briefwechsel zwischen den Partnern effektiv vor neugierigen Blicken und digitalem Ausspähen geschützt.

Fazit

Nachdem die drei Schritte Beantragen, Verteilen und schließlich das Benutzen eines Zertifikats zum Verschlüsseln und Signieren durchgeführt wurden, ist es für Nutzer der DFN-PKI möglich, vertraulich und sicher mit anderen per E-Mail zu kommunizieren. Weder staatliche Stellen noch andere Angreifer haben die Möglichkeit, die Verschlüsselung bzw. Signatur zu brechen und so Inhalte einer E-Mail zu lesen oder zu verändern. Die Nutzung von Zertifikaten verlangt jedoch vom Nutzer ein wenig Einarbeitungszeit und Sorgfalt bei der Sicherung von Schlüsseln - das Ergebnis ist es aber in vielen Fällen wert!

Viele Rechenzentren oder IT-Abteilungen in der DFN-Community unterstützen ihre Mitarbeiter und Studierende bei der Beantragung und Einrichtung von Zertifikaten ◆.

Info

Dieser Artikel ist eine gekürzte Version eines vierteiligen Artikels aus den GWDG-Nachrichten. Die Originalbeiträge finden Sie als PDF unter http://www.gwdg.de/fileadmin/inhaltsbilder/Pdf/GWDG-Nachrichten/GN_Special_01-2014_www.pdf. Diese Beiträge enthalten die kompletten Anleitungen mit Screenshots auch für in diesem Artikel nicht erwähnte Systeme.

Sicherheit aktuell

Redaktion: **Dr. Ralf Gröper** (DFN-Verein), **Jürgen Brauckmann**) (DFN-Verein)

FREAK-Attack: Konfiguration von TLS-Servern prüfen

Am 3. März 2015 wurde ein neuer Angriff auf verschiedene TLS-Implementierungen wie Safari und openssl bekannt, der wieder einmal deutlich macht, wie wichtig eine korrekte Konfiguration von TLS-Servern ist.[1,2] Ein aktiver Man-In-The-Middle kann unter bestimmten Umständen einen Client dazu bringen, alte und vollkommen unsichere SSL-Algorithmen zu akzeptieren. Dadurch kann die Verbindung vom Angreifer sehr leicht entschlüsselt werden. Der Angriff kann nur durchgeführt werden, wenn die folgenden beiden Bedingungen zusammen erfüllt sind:

- Der Client verwendet eine verwundbare TLS-Software
- Der Server erlaubt veraltete Cipher Suites4

Die FREAK-Attacke kann also, wie zahlreiche anderen Angriffe auf verschlüsselte Verbindungen in der letzten Zeit, von jedem Administrator eines TLS-Servers nur durch Konfigurationseinstellungen abgewehrt werden. Es ist dringend zu empfehlen, regelmäßig die Konfigurationseinstellungen der TLS-Server zu überprüfen und beispielsweise mit den Anleitungen von BetterCrypto.org abzugleichen. Externe Werkzeuge wie der Test von SSL Labs[3] können diese Arbeit deutlich erleichtern. Bei der Nutzung von externen Diensten muss allerdings beachtet werden, dass damit Daten über die geprüften Server an Dritte weitergegeben werden. ◆

Kürzere Laufzeit für neu ausgestellte Serverzertifikate in der DFN-PKI

Wie bereits seit 2012 in der Policy der DFN-PKI verankert, wird seit dem 31.03.2015 die maximale Gültigkeit von neu ausgestellten Serverzertifikaten in der DFN-PKI, Sicherheitsniveau "Global", auf 39 Monate beschränkt. Die vorher mögliche Laufzeit von 5 Jahren ist nach den "Baseline Requirements" des CA/Browser-Forums, zu deren Einhaltung die DFN-PKI zur Aufrechterhaltung der Browserverankerung verpflichtet ist, nicht mehr erlaubt. Durch die automatischen Hinweismails werden Serveradministratoren aber frühzeitig und mehrfach vor dem Ablaufen von Zertifikaten gewarnt, so dass rechtzeitig ein neues Zertifikat beantragt werden kann. ◆

1) https://www.smacktls.com/#freak
2) http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html
3) https://www.ssllabs.com/ssltest/
4) https://www.pki.dfn.de/fileadmin/PKI/anleitungen/Interne-Namen.pdf
5) https://cabforum.org/wp-content/uploads/Guidance-Deprecated-Internal-Names.pdf

Interne Domainnamen

In einigen Einsatzszenarien ist es nützlich oder sogar erforderlich, Web- oder sonstige Server mit Zertifikaten für interne Domainnamen wie „mail.local" oder reservierte IP-Adressen wie 192.168.6.1 auszustatten. Da diese Daten aber nicht eindeutig einem einzigen Server zugeordnet sind, ist die Existenz und die Nutzung solcher Zertifikate unter einer öffentlich vertrauten im Browser vorinstallierten CA wie der DFN-PKI (Sicherheitsniveau „Global") ein potentielles Sicherheitsrisiko. Daher schreiben die Baseline Requirements des CA/Browser-Forums schon seit einiger Zeit vor, dass solche Zertifikate nur noch mit einer maximalen Laufzeit bis zum 30. Oktober 2015 ausgestellt werden. Am 01. Oktober 2016 müssen alle noch gültigen betroffenen Zertifikate, die eventuell früher mit einer längeren Laufzeit ausgestellt wurden, gesperrt werden. Lässt sich die Verwendung von internen Domainnamen oder reservierten IP-Adressen in Zertifikaten nicht vermeiden (z. B. durch Umbenennungen), so müssen diese in Zukunft von nicht im Browser vorinstallierten CAs ausgestellt werden. Eine ausführliche Beschreibung und weitere Hinweise zu dieser Problematik finden sich in einem Dokument, das von der DFN-PKI bereitgestellt wird[4]. Vom CA/Browser-Forum steht ebenfalls ein Dokument mit Hinweisen zur Verfügung[5]. ◆

Kontakt

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

Lifestyle contra Sicherheit

Die rechtlichen Herausforderungen von „Bring Your Own Device“

Die Rechenleistung und Komplexität mobiler Endgeräte ist in den letzten Jahren derart gestiegen, dass sie mit herkömmlichen PCs mithalten oder diese sogar leistungstechnisch übersteigen. Überall und jederzeit ist damit der Zugriff auf lokale Anwendungen und Daten möglich, meist auch mit einer direkten Verbindung zum Internet. Gleichzeitig bieten die Cloud-Technologien einen nahezu unbegrenzten Zugang auf global gespeicherte Daten über diese Geräte. Neben der Wirtschaft hat auch die öffentliche Verwaltung die vielfältigen und flexiblen Möglichkeiten dieser Geräte für sich entdeckt. Mitarbeitern ist eine gewohnte und einfache Arbeitsumgebung sehr wichtig. Nirgends können sie derartige Umstände besser vorfinden als auf ihren eigenen Endgeräten. Es stellt sich daher die Frage, welche rechtlichen Probleme bei der Nutzung privater Endgeräte zu dienstlichen Zwecken („Bring Your Own Device“, kurz „BYOD“) bestehen.

Text: **Kevin Kuta** (Forschungsstelle Recht im DFN)

Foto © Blend Images - Jose Luis Pelaez Inc/getty images

Dieser Beitrag stellt den ersten Teil einer Reihe zu diesem Themenkomplex dar, wobei zunächst allgemeine Fragen besprochen, die Sicht der Aufsichtsbehörden dargestellt und haftungsrechtliche Gesichtspunkte erörtert werden. Am Ende der Darstellung des jeweiligen Rechtsgebietes werden Handlungsempfehlungen beschrieben, die gleichzeitig als eine Art Checkliste genutzt werden können.

I. Begriffsbestimmung

Unter „Bring Your Own Device“ (kurz: BYOD) versteht man die Einbringung und Einbindung privater IT-Endgeräte des Arbeitnehmers für die dienstliche Nutzung beim Arbeitgeber. Abweichend von der strikten Übersetzung des Wortes „Device“ mit „Gerät“ muss ein umfassendes Verständnis des Device-Begriffes angelegt werden, sodass neben IT-Endgeräten auch Softwares, Applikationen, Datenbanken, Services und Ähnliches von diesem Begriff umfasst sind. Teilweise werden die Begriffe „Bring Your Own Device“ und „Consumerization of IT“ parallel verwendet. Im Detail beschreiben sie jedoch unterschiedliche Phänomene. Mit „Consumerization of IT“ ist die beliebte und steigende Nutzung von leicht bedienbaren und für den privaten Bereich optimierten mobilen Endgeräten (Consumer-Grade-Geräte wie Notebooks, Tablets oder Smartphones) im Privatbereich sowie in allen Ebenen eines Unternehmens bis in die Führungsetagen gemeint. Demgegenüber drückt „Bring Your Own Device“ die bewusste strategische Entscheidung aus, dass private Endgeräte für die dienstliche Nutzung zugelassen werden.

Die Initiative für die Einbringung der privaten Endgeräte in die IT-Landschaft des Arbeitgebers kann sowohl von diesem selbst als auch vom Arbeitnehmer ausgehen. Aktuell nutzen etwa 70% der Arbeitnehmer in Deutschland eigene IT-Endgeräte für dienstliche Zwecke am Arbeitsplatz. Am häufigsten werden dabei Personal Computer oder Laptops genutzt (45%), gefolgt von Smartphones (30%) und weiteren Geräten. Knapp 20% der von dem Phänomen „BYOD“ betroffenen Unternehmen gewähren den privaten Endgeräten dabei (in Teilen sogar uneingeschränkten) Zugriff auf die dienstliche IT-Infrastruktur. Eine Vielzahl von Unternehmen (etwa 40%) möchte laut einer Umfrage sogar bis zum Jahr 2016 vollständig und verpflichtend auf „BYOD“ umsteigen. Neben dem Cloud Computing handelt es sich bei „BYOD“ nach den Aussagen vieler Experten um den nächsten Megatrend in der IT-Branche. Der Einsatz privater Endgeräte für dienstliche Zwecke wird in den nächsten Jahren vermutlich weiter zunehmen. Eine langfristige Durchsetzung hängt aber wahrscheinlich in erster Linie davon ab, inwieweit die (vor allem rechtlichen) Umsetzungsschwierigkeiten gelöst werden können.

II. Ausgangslage und Effekte

Es stellt sich natürlich die Frage, wie es zu diesem Trend der Einbringung eigener Endgeräte am Arbeitsplatz kommt. Die IT in Unternehmen sowie der öffentlichen Verwaltung ist oftmals veraltet und dementsprechend langsamer als der auf dem Markt übliche Standard, sodass als einer der Hauptbeweggründe für die Umsetzung von „BYOD“ in der technischen Überlegenheit und

Foto © cydonna/photocase.de

Aktualität der privaten IT zu sehen ist. Gleichzeitig werden die vom Arbeitgeber auferlegten (und in den meisten Fällen auch notwendigen) Sicherheitsmaßnahmen vom Arbeitnehmer als Behinderung wahrgenommen. Die Entwicklung bei mobilen Endgeräten, insbesondere im Smartphone- und Tablet-PC-Sektor, schreitet schnell voran. Dementsprechend wollen die Mitarbeiter ihre privaten leistungsfähigeren und nutzerfreundlicheren Endgeräte einsetzen. Sie können ihre eigene, bekannte Hardware benutzen und müssen nicht noch ein weiteres, bisher fremdes Gerät verwenden, sodass eine Umgewöhnung auf eine komplett neue Hard- und Software vermieden wird, was auch einen sinkenden Schulungsbedarf für den Arbeitgeber zur Folge hat.

Auf diese Weise ist sogar eine Kombination von dienstlichen und privaten Aufgaben möglich. Berufliche und private Kontakte können mittels eines Gerätes unkompliziert gepflegt werden. Dies kann eine erhöhte Motivation der Beschäftigten zur Folge haben und gleichzeitig die Effizienz und Produktivität merklich steigern. Auch können sich dadurch Auswirkungen auf die Außendarstellung und Attraktivität des Arbeitgebers ergeben, da er so flexibler und mitarbeiterfreundlicher erscheint. Die erhöhte Zufriedenheit der Mitarbeiter und die gesteigerte Identifikation mit dem Arbeitgeber können neben einer erhöhten Produktivität zudem eine erhöhte Erreichbarkeit mit sich bringen. Gleichzeitig können für ihn Einsparungspotentiale entstehen, da der Arbeitgeber deutlich weniger Hardware anschaffen muss. Dieses letztgenannte Argument kann sich aber auch (wie einige Beispiele in den letzten Jahren beweisen) als Trugschluss erweisen, da durch den erhöhten Managementbedarf der mitarbeitereigenen Endgeräte sowie mögliche Ausgleichszahlungen an die Arbeitnehmer für die Einbringung der eigenen Endgeräte nicht zu unterschätzende Kosten entstehen.

Mit der Durchmischung von dienstlicher und privater Hardware sowie Daten gehen neben den Wohlfühl-Faktoren aber auch erhebliche Gefahren einher. Neben rechtlichen Vorkehrungen, wobei hier insbesondere der Datenschutz zu nennen ist, müssen technische Rahmenbedingungen geschaffen werden. Entscheidet sich ein Arbeitgeber für die Einführung von „BYOD“, muss eine Gesamtstrategie unter Berücksichtigung sämtlicher Umstände des Einzelfalls entwickelt werden. Nur auf diese Weise kann man die rechtlichen und technischen Hürden angemessen überwinden.

III. Sicht der Aufsichtsbehörden

Obwohl sich die Länder nur sehr verhalten zum Thema „BYOD“ äußern, ist die Meinung der einzelnen Aufsichtsbehörden der Länder zu diesem Thema recht einheitlich: Eine rechtssichere Handhabe der dienstlichen Nutzung von privaten Endgeräten ist nur äußerst schwer bis gar nicht möglich.

ULD Schleswig-Holstein
Das Unabhängige Zentrum für Datenschutz (ULD) Schleswig-Holstein hat sich im Jahre 2009 zu dieser Thematik geäußert. Danach sei die konsequente Einhaltung technisch-organisatorischer Maßnahmen auf privaten Endgeräten nicht möglich. Der Einsatz privater Endgeräte zur Verarbeitung dienstlicher Daten sei weder im einschlägigen Landesdatenschutzgesetz (LDSG) noch in der Landesdatenschutzverordnung (DSVO) vorgesehen und daher grundsätzlich unzulässig. Die Gewährleistung einer ordnungsgemäßen Ausgestaltung der Hardware, von Art und Umfang der zulässigen Nutzung sowie einer effektiven Kontrolle der technischen und organisatorischen Sicherheitsmaßnahmen anhand der IT- und Sicherheitskonzepte der datenverarbeitenden Stelle sei nicht wirksam möglich. Die Verarbeitung personenbezogener dienstlicher Daten beim Einsatz privater Endgeräte sei nur ausnahmsweise mit sog. „Terminalserverdiensten“ möglich, wobei spezielle technische und organisatorische Sicherheitsmaßnahmen notwendig seien. Mittels einer derartigen Lösung wird neben der Authentifizierung am privaten Endgerät eine weitere Authentifizierungs- und Autorisierungsebene eingefügt, mit der eine Terminalserversitzung separat aufgebaut wird, sodass im Ergebnis nur Bildschirminhalte übertragen werden, die Dateien jedoch zu jeder Zeit auf dem Server der datenverarbeitenden Stelle bleiben.

Mecklenburg-Vorpommern
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern empfiehlt nachdrücklich nur behördeneigene Geräte einzusetzen, da nur auf diese Weise eine Umsetzung der rechtlichen Vorgaben mit einem angemessenen Arbeitsaufwand möglich sei. Zudem wird zu einer sorgfältigen Planung und möglichst restriktiven Handhabung von mobilen Endgeräten hinsichtlich des Zugriffs dieser Geräte auf die Behördeninfrastruktur geraten. „BYOD“ führe zu erheblichen Sicherheitsrisiken und sei eine schwere Aufgabe für die einzelnen Abteilungen der öffentlichen Verwaltung. Voraussetzung für eine Nutzung privater Endgeräte zu dienstlichen Zwecken sei eine geeignete Administrationsumgebung, mittels derer die dienstliche und private Nutzung getrennt und gleichzeitig die nutzerseitigen Administrationsmöglichkeiten wirksam verhindert oder zumindest erheblich eingeschränkt werden.

Hessen
Der Hessische Datenschutzbeauftragte hält die rechtlichen und technischen Probleme im Zuge des Einsatzes von spezifisch mitarbeitereigener Hardware zurzeit für unüberwindbar. In erster Linie sei eine Trennung von beruflicher und privater Ebene zwingend erforderlich, wobei aber eine Prüfung durch eine unabhängige Stelle zu erfolgen habe, ob die derzeit verfügbaren Produkte und technischen Ansätze eine wirksame Trennung der beiden Ebenen sicherstellen können. Zum gegenwärtigen Zeitpunkt könn-

ten nur solche dienstliche Daten auf privaten Endgeräten verarbeitet werden, die zwangsläufig in den privaten Bereich des Mitarbeiters ausstrahlen, wie etwa Termine. Es müsse eine weitestgehende Reduzierung des Datenumfangs erfolgen. Gleichzeitig müsse gewährleistet werden, dass bei einer unbefugten Kenntnisnahme durch Dritte keine Beeinträchtigungen für die Betroffenen im Hinblick auf ihre gesellschaftliche Stellung oder wirtschaftlichen Verhältnisse zu erwarten sei.

Berlin
Nach dem Berliner Beauftragten für Datenschutz und Informationsfreiheit müsse das Phänomen „BYOD" weiter beobachtet werden. Die Probleme, Bedrohungen und Sicherheitsmaßnahmen seien einerseits bekannt, andererseits würden Lösungen dafür bereits eingehend diskutiert. Es bedürfe einer Kombination verschiedener rechtlicher und technischer Maßnahmen zur Beherrschung der durch die Nutzung von privaten Endgeräten im dienstlichen Umfeld entstehenden Risiken. Es wird in diesem Zuge eindringlich vor den Gefahren von „BYOD" gewarnt. Gleichzeitig hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit die Einführung von „BYOD" für den Bereich der öffentlichen Verwaltung für unzulässig erklärt bzw. für eine Zulassung in der öffentlichen Verwaltung nur in absoluten Ausnahmefällen plädiert.

Düsseldorfer Kreis
Der Düsseldorfer Kreis, ein Gremium bestehend aus den obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen (= privaten) Bereich, hat die Problematik zwar bereits erkannt, jedoch noch keine gemeinsame Stellungnahme abgegeben. Bisher existiert nur ein Beschluss dieses Gremiums über die datenschutzgerechte Nutzung von Smartphones, wobei nicht auf die Besonderheiten von „BYOD" eingegangen wird.

Bundesamt für Sicherheit in der Informationstechnologie (BSI)
Seitens des Bundesamtes für Sicherheit in der Informationstechnologie wurde im Hinblick auf „BYOD" ein Papier angekündigt. Es ist auch zu erwarten, dass dieses Thema sowie Maßnahmenempfehlungen dazu in den Grundschutzkatalog des BSI Einzug nehmen werden. Dahingehende Maßnahmen sind zum gegenwärtigen Zeitpunkt jedoch noch nicht erfolgt.

IV. Haftungsrecht

Im Schadens- bzw. Haftungsrecht müssen zwei Problemkreise auseinander gehalten werden. Auf der einen Seite stehen sensible Daten des Arbeitgebers. In diesem Punkt steckt aufgrund der Zugriffsmöglichkeit Dritter ein hohes Gefahrenpotential. Auf der anderen Seite stehen die eingebrachten Endgeräte des Arbeitnehmers. Sobald der Arbeitnehmer mit Zustimmung des Arbeitgebers private Geräte für dienstliche Zwecke ins Unternehmen einbringt oder der Arbeitgeber eine solche Vorgehensweise zumindest duldet, trifft ihn eine Schutzpflicht für das vom Arbeitnehmer eingebrachte Eigentum. Außerdem ist der Mitarbeiter nicht zur Ersatzbeschaffung defekter oder verloren gegangener Geräte verpflichtet. Neben diesen zwei Problemkreisen kann auch der private Internetanschluss des Mitarbeiters einige Problemherde eröffnen.

Datenbestände des Arbeitgebers
In der heutigen Zeit sehen sich Arbeitgeber mit einer Vielzahl von Daten konfrontiert, wobei es sich sowohl um eigene Daten, als auch solche von Dritten handeln kann. Durch den Einsatz privater Endgeräte besteht die Gefahr, dass Dritte Zugriff auf betriebliche Datenbestände erlangen. Dabei kann es sich um Angehörige aus dem Familien- und Bekanntenkreis handeln, jedoch kommen auch fremde Personen in Betracht, etwa im Falle eines Diebstahls. Zwar ist die Kenntnisnahme als solche schon äußerst problematisch, beispielsweise vor dem Hintergrund des Datengeheimnisses. Die Löschung von Daten stellt aber den „worst case" bei der Zugriffsmöglichkeit durch dritte Personen dar, wobei dies umso wahrscheinlicher wird, wenn Kinder auf die dienstlichen Daten zugreifen können. Diese gesamte Problematik wird noch gravierender, wenn die Daten dem Arbeitgeber von einem Dritten zur Be- oder Weiterverarbeitung überlassen wurden.

Oftmals bieten private Sicherheitssoftwares (wie etwa Antivirenprogramme oder Firewalls) im Vergleich zu Varianten für den gewerblichen bzw. geschäftlichen Bereich einen geringeren Schutz und sind zudem nicht auf die Verwendung im dienstlichen Rahmen abgestimmt und eingestellt. Dadurch entsteht die Gefahr der Infektion des privaten Geräts mit Schadsoftware. Sofern dieses Gerät, wie häufig im Rahmen von „BYOD", auch noch gänzlich in die dienstliche IT-Infrastruktur eingebunden ist, ist die Wahrscheinlichkeit deutlich größer, dass auch diese Systeme infiziert werden. Daneben besteht die Gefahr der Ausspähung von Betriebs- und Geschäftsgeheimnissen sowie des Datenverlustes. Private Applikationen können unbemerkt auf dienstliche Daten zugreifen und so neben geheimhaltungsbedürftigen Informationen auch E-Mail-Bestände oder Kontaktdaten auslesen. In diesem Zusammenhang ist insbesondere das unter technisch versierten Mitarbeitern verbreitete „Jailbreak" bzw. „Jailbreaking" eine Bedrohung für die dienstlichen Systeme, da durch die Aufhebung der herstellerseitigen Sperrung bestimmter Funktionen und deren anschließender Veränderung viele Einfallstore für Angriffe geschaffen werden.

Hinzu kommt, dass im Schadensfall (etwa bei einem Datenverlust) möglicherweise nur eine beschränkte Haftung des Arbeitnehmers besteht. In diesem Falle finden nämlich die arbeitsrechtlichen Grundsätze des innerbetrieblichen Schadensausgleichs Anwendung. Daraus ergibt sich eine abgestufte Arbeitnehmer-

haftung, die vom jeweiligen Verschuldensgrad des Arbeitnehmers abhängig ist. Bei Vorsatz oder grober Fahrlässigkeit haftet der Arbeitnehmer grundsätzlich in voller Höhe, wohingegen bei mittlerer Fahrlässigkeit eine anteilige Haftung besteht und der Arbeitnehmer nur bei leichter und leichtester Fahrlässigkeit gar nicht haftet. Anwendungsbeispiele im Rahmen von BYOD können die schuldhafte Verletzung von Sorgfaltspflichten oder der (bewusste oder unbewusste) Einsatz schadhafter Software sein. Bei der soeben dargestellten Einteilung handelt es sich jedoch nur um eine grobe Orientierungshilfe. Es kommt vielmehr immer auf die konkreten Umstände des Einzelfalles an. Neben dem Grad des Verschuldens sind insbesondere die konkrete Schadenshöhe und die sich daraus ergebende Zumutbarkeit der Schadensübertragung auf den Arbeitnehmer vor dem Hintergrund seiner wirtschaftlichen Leistungsfähigkeit zu beachten. Letztlich besteht für den Arbeitgeber aber immer die Gefahr, dass er den Arbeitnehmer bei Schäden nicht in Regress nehmen kann.

Schutzpflicht für private Endgeräte

Die Endgeräte der Mitarbeiter als solche bringen schon einige Haftungsrisiken mit sich. Auch die mitarbeitereigene Hardware bedarf der Wartung und Reparatur. Daneben sind in regelmäßigen Abständen Softwareupdates unumgänglich. Mit diesen Arbeiten an Hard- und Software geht auch ein Schadensrisiko einher, das je nach eingesetztem Produkt aus dem finanziellen Blickwinkel nicht zu unterschätzen ist. Die Geräte können außerdem beschädigt werden, verloren gehen, gestohlen werden oder auf sonstige Art abhanden kommen. Bei Verlust oder Beschädigung besteht eine Benachrichtigungspflicht des Arbeitnehmers gegenüber dem Arbeitgeber, vor allem auch wegen der auf dem Gerät befindlichen dienstlichen Datenbestände. Dabei darf „BYOD“ nicht zur Umgehung des Betriebsrisikos führen, das der Arbeitgeber zu tragen hat. Dementsprechend ist der Arbeitgeber regelmäßig zur Zahlung eines Aufwendungsersatzes für die dienstliche Nutzung des Privatgeräts verpflichtet (vgl. §§ 670, 675 Bürgerliches Gesetzbuch (BGB)). Daneben steht dem Arbeitnehmer für risikotypische Schäden am Gerät nach § 670 BGB analog ein Ausgleichsanspruch zu, wobei es sich hierbei um eine verschuldensunabhängige Haftung handelt. In der Regel wird ein pauschaler vertraglicher Ausschluss dieser Ersatzpflichten gegen das AGB-Recht verstoßen und damit rechtswidrig sein. Der Arbeitgeber kann das Aufwendungsersatzverlangen hingegen dann zurückweisen und eine Zahlung verweigern, wenn die Vergütung seitens des Arbeitgebers im Rahmen der Anschaffung des Gerätes bereits das Schadensrisiko abdeckt, weshalb diesbezüglich eine klare Abrede zwischen den Parteien erforderlich ist.

Privater Internetanschluss

Die Nutzung des privaten Internetanschlusses zu dienstlichen Zwecken kann ebenfalls Probleme hervorbringen. An dieser Stelle findet zwar eine starke Vermengung von „BYOD“ und „Telearbeit“ statt, nichtsdestotrotz muss es im Rahmen von „BYOD“ berück-

Foto © Labor3

sichtigt werden. Einige Internet-Service-Provider differenzieren zwischen der privaten und dienstlichen bzw. gewerblichen Nutzung. Für diese verschiedenen Nutzungsarten werden vom Diensteanbieter regelmäßig unterschiedliche Entgelte gefordert. Ist der private Internetanschluss nur für die private Nutzung ausgelegt, wird dieser aber für dienstliche Zwecke genutzt, kann möglicherweise eine Vertragsverletzung vorliegen, woraus sich ein Schadensersatzverlangen des Internet-Service-Providers sowie eine Kündigung des Telefon-/Internetprovidervertrags aus wichtigem Grund ergeben kann.

V. Handlungsempfehlungen

Zur Vorbeugung von Haftungsfällen können im Vorfeld einige Maßnahmen ergriffen werden, damit die Gefahren möglichst gering gehalten werden und die Einführung von „BYOD“ somit erleichtert wird. Die nachfolgende Darstellung der Handlungsempfehlungen dient gleichzeitig als eine Art Checkliste.

1. Als oberstes Gebot gilt vorweg, dass aus Gründen der Rechtssicherheit, Klarheit und Transparenz sämtliche Absprachen zwischen Arbeitgeber und Arbeitnehmer schriftlich festgehalten werden sollten.

2. Eine Vereinbarung über regelmäßige Sicherungskopien durch den Arbeitnehmer erscheint ratsam. Auf diese Weise kann ein Datenverlust weitestgehend eingeschränkt werden.

3. Zur Vermeidung von Sicherheitslücken und Datenverlusten ist eine einheitliche Administration durch den Arbeitgeber zu empfehlen. In diesem Zusammenhang sollte der Arbeitgeber einerseits geeignete Sicherheitssoftware zur Verfügung stellen, andererseits sollten betriebliche Vereinbarungen Regelungen über die Haftung bei Verlust oder Beschädigung der Geräte oder betrieblicher Daten enthalten und eindeutig festlegen, wer Reparaturen in Auftrag gibt und deren Kosten trägt. Dadurch kann für beide Parteien das Schadens- und Kostenrisiko eindeutig festgelegt werden, wer also in welchen Konstellationen haftet und welche Partei unter welchen Voraussetzungen das Betriebsrisiko trägt. Darüber hinaus sollte seitens des Arbeitgebers eine regelmäßige Wartung der Privatgeräte durchgeführt werden. Ergänzend kann der Mitarbeiter zur selbständigen Überprüfung des Geräts verpflichtet werden. Da die Betriebshaftpflichtversicherung mitarbeitereigene Hardware regelmäßig nicht abdeckt, ist der Abschluss einer gesonderten Geräteversicherung ratsam, wobei die sich daraus ergebende Kostentragungspflicht eindeutig zugewiesen und geregelt werden sollte.

4. Dem Arbeitnehmer sollte für den Fall des Verlustes eines Geräts eine Benachrichtigungspflicht auferlegt werden. Dies hat insbesondere dann zu gelten, wenn auf dem privaten Endgerät dienstliche Daten gespeichert wurden und dieses Gerät nun gestohlen worden, verloren gegangen oder auf andere Weise abhandengekommen ist. Jedoch kann ein Missbrauch selbst dann nicht ausgeschlossen werden, wenn keine Daten auf dem Gerät gespeichert wurden, da schon die Preisgabe von Verbindungsinformationen zu IT-Systemen des Arbeitgebers diesen angreifbar machen können. Dementsprechend ist eine Benachrichtigungspflicht des Mitarbeiters bei einem Geräteverlust generell empfehlenswert.

5. Neben der einheitlichen Administration sollte die Einstellung der Geräte-Konfiguration ebenfalls zentral durch den Arbeitgeber vorgenommen werden. In diesem Zuge sollten die Arbeitnehmer im Rahmen einer Vereinbarung dazu verpflichtet werden, diese Einstellungen zu verwenden und nicht zu verändern. Ferner sollte der Zugriff auf das private Gerät von der Eingabe eines Passworts abhängig gemacht werden, sodass der Zugriff Dritter (etwa Familienangehörige) eingeschränkt wird. Auch im Hinblick auf den Schutz von Betriebs- und Geschäftsgeheimnissen ist die verbindliche Vorgabe eines Passworts ratsam, zumal diese Daten oftmals vertraglichen Geheimhaltungspflichten gegenüber Dritten unterliegen. Im Rahmen der Vereinbarung sollte der Arbeitnehmer auch verpflichtet werden, das Passwort gegenüber Dritten geheim zu halten und sicher aufzubewahren. ◆

Anmerkung

Einen ausführlichen Leitfaden zur Handhabung von „Bring Your Own Device“ und weitere Handlungsempfehlungen der Forschungsstelle Recht im DFN finden sich unter:
https://www.dfn.de/rechtimdfn/empfehlungen/handlungsempfehlungen/

Freies Wissen für alle?

Das neu eingeführte Zweitveröffentlichungsrecht für Urheber wissenschaftlicher Beiträge

Die Diskussionen über eine Anpassung des Urheberrechts an das digitale Zeitalter sind weiterhin in vollem Gange. Zu den wesentlichen Herausforderungen zählt es dabei auch, die infolge des digitalen Wandels entstandenen Bedürfnisse der Wissenschaft im geltenden Urheberrecht zu berücksichtigen. Hier prallen die Interessen der Universitäten und Länder mit den Interessen der wissenschaftlichen Verlage aufeinander. Dem Gesetzgeber kommt insofern die Aufgabe zu, die gegensätzlichen Positionen in einen Ausgleich zu bringen. Nunmehr existiert seit dem 1.1.2014 ein sog. Zweitveröffentlichungsrecht im Urheberrechtsgesetz, das für Urheber wissenschaftlicher Publikationen gilt. Dieses soll den Weg für „Open Access“ – frei verfügbares Wissen im Internet – freimachen.

Text: **Philipp Roos** (Forschungsstelle Recht im DFN)

Foto © complize/photocase.de

I. Hintergründe und Zielsetzung

Die Wissenschaftsvertreter klagen seit jeher über die Beschränkungen, die das Urheberrecht der Lehre und Forschung auferlegt. Dass es in Anbetracht der Digitalisierung tatsächlich Anpassungen und Überarbeitungen des Urheberrechts bedarf, hat auch der Gesetzgeber wahrgenommen. Insbesondere das „Zweite Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft" (sog. Zweiter Korb), dessen Regelungen zum 1. Januar 2008 in Kraft traten, enthielt einige bemerkenswerte Neuregelungen mit Bedeutung für Wissenschaft und Forschung. Damit setzte die Bundesrepublik Deutschland die EG-Richtlinie zur „Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft" (sog. InfoSoc-Richtlinie) um. Wie die entsprechenden Normen auszulegen sind, beschäftigte die Gerichte in letzter Zeit besonders intensiv.

So gab es im September 2014 erfreuliche Nachrichten für die Wissenschaftsvertreter, als der Gerichtshof der Europäischen Union (EuGH) den Weg für digitale Leseplätze in Hochschulbibliotheken weitgehend ebnete (s. dazu Roos, Weniger Papier ist mehr! – Europäischer Gerichtshof macht den Weg für digitale Leseplätze frei, DFN-Infobrief Recht 11/2014; Roos, Bibliothek 2.0: Alles digital, oder was? – Schlussanträge des Generalanwalts des Europäischen Gerichtshofs zur Auslegung der Bibliotheksschranke, DFN-Infobrief Recht 8/2014). In absehbarer Zeit wird der Bundesgerichtshof (BGH) wieder zu digitalen Leseplätzen entscheiden und die Vorgaben des obersten europäischen Gerichts umsetzen müssen. Konkret geht es um die Auslegung der Norm des § 52b Urheberrechtsgesetz (UrhG), der sog. Bibliotheksschranke.

Eine andere vielbeachtete Entscheidung erging hinsichtlich § 52a UrhG, der sog. Bildungsschranke. Die Bildungsschranke trifft Bestimmungen über den Umgang mit urheberrechtlich geschützten Werken, die Dozenten im Rahmen ihres Unterrichts im Internet hochladen möchten. Zwar rief diese Entscheidung des BGH nicht nur Applaus aus den Kreisen der Wissenschaft hervor, jedoch wurden die Gesetzesmerkmale der Norm immerhin weiter konkretisiert (s. dazu Hinrichsen, Ende gut, alles gut? – Die unendliche Geschichte des § 52a UrhG. Bundesgerichtshof konkretisiert offene Fragen bei sog. Bildungsschranke, DFN-Infobrief Recht 2/2014).

Nach langen Diskussionen innerhalb der beteiligten Kreise und in den Gesetzgebungsorganen existiert seit dem 1.1.2014 eine neue urheberrechtliche Bestimmung mit Hochschulbezug, die

Foto © Feng Yu / fotolia

auch neue Auslegungsfragen hervorruft. In § 38 Abs. 4 UrhG ist ein Zweitveröffentlichungsrecht für die Urheber wissenschaftlicher Publikationen vorgesehen. Dort heißt es:

„Der Urheber eines wissenschaftlichen Beitrags, der im Rahmen einer mindestens zur Hälfte mit öffentlichen Mitteln geförderten Forschungstätigkeit entstanden und in einer periodisch mindestens zweimal jährlich erscheinenden Sammlung erschienen ist, hat auch dann, wenn er dem Verleger oder Herausgeber ein ausschließliches Nutzungsrecht eingeräumt hat, das Recht, den Beitrag nach Ablauf von zwölf Monaten seit der Erstveröffentlichung in der akzeptierten Manuskriptversion öffentlich zugänglich zu machen, soweit dies keinem gewerblichen Zweck dient. Die Quelle der Erstveröffentlichung ist anzugeben. Eine zum Nachteil des Urhebers abweichende Vereinbarung ist unwirksam."

§ 38 Abs. 4 UrhG wurde im Zuge des „Gesetzes zur Nutzung verwaister und vergriffener Werke und weiteren Änderungen des Urheberrechtsgesetzes" (BT-Drucks. 17/13423) in den Gesetzestext aufgenommen. Ziel der Norm ist es, die Potenziale des Internets für die digitale Wissensgesellschaft auszunutzen und für einen möglichst ungehinderten Wissensfluss zu sorgen. So sollen Forschungsergebnisse frei verfügbar sein, um auf Basis dieser Ergebnisse weiter forschen zu können.

Wesentlicher Beweggrund des Gesetzgebers, § 38 Abs. 4 UrhG einzufügen, ist das vertragliche Ungleichgewicht zwischen den Autoren wissenschaftlicher Beiträge und den Wissenschaftsverlagen. Auf dem teilweise quasi-monopolistischen Markt wissenschaftlicher Verlage sind die Autoren wissenschaftlicher Werke vielmals derart auf die Verlage angewiesen, dass die Verlage die Vertragsbedingungen frei vorgeben können und sich sämtliche ausschließlichen Nutzungsrechte – insbesondere auch für den Onlinebereich – einräumen lassen. Zugleich sind die Verlagsprodukte dann aber finanziell so kostspielig, dass die Bibliotheken kaum wissen, wie der Erwerb relevanter Literatur finanziert werden soll. Das gilt vor allem für die Bereiche Naturwissenschaft, Technik und Medizin. Hinter der Norm steht daher auch ein monetärer Beweggrund, der darin liegt, den Effekt der Doppelfinanzierung zu vermeiden: Werden die Forschungen schon aus öffentlicher Hand finanziert, erfordert der Status quo auch die Anschaffung der publizierten Forschungsergebnisse und damit den Einsatz von Steuergeldern. Das soll nun – zumindest im Bereich der wissenschaftlichen Zeitschriften und unter den gesetzlichen Einschränkungen (dazu sogleich) – begrenzt werden. Das Stichwort lautet Open Access, also freier Zugang zu wissenschaftlicher Literatur im Internet.

Der Gesetzgeber sah es als gebotene Lösung an, ein unabdingbares Zweitveröffentlichungsrecht im Urhebervertragsrecht (§§ 31 ff. UrhG) zu normieren. Es handelt sich gesetzestechnisch also nicht um eine urheberrechtliche Schranke (wie bspw. bei den angesprochenen §§ 52a, 52b UrhG), die eine erlaubnisfreie Nutzung des Werkes durch einen bestimmten Personenkreis oder die Allgemeinheit erlaubt. Vielmehr bestimmt der Urheber, ob er – im Falle des Vorliegens der Voraussetzungen – von seinem Zweitveröffentlichungsrecht Gebrauch macht.

II. Wissenschaftlicher Beitrag im Sinne von § 38 Abs. 4 UrhG

Das Zweitveröffentlichungsrecht des Urhebers gilt jedoch nicht für alle publizierten Beiträge von Wissenschaftlern und Forschern. Im Wesentlichen müssen drei Grundvoraussetzungen erfüllt sein, damit § 38 Abs. 4 UrhG zugunsten des Urhebers eingreift:

- Es muss sich um einen wissenschaftlichen Beitrag handeln.
- Die Entstehung des Beitrags ist im Rahmen einer mindestens zur Hälfte mit öffentlichen Mitteln geförderten Forschungstätigkeit entstanden.
- Der Beitrag erschien in einer periodisch erscheinenden Sammlung.

Keine allzu großen Probleme bereitet die Feststellung, ob es sich um einen wissenschaftlichen Beitrag handelt. Die Norm verlangt zunächst, dass ein urheberrechtlich geschütztes Werk vorliegt. Solche urheberrechtlich geschützten Werke führt § 2 Abs. 1 UrhG beispielhaft auf. Als „wissenschaftlicher Beitrag" kommen vor allem Texte (Sprachwerke) in Frage. Zu denken ist aber auch an wissenschaftliche oder technische Darstellungsformen, etwa Zeichnungen, Pläne, Karten, Skizzen und Tabellen. Diese müssen jeweils als persönliche geistige Schöpfungen zu qualifizieren sein, was sich in aller Regel bereits aus ihrer individuellen Gedankenführung oder Darstellungsform ergibt. Das Merkmal der „Wissenschaftlichkeit" wird im Urheberrecht sehr weit ausgelegt – auch einfachste wissenschaftliche Erkenntnisse sind davon umfasst.

Schon genauer untersucht werden muss, ob der Beitrag im Rahmen einer Forschungstätigkeit entstanden ist. Eine Forschungstätigkeit liegt immer dann vor, wenn nicht ausschließlich didaktische Inhalte vermittelt werden. Damit dürften in aller Regel selbst Klausurmusterlösungen als Forschungstätigkeit gelten, da es hier nicht ausschließlich um das „Wie" des Lehrens geht, sondern konkreter Lehrstoff aufbereitet wird. Etwas unklar ist, unter welchen Bedingungen der Beitrag als „im Rahmen" der Forschungstätigkeit entstanden gilt. Das Merkmal könnte sowohl zeitlich als auch inhaltlich verstanden werden. Die besseren Gründe sprechen jedoch dafür, „im Rahmen" als inhaltliches Kriterium zu begreifen. Daraus folgt, dass die jeweilige Publika-

tion nicht während der Laufzeit der Forschung veröffentlicht werden muss. Ein gegenteiliges Verständnis würde die Norm in einem Maße beschränken, das ihrem Zweck zuwider liefe. Da regelmäßig Forschungsergebnisse und nicht bloß Zwischenstände publiziert werden, würde sonst die weit überwiegende Anzahl von Publikationen aus dem Anwendungsbereich der Norm herausfallen. Insofern ist lediglich zu verlangen, dass der Beitrag im unmittelbaren inhaltlichen Zusammenhang mit der jeweiligen Forschungstätigkeit steht.

Ein weiteres von der Publikation zu erfüllendes Kriterium liegt darin, dass sie im Rahmen einer zumindest zur Hälfte mit öffentlichen Mitteln geförderten Forschungstätigkeit entstanden sein muss. Blickt man auf das hitzig geführte Gesetzgebungsverfahren und vorangegangene in der Diskussion befindliche Formulierungsvorschläge, wird ersichtlich, dass es sich hierbei um eine den Anwendungsbereich beschränkende Voraussetzung handelt. Es sind ausschließlich Forschungstätigkeiten erfasst, die im Rahmen der öffentlichen Projektförderung oder an einer institutionell geförderten außeruniversitären Forschungseinrichtung durchgeführt werden. Der Gesetzgeber geht davon aus, dass hier ein weitergehendes öffentliches Interesse an den Forschungsergebnissen besteht als bei rein universitärer Forschung. Rein universitäre Forschung und deren Ergebnisse sind somit nämlich vom Zweitveröffentlichungsrecht ausgenommen. Der Bundesrat, aber auch die juristische Literatur üben scharfe Kritik an dieser Limitierung des Zweitveröffentlichungsrechts und plädieren für eine verfassungskonforme Auslegung. Durch eine verfassungskonforme Auslegung soll das gesamte wissenschaftliche Personal erfasst sein. Der Kritik ist darin beizupflichten, dass die Norm tatsächlich zu einer Ungleichheit führt, deren angeführter sachlicher Grund nicht zu überzeugen vermag. Auch die universitäre Forschung kann einen erheblichen Beitrag für die Forschung leisten, ohne dass es auf weitere Geldgeber ankommt. Rechtssicherheit verspricht derzeit allerdings nur eine öffentliche Zugänglichmachung von Artikeln, die im Rahmen von Drittmittelprojekten oder an außeruniversitären Einrichtungen entstanden sind.

Der wissenschaftliche Beitrag muss des Weiteren in einer periodisch mindestens zweimal jährlich erscheinenden Sammlung erschienen sein. Darunter können alle wissenschaftlichen Zeitschriften verstanden werden. Nicht umfasst sind – zumindest in aller Regel – Schriftenreihen, Monographien, Kommentare oder Tagungsbände. Außerdem ist zu beachten, dass die Sammlung unter Geltung des Zweitveröffentlichungsrechts erschienen sein muss – also frühestens am 1.1.2014.

III. Einschränkungen

Sollte die wissenschaftliche Publikation als Werk i.S.d. § 38 Abs. 4 UrhG bewertet werden können, müssen in einem nächsten Schritt die von der Norm vorgegebenen Einschränkungen beachtet werden. Diese Einschränkungen dienen überwiegend den Interessen der Wissenschaftsverlage und verfolgen das Ziel eines Interessenausgleichs.

Eine wesentliche Einschränkung ergibt sich daraus, dass die Zweitveröffentlichung keinem gewerblichen Zweck dienen darf. Es dürfen folglich keine Honorarzahlung oder andere geldwerte Vorteile eingestrichen werden. Im Übrigen darf auch das Webangebot, wo die Zweitveröffentlichung erfolgt, keinen gewerblichen Zweck verfolgen. Diese Feststellung kann in manchen Fällen schwierig sein, etwa wenn das Webangebot von einem (anderen) Verlag mit kostenfreiem Zugang betrieben wird. Hier stellt sich bereits die Frage, ob der Autor nicht gegen vertragliche Nebenpflichten verstößt, wenn er das Werk dort hochlädt. Letztlich sind die Universitäten gefragt: Diese sollen – nach der Vorstellung des Gesetzgebers – entsprechende Portale einrichten und etablieren. Die Intention des Autors muss es sein, der Wissenschaft und Allgemeinheit die Forschungsergebnisse zur Förderung weiterer Forschung zur Verfügung zu stellen.

Der Gesetzgeber hat zudem eine Sperrfrist für die Ausübung des Zweitveröffentlichungsrechts in das Gesetz aufgenommen. Diese beträgt zwölf Monate ab dem Zeitpunkt der Veröffentlichung. Hierbei handelt es sich abermals um ein Zugeständnis an die Verleger, die die mit der Publikation verbundenen Kosten zunächst amortisieren können sollen. Insofern können Autoren frühestens seit dem 1.1.2015 erstmals von ihrem möglichen Zweitveröffentlichungsrecht Gebrauch machen.

Der Beitrag darf lediglich in der akzeptierten Manuskriptversion öffentlich zugänglich gemacht werden. Folglich dürfen keine Kopien oder Scans des Artikels, wie er in der Sammlung erschienen ist, eingestellt werden. Das vom jeweiligen Verlag genutzte Layout darf nicht genutzt und somit dürfen auch keine Druckfahnen zur Verfügung gestellt werden. Allerdings ist es zulässig – und wegen der Zitierfähigkeit des Beitrags sogar geboten –, kenntlich zu machen, welcher Seitenzahl der jeweilige Abschnitt zugeordnet werden kann. Dies kann durch Seitenumbrüche oder ähnliche Funktionen von Textverarbeitungsprogrammen erreicht werden. Weiterhin dürfen und sollten mit dem Verlag abgestimmte Änderungen und Überarbeitungen in das hochgeladene Manuskript eingearbeitet sein, um Unstimmigkeiten zwischen dem in der Sammlung erschienenen und dem öffentlich zugänglichen Dokument zu vermeiden.

IV. Fazit

Sind sämtliche der Voraussetzungen erfüllt und werden die Einschränkungen berücksichtigt, ist der Weg für eine Zweitveröffentlichung frei. „Open Access“ kann somit Einzug in die deutsche Wissenschaft halten. Die Manuskripte können zur freien Verfügung in das Internet hochgeladen werden.

Mit § 38 Abs. 4 UrhG existiert eine neue Vorschrift, die das Urheberrecht an das digitale Leben anpassen soll und der Wissenschaftsförderung dient. Es handelt sich dabei um eine Kompromisslösung, mit der sowohl Wissenschaftler als auch Verlage leben können. Ärgerlich ist jedoch die Beschränkung auf im Rahmen außeruniversitärer Forschung oder von Drittmittelprojekten entstandener Beiträge. Dies sorgt neben der beschränkten Verfügbarkeit der Forschungsergebnisse zugleich für eine vermeidbare Ungleichbehandlung der Hochschulmitarbeiter, deren sachliche Begründung nicht zu überzeugen vermag.

Der Spielball liegt nun bei den Ländern und Universitäten. Diese haben entsprechende Plattformen zu errichten, die es Wissenschaftlern ermöglichen, ihre Beiträge fachbezogen und ohne großen Aufwand zur freien Verfügung zu stellen. Weiterhin müssen diese Portale so strukturiert sein, dass die Werke seitens der Nutzer auch unkompliziert aufgefunden werden können. Es ist daher an die Universitäten zu appellieren, sich möglichst rasch dem Aufbau entsprechender Strukturen zu widmen. Das zu verfolgende Ziel muss eine „One-stop-Plattform“ sein, auf der sämtliche Werke aufzufinden sind. Eine Zersplitterung sollte vermieden werden, will man das hart erkämpfte Zweitveröffentlichungsrecht nicht selbst entwerten. Denkbar sind auch fachbezogene Portale, die jedoch mit einer großen Open-Access-Suchplattform kombiniert werden könnten.

Weiterhin muss die „frohe Kunde“ auch an die Hochschulmitarbeiter herangetragen werden. Nur Hochschulmitarbeiter, die sich der neuen Rechtslage bewusst sind, können und werden ihr Zweitveröffentlichungsrecht auch tatsächlich nutzen. Die Justiziariate sind daher aufgerufen, entsprechende Schulungen und Checklisten zu erstellen. Insbesondere die Nachricht, dass es sich bei dem Zweitveröffentlichungsrecht um ein unabdingbares Recht handelt – also ein Recht, das der Verlag nicht ausschließen oder einschränken kann –, muss sich bei den Wissenschaftlern verbreiten.

Noch steht „Open Access“ in der Hochschullandschaft am Anfang – sofern Universitäten, Hochschulmitarbeiter und Nutzer die Chancen des Zweitveröffentlichungsrechts nutzen, könnte es jedoch nicht weniger als den Startschuss für einen einschneidenden Wandel in der Wissensverbreitung bedeuten. ◆

Übersicht über die Mitgliedseinrichtungen und Organe des DFN-Vereins

(Stand: 05/2015)

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 Organe des DFN-Vereins sind:

die Mitgliederversammlung
der Verwaltungsrat
der Vorstand

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 11. 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)

Prof. Dr. Ulrike Gutheil
(Technische Universität Berlin)

Dir. u. Prof. Dr. Siegfried Hackel
(Physikalisch-Technische Bundesanstalt Braunschweig)

Dr.-Ing. habil. Carlos Härtel
(GE Global Research)

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

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

Prof. Dr. Peter Schirmbacher
(Humboldt-Universität zu Berlin)

Prof. Dr. Horst Stenzel
(Fachhochschule Köln)

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

Dr. Harald Ziegler
(Friedrich-Schiller-Universität Jena)

Der Verwaltungsrat hat als ständige Gäste

einen Vertreter der Hochschulrektorenkonferenz:

Herr Prof. Dr. Andreas Bertram
(Präsident der Hochschule Osnabrück)

einen Vertreter der Hochschulkanzler:

Herr Christian Zens
(Kanzler der Stiftung Europa-Universität Viadrina, Frankfurt/Oder)

einen Vertreter der Kultusministerkonferenz:

Herr Jürgen Grothe
(SMWK Dresden)

den Vorsitzenden der jeweils letzten Mitgliederversammlung:

Herr Prof. Dr. Gerhard Peter
(Hochschule Heilbronn)

den Vorsitzenden des ZKI:

Herr Martin Wimmer
(Universität Regensburg)

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

Prof. Dr. Ulrike Gutheil
Stellv. Vorsitzende

Dr. Rainer Bockholt
Stellv. Vorsitzender

Der Vorstand wird beraten von einem Technologie-Ausschuss (TA), einem Betriebsausschuss (BA) und einem Ausschuss für Recht und Sicherheit (ARuS), der zugleich auch als Jugendschutzbeauftragter für das DFN fungiert.

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.

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Albstadt	Hochschule Albstadt-Sigmaringen (FH)
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Hochschule Aschaffenburg
Augsburg	Hochschule für angewandte Wissenschaften, Fachhochschule Augsburg
	Universität Augsburg
Bad Homburg	Dimension Data Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	BBB Management GmbH
	Beuth Hochschule für Technik Berlin – University of Applied Sciences
	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
	Bundesanstalt für Materialforschung und -prüfung
	Bundesinstitut für Risikobewertung
	Deutsche Telekom AG Laboratories
	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)
	T-Systems International GmbH
	Umweltbundesamt
	Universität der Künste Berlin
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum Berlin für Sozialforschung gGmbH (WZB)
Biberach	Hochschule Biberach
Bielefeld	Fachhochschule Bielefeld
	Universität Bielefeld
Bingen	Fachhochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Fachhochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Fachhochschule Georg Agricola für Rohstoff, Energie und Umwelt zu Bochum
Bonn	Bundesministerium des Innern
	Bundesministerium für Umwelt, Naturschutz, Bau u. Reaktorsicherheit
	Deutsche Forschungsgemeinschaft (DFG)
	Deutscher Akademischer Austauschdienst e. V. (DAAD)
	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	Rheinische Friedrich-Wilhelms-Universität Bonn
	Zentrum für Informationsverarbeitung und Informationstechnik
Borstel	FZB, Leibniz-Zentrum für Medizin und Biowissenschaften
Brandenburg	Fachhochschule Brandenburg
Braunschweig	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
	Stadtbildstelle Bremerhaven
Chemnitz	Technische Universität Chemnitz
	TUCed – Institut für Weiterbildung GmbH
Clausthal	Clausthaler Umwelttechnik-Institut GmbH (CUTEC)
	Technische Universität Clausthal-Zellerfeld
Coburg	Hochschule für angewandte Wissenschaften, Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus-Senftenberg
Darmstadt	European Space Agency (ESA)
	Evangelische Hochschule Darmstadt
	GSI Helmholtzzentrum für Schwerionenforschung GmbH
	Hochschule Darmstadt
	Merck KGaA
	Technische Universität Darmstadt
	T-Systems International GmbH
Deggendorf	Hochschule für angewandte Wissenschaften, Fachhochschule Deggendorf
Dortmund	Fachhochschule Dortmund
	Technische Universität Dortmund
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
Düsseldorf	Fachhochschule Düsseldorf
	Heinrich-Heine-Universität Düsseldorf
	Information und Technik Nordrhein-Westfalen (IT.NRW)
	Kunstakademie Düsseldorf
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Hochschule Emden/Leer
Erfurt	Fachhochschule Erfurt
	Universität Erfurt

Erlangen	Friedrich-Alexander-Universität Erlangen-Nürnberg
Essen	Rheinisch-Westfälisches Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Fachhochschule Flensburg
	Universität 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
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	Ernst-Moritz-Arndt-Universität Greifswald
	Friedrich-Loeffler-Institut, Bundesforschungsinstitut für Tiergesundheit
Hagen	Fachhochschule Südwestfalen, Hochschule für Technik und Wirtschaft
	FernUniversität in Hagen
Halle/Saale	Institut für Wirtschaftsforschung Halle
	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-Harburg
	Universität Hamburg
Hameln	Hochschule Weserbergland
Hamm	SRH Hochschule für Logistik und Wirtschaft Hamm
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe
	Hochschule Hannover
	Gottfried Wilhelm Leibniz Bibliothek – Niedersächsische Landesbibliothek
	Gottfried Wilhelm Leibniz Universität Hannover
	HIS Hochschul-Informations-System GmbH
	Hochschule für Musik, Theater und Medien
	Landesamt für Bergbau, Energie und Geologie
	Medizinische Hochschule Hannover
	Technische Informationsbibliothek und Universitätsbibliothek
	Stiftung Tierärztliche Hochschule
Heide	Fachhochschule Westküste, Hochschule für Wirtschaft und Technik
Heidelberg	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	Network Laboratories NEC Europe Ltd.
	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
Ilmenau	Bundesanstalt für IT-Dienstleistungen im Geschäftsbereich des BMVBS
	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 Altersforschung – Fritz-Lipmann-Institut e. V. (FLI)
Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Fachhochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	Fachinformationszentrum Karlsruhe (FIZ)
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe – Technik und Wirtschaft
	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
	Fachhochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Katholische Hochschule Nordrhein-Westfalen
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln gGmbH
	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	Hochschule Ostwestfalen-Lippe
Lübeck	Fachhochschule Lübeck
	Universität zu Lübeck
Ludwigsburg	Evangelische Hochschule Ludwigsburg
Ludwigshafen	Fachhochschule Ludwigshafen am Rhein
Lüneburg	Leuphana Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Leibniz-Institut für Neurobiologie Magdeburg
Mainz	Fachhochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Universität Koblenz-Landau
Mannheim	Hochschule Mannheim
	TÜV SÜD Energietechnik GmbH Baden-Württemberg
	Universität Mannheim
	Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW)
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Philipps-Universität Marburg
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 München (FH)
	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.
	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, Fachhochschule
Oldenburg	Carl von Ossietzky Universität Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück (FH)
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Deutsche Gesellschaft zum Bau und Betrieb von Endlagern für Abfallstoffe mbH
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
Rosenheim	Hochschule für angewandte Wissenschaften – Fachhochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn Rhein-Sieg
Schmalkalden	Fachhochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Siegen	Universität Siegen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Fachhochschule 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	Hochschule Ulm
	Universität Ulm
Vechta	Universität Vechta
	Private Fachhochschule für Wirtschaft und Technik
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 Solutions for Research GmbH
Wiesbaden	Hochschule RheinMain
	Statistisches Bundesamt
Wildau	Technische Hochschule Wildau (FH)
Wilhelmshaven	Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth

Wismar	Hochschule Wismar
Witten	Private Universität Witten/Herdecke gGmbH
Wolfenbüttel	Ostfalia Hochschule für angewandte Wissenschaften
	Herzog August Bibliothek
Worms	Hochschule Worms
Wuppertal	Bergische Universität Wuppertal
Würzburg	Hochschule für angewandte Wissenschaften – Fachhochschule Würzburg-Schweinfurt
	Julius-Maximilians-Universität Würzburg
Zittau	Hochschule Zittau/Görlitz
Zwickau	Westsächsische Hochschule Zwickau