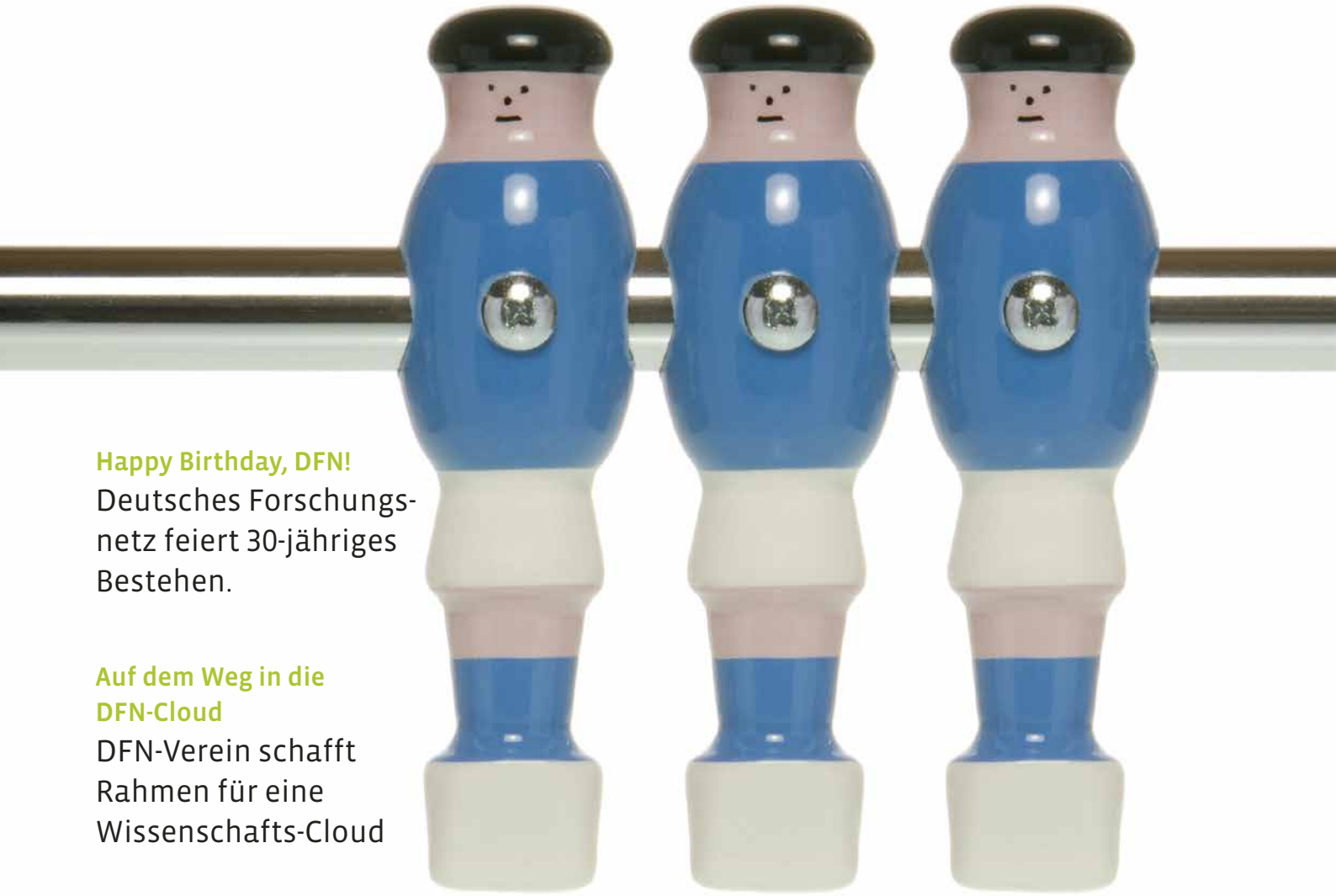
Deutsches Forschungsnetz Mitteilungen Ausgabe 86 | Mai 2014
www.dfn.de

DFN

Mitteilungen



Happy Birthday, DFN!
Deutsches Forschungsnetz feiert 30-jähriges Bestehen.

Auf dem Weg in die DFN-Cloud
DFN-Verein schafft Rahmen für eine Wissenschafts-Cloud

Per Superchannel durch das X-WiN

Start des DFN-Terabit-Testbeds erfolgreich!

9 770177 689001

Impressum

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

DFN-Verein
Alexanderplatz 1, 10178 Berlin
Tel.: 030 - 88 42 99 - 0
Fax: 030 - 88 42 99 - 70
Mail: dfn-verein@dfn.de
Web: www.dfn.de

ISSN 0177-6894

Redaktion: Kai Hoelzner (kh)
Gestaltung: Labor3 | www.labor3.com
Druck: Rüss, Potsdam

Fotonachweis:
Titelfoto © Markus Brunner - Imagebroker/F1-online
Seite 4 © Torsten Kersting
Seite 6/7 © DerProjektor/photocase.de
Seite 32/33 © fotofilia/photocase.de

Prof. em. Dr. Eike Jessen
Gründungsvorstand des DFN-Vereins

30 Jahre Deutsches Forschungsnetz – der Erfolg einer Gemeinschaft

30 Jahre Deutsches Forschungsnetz – die Gründungsversammlung am 30. März 1984 in Birlinghoven ließ kaum ahnen, was DFN einmal sein würde, Deutschland lag in der Nutzung von Netzen etwa vier Jahre zurück gegen die USA und gegen England. Die am Markt tätigen Hersteller versuchten im kommenden DFN ihre Domänen, ihre Netzarchitekturen durchzubringen, die Vielfalt der Rechnerausstattungen in der Wirtschaft nicht respektierend. Sehr wohl gab es lokale Erfahrungen in der Wissenschaft mit Aufbau und Betrieb von Netzen, so etwa in Berlin (Ost und West!), in Dresden, in Karlsruhe und in der D(FV)LR.

Die führenden Netze anderer Länder waren durch weitsichtige Behörden, so z.B. das Department of Defense, die National Science Foundation oder – in Großbritannien – schlicht durch königliches Dekret gestartet worden. Auch im Bundesministerium für Forschung und Technologie wurde die Notwendigkeit klar erkannt, ein Netz für die Wissenschaft in Deutschland bereitzustellen.

So kam es am 30. März 1984 in Gegenwart des Bundesforschungsministers Dr. Heinz Riesenhuber zum Gründungsakt für den Verein zur Förderung eines Deutschen Forschungsnetzes. Auf die Sachkunde und Verantwortung seiner Mitglieder gegründet wurde mit der Vereinsform eine organisatorische Struktur erschaffen, die sich – allein ein Blick auf die Entwicklung der im Netz verfügbaren Bandbreiten von damals 9,6 Kilobit/s auf heute 100 Gigabit/s zeigt dies – nicht nur politisch, sondern auch technisch in großartiger Weise bewährt hat. Ähnliche Prinzipien der Selbstverantwortung der Anwender wurden in den USA erst Mitte der 90er Jahre durch das Internet2 aufgenommen.

Der „DFN-Verein“ erwies sich als flexibel genug, um für über 350 Mitglieder eine entscheidungs- und handlungsfähige Basis zu entwickeln, die im Jahr 2000 das Wissenschaftsnetz in die Spitze der Technologie aufsteigen ließ und es nach Transportvolumen und Zahl der Benutzer zum größten Wissenschaftsnetz der Erde machte.

Natürlich haben wir im DFN auch einfach Glück gehabt. Da waren die Vielen, die Verantwortung im DFN übernahmen, aber zugleich Verantwortung trugen in den Wissenschaftseinrichtungen, in der Wirtschaft und in den Organisationen der DV-Infrastruktur, wie der Arbeitskreis der Leiter wissenschaftlicher Rechenzentren (ALWR) und die Zentren für Kommunikation und Informationsverarbeitung (ZKI). Auch als die Bundesregierung sich 2002 aus der „Fehlbedarfsfinanzierung“ des Netzes zurückzog, erlaubten uns die von der Wirtschaft im Internet-Hype aufgebauten großen Leitungskapazitäten den schnell ansteigenden Kommunikationsbedarf der Wissenschaft ohne Kostenerhöhung zu decken. Als eines der ersten europäischen Wissenschaftsnetze hat das DFN bereits Anfang des vergangenen Jahrzehnts auf wirtschaftlich eigenen Füßen gestanden. Damit einher ging die frühzeitige Beschaffung eigener Leitungskapazitäten zu Gunsten maximaler Nachhaltigkeit und der Möglichkeit, technische Innovationen zum jeweils frühestmöglichen Zeitpunkt implementieren zu können.

Die Organisation und das Management-Schema des DFN erwies sich ebenso tüchtig, als 1989 die neuen Bundesländer dem DFN beitraten und als 1994 die Trägerorganisation für das europäische Wissenschaftsnetz GEANT, DANTE zu gründen war, eine Entwicklung, die für immer mit dem Namen von Klaus Ullmann verbunden ist.

So kann man dem Geburtstagskind mit großem Recht gratulieren, nicht ohne dass wir DFNs uns alle väterlich auf die Schulter klopfen und rufen „weiter so!“.

Unsere Autoren dieser Ausgabe im Überblick

1 Kai Hoelzner, DFN-Verein (hoelzner@dfn.de); **2** Dr. Christian Grimm, DFN-Verein (grimm@dfn.de); **3** Jochem Pattloch, DFN-Verein (pat@dfn.de); **4** Michael Röder, DFN-Verein (roeder@dfn.de); **5** Robert Stoy, DFN-Verein (stoy@noc.dfn.de)
6 Roland Karch, Friedrich-Alexander-Universität Erlangen-Nürnberg (roland.karch@fau.de); **7** Anna Roth, DFN-Verein (presse@dfn.de);
8 Prof. Dr.-Ing. Erwin P. Rathgeb, Universität Duisburg-Essen (erwin.rathgeb@uni-due.de);
9 Dirk Hoffstadt, Universität Duisburg-Essen (dirk.hoffstadt@uni-due.de);
10 Prof. Dr. Marcel Waldvogel, Universität Konstanz (marcel.waldvogel@uni-konstanz.de);
11 Klaus Herberth, Universität Konstanz (klaus.herberth@uni-konstanz.de);
12 Daniel Scharon, Universität Konstanz (daniel.scharon@uni-konstanz.de);
13 Jürgen Brauckmann, DFN-CERT GmbH (brauckmann@dfn-cert.de);
14 Reimer Karlsen-Masur, DFN-CERT GmbH (karlsen-masur@dfn-cert.de);
15 Dr. Ralf Gröper, DFN-Verein (groeper@dfn.de); **16** Susanne Thinius, Forschungsstelle Recht im DFN (recht@dfn.de); **17** Julian Fischer, Forschungsstelle Recht im DFN (recht@dfn.de)

Inhalt


557

Wissenschaftsnetz

30 Jahre DFN

Text: **Kai Hoelzner** (DFN-Verein)

Der Verein zur Förderung eines Deutschen Forschungsnetzes e. V. feiert in diesem Jahr sein 30-jähriges Bestehen. Seit seiner Gründung im Jahr 1984 gehört der DFN-Verein zu den Kräften, die bei der Verbreitung der Datenkommunikation in Deutschland Maßstäbe gesetzt haben.

Rechner und Netze haben seither die Wissenschaft in einer Weise verändert, die in den Gründungstagen des DFN-Vereins kaum zu erahnen war. Die enormen Datenmengen, mit denen Wissenschaftler heute umgehen, erfordern zwingend, geeignete Infrastrukturen in Form von Rechenkapazitäten, Speichern und Netzen aufzubauen, um Wissen verfügbar und bearbeitbar zu halten. Den beiden klassischen Erkenntniswegen Theorie und Empirie hat sich dabei in vielen Disziplinen der Wissenschaft ein dritter Erkenntnisweg hinzugesellt, der die gegenseitige Abhängigkeit von Theoriebildung und empirischer Beobachtung um einen Drittes – die Simulation – erweitert. Kaum ein Forschungsprojekt kommt heute ohne Simulation und Modellierung aus. Sei es in der Astrophysik, der Genetik, der Teilchenphysik oder in der Medizin. Das Potenzial von Rechnern, Erkenntnis durch Simulation und Modellierung zu befördern und das Potenzial von Netzen, die dafür nötigen Ressourcen wie auch die Ergebnisse ubiquitär verfügbar zu machen, führt derzeit in einer Vielzahl von Wissenschaftsprojekten zu großen Fortschritten.

Mit dem DFN als technologische und organisatorische Plattform haben sich die im DFN-Verein organisierten 320 Hochschulen und außeruniversitären Wissenschaftseinrichtungen in Deutschland eine technologische und zugleich organisatorische Plattform erschaffen, die sich jenseits von politischer Bevormundung und industrieller Einflussnahme ausschließlich an den Bedarfen und Visionen der Wissenschaft orientiert.

Eine ganze Generationenfolge von Wissenschaftsnetzen – angefangen mit dem x.25-Wissenschaftsnetz, dem Breitbandwissenschaftsnetz B-WiN, seinem Nachfolger, dem G-WiN, mit dem zum ersten Mal die Gigabitschwelle in der Datenkommunikation durchstoßen wurde, bis hin zum heutigen X-WiN, dessen Leistungsfähigkeit seit 2004 fortlaufend gesteigert und an die Bedarfe in der Wissenschaft angepasst wird – stellt die technische Grundlage für den Erfolg des DFN dar.

Mit Anschlusskapazitäten von bis zu 100 Gigabit/s und einem Terabit-fähigen Kernnetz, das sich zwischen 60 Kernnetz-Standorten aufspannt, zählt das vom DFN-Verein betriebene Wissenschaftsnetz X-WiN heute zu den leistungsfähigsten Kommunikationsnetzen weltweit. 11.000 Kilometer Glasfaser liegen in der betrieblichen Ver-

Foto: © Ruth Black/iStock

antwortung des DFN-Vereins. Mit der Geschäftsstelle des DFN-Vereins in Berlin und einer Reihe spezialisierter Teams wie dem Network Operation Center ‚DFN-NOC' in Stuttgart, dem DFN-CERT in Hamburg, dem DFN-Labor in Erlangen oder der DFN-Forschungsstelle Recht an der Universität Münster versorgt der DFN-Verein seine Mitglieder und Anwender nicht nur mit hoch leistungsfähigen Anschlüssen an das Wissenschaftsnetz, Internet-Services oder netznahen Dienstleistungen, sondern unterstützt sie in vielfältiger Weise in allen Fragen, die die Nutzung und Nutzbarmachung von Netztechnologien in der Wissenschaft betreffen.

Auf Basis dieser technologischen und organisatorischen Plattform hat der DFN-Verein eine Vielzahl von Diensten und Services entwickelt, die den Anwendern mit dem Anschluss an das Wissenschaftsnetz zur Verfügung stehen. Von DFNRoaming und DFN-MailSupport über DFN-PKI und DFN-AAI bis hin zum Videokonferenzdienst des DFN, dem DFNFernsprechen oder spezialisierten Diensten und Services wie DFN-SAP oder DFN-VPN stehen den Nutzern eine Fülle von Diensten zur Verfügung, die in den meisten Fällen im Entgelt für einen X-WiN-Anschluss enthalten sind. Diese Dienststruktur stellt im Deutschen Forschungsnetz das Getriebe dar, mit dem die Potenziale des Wissenschaftsnetzes für die Anwender in vielfältiger Weise nutzbar werden.

Das Netz und die Dienste des DFN stellen – gemeinsam mit einer Vielzahl von Partnernetzen, die in einem globalen Verbund von Wissenschaftsnetzen miteinander verknüpft sind – eine technologische Plattform dar, mit der wissenschaftliche Ressourcen weltweit nutzbar gemacht werden. Dabei richtet sich der Fokus der Mitglieder, Mitstreiter und Mitarbeiter des DFN mit unvermindertem Engagement auf künftige Herausforderungen. Im Februar dieses Jahres startete das vom DFN-Verein ins Leben gerufene DFN-Terabit-Testbed, mit dem die Tür für Datenübertragungen im Multi-Terabit-Bereich aufgestoßen wurde. Parallel dazu wird im DFN-Verein derzeit ein Modell für eine DFN-Cloud entwickelt, die es Mitgliedseinrichtungen erlaubt, sich technische Ressourcen und Kompetenzen untereinander zur Verfügung zu stellen. Der DFN-Verein schafft hierfür einen Rahmen, innerhalb dessen Cloud-Dienste im ganzen DFN genutzt werden können.

Das frühzeitige Engagement des DFN-Vereins für die Weiterentwicklung von Netz und Diensten ist immer wieder Ergebnis eines breit angelegten und tiefgreifenden Willensbildungsprozesses, der durch die Mitglieder im DFN-Verein initiiert und vorangetrieben wird. In der Regel geht der Entwicklung eines Dienstes eine Initiative besonders engagierter Mitglieder in den Vereinsgremien voraus.

Kennzeichnend für die vom DFN-Verein erschaffene Infrastruktur und die darauf entwickelten Dienste und Services ist aber nicht allein deren organisatorische und technische Verankerung in der nationalen Wissenschafts-Community, sondern auch die europa- und weltweite Integration der technischen Infrastruktur und die internationale Harmonisierung der Dienste. So sind vom DFN-Verein angebotene Dienste wie DFN-Roaming oder Videoconferencing international nutzbar. Eine Reihe von internationalen Initiativen wie die vom DFN in die Wissenschaftsnetze der Nachbarstaaten eingerichteten Cross-Border-Fibres, die zusätzlich zum zu den GÉANT-Anschlüssen des X-WiN Kapazitäten für grenzübergreifende VPNs bereitstellen, aber auch die Mitarbeit in einer Reihe von europäischen Integrationsprojekten wie der Föderationsinitiative eduGAIN, dank derer sich die DFN-AAI europaweit nutzen lässt, fördert die Weiterentwicklung des DFN auf nationaler und internationaler Ebene. Schließlich ist an dieser Stelle auch der Transfer von nationalen Entwicklungen wie dem Überwachungs-Tool PerfSONAR zu erwähnen. Einstmals für den Gebrauch im G-WiN entwickelt wird perfSONAR heute im europäischen Wissenschaftsnetz und in einer Reihe von Partnernetzen eingesetzt und unter europäischer Beteiligung weiterentwickelt. Umgekehrt finden sich im DFN-Portfolio Dienste wie etwa der DFN-Terminplaner, der zunächst von europäischen Partnern aufgesetzt wurde und heute auf nationaler Ebene weiterentwickelt wird.

Netz und Dienste des DFN-Vereins sind heute gleichermaßen tief in die nationale Community wie in den internationalen Verbund der Wissenschaftsnetze integriert. Die Bedeutung, die das DFN für die Wissenschaft erlangt hat, ergab sich hierbei weder natürlich, noch auf irgendeine Form äußerer Vorgabe, sondern entspringt in ihrem Innersten dem Streben der Wissenschaft, Datenkommunikation und ihren Nutzen für die Wissenschaft selbstbestimmt zu entwickeln und voranzutreiben.

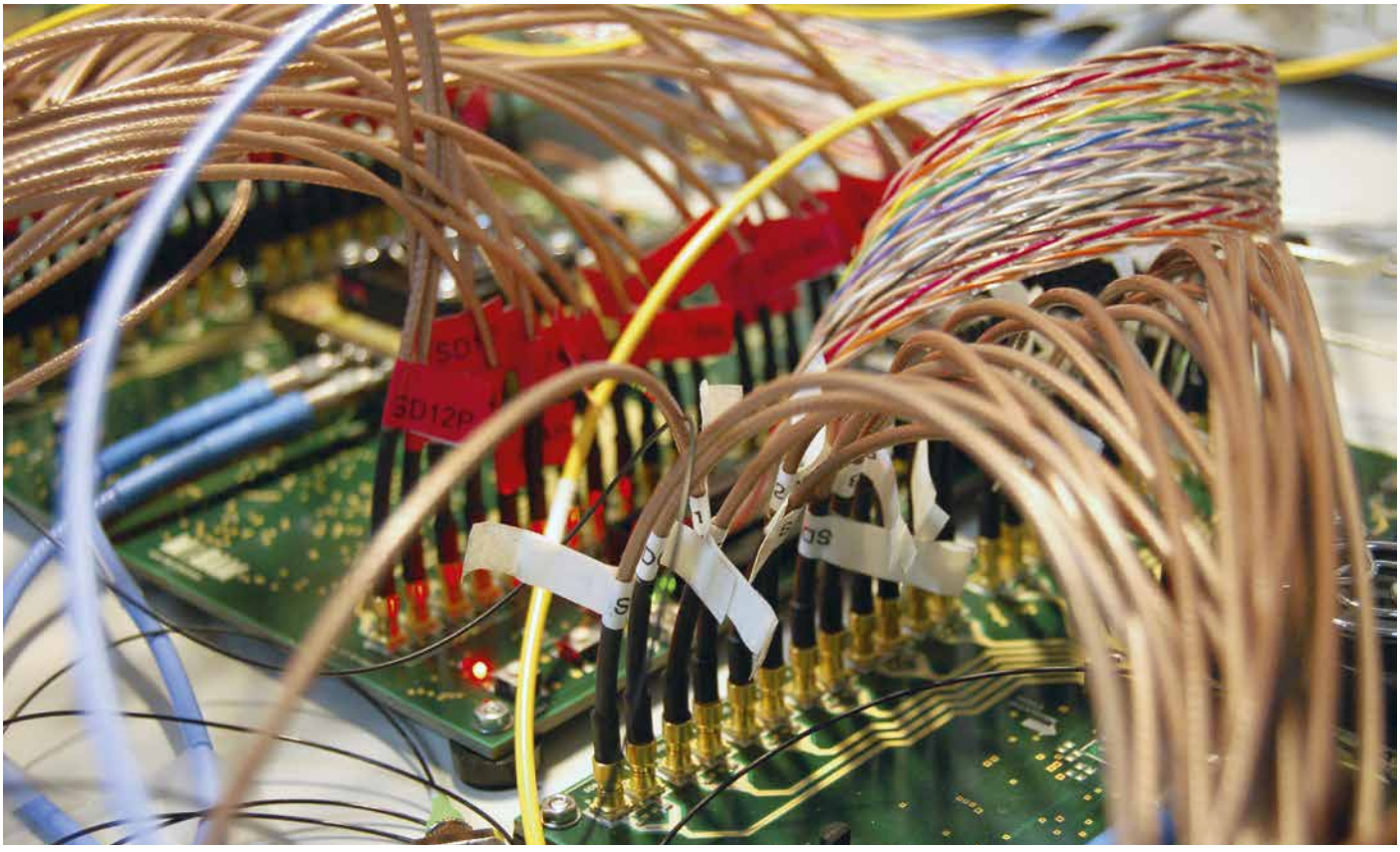
Die Bedeutung, die das Deutsche Forschungsnetz für Mitglieder und Anwender in den vergangenen drei Jahrzehnten gewonnen hat, hängt wesentlich mit der besonderen Verfasstheit seiner Mitglieder zusammen, die sich nicht allein mit großem Engagement frühzeitig mit neuen Themen und Technologien auseinandersetzen, sondern die auch bereit sind, eigene Interessen in einem breit angelegten Willensbildungsprozess mit Gemeinschaftsinteressen abzugleichen.

Nicht zuletzt ist es aber die Kompetenz einer aus vielen hundert Mitstreitern bestehenden Community, die sich im DFN-Verein bündelt und wirksam wird und die bis heute ein Garant für ein besonderes Maß an Qualität von Netz und Diensten ist. Der inzwischen drei Jahrzehnte fortdauernde Erfolg des DFN, die jüngsten Entwicklungen bei Netz und Diensten und schließlich das niemals nachlassende Engagement seiner Mitglieder und Anwender können als positives Zeichen gelesen werden für die künftige Entwicklung des Deutschen Forschungsnetzes. ◆

Per Superchannel durch das X-WiN – Start des DFN-Terabit-Testbeds erfolgreich!

Die im Deutschen Forschungsnetz organisierten wissenschaftlichen Einrichtungen zünden bei ihrem selbst organisierten Datennetz, dem Wissenschaftsnetz X-WiN, die nächste Leistungsstufe. Mit dem DFN-Terabit-Testbed erprobt der DFN-Verein derzeit Verbindungen mit einer Bandbreite von 1 Terabit/s. Ein erster erfolgreicher Test zur Datenübertragung mit Terabit-Technologie fand am 26. Februar 2014 auf einer Kernnetz-Strecke des X-WiN zwischen der Technischen Universität Dresden und der Bergakademie Freiberg statt.

Text: **Kai Hoelzner** (DFN-Verein)



Detail einer Transceiver-Platine des Testaufbaus für das DFN-Terabit-Testbed.

Terabit im Feldversuch

Wie in einer Wellenbewegung erstarrt verbinden kupferne Kabel, vielfarbige Litzen und gelb ummantelte Fasern ein Tableau waldgrüner Platinen, die am X-WiN-Standort im Rechenzentrum der Technischen Universität Dresden zu einem allersten Prototyp eines Terabit-Transponders aufgebaut sind. Dahinter türmen sich schon in schützende Stahlgehäuse verbaute Elemente, Messgeräte und Monitore, mit denen seit dem frühen Morgen bereits die Faser eingemessen und immer wieder Feinjustierungen des aufmodulierten Datensignals vorgenommen wurden. Das geordnete Chaos auf der lichtgrauen Tischplatte, die für gewöhnlich ein Telefon und höchsten einmal die Tasche eines Rechenzentrum-Mitarbeiters zu tragen hat, ist nichts anderes als das Innenleben der nächsten, superschnellen Transponder-Generation, mit der das Wissenschaftsnetz in einigen Jahren einmal ausgestattet sein wird.

Bis dahin aber ist es noch ein langer Weg. Ein Weg, dessen erste Kilometer an diesem Vormittag über einen ca. sechzig Kilometer langen Faser-Abschnitt des Deutschen Forschungsnetzes führen, der den Standort Dresden mit dem frisch eingerichteten Kernnetzknoten an der TU Bergakademie Freiberg verbindet. Es ist der 26. Februar 2014 und ziemlich genau um 12 Uhr Ortszeit werden hier in Dresden erstmals Daten mit Terabit-Kapazität in eine Netzwerkschleife geschickt, um innerhalb weniger Millisekunden zur TU Dresden zurückzukehren.

Dafür generiert ein Zufallsgenerator eine Zahlenfolge, die eingespeist in das temporäre Netz-Labor in ein moduliertes Signal verwandelt und von dort über ein unscheinbares Faserpaar in einen der Multiplexer geführt wird, die nebenan in den Einschubschränken ihren Dienst verrichten. Von hier aus geht es mit Terabit-Kapazität über eine gewöhnliche Wellenlänge des X-WiN in Richtung Bergakademie Freiberg und von dort über eine Schleife nonstop zurück ins Dresdner Rechenzentrum.

Gruppenbild nach erfolgreicher Terabit-Übertragung: Das Team aus Mitarbeitern des Tera Santa-Konsortiums, des DFN-Vereins, der TU-Dresden und des KIT Karlsruhe.

Wenige Millisekunden später erreicht der zurückgekehrte Datenstrom den Transceiver, den er eben erst in Gegenrichtung verlassen hat, um wieder in eine lesbare Zahlenfolge aufgelöst zu werden, die, sofern das System einwandfrei arbeitet, identisch mit jener Folge ist, die vor Millisekunden losgeschickt wurde.

Das Team

Nichts was an diesem Morgen auf dem Tisch zu sehen ist, scheint ein Serienbauteil zu sein. Weder die Modulatoren noch Transceiver haben je zuvor mit Terabit-Kapazität gearbeitet. Entwickelt wurden die Prototypen vom israelischen Tera Santa-Konsortium, einem Zusammenschluss vornehmlich israelischer Netzwerkausrüster bzw. deren Zulieferer mit mehreren Spitzenuniversitäten Israels. Neben dem Konsortialführer ECI Telecom – dem aktuellen Netzwerkausrüster des Deutschen Forschungsnetzes – und dem global agierenden Technologie-Zulieferer Finisar besteht Tera Santa aus insgesamt sieben in Israel ansässigen High-Tech-Firmen und fünf Universitäten, die gemeinsam die weltweit ersten „Terabit Orthogonal Frequency Division Mulitplexing“ (OFDM) basierten Netzkomponenten entwickelt haben. Neben ECI und Finisar gehören zu diesem Konsortium auch Orckit Corrigent, MultiPhy, Optiway, Civcom, Bezeq International, das israelische Technologie Institut, die Ben-Gurion Universität, die Hebräische Universität zu Jerusalem, die Bar-Ilan Universität und die Universität von Tel-Aviv.

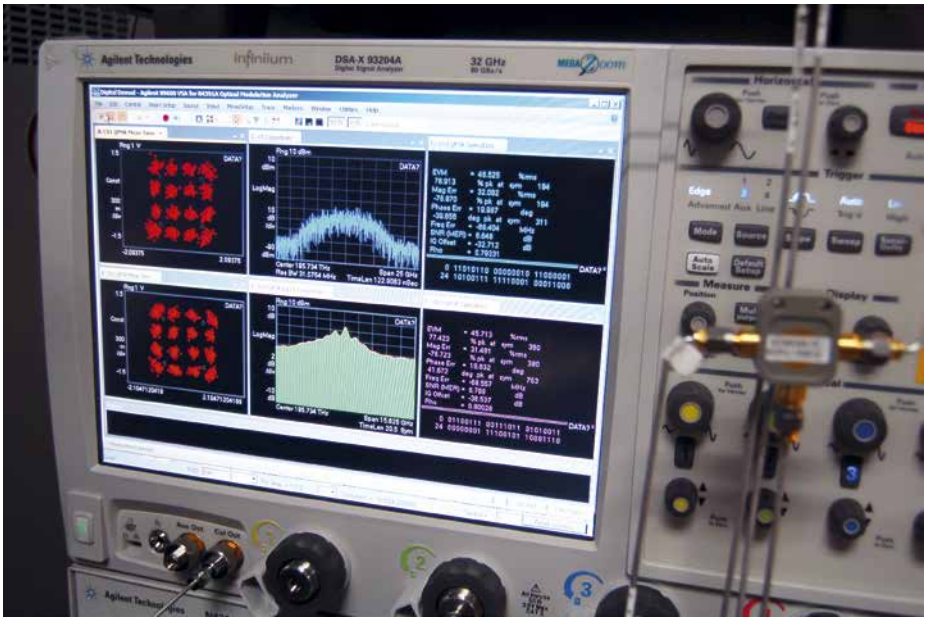
Ein Team des Tera Santa-Konsortiums, Netzwerk-Spezialisten des DFN-Vereins, Mitarbeiter des Rechenzentrums der TU-Dresden sowie zwei in letzter Minute zum Team dazugestoßene Kollegen des Karlsruher Instituts für Technologie sind bereits seit den frühen Morgenstunden damit beschäftigt, die Vielzahl einzelner Komponenten zu verkabeln, Messgeräte anzuschließen und Tests durchzuführen. Insgesamt 15 Techniker drängen sich an diesem Vormittag im nicht gerade weitläufigen Raum, in dem der Kernnetzknoten des X-WiN gehostet wird. Mit vereinten Kräften wollen sie dafür sorgen, dass bei diesem ersten Feldtest der ‚Coherent Terabit Technologie‘, die ECI und das Tera Santa-Konsortium entwickelt haben, die empfangenen Daten identisch mit den versendeten sein werden. Eine zentrale Bedeutung kommt in diesem Zusammenhang einem Monitor zu, auf dem eine Matrix von sechzehn mehr

oder weniger runden Feldern zu erkennen ist, die bei näherem Hinschauen ihrerseits aus vielen einzelnen Pünktchen bestehen. Je klarer die Konturen dieser Punkte, desto sauberer ist die Übertragung der Daten. Wenn auch nur ein kleines Pünktchen seinen Zielbereich auf der Matrix verlässt und sich ins benachbarte Kästchen mogelt, wird das Signal unsauber und kann beim Eintreffen nicht mehr klar detektiert werden.

Mehr Daten dank komplexerer Modulationsmethoden

Das Verfahren, mit dem die Daten auf den informationstragenden Photonenstrom in der Faser moduliert werden, nennt sich ‚QAM16'. QAM steht für Quadraturamplitudenmodulation und bis heute kommt auf den Faserverbindungen der weltweiten Datennetze ausschließlich QAM4 zum Einsatz. Der Sprung von 100-Gigabit- auf Terabit-Kapazität wird wesentlich damit zu tun haben, ob es gelingt, QAM16 in Glasfaser-Architekturen zum Laufen zu bringen. Im Labor ist dies bereits gelungen. Ob die Fasern und die Geräte-Peripherie bestehender Netze geeignet sind, QAM16 auch auf Weitverkehrsstrecken einzusetzen, muss sich am heutigen Tag zeigen. Je höher nämlich die Dichte der Information, desto störanfälliger wird das auf den Lichtleiter aufmodulierte Signal. Und je länger eine Faser ist, desto stärker wird das ‚Rauschen' und desto leichter mogelt sich eins der Pünktchen ins falsche Feld.

Zwei verschiedene Verfahren wurden im Tera Santa-Konsortium für die Realisierung höherer Datendichte vorbereitet. Mittels orthogonaler Frequenzmultiplexverfahren (OFDM) werden die zu übertragenden Daten hierbei auf mehrere Teildatenströme mit niedriger Datenrate aufgeteilt. Diese Teildatenströme werden jeder für sich per Quadraturamplitudenmodulation mit geringer Bandbreite moduliert und anschließend zu Hochfrequenz-OFDM-Signalen umgewandelt und auf einem Superchannel übertragen. Dieser löst das bisherige 50-GHz-Kanalraster der Datenübertragung auf Lichtleitern auf und ersetzt es durch ‚breitere' Frequenzbänder von bis zu 187,5 GHz.



Fortlaufende Messungen zur Überwachung und Analyse des Testsignals.

Hier nun findet sich technisch gesehen die Schnittstelle zur aktuellen Multiplexer-Generation im X-WiN. In den meisten Netzen kommen derzeit ROADM (Reconfigurable Optical Add-Drop Multiplexer) zum Einsatz, die Kanäle ausschließlich im 50-GHz-Raster vermitteln können. Die im X-WiN eingesetzten Geräte der Apollo-Serie von ECI hingegen verfeinern diese Granularität auf minimal 12,5 GHz (sog. Flex-Grid ROADMs) und ermöglichen dadurch eine dichtere Anordnung mit der Folge einer höheren Anzahl von Super-Channels im C-Band.

Das Terabit-Testbed des DFN-Vereins dient nicht allein dem Nachweis, dass Terabit-Übertragungen bereits im heutigen Netz-Ökosystem des DFN möglich sind, sondern auch dafür, verschiedene Implementierungsansätze für die OFDM-Algorithmen zu testen. Bei der sogenannten „Technion-Lösung" werden 1024 OFDM-Träger parallel auf der Spektral-Achse verarbeitet, während die „MultiPhy-Lösung" 128 OFDM-Signale parallel auf der Zeitachse verarbeitet. Als Transceiver kommt dabei ein optischer Software-Defined-1-Terabit-Transceiver von Finisar zum Einsatz, der die verschiedenen Modulationsalgorithmen innerhalb des im Testbed genutzten 200-Ghz-S Superchannel-Signals parallel zum bislang im X-WiN genutzten 50-Gigahertz-Raster zu übertragen in der Lage ist.

Mehr Netzintelligenz auf tieferen Schichten

Das Konzept für die Entlastung der Datenautobahnen lautet derzeit: Mehr Netzintelligenz auf die tiefer liegenden Schichten des Internets bringen. Übersetzt heisst das, nach Möglichkeit nicht an jedem Netzwerkknoten die Container auszuladen, die Zielinformation zu erfassen und ihn erneut in Lichtimpulse zu verwandeln, um sechzig oder achtzig Kilometer weiter, am nächsten Kernnetzknoten, wieder alles auszupacken, die Zielinformationen auszulesen, einzupacken, auf das Lichtgleis setzen. Das Station-to-Station-Prinzip stammt noch aus der Frühzeit des Internet und ermöglicht, dass sich Datenpakete auch bei einem Totalausfall einzelner Strecken eigenständig einen Weg durchs Netz suchen.

Wer heute Daten über Weitverkehrsnetze schickt, nutzt dabei möglicherweise schon ‚Trunks'. So nennen sich große Datenkanäle, auf denen Datenströme seit einigen Jahren gebündelt über weite Distanzen im Netz gesendet werden und erst kurz vor Erreichen ihres Zieles – am letzten großen Verladehafen – geöffnet werden. Diese Trunks bündeln mehrere Bandbreiten in einem großen Datenstrom. Leicht zu rechnen: Bis zu zehn 1-Gigabit-Verbindungen passen auf einen 10G-Trunk, von denen wiederum zehn Stück auf einem 100G-Trunk zusammengefasst werden, der dann zum Beispiel von einem Kernnetzknoten in Hamburg nach Frankfurt am Main führt, um etwa die Datenströme, die per Überseekabel das Festland erreichen, unterbrechungslos bis kurz vor die Haustür des De-CIX zu liefern.

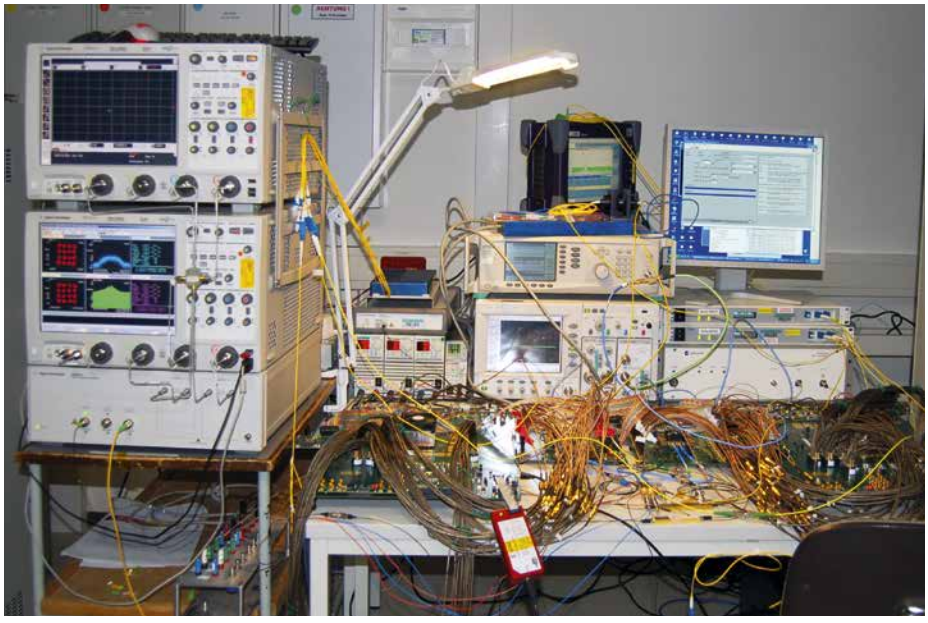
Selbst die Gigabit-breiten Datenströme, die bei Kollisionen in einem Teilchenbeschleuniger innerhalb von Millisekunden in Netze eingespeist werden, lassen sich mit derzeitigen Kapazitäten noch ebenso zuverlässig transportieren wie eine einfache E-Mail. Gleichwohl sind die derzeitigen Übertragungstechnologien mit Erreichen der 100-Gigabit/s-Schwelle an eine physikalische Grenze gestoßen. Wer 200 Gigabit/s übertragen will, muss einen zusätzlichen Kanal buchen. Das ist kein Problem, wenn man wie das Deutsche Forschungsnetz über ganze Fasern verfügt und einfach eine weitere Wellenlänge schalten kann. Aber irgendwie fühlt es sich trotzdem so an, als müsste man einen zusätzlichen Sitzplatz im Flugzeug buchen, nur weil man zwei Koffer im Gepäck hat.

X-WiN ist Terabit-tauglich

Dies könnte sich bald ändern. Auch wenn an diesem Morgen noch verschiedene Modulationsverfahren ausprobiert werden, kann festgehalten werden, dass die Coherent-Terabit-Technologie des Tera Santa-Konsortiums spätestens mit der gegen 12.30 Uhr erfolgreich durchgeführten Übertragung des Datenstroms dem reinen Experimentierstadium entwachsen ist. Bis zu 1,2 Terabit beginnen in den Mittagsstunden des 26. Februar 2014 über eine ‚normale' X-WiN-Faser auf 120 Kilometern zwischen Dresden und Freiberg parallel zum Produktionsbetrieb des Deutschen Forschungsnetzes zu fließen.

Der Test zeigt dabei nicht nur, dass es sich bei den hier auf dem Tisch aufgereihten Komponenten um ausgereifte Technologie handelt, sondern auch, dass das X-WiN ohne jegliche Modifikationen des technischen Environments in der Lage ist, Terabit-Datenströme in die optische Plattform zu integrieren. Bereits in seiner aktuellen Ausstattung zählt das X-WiN zu den fortschrittlichsten Netzwerk-Infrastrukturen weltweit. Pro Faser stehen mit der derzeit verwendeten Technologie 88 Kanäle zur Verfügung, die über State-of-the-Art-ROADMs angesprochen werden. Auf den mehr als 11.000 km Fasern des X-WiN sind dank dieser Technik derzeit eine Fülle von 10G-und 100G-Kanälen im Betrieb.

DFN-Verein und Tera Santa-Konsortium ist mit Durchbrechen der Terabit-Schwelle einer der größten Technologiesprünge in der Datenübertragung seit Einführung optischer Multiplex-Verfahren gelungen. Als erster Meilenstein des DFN-Terabit-Testbeds wird auf Basis dieses Feldtests in den kommenden Monaten an der Weiterentwicklung der Terabit-Technologie mit höherer Reichweite gearbeitet. Es gilt, Terabit-Technologie noch tiefer in die vorhandene Technologie-Umgebung des X-WiN zu integrieren und nach und nach zur Produktionsreife zu führen. Hierfür werden in den kommenden Monaten weitere Feldtests auf einer sukzessiv erweiterten Teststrecke stattfinden. ◆



Testaufbau für den Terabit-Transceiver am X-WiN-Knoten im Rechenzentrum Dresden.

Auf dem Weg in die DFN-Cloud

Nach zwei Jahren spannender Diskussion wird die DFN-Cloud konkret. Erste Services können voraussichtlich noch in diesem Jahr einer breiten Anwenderschaft angeboten werden. Die DFN-Cloud ermöglicht die Nutzung lokaler Cloud-Lösungen für alle Teilnehmer des DFN-Verbunds.

Text: **Kai Hoelzner, Jochem Pattloch** (DFN-Verein)

Foto: © KONG/photocase.de

Cloud-Kompetenz vorhanden

Die Verlagerung von Rechen- und Speicherleistungen in eine Cloud stellt für die Wissenschafts-IT ein interessantes Service-Modell mit großem Innovationpotenzial dar. Vorhandene Ressourcen lassen sich dynamisch auf anfragende Nutzer verteilen, die unabhängig von der geografischen Position der Ressourcen und der Nutzer bereitgestellt werden. Ressourcen können dabei kurzfristig hinzugebucht oder freigegeben werden und verschaffen den Einrichtungen mehr Elastizität bei der Planung ihrer IT.

Bislang wurde das Thema Cloud, insbesondere wegen seiner Risiken in Bezug auf Sicherheit, Informationsschutz und Nachhaltigkeit, vor allem in Hinblick auf kommerzielle Cloud-Lösungen diskutiert. Wenig beachtet blieb in diesem Zusammenhang der Umstand, dass wissenschaftliche Einrichtungen sehr wohl in der Lage sind, selbst als erfolgreicher Anbieter von Cloud-Diensten für die Wissenschaft aufzutreten. Einzelne Einrichtungen haben entsprechende Willensbekundungen bereits abgegeben oder stellen bereits einen Cloud-Dienst für die von ihnen versorgten Einrichtungen zur Verfügung.

Doch auch wenn es für manchen DFN-Anwender nicht unattraktiv wäre, Cloud-Ressourcen aufzubauen und auch Nutzern anderer Einrichtungen zur Verfügung zu stellen, existieren eine Reihe von Fragen, die zu klären sind, bevor die eigene Cloud nach außen geöffnet werden kann. Hier sind sowohl Fragen des Informationsschutzes als auch der Umlagefinanzierung und der Governance zu nennen. Seit längerem wird deshalb innerhalb der DFN-Community diskutiert, ob und wie sich Clouds im DFN-Kontext realisieren lassen.

Vorteile von Wissenschafts-Clouds

Sofort nachdem das Thema Cloud zum ersten Mal auf der Agenda einer Mitgliederversammlung stand, setzte ein breiter Willensbildungsprozess innerhalb der DFN-Community und eine intensive Diskussion der technischen und administrativen Möglichkeiten und Rahmenbedingungen ein. In einer rege geführten Diskussion wurde deutlich, dass Clouds auch für Wissenschaftseinrichtungen ein funktionierendes Geschäftsmodell sein könnten. Eine DFG-Empfehlung[1] fasst die Vorteile für Cloud-Nutzer und Cloud-Anbieter wie folgt zusammen:

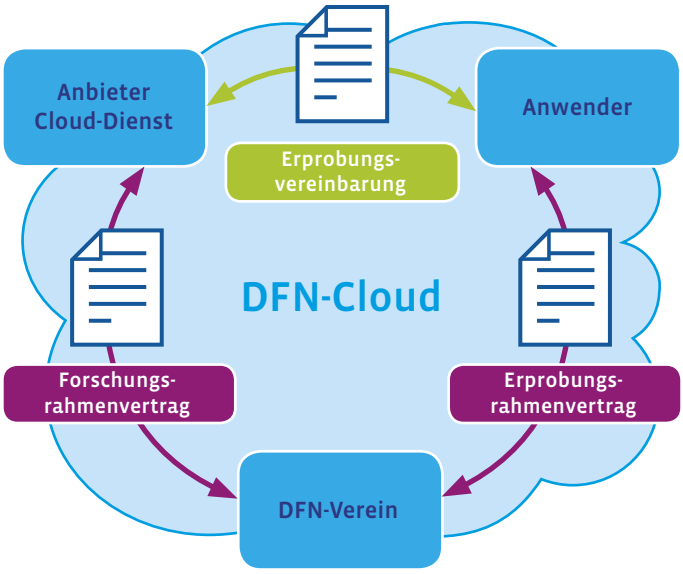
„Als Vorteile für die Nutzer gelten die Einsparung von Anschaffungskosten für Hard- und Software sowie die Möglichkeit einer individuellen Skalierung der benötigten Kapazitäten je nach Bedarf und ohne eine längere Bindung, wie sie sich aus einer Beschaffung von Hardware ergibt. Des Weiteren lässt sich der Aufwand für Wartung, Weiterentwicklungen, Lizenz- und Personalkosten bis auf ein Minimum reduzieren. Die Verlagerung der operativen Verantwortung auf den Cloud-Anbieter führt ebenfalls zu geringerem Zeit- und Kostenaufwand. Ein weiterer wichtiger Vorteil besteht in der möglichen Nutzung gemeinsamer Plattformen für verschiedene Einrichtungen und Nutzergruppen. So kann die Arbeit an gemeinsamen Projekten im Forschungsbereich aber auch in der Lehre bei einer dezentralen Verteilung der Nutzer durch den Einsatz gemeinsam genutzter Speicher-, Rechen- oder Bibliotheks-Clouds wesentlich vereinfacht werden. Nutzer von Cloud-Angeboten können mit geringen initialen Kosten neue Konzepte erproben und entwickeln."

Cloud als Teil des DFN-Dienst-Portfolios?

Im Zusammenhang mit Wissenschafts-Clouds wurde zunächst die Frage besonders intensiv diskutiert, ob der DFN-Verein selbst eine solche Cloud aufbauen und betreiben könne. Schließlich, so die Wahrnehmung in der Mitgliedschaft, verfüge der DFN-Verein über große Kompetenz beim Netz und netznahen Diensten, sei geübt in Fragen der Ausschreibung, Zertifizierung und der technischen Überwachung und verfüge als Verein mit einer Vielzahl aktiver Mitglieder und Nutzer nicht zuletzt über eine Struktur, die die kommunikativen und organisatorischen Abläufe beim Aufbau und Betrieb eines solchen Cloud-Dienstes durchaus begünstigen würde. Doch wie viel Kompetenz der DFN-Verein in netznahen Dienstleistungen auch haben mag – die Kompetenz beim Anbieten von virtuellen Maschinen oder Speichern, aber auch die Kompetenz beim Betrieb von Plattformen wie (Netz-) Bibliotheken, Datenbanken, Computing- oder Analyse-Lösungen liegt eindeutig bei den IuK-Zentren der Mitglieder.

Der DFN-Verein schafft mit der DFN-Cloud den organisatorischen und fachlichen Rahmen, innerhalb dessen vorhandene wissenschaftliche Cloud-Lösungen von allen Teilnehmern am DFN-Verbund genutzt werden können.

[1] „Cloud-Dienste - Addendum zu den Empfehlungen der Kommission für IT Infrastruktur 2011-2015" (http://www.dfg.de/foerderung/info_wissenschaft/info_wissenschaft_14_07/)



Konzept der DFN-Cloud: Anbieter und Nutzer schließen Rahmenverträge für Erforschung und Erprobung der DFN-Cloud ab und treffen für einzelne Cloud-Lösungen untereinander eine Erprobungsvereinbarung.

Die bessere Lösung: DFN-Verein schafft Rahmen für Cloud-Services

Seitens der Mitgliedseinrichtungen des DFN wird es durchaus als positive Herausforderung gesehen, selbst Clouds zu etablieren. Eine Reihe von Rechenzentren agiert technisch gesehen längst als Anbieter von Speicherplatz, etwa wenn sie wissenschaftliche Großprojekte mit ihrem gewaltigen Speicherbedarf bedienen. Vor allem in den Einrichtungen selbst befinden sich die Rechenzentren heute bereits in der Rolle eines Cloud-Betreibers. Mitarbeiter und Studierende nutzen Speicherplatz im Netz der Hochschule, greifen auf Software zu oder nutzen Rechenkapazitäten im lokalen Netz. Aus der Nähe betrachtet wurde deutlich, dass die Kompetenz zum Aufbau von Clouds in vielen DFN-Mitgliedseinrichtungen mehr als vorhanden ist.

Die eigentliche Hürde, so stellte sich in den Diskussionen heraus, liegt in der Frage, wie Clouds sich gegenüber Dritten in administrativer, rechtlicher und finanzieller Hinsicht organisieren lassen. Hier wiederum kommt die spezielle Kompetenz des DFN-Vereins ins Spiel, eine funktionierende organisatorische Struktur erschaffen zu können, in der Anwender im DFN miteinander als Anbieter und nutzende Einrichtung von Diensten in einem sicheren rechtlichen Rahmen und mit einer allseits akzeptierten Governance- und Finanzierungs-Struktur zusammenarbeiten können.

Je intensiver das Thema Wissenschafts-Cloud in der DFN-Community diskutiert wurde, desto deutlicher wurde nicht nur, dass die technischen Ressourcen für Cloud-Services in einer Reihe von Einrichtungen längst vorhanden sind, sondern auch, dass sich Anbieter und Nutzer auf ein gemeinsames Verständnis z. B. in Bezug auf Informationssicherheit, Haftungsfragen und die Offenheit und Interoperabilität von technischen Lösungen einigen können. Dies spiegelt sich nun in den Verträgen wider, die der DFN-Verein als formalen Rahmen der DFN-Cloud in Rücksprache mt seinen Mitgliedern und Anwendern entwickelt hat.

Im Ergebnis lässt sich das Konzept der DFN-Cloud auf eine einfache Formel bringen: Der DFN-Verein schafft mit der DFN-Cloud den organisatorischen und fachlichen Rahmen, innerhalb dessen vorhandene wissenschaftliche Cloud-Lösungen von allen Teilnehmern am DFN-Verbund genutzt werden können.

Die Aufgabe für den DFN-Verein könnte darin bestehen, die Anforderungen der verschiedenen Perspektiven sowohl von Anbietern wie von Nutzern der Cloud vertraglich zu berücksichtigen und zu moderieren. Zur Ausgestaltung der Regelungen für föderierte DFN-Dienste wurden drei Arten von Vereinbarungen konzipiert:

- ein Forschungsrahmenvertrag, den der DFN-Verein mit jeder Einrichtung abschließt, die föderierte DFN-Dienste anbieten möchte,
- ein Erprobungsrahmenvertrag, den der DFN-Verein mit jeder Einrichtung abschließt, die föderierte DFN-Dienste nutzen möchte,
- ein Formulierungsvorschlag für Erprobungsvereinbarungen, die für jedes Nutzungsverhältnis bilateral zwischen den Anbietern und Nutzern von föderierten DFN-Diensten abgeschlossen werden.

Gestaltende Moderation erforderlich

Ein wesentliches Unterscheidungsmerkmal von Clouds ist das Betriebsmodell. Hierbei wird im Wesentlichen zwischen Public- und Private-Clouds und zwischen Hybriden aus Public- und Private-Clouds und Community-Clouds unterschieden. Eine Public-Cloud wird auf externen Ressourcen eines Anbieters betrieben und kann von einer breiten Öffentlichkeit in Anspruch genommen werden, während die Private-Cloud einer a priori definierten Gruppe von Nutzern (z.B. Mitgliedern einer Organisation) meist auf lokalen Ressourcen zur Verfügung steht. Innerhalb der DFN-Community finden sich bis dato vor allem Clouds, die von Rechenzentren für die eigene Einrichtung oder für eine spezielle Community – zum Beispiel eine Forschungseinrichtung – oder aber regional begrenzt für mehrere Wissenschaftseinrichtungen etwa innerhalb eines bestimmten Bundeslandes erbracht werden. Ziel der DFN-Cloud ist, wissenschaftliche Private-Clouds oder Community-Clouds mit eng umrissener Nutzerschaft für eine breitere DFN-Community zu öffnen, wobei die Nutzung aber durch einen zuvor klar definierten und durch Verträge gesicherten Rahmen geschützt wird.

Kommende Aufgaben des DFN-Vereins

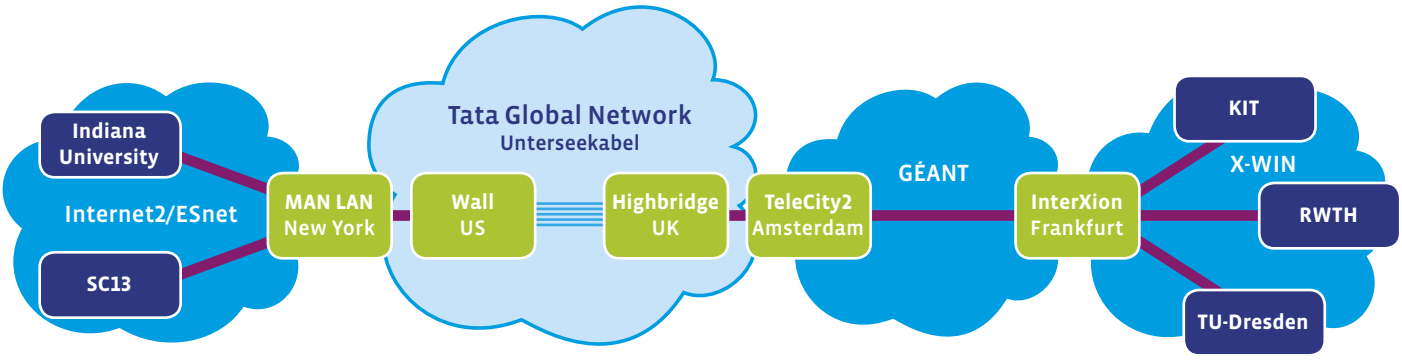
Bereits heute sind erste Verträge für die Erbringung von Diensten in der DFN-Cloud geschlossen. Die Aufgabe des DFN-Vereins liegt in den kommenden Monaten darin, Verträge mit weiteren Anbietern und Nutzern abzuschließen und die Parteien zusammenzubringen. Dabei sollen die Interoperabilität ähnlicher Cloud-Dienste befördert und die Wechselmöglichkeit zwischen ihnen offen gestaltet werden. Entscheidend ist auch, die Dynamik bestehender Cloud-Dienste zu verfolgen und im Hinblick auf eine übersichtliche DFN-Cloud einwirken zu lassen.

Um die nötigen Impulse für das Entstehen und die Nutzung von Clouds zu geben, bedarf es nicht zuletzt eines regen Austauschs zwischen Anbietern und Nutzern. Hier ist der DFN-Verein auf die aktive Mitwirkung seiner Mitglieder und Anwender angewiesen, um eine DFN-Cloud mit maßgeschneiderten IuK-Diensten für die Wissenschaft in Deutschland zu etablieren. ◆

Next Stop Indiana: Anwender im DFN nutzen erste 100-Gigabit/s-Verbindungen in die USA

Das Deutsche Forschungsnetz hat erste transatlantische Verbindungen mit einer Kapazität von 100 Gigabit/s zwischen Anwendern in Deutschland und den USA in Betrieb genommen. Gemeinsam mit DANTE als Betreiber des europäischen Forschungsnetz-Backbones GÉANT sowie den amerikanischen Forschungsnetzen ESnet und Internet2 konnten Anwender im DFN eine 100G-Strecke zwischen Frankfurt/Main und New York über mehrere Wochen intensiv testen. Der transatlantische Abschnitt von Amsterdam nach New York ist das Ergebnis der internationalen „Advanced Northatlantic 100G“ (ANA-100G) Kooperation.

Text: **Dr. Christian Grimm** (DFN-Verein)



Die transatlantische 100-Gigabit/s-Infrastruktur ermöglichte erste 100G-Verbindungen zwischen Anwendern im DFN und Einrichtungen in den nordamerikanischen Forschungsnetzen Internet2 und ESnet.

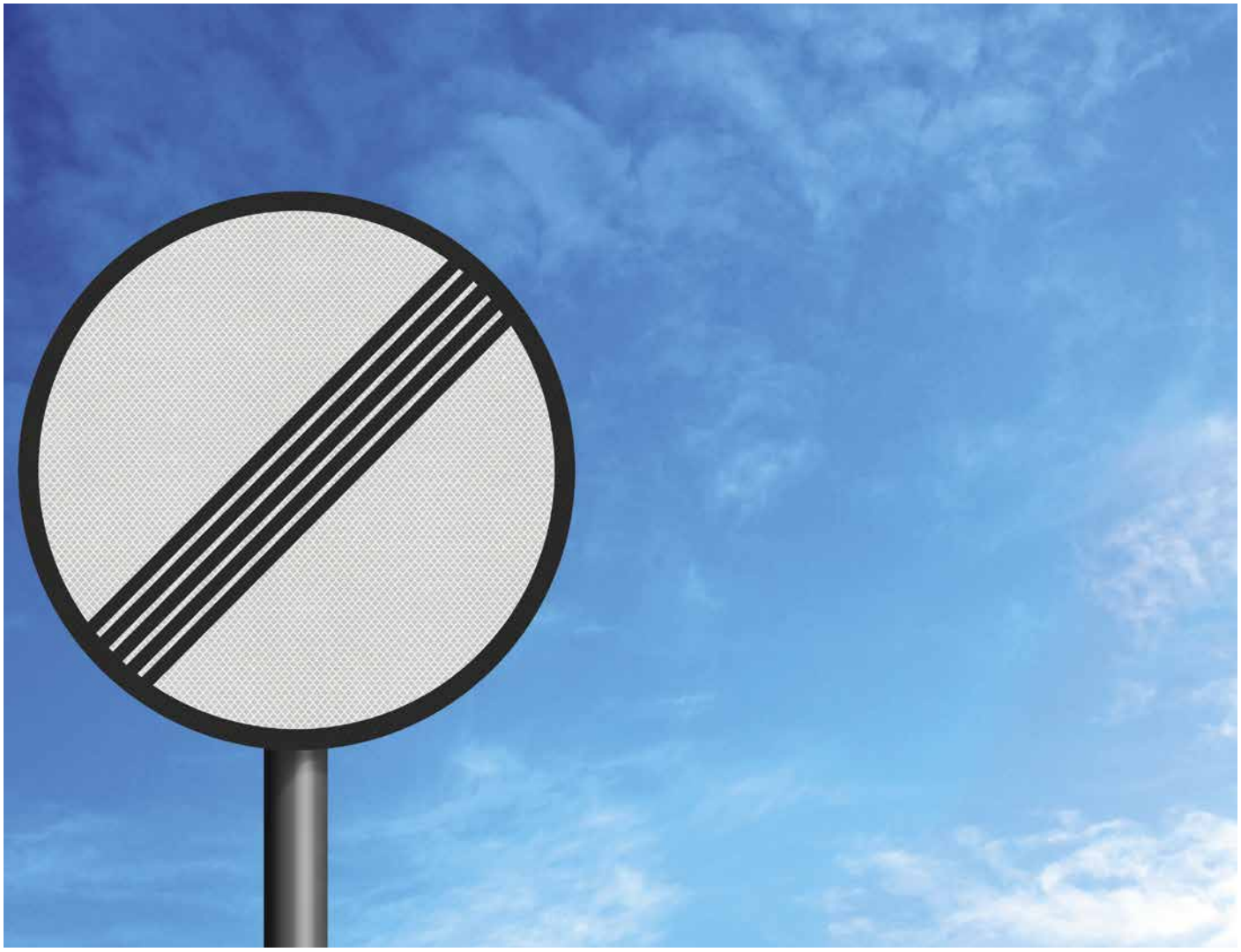


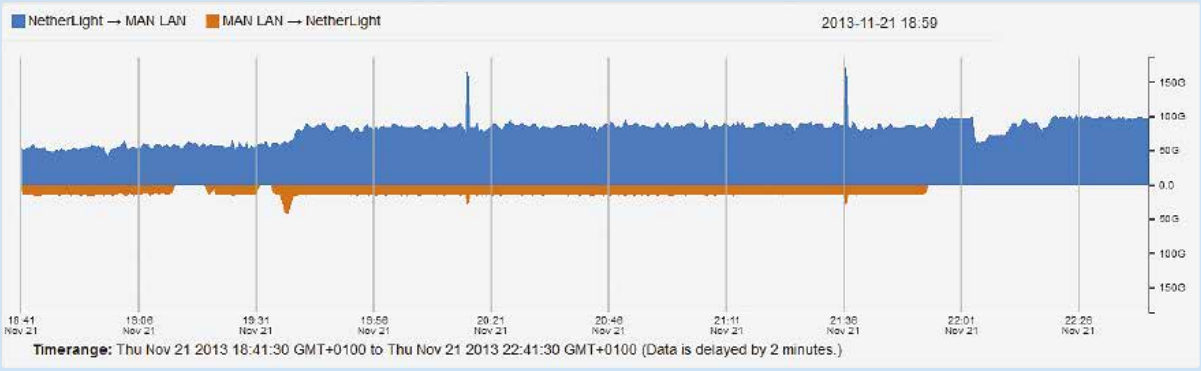
Foto: © Becky Stares/fotolia.com

Anlässlich der Supercomputing Konferenz SC13, die vom 17. bis 22. November 2013 in Denver (USA) stattfand, hat das Steinbuch Centre for Supercomputing (SCC) des Karlsruher Instituts für Technologie (KIT) erste Anwendungen im 100G-Bereich über den Atlantik demonstriert. Wissenschaftler aus Karlsruhe und den USA nutzten den 100G-Link dabei zum Austausch von Experiment-Daten des Large Hadron Colliders in Genf.

Im Dezember und Januar konnten die Rechenzentren der Technischen Universität Dresden und der Rheinisch-Westfälischen Technischen Hochschule (RWTH) Aachen die transatlantische 100G-Verbindung gemeinsam mit der Indiana University in den USA testen. Gegenstand der Untersuchungen war die ultrabreitbandige Kopplung von Speichersystemen über das verteilte Dateisystem Lustre. KIT, TU Dresden und RWTH Aachen gehören somit zu den ersten Einrichtungen überhaupt, die 100G-Verbindungen zwischen Europa und den USA exklusiv untersuchen konnten.

Mit der Untersuchung transatlantischer 100G-Verbindungen folgt der DFN-Verein konsequent seiner Strategie einer bedarfsgerechten Einführung von 100G-Technologie für die Wissenschaft. Nach der Implementierung von 100-Gigabit/s-Verbindungen im Kernnetz des deutschen Wissenschaftsnetzes wurden im vergangenen Jahr erste Anwenderanschlüsse für die Hochschulen in Deutschland und die Übergänge zu den europäischen und nordamerikanischen Wissenschaftsnetzen mit 100G-Technologie ausgerüstet.

Parallel zum nationalen Ausbau des Wissenschaftsnetzes wurde jüngst auch das gesamte europäische Forschungsnetz-Backbone GÉANT mit 100G-Technologie ausgestattet. GÉANT verbindet die



Datenlast auf der transatlantischen 100-Gigabit/s-Verbindung während des Testbetriebs zwischen dem KIT Karlsruhe und der Supercomputing 2013 in Denver am 21. November 2013 (blau: EU -> USA, orange: USA -> EU).

Wissenschaftsnetze in Europa untereinander und unterhält im Rahmen internationaler Kooperationen derzeit direkte Verbindungen zu 65 weiteren Wissenschaftsnetzen weltweit. Der DFN-Verein gehört zu den Initiatoren von GÉANT und dessen Betreibergesellschaft DANTE.

Vom Ausbau der Kapazitäten in den Wissenschaftsnetzen auf 100-Gigabit/s werden in Zukunft neben den traditionellen Heavy-Usern unter den Hochschulen in Deutschland vor allem auch international kooperierende Großforschungseinrichtungen und Projekte profitieren. So wird das teilweise vom Deutschen Forschungsnetz bereitgestellte Netz für die LHC-Experimente des CERN in Deutschland künftig auf der 100G-Infrastruktur aufsetzen.

Die Zahl der wissenschaftlichen Rechenzentren in Deutschland, die sich für die oberste Leistungsklasse im DFNInternet-Dienst mit 100 Gigabit/s entscheiden, könnte sich in Zukunft rasch vergrößern. Seit Jahren treibt der DFN-Verein seine Strategie voran, eine möglichst große Zahl von Anwendern direkt an das Kernnetz X-WiN anzuschließen, um kostspielige und in der Regel leistungsschwächere Zugangsleitungen zu vermeiden. Fast alle größeren Wissenschaftseinrichtungen stellen heute Kernnetzknoten des annähernd 11.000 Kilometer Glasfasern umfassenden X-WiN dar, dessen Streckenführung konsequent an die geografische Topologie der deutschen Wissenschaftsstandorte angepasst wurde. ◆

Mit Brief und Siegel

Über den Jahreswechsel hat der Dienst DFN-MailSupport das Auditor-Testat „Einstiegsstufe“ erfolgreich absolviert. Für die Anwender des Deutschen Forschungsnetzes ist es damit ab sofort möglich, den Dienst im Regelbetrieb zu nutzen.

Text: **Michael Röder** (DFN-Verein)

Foto: © malerapaso/iStock.

Das Vertrauen in die Sicherheit unserer Kommunikationswege wurde in der jüngeren Vergangenheit mehr denn je auf die Probe gestellt. An jeder Stelle, an der wir von „Heartbleed“ oder „BSI-Passwortattacke“ lesen, ist es unvermeidbar, sich die folgenden Fragen zu stellen: Wie sicher kommunizieren wir? Wie teilen wir unseren Partnern sensible Informationen mit? Und wer garantiert uns, dass die von uns gewählte Form der Kommunikation tatsächlich den Ansprüchen genügt, die wir benötigen? Die Antwort lautet: zertifizierte Sicherheit ist Pflicht!

In Form einer zentralen, vertrauenswürdigen Stelle erarbeitet das Bundesministeriums für Sicherheit in der Informationstechnik (BSI) einen Maßnahmenkatalog, der für einheitliche Standards sorgt, an denen sich die Infrastrukturen genutzter Kommunikationskanäle messen und unterscheiden lassen – und diese Maßnah-

men gehen weit über die bloße Umsetzung technischer Standards hinaus. Gerade dann, wenn es darum geht, bewährte Strukturen aufzubrechen, wächst der administrative Aufwand. Die gezielte Umsetzung konkreter technischer und organisatorischer Maßnahmen ist es aber, die einen vertrauenswürdigen Dienst charakterisiert – Vertrauen ist keine App, die via Klick auf dem breit aufgestellten Markt der Kommunikationsdienstleister eingekauft werden kann. Die Basis für gegenseitiges Vertrauen liegt darin, glaubhaft zu versichern, dass alle Vorkehrungen getroffen wurden, um eine anerkannte Sicherheitsstufe mit vertretbarem Aufwand zu erreichen. Als Zeugnis davon kann ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz dienen.

Der Dienstinhalt Spamerkennung ist nicht neu. Auch abseits vielerorts eingesetzter Appliances ist durch unterschiedliche Herangehensweisen eine Vielzahl verschiedener Techniken in der Welt der wissenschaftlichen Einrichtungen entstanden, die an ihrem jeweiligen Einsatzort über viele Jahre hinweg für ein besonderes Know-how und zuverlässige Ergebnisse gesorgt haben. Von dieser geballten Expertise konnte der DFN-Verein an zahlreichen Stellen bei der Implementierung des Dienstkonzeptes profitieren. Dabei sind jedoch nicht alle Ansätze untereinander kompatibel, sie schließen sich teilweise sogar gegenseitig aus. Das bedeutet, dass bei der Nutzung eines zentralen DFN-Dienstes jede Einrichtung in die Lage versetzt werden soll, ihre gesammelte Erfahrung möglichst effektiv auf die Arbeit des Dienstes abbilden zu können, um den Wechsel so wenig aufwendig wie möglich zu gestalten.

Dieser Effekt soll durch den Einsatz eines Web-Portals erreicht werden. Innerhalb des Portals werden Benutzerrollen definiert, die den lokalen Mail-Admins die Möglichkeit geben, beispielsweise den Zeitpunkt bestimmter Prüfvorgänge zu ändern. Es kann zum Beispiel durchaus zu unterschiedlichen Ergebnissen führen, wann die Verifizierung des MIME-Typs stattfindet. Kann die Prüfung vor dem vollständigen Einliefern der E-Mail abgeschlossen werden, ist es erlaubt, die E-Mail abzulehnen. Ist die E-Mail jedoch einmal vollständig eingeliefert worden, lässt das Datenschutzgesetz keine Ablehnung mehr zu – die Nachricht muss dann zugestellt werden. Darüber hinaus kann der Admin die Adressierung seiner Mail-Exchange-Adressen im Portal ändern. Auch die Einrichtung von Testdomains und Beendigung der Teilnahme am Dienst sind über die Weboberfläche steuerbar. Neue Nutzer des Portals sind jederzeit dazu eingeladen, am Testbetrieb teilzunehmen!

Bei dem Betrieb eines mandantenfähigen Portals sorgt das Bundesdatenschutzgesetz für eindeutige Vorgaben deren Bedeutung im Zusammenhang mit den aktuellen Datenschutzaffären eine ganz besondere Brisanz bekommt. Immer dann nämlich wenn personenbezogene Daten erhoben oder verarbeitet werden, ist der ausführende Dienstleister verpflichtet, die Einhaltung technischer und organisatorischer Maßnahmen zum Schutz der Daten sicherzustellen. Unter anderem müssen Regeln getroffen werden, die garantieren, dass betroffene Daten nur für einen bestimmten Zeitraum in der technischen Infrastruktur verbleiben. Natürlich müssen auch Vorgaben existieren, die nachvollziehbar dafür sorgen, dass die Weitergabe an Dritte unter technisch und organisatorisch vertretbaren Bedingungen ausgeschlossen werden kann. Damit sich nicht jede am Dienst teilnehmende Einrichtung persönlich davon überzeugen muss, dass der DFN-Verein für eine angemessen gesicherte Betriebsumgebung Sorge trägt, haben wir uns dazu entschieden, die Prüfung stellvertretend durch einen BSI-Auditor im Zuge der ISO-27001-Zertifizierung auf Basis von IT-Grundschutz durchführen zu lassen. Die erste Hürde auf dem Weg zum Zertifikat konnte Ende des vergangenen Jahres mit dem bestandenen Auditor-Testat „Einstiegsstufe“ genommen werden. Zur weiteren Bearbeitung gewährt das BSI einen Zeitraum von 24 Monaten für die Umsetzung aller notwendigen Maßnahmen, um das Auditor-Testat „Aufbaustufe“ zu erhalten. Erst der Erhalt beider Testate bildet die Grundlage eines ISO-27001-Zertifikates auf Basis von IT-Grundschutz.

Mit dem Jahreswechsel waren damit alle Voraussetzungen erfüllt, um den Dienst DFN-MailSupport vom Pilotbetrieb in den Regelbetrieb fließend übergehen zu lassen. Die Vertragsunterlagen bestehen aus einer Dienstvereinbarung und einer Vereinbarung zur Datenauftragsverarbeitung. Sie werden seit Anfang 2014 an alle bis dahin eingetragenen Testnutzer des Dienstes verschickt. Wichtig: Nur die Unterzeichnung beider Vertragsteile führt zur Teilnahme am Dienst! Interessierte Einrichtungen können die Vertragsdokumente via mailsupport@dfn.de anfordern. Da die Einrichtungen durch die Teilnahme an der Auftragsdatenverarbeitung zur Führung eines Verfahrensverzeichnisses verpflichtet werden, steht beim DFN-Verein bereits ein weiteres Dokument kurz vor der Veröffentlichung. Darin werden die ergriffenen technischen und organisatorischen Maßnahmen in Funktionsgruppen zusammengefasst und beispielhaft aufgeführt. Das Ergebnis ist ein überschaubares Papier, das inhaltlich den sicherheitsrechtlichen Aspekten gerecht wird und eine Abstraktionsebene über den tatsächlichen Maßnahmen durch seinen zusammenfassenden Charakter für Übersichtlichkeit und Verständnis sorgt – es soll den Einrichtungen bei der Erarbeitung ihres Verfahrensverzeichnisses behilflich sein. ◆

Kurzmeldungen

Münchner City wird WLAN-Campus

In Kooperation mit der Stadt München, den Stadtwerken München (SWM) und dem DFN-Verein hat das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) sein Campus-WLAN-Netz vergrößert. Studierende, Wissenschaftler und Forscher in München können, sofern sie im DFN oder in einem anderen europäischen Wissenschaftsnetz bereits für eduroam registriert sind, künftig sämtliche ‚M-LAN'-Hotspots nutzen, die von den SWM in der Münchner Innenstadt bereitgestellt werden. Vor kurzem erst hatten die Katholische Universität Eichstätt-Ingolstadt und die Technische Hochschule Ingolstadt mit den örtlichen Versorgern und der Stadtverwaltung Ingolstadt eine Kooperation für die Einbindung innerstädtischer WLAN-Hotspots in die Infrastruktur von DFN-Roaming/eduroam gestartet.

Eduroam ist eine europäische Wissenschaftsinitiative, die es allen Nutzern der teilnehmenden Organisationen weltweit erlaubt, nationale Wissenschaftsnetze sowie das Internet auf sichere Art und Weise zu nutzen. ◆
https://www.dfn.de/dienstleistungen/dfnroaming/

DFN-Webkonferenzen ab sofort verschlüsselt

Der DFN-Webkonferenzdienst wird gegenwärtig mit der Software Adobe Connect realisiert und ist mit der AAI des DFN-Vereins (DFN-AAI) gekoppelt. 422 Einrichtungen mit über 11.350 autorisierten Konferenzveranstaltern sind derzeit für den Dienst registriert. Im Rahmen eines Pilotbetriebs ist für das Webkonferenzsystem ab sofort eine Verschlüsselung aktiviert. Die Medienströme (Audio, Video und Daten) werden standardmäßig über den https Port ausgetauscht. Bisher wurde nur die Signalisierungsphase verschlüsselt.

Die Umstellung auf das verschlüsselte Verfahren erfolgt auf Client-Seite automatisch. Eine spezielle Konfiguration des Clients ist nicht notwendig. Ob eine Verbindung verschlüsselt ist, lässt sich an einer grünen Kontrollleuchte ablesen, die neben einem Schlosssymbol auf der Webseite des Konferenzfensters im Browser zu sehen ist.

Größere Nutzungskapazität bei DFNVC

Um der gestiegenen Nachfrage in der DFN-Community nach Mehrpunkt-Videokonferenzen gerecht zu werden, stehen im DFN-Videokonferenzdienst künftig zwei zusätzliche H.323-Multipoint Control Units für die Durchführung von VC-Meetings zur Verfügung.

Insgesamt versorgen nunmehr sechs MCUs den Dienst, die aus Sicherheits- und Management-Gründen an verschiedenen Standorten im X-WiN installiert sind. Jede MCU kann dabei bis zu vierzig Teilnehmer parallel im Full-HD-Modus mit Mehrpunkt-Videokonferenzen bedienen. ◆
https://www.dfn.de/dienstleistungen/dfnvc/

Neue Kernnetstandorte im X-WIN

Seit Beginn des Jahres ist die Bergakademie Freiberg direkt an das Kernnetz des X-WiN angeschlossen. Der neue Kernnetzstandort ermöglicht, Anwender im Raum Freiberg mit kostengünstigeren Zugangsleitungen an das X-WiN anzubinden, als dies bislang der Fall war.

Ein weiterer neuer Kernnetzknoten des X-WiN wurde im vergangenen Jahr am Standort Hamburg Wendenstraße eingerichtet. Dieser dient seit kurzem als zweiter Übergang zum europäischen Forschungsbackbone GÉANT, der bisher einzig über einen Übergabepunkt in Frankfurt/Main realisiert wurde. Der neue Übergabepunkt zum GÉANT ist per „long haul" über eine direkte 100-Gigabit-Verbindung mit dem Supercore-Standort an der TU Berlin verbunden.

Ebenfalls am Standort Wendenstraße wurde ein Peering-Point eingerichtet, der einen komfortablen Übergang zu Netzwerken von zum Beispiel Google gewährleistet. ◆

Begrüßungsschild des Campus der Technischen Universität Bergakademie Freiberg. *Foto: Rober Porter*

perfSONAR – das Schweizer Taschenmesser für Netzwerk-performancemessungen

Text: **Robert Stoy** (DFN-Verein), **Roland Karch** (Friedrich-Alexander-Universität Erlangen-Nürnberg)

Foto: © uatp2/iStock

perfSONAR – Vom Projekt zum professionellen Tool-Kit

Beim Betrieb von Weitverkehrsnetzen, VPNs und Multidomain-Netzwerkinfrastrukturen ist es wichtig, sowohl deren Leistung ständig zu überprüfen, als auch beim Aufkommen von Problemen entsprechende Diagnosemöglichkeiten zur Verfügung zu haben. Für diese Zwecke gibt es eine Vielzahl von Werkzeugen und Messmethoden, die von den weithin bekannten Ping- oder Traceroute-Werkzeugen über SNMP-basierte Datensammlungen bis hin zu mächtigen und spezialisierten Programmen zur Überwachung von Paketlaufzeiten, des Routings oder dem erreichbaren Datendurchsatz zwischen beliebigen Endpunkten im Netz reichen.

Für die spezifischen Anforderungen an die Messung und Überwachung von Daten-Verbindungen im Bereich des wissenschaftlichen Netzwerkens wurde im Jahr 2002 ein Projekt zur Leistungsmessung in Forschungsnetzen initiiert, in dem ein System namens perfSONAR zur Leistungsmessung insbesondere auch in heterogenen Netzen zwischen verschiedenen Domänen entwickelt wurde.

Als eine Middleware sollte perfSONAR verschiedene Datenquellen der Leistungsmessung in einem einheitlichen Protokoll darstellen und sie über administrative Netzwerkgrenzen hin nutzbar machen.

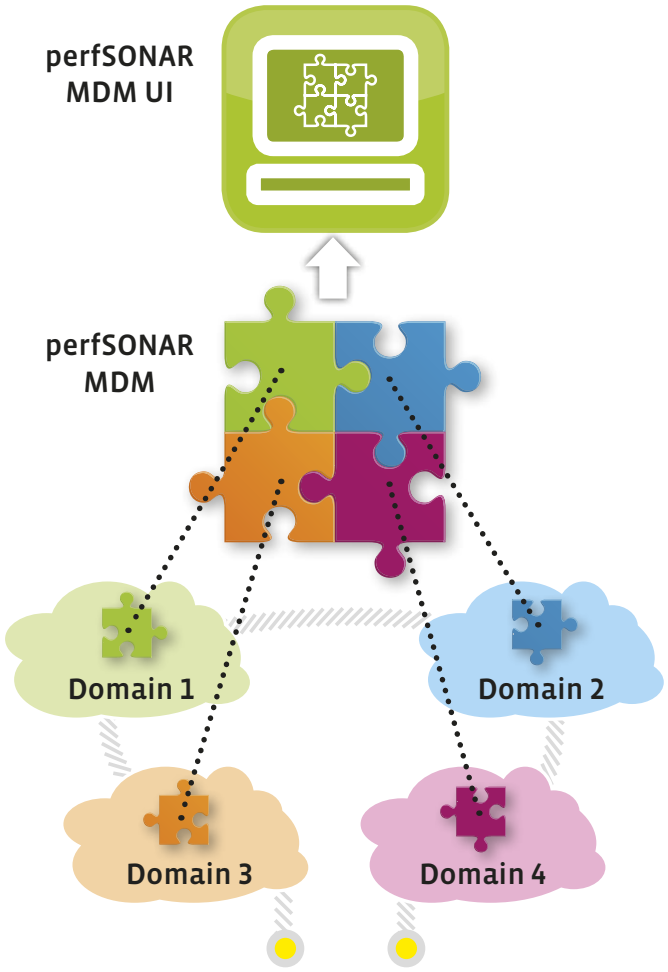
Aufbauend auf diesem Konzept begann 2004 die Design- und Entwicklungsarbeit für perfSONAR im Rahmen einer „Joint Research Activity“ des Projekts GÉANT2 in Kooperation mit US-Partnern von Internet2 und ESnet. Wichtig im Rahmen dessen war perfSONAR als Protokoll zur Durchführung von Messungen und Austausch von Daten in einer heterogenen Umgebung.

Zur Zielsetzung von perfSONAR gehörte es, über Ende-zu-Ende Netzwerkpfade und dessen Abschnitte Basis-Netzkennzahlen bereitzustellen. Dies sind die Auslastung von Links, Paketlaufzeiten (Delay) und deren Schwankung (Jitter) sowie Paketverluste, die im Übertragungsweg oder in Netzknoten auftreten. Hierbei sollte zwischen IPv4 und IPv6 sowie zwischen unicast und multicast unterschieden werden. Bereitgestellt werden sollte perfSONAR als Open Source Software.

Heute wird perfSONAR im GÉANT sowie in einer Vielzahl nationaler Forschungsnetze wie dem X-WiN, dem Abilene-Netzwerk der Internet2-Initiative, dem Nordamerikanischen ESnet (Netzwerk des Department of Energy in den USA) oder dem Brasilianischen Forschungsnetz RNP eingesetzt. Dabei beinhaltet perfSONAR deren Messinfrastruktur, die interoperablen Software-Pakete und schließlich das Kommunikationsprotokoll.

Architektur von perfSONAR

Die Implementierung von perfSONAR wird für den Anwender über mehrere Einzelkomponenten greifbar. Die Web-Schnittstelle, in der GÉANT-Implementierung ist dies das user interface ‚perfsonarUI‘, erlaubt den Zugriff auf verschiedene Arten von Messungen aus verteilten Quellen. Es handelt sich um eine zentrale Komponente, die die gesamte Interaktion zwischen Nutzer und Dienst abwickelt. Das stark verteilte Konzept von perfSONAR als Infrastruktur wird durch sie einfach bedienbar. Die Benutzerschnittstelle greift dabei schon während der Formulierung der Anfrage auf weitere Komponenten zu. Als ein Verzeichnisdienst agiert der Lookup Service zum dynamischen Auffinden von verschiedenen Datenquellen. Die so gefundenen und verfügbaren Dienste werden dann nach Art und Namen sortiert dem Benutzer zur Auswahl präsentiert. Sobald perfsonarUI alle benötigten Informationen über die Daten- oder Messanfragen hat, schickt es im Hintergrund eine entsprechende perfSONAR-Nachricht an die eigentlichen Datenquellen. Grob gliedern kann



Aktuell eingesetzte perfSONAR-Komponenten im X-WiN.

man diese nach Measurement Archive (MA) oder Measurement Point (MP). MA-Instanzen speichern Ergebnisse von vergangenen Messungen, dies können entweder vorher fest geplante und ständig ausgeführte Messungen sein oder auch von Nutzern direkt initiierte Tests. Über HADES werden Paketlaufzeiten, -verluste und daraus abgeleitete weitere Metriken unidirektional erfasst. Mit regelmäßigen Traceroute-Tests wird auch der Weg der Messungen durch das Netz erfasst. Bandbreitentestergebnisse des ‚Bandwidth Test Controller' BWCTL werden im Archiv BWCTL MA gespeichert. All diese Metriken erlauben eine sehr präzise Einschätzung der Dienstgüte und Analyse möglicher Probleme von IP-Verbindungen. MP-Instanzen auf der anderen Seite werden für das Ausführen von genau durch den Nutzer spezifizierten Messungen eingesetzt. Die angefragten Messungen können hier ebenfalls Paketlaufzeit- oder Bandbreitenmessungen sein, an einer Unterstützung für Traceroute wird aktuell gearbeitet.

perfSONAR als Produkt wird im Rahmen des EU-Projekts GN3plus von einem Team aus aktuell 16 Teilnehmern weiterentwickelt. Die Schwerpunkte liegen bei der Verbreitung der Software, der Definition neuer Anwendungsszenarien (Use Cases), der Konvergenz mit externen perfSONAR-Implementierungen und der Anpassung an Innovationen aus Standardisierungsgremien.

Zum aktuellen Zeitpunkt gibt es innerhalb des GÉANT-Projekts 23 Messpunkte in 20 NRENs. Im GÉANT-Netz selbst sind 18 Messpunkte für weltweite Messungen verfügbar. Im X-WiN werden zur Qualitätssicherung bereits seit einigen Jahren Messpunkte in den Netzknoten betrieben, in denen unter anderem die perfSONAR-Komponenten HADES und BWCTL laufen. Diese messen mit künstlich erzeugtem Messverkehr zwei wichtige Basis-Kenngrößen zur Qualitätsbestimmung:

Zum einen die Einweglaufzeit der Pakete durch das Netz, und zum anderen das Paketverlustverhältnis, also das Verhältnis von verloren gegangenen zu übertragenen Paketen.

Diese Basis-Kenngrößen im Netz bestimmen maßgeblich die von den Nutzern wahrgenommene Qualität der Anwendungen. Neben den Real-Zeit-Anwendungen wie z.B. Video-Konferenzen sind dies meistens Datenübertragungen. Hier ist für den Nutzer das sichtbare Qualitätsmerkmal die für einen einzelnen Datenstrom verfügbare Bandbreite oder präziser: der Datendurchsatz, welcher durch das Transportprotokoll TCP unter Berücksichtigung des im Netzwerkpfad vorhandenen Paketverlustverhältnisses und der Einweglaufzeit gesteuert wird.

Bei dieser Anwendung darf jedoch nicht vergessen werden, dass TCP alleine in den End-Systemen implementiert ist, und dort der jeweils eingesetzte ‚TCP-Dialekt' und dessen einstellbare Parameter ebenso die Qualität bestimmende Größen sind.

Daher werden in der perfSONAR Infrastruktur die Messpunkte auch als Referenzsysteme betrieben, zwischen denen mittels BWCTL außerdem periodische TCP-Messungen durchgeführt werden. Es wird somit die Qualität an der Schnittstelle zur Anwendungsschicht verifiziert, oder aber eventuell bestehende Probleme im Netz werden erkannt, welche alleine durch die Basis-Kenngrößen nicht erfasst werden können.

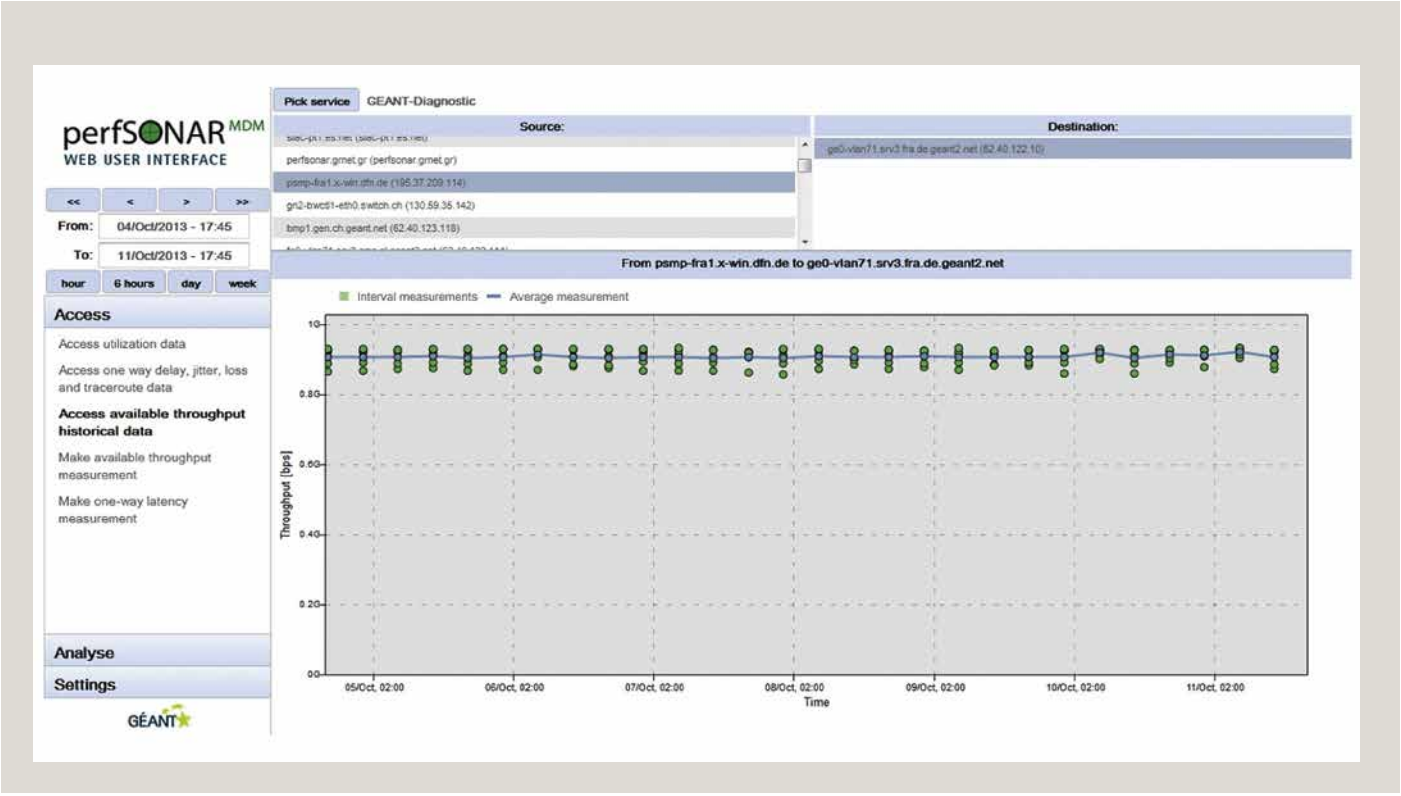
Zusätzlich dienen die Messergebnisse als Referenz und unterstützen die Ursachenfindung und Lokalisierung bei komplexen Ende-zu-Ende Performance-Problemen.

Nutzung des perfsonarUI zur Analyse von Performance-Problemen

Derzeit wird die Messinfrastruktur im X-WiN um weitere perfSONAR-Komponenten erweitert. Damit wird eine effektivere Analyse von Performance-Problemen ermöglicht und darüber hinaus die Kompatibilität mit weiteren perfSONAR-basierten Messinfrastrukuren in internationalen Forschungsnetzen hergestellt. Insgesamt wird dadurch die Möglichkeit geschaffen, Performance-Probleme nicht nur über das X-WiN, sondern auch über internationale Pfade effektiv zu analysieren und schließlich deren Ursachen aufzuspüren.

Eine wichtige Komponente darunter ist eine effektiv nutzbare grafische Benutzeroberfläche. Im europäischen GN3-Projekt wurde dazu das webbasierte perfsonarUI entwickelt. Eine Instanz des perfsonarUI wurde im X-WiN zur Nutzung für das DFN-NOC installiert. Damit werden dort Experten befähigt, bedarfsgerechte Messungen zwischen den Messpunkten durchzuführen und auf historische Messergebnisse zuzugreifen. Zugleich kann das perfsonarUI eine Ansicht von passiv gemessenen Interfacezählern in den Routern entlang eines gegebenen Pfades bieten und so eine Sicht auf die Auslastung und Fehlerzähler einzelner Links ermöglichen.

Die Ursachensuche bei einem Performance-Problem kann im ersten Ansatz mit Hilfe des perfsonarUI effektiv nach einem festen Schema ablaufen: Zuerst wird der Pfad durch das Netz zwischen zwei Messpunkten direkt oder möglichst nahe an den Endpunkten erfasst. Im nächsten Schritt werden die Abschnitte im Ende-zu-Ende-Pfad weiter analysiert. Über die Pfadabschnitte werden vorhandene Messergebnisse der Einweglaufzeiten, der TCP-Durchsätze und der Interface-Zähler aus den Routern im Pfad verglichen und hinsichtlich Auffälligkeiten untersucht. Falls es während der Analyse noch fehlende Messergebnisse gibt, dann können diese bedarfsgerecht durch weitere Messungen ergänzt werden. Während der anschließenden Ursachensuche gibt es viele Verzweigungen in der Analyseprozedur. Dabei sind die von



Periodische Datendurchsatzmessungen zwischen DFN und GÉANT über den Zeitraum einer Woche, dargestellt im User-Interface ‚perfsonarUI'.

perfSONAR bereitgestellten Messwerkzeuge und Messwerte ein unverzichtbares Hilfsmittel.

Hardware für die Messpunkte

Für die ausschließliche Messung der Einweglaufzeiten werden in den X-WiN-Knoten seit einigen Jahren Messrechner mit besonders genauen Uhren betrieben, die ihr Zeitsignal über Antennen von GPS-Satelliten erhalten.

Parallel dazu wurden im Bedarfsfall die Software-Komponenten HADES und BWCTL auf getrennter Hardware eingesetzt. Diese Art der Messungen stellt zwar keine besonderen Anforderungen an die Zeitgenauigkeit im Messrechner, aber zunehmend höhere Anforderungen an die Geschwindigkeit bei Datenerzeugung, Datentransport und Datenverarbeitung.

Im Zuge der X-WiN-Leistungssteigerung wurde aufgrund der gestiegenen Anforderungen an die Messpunkte hinsichtlich Leistungsfähigkeit und Kontinuität der Qualitätsmessungen, aber auch zur Verringerung des Betriebsaufwands, Platz- und Stromverbrauchs eine neue Hardware-Generation für die Messpunkte im X-WiN zusammengestellt. Die neue Hardware basiert auf Standard-Servern mit Multiprozessor-Architektur und ist platzsparend in den X-WiN-Knoten integrierbar. Dabei bestand eine Herausforderung darin, die Hardware für die Messpunkte so auszulegen und die Software so anzupassen, dass sowohl die datenintensiven Durchsatzmessungen als auch die zeitgenauen Einweglaufzeiten gleichzeitig und mit unverändert hoher Genauigkeit durchgeführt werden können.

Nach ersten Tests im Labor und Anpassung der Software wurde das neue Betriebsmodell der Messpunkte an zunächst wenigen Testinstallationen im X-WiN erfolgreich verifiziert, so dass nun während des weiteren Umbaus der X-WiN-Knoten sukzessive die alten Messpunkte ersetzt werden können. ◆

Berlin – Bischkek in 101 Millisekunden

Die Seidenstraße ist bekannt als eine legendäre Reiseroute, die sich über tausende von Kilometern von Europa über den Nahen und Mittleren Osten bis nach China erstreckte. Der Austausch von Informationen und Waren auf diesem Weg dauerte einst viele Monate. Dank des von der europäischen Netzwerkorganisation DANTE Ltd. koordinierten zentralasiatischen Forschungsnetzes CAREN und dessen Anbindungen an den europäischen Wissenschaftsbackbone GÉANT braucht es heute nur Millisekunden, um tausende von Kilometern zwischen Zentralasien und Europa zu überbrücken. Wissenschaftler aus Turkmenistan und Kirgisistan arbeiten heute dank CAREN intensiv mit Kollegen aus Deutschland zusammen. Sie führen Projekte im Bereich grüner Technologien durch, erforschen gemeinsam die Gletscherschmelze in Europa und Asien und betreiben ein gemeinsames Frühwarnsystem für Flutkatastrophen in Bergregionen.

Text: **Anna Roth** (DFN-Verein)

Highspeed-Link für zentralasiatische Wissenschaftler

Verantwortlich für diese moderne Hochgeschwindigkeitsverbindung zwischen Europa und Zentralasien ist die europäische Netzwerkorganisation DANTE (Delivery of Advanced Network Technology to Europe) in Zusammenarbeit mit der europäischen Kommission und den nationalen Forschungsnetzen in Europa und Asien. DANTE Ltd. engagiert sich neben dem Betrieb des europäischen Backbones GÉANT und dem Aufbau interkontinentaler Verbindungen seit vielen Jahren auch für die Förderung von überregionalen Wissenschaftsnetzinitiativen insbesondere in Schwellenländern. Neben dem Flaggschiff-Projekt GÉANT in Europa leitet DANTE Netzwerkprojekte in Afrika, Zentralasien und im Mittelmeerraum. Durch den globalen Ausbau von breitbandigen Wissenschaftsnetzen soll die internationale Zusammenarbeit von Wissenschaftlern stetig gefördert und verbessert werden. Auf dieser Grundlage erst wird es möglich, lokale Projekte, wie die Weiterentwicklung von Solartechnologie und die Installation von Flutwarnsystemen in Zentralasien zu realisieren.

Das Wissenschaftsnetzwerk CAREN (Central Asian Research and Education Network) vernetzt seit Juli 2010 über eine halbe Million Studierende und Wissenschaftler in Zentralasien und stellt direkte Verbindungen nach Europa her. Die angebundenen, nationalen Forschungsnetze sind Kasachstans ‚KazRENA', Kirgisistan ‚KRENA', Tadschikistans ‚TARENA' sowie das turkmenische ‚TuRENA'. Ein potenzieller Kandidat für die Anbindung an CAREN ist derzeit auch Usbekistans Wissenschaftsnetz ‚uzscinet'.

Turkmenistan erzielt „grünen" Fortschritt

Wie wichtig die Unterstützung der zentralasiatischer Forschungsnetze auch für Europa ist, zeigt ein laufendes Projekt in Turkmenistan. Dort ist das lokale Wissenschaftsnetz TuRENA an CAREN gekoppelt und ermöglicht in Verbindung mit dem europäischen Wissenschaftsnetz GÉANT eine internationale Zusammenarbeit im Bereich Solartechnologie. Im Fokus dieser Forschungsarbeit steht die Förderung von ‚grüner Energie'. Dabei sollen nicht nur neue Ressourcen zur Energiegewinnung erschlossen werden, vor allen Dingen sollen lokale Ingenieure mit dem dafür nötigen Wissen versorgt werden.

Das Solarprojekt wird durch eine E-Learning-Plattform namens „e-sapak" unterstützt, die die Bereitstellung und den Austausch von Informationen, Online-Lehrstunden und Videokonferenzen zwischen Europa nach Turkmenistan ermöglicht. Seit Einführung wurden mittels e-sapak und den Verbindungen von CAREN bereits mehr als 700 Studierende und Wissenschaftler aus- und weitergebildet.

Hochland in Tadschikistan, fast die Hälfte des Staatsgebietes liegt auf einer Höhe von über 3000 Metern. *Foto: © annaia/photocase.de*

Mit einem Durchschnitt von 7,4 Sonnenstunden pro Tag bietet Turkmenistan besondere Witterungsverhältnisse, von denen deutsche Forscher profitieren können. Dort kann die Solartechnologie unter deutlich besseren klimatischen Bedingungen getestet werden als in Deutschland. Gemessen wird diese Leistung in Echtzeit über ein von der Turkmenistan Academy of Science bereitgestelltes Testbed. Das ermöglicht die Untersuchung der Einflüsse von Temperatur, UV-Strahlung, Windgeschwindigkeit und Staub auf die Energieproduktion ohne Zeitverzögerungen.

Eine spezielle Web-Box misst meteorologische Daten wie Feuchtigkeit, Sonnenstrahlung, Temperatur oder Luftdruck. Die Wissenschaftsnetze CAREN, GÉANT, X-WiN und TuRENA stellen sicher, dass Daten in Echtzeit von Turkmenistan nach Deutschland gelangen. Dadurch ist es den Wissenschaftlern in beiden Ländern möglich, flüssig und schnell miteinander zu kommunizieren, um die Leistung des Equipments stetig zu optimieren. Die Echtzeit-Überwachung von Leistungsdaten soll fester Bestandteil eines zukünftigen Kontroll- und Überwachungssystems werden.

Letztendlich soll die Kombination von E-Learning und Überwachung die Möglichkeit eröffnen, in Turkmenistan eine dynamische Solarindustrie aufzubauen. Für die Pläne, in Zukunft nachhaltige Energie bereitzustellen, ist die Zusammenarbeit der Wissenschaftsnetzwerke essentiell und wird daher weiterhin im Fokus der Förderung stehen.

Kirgisistan erzielt nachhaltigen Fortschritt

Circa tausend Kilometer östlich von Turkmenistan liegt Kirgisistan. In dem gebirgigen Binnenstaat, der im Norden an Kasachstan und im Süden an China grenzt, erhält die Zusammenarbeit von GÉANT, CAREN, dem nationalen Forschungsnetz KRENA und den nationalen Forschungsnetzen Europas eine wesentliche Bedeutung für die vor Ort lebenden Menschen. Durch schmelzende Gletscher kommt es in Kirgisistan, dessen Landfläche zu 94 % aus Hochgebirgen besteht und dessen höchste Gipfel sich mehr als sieben Kilometer über den Meeresspiegel erheben, oft zu Überflutungen und Schlammlawinen, die das Leben und die Lebensgrundlage der Menschen gefährden. Ein europäisch-kirgisisches Wissenschaftsprojekt widmet sich den für das Land verheerenden Auswirkungen des Klimawandels. „EURAS-CLIMPACT“ heißt das von der EU finanzierte Projekt, das die Einflüsse des Klimawandels auf Gletscher in Österreich, Schweden und Kirgisistan untersucht. Internationale Kooperation bei der Überwachung und der laufender Austausch von Messdaten der schmelzenden Gletscher soll in Europa und Asien ein verständliches Gesamtbild erzeugen, um die Auswirkungen des Klimawandels besser verstehen zu lernen und Präventionsmaßnahmen zum Schutz der Bevölkerung ergreifen zu können.

CAREN im Überblick

Gestartet im Januar 2009, hat das ‚Central Asian Research and Education Network‘ CAREN folgende Ziele:

- Aufbau und Betrieb eines Hochleistungsnetzes für Forschung und Bildung in Zentralasien mit minimalen Verbindungskapazitäten von 34 Mbps.
- Verbesserung der intraregionalen Konnektivität Zentralasiens durch Ersatz bestehender Satellitenverbindungen mit terrestrischen Fasern.
- Förderung von F&E-Kooperationen zwischen Zentralasien und Europa über die Verbindung zum GÉANT.
- Synergien mit User-Communities in den Nachbarregionen Ostasiens (TEIN) und des Südkaukasus (BSI).
- Katalysator für die Entwicklung von nachhaltigen nationalen Forschungsnetzen in den fünf ehemaligen Sowjetrepubliken Kasachstan, Kirgisistan, Tadschikistan, Turkmenistan und Usbekistan.
- Unterstützung und Förderung der Zusammenarbeit von Netzwerkanwendungen in Bereichen mit gesellschaftlichen Auswirkungen wie Telemedizin, Seismologie, E-Learning, Energie- und Wasserressourcen-Management und Umweltwissenschaft .

Traceroute der Datenverbindung von Berlin nach Bischkek. Über X-WiN, GÉANT, CAREN, das kirgisische Forschungsnetz KRENA benötigen die IP-Pakete nur 101 Millisekunden, um von der Geschäftsstelle des DFN-Vereins bis in die Universität von Bischkek zu gelangen.

```
$ traceroute www.university.kg
traceroute to www.university.kg (178.217.170.83), 30 hops max, 60 byte packets
 1  188.1.XXX.XXX (188.1.XXX.XXX)  0.925 ms  1.098 ms  1.238 ms
 2  cr-fra1.x-win.dfn.de (188.1.XXX.XXX)  2.664 ms  2.718 ms  2.768 ms
 3  dfn.mx1.fra.de.geant.net (62.40.124.217)  2.429 ms  2.533 ms  2.528 ms
 4  caren-gw.mx1.fra.de.geant.net (62.40.125.9)  2.466 ms  2.511 ms  2.507 ms
 5  krena.caren-noc.net (195.54.180.110)  100.594 ms  100.410 ms  100.579 ms
 6  178.217.168.26 (178.217.168.26)  101.385 ms  101.632 ms  100.072 ms
```

Nachtansicht von Astana (Kasachstan). *Foto © Cosmopol/iStock.*

Auf über 3000 Metern Höhe im zentralasiatischen Hochgebirge Tien Shan befindet sich die Gottfried Merzbacher Forschungsstation des GeoForschungsZentrums (GFZ) Potsdam. Sie ist der Vorreiter im Bereich der Überwachung und Präventivarbeit, um die Auswirkungen des Klimawandels zu entschärfen. In Zusammenarbeit mit dem Zentralasiatischen Institut für Angewandte Geowissenschaften (ZAIAG) in Bischkek werden zahlreiche Daten über lokale Umweltbedingungen, Eisdicke, Gletschergeschwindigkeit und seismische Aktivitäten gesammelt. Die Wissenschaftsnetze ermöglichen es, dass diese Daten verschiedenen Forschern auf der ganzen Welt über die Geo Database of Central Asia (GDB) zugänglich gemacht werden können. Für den reibungslosen Datenaustausch ist das Projekt auf die Leistungsfähigkeit von Wissenschaftsnetzen angewiesen. Die gesammelten Daten müssen in großer Menge, schnell, verlässlich und auch im Austausch mit abgelegenen Orten transportiert werden. Vor allem bei Überschwemmungskatastrophen und Schlammlawinen ist es unabdingbar, dass Messergebnisse so schnell wie möglich zu Überwachungsstationen und weiter in die Frühwarnsysteme übermittelt werden. Nur so können Frühwarnsysteme funktionieren und Modelle über das weitere Gletscherverhalten zeitnah realisiert werden.

Zu den vorbereitenden Maßnahmen einer nachhaltigen Arbeit gehört auch die Etablierung von E-Learning. Den Auswirkungen des Klimawandels kann nur entgegengewirkt werden, wenn das dafür nötige Wissen vorhanden ist. Durch die Kooperation der Wissenschaftsnetze KRENA, CAREN, DFN und GÉANT sollen Forschern und Studierenden aus Zentralasien und Europa Multimediainhalte wie Karten, Satellitenbilder, geophysikalische Daten und Luftaufnahmen sowie eine umfassende Online-Bibliothek zur Verfügung gestellt werden. Wissenschaftler können durch einen virtuellen Vortragsraum neue Erkenntnisse und Informationen in Echtzeit austauschen. Durch diese Zusammenarbeit können beide Seiten voneinander lernen und ihr Wissen miteinander vernetzen. ◆

Campus

Voice over IP Security – Verteiltes Sensorsystem zur Erkennung von SIP-basierten Angriffen im DFN
von Dirk Hoffstadt, Prof. Dr.-Ing. Erwin P. Rathgeb

Chat in Forschung und Lehre? Sicher!
von Prof. Dr. Marcel Waldvogel, Klaus Herberth, Daniel Scharon

Voice over IP Security – Verteiltes Sensorsystem zur Erkennung von SIP-basierten Angriffen im DFN

Die Kommunikation mit „Voice over IP“ (VoIP) auf der Basis des Session Initiation Protokolls (SIP) löst die klassische Telefonie zunehmend ab und macht die Unterstützung offener SIP-Schnittstellen deshalb auch im Bereich der IP-basierten Nebenstellenanlagen unverzichtbar. Dadurch wird allerdings die Telefonie von einer geschlossenen – und damit vergleichsweise sicheren – Basis auf eine offene, sehr viel verwundbarere Plattform migriert. Einhergehend mit dieser Entwicklung haben sich die Kosten für die VoIP-Telefonate stetig reduziert, wobei auch ein Trend zur Pauschalisierung der Nutzungsentgelte zu beobachten ist. Durch diese technischen und wirtschaftlichen Veränderungen sind neue Risiken und Missbrauchsmöglichkeiten im Bereich der Telefonie entstanden.

Text: **Dirk Hoffstadt, Prof. Dr.-Ing. Erwin P. Rathgeb** (Universität Duisburg-Essen)

Foto © Yeko Photo Studio/fotolia.de

Eine Problematik besteht darin, dass die geringen Kosten für VoIP-Telefonate die Telefonie attraktiv für den Missbrauch von Anrufen zum Zwecke der Werbung oder Störung gemacht haben. Diese Problematik wird allgemein mit dem Begriff SPIT (SPAM over Internet Telephony) bezeichnet. ‚Toll Fraud' ist eine zweite Problematik, die durch die flächendeckende Einführung von VoIP kritisch werden kann. VoIP bietet die Möglichkeit, sich unabhängig vom aktuellen Aufenthaltsort über das Internet bei dem jeweiligen Heimatnetzbetreiber anzumelden und über das dortige Nutzerkonto Gespräche zu führen. Da Gespräche in die Mobilfunknetze, zu Sonderrufnummern und ins Ausland weiterhin oft nicht pauschaliert abgerechnet werden, ist es attraktiv, sich durch gefälschte Anmeldungen an fremden Nutzerkonten solche Gespräche kostenlos zu erschleichen. Ein DoS-Angriff auf VoIP-Server darf als dritte Problematik ebenfalls nicht vernachlässigt werden.

Mehrjährige Untersuchungen [1-4] des Lehrstuhls „Technik der Rechnernetze" an der Universität Duisburg-Essen zeigen, dass an das Internet angeschlossene Kommunikationsanlagen mit SIP-Schnittstellen schnell entdeckt werden und dass in der Folge mehrstufige Angriffsversuche unternommen werden. Ähnlich wie bei der Entwicklung der Bedrohungen für Internetrechner durch Würmer, Denial of Service, SPAM und andere Angriffe sind die momentan auftretenden Angriffe als Vorboten eines stetig wachsenden neuen „Marktes" anzusehen. Ein Feldtest, der im September 2008 begann und bis heute aktiv ist, zeigt, dass das Angriffsmuster ‚Toll Fraud' anfangs nur sporadisch auftauchte, seit Anfang 2010 jedoch kontinuierlich zunimmt. Dieser vierstufige Angriff tritt inzwischen mit deutlich höherer Intensität auf (mehrere Millionen SIP-Nachrichten pro Tag). Die Analysen des Datenbestands zeigen nun deutlich, dass neben automatisierten Angriffswerkzeugen (Sipvicious, sundayddr) für die Übernahme von Accounts (Registration Hijacking) auch manuelle, gezielte Angriffe mit Softphones erfolgen, um die übernommenen Accounts zum Telefonieren zu verwenden (z.B. Anrufe in das Ausland). Daher ist anzunehmen, dass das Aufkommen solcher Angriffe in den nächsten Jahren weiterhin steigen wird – insbesondere da zunehmend umfangreiche SIP-Funktionalität in weit verbreitete Home-Gateways (z.B. FritzBox) und TK-Anlagen integriert wird und zukünftig auch direkte Verbindungen zwischen Endgeräten (ohne Mitwirkung von SIP-Infrastrukturkomponenten) möglich werden.

Im Rahmen des vom BMBF geförderten Projektes „Schutz vor Missbrauch und Bedrohung von VoIP-Netzwerken (SUNSHINE)" [5] wurde in Zusammenarbeit mit Fraunhofer FOKUS, der GeNUA mbH und der ISACO GmbH sowie den Industriepartnern Kabel Deutschland und der TELES AG ein Framework zur Verhinderung von Betrug und Missbrauch auf der Basis von VoIP-Kommunikationstechnologien entwickelt. Eine Hauptkomponente des Frameworks ist das „Security Sensor System", das vom Lehrstuhl Technik der Rechnernetze entwickelt wurde. Dieses kann auch eigenständig genutzt werden und wird in einer erweiterten Form in diesem Beitrag vorgestellt.

Security Sensor System

Grundkonzept

Das Security Sensor System basiert auf einer verteilten, zustandsbehafteten Analyse von SIP-Nachrichten. Bei den Sensoren handelt es sich um eine leichtgewichtige Softwarekomponente, die verteilt auf verschiedenen Hardware- und Softwareplattformen eingesetzt werden kann. Mit einem XML-Regelwerk für bekannte Angriffe wird die signaturbasierte Erkennung von SIP-basierten Angriffen in Echtzeit ermöglicht. Die Erkennung verläuft vollständig passiv, so dass der Sensor auch in produktiven Umgebungen eingesetzt werden kann, ohne Störungen zu verursachen (z.B. Monitoring-Port). Zur optimalen verteilten Erkennung sind die Sensoren durch eine Kommunikations- und Steuerungsschnittstelle an den zentralen Sensordienst (SCS) angeschlossen. Erkannte Angriffe werden automatisch an den SCS gemeldet. Dieser dient der Verwaltung der verteilten Sensoren (Konfiguration, Regelwerk, Management) und der Korrelation der empfangenen Sensor-Alarmmeldungen auf der Basis von SCS-Regeln, so dass Abwehr-Komponenten (z.B. Firewall) in Echtzeit benachrichtigt werden können.

Implementierung

Der Sensor Central Service (SCS) stellt für alle Sensoren die Konfiguration sowie die Verteilung der Signaturen bereit und nimmt die Alarmmeldungen der Sensoren im Falle eines Angriffs (Regelverletzung) entgegen. Die Kommunikation zwischen SCS und Sensor erfolgt TLS-verschlüsselt (HTTPS) und ist mit Zertifikaten abgesichert. Die Sensoren authentisieren sich am Zentraldienst mithilfe einer Sensor-

[1] Dirk Hoffstadt, Stefan Monhof, and Erwin P. Rathgeb, „SIP Trace Recorder: Monitor and Analysis Tool for threats in SIP-based networks," in TRaffic Analysis and Classification Workshop (IWCMC2012-TRAC), Limassol, Cyprus, Aug. 2012.
[2] Dirk Hoffstadt, Alexander Marold, and Erwin Rathgeb, „Analysis of SIP-Based Threats Using a VoIP Honeynet System," in Conference proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012), Liverpool, UK, 2012.
[3] Hoffstadt, Dirk; Wolff, Niels; Monhof, Stefan; Rathgeb, Erwin P.: Improved Detection and Correlation of Multi-Stage VoIP Attack Patterns by using a Dynamic Honeynet System In: ICC 2013 : IEEE International Conference on Communications; June 9, 2013 - June 13, 2013, Budapest, Hungary Piscataway, NJ: IEEE (2013)
[4] Aziz, Adnan; Hoffstadt, Dirk; Ganz, Sebastian; Rathgeb, Erwin P.: Development and Analysis of Generic VoIP Attack Sequences Based on Analysis of Real Attack Traffic In: Conference proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-13); Melbourne, Australia, 16-18 July, 2013 Piscataway, NJ: IEEE (2013)
[5]: D. Hoffstadt, E. Rathgeb, M. Liebig, Y. Rebahi, and T. Q. Thanh "A Comprehensive Framework for Detecting and Preventing VoIP Fraud and Misuse," International Conference on Computing, Networking and Communication (ICNC), February, 2014.

ID und eines Passworts, welche bei jeder Anfrage mitgeschickt werden.Die Verwendung von HTTP-Keep-Alive ermöglicht den Austausch vieler Anfragen und Antworten, ohne dass neue TCP- oder SSL-Verbindungen aufgebaut werden müssen.

Die von den Sensoren empfangenen Reports werden in einer MySQL-Datenbank gespeichert und durch die Analysekomponente unter Berücksichtigung der SCS-Regeln verarbeitet. Mit Hilfe der SCS-Regeln können Zusammenhänge bzw. Abhängigkeiten zwischen einzelnen Sensor-Regeln definiert werden. Ist eine SCS-Regel zutreffend, können verschiedene Aktionen über das „Export Interface“ durchgeführt werden, wie z.B. das Senden einer Benachrichtigung an eine Firewall zum Blockieren eines aktuell laufenden Angriffs. Die Management-Website informiert über den aktuellen Status der angebundenen Sensoren inklusive des Standortes und der eindeutigen Sensor-ID. Weiterhin können eingehende Alarmmeldungen der Sensoren eingesehen und die Verarbeitung der SCS-Regeln kontrolliert werden.

Der Sensor ist objektorientiert in C++ bzw. in Java entwickelt und verwendet die Bibliothek „libpcap“, die eine einfache Arbeit mit Netzwerkschnittstellen und Plattformunabhängigkeit ermöglicht. Verschiedene Prozessorarchitekturen, wie x86/x64, MIPSEL (FRITZ!Box) oder ARM (Raspberry Pi) werden unterstützt. Die dabei eingesetzten Betriebssysteme basieren auf Linux.

Die Angriffssignaturen beschreiben eine Folge von SIP-Nachrichten, für die gewisse zeitliche Bedingungen gelten (z.B. „alle Nachrichten einer Regel müssen innerhalb von 5 Sekunden empfangen werden“). Die SIP-Header-Felder sowie Netzwerk- und Transportschicht-Informationen (IP-Adressen und Ports) können innerhalb der Signaturen mit fest vorgegebenen Werten oder mit Werten von früheren Nachrichten der Folge verglichen werden. Der Sensor sammelt und filtert SIP-Nachrichten (per PCAP-Filter). Alle gesammelten SIP-Nachrichten werden sofort in eine Warteschlange gestellt, auf die der nächste Prozess zugreift. Dies ermöglicht eine nebenläufige Verarbeitung der SIP-Nachrichten. Alle eingehenden SIP-Nachrichten werden mit den vordefinierten Angriffssignaturen verglichen. Dazu werden die SIP-Nachrichten einzeln der Warteschlange entnommen und mit der ersten Nachricht jeder Angriffssignatur verglichen. Da jede Signatur eine Folge von SIP-Nachrichten enthalten kann, werden die eingehenden SIP-Nachrichten zusätzlich mit bereits aktiven Signaturen verglichen. Dabei werden die definierten zeitlichen Bedingungen berücksichtigt. Sollten für eine Nachricht alle Vergleiche negativ ausfallen, wird die Nachricht ignoriert. Fällt der Vergleich einer Nachricht mit der letzten Nachricht einer aktiven Angriffssignatur positiv aus, so wird eine Benachrichtigung an den zentralen Dienst gesendet. Die Benachrichtigung enthält die eindeutige Nummer der verletzten Regel, die Sensor-ID, einen Zeitstempel sowie die Quell- und Ziel-IP-Adresse (inkl. Port-Angaben).

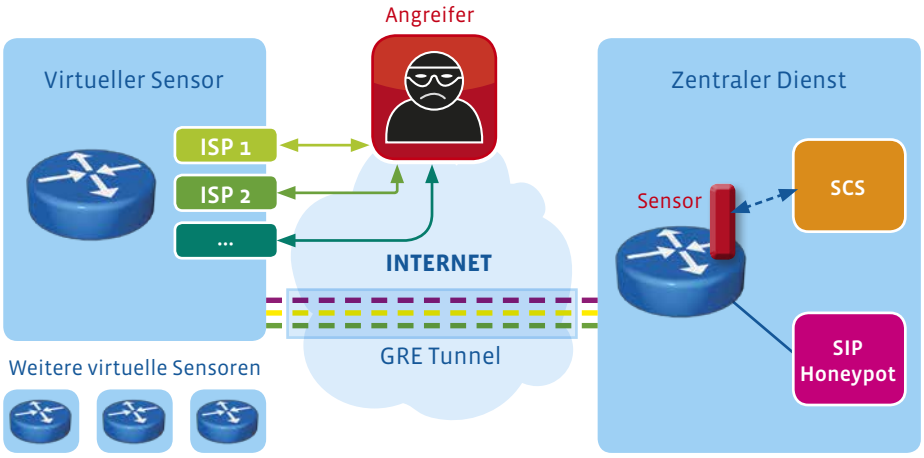


Abb. 1: Architektur virtueller Sensor.

Szenarien

Die beschriebene verteilte Architektur eignet sich besonders für Produktivnetzwerke, da hier aus datenschutzrechtlichen Gründen über die IP-Adresse hinaus keine personenbezogenen Daten der Kommunikationsverbindung an den SCS übertragen werden, so dass kein Rückschluss auf die Telefonie-Verbindung möglich ist (z.B. Rufnummern, Nebenstellen). Die Voraussetzung für dieses Einsatzszenario ist jedoch die Installation und der Betrieb der Softwarekomponente an jedem Standort mit SIP-Komponenten, so dass sich ein entsprechender Aufwand für die Integration des Sensors in das Produktivnetz ergibt.
Um die Erkennung von SIP-basierten Angriffen zu vereinfachen und weitere Messstellen im Internet ohne produktiven SIP-Verkehr zu erschließen, wurde in Zusammenarbeit mit der Forschungsplattform NorNet [6] ein neuer, erweiterter Ansatz für das Sensorsystem entwickelt. Mit Hilfe dieser neuen „virtuellen Sensoren“ ist es mit geringstem Aufwand möglich, beliebige öffentliche IP-Adressen als Messstelle in das System zu integrieren. Das System ist sehr gut skalierbar und alle aktiven, ressourcenbeanspruchenden Komponenten befinden sich an einem zentralen Standort, so dass für den virtuellen Sensor an der eigentlichen Messstelle ein nur minimaler Aufwand besteht. Das Ziel dieses Szenarios ist das großflächige Monitoring von Angreifer-Aktivitäten. Um die Erkennung der gesamten Angriffskette zu ermöglichen, müssen ankommende SIP-Anfragen beantwortet werden. Hierzu wird

[6] D. Thomas: `The NorNet Testbed: A Platform for Evaluating Multi-Path Transport in the Real-World Internet, in Proceedings of the 87th IETF Meeting, Berlin/Germany, July 30, 2013.

außerhalb von Produktivnetzwerken eine VoIP-Nebenstellenanlage mit Hilfe eines Honeypot-Systems nachgebildet.

Abbildung 1 zeigt die Architektur des Systems mit virtuellen Sensoren. Am Standort Essen befindet sich nur ein einzelner, zentraler Sensor, der direkt vor Ort mit dem SCS gekoppelt ist. Darüber hinaus existiert hier die aktive Honeypot-Instanz. Durch die Anordnung der Analyse- und Honeypot-Komponenten auf nur einem Server in Essen werden die Wartung und die Fehlerbehebung stark vereinfacht. Dieser zentrale Standort ist über VPN-Tunnel (GRE-Protokoll) mit Standorten auf der ganzen Welt verbunden, wo sich jeweils ein virtueller Sensor befindet. Bei den virtuellen Sensoren handelt es sich um virtuelle Maschinen oder kleine Embedded-Systeme, die über ein Standard-Linux-System verfügen. Mit Hilfe von Linux-Bordmitteln werden eingehende SIP-Pakete durch die VPN-Tunnel an das Honeypot-System in Essen weitergeleitet. Dort wird der gesamte eingehende SIP-Datenverkehr durch den zentralen Sensor analysiert und bei Verletzung einer Regel wird automatisch eine Benachrichtigung an den SCS versendet. Es ist wichtig, dass der gesamte Angriffsverkehr von einem virtuellen Sensor zum Honeypot-Server und über den gleichen Weg zurück zum Angreifer geleitet wird. Mit Hilfe von Routingregeln werden die vom Honeypot generierten Antwortpakete durch den zugehörigen Tunnel wieder an die eingehende, öffentliche Schnittstelle des entsprechenden virtuellen Sensors zurückgeleitet, so dass die interne Struktur für den Angreifer verborgen bleibt. Aus der Sicht des Angreifers erfolgt lediglich eine Kommunikation zwischen virtuellem Sensor und dem Angreifer.

Der Aufwand und das Risiko für den Betrieb einer Messstelle auf Basis des virtuellen Sensors sind minimal, da für die Messung unbelegte IP-Adressen verwendet werden können und kein Kontakt zu Produktivnetzwerken notwendig ist (z.B. Installation in der DMZ). Es besteht kein Installations- oder Managementaufwand, da der virtuelle Sensor betriebsbereit als virtuelle Maschine oder als kleine Hardwarebox zur Verfügung gestellt wird. Die technischen Details zu diesem Ansatz wurden in [7] veröffentlicht. Analyse- oder Honeypot-Komponenten müssen im Vergleich zum verteilten Ansatz nicht betrieben werden, so dass die Paketweiterleitung mit sehr geringen Ressourcen möglich ist. Der zentrale Ansatz eignet sich besonders für Forschungsnetze mit breitbandiger Anbindung, wie z.B. DFN oder NorNet, da hier die Weiterleitung von Paketen nicht durch asymmetrische oder langsame Verbindungen behindert wird.

Betriebserfahrung

Das Szenario mit virtuellen Sensoren wird im NorNet bereits seit Oktober 2013 erfolgreich eingesetzt. Aktuell sind 16 Messstellen aktiv, die über 28 unterschiedliche Provider (öffentliche IP-Adressen z.B. in Norwegen und China) angebunden sind. Bis heute wurden aus über 6 Millionen Paketen 2.644 unterschiedliche Angreifer auf Basis der Quell-IP-Adresse erkannt. Die ersten Auswertungen zeigen, dass die Bedrohung auf SIP-Komponenten stetig ansteigt. Angreifer suchen großflächig über Netzwerkgrenzen hinweg nach aktiven SIP-Servern und greifen diese dann gezielt an, um Nebenstellen zu übernehmen.

Im DFN konnte durch die Kooperation mit der Universität Kaiserslautern der erste virtuelle Sensor installiert werden. Dieser wurde in Form einer vorkonfigurierten virtuellen Maschine an das Rechenzentrum übergeben und dort mit geringem Aufwand in Betrieb genommen. Seit dem 25.02.2014 sind am Standort Kaiserslautern 37.510 SIP-Angriffspakete eingegangen und 259 Angreifer wurden identifiziert. Neben dem Auffinden von SIP-Servern (114 Angriffe) wurde auch hier deutlich, dass die Angreifer Accounts übernehmen wollten (97 Angriffe). Darüber hinaus hat das System bereits 57 ‚Toll Fraud'-Versuche zu unterschiedlichen Zielrufnummern detektiert (siehe Abbildung 2). Die ersten Angriffsstufen werden mit im Internet freierhältlichen Toolboxen wie z.B. SIPvivious („friendly-scanner") durchgeführt. Für die ‚Toll-Fraud' - Versuche werden hingegen bekannte Softphones verwendet (z.B. Eyebeam).

Damit wir die flächendeckende Überwachung der SIP-basierten Angriffe weiter ausbauen und somit verlässliche Daten für Abwehrkomponenten zur Verfügung stellen können, suchen wir innerhalb des DFN dringend weitere Kooperationspartner, die mit geringstem Aufwand eine eigene Messstelle in Betrieb nehmen würden. ◆

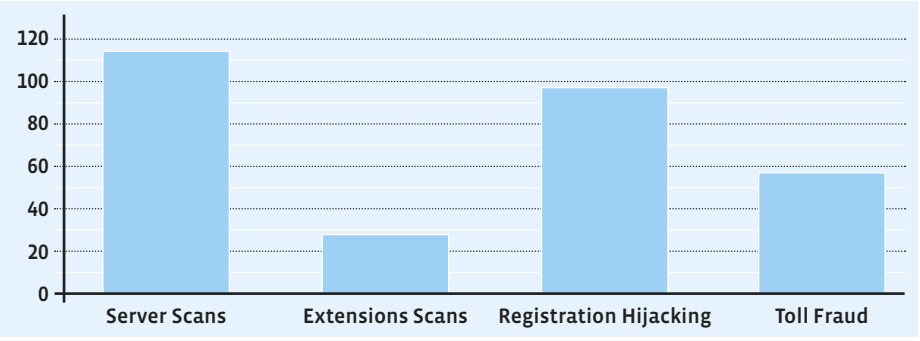


Abb. 2: Anzahl der Angriffe pro Angriffstyp (Kaiserslautern).

[7] Adnan Aziz, Dirk Hoffstadt, Erwin Rathgeb:, Thomas Dreibholz: A Distributed Infrastructure to Analyse SIP Attacks in the Internet; IFIP Networking 2014; Trondheim, Norway; 2014

Chat in Forschung und Lehre? Sicher!

Instant Messaging, Audio- und Videoanrufe, kurz Chat, ist aus unserem täglichen Leben nicht mehr wegzudenken. Die meisten nutzen dafür geschlossene Systeme, die für den Privatgebrauch bequem sind, für den dienstlichen Einsatz in Forschung und Lehre aber an Datenschutz und Privatsphäre scheitern. Das muss nicht so sein: Auf Basis des offenen, föderierten Extensible Messaging and Presence Protocols (XMPP) bietet WISEchat webbasiert und -integriert die Sicherheit, den Komfort und die Erweiterbarkeit, die eine moderne Hochschule braucht. Die Hintergründe, Vorteile und Zukunftssicherheit erläutern wir anhand einiger konkreter Beispiele.

Text: **Prof. Dr. Marcel Waldvogel, Klaus Herberth, Daniel Scharon** (Universität Konstanz)

Foto © S. Engels/fotolia.com

Herausforderungen

- Heterogene Nutzerschaft
- Keine Medienbrüche und neue Adressen
- Datenschutz (Personalabteilung, Studierendenadministration, Studienberatung, Fernwartung, ...)
- Höchste Privatsphäre (psychologische Beratung)
- Organisationsübergreifende Kommunikation
- Einfach nutzbar und integrierbar (auch webbasiert)

Die Hochschulen bieten ein wachsendes und flexibles Portfolio an Dienstleistungen für eine sehr heterogene Klientel an, welche stetigen Änderungen unterliegt. Dadurch ist es besonders wichtig, dass Unklarheiten, Rückfragen und Anliegen möglichst einfach und unkompliziert erledigt werden.

Heute erfolgt das häufig über den Medienbruch zum Telefon: Internes Telefonverzeichnis aufrufen; Name eingeben; hoffen, dass die Telefonnummer der richtigen Frau Meier gehört; zum Telefonhörer greifen und diese Nummer eingeben. Wie viel einfacher wäre es doch, wenn direkt beim Erhalt der unklaren E-Mail – unabhängig vom verwendeten Programm – direkt eine Chatrückfrage gestellt werden könnte, je nach Anspruch mittels Text, Audio oder Video.

Der Bedarf beschränkt sich jedoch nicht allein auf Kommunikation innerhalb einer Hochschule. Nicht nur Forscher sind in ständig wechselnden Konstellationen über die Hochschulgrenzen hinaus aktiv und möchten ihre Kommunikation mit möglichst wenig Aufwand erledigen. Neben den DFN-Diensten Video- und Webkonferenz [1] für formelle oder regelmäßige Nutzung weichen sie häufig auf Dienste wie Skype aus, die für Ad-hoc-Treffen mit beliebigen Teilnehmern schneller und einfacher sind.

Einfachheit als Ziel

Für den dienstlichen Einsatz in Forschung und Lehre sind ‚Skype', ‚Google Hangout' und ähnliche Tools nicht geeignet: Sie können weder in bestehende Abläufe integriert werden, noch genügen sie den Erfordernissen des Datenschutzes und den Anforderungen an den Schutz der Privatsphäre[2]. Für eine breite Akzeptanz jeden Dienstes ist aber die einfache Nutzung das A und O. Dazu zählt insbesondere, dass für die ersten Schritte keine Softwareinstallation notwendig sein darf [3] – ein Ziel, welches mittels dem hier vorgestellten sicheren Chat (WISEchat: Web, integrated, secure, extensible chat) vollständig erreicht wird.

XMPP?

Das Extensible Messaging and Presence Protocol (XMPP, 1999 als Jabber gegründet), ist ein gemeinsam von der ‚Internet Engineering Task Force' und der ‚XMPP Standards Foundation' vorangetriebener, offener und erweiterbarer Kommunikationsstandard auf Basis von XML. Neben den ursprünglichen Zielen, Instant Messaging und Anwesenheitsinformationen auszutauschen, wurde dies in der Zwischenzeit vielseitig erweitert. Zusätzlich zu Mainstreamfunktionen wie Verwaltung von Freundeslisten, Diskussionräumen, Verbindung über Audio und Video gibt es auch Clients, welche mit dem von XMPP zur Verfügung gestellten Transportmechanismus zusätzlich anwendungsspezifische Protokolle wie z.B. für kollaborative interaktive Whiteboards anbieten.

Die Client-/Server-Struktur von XMPP ähnelt der von Email: Die Programme der Nutzer verbinden sich mit dem XMPP-Server der lokalen Einrichtung. Die XMPP-Server bilden auf Basis der DNS-Einträge und der Kontaktwünsche der Nutzer eine dynamische Föderation. Für den Benutzer verläuft das transparent und unter Schutz seiner Privatsphäre, da nur Informationen geteilt werden, die er freigegeben hat.

Eigenschaften von XMPP

- Offener Standard mit vielen Clients
- Keine zusätzliche Adresse (gleich wie E-Mail)
- Autokonfiguration
- Globale Föderation (keine zentrale Instanz)
- Server einfach aufzusetzen
- Unterstützt Instant Messaging, Audio-/Videogespräche und -konferenzen, Desktop Sharing u.v.a.m.
- Privatsphäre und Sicherheit werden großgeschrieben
- Einbettung in Webseiten, -anwendungen und -prozesse
- Synchrone und asynchrone Kommunikation

[1] https://www.vc.dfn.de
[2] Heise Security: „Vorsicht beim Skypen – Microsoft liest mit", http://heise.de/-1857620 (14. Mai 2013) und Heise News: „Neue Nutzungsbedingungen bei Skype: Zentrale Zwischenspeicherung und Kontrollen", http://heise.de/-2126390 (27. Februar 2014)
[3] Unsere Erfahrung zeigt, dass sich viele Nutzer lieber regelmäßig in ein Webmailsystem einloggen und Beschränkungen bei Komfort und Funktionsumfang in Kauf nehmen, als einen lokalen Mailclient zu installieren. Selbst auf den winzigen Bildschirmen der Smartphones kämpfen sich einige lieber durch Webmail.
[4] http://j-u-n-e.org

In Deutschland bieten rund 40 Hochschulen XMPP an, viele davon sind im Jabber University Network (JUNe) zusammengeschlossen [4]. Viele Hochschulen weltweit, aber auch Freemailanbieter von GMX bis Google bieten ihren Nutzern ebenfalls XMPP-Zugang, so dass mit XMPP die ganze Welt offensteht.

WISEchat!

Wie oben erläutert ist es schwierig, Forscher und Studierende zur Installation oder gar Nutzung von neuen Anwendungen zu motivieren, besonders wenn es „nur“ um mehr Sicherheit geht. Für viele Arbeitsvorgänge ist das aber auch gar nicht notwendig: Homepages von Forschern, Informationsseiten der Verwaltung, Support- und Beratungsseiten, Webmail oder sonstige Groupware begleiten uns bei der täglichen Arbeit im akademischen Umfeld. Es ist unmöglich, alle Informationen auf allen Seiten immer aktuell zu halten und alle möglichen Spezialfragen zu beantworten; dann aber sollte zumindest die Möglichkeit zur unmittelbaren Rückfrage gegeben sein.

Dank der massiven Fortschritte der letzten Jahre bei den offenen Webstandards wie HTML5 und WebRTC kann nun vieles, was früher nur mit Spezialanwendungen machbar war, auch mit offenen Standards erledigt werden. WISEchat stellt vor diesem Hintergrund ein Konzept dar, welches durch einfachste Integration bestehende Webseiten und -anwendungen transparent um Funktionen für Instant Messaging inklusive Videokonferenz erweitern und neue Beratungs- und Kommunikationskanäle eröffnen kann, bei denen die Privatsphäre durch Ende-zu-Ende-Verschlüsselung gesichert ist.

Das Konzept WISEChat wird an der Universität Konstanz mittels der Open-Source-Bibliothek jsxc[5] (Javascript XMPP Client) umgesetzt. Im Folgenden finden sich einige Anwendungsbeispiele und Nutzungsmöglichkeiten.

Webmail und Groupware

Eine der offensichtlichsten Integrationsmöglichkeiten bietet Webmail: Statt auf eine frisch eingegangene Mail mit einem Pingpong an Rückfragen zu reagieren, kann der Absender direkt kontaktiert werden. Dank der Integration der Chatfunktion als Javascript-Bibliothek können direkt im Browser Emailadressen identifiziert, mit der Freundesliste abgeglichen und mit Bullets versehen werden, welche anzeigen, ob der Nutzer hinter dieser Adresse online ist. Über diese Bullets ist auch die andere Richtung der nahtlosen Integration möglich: Ein Klick darauf, und ein Chatfenster öffnet sich.

Native Clients

- Windows: Jitsi, Pidgin, Gajim
- MacOS X: Jitsi, Adium
- Linux: Jitsi, Pidgin, Gajim, Telepathy
- Android: Xabber, ChatSecure, Jitsi
- iOS: Monal, ChatSecure

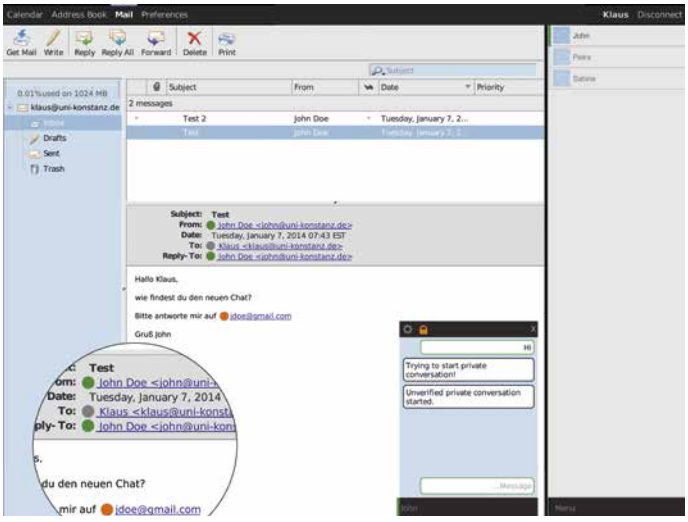


Abb. 1: Die Groupware SOGo, rechts mit WISEchat. Die Chatfunktion hat Emailadressen aus der Hauptapplikation extrahiert und mit Präsenzbullets annotiert, welche auch direkt einen Chat starten können.

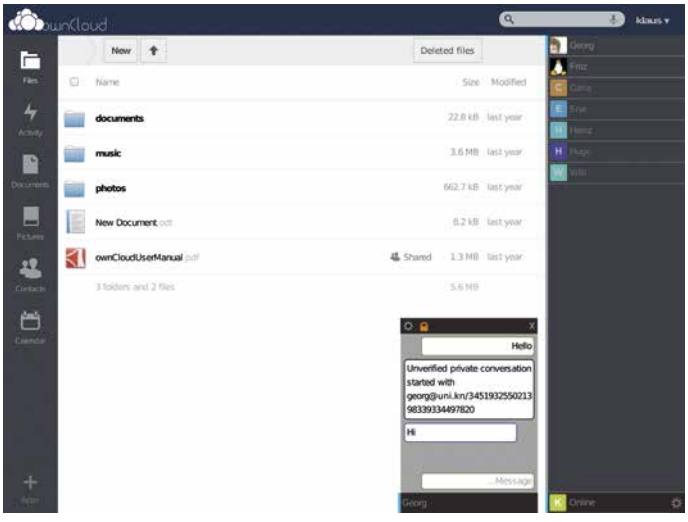


Abb. 2: Beim gemeinsamen Arbeiten an Dokumenten sind Diskussionen besonders hilfreich.

[5] http://jsxc.org

Zusammenarbeit

Ebenfalls sehr praktisch sind Chatfunktionen bei der Gestaltung, Anpassung und Verwaltung von Dokumenten. Gerade beim gemeinsamen Arbeiten an Texten sind Rückfragen und rasche Reaktionen unerlässlich.

Beratung

Viele Webseiten enthalten Kontaktinformationen. Diese können ebenfalls automatisch für XMPP-Chat verwendet werden. Neben Supportseiten (s. Abb. 3) können auch Studienberatung oder die psychologische Beratungsstelle auf diese Weise erweitert werden.

Im Gegensatz zu existierenden Chat-Support-Lösungen, die lediglich synchrone Kommunikation erlauben, ermöglicht XMPP, Nachrichten bei Abwesenheit auch asynchron zu behandeln, was die Vorteile von Chat-Support und Mail-Support vereint. Gleichzeitig wird so mit XMPP auch die bestehende Infrastruktur genutzt und ermöglicht damit den Nutzern den Einstieg in eine plattformübergreifende, föderierte Instant-Messaging-Infrastruktur.

Gerade in diesen Fällen sind auch die Möglichkeiten von WebRTC hilfreich, wie sie z.B. in den Browsern Firefox und Chrome implementiert sind: Zusätzlich zum Textchat können auch Audio und Video zugeschaltet werden oder der Desktop eines Anfragers für die Beraterin übermittelt werden.

So bietet XMPP bei Textnachrichten auch die Möglichkeit, „hinter vorgehaltener Hand“ zu sprechen (englisch „Off-The-Record Messaging“ (OTR)). Dies erlaubt es den beiden Parteien, verschlüsselt zu kommunizieren; dabei werden aber nicht nur wie sonst üblich unerwünschte Dritte ausgeschlossen, es ist zusätzlich nicht einmal einem der beiden Diskussionspartner möglich, aufgrund der Protokolldaten einem Dritten zu beweisen, wer der am Chat Beteiligten welchen Satz gesagt hat. Damit sind auch vertrauliche Diskussionen möglich.

Abb. 3: Auch Webseiten können durch einfache Änderungen um Chatfunktionen erweitert werden, hier am Beispiel des CMS Typo3.

Ebenso können XMPP-Server anonyme Konten erlauben, was für Anfragen aus der Öffentlichkeit oder von Studieninteressierten besonders nützlich ist. Die Verwendung dieser anonymen Konten wird vom Administrator dann sinnvollerweise auf diese besonderen Dienste beschränkt.

Schlussfolgerungen

Durch die Webintegration können Hürden abgebaut und der Servicegedanke der Hochschulen weiter ausgebaut werden. Durch die offene Architektur können Poweruser auch ihre nativen Clients auf Desktop oder Smartphone verwenden und ohne Medienbruch mit den Webnutzern interagieren. Dank der offenen Architektur von XMPP sind auch Konferenzen (Text, Audio, Video, Screensharing) möglich, auch wenn sie bisher in der Webumgebung noch nicht implementiert sind.

XMPP wird durch seine Eigenschaften, Tools und Verbreitung im Trend zu integrierter Kommunikation eine wichtige Rolle spielen. Mit XMPP und WISEchat kann jede Hochschule selbst mit wenig Aufwand einen interoperablen Grundstein legen, der flexibel und effizient ganz nach dem individuellen Bedarf ausgebaut werden kann. ◆

SSL-Authentisierung mit Nutzerzertifikaten

Eine sichere Alternative zu Benutzername/Passwort

Text: **Jürgen Brauckmann, Reimer Karlsen-Masur** (DFN-CERT GmbH)

Foto: © LordRunar - iStock.

Überblick

Die Verwendung von Nutzername/Passwort zur Anmeldung an Diensten hat bekanntermaßen diverse Nachteile. Wenn Nutzer ihr Passwort selbst wählen, setzen sie ein zu schwaches. Wird das Passwort dem Nutzer zugeteilt, schreibt er es auf, so dass es von Dritten gefunden werden kann. Die Wiederverwendung von Passwörtern an mehreren Diensten ist ein Sicherheitsrisiko, und eine diensteübergreifende Identität ist nicht ohne Zusatzaufwand zu erreichen. Zudem sind Passwort-Rate-Angriffe ein Risiko.

In der DFN-PKI werden seit vielen Jahren sowohl für Server wie auch für Nutzer X.509 Zertifikate ausgestellt. Wir möchten hier zeigen, wie sich Server- und Nutzerzertifikate für eine gegenseitige Authentisierung kombinieren lassen, um ein sicheres Login ohne Nutzername/Passwort realisieren zu können.

Authentisierung mit Nutzerzertifikaten vermeidet die Nachteile von Passwörtern: Der Nutzer muss sich nicht für jeden Dienst ein eigenes Passwort merken, sondern hat ein einziges Zertifikat, das vielfältig einsetzbar ist. Zertifikate haben ein gleichmäßiges Sicherheitsniveau, das nicht durch Nutzer mit zu schwachen Passworten am Server zerstört werden kann. Passwort-Rate-Angriffe gegen den Server sind prinzipbedingt nicht möglich. Daher ist eine Authentisierung mit Nutzerzertifikaten deutlich vertrauenswürdiger als Passwörter, was sich auch in der juristischen Bewertung widerspiegeln kann, wenn es z.B. um eine Anmeldung für wichtige Vorgänge wie Prüfungsanmeldungen geht. Voraussetzung für eine Authentisierung mit Nutzerzertifikaten ist zunächst einmal der Einsatz eines Serverzertifikats.

Serverzertifikate

Zertifikate für Server dienen zur Absicherung von Netzwerkverbindungen über das SSL-Protokoll (bzw. dem heute verwendeten Nachfolger TLS, wobei der Sprachgebrauch bei der Bezeichnung SSL blieb). SSL wird sehr häufig zusammen mit HTTP verwendet. Diese Kombination wird dann HTTPS genannt.

Üblicher Einsatzzweck von HTTPS sind alle „wichtigeren“ Dienste im Web, bei denen es nicht nur um einen öffentliche Informationsabruf, sondern um vertrauliche Kommunikation geht, wie z.B. Online-Banking, Web-Shops oder Webmail. Für andere Dienste wie E-Mail, Verzeichnisdienste oder Autorisierungsdienste (RADIUS) gibt es ebenfalls Varianten, die SSL nutzen.

SSL mit Serverzertifikaten bietet zwei Funktionen:

- Der Server authentisiert sich gegenüber dem Client. Vertraut der Client der Zertifizierungsstelle, die das Serverzertifikat ausgestellt hat, so kann er sich sicher sein, mit dem richtigen Server verbunden zu sein und nicht durch eine Man-in-the-Middle-Attacke angegriffen und abgehört zu werden. Damit der Client der Zertifizierungsstelle vertraut, muss in der Regel das zugehörige Wurzelzertifikat in der Software vom Hersteller vorinstalliert sein. In der DFN-PKI wird dieses durch das Wurzelzertifikat „Deutsche Telekom Root CA 2“ erreicht.
- Nach erfolgter Authentisierung wird die Verbindung verschlüsselt und ist anschließend (im Rahmen der Stärke der verwendeten Algorithmen) abhör- und manipulationssicher.

Nutzerzertifikate

So wie sich ein Dienst mit seinem Serverzertifikat gegenüber dem Webbrowser (und damit dem Nutzer) authentisiert, kann sich auch der Nutzer mit seinem eigenen, individuellen Nutzerzertifikat gegenüber dem Dienst authentisieren. Damit Nutzerzertifikate zur Authentisierung durch den Webserver verwendet werden können, muss der Server, genau wie der Client, der Zertifizierungsstelle vertrauen, die das Nutzerzertifikat ausgestellt hat. Die Nutzerzertifikate enthalten Angaben über den Inhaber, wie z.B. seinen Namen, die zugehörige Organisation und eventuell seine E-Mail-Adresse. Wie bei den Serverzertifikaten sind die Daten deshalb vertrauenswürdig, weil sie bei der Ausstellung des Zertifikats mit den in der Policy der Zertifizierungsstelle festgelegten Regeln verifiziert wurden.

Daher darf der Betreiber eines Webservers nicht einfach allen in seinem Betriebssystem vorinstallierten Zertifizierungsstellen vertrauen, sondern muss genau definieren, von welchen Zertifizierungsstellen die Zertifikate seiner Nutzer kommen dürfen.

Beschränkte Nutzerzertifikate nur für die Authentisierung

Nutzerzertifikate können grundsätzlich neben der Client-Authentisierung auch zur Signatur und Verschlüsselung von E-Mails oder anderen Daten eingesetzt werden. Das ist im Prinzip sehr praktisch, erfordert aber ein wenig Vorsicht: Verliert der Nutzer seinen privaten Schlüssel oder die Passphrase, sind die verschlüsselten Daten verloren. Daher empfiehlt sich grundsätzlich ein Backup von Zertifikaten und ihren privaten Schlüsseln. Idealerweise wird dieses Backup nur von den Nutzern selbst durchgeführt, um die Vertrauenswürdigkeit der Zertifikate nicht zu gefährden. Allerdings wird man Nutzer oft überfordern, wenn man von ihnen ein sicheres Backup verlangt.

Werden die Zertifikate dienstlich eingesetzt und werden potentiell wichtige Daten damit verschlüsselt, so hat die Einrichtung der Nutzer offensichtlich ein Interesse, das Backup selbst in die Hand zu nehmen. Sichere zentrale Backup-Prozesse sind aber aufwändig.

Deshalb kann es sinnvoll sein, Nutzerzertifikate prinzipiell ohne E-Mail-Verschlüsselungsoption auszustellen. In diesem Fall kann es nämlich keine verschlüsselte Daten oder E-Mails geben, für die man im Zweifel ein Backup des Zertifikats bräuchte.

Foto © maheyfotolia.com

Speicherung von Zertifikaten

Zu Server- und Nutzerzertifikaten gehört immer ein Schlüsselpaar, bestehend aus öffentlichem und privatem (geheim) Schlüssel. Der Zugriff auf diesen privaten Schlüssel ermöglicht die Funktionen, die nur der Inhaber des Zertifikats durchführen können soll: Authentisierung gegenüber einer anderen Partei und Entschlüsselung von Daten.

Daher muss der private Schlüssel vor einem Zugriff durch andere geschützt werden.

Im Dateisystem
Wird der private Schlüssel im Dateisystem abgespeichert, so muss er immer durch eine Passphrase geschützt sein. Beispiele für die Speicherung im Dateisystem sind private Schlüssel in der Zertifikatverwaltung von Mozilla-Produkten („Mozilla Network Security Services Keystore"), in der Registry unter Windows, als sogenannte PEM- oder PKCS#12-Dateien oder im Keystore von Java. Bei Serverzertifikaten kann der Schutz des Schlüssels durch eine Passphrase mit einem Verfügbarkeitsziel kollidieren: Ein unbeaufsichtigter, automatischer Neustart des Servers ist beim Einsatz von Passphrases für den Schlüssel nicht mehr möglich. Trotz Passphrase ist auch immer ein Schutz des privaten Schlüssels durch Dateisystemrechte erforderlich, damit andere Nutzer auf demselben System diesen nicht kopieren können.

Auf Hardware
Außer im Dateisystem können private Schlüssel auch auf speziellen Hardware-Komponenten wie Smartcards und USB-Krypto-Token gespeichert werden.

Der private Schlüssel kann in Hardware-Komponenten besser geschützt werden als in einem Dateisystem. Das Kopieren des privaten Schlüssels kann verhindert werden, und der Schutz durch eine Passphrase kann durch Fehleingabezähler deutlich verbessert werden.

Hardware-Komponenten müssen in die verwendete Software extra integriert werden. Dies geschieht mit Treibersoftware. Hier gibt es zwei grundlegende Varianten:

- Microsoft Crypto API ist ein API-Standard und Treibersystem für Microsoft-Produkte.
- PKCS#11 ist ein API-Standard, der auf allen Nicht-Microsoft-Systemen verbreitet ist.

Vor- und Nachteile der Authentisierung mit Nutzerzertifikaten

Die Nutzung von Nutzerzertifikaten zur Authentisierung bringt eine Reihe von Vorteilen gegenüber anderen Authentisierungsverfahren:

- Die Authentisierung des Nutzers ist eine Zwei-Faktor-Authentisierung:
  1. *Der Besitz des privaten Schlüssels (entweder als Datei oder als Hardware-Krypto-Token).*
  2. *Die Kenntnis des Passworts zur Aktivierung des privaten Schlüssels im Token.*
- Es wird keine Nutzername/Passwort-Kombination über eine vielleicht sogar unverschlüsselte Netzwerkverbindung transportiert.
- Ein Nutzerzertifikat realisiert automatisch eine einheitliche Identität über mehrere Dienste hinweg. Dienstespezifische Kennungen können dadurch abgelöst werden.
- Auch bei einem Wechsel des Zertifikats bleibt die Identität (der Name im Zertifikat) gleich, und die Authentisierung funktioniert unverändert auch mit dem neuen Zertifikat.
- Ein Nutzerzertifikat kann zur Anmeldung an mehreren Diensten benutzt werden, ohne auf die Problematik von wiederverwendeten Passwörtern achten zu müssen.

Beispiele für Systeme, bei denen eine Anmeldung mit Nutzerzertifikaten als einheitlicher Identität „out of the box" mög-

lich und erprobt ist: Wiki, Content-Management-System, Trouble-Ticket-System, Anmeldung am WLAN (eduroam), Kalenderanwendung, Versionskontrollsysteme, Anmeldung am IMAP- und SMTP-Server usw.

Das Interessante dabei: Diese Anwendungen müssen nicht erst mühsam in eine Single-Sign-On-Lösung eingezwängt oder mit Identity Providern zusammengeschlossen werden, sondern die einheitliche Identität kommt ausschließlich durch das Zertifikat zustande.

Trotzdem haben gerade im Dateisystem gespeicherte Nutzerzertifikate auch Nachteile: Für den normalen Anwender ist die Speicherung intransparent. Deshalb wird beispielsweise öfters vergessen, bei einer Neuinstallation eines Systems das Zertifikat zu kopieren. Ein weiterer Nachteil ist die Tatsache, dass moderne Malware inzwischen auch versucht, Nutzerzertifikate anzugreifen und nicht 100%ig ausgeschlossen werden kann, dass ein im Dateisystem gespeichertes Nutzerzertifikat gestohlen wird. Diese Nachteile können durch den Einsatz von Hardware-Krypto-Token zur Speicherung der Nutzerzertifikate ausgeglichen werden:

- Nutzer haben ihren Schlüssel „direkt in der Hand“. Die Analogie mit physikalischen Türschlüsseln kann helfen, die Aufmerksamkeit der Nutzer zur richtigen Verwendung der Zertifikate zu steigern.
- Es ist kein unbemerktes Entwenden oder Kopieren des privaten Schlüssels durch Angreifer möglich.
- Nutzer werden besser vor einer selbst verschuldeten Fehlbedienung geschützt und können ihren privaten Schlüssel und das Zertifikat nicht aus Versehen löschen, überschreiben oder unbemerkt verlieren.

Allerdings gibt es auch für Hardware-Krypto-Token Nachteile. Zunächst sind dabei die Kosten für die Beschaffung zu nennen. Des Weiteren kann die Integration problematisch sein: Nicht jede Client-Anwendung unterstützt die Verwendung von Hardware-Krypto-Token.

Ein weiteres Problem liegt in der Verfügbarkeit der Treiber: Es gibt nicht für jedes Hardware-Krypto-Token Unterstützung für jedes Betriebssystem – insbesondere ist die Nutzung auf mobilen Endgeräten mit iOS, BlackBerry OS oder Android praktisch nicht möglich (abgesehen von teuren Spezial-Lösungen wie dem „Merkel-Phone“).

Deshalb hat die Einführung von Hardware-Krypto-Token immer Projekt-Charakter.

Konfiguration der Client-Authentisierung

Die Konfiguration für die Client-Authentisierung ist nicht viel komplexer als die Konfiguration von SSL selbst. Allerdings muss sorgfältig gearbeitet werden, da Kleinigkeiten dafür sorgen können, dass entweder zu viele (unerwünschte) Nutzer Zugang erhalten oder aber der Webserver gar nicht mehr zugänglich ist. Das folgende Beispiel ist für einen Apache httpd.

Erster Schritt: Vertraute Wurzelzertifizierungsstellen

Um das vom Webbrowser geschickte Nutzerzertifikat zu validieren, benötigt der Webserver die Zertifikate der Wurzelzertifizierungsstelle der Nutzerzertifikate in einem eigenen Verzeichnis, das mit der Einstellung SSLCACertificatePath konfiguriert wird.

```
# Verzeichnis mit den vertrauten Wurzel-CA-Zertifikaten
#
SSLCACertificatePath /etc/apache2/ssl/trust-store-for-client-auth/ca-certs
```

Die Wurzelzertifikate müssen in dem konfigurierten Verzeichnis im PEM-Format vorliegen und einen speziellen Dateinamen haben, damit der Apache sie korrekt nutzt. Unter Linux muss zum Erzeugen der speziellen Dateinamen das Werkzeug c_rehash genutzt werden.

Im Falle der DFN-PKI Global Hierarchie ist nur das Zertifikat „Deutsche Telekom Root CA 2” nötig.

Zweiter Schritt: OCSP oder Sperrlisten konfigurieren

Nutzerzertifikate können aus den verschiedensten Gründen gesperrt werden. Damit der Apache gesperrten Zertifikaten den Zugriff verweigert, muss die Abfrage von Sperrinformationen, z.B. über OCSP, konfiguriert werden.

```
# OCSP konfigurieren
#
SSLOCSPEnable on

# Anzusprechender OCSP-Responder, wenn das Zertifikat
# keine eigene OCSP-Responder-URL enthält
#
SSLOCSPDefaultResponder http://ocsp.pca.dfn.de/OCSP-Server/OCSP

# OCSP-Responder aus dem Zertifikat verwenden, wenn
# vorhanden
#
SSLOCSPOverrideResponder off
```

OCSP ist ab Apache 2.3 nutzbar. Alternativ können auch Sperrlisten (CRLs) verwendet werden.

Dritter Schritt: Client-Authentisierung anschalten
Nach der Konfiguration der Wurzelzertifikate und der Sperrinformationen kann nun die Authentisierung innerhalb eines Virtual-Hosts oder auch eines Directory-Kontextes angeschaltet werden:

```
<VirtualHost www.example.org:443>
 # SSL anschalten
 #
 SSLEngine on

 # Verifizierungstiefe. Muss für die DFN-PKI auf 3 oder größer
# gesetzt werden
#
 SSLVerifyDepth 3

 # Client-Authentisierung anschalten. Kein Zugriff ohne
 # Client-Zertifikat
 #
 SSLVerifyClient require
 SSLOptions +StrictRequire
...
</VirtualHost>
```

Mit diesen Parametern wird der Zugriff auf all die Nutzer beschränkt, die sich mit einem Zertifikat aus der PKI unterhalb der konfigurierten Wurzelzertifikate ausgewiesen haben. Im Fall der DFN-PKI können das dann Nutzer aus allen Sub-CAs unterhalb der Deutsche Telekom Root CA 2 sein, also von deutlich mehr als 300 Einrichtungen. Es müssen daher weitere Einschränkungen konfiguriert werden, um nur die Nutzer von gewünschten Einrichtungen und nur bestimmte Nutzergruppen zu erlauben.

Vierter Schritt: Beschränkung des Zugriffs
Generell gibt es verschiedene Möglichkeiten, wie eine Zugriffsbeschränkung durchgeführt werden kann. Hierbei muss besonders darauf geachtet werden, dass nicht aus Versehen Nutzer aus den falschen Sub-CAs Zugriff erlangen. Wird beispielsweise nur nach einem Namen „Max Mustermann“ geprüft, so könnte dieser Name ja in mehreren Sub-CAs innerhalb der PKI vergeben werden. Daher müssen immer auch noch weitere Informationen über das Sub-CA-Zertifikat kontrolliert werden.

Beschränkung mit SSLRequire
Innerhalb eines Directory- oder .htaccess-Kontext kann mit der Direktive SSLRequire direkt spezifiziert werden, welche Zertifikate Zugriff haben. Mit folgendem Beispiel wird der Zugriff auf den Nutzer mit CN „Max Mustermann“ in der CA „Global Services CA“ beschränkt.

```
<directory /srv/www/authtest>
SSLRequire ( %{SSL_CLIENT_I_DN} eq „CN=DFN-Verein CA
Services,O=DFN-PKI,O=DFN-Verein,C=DE“ \
and %{SSL_CLIENT_CERT_CHAIN_1} =~ m|/9jJI/
MGLnPRv5COrZxbcwL7WSqp\n-----END | \
and %{SSL_CLIENT_S_DN_CN} eq „Max Mustermann“)

</directory>
```

Die Auswertungssprache ist sehr umfangreich. Für Details muss die Dokumentation von Apache herangezogen werden (für Version 2.4: http://httpd.apache.org/docs/2.4/mod/mod_ssl.html).

Beschränkung mit FakeBasicAuth
Alternativ kann der FakeBasicAuth-Mechanismus verwendet werden. Hierbei wird der Apache ähnlich konfiguriert wie für Nutzername/Passwort-Authentisierung. Anstelle von Nutzernamen wird der DN des Zertifikats in einer leicht zu wartenden Textdatei konfiguriert.

Beschränkung durch die Anwendung
Wenn im Apache eine komplexere Anwendung mit eigener, X.509-Zertifkate unterstützenden Nutzerverwaltung läuft, so sollte natürlich dieser Mechanismus verwendet werden. Aber auch hierbei muss auf die Beschränkung auf die richtigen Zertifizierungsstellen geachtet werden.

Fazit

Eine Authentisierung mit Nutzerzertifikaten kann eine interessante Alternative zu Nutzername/Passwort-Mechanismen sein, und gewährleistet ein gleichmäßigeres Sicherheitsniveau. Allerdings erfordert die Ausgabe der Zertifikate einen gewissen Aufwand, und die Akzeptanz bei nicht technischen Nutzern ist nicht automatisch gegeben. Hardware-Krypto-Token können das Verständnis der Nutzer für ihr Zertifikat deutlich erhöhen, auch wenn man sich dabei vorab intensiv mit Treiber- und Kompatibilitätsfragen befassen muss.

Die Einrichtung im Webserver ist einfach und unproblematisch. Die Sicherheit der Systeme wird erhöht, da die Angreifbarkeit über schwache oder aufgeschriebene Passworte abgewehrt wird und Passwort-Rate-Angriffe gegen den Server prinzipiell nicht möglich sind.

Insbesondere die einheitliche Identität über mehrere Systeme hinweg, die man bei der Verwendung von Zertifikaten automatisch ohne weiteren Aufwand erhält, ist sowohl für Administratoren als auch für Nutzer eine große Erleichterung. ◆

Sicherheit aktuell

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

SHA-2 in der DFN-PKI

In der letzten Ausgabe der DFN-Mitteilungen wurde an dieser Stelle über die bevorstehende Umstellung der DFN-PKI auf den SHA-2 Algorithmus berichtet, ohne dass ein konkretes Datum für die Umstellung angegeben werden konnte. Im November 2013 hat Microsoft angekündigt, dass ab 2017 in Windows keine mit SHA-1 ausgestellten Zertifikate mehr akzeptiert werden. Da dies neben den Zertifikaten für Server und Nutzer auch für Sub-CA-Zertifikate gelten wird, muss die DFN-PKI insgesamt inklusive aller Sub-CAs-Zertifikate umgestellt werden. Details zur Umstellung sind auf den Webseiten der DFN-PKI unter https://www.pki.dfn.de/faqpki/faqpki-sha2/ zusammengefasst. ◆

Veröffentlichung von gestohlenen Passwort-Daten

Im Oktober 2013 wurde durch die Firma Adobe veröffentlicht, dass von Systemen unter ihrer Kontrolle ca. 153 Millionen E-Mail-Adressen mit zugehörigen Passwörtern gestohlen wurden. In der Folge wurden die betroffenem E-Mail-Adressen von Adobe direkt angeschrieben und empfohlen, die gestohlenen Passwörter nicht mehr zu verwenden, d.h. neue Passwörter zu setzen. Im November 2013 wurden der komplette Datensatz im Internet veröffentlicht. Verschiedene Einrichtungen im DFN haben die Daten genutzt, um betroffene Benutzer im eigenen Hause zusätzlich zu informieren und dedizierte Anweisungen zu erteilen. Da durch die offensive Informationspolitik von Adobe und der direkten Information betroffener E-Mail-Adressen das allgemeine Ziel der breit gestreuten Information erreicht war, wurden seitens DFN-CERT keine weiteren Maßnahmen unternommen. Kurz darauf startete das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Januar 2014 eine bisher nicht vorgekommene Aktion: Nachdem das BSI im Zusammenhang mit Ermittlungen gegen Computer-Kriminelle Erkenntnisse über 16 Millionen „gestohlene“ Datensätze erhielt und zunächst nur einzelne öffentliche Verwaltungsstellen über die betroffenen Benutzer in diesen Häusern informiert hatte, wurde allen Benutzern über eine eigens dafür entwickelte Web-Anwendung eine Prüfmöglichkeit verschafft. Durch die Eingabe einer zu prüfenden E-Mail-Adresse konnte eine E-Mail an diese Adresse angefordert werden, falls sie in dem Datensatz enthalten ist. Das BSI konnte den CERTs aus rechtlichen Gründen die komplette Liste oder Auszüge davon nicht übergeben. Daher hatte auch das DFN-CERT keine Möglichkeit, die Anwender direkt über betroffene E-Mail-Adressen zu informieren. Das DFN-CERT hat die Anwender aber über die Aktion des BSI informiert und diese konnten so intern entsprechende Maßnahmen einleiten.

Anfang April 2014 wurde erneut bekannt, dass deutsche Strafverfolgungsbehörden über einen weiteren Datensatz mit 18 Millionen E-Mail-Adressen und zugehörigen Passwörtern verfügen. Das BSI hat angekündigt, CERTs in Deutschland diesmal den Zugriff auf die Daten zu ermöglichen. Das DFN-CERT hat die entsprechenden Daten für die Anwender im DFN angefordert und wird sie entsprechend weiterverteilen. Bei Redaktionsschluss der DFN-Mitteilungen lag der Datensatz mit den betroffenen DFN-Anwendern allerdings noch nicht vor. ◆

Re-Audit der DFN-PKI

Im Dezember 2013 wurde wie geplant das Audit der DFN-PKI nach ETSI TS 102 042 durch den TÜViT erneuert. Jährliche Re-Audits stellen sicher, dass das Sicherheitsniveau der DFN-PKI weiterhin den zugrundeliegenden Standards entspricht. Aufgrund geänderter Anforderungen durch die Softwarehersteller wie Mozilla und Microsoft musste das Profil, nach dem die DFN-PKI auditiert wird, angepasst werden: Statt „LCP“ (Leightweight Certification Policy) wird die DFN-PKI nun nach „OVCP“ (Organizational Validation Certificates Policy) auditiert. Dieses Profil beinhaltet die Baseline Requirements des CA/Browser Forums. So wird sichergestellt, dass auch diese Anforderungen erfüllt werden, wie es die Softwarehersteller in ihren jeweiligen Programmen für Root-CAs fordern. Die Verankerung der DFN-PKI in allen gängigen Browsern und Betriebssystemen ist somit weiterhin sichergestellt. ◆

Kontakt

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

Stream' dich ins (Un-)Glück

Eine der noch ungeklärten Rechtsstreitigkeiten entfachte vor kurzem erneut im deutschen Online-Film-Bereich. Nach Abmahnungen tausender angeblicher Nutzer von Porno-Inhalten im Netz durch einen Regensburger Anwalt ist sich die Rechtswelt so uneinig wie nie zuvor, wenn es um das Streaming geht. Rechtliche Regelungen dazu fehlen gänzlich. Die Frage, ob das Streamen urheberrechtlich geschützter Inhalte gegen das Urheberrecht verstößt, ist bislang ungeklärt. Eine Klärung seitens der Gerichte ist nicht in Sicht – dafür die Weiterführung einer kontroversen Debatte über die Legalität dieser Handlungen.

Text: **Susanne Thinius** (DFN-Verein)

Foto © Mars Bars /iStock.

Der Hintergrund

In Deutschland wurden kürzlich tausende Internetnutzer von Abmahnungen ereilt, weil sie sich – angeblich – auf den Seiten des Pornofilm-Anbieters Redtube.com getummelt hatten – und dort urheberrechtlich geschützte Sexfilme abgerufen haben sollen. Mitunter wurden die Abgemahnten aufgefordert 250 € zu zahlen. Eine in der Schweiz ansässige Firma mit dem Namen „The Archive AG“ erteilte einem Regensburger Anwalt (Urmann&Collegen) das Mandat, die Abmahnungen zu versenden. Dieser argumentierte gegenüber dem LG Köln, beim Streamen schaffe die technisch notwendige Zwischenspeicherung eine Raubkopie, die der eigentliche Rechteinhaber nicht genehmigt habe. Dadurch erlangte der Anwalt Auskunftsbeschlüsse des Landgerichts (LG) Köln, mit welchen er an die bestimmten IP-Adressen zuzuordnenden Namen und Anschriften der angeblichen Video-Stream-Nutzer kam (durch Herausgabe seitens der Telekom), um sie abzumahnen. Ob der Archive AG überhaupt die Online-Verwertungsrechte zustehen und wie sie an die IP-Adressen der Abgemahnten kam, ist laut Medienberichten unklar. Die bereits gezahlten 250 € Schadensersatz sehen die Abgemahnten wohl nicht wieder, da die Hintermänner des Schweizer Abmahnunternehmens untergetaucht sind.

Streaming oder Download und: wann ich eigentlich vervielfältige

Aufgrund dieses Sachverhalts stellt sich in der Rechtswelt die immer noch ungeklärte und umstrittene Frage, ob die Zwischenspeicherung von Inhalten beim Streaming ohne Einwilligung des Berechtigten eine urheberrechtlich relevante Vervielfältigungshandlung und mithin eine möglicherweise strafbare Urheberrechtsverletzung darstellt (gemäß §§ 106, 108 Urheberrechtsgesetz, (UrhG)). Höchstrichterliche Rechtsprechung sowie rechtliche Rahmenbedingungen gibt es dazu (noch) nicht, seit dem jüngsten Beschluss des LG Köln (Beschluss vom 24.1.2014, Az. 209 O 188/13) nun jedoch eine Tendenz. Zunächst ein Überblick darüber, wie Streaming und Download technisch und rechtlich einzuordnen sind:

Beim Streaming, also dem Abspielen von Medieninhalten direkt aus dem Netz, werden im Gegensatz zum Download die in Paketen ankommenden Dateien nur in einem temporären Datenpuffer und nicht dauerhaft gespeichert. Deren Inhalte können im Vergleich zum Download schon während des Ladevorgangs wiedergegeben werden. Diese (wenn auch nur vorübergehende) Zwischenspeicherung ist die körperliche Festlegung des Inhalts der gestreamten Daten, eine komplette oder teilweise Vervielfältigung des Werkes (im vorliegenden Streitfall ein Filmwerk nach § 2 Abs. 2 Nr. 6 UrhG) resultiert daraus. Die Zwischenspeicherung kann abhängig von ihrer Art bis zu 5 Sekunden dauern (so beispielsweise beim Client-Puffer im Web-Server-basierten Betrieb). Die zwischengespeicherten Teilstücke der übertragenen Daten werden dann, nachdem sie in den sogenannten Cache-Speicher verschoben worden sind, normalerweise durch Beenden des Media-Players (Software zur Darstellung der Inhalte), Schließen des Browsers, Überschreiben der Datei oder Herunterfahren des Computers automatisch gelöscht. Für die Einordnung als urheberrechtlich relevante Vervielfältigungshandlung spielen die Dauer und die anschließende Löschung der Daten allerdings keine Rolle. Nach überwiegender Meinung ist dies also dennoch als Vervielfältigung zu qualifizieren. Andere Stimmen in der Literatur wenden hiergegen ein, dass wegen der zerstückelten Pufferung auf dem Nutzerrechner nur wenige Elemente kopiert werden. Diese seien nicht als Werk im Sinne des § 2 Abs. 2 UrhG zu qualifizieren und daher nicht urheberrechtlich schutzfähig. Eine Verletzung von Urheber- oder sonstigen Leistungsschutzrechten komme daher schon nicht in Betracht.

Im Prinzip muss im Einzelfall entschieden werden, ob es sich bei der Zwischenspeicherung um eine konkrete Vervielfältigung handelt oder nicht, da dies aufgrund der Mannigfaltigkeit der Zwischenspeicherungsmöglichkeiten beim Streaming nicht pauschal beantwortet werden kann. Einer solchen Einzelfallentscheidung steht allerdings entgegen, dass rückblickend meist nicht festgestellt werden kann, ob und inwieweit die verschiedenen (zwischengespeicherten) Teile schutzfähig waren. Technisch kommt man hier also an seine Grenzen.

Die Ausgangsfrage nach der urheberrechtlichen Bewertung des Streamings bzw. der vorübergehenden Zwischenspeicherung lässt sich demnach nicht eindeutig klären.

Stimmen aus der Rechtswelt und der Bundesregierung zur Streitfrage

Da es derzeit keine rechtlichen Rahmenbedingungen für das Streamen von Inhalten aus dem Netz gibt, ist es Aufgabe der nationalen Gerichte und des EuGH, die juristischen Fragestellungen um das Streaming zu beantworten. Gerade unter Anwälten wird momentan heftig über die rechtliche Einordnung des Streaming debattiert. Entgegen der Auffassung des Regensburger Anwalts setzt sich in der Literatur mehr und mehr die Auffassung durch, dass beim Streaming – anders als der Download im Rahmen des Filesharing – keine dauerhafte Kopie beim Nutzer angelegt wird, lediglich ein kurzer Datenpuffer. Streamen sei nur ein Anschauen; selbst bei illegal ins Netz gestellten Inhalten und daher - anders als das Vervielfältigen - nicht verboten. Die Bundesregierung sieht dies ganz ähnlich. Das Streamen von Videos stelle keine Urheberrechtsverletzung dar. Dies folgt aus

einer jüngst in Auftrag gegebenen Kleinen Anfrage der Linksfraktion an die Regierung (BT-Drs. 18/195). Danach seien Videostreams im Browser nicht als Raubkopie zu bewerten. Eine Stellungnahme, ob es sich bei der Zwischenspeicherung um ein Vervielfältigen handelt oder nicht, unterblieb indes in diesem Zusammenhang. Hier verweist die Bundesregierung lieber auf den EuGH, als selbst Rechtsunsicherheiten zu beseitigen.

LG Köln revidiert Rechtsauffassung

Das LG Köln hat nun ebenfalls auf vier Beschwerden der Abgemahnten gegen die eingangs erwähnten Auskunftsbeschlüsse reagiert und befunden, dass die Auskunftsbeschlüsse die Anschlussinhaber/Abgemahnten in ihren Rechten verletzten. Damit revidiert es seine eigene ursprüngliche Rechtsauffassung. Begründet wird die Auffassung – kurz und knapp – damit, dass man seitens des Gerichts zunächst von einem Download und nicht einem Streamen der Videos ausgegangen war. Als ob das Gericht den Wortlaut der Bundesregierung-Stellungnahme eins zu eins übernommen hätte, betonen auch die Kölner Richter, dass das bloße Streaming grundsätzlich noch keinen relevanten rechtswidrigen Verstoß gegen das Urheberrecht (insbesondere keine Vervielfältigung im Sinne des § 16 UrhG) darstelle. Ebenso kurz und knapp beziehen sie dann § 44a UrhG in ihre Überlegungen ein: Das Streamen von Video-Dateien sei demnach bei „nur vorübergehender Speicherung aufgrund einer nicht offensichtlich rechtswidrig hergestellten beziehungsweise öffentlich zugänglich gemachten Vorlage“ von § 44 a Nr. 2 UrhG gedeckt. Doch was versteckt sich hinter dieser kryptischen Formulierung?

Lösung des Problems: Schrankenregelungen aus dem UrhG

§ 44 a UrhG ist eine sogenannte Schrankenregelung, die die erlaubnisfreie Nutzung zu Gunsten legitimer Interessen der Allgemeinheit regelt. Nach dem Wortlaut sind „vorübergehende Vervielfältigungshandlungen, die flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen, zulässig“. Ihr alleiniger Zweck muss dabei entweder die Ermöglichung der Übertragung in einem Netz zwischen Dritten durch einen Vermittler (§ 44 a Nr. 1 UrhG) oder die Ermöglichung der rechtmäßigen Nutzung eines Werkes oder sonstigen Schutzgegenstandes (§ 44 a Nr. 2 UrhG) sein und darf keine eigenständige wirtschaftliche Bedeutung haben. Unproblematisch handelt es sich bei den Vervielfältigungen im Cache-Speicher um vorübergehende, flüchtige oder begleitende Vervielfältigungen, deren Speichervorgang der technisch unversierte Durchschnittsnutzer nicht einmal bemerken wird (so zumindest Stolz, „Rezipient = Rechtsverletzer…? (Keine) Urheberrechtsverletzung durch die Nutzung illegaler Streaming-Angebote“, Multimedia und Recht 2013, 353). Zudem sei die Vervielfältigung unabdingbar für die Wiedergabe des Streams und mithin wesentlicher Bestandteil im Sinne der Vorschrift.

Einzig die Merkmale der rechtmäßigen Nutzung sowie der eigenständigen wirtschaftlichen Bedeutung können unter Umständen problematisch sein. Bei Ersterem wird jedoch von Stolz vertreten, dass der reine Werkgenuss immer eine rechtmäßige Nutzung darstelle. Zudem befürworte die § 44 a UrhG zugrundeliegenden Harmonisierungs-RL (dort Art. 5 Abs. 1) die grundsätzliche Privilegierung des Browsings und Cachings für die Gewährleistung der effizienteren Nutzung von Internetinhalten. Auch eine eigenständige wirtschaftliche Bedeutung sei abzulehnen, so Stolz in seinem Aufsatz, wenn die Zwischenspeicherung nur der rechtmäßigen Nutzung diene und keine weitere Verwertung der empfangenen Daten erlaube. Insofern dürfte § 44 a Nr. 2 UrhG den Nutzern im hiesigen Verfahren zur Seite stehen. Als potentielle Schrankenregelung kommt zudem § 53 UrhG in Betracht: einzelne Vervielfältigungen durch eine natürliche Person zum privaten Gebrauch sind ohne Erwerbszweck danach zulässig. Dies allerdings nur, wenn es sich nicht um offensichtlich rechtswidrig hergestellte oder rechtswidrig öffentlich zugänglich gemachte Vorlagen handelt, so § 53 Abs. 1 UrhG. Das Erfordernis der nicht offensichtlich rechtswidrig hergestellten oder rechtswidrig öffentlich zugänglich gemachten Vorlage kann allerdings bei der Bereitstellung von oft illegalen Inhalten auf Pornoseiten wie im Ausgangsfall durchaus bezweifelt werden.

Hochschulkonsequenzen und Fazit

Solange der Nutzer es nicht unternimmt, (auch) illegale Streaming-Angebote auf andere Weise als durch reinen „Werkgenuss“ zu verwenden, ist eine Urheberrechtsverletzung mit ihren möglichen Konsequenzen (Strafbarkeit des Nutzers, Schadensersatzforderungen gegen ihn) nach derzeitigem Stand abzulehnen. Höchstrichterliche Rechtsprechung zur juristischen Bewertung des Streaming, insbesondere zur rechtlichen Einordnung des Zwischenspeicherungsprozesses und der Handhabung von illegal bereitgestellten Inhalten, gibt es noch nicht, ganz zu schweigen von einer gesetzlichen Ausgestaltung. So lange muss sich die Rechtswelt mit den bestehenden Vorschriften des UrhG (§§ 44a, 53) zufrieden geben. Dass die Bundesregierung im Rahmen der Kleinen Anfrage der Linken ankündigt, sie wolle das Urheberrecht den Erfordernissen und Herausforderungen des digitalen Zeitalters anpassen und dabei die digitalen Nutzungspraktiken berücksichtigen“, zeigt die Ratlosigkeit beim Umgang mit technischen Entwicklungen. Eine Einbeziehung des Gesetzes gegen unseriöse Geschäftspraktiken (vertiefend dazu Thinius, „Gut gemeint – aber auch gut genug? – Infobrief Recht 12/2013)

erscheint in diesem Zusammenhang notwendiger denn je, insbesondere was Massenabmahnungen und überhöhte Anwaltsforderungen angeht.

Insbesondere das Video-Streaming gewinnt seit einigen Jahren immer mehr an (auch ökonomischer) Bedeutung. Wichtigstes Praxis-Beispiel ist das Video-Portal YouTube. Hier werden pro Tag bis zu drei Milliarden Videodaten abgerufen. Der Download, beispielsweise beim Filesharing, tritt zunehmend in den Hintergrund und die rechtlichen Probleme verlagern sich vom Download zum Streaming. Hier müssen entweder Gesetzesanpassungen oder Korrekturen durch die Rechtsprechung stattfinden und so für Rechtsklarheit sorgen. Denn wenn alles bleibt wie bisher, wird das Streamen (auch illegaler Inhalte) weiterhin strafrechtlich nicht verfolgt werden.

Auch an Hochschulen dürfte die aktuelle Streaming-Debatte nicht unbemerkt vorbeigehen. Denn bedenkt man, dass der Streaming-Hype auch Studenten und Mitarbeiter erfasst hat, so muss man sich nach den möglichen Konsequenzen fragen. Wer ist verantwortlich, wenn illegale Inhalte durch Hochschulangehörige gestreamt werden, vielleicht sogar am Arbeitsplatz? Der Streamende selbst oder gar die Hochschule bzw. stellvertretend der Kanzler oder Präsident? Im Hinblick auf die Störerhaftung (vertiefend dazu u.a. Kuta, „Der Host-Provider als Gehilfe – Ein Einzelfall oder die Regel?“ Infobrief Recht 5/2012) kann sogar die Hochschule unter bestimmten Voraussetzungen für urheberrechtsverletzende Handlungen ihrer Angehörigen haftbar gemacht werden.

Die aktuelle Debatte verursacht daher eine Rechtsunsicherheit auch an deutschen Hochschulen. Es wäre wünschenswert, endlich Klarheit zu schaffen. Gesetzgeber und Gerichte sind gefragt! Bis zu einer einheitlichen und bestenfalls höchstrichterlichen Rechtsprechung ist daher mehr denn je Vorsicht geboten vor unseriösen Abmahnungen. ◆

Gerne übernehme ich diesen Job!

Landesarbeitsgericht Düsseldorf: Betriebsbedingte Kündigung des Datenschutzbeauftragten unwirksam

Neben der Position im Betriebs- oder Personalrat bietet auch die Stellung eines Datenschutzbeauftragten die Möglichkeit, Einfluss auf Vorgänge im Unternehmen oder einer öffentlichen Einrichtung nehmen zu können. Mit der Stellung ist jedoch auch abseits des auferlegten Tätigkeitsfeldes eine gewisse Attraktivität verbunden, wenn es darum geht, dass einem Teil der Belegschaft oder ganz konkret diesem Arbeitnehmer gekündigt werden soll. Das Landesarbeitsgericht Düsseldorf bestätigt mit einem Urteil vom 23.07.2012 (Az. 9 Sa 593/12) die mit der Position des Datenschutzbeauftragten verbundene Sonderstellung.

Text: **Julian Fischer** (DFN-Verein)

Foto: © Frank van den Bergh/iStock.

I. Hintergrund

Kaum eine juristische Materie beinhaltet von vorneherein so viel Potenzial für Streitigkeiten wie das Arbeitsrecht. Dies hängt insbesondere damit zusammen, dass sich die betroffenen Parteien von Arbeitgeber und Arbeitnehmer in einem Ungleichgewicht befinden, welches das Gesetz und die Gerichte bestmöglich auszugleichen versuchen.

Kündigungsmöglichkeiten des Arbeitgebers

Hierzu zählt vor allem das Druckmittel der Kündigung, welches dem Arbeitgeber nur in bestimmten Konstellationen und möglichst schonend gegenüber dem Arbeitnehmer zur Verfügung gestellt werden soll. § 626 des Bürgerlichen Gesetzbuches (BGB) bestimmt daher, dass eine außerordentliche Kündigung nur bei Vorliegen eines wichtigen Grundes möglich ist. Die Rechtsprechung verlangt dabei, dass

1. der Kündigungssachverhalt als solcher generell geeignet sein muss, eine außerordentliche Kündigung zu begründen und zudem
2. die Kündigung unter Berücksichtigung aller Umstände des Einzelfalls im Rahmen einer Interessenabwägung, insbesondere unter Berücksichtigung des sog. Ultima-Ratio-Prinzips – und damit erst als zuletzt in Betracht zu ziehendes Mittel – gerechtfertigt sein muss.

Für das Vorliegen dieser Voraussetzungen trägt der Arbeitgeber die Darlegungs- und Beweislast.

Neben den hohen Voraussetzungen einer außerordentlichen Kündigung steht es dem Arbeitgeber offen, seinem Beschäftigten ordnungsgemäß, d. h. unter Einhaltung der gesetzlichen Kündigungsfrist, zu kündigen. Allerdings wird auch dieses Recht häufig durch gesetzliche oder vertragliche Bestimmungen eingeschränkt. So bestimmt etwa das Kündigungsschutzgesetz, dass nach dem Ablauf der Probezeit von in der Regel 6 Monaten die Kündigung nur dann wirksam ist, sofern sie nicht sozial ungerechtfertigt ist. Eine ordentliche Kündigung kann daher sozial ungerechtfertigt und damit unwirksam sein, wenn soziale Gesichtspunkte nicht oder nicht ausreichend berücksichtigt wurden, weil insbesondere personen-, betriebs- oder verhaltensbedingte Gründe nicht vorlagen. Die Kündigungsfrist ist die Zeitspanne, die zwischen dem Zugang der Kündigung beim Arbeitnehmer und der tatsächlichen Beendigung des Arbeitsverhältnisses in jedem Fall liegen muss. Die Länge der Kündigungsfrist bestimmt sich danach, wie lange der Arbeitnehmer bereits im Betrieb beschäftigt ist. Hierzu wird in § 622 Abs. 2 BGB eine Kündigungsfrist von einem Monat für den Fall einer zweijährigen Dauer des Arbeitsverhältnisses festgelegt. Anschließend steigt die Kündigungsfrist auf zwei, drei, vier, fünf, sechs oder sieben Monate bei einer jeweiligen Dauer der Beschäftigung von fünf, acht, zehn, zwölf, fünfzehn oder zwanzig Jahren. Diese gesetzlichen Kündigungsfristen dürfen auch nicht durch eine Vereinbarung im Arbeitsvertrag zulasten des Arbeitnehmers verkürzt werden.

Arbeitnehmer, die zusätzlich eine Stelle im Betriebs- bzw. Personalrat bekleiden, genießen gegenüber den allgemeinen ordentlichen Kündigungsregeln einen besonderen Kündigungsschutz. Hierdurch soll gewährleistet werden, dass die Beschäftigten, die eine derartige Position ausfüllen, ohne Furcht vor dem Verlust des Arbeitsplatzes ihre Aufgaben wahrnehmen können. Denn gerade durch die ernsthafte Wahrnehmung der mit einer solchen Position verbundenen Aufgaben wird der Mitarbeiter oftmals zwangsläufig in Meinungsverschiedenheiten mit dem Arbeitgeber geraten, sodass der Arbeitgeber ein Interesse daran haben könnte, diesen unliebsamen Mitarbeiter möglichst umgehend zu kündigen. Dieser sog. Sonderkündigungsschutz besagt, dass ordentliche Kündigungen grundsätzlich ausgeschlossen sind und lediglich außerordentliche Kündigungen unten den genannten hohen Voraussetzungen möglich sind. Eine Ausnahme von dieser Regel stellt die ordentliche betriebsbedingte Kündigung dar, sofern dieser der Fall einer Betriebsstilllegung oder der Stilllegung einer Betriebsabteilung zugrunde liegt und der Betroffene nicht von einer anderen Abteilung übernommen werden kann (§ 15 Abs. 5 S. 2, Abs. 4 Kündigungsschutzgesetz (KSchG)).

Sonderposition des Datenschutzbeauftragten

Eine ähnlich komfortable Position gewährt das Gesetz dem Datenschutzbeauftragten in § 4f Abs. 3 S. 4 Bundesdatenschutzgesetz (BDSG). Auch hier muss der Arbeitgeber ohne das Mittel der ordentlichen Kündigung auskommen, da die datenschutzrechtliche Vorschrift von ihm den Nachweis darüber verlangt, dass Tatsachen vorliegen, welche diesen zur Kündigung aus wichtigem Grund ohne die Einhaltung der Kündigungsfrist berechtigen. Das heißt, dass eine Kündigung des Datenschutzbeauftragten nur zulässig ist, wenn das Vorliegen eines zur außerordentlichen Kündigung berechtigenden Grundes im Sinne des § 626 BGB besteht. Zwar gilt die Regelung prinzipiell nur für den pflichtgemäß zu bestellenden und nicht für den freiwillig bestellten Datenschutzbeauftragten, allerdings sind öffentliche Stellen (z.B. Hochschulen), die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, unabhängig von der Zahl der beschäftigten Personen zur Bestellung eines Datenschutzbeauftragten verpflichtet (§ 4f Abs. 1 S. 1 BDSG).

Sollte der Mitarbeiter als Datenschutzbeauftragter ordnungsgemäß abberufen worden sein, so darf der Arbeitgeber den Arbeitnehmer auch dann frühestens ein Jahr später auf ordentlichem Wege kündigen (§ 4f Abs. 3 S. 6 BDSG). Die Abberufung des Datenschutzbeauftragten einer öffentlichen Stelle kommt indes wiederum nur in Betracht, wenn ein besonderer Grund im Sinne des § 626 BGB vorliegt oder Umstände gegeben sind, die unter Berücksichti-

gung des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung der Beschäftigung unzumutbar machen. Hierbei kommen sowohl diejenigen Aspekte in Betracht, die eine weitere Beschäftigung als Datenschutzbeauftragter betreffen, als auch solche, die dem allgemeinen Arbeitsverhältnis bzw. seinem nichtdatenschutzrechtlichen Teil entstammen. In Bezug auf seine Position als Datenschutzbeauftragter dürften hierzu etwa die Kriterien der erforderlichen Fachkunde auf dem Gebiet des Datenschutzes sowie das Privileg der Weisungsfreiheit eine besonders große Rolle spielen.

II. Das Urteil des Landesarbeitsgerichts Düsseldorf

1. Der Sachverhalt

Der Entscheidung des Landesarbeitsgerichts Düsseldorf vom 23.7.2012 (Az. 9 Sa 593/12) lag der Sachverhalt eines 55-jährigen verheirateten Datenschutzbeauftragten zugrunde, der seit 15 Jahren als kaufmännischer Angestellter im Bereich der elektronischen Datenverarbeitung beschäftigt wurde. In dieser Zeit war er in unterschiedlichen Bereichen des Unternehmens tätig: So wurde er neben der allgemeinen Verwaltung unter anderem auch im Qualitätsmanagement und später als Leiter des Bereichs IT eingesetzt. Im Jahre 2004 wurde er dann von seinem Arbeitgeber zum Datenschutzbeauftragten berufen. Vier Jahre später übernahm er dieselbe Funktion zusätzlich in der Tochtergesellschaft des Unternehmens.

Im Rahmen einer Restrukturierung des Unternehmens sollten im Jahr 2010 einige Verwaltungsbereiche ausgegliedert werden. Hierzu gehörte auch der Bereich des betroffenen Arbeitnehmers, der einem Übergang seines Arbeitsverhältnisses auf den Teilbereich der ausgelagerten GmbH allerdings widersprach. Unmittelbar darauf wurde der Arbeitnehmer im September 2011 als Datenschutzbeauftragter abberufen. Ebenfalls nur wenige Tage später wurde ihm dann außerordentlich betriebsbedingt gekündigt. Sowohl gegen die Abberufung als Datenschutzbeauftragter als auch gegen die Kündigung erhob der Arbeitnehmer Klage vor dem Arbeitsgericht Krefeld.

2. Das erstinstanzliche Arbeitsgerichtsurteil und das Berufungsurteil des Landesarbeitsgerichts

Das Arbeitsgericht Krefeld gab dem Arbeitnehmer hinsichtlich der Unrechtmäßigkeit seiner Entlassung Recht. Die Abberufung als Datenschutzbeauftragter hielten die Richter im erstinstanzlichen Urteil vor dem Arbeitsgericht Krefeld dagegen für berechtigt und wiesen den Wunsch des Arbeitnehmers auf Rückgängigmachung der Abberufung ab. Gegen dieses Urteil legten sowohl das Unternehmen als auch der Arbeitnehmer Berufung beim Landesarbeitsgericht Düsseldorf ein. Dieses schloss sich jedoch in beiden Punkten dem Urteil sowie den Ausführungen der Vorinstanz an.

Unrechtmäßigkeit der außerordentlichen Kündigung

Die Richter der Berufungsinstanz führten in ihrer Entscheidung an, dass der Arbeitnehmer als Datenschutzbeauftragter berufen worden sei, was dazu führt, dass sein Arbeitsverhältnis während der Zeit der Bestellung und bis zu einem Jahr nach der Abberufung nicht ordentlich gekündigt werden kann. Daher komme lediglich eine außerordentliche Kündigung aus wichtigem Grund in Betracht. Hierzu müssten Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Dienstverhältnisses nicht zugemutet werden könne. Die Richter merkten insoweit an, dass sich das Unternehmen hinsichtlich der ausgesprochenen Kündigung lediglich auf betriebsbedingte Gründe berufen hatte. Eine Kündigung, die auf rein betriebsbedingten Erwägungen beruhe, sei jedoch nicht geeignet, eine außerordentliche Kündigung zu rechtfertigen. Sogar im Insolvenzfall, wenn eine betriebliche Weiterbeschäftigung für den Arbeitnehmer entfällt, soll für den Arbeitgeber nicht die Möglichkeit bestehen, sich umgehend von seinem Arbeitnehmer zu trennen.

Eine Ausnahme komme lediglich dann in Betracht, wenn der Arbeitgeber, aufgrund des hier vorliegenden Wegfalls der ordentlichen Kündbarkeit, zur Aufrechterhaltung eines sog. sinnentleerten Arbeitsverhältnisses gezwungen würde. Diese von der Rechtsprechung entwickelte Sondersituation liege aber nur dann vor, wenn den Gehaltszahlungen über einen langen Zeitraum keine entsprechende Arbeitsleistung mehr gegenüberstehe. Voraussetzung hierfür sei wiederrum, dass der Arbeitgeber nachweislich alles Zumutbare versucht habe, den Arbeitnehmer auf anderem Wege zu beschäftigen, was ihm im Endeffekt dann aber nicht möglich gewesen sei. Anhaltspunkte dafür, dass der Arbeitgeber der ihn insoweit treffenden Fürsorgepflicht zur Weiterbeschäftigung nachgekommen ist, indem er versucht habe, den Arbeitnehmer auf andere Weise einzusetzen, seien vorliegend aber nicht feststellbar gewesen. Zudem sei die Weiterbeschäftigungsmöglichkeit des Arbeitgebers keinesfalls – wie von Unternehmensseite vorgebracht – auf die Arbeitsplätze des ausgelagerten Teilbereiches beschränkt. Mit der geäußerten Ablehnung zum Betriebsübergang mache der Arbeitnehmer nur von dem ihm gesetzlich eingeräumten Recht Gebrauch. Er ist in einem derartigen Fall so zu behandeln, als wenn überhaupt kein Betriebsübergang stattgefunden habe, sodass der Beschäftigungsanspruch die gesamten Arbeitsplätze im Betrieb erfasse. Insgesamt erteilten die Richter damit auch der sog. sinnenleerten Kündigung, damit eine Absage, die sich aber ohnehin auf absolute Ausnahmefälle beschränken soll.

Besonders interessant sind die ergänzenden Ausführungen des Gerichts zu der Möglichkeit, den Datenschutzbeauftragten auf Grundlage von § 15 Abs. 5 S. 2, Abs. 4 KSchG betriebsbedingt ordentlich kündigen zu können. Die Norm, welche vorsieht, dass

unter gewissen Umständen Betriebs- oder Personalratsmitgliedern ausnahmsweise ordentlich gekündigt werden kann, sofern der Betrieb oder die Abteilung des Beschäftigten stillgelegt worden ist, könne vorliegend bereits nicht angewendet werden. Die Stellung des Datenschutzbeauftragten sei insoweit nicht vergleichbar mit der gesetzlichen Situation eines Betriebs- oder Personalratsmitglieds. Mit der Regelung des § 4f BDSG sei bereits eine eigenständige Vorschrift für Datenschutzbeauftragte geschaffen worden, sodass die entsprechende Vorschrift des KSchG nicht mehr ergänzend herangezogen werden könne. Hätte der Gesetzgeber einen vergleichbaren Ausnahmetatbestand für die Möglichkeit einer ordnungsgemäßen Kündigung gewollt, so hätte er diesen ebenfalls in der Norm des § 4f BDSG verortet.

Abberufung als Datenschutzbeauftragter

Zudem nahmen die Richter Stellung zur Abberufung des Datenschutzbeauftragten, wobei sie hierbei der Unternehmensleitung Recht gaben und die Abberufung als zulässig einstuften. Das Gericht sah, aufgrund der Funktion des Arbeitsnehmers als Leiter der IT-Abteilung sowie der gleichzeitig bekleideten Tätigkeit als Datenschutzbeauftragter, die Gefahr einer Interessenkollision als gegeben an. Es bestehe mitunter die Möglichkeit, dass der Arbeitnehmer seine eigene Arbeit kontrollieren müsse, was dazu führen könne, dass er seine Arbeit nicht mehr weisungsfrei selbst überprüfen könne. Der damit objektiv bestehende Interessenkonflikt mache es ihm unmöglich, beide Funktionen im Unternehmen auszuführen und rechtfertige damit die Abberufung als Datenschutzbeauftragter.

III. Fazit und Konsequenzen für die Praxis

Das Urteil des Landesarbeitsgerichts macht einmal mehr deutlich, wie schwierig es ist, einem Datenschutzbeauftragten bzw. einem Arbeitnehmer, der eine besondere Stellung im Unternehmen einnimmt, zu kündigen. So zeigen die Ausführungen der Richter, dass es hierzu immer besonderer Gründe bedarf, die im Rahmen einer Interessenabwägung den Ausspruch einer

Foto: Justizzentrum Düsseldorf, © Ralf Huels

außerordentlichen Kündigung rechtfertigen. Rein betriebsbedingte Gründe genügen dabei nicht, da die Unsicherheit über den künftigen Arbeitsbedarf zu dem vom Arbeitgeber zu tragenden Wirtschafts- und Betriebsrisiko zählt. Die Möglichkeit einer ordentlichen Kündigung, unter Einhaltung der gesetzlichen Kündigungsfristen, besteht bei Mitarbeitern, denen eine entsprechende Sonderstellung (Betriebs- bzw. Personalrat, Datenschutzbeauftragter) zukommt, ebenfalls nicht.

Die ordentliche Kündigung des Datenschutzbeauftragten kommt, unter Berücksichtigung des Urteils, nunmehr auch dann nicht in Betracht, wenn dieser in einer Abteilung tätig ist, die stillgelegt wird und der Beschäftigte von keiner anderen Abteilung übernommen werden kann. Die in derartigen Fällen für Betriebs- und Personalräte eingreifende Vorschrift (§ 15 Abs. 5 S. 2, Abs. 4 KSchG) kann nach Auffassung des Gerichts nicht auf den Datenschutzbeauftragten übertragen werden. Insoweit muss § 4f BDSG, der die nähere Stellung des Datenschutzbeauftragten betrifft, als abschließend betrachtet werden. Zwar wird diese Ansicht in der Literatur mitunter anders gesehen. Richtigerweise muss jedoch bedacht werden, dass zum Zeitpunkt der Einführung von § 4f BDSG dem Gesetzgeber der Sondertatbestand im KSchG bereits bekannt gewesen ist und er keinen Hinweis auf eine entsprechende Anwendbarkeit erteilt hat. Bis der Gesetzgeber möglicherweise ergänzend Stellung bezieht oder das Bundesarbeitsgericht dieser Ansicht im Rahmen der nachträglich zugelassenen Revision eine Absage erteilt, dürfte in derartigen Konstellationen der Ausspruch einer betriebsbedingten ordentlichen Kündigung unwirksam sein. Diese Situation kann für die Hochschulen vor allem dann relevant werden, wenn sie aufgrund des temporär erhöhten Arbeitsbedarfs gleich mehrere Datenschutzbeauftragte bestellt hat, die sie fortan aber nicht benötigt.

In einem solchen Fall ließe sich zwar mit dem damit für die Hochschule entstehenden Zwang zur Aufrechterhaltung eines sog. sinnentleerten Arbeitsverhältnisses argumentieren. Der bloße Umstand einer Umorganisation bzw. der Wegfall eines Beschäftigungsfeldes genügt in derartigen Fällen aber ebenfalls nicht, um eine erforderliche außerordentliche Kündigung rechtfertigen zu können. Der Arbeitgeber ist wegen des Ausschlusses der ordentlichen Kündigung in einem besonderen Maße verpflichtet, die Kündigung durch geeignete andere Maßnahmen zu vermeiden. Wird es ihm irgendwie möglich sein, das Arbeitsverhältnis sinnvoll fortzusetzen, ist es ihm regelmäßig auch zumutbar, den Arbeitnehmer an anderer Stelle einzusetzen. Erst wenn alle denkbaren Lösungsversuche ausscheiden, gestatten die Gerichte dem Arbeitgeber, durch das Mittel der sog. sinnentleerten betriebsbedingten außerordentlichen Kündigung sich doch noch vom Arbeitnehmer trennen zu können. Derartige extreme Ausnahmefälle sind aber ausgesprochen selten.

Bis dahin verbleibt allenfalls noch die Möglichkeit, den Datenschutzbeauftragten abzuberufen und ihm hierdurch seine Sonderposition zu entziehen. Allerdings erfordert auch die Abberufung des Datenschutzbeauftragten das Bestehen eines besonderen Grundes. Nur wenn Tatsachen oder Umstände bestehen, die unter Berücksichtigung des Einzelfalls und Abwägung der Interessen beider Vertragsparteien eine Fortsetzung der Beschäftigung unmöglich machen, steht einer wirksamen Abberufung nichts im Wege. Eine solche kann unter anderem dann gegeben sein, wenn mit der Aufrechterhaltung der Position die Gefahr eines Interessenkonfliktes gegeben ist. So sahen etwa die Richter eine derartige Situation vorliegend als gegeben an, bei der ein Datenschutzbeauftragter weiterhin eine Mitarbeiterstellung im Unternehmen bekleidet, deren wesentliche Arbeitstätigkeit er durch seine Doppelfunktion hätte selbst kontrollieren müssen. Ansonsten dürften die Fälle der Abberufung eines Datenschutzbeauftragten im Wesentlichen auf schwerwiegende persönliche Verfehlungen oder mangelnde fachliche Fähigkeiten begrenzt sein. Gerade Letztere dürfte jedoch nach vorheriger Einstellung nur schwer festzumachen zu sein. Zudem fällt bei öffentlichen Stellen – anders als bei einem vom Unternehmen bestellten Datenschutzbeauftragten – die Möglichkeit weg, dass die Abberufung des Datenschutzbeauftragten auf Verlangen der Aufsichtsbehörde durchgesetzt werden kann (§ 4f Abs. 4 S. 4 BDSG).

Insgesamt lässt sich dem Urteil damit vor allem die Erkenntnis entnehmen, wie wichtig bereits die sorgsame Auswahl des Arbeitnehmers zur Bekleidung der Position des Datenschutzbeauftragten ist. Insbesondere öffentliche Hochschulen sollten dieses im Hinterkopf haben, da sie als öffentliche Stelle zur Bereitstellung eines Datenschutzbeauftragten gesetzlich verpflichtet sind. Wird im Rahmen der Einstellung nicht ausreichend genug hingeschaut, kann sich dieses im späteren Verlauf rächen. Das Arbeitsrecht stellt an eine wirksame Abberufung oder Kündigung sehr hohe Anforderungen. Auch die Rechtsprechung scheint sich bisher dieser Leitlinie mehr und mehr anzuschließen. Ob dieser Trend sich fortsetzt, wird unter anderem das hierzu erwartete Revisionsurteil des Bundesarbeitsgerichts zeigen. ◆

Übersicht über die Mitgliedseinrichtungen und Organe des DFN-Vereins

(Stand: 05/2014)

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 10. Wahlperiode sind Mitglieder des Verwaltungsrates:
Prof. Dr. Hans-Joachim Bungartz (TU München)
Prof. Dr. Rainer W. Gerling (MPG München)
Prof. Dr. Ulrike Gutheil (TU Berlin)
Dir. u. Prof. Dr. Siegfried Hackel (PTB Braunschweig)
Dr.-Ing.habil. Carlos Härtel (GE Global Research)
Prof. Dr.-Ing. Ulrich Lang (Univ. zu Köln)
Prof. Dr. Joachim Mnich (DESY)
Prof. Dr. Wolfgang E. Nagel (TU Dresden)
Prof. Dr. Bernhard Neumair (KIT)
Dr.-Ing. Christa Radloff (Univ. Rostock)
Prof. Dr. Peter Schirmbacher (HU zu Berlin)
Dr. Wolfgang A. Slaby (Kath. Univ. Eichstätt-Ingolstadt)
Prof. Dr. Horst Stenzel (FH Köln)

Der Verwaltungsrat hat als ständige Gäste
einen Vertreter der KMK:
gegenwärtig Herrn Jürgen Grothe (SMWK Sachsen)

einen Vertreter der HRK:
gegenwärtig Prof. Dr. Joachim Metzner (ehem. Präsident der FH Köln)

einen Vertreter der Hochschulkanzler:
gegenwärtig Herrn Thomas Schöck (Kanzler der Universität Erlangen-Nürnberg)

den Vorsitzenden des ZKI:
gegenwärtig Herrn Martin Wimmer (Universität Regensburg)

den Vorsitzenden der Mitgliederversammlung:
gegenwärtig Prof. Dr. Gerhard Peter (HS Heilbronn)

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
Prof. Dr. Bernhard Neumair

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	Hochschule Amberg-Weiden für angewandte Wissenschaften
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Hochschule Aschaffenburg
Augsburg	Hochschule für angewandte Wissenschaften, Fachhochschule Augsburg
	Universität Augsburg
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)
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin (FUB)
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hochschule der populären Künste (hdpk)
	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)
	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 und 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
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)
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
	Fachhochschule Frankfurt am Main
	Johann Wolfgang Goethe-Universität Frankfurt am Main
	KPN EuroRings B.V.
	Philosophisch-Theologische Hochschule St. Georgen e.V.
	Senckenberg Gesellschaft für Naturforschung
	Stonesoft Germany GmbH
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 mbH
	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
	Datenlotsen Informationssysteme GmbH
	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-Fachhochschule 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	Fachhochschule 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
Oberursel	Dimension Data Germany AG & Co. KG
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
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
	NextiraOne Deutschland GmbH
	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 (FH)
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	Fachhochschule 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