DFN
Mitteilungen

(Nur) der Name bleibt

X-WiN: Eine neue Technikgeneration zieht ein

Copernicus – observing the earth
Der Weg der Daten über das Deutsche Forschungsnetz

GÉANT Testbeds Service
Was kann der neue Service?

9 770177 689001

Impressum

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

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

ISSN 0177-6894

Redaktion: Nina Bark
Gestaltung: Labor3 | www.labor3.com
Druck: Schöne Drucksachen, Berlin

Fotonachweis:
Titelfoto © Stephan Zabel / iStockphoto.de
Seite 6/7 © Angelika Schwarz / iStockphoto.de
Seite 42/43 © franky2010 / fotolia.de

Prof. Dr. Gerhard Peter
Altrektor der Hochschule Heilbronn,
ehem. Leiter der DFN-Nutzergruppe
Hochschulverwaltung

Eine der ältesten Einrichtungen im DFN kommt in die Jahre und ist doch mit 25 Jahren jung geblieben.

Als langjähriger, ehemaliger Sprecher der DFN-Nutzergruppe Hochschulverwaltung möchte ich die Gelegenheit nutzen, allen jenen zu danken, die in den vergangenen Jahren zum Gelingen der Tagungen und zu der laufenden Arbeit der Nutzergruppe beigetragen haben. Dies auf freiwilliger Basis so lange erfolgreich zu machen ist außergewöhnlich.

Das Bewusstsein, dass die Möglichkeiten des Netzes nicht nur Forschung und Lehre in den verschiedenen Wissenschaftsdisziplinen verändert hat und auch weiterhin beeinflussen wird, sondern vor allem auch tief in die Struktur der Institution Hochschule und deren Management eingreift, ist der Grund dafür, dass die Nutzergruppe Hochschulverwaltung ungebrochen erfolgreich gearbeitet hat und weiterhin arbeiten wird.

Die Initiatoren von einst sind jetzt alle im Ruhestand und es kann festgestellt werden, dass der Generationswechsel gelungen ist.

Der Nutzergruppe ist außerdem etwas Erstaunliches gelungen. Trotz intensiver, langjähriger Arbeit ist die Gruppe zusammengewachsen und die Mitglieder sind sich freundschaftlich verbunden. Obwohl intensiv gearbeitet wird, macht die Arbeit in der Gruppe einfach Spaß und ist vielleicht damit der Grund, weshalb sie so erfolgreich ist.

Das 25-jährige Jubiläum werden wir an der Fachhochschule der Sächsischen Verwaltung Meißen am 7. Oktober feiern.

Unsere Autoren dieser Ausgabe im Überblick

1 Felix von Eye, Leibniz-Rechenzentrum-LRZ (felix.voneye@lrz.de); **2** Michael Grabatin, Universität der Bundeswehr München (michael.grabatin@unibw.de); **3** Prof. Dr. Wolfgang Hommel, Universität der Bundeswehr München (wolfgang.hommel@unibw.de); **4** Michael Röder, DFN-Verein (roeder@dfn.de); **5** Dr. Stefan Piger, DFN-Verein (piger@dfn.de); **6** Dr. Leonie Schäfer, DFN-Verein (schaefer@dfn.de); **7** Dr. Jakob Tendel, DFN-Verein (tendel@dfn.de); **8** Dr.-Ing. Susanne Naegele-Jackson, Regionales Rechenzentrum Erlangen RRZE (susanne.naegele-jackson@fau.de); **9** Dr. Peter Kaufmann, DFN-Verein (kaufmann@dfn.de); **10** Bernhard Schmidt, Leibniz-Rechenzentrum-LRZ (bernhard.schmidt@lrz.de); **11** Daniel Feuchtinger, Leibniz-Rechenzentrum-LRZ (daniel.feuchtinger@lrz.de); **12** Prof. Dr. Helmut Reiser, Leibniz-Rechenzentrum-LRZ (helmut.reiser@lrz.de); **13** Prof. Dr. Gerhard Peter, HS-Heilbronn (gerhard.peter@hs-heilbronn.de); **14** Prof. Dr. Andreas Hanemann, Fachhochschule Lübeck (hanemann.andreas@fh-luebeck.de); **15** Sergej Schumilo, OpenSource Security (sergej@os-t.de); **16** Ralf Spenneberg, OpenSource Security (ralf@os-t.de); **17** Dr. Ralf Gröper, DFN-Verein (groeper@dfn.de); **18** Clara Ochsenfeld, Forschungsstelle Recht im DFN (recht@dfn.de); **19** Florian Klein, Forschungsstelle Recht im DFN (recht@dfn.de)

Inhalt

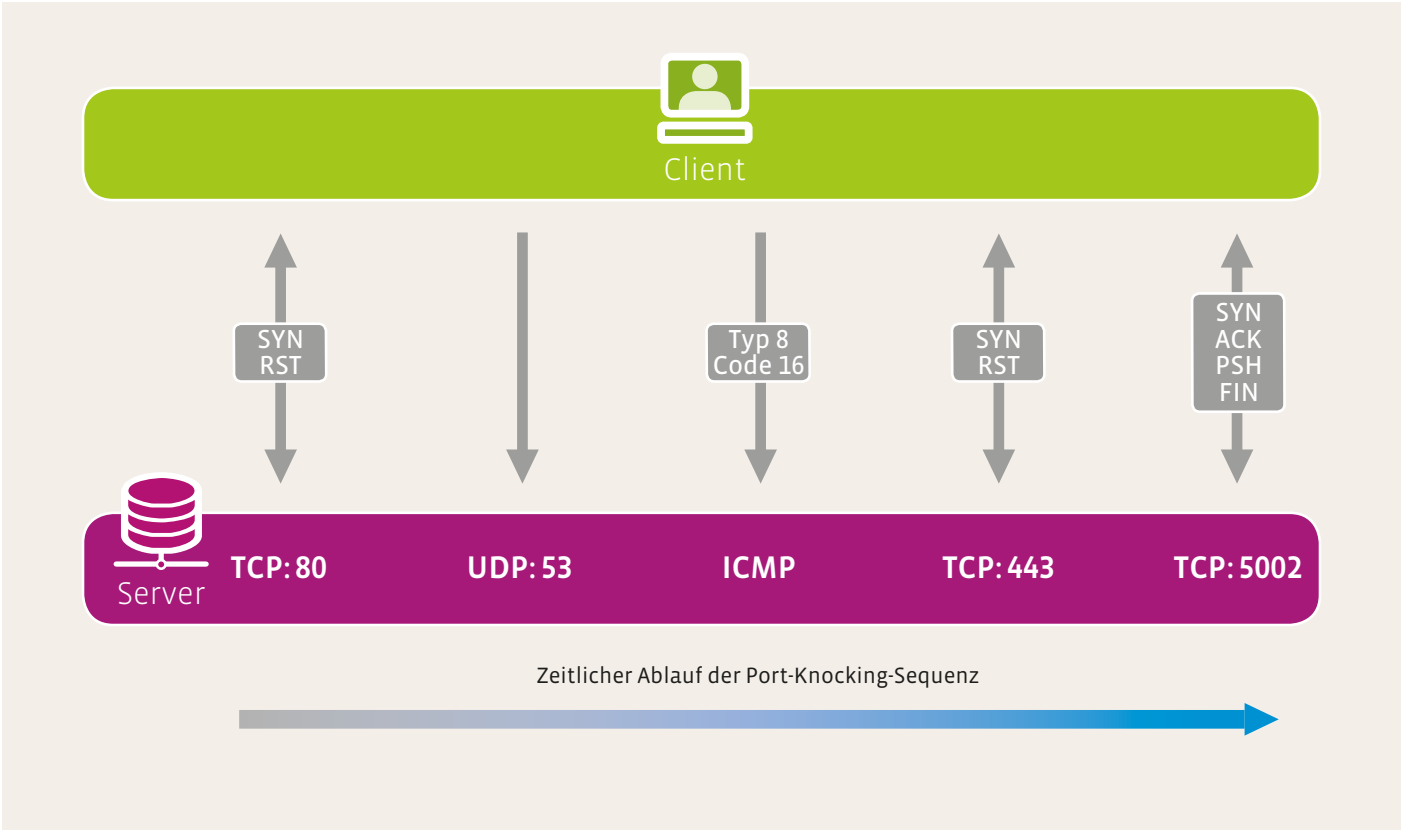
Wissenschaftsnetz

DFN „X-WiNner-Award“ – der Gewinnerbeitrag des Jahres 2015

Netzbasierte Erkennung von mittels Port Knocking versteckten Diensten und Backdoors

Sollen Serverdienste nicht weltweit und trotzdem für jeden erreichbar angeboten werden, gibt es neben dem klassischen Firewall-Ansatz auch eine weitere Technik: Port Knocking. Bei dieser Technik wird ein Server-Port erst dann für eine Nutzung geöffnet, wenn eine vorab festgelegte Folge von speziellen Paketen an den Server geschickt wurde.

Text: **Felix von Eye, Michael Grabatin und PD Dr. Wolfgang Hommel** (Leibniz-Rechenzentrum)



Neben der legitimen Nutzung dieser Technik bietet diese für einen Angreifer eine interessante Methode, um seine Präsenz auf einem erfolgreich kompromittierten System zu verschleiern. Zumeist versucht ein Angreifer ein Zielsystem unter seine Kontrolle zu bringen, wobei er seine Aktivitäten durch die Nutzung von Rootkits vor den Augen von lokalen Sicherheitssystemen und Administratoren verschleiern kann.

Ähnlich wie Rootkits funktioniert auch ein Port-Knocking-geschützter Serverport. Da aktive Scans die Port-Knocking-Sequenz nicht kennen, werden sie den Port nicht als geöffnet bzw. genutzt markieren. Somit ist es einem Angreifer auch möglich, unbemerkt von den Sicherheitsscans der Netzadministratoren zu kommunizieren. Dass dies kein theoretisches Konstrukt ist, sondern ebenfalls schon aktiv ausgenutzt wurde, zeigt der Bericht [1] über die Freenode IRC Port-Knocking-Backdoor.

Abbildung 1 zeigt als Beispiel eine Port-Knocking-Sequenz, bei der durch den Client nacheinander verschiedene spezielle Pakete verschickt werden: Port 80 mit TCP, Port 53 mit UDP, ein ICMP-Paket mit speziellen Header-Informationen, Port 443 mit TCP und schließlich ein vollständiger Verbindungsaufbau auf Port 5002 mit TCP.

Im Folgenden soll nun ein neuer Ansatz beschrieben werden, mit dessen Hilfe man Backdoors und versteckte Dienste erkennen kann. Unter günstigen Voraussetzungen ist es zudem möglich, die verwendete Port-Knocking-Sequenz zu erkennen.

Neuer Ansatz

Zum Erkennen versteckter Dienste sind im Wesentlichen drei Komponenten nötig. Neben einer Komponente zur Aufzeichnung von Flow Records, die üblicherweise durchgehend laufen sollte, und einer Komponente zur Auswertung aller Daten existiert ebenfalls eine Komponente, die regelmäßig Portscans ausführt.

Die hier vorgestellte Erkennung von versteckten Diensten nutzt als Datenbasis zum einen Portscans und zum anderen Flow Records. Die Portscans werden im gewählten Ansatz für zwei verschiedene Zwecke verwendet: Zum einen werden durch einen Portscan alle regulären Dienste identifiziert, da sich ein Netzadministrator mit Hilfe von Portscans einen Überblick über die in seinem Netz laufenden Dienste verschaffen kann. Werden diese Portscans regelmäßig durchgeführt und miteinander verglichen, so können neue, potentiell nicht erwünschte Dienste aufgespürt werden [2]. Durch eine Filterfunktion können somit alle Flow Records der regulären Dienste aussortiert werden, was die Menge der zu analysierenden Flow Records signifikant reduziert. Leider ist es unvermeidlich, dass Dienste, die zwischen zwei Portscan-Durchläufen neu installiert oder grundlegend umkonfiguriert werden, in dieser Zeit nicht als reguläre Dienste erkannt werden. Dieses Problem sollte jedoch mit einer Change-Management-Dokumentation, kurzen Zeitintervallen zwischen zwei Portscans oder dem möglichen Umstand, dass neue Dienste in der ersten Zeit zunächst nur wenig frequentiert sind, in der Praxis abgefedert werden können.

Zum anderen ist es mit Hilfe von Portscans möglich, mit einer gewissen Wahrscheinlichkeit zu ermitteln, ob es sich bei einem System um ein Server- oder um ein Clientsystem handelt, indem typische Serverdienste ermittelt werden. Dies ermöglicht unter anderem, die evilshell-Backdoor [3] zu erkennen, da es für ein Serversystem üblicherweise hinreichend unwahrscheinlich ist, eine Kommunikation nach außen anzustoßen, wenn es sich nicht um Update-, Zeit-, DNS-Server oder ähnliches handelt. Diese Sonderfälle sind leicht beherrschbar, indem man die Ziel-IP-Adressen legitim kontaktierter Server in einer Ausnahmeliste behandelt. Insbesondere ist damit auch die Server-Server-Kommunikation vieler Dienste (z. B. SMTP oder HTTP-Proxy) innerhalb des eigenen Netzes einfach zu entdecken.

Um nun potentielle Port-Knocking-Sequenzen aufzuspüren, werden die Flow Records an einem zentralen Punkt gesammelt und, wie oben bereits erwähnt, mit den letzten Portscanningergebnissen abgeglichen. Dabei werden nur Verbindungen gespeichert, deren Kommunikation mit einem bisher nicht genutzten Port verläuft. Somit werden alle Verbindungen mit bereits bekannten Ports aussortiert.

Nun werden die Verbindungen analysiert und in kleine zeitliche Intervalle eingeteilt. Innerhalb dieser Intervalle wird untersucht, ob Verbindungen existieren, bei denen nach mehreren Versuchen mit unterschiedlichen Ports und Protokollen eine erfolgreich aufgebaute Verbindung registriert wurde, wobei die Richtung des erfolgreichen Verbindungsaufbaus irrelevant ist. Dabei muss beachtet werden, dass sich bei den initialen Verbindungsversuchen mindestens einmal der Port oder das Protokoll unterscheiden muss, um beispielsweise häufig in der Praxis anzutreffende mehrmalige Verbindungsversuche wegen Verbindungsfehlern nicht als irreguläres Verhalten zu melden.

Da es bei den Malware-Beispielen bislang meist der Fall ist, dass feste Port-Knocking-Sequenzen verwendet werden, können die gefundenen Sequenzen gespeichert werden, was einem Administrator die Möglichkeit verschafft, den restlichen Netztraffic

nach genau dieser Signatur abzusuchen, um ggf. weitere Systeme mit den gleichen versteckten Diensten zu identifizieren. Da jedoch ein Angreifer ein solches Verhalten jederzeit mit wenig Aufwand ändern kann oder z. B. nur noch One-Time-Port-Knocking-Sequenzen verwendet, ist dies nur ein optionales Feature und es ist unabhängig von dem restlichen Erkennungsverfahren.

Fazit

Port Knocking hat sich bewährt, um Dienste wie den SSH-Zugriff auf Server weltweit über das Internet zu ermöglichen, ohne sie den Risiken durch eine direkte Erreichbarkeit durch Angreifer auszusetzen. Das Verfahren funktioniert jedoch so gut, dass selbst die Administratoren nicht mehr einfach erkennen können, welche derart versteckten Dienste in ihren Netzen betrieben werden. Problematisch ist dies insbesondere dann, wenn Systeme kompromittiert wurden und der Angreifer einerseits seine Aktivitäten auf dem System durch Rootkits lokal komplett verbirgt und andererseits eine per Port Knocking geschützte Backdoor einrichtet.

In diesem Beitrag wurde ein Verfahren vorgestellt, mit dem Flow-Record-basierte Aufzeichnungen des Netzverkehrs auf Anzeichen typischer Port-Knocking-Backdoors untersucht werden können. Durch eine Korrelation mit vorhandenem Wissen über legitime Serverdienste im Netz, das beispielsweise mit vorgelagerten Portscans gewonnen wurde, lässt sich der auszuwertende Flow-Record-Datenbestand auf ein beherrschbares Maß reduzieren. Tests einer prototypischen Implementierung in einer Laborumgebung zeigen dennoch, dass noch ein für heuristisches Security-Monitoring nicht unüblich hoher Anteil an False Positives auftreten kann, die jedoch ausgefiltert werden können. Die Tests zeigen auch, dass für die Erkennung komplexerer Port-Knocking-Sequenzen noch wesentlich effizientere Auswertealgorithmen benötigt werden, um nicht nur die derzeit einfach verfügbaren, trivial implementierten Backdoors zuverlässig erkennen zu können. ◆

Der „X-WiNner-Award“ des DFN Vereins

Das DFN-Forum Kommunikationstechnologien ist seit 2008 das neue Format der ehemaligen „DFN-Arbeitstagung über Kommunikationsnetze“. Dabei versteht sich das Forum als eine wissenschaftliche Tagung, deren primäre Zielgruppe (aber nicht nur!) junge vielversprechende Nachwuchswissenschaftler aus netznahen Themenkreisen sind. Die adressierten Themenkreise sind „Neue Netztechnologien und Infrastruktur“, „ITC Management und Sicherheit“, „Infrastrukturen für eResearch“ und „IT Zukunftsperspektiven“.

Aus den Einreichungen wählt das Programmkomitee aus erfahrenen und etablierten Gutachtern etwa ein Dutzend der besten Beiträge aus, die dann in der Veranstaltung von den Autoren präsentiert werden. Dort müssen sie sich dann kritisch-freundlichen Rückfragen und Kommentaren stellen. Abgerundet wird das Programm durch „Invited Speakers“, die zu topaktuellen Themen aus der netznahen IT vortragen, und durch ein hochkarätiges Panel, welches in Form einer Podiumsdiskussion tagesaktuelle Themen aufgreift und aus verschiedensten Blickwinkeln beleuchtet.

Um den Anreiz für hervorragende Nachwuchswissenschaftler noch zu erhöhen, ihre Beiträge beim DFN-Forum einzureichen, wurde der „X-WiNner-Award“ entwickelt. Der Preis wird für den besten NachwuchswissenschaftlerInnen-Beitrag, dessen Hauptautor bei der Einreichung noch nicht promoviert ist, verliehen. Dabei ist das primäre Auswahlkriterium immer die Qualität des eingereichten Beitrags, über die das Programmkomitee schon bei der Auswahl diskutiert. Die letztendliche Entscheidung fällt dann nach Urteil der Juroren Professorin Gabi Dreo-Rodosek und Professor Paul Müller, die die Qualität der Präsentation und des Vortrags hinzuziehen.

Der X-WiNner-Award ist neben der immateriellen Ehre und Anerkennung in der Fachcommunity auch mit einem Preisgeld in Höhe von 1000 EUR dotiert. Als Sponsor für diesen Preis konnte die Geschäftsstelle des DFN-Vereins die Firma Dimension Data gewinnen.

Die erstmalige Verleihung des X-WiNner-Award auf dem 8. DFN-Forum Kommunikationstechnologien in Lübeck im vergangenen Jahr wird von allen Beteiligten als voller Erfolg gewertet, so dass wir uns sehr freuen, auch in diesem Jahr auf dem 9. DFN-Forum an der Universität Rostock diesen Nachwuchspreis wieder verleihen zu können. Die Einreichungen sind jedenfalls vielversprechend!

Literatur

[1] NCC Group. Analysis of the Linux backdoor used in freenode IRC network compromise. https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/october/analysis-of-the-linux-backdoor-used-in-freenode-irc-network-compromise/, Oktober 2014.

[2] Felix von Eye, Stefan Metzger und Wolfgang Hommel. Dr. Portscan: Ein Werkzeug für die automatisierte Portscan-Auswertung in komplexen Netzinfrastrukturen. In Christian Paulsen, Hrsg., Sicherheit in vernetzten Systemen: 20. DFN-Workshop, Seiten C-1–C-21, Norderstedt, Deutschland, Januar 2013. Books on Demand.

[3] Simpp. evilshell.c – backdoor remote connect. http://packetstormsecurity.com/files/69560/evilshell.c.html, September 2008.

Plakette drauf, der Nächste bitte – Infrastruktur auf dem Prüfstand

Eine Vielzahl von Daten ist schützenswert. Um das potenzielle Risiko eines Fremdzugriffs auf Daten bewerten oder verringern zu können, müssen Datenschutz und Datensicherheit eng miteinander verknüpft werden.

Text: **Michael Röder** (DFN-Verein)

Foto © katrin_timoff/fotolia.de

Datenschutz …

Jeder Mensch darf selbst bestimmen, welche privaten Informationen er bereit ist, mit der Öffentlichkeit zu teilen: jede Einwohnerin und jeder Einwohner der Bundesrepublik Deutschland besitzt das Recht auf informationelle Selbstbestimmung. Wenn die Verwendung privater Daten zur Erfüllung einer Aufgabe oder eines Dienstes dennoch erforderlich ist, muss der Dienstanbieter dafür sorgen, diese Daten vor Verfälschung und Missbrauch zu beschützen. Die effektivste Methode, um Daten zu schützen ist die Datensparsamkeit:

> *„Erhebe, verarbeite und nutze so wenige Daten wie möglich und nicht mehr als unbedingt nötig“*

… und Datensicherheit

Das Datenschutzrecht verpflichtet die jeweils verantwortliche Stelle zum Ergreifen konkreter technischer und organisatorischer Maßnahmen (TOMs), um die Vorgaben der Datenschutzgesetze zu gewährleisten.

Die Daten- bzw. IT-Sicherheit hält vom Vier-Augen-Prinzip über Schließsysteme und Videokameras bis zur Firewall am Übergang zwischen zwei Netzbereichen eine große Vielfalt an Werkzeugen bereit, um sensible Daten, wie beispielsweise personenbezogene Daten, abzusichern. Datensicherheit stellt aber auch Ansprüche an die Verfügbarkeit der Daten. Redundanzen können dabei sowohl im Falle einer Unterbrechung der Stromversorgung als auch beim Vorbeugen vor dem Verlust von Inhalten hilfreich sein.

Verarbeitung personenbezogener Daten im Auftrag

Wird ein Prozess der Datenverarbeitung ganz oder teilweise ausgelagert, kann eine Verarbeitung personenbezogener Daten im Auftrag vorliegen. Personenbezogene Daten sind Daten, die unmittelbar oder mit geringem Aufwand auf eine bestimmte oder bestimmbare natürliche Person schließen lassen. Dazu zählen unter anderem E-Mail-Adressen, Telefon- / Telefax-Nummern, Anschrift, etc.

Wenn personenbezogene Daten im Auftrag verarbeitet werden, bleibt die auftraggebende Einrichtung verantwortliche Stelle im datenschutzrechtlichen Sinne. In diesem Fall wird eine schriftliche Vereinbarung über die Gestaltung des Datenverarbeitungsprozesses abgeschlossen: die sogenannte Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag oder auch Auftragsdatenverarbeitung (ADV).

Wesentlicher Bestandteil der ADV ist die Verankerung einer Kontrollpflicht. Die verantwortliche Stelle darf und muss die verarbeitende Stelle in regelmäßigen Abständen auf die korrekte Durchführung der TOMs kontrollieren.

Zertifizierung des Dienstanbieters als Unterstützung der Kontrollpflicht

Der DFN-Verein unterstützt die Anwender seines Dienstes DFN-MailSupport bei ihrer Pflicht, den Dienst und die dafür benötigte Infrastruktur zu überprüfen.

Um Einrichtungen, die am Dienst DFN-MailSupport teilnehmen, den Aufwand zu erleichtern, selbst die gesamte Infrastruktur zu überprüfen, lässt der DFN-Verein die Bestandteile dieses Dienstes durch einen unabhängigen BSI-zertifizierten Auditor bewerten. Das Votum des Auditors wird in einem Auditbericht festgehalten und kann von der teilnehmenden Einrichtung für die Erfüllung der eigenen Kontrollpflicht in Betracht gezogen werden. ◆

DFN-MailSupport hat Auditierung der Aufbaustufe nach ISO 27001 auf Basis von IT-Grundschutz erfolgreich absolviert

DFN-MailSupport hat zum Oktober 2015 im Anschluss an das Audit der Aufbaustufe nach ISO 27001 auf Basis von IT-Grundschutz ein positives Votum erhalten. Im März 2016 fand das Datenschutzaudit statt.

DFN-MailSupport ist eine E-Mail-Filterstruktur mit der Aufgabe, das Aufkommen schädlicher Inhalte im Wissenschaftsnetz zu reduzieren. Dabei wird versucht, den Schadgehalt eingehender E-Mails automatisch anhand diverser Kriterien zu bewerten. Wird das Ergebnis vom Endnutzer anders interpretiert, kann er das Verhalten des Filters durch Trainingsprozesse konditionieren. Denn mancher Newsletter ist im einen Büro unerwünschter Spam, während er für das Büro nebenan unverzichtbare Neuigkeiten enthält. Unter anderem deshalb stellt DFN-MailSupport besondere Ansprüche an die Konfigurierbarkeit einzelner Filterparameter. Zu diesem Zweck steht den Anwendern online eine Plattform zur Verfügung, über welche der Dienst gezielt auf die Anforderungen der teilnehmenden Einrichtung angepasst werden kann.

Um über Erfolg oder Misserfolg bei der Einlieferung einer Mail zu entscheiden, werden diverse Filtermethoden eingesetzt, wie beispielsweise:

- Real-time-Blacklisten: RBL geben Aufschluss darüber, ob der Absender in der Vergangenheit durch den Versand unerwünschter Inhalte bereits negativ aufgefallen ist.
- Adressverifikation: Die Prüfung der Zieladresse gegen alle verfügbaren Postfächer und Aliase eines Teilnehmers verrät, ob das Empfängerpostfach tatsächlich existiert. Häufig werden Zieladressen von Spammern automatisch generiert. Die Spam-Mail wird dann nur eingeliefert, wenn zufällig ein Postfach mit dieser Adresse vorhanden ist.
- PreGreet-Check: Das Transportprotokoll, das zum Mailversand genutzt wird, definiert eigene Sicherheitsmechanismen. Darüber kann ein Mailserver herausfinden, ob er eine Mail von einem seriösen Einlieferer erhält, oder ob der versendende Server gegen technische Standards verstößt. Beim PreGreet-Check verzögert der Server nach Annahme der TCP-Verbindung seine eigene SMTP-Greeting-Message. Wartet die Gegenstelle diese Verzögerung nicht ab, verstößt sie gegen die Spezifikation des SMT-Protokolls und wird abgelehnt.

Ob eine Mail unerwünscht sein könnte oder einen Virus mit sich führt, lässt sich allerdings nur herausfinden, indem der gesamte Inhalt der Nachricht auf Spameigenschaften bzw. auf die Signaturen bekannter Schadsoftware hin untersucht wird. Dabei ist es unvermeidbar, auch erwünschte E-Mails mit anstandslosem Inhalt zu scannen. Deshalb werden in einem solchen Szenario immer auch personenbezogene Daten verarbeitet. Um die ordnungsgemäße Verarbeitung personenbezogener Daten zu dokumentieren, hat sich der DFN-Verein für die regelmäßige Durchführung eines Datenschutzaudits entschlossen.

Datenschutz stellt hohe Anforderungen an die IT-Sicherheit.

Aus diesem Grund wird bei der Auditierung von DFN-MailSupport dem Datenschutzaudit ein Audit nach ISO 27001 auf der Basis von IT-Grundschutz vorgelagert. Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) definiert durch die Einstiegsstufe und die Aufbaustufe zwei Vorstufen bevor das eigentliche Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz erteilt wird.

Jede einzelne Stufe muss innerhalb eines Zeitraumes von 24 Monaten durch die nächsthöhere Stufe abgelöst werden. Im Anschluss an jede erfolgreich absolvierte Vorstufe wird erneut ein Datenschutzaudit durchgeführt.

Die Rollen der beteiligten Parteien

Beim Dienst DFN-MailSupport werden zwei Rollen definiert:

- Anbieter und
- Anwender

Der DFN-Verein betreibt als Anbieter die Infrastruktur und gestaltet den Dienst. Eine Einrichtung aus Wissenschaft und Forschung, die vom Aufwand des DFN-Vereins profitieren möchte, kann Anwender werden. Bei einer Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag (ADV) gibt es dieselben Rollen. Diese tauschen allerdings die Plätze:

- Auftraggeber der ADV: ist die am Dienst DFN-Mail-Support teilnehmende Einrichtung
- Auftragnehmer der ADV: ist der DFN-Verein

Denn wenn eine Einrichtung den Dienst DFN-MailSupport nutzen möchte, erteilt sie dem DFN-Verein den Auftrag, personenbezogene Daten für ihre Bedürfnisse zu verarbeiten. Sie bleibt weiterhin verantwortlich für die verarbeiteten Daten.

(Nur) der Name bleibt

Die Erneuerung des Wissenschaftsnetzes erfolgte seit Gründung des DFN-Vereins periodisch mit steigenden Anforderungen durch die Teilnehmer und der Verfügbarkeit leistungsfähigerer Netztechnik. Auch aktuell befindet sich das Wissenschaftsnetz wieder in einer Phase der Erneuerung.

Text: **Stefan Piger** (DFN-Verein)

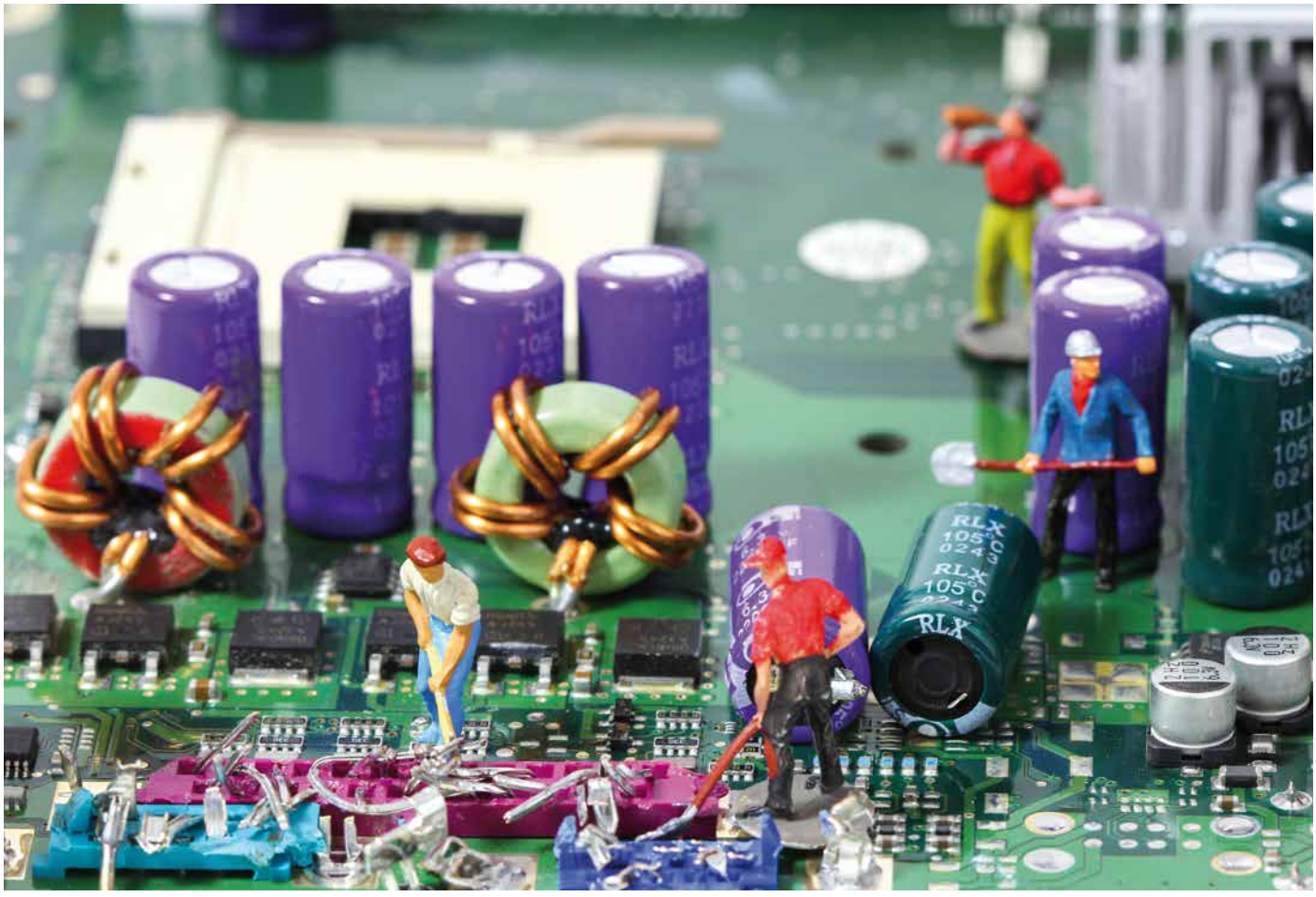


Foto © jarts/photocase.com

Einleitung

In den früheren Implementierungen des Wissenschaftsnetzes (B-WiN, G-WiN) wurde die neue Infrastruktur parallel zur bestehenden komplett neu aufgebaut. Bei Betriebsbereitschaft wurde der Wirkverkehr auf die neue Netzgeneration überführt und der Vorgänger abgeschaltet. Zuletzt wurde dieses Vorgehen 2006 mit dem Übergang auf das X-WiN gewählt.

Ein Generationswechsel der gesamten Netztechnik in einem Schritt ist heute durch den deutlich komplexeren Aufbau des X-WiN gegenüber seinen Vorgängern nicht mehr möglich. Durch die unterschiedlichen Innovationszyklen der eingesetzten Systeme und die sauber definierten Schnittstellen zwischen den Plattformen ist er aber auch nicht notwendig. Somit können die erforderlichen Arbeiten über einen längeren Zeitraum verteilt werden und weitgehend ohne kostenintensiven Parallelaufbau erfolgen.

Was bisher geschah: Ein Rückblick auf die Jahre 2012-2014

Als erste zu erneuernde Plattform wurde in 2012 die Optische Plattform und damit die im X-WiN eingesetzte DWDM-Technik ausgewählt, da hier großes Einsparpotential durch den Wechsel des Betreibermodells erwartet wurde und der Innovationszyklus in diesem Bereich am weitesten fortgeschritten war. Angestrebt und nachfolgend auch umgesetzt wurde der Übergang von einem statischen DWDM-System mit festen Pfadverläufen von WDM-Verbindungen durch das Kernnetz zu einem vollständig flexiblen System mit frei wählbaren und aus der Ferne beeinflussbaren Verbindungen. Außerdem konnten mit der neuen DWDM-Technik 2013 erstmals Verbindungen mit 100 Gbit/s im X-WiN geschaltet werden.

Mit dem Wechsel auf die neue Optische Plattform und die damit verbundenen geringeren Kosten für die Multiplexer-Technik konnten seit 2012 auch eine Anzahl von neuen Kernnetzknoten realisiert werden. Ausgehend von den 56 Bestandsknoten wurden bis heute neun weitere Knoten aufgebaut und größtenteils bereits in Betrieb genommen. Mit dem Aufbau dieser zusätzlichen Kernnetzknoten verfolgt der DFN-Verein zwei Ziele: Zum einen dienen sie der Erhöhung der Verfügbarkeit von hochbandbreitigen DFNInternet-Diensten, zum anderen lassen sich durch die Verkürzung der Wege Kosteneinsparungen im Bereich der Teilnehmeranbindungen erreichen.

Die zweite große Migration fand noch während der Umstellung der DWDM-Technik statt und betraf den SuperCore der IP-Plattform. Die vier Router dieser Plattform, die die Übergänge zwischen den Ketten der X-WiN-Router sowie zu den Peerings realisieren, wurden noch in 2012 ausgetauscht. Ziel war es, die mit der neuen DWDM-Technik ermöglichten zusätzlichen Kapazitäten, insbesondere weitere 10-Gigabit-Ethernet-Verbindungen terminieren zu können und den SuperCore auf die kommende 100-Gigabit-Ethernet-Technik vorzubereiten. Nach erfolgter Migration auf die neuen Systeme wurde 2013 die 100-Gigabit-Ethernet Technologie erstmals auf den Verbindungen des SuperCore eingesetzt.

Weitere Arbeiten in 2013 und 2014 betrafen die Infrastruktur des Kernnetzes. Hier wurde insbesondere die Stromversorgung der X-WiN-Technik mit dem Aufbau weiterer USV-Anlagen auf sichere Beine gestellt. Insgesamt wurde die Zahl der im Betrieb befindlichen USV-Anlagen mit heute 39 bei 65 Kernnetzknoten mehr als verdoppelt und damit die Stabilität des Netzbetriebs entscheidend verbessert.

Abseits des Zentrums: Die Erneuerung des Zugangsnetzes

Für die Teilnehmer am DFNInternet-Dienst gibt es verschiedene Optionen der Anbindung an das Kernnetz des X-WiN. Die einfachste und leistungsfähigste in Bezug auf die realisierbare Bandbreite ist ein lokaler Anschluss an einen Kernnetzknoten. Diese Variante können jedoch nur Einrichtungen nutzen, auf deren Campus der Kernnetzknoten errichtet wurde bzw. die über das lokale Netz der gastgebenden Einrichtung erreichbar sind.

Für die meisten Teilnehmer müssen andere Wege der Anbindung gefunden werden. In der Regel wird hier auf Verbindungen kommerzieller Carrier zurückgegriffen, welche am Markt beschafft werden. Zum Einsatz kommen in geringerer Anzahl Dark-Fibre-Verbindungen; die Mehrzahl sind auf SDH- bzw. zunehmend auf Carrier-Ethernet-basierende Ethernet-Verbindungen mit Bandbreiten zwischen 100 Mbit/s und 10 Gbit/s. Derzeit sind für den DFNInternet-Dienst über 700 dieser Verbindungen in Betrieb.

Um für die Teilnehmer einen kosteneffizienten Dienst mit regelmäßigen Anpassungen der Bandbreiten in den Kategorien des DFNInternet-Dienstes realisieren zu können, werden die Teilnehmeranbindungen periodisch neu ausgeschrieben und damit europaweit in den Wettbewerb gestellt. 2014 wurde eine Ausschreibung dieser Art von der DFN-Geschäftsstelle vorbereitet und dann im Laufe des Jahres 2015 durchgeführt (siehe dazu die Kurzmitteilung auf Seite 19).

Die neuen Anbindungen werden voraussichtlich im Laufe des zweiten Quartals 2016 beauftragt, nachfolgend realisiert und in Betrieb genommen.

Verstärkung des Kerns: Die Erweiterung des SuperCore

Das X-WiN erlebt seit Anfang 2015 eine deutliche Steigerung des transferierten Datenvolumens. Flachten die Steigerungsraten in den Jahren 2012–2014 auf im Mittel 18% im Jahresvergleich der betrachteten Monate ab, stiegen sie seit Jahresbeginn 2015 auf im Mittel 34 % an. Das X-WiN transportiert damit in Spitzenmonaten wie dem Januar 2016 über 34 PB an Daten.

Diese gewaltigen Datenvolumina müssen zwischen den Anwendern sowie zwischen diesen und den Außenanbindungen des X-WiN vermittelt werden. Um diesem Wachstum Rechnung zu tragen und auf weiteres Wachstum vorbereitet zu sein, wurde der SuperCore der IP-Plattform in 2015 erheblich ausgebaut.

Das primäre Ziel war es, den Bedarf an 100-Gigabit-Ethernet-Schnittstellen zu decken. Diese Schnittstellen werden insbesondere für den Ausbau der Verbindungen zwischen den Systemen des SuperCore benötigt, zunehmend aber auch für die Anbindung der größten DFNInternet-Teilnehmer sowie für den Ausbau der wichtigsten Außenanbindungen des X-WiN.

Da die seit 2013 eingesetzte Technik nicht die notwendige Dichte an Schnittstellen bereitstellen konnte, wurden die jetzt verfügbaren, erheblich leistungsfähigeren Systeme beschafft und an den bestehenden Kernnetzknoten Berlin, Erlangen, Frankfurt und Hannover installiert. Mit diesem Ausbauschritt konnten die Verbindungen im SuperCore auf je Kante 2 x 100 Gbit/s (vgl. Abbildung 1) sowie der Übergang zum wichtigsten kommerziellen Internet-Austauschpunkt DE-CIX ebenfalls auf 2x100 Gbit/s (vgl. Abbildung 2) ausgebaut werden.

Das zweite mit der Erweiterung des SuperCore verfolgte Ziel war die Reduktion der Paketlaufzeiten zwischen direkt am SuperCore angebundenen Teilnehmern und den kleineren Einrichtungen, die auf den X-WiN-Router-Systemen (xr) terminieren. Zur Realisierung dieses Ziels kamen die an den vier inneren Standorten des SuperCore ausgebauten Router zum Einsatz. Diese wurden an die vier neuen SuperCore-Standorte in Essen, Garching, Hamburg und Leipzig verbracht und mit jeweils einer 100G-Verbindung an zwei Router des inneren SuperCore angebunden (vgl. Abbildung 1). Diese Arbeiten wurden im zweiten Halbjahr 2015 durchgeführt.

Für das erste Halbjahr 2016 sind weitere Umschaltungen zur Verkürzung der direkten Anwenderanbindungen sowie zur Vereinfachung der X-WiN-Topologie durch Auftrennen langer und stark vermaschter Ketten der X-WiN-Router geplant.

Schau was kommt von draußen rein: Schutz vor DDoS-Angriffen im X-WiN

Mit der Erhöhung der Übertragungskapazität im SuperCore des X-WiN verfolgt

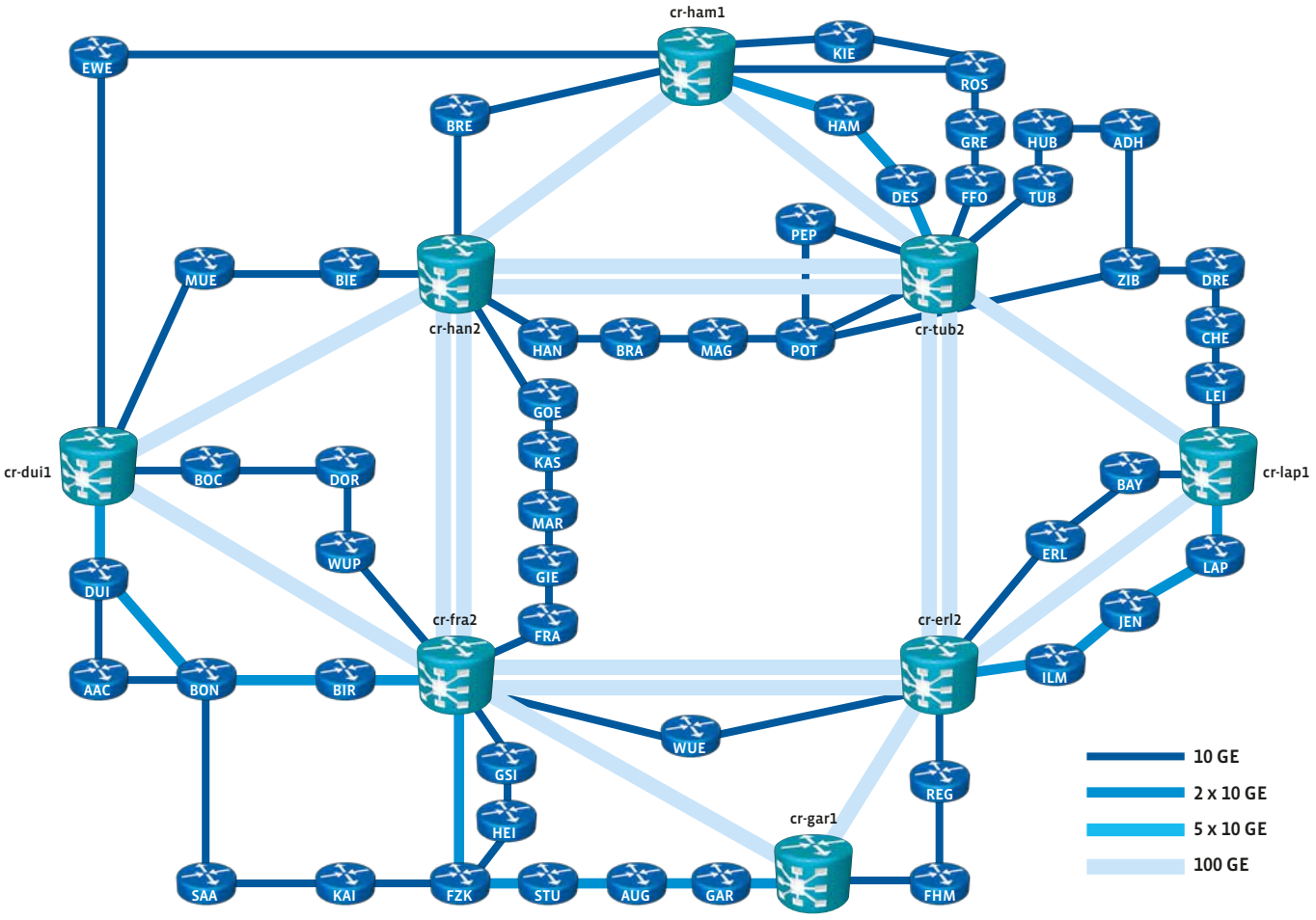


Abbildung 1

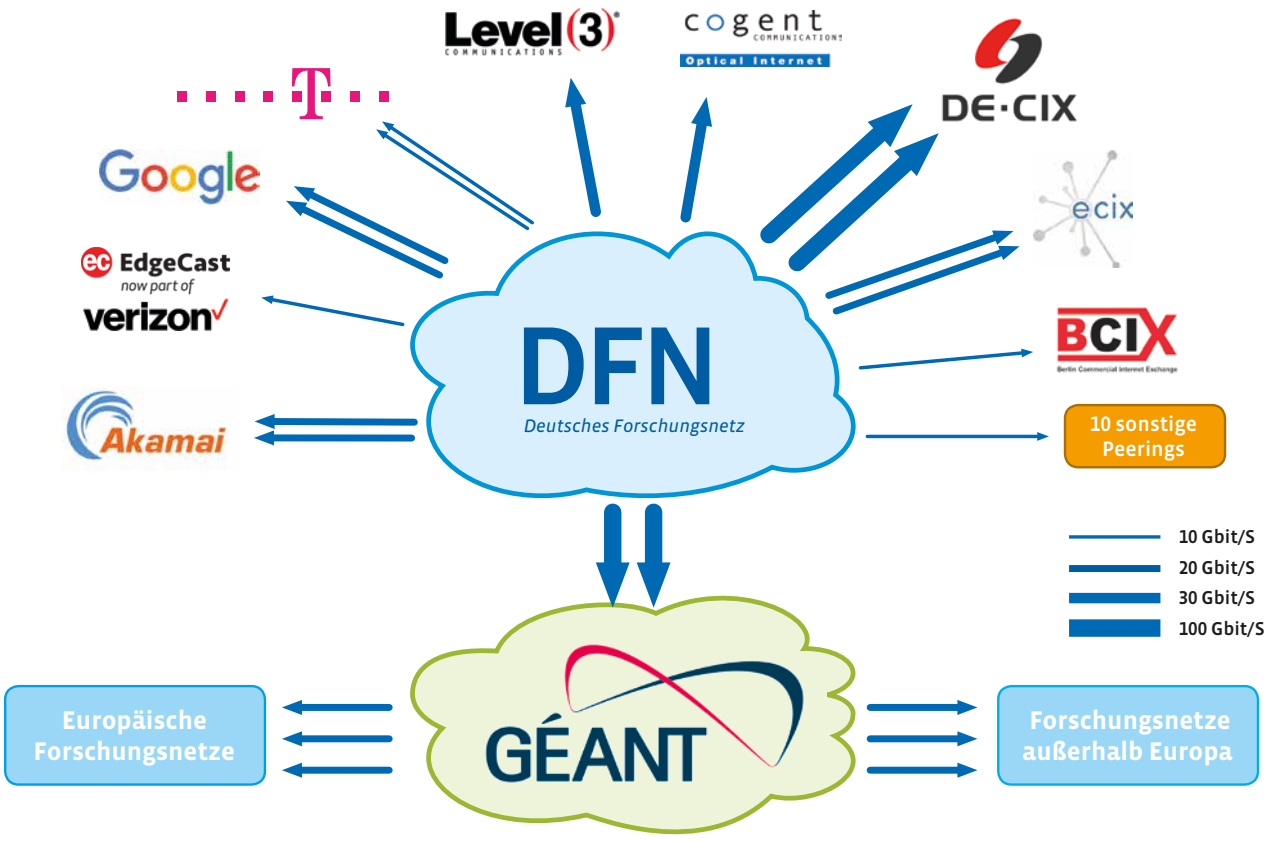


Abbildung 2

der DFN-Verein zwei Ziele. Wie im obigen Abschnitt dargelegt, ist seit etwa einem Jahr ein deutlich erhöhtes Wachstum des Datenvolumens zu beobachten, welches mit hoher Dienstqualität transportiert werden muss.

Gleichzeitig dient aber der Ausbau des SuperCore auch dem Schutz gegen zunehmend häufiger auftretende Distributed Denial-of-Service-Angriffe (DDoS). DDoS-Angriffe treten ohne Vorwarnung auf und laufen in der Regel über die Außenanbindungen (vgl. Abbildung 2) in das X-WiN ein. Die Außenanbindungen des X-WiN werden jedoch zur Gewährleistung einer optimalen Dienstqualität auch in der Kommunikation mit externen Netzen kontinuierlich und bedarfsgerecht ausgebaut, so dass das Problem hochbandbreitiger DDoS-Angriffe praktisch in das X-WiN verlagert wird.

Allein die Erhöhung der Kapazität des SuperCore würde jedoch zur Abwehr von DDoS-Angriffen nicht ausreichen, da die verfügbaren Bandbreiten in Richtung der Teilnehmer erheblich geringer werden. Beim Verlassen des SuperCore stehen heute meist nur noch 10–20 Gbit/s, am Anwenderübergang häufig nur noch wenige Hundert Mbit/s zur Verfügung. Gravierender noch als die Überlastung einer einzelnen Teilnehmeranbindung ist die Überlastung von X-WiN Router-Ketten, da hier viele Teilnehmer gleichzeitig betroffen sind. Diese Überlastungen können dadurch auftreten, dass eine Drosselung des Verkehrs in Richtung von Teilnehmeranbindungen derzeit erst auf dem direkten Übergang zum Teilnehmer stattfindet.

Ausgehend von der skizzierten Problemstellung arbeitet der DFN-Verein derzeit an zwei sich ergänzenden Strategien.

Die erste ist der architektonische Umbau des X-WiN, damit bereits am Übergang vom SuperCore in die Router-Ketten der Verkehr in Richtung eines Teilnehmers auf das ihm zur Verfügung stehende Maximum begrenzt wird. Da dieses Maximum deutlich unterhalb der in der Router-Kette bereitgestellten Gesamtkapazität liegt, wird ein Schutz der in einer Router-Kette terminierten aber nicht direkt durch den DDoS-Angriff adressierten Teilnehmer erreicht.

Die zweite Strategie betrifft die Fähigkeit zur gezielten Filterung von Angriffsverkehr am Übergang zu anderen Netzen. Diese auch als DDoS-Mitigation bezeichnete Funktionalität wurde in 2015 vom DFN-CERT als Erweiterung des bereits im Einsatz befindlichen DDoS-Analyse-Werkzeug DFN-NEMO entwickelt. Mit dieser Erweiterung hat der DFN-Verein die Möglichkeit, exakt spezifizierten Angriffsverkehr direkt auf den Router-Systemen des SuperCore und damit beim Eintritt in das X-WiN in der Bandbreite zu begrenzen bzw. auf dem DDoS-Mitigations-System vollständig auszufiltern.

Zu diesem Zweck kommuniziert das DDoS-Mitigations-System mittels einer BGP-Erweiterung (BGP FlowSpec) welcher Verkehr in der Bandbreite limitiert oder auf das Mitigations-System umgeleitet wird, wo er weiterbehandelt wird. Das Mitigations-System besteht dabei aus einer leistungsfähigen Server-Hardware, die auf Line-Cards in den vier inneren SuperCore-Routern verbaut ist. Nach ersten Tests der produktionsnahen Software geht der DFN-Verein davon aus, dass auch DDoS-Angriffe mit hohen Datenraten effektiv abgewehrt werden können.

Mit den skizzierten Strategien wird ein effektiver Schutz der X-WiN IP-Plattform erreicht. Ein ausführlicher Artikel zum Thema DDoS-Abwehr, in dem auch ein künftiger Dienst für die Teilnehmer vorgestellt wird, folgt in einer der nächsten DFN-Mitteilungen.

Blick in die Glaskugel: Ausblick auf eine neue Aggregations-Plattform für das X-WiN

Nachdem die meisten technischen Plattformen des X-WiN modernisiert sind, verbleiben noch die als X-WiN-Router bzw. als Aggregations-Plattform bezeichneten Systeme aus der ursprünglichen technischen Infrastruktur des X-WiN zur Erneuerung. Diese Router vom Typ Cisco 7609 sind an den meisten X-WiN Kernnetzknoten verbaut und erfüllen seit ihrer Einführung in 2005/2006 die Funktion, IP-Verkehr im X-WiN zu vermitteln, VPN-Strukturen bereitzustellen und Teilnehmeranschlüsse abzuschließen und zu aggregieren.

Seit 2012 ist absehbar, dass diese Systeme keine weitere Produktpflege durch den Hersteller erfahren werden. Des Weiteren kommen die Systeme mit der letzten Leistungssteigerung von DFNInternet in 2013 in Bezug auf ihre technischen Kapazitäten an ihre Grenzen. Der DFN-Verein terminiert daher zunehmend die größeren DFNInternet-Dienste direkt auf den Systemen des SuperCore, die dazu mittels Verbindungen auf der Optischen Plattform zu den Standorten des SuperCore verlängert werden. Parallel dazu plant der DFN-Verein eine Nachfolgeplattform für diese Systeme. Es ist absehbar, dass die für die Teilnehmer bereitgestellten Übertragungskapazitäten weiter steigen werden, so dass diese Systeme eine hohe Anzahl von Gigabit-Ethernet und 10-Gigabit-Ethernet-Schnittstellen bereitstellen können müssen. Auch sind Anbindungen an den SuperCore mit 100-Gigabit-Ethernet perspektivisch erforderlich. Durch neue Kooperationsszenarien zwischen den Teilnehmern werden zudem die bereitzustellenden Funktionalitäten auf Layer-2 und Layer-3 umfangreicher. Während auf IP-Routing mit voller Internet-Routing-Tabelle durch die künftige logische Terminierung von Teilnehmer-Diensten auf den Systemen des SuperCore verzichtet werden kann, werden Layer-2- und Layer-3-VPN sowohl in der Variante Punkt-zu-Punkt als auch Multi-Punkt-zu-Multi-Punkt erforderlich sein. Durch die zunehmende Zahl von Rechenzentrumskopplungen werden Fähigkeiten, wie die VLAN-Trunks der Teilnehmer transparent transportieren zu können, ebenfalls notwendig.

Auch sind die betrieblichen Anforderungen nicht zu vernachlässigen: So muss sich das Management und Monitoring der künftigen Aggregations-Plattform nahtlos in die bestehenden Prozesse der DFN-Geschäftsstelle einfügen. Auch sollen die künftigen Systeme wertvollen, da oftmals knappen Einbauraum an den Kernnetzknoten einsparen und im Vergleich zu den Bestandssystemen mit weniger elektrischer Leistung auskommen. Schließlich müssen die Kosten für Investition und Betrieb für den DFN-Verein tragbar sein.

Fazit

Das X-WiN wird seit 2012 kontinuierlich erneuert. Auch in 2016 und 2017 sind noch bedeutende technologische, wirtschaftliche und betriebliche Weiterentwicklungen notwendig. Insbesondere stellt der Ersatz der heutigen Aggregations-Plattform (X-WiN-Router vom Typ Cisco 7609) sowie der Übergang auf die neuen Teilnehmeranbindungen eine große Herausforderung dar. Diese Arbeiten werden das X-WiN jedoch in ihrem Zusammenwirken auf ein neues Niveau führen und für künftige Herausforderungen ein stabiles Fundament bilden. ◆

Kurzmeldungen

Vergabeverfahren für Teilnehmeranbindungen erfolgreich abgeschlossen

Der DFN-Verein schreibt periodisch die Teilnehmeranbindungen für den DFNInternet-Dienst europaweit neu aus. Ziel dieses Vorgehens ist es, für die Teilnehmer einen kosteneffizienten Dienst mit regelmäßigen Anpassungen der Bandbreiten in den Kategorien des DFNInternet-Dienstes realisieren zu können. Eine weitere Ausschreibung dieser Art wurde von der DFN-Geschäftsstelle in 2014 vorbereitet und im Laufe des Jahres 2015 durchgeführt. Neben Einsparungen bei gleichzeitiger Erhöhung der Übertragungskapazitäten war ein bedeutendes Ziel die Realisierung von redundanten Teilnehmeranbindungen, wo dies gewünscht aber bisher nicht umsetzbar war. Um die Schaffung der dafür notwendigen Infrastruktur für die Bieter im Verfahren wirtschaftlich zu machen, wurde eine lange Laufzeit der Rahmenverträge über sieben Jahre gewählt, so dass sich Investitionen für die Bieter amortisieren können, ohne aber die laufenden Ausgaben für den DFN-Verein zu erhöhen. Als Schutz für die wirtschaftliche Stabilität des DFN-Vereins sind Sonderkündigungsrechte Bestandteil der Rahmenverträge, die bei gravierenden Veränderungen, wie bspw. der Kündigung von DFNInternet-Diensten, durch Teilnehmer greifen.

Alle Anbindungen wurden als Realisierungsoptionen jeweils in der einfachen, und wo vom Anwender gewünscht, auch in der redundanten Variante ausgeschrieben. Zukünftige Leistungssteigerungen wurden dadurch berücksichtigt, dass für jeden Teilnehmer eine Mindestbandbreite und eine Aufrüstbandbreite anzubieten war. Erstere entspricht der heute für den jeweiligen Teilnehmer realisierten Bandbreite, letztere einer in den meisten Fällen um den Faktor 10 erhöhten. So wurden bspw. für einen redundant angebundenen Teilnehmer in der Kategorie I05 (heute 2 x 350 Mbit/s) eine Anbindung mit redundant 1 Gbit/s als Mindestbandbreite und 10 Gbit/s als Aufrüstbandbreite ausgeschrieben.

Nach dem vorgeschalteten Teilnehmerwettbewerb, der auf sehr großes Interesse bei potentiellen Anbietern stieß, fand das Angebotsverfahren im 2. Halbjahr 2015 statt. Die Auswertung der eingegangenen Angebote, die sich im vierstelligen Bereich bewegten, erfolgte im ersten Quartal 2016. Neben der erwarteten Generierung von Einsparpotentialen für die Beauftragung von Teilnehmeranbindungen konnte auch die Anzahl der Carrier mit einem abgeschlossenen Rahmenvertrag deutlich erhöht werden.

Die neuen Anbindungen werden ab dem zweiten Quartal 2016 beauftragt, nachfolgend von den Carriern realisiert und durch den DFN-Verein in Betrieb genommen. ◆

Foto © Nikadat / iStockphoto.de

Brückenschlag zwischen den Ländern der Eastern Partnership (EaP) und der europäischen Forschungsgemeinschaft

EaPConnect, ein EU-gefördertes Projekt zwischen der Eastern Partnership Region (EaP) und dem pan-europäischen Netzwerk GÉANT, berichtet erste Erfolge.

Text: **Leonie Schäfer** (DFN-Verein)

The bridge of peace, Tbilisi, Georgia foto © ET1972/iStockphoto.de

Die Eastern Partnership (EaP) ist eine regionale und multilaterale Initiative zwischen der EU und den sechs EaP-Partnerländern Armenien, Aserbaidschan, Weißrussland, Georgien, Moldawien und der Ukraine. Die Partnerschaft bietet Unterstützung und Hilfe für Reformen in den Bereichen Demokratie, Menschenrechte, Marktwirtschaft, Nachhaltigkeit und e-Infrastruktur.

Das Eastern Partnership Connect Project (EaPConnect) hat zum Ziel, ein regionales High-Speed Netzwerk, ausgerichtet auf Forschung und Bildung aufzubauen, welches die EaP-Länder mit dem europäischen Forschungsnetz GÉANT verbindet. Im Rahmen des Projekts werden die e-Infrastruktur und zugehörige Dienste weiter ausgebaut und die Integration von Studenten und Forschern in den europäischen Forschungsraum durch die Anbindung an das europäische Netzwerk GÉANT gefördert.

Der DFN Verein ist Partner in EaPConnect und unterstützt die EaP-Länder durch die Organisation von Weiterbildungen und im Marketingbereich (z. B. für die Dienste eduroam und eduGAIN).

Zu Beginn des Jahres starteten Georgien und Armenien mit der Bereitstellung von Verbindungen zum GÉANT Netzwerk. GRENA und ASNET-AM sind bereits gut etablierte Forschungsnetze, welche die wichtigsten F&E-Einrichtungen in Georgien und Armenien seit über zwei Jahrzehnten miteinander verbinden. Zwei neue 1G-Links ermöglichen nun über 50 weiteren Universitäten und Forschungseinrichtungen den Beitritt zur GÉANT Community.

Bereits heute arbeiten Mitgliedsinstitute von GRENA und ASNET-AM mit globalen Partnern wie dem CERN, in Bereichen wie Hochenergiephysik, Meteorologie, Klimawandel und Seismologie zusammen. Eine direkte Anbindung an GÉANT wird den Forschern ermöglichen, diese Zusammenarbeit noch zu intensivieren.

Der nächste Arbeitsschritt ist die Anbindung von AzScienceNet, dem aserbaidschanischen NREN, an GÉANT. Hier wurden gerade die Vertragsverhandlungen aufgenommen. Des Weiteren ist eine Ausschreibung in Vorbereitung, die darauf zielt, das weißrussische NREN UIIP NASB an das pan-europäische Netzwerk anzubinden.

Bis zum Jahr 2016 wird erwartet, dass die Länder der Eastern Partnership komplett an GÉANT angebunden sind. Für die europäische Forschungsgemeinschaft stellt diese Erweiterung eine willkommene Ergänzung ihrer Expertise u. a. in den Bereichen Physik, Klimawandel, Katastrophenbekämpfung und Life Sciences dar. ◆

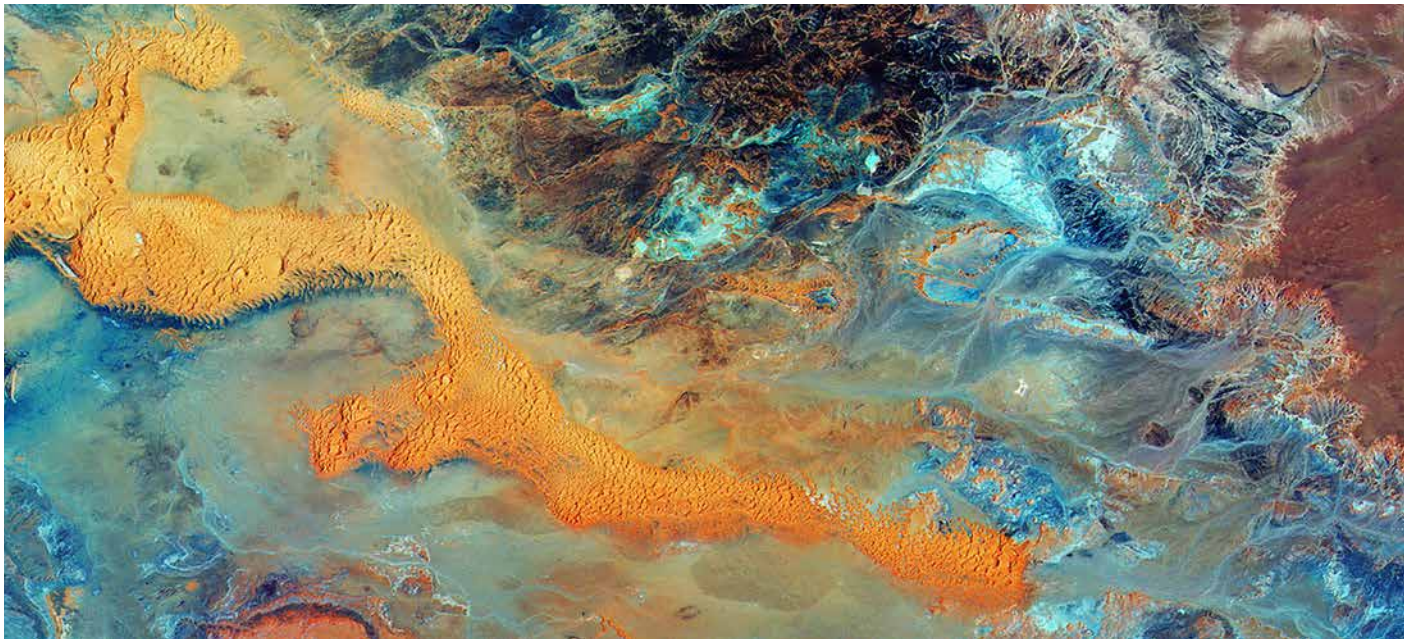
Yerevan and Mont Ararat, Armenia © marlenka/iStockphoto.de

Europas Blick auf die Erde

Wie die Wissenschaftsnetze das Copernicus Programm unterstützen

Copernicus ist ein über mehrere Jahrzehnte angelegtes Erdbeobachtungsprogramm, welches von der Europäischen Kommission (EC) ins Leben gerufen wurde. Ziel ist die systematische Erdbeobachtung durch satellitengestützte Fernerkundung sowie der Aufbau von boden- und seegestützen Beobachtungs-Infrastrukturen.

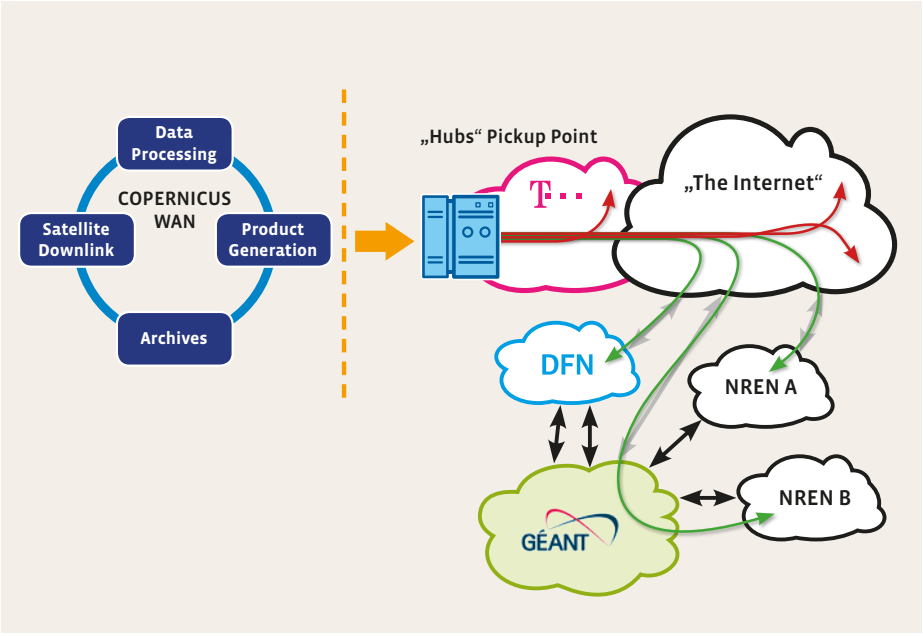
Text: **Dr. Jakob Tendel** (DFN-Verein)

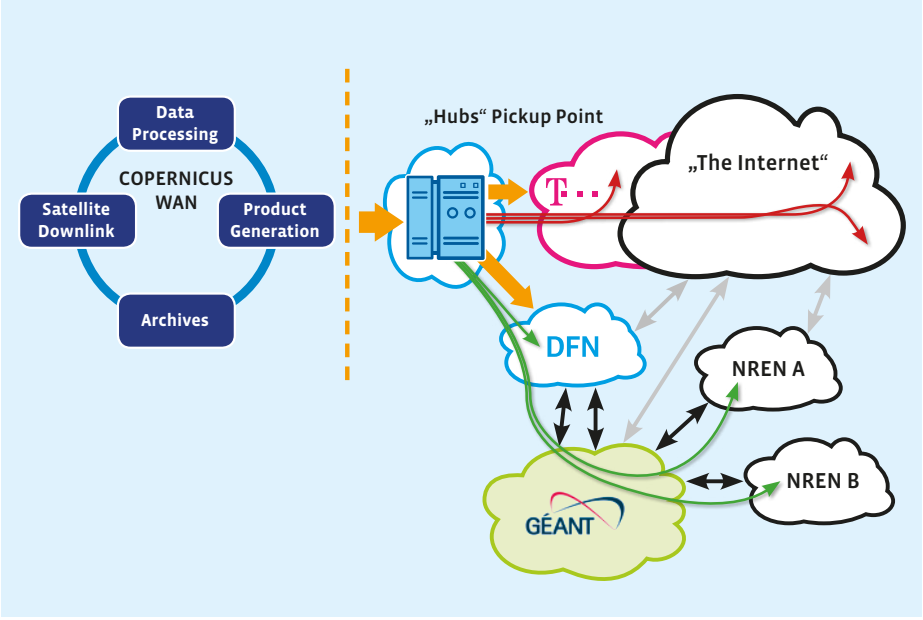


Echtfarb- und Strukturaufnahme der libyschen Wüste, aufgenommen von der Satellit Sentinel 2. Foto © ESA/ATG Medialab

Copernicus schafft eine moderne und leistungsfähige Infrastruktur für die Erdbeobachtung und darauf aufbauende Dienstleistungen aus dem Bereich der Geoinformation. Die gewonnenen Informationen werden nicht nur der Wissenschaft zugänglich gemacht, sie haben auch einen wirtschaftlichen und gesellschaftlichen Nutzen. So werden Entscheider der Politik, z. B. aus dem Bereich Landwirtschaftsplanung oder Katastrophenschutz, mit einer breiten Palette aktueller Beobachtungsdaten versorgt. Um die Zugänglichkeit der Daten und den daraus resultierenden volkswirtschaftlichen Nutzen zu maximieren, hat die EC die freie und kostenlose Verfügbarkeit der Daten zum zentralen Element des Vorhabens erklärt und dafür die Bereitstellung der Daten mittels allgemein verfügbarer Internet-Technologie realisiert.

Um den wissenschaftlichen Nutzern der Copernicus Daten weltweit einen optimalen Zugang zu den Daten zu ermöglichen, wurde ein direkter Zugang von der Daten-Infrastruktur der ESA zum GÉANT Netz realisiert. Von dort können die Daten zu den angeschlossenen Wissenschaftsnetzen übertragen werden. Diese Lösung erlaubt die Nutzung der dedizierten Infrastruktur der Forschungsnetze, zu denen der Großteil der





wissenschaftlichen Nutzer bereits Zugang hat. Außerdem wird dadurch eine potenziell kostenintensive Auslastung der kommerziellen Peerings einzelner Wissenschaftsnetze vermieden. Die Datenquelle der ESA befindet sich in Frankfurt a.M., somit ist der DFN als nationales Forschungsnetz für die Herstellung des GÉANT Anschlusses verantwortlich.

Entstehung

Copernicus, zuvor Global Monitoring for Environment and Security (GMES, deutsch: Globale Umwelt- und Sicherheitsüberwachung) genannt, wurde im Jahre 1998 gemeinsam von der Europäischen Kommission (EC) und der Europäischen Weltraumorganisation (ESA) gegründet.

Ziel des Programms ist es nicht nur vereinzelt auftretende, für die Forschung relevante Phänomene zu untersuchen, sondern die zeitliche Entwicklung des gesamten Erde-Atmosphäre-Ozean Systems viel besser laufend zu erfassen. Die daraus gewonnenen Daten sind für eine breite Zielgruppe von Relevanz. Neben Wissenschaften und Wettervorhersagen stellen die Informationen einen großen Nutzen für viele weitere Bereiche dar. Die durch Copernicus gewonnenen Informationen reichen von zeitlich und räumlich hoch aufgelösten Erfassungen der Vegetation, über die genaue Lage von Gewässern inklusive Wasserpegel, bis hin zu präzisen Messungen der atmosphärischen Zusammensetzung. Diese Vielfalt an Datenprodukten zusammen mit ihrer langjährigen planbaren Verfügbarkeit erlaubt es Nutzern von Regierungsbehörden bis zu kleinen Unternehmen neue, von zuverlässigeren Messungen unterstütze Entscheidungsprozesse zu entwickeln.

Innerhalb von Copernicus produzieren die Sentinel Satelliten die größten Datenmengen. Jede Reihe der Satelliten (Sentinel 1-6) ist mit eigenen Sensoren ausgestattet und untersucht andere Themenschwerpunkte. Zur Absicherung bei Ausfällen sollen sich mittelfristig jeweils mehrere identische Exemplare (z. B. 1A, 1B, 1C) zusammen im Orbit befinden, was auch eine häufigere Abtastung jeder Stelle auf der Erdoberfläche gewährleistet. Sentinels -1 bis -3 (siehe Informationskasten) und -5p sind jeweils eigenständige Satellitentypen, die weiteren Sentinels sind Sensorgruppen auf anderen Satellitenplattformen. Der erste Satellit, Sentinel 1A, startete 2014, gefolgt von Sentinel 2A 2015 und Sentinel 3A Anfang 2016. Im Laufe dieses Jahres sollen noch die Sentinels -1B, -5p, und -2B in ihre Umlaufbahn gebracht werden.

Die Sentinels erzeugen jeweils beträchtliche Datenströme (Terrabytes pro Tag), welche als sogenannte „Level 1“ Datenprodukte verfügbar gemacht werden. Aus diesen Sensor-Rohdaten werden thematisch gegliedert weiterführende „Level 2“ Datenprodukte erzeugt. Diese Copernicus Diens-

Sentinel 1
Hochauflösendes Radar
Schwerpunkt: Topografie
Sentinel-1A seit April 2014
Sentinel-1B ab April 2016

Sentinel 2
Hochauflösende Farbbilder
Schwerpunkt: Vegetation
Sentinel-2A seit Juni 2015
Sentinel-2B ab Herbst 2016

Sentinel 3
Farbbilder, Mikrowellen, Radar
Schwerpunkt: Meeresoberfläche
Sentinel-3A seit Februar 2016
Sentinel-3B ab 2017

te werden jeweils federführend von einer europäischen Einrichtung entwickelt (siehe Tabelle Seite 23 unten).

Verbindung zu den Wissenschaftsnetzen

Die Anbindung des Copernicus Datacenters der ESA an die Wissenschaftsnetze ist Ergebnis eines seit 2013 geführten Dialogs zwischen der ESA und den Wissenschaftsnetzen, vertreten durch GÉANT und den DFN. Die EUMETSAT (die Europäische Organisation für die Nutzung meteorologischer Satelliten) ist ebenfalls für die Erstellung und Verbreitung eines Teils der Copernicus Daten zuständig, nutzt dafür jedoch ihre eigene technische Infrastruktur, welche bereits an die Wissenschaftsnetze angebunden ist. Der DFN ist für die Anbindung sowohl der ESA als auch der EUMETSAT an die Wissenschaftsnetze erster Anlaufpunkt, da sich die Copernicus Datacenter beider Einrichtungen im Raum Frankfurt a.M. befinden.

Um die Verbindung der ESA Infrastruktur zum X-WiN herzustellen, wurde zusammen mit GÉANT die Einrichtung eines DFNInternet-Dienstes nach Kategorie I11 (1x10Gbit/s) für den Standort vereinbart. Neben der Erreichbarkeit aus dem X-WiN erlaubt dieser Dienst auch die Mitnutzung der GÉANT Anbindungen des DFN zur Versorgung von Teilnehmern aller an GÉANT angebundenen Wissenschaftsnetze. Da die von Anfang an bestehende Anbindung des ESA Datacenters an einen kommerziellen Internet-Provider bestehen bleibt, mussten im Interesse einer stabilen Routenfindung einige Anpassungen an der Netzwerk-Konfiguration vorgenommen werden. Damit die Datenströme bereits am Ursprung zuverlässig anhand der IP-Adresse des abrufenden Endnutzers dem zu nutzenden Übertragungsweg (kommerzielles Internet, Wissenschaftsnetze) zuzuordnen sind, wird die Datenquelle in einem eigenen public-AS („Autonomous System“) liegen, welches mit den verfügbaren Verteilernetzen gleichberechtigte Peerings unterhält. So kann die Routing-Funktion des Ursprungs-Systems standardkonform per BGP Protokoll die über die Verteilernetze jeweils erreichbaren Endnutzer unterscheiden und es ist im Falle einer Dienstunterbrechung auf einem der zwei Verteilernetze eine Umleitung des Verkehrs über die andere Anbindung möglich. Die Vorbereitungsphase für dieses Vorhaben ist mit der Vertragsunterzeichnung Ende 2015 abgeschlossen, die Bereitstellung durch den DFN erfolgte im April 2016. ◆

Landüberwachung →	Europäische Umweltbehörde EEA
Überwachung der Meeresumwelt →	Mercator Ocean
Katastrophen- und Krisenmanagement →	Europäische Kommission
Überwachung der Atmosphäre →	ECMWF
Überwachung des Klimawandels →	ECMWF

Der neue GÉANT Testbeds Service

Seit April 2013 entwickelt das europäische Wissenschaftsnetz GÉANT den GÉANT Testbeds Service (GTS). Dieser Service stellt den Benutzern individuelle Testbedumgebungen für experimentelle Untersuchungen neuer Netztechnik zur Verfügung. Die GTS-Architektur bietet dafür eine wissenschaftliche Plattform mit voneinander isolierten virtuellen Netzen für die Forschungs- und Wissenschaftscommunity in Europa. Nutzer können sich virtuelle Ressourcen (Rechnerkapazität, Speicherplatz, Routingkapazitäten, usw.) und virtuelle Netzstrukturen zusammenstellen und damit ein eigenes Netz erzeugen.

Text: **Dr. Peter Kaufmann** (DFN-Verein), **Dr.-Ing. Susanne Naegele-Jackson** (Regionales Rechenzentrum Erlangen)

Foto © Liufuyu/iStockphoto.de

Einleitung

Derzeit stellt das GÉANT-GTS eine Netzdomain dar. Diese wird durch eigene NREN-GTS-Domains ergänzt und zu einem Multi-Domain-GTS (MD-GTS) ausgebaut. Dies ermöglicht den Nutzern den Zugang zu Ressourcen, deren Verfügbarkeit im eigenen NREN eingeschränkt ist.

Durch die Multi-Domain-Fähigkeit des GTS ist es möglich, dass ein Benutzer sich z. B. am zukünftigen DFN-GTS anmeldet und dort Ressourcen bucht, die dann aber von anderen GTS-Anbietern zur Verfügung gestellt werden, falls zur Zeit der Reservierung diese gewünschten Ressourcen nicht im DFN-GTS vorrätig sind.

Darüber hinaus ist GTS auch grundsätzlich mit anderen Domains oder Testbeds interoperabel, die keinen MD-GTS-Service zur Verfügung stellen. Um z. B. ein Labor, einen Tagungsort oder eine Projekteinrichtung an GTS anzubinden, ist es möglich, in der gewünschten Topologiebeschreibung des Virtuellen Netzes ein „Externes Interface“ zu definieren. Zu diesem Interface kann dann ein Tunnel vom Labor o. Ä. eingerichtet werden.

Teil 1 dieses Artikels erklärt die Eigenschaften von Software Defined Networks (SDN) und gibt eine Beschreibung des GÉANT-GTS. Im zweiten Teil, welcher in der nächsten Ausgabe der DFN-Mitteilungen zu finden sein wird, werden die technischen Details der GTS-Infrastruktur und die geplante DFN-GTS-Domain beschrieben.

Was ist SDN?

Der Einsatz von virtuellen Maschinen statt eigener Hardware ist in der Serverwelt für die unterschiedlichsten Anwendungen schon lange Realität. Dadurch lassen sich Anwendungen mit geringerem Kosten- und Arbeitsaufwand flexibler bedienen und unterstützten. Diese Vorteile sollen nun auch im Netzbereich genutzt werden. Ein Datennetz wird nicht mehr nur als physische Infrastruktur auf einer Ebene verstanden. Dazu ist es notwendig, mit Hilfe einer Software das Netz programmierbar zu machen, d. h. es muss der Datenverkehr (DataPlane) vom Kontrollverkehr (ControlPlane) getrennt werden, so dass über der physischen Netzinfrastruktur viele virtuelle Netze für unterschiedlichste Anwendungen aufgebaut werden können.

Seit einigen Jahren werden virtuelle Netze unter dem Begriff von Software-Defined-Networks (SDN) entwickelt und in vielen Umgebungen erprobt. Virtuelle Netze werden auf den physischen Netzen aufgesetzt und stellen eigene abgeschlossene

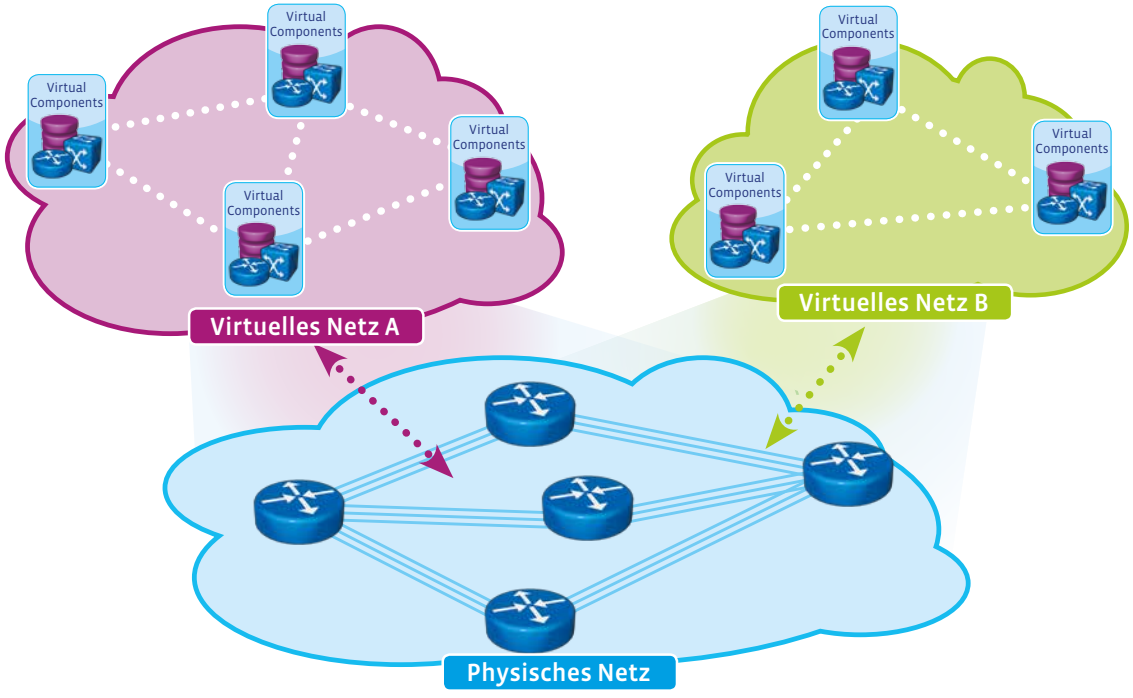


Abbildung 1: Zwei Virtuelle Netze (SDN) auf dem physischen Netz

Netzumgebungen zur Verfügung. Frühe Beispiele für solche Testbeds waren die Projekte FEDERICA und NOVI (siehe dazu [1] , [2]).

In virtuellen Netzen sind sowohl die Netzverbindungen als auch die Hardware (Router, Switches, Rechner, usw.) virtualisiert (Abbildung 1), also nicht mehr allein nur die Netzverbindungen, wie im Bereich der VLAN-Konzepte üblich. Die vollständige Virtualisierung aller Netzbestandteile ermöglicht den Aufbau und das Management eigener Teilnetze durch die Nutzer. Im Rahmen der vom Betreiber des physischen Netzes bereitgestellten Ressourcen (Verbindungen mit Bandbreiten, Routing-/Switchingkapazitäten, Computerserver, usw.) kann ein Nutzer sich ein eigenes Netz mit Strukturen, Routingmechanismen und Kapazitäten aufbauen.

Der Anreiz für die Umsetzung virtueller Netze liegt in der effektiven Verwendung aller Ressourcen (Netzkapazitäten, Rechner, Netzequipment) durch eine dynamische Nutzung (dynamisches asynchrones Multiplexing), welche bereits aus dem Cloudcomputing bekannt ist. Die flexible, dynamische Umsetzung dieser Anforderungen kann nur mittels Software gelingen, im Unterschied zu Hardware/Firmware-Lösungen. In der Startphase der Netzvirtualisierung waren die Softwarelösungen vor allem als flexible und schnell konfigurierbare Testbeds für experimentelle Netztechnikuntersuchungen gedacht. Mit der wachsenden Stabilität der virtuellen Netze werden sie aber auch für den operativen Produktionseinsatz immer interessanter.

Für durch Software definierte virtuelle Netze werden offene, standardisierte Interfaces zu Routing/Flow-Tables in den Netzkomponenten benötigt. Dadurch können Software/Controller auf einem Server die Interfaces ansprechen und den Verkehrsfluss je nach Anwendung und Policy steuern. Viele Hersteller bieten inzwischen (teilweise unterschiedliche) SDN Lösungen und Controller Software an. Dabei ist das „Software-Defined“ nicht wirklich neu, denn schon „immer“ werden Netze mittels proprietärer Betriebssystem-Software auf Routern und Switches konfiguriert, überwacht und gesteuert. Insofern kann jeder Hersteller ohne viele Verrenkungen diese Fähigkeit abstrakt für sich beanspruchen. Die neue Qualität einer SDN-Umgebung zeigt sich vor allem darin, dass die Betreiber (und die Nutzer) eines SDN einfache aber mächtige und herstellerunabhängige Kontrollmöglichkeiten zum Betrieb eines eigenen SDN in die Hand bekommen.

Die Herausforderung besteht insgesamt darin, die herstellerspezifischen Kontroll- und Managementlösungen effektiv in offene Lösungen zu überführen.

Eine solche SDN-basierte Lösung sollte flexibel auf neue und zukünftige Ressourcen und Technologien erweiterbar sein. Die Trennung in DataPlane und ControlPlane ist dafür eine wichtige Voraussetzung.

Das prominenteste Beispiel für eine Umsetzung von SDN stellt wohl das in Stanford entwickelte OpenFlow-Konzept dar, wel-

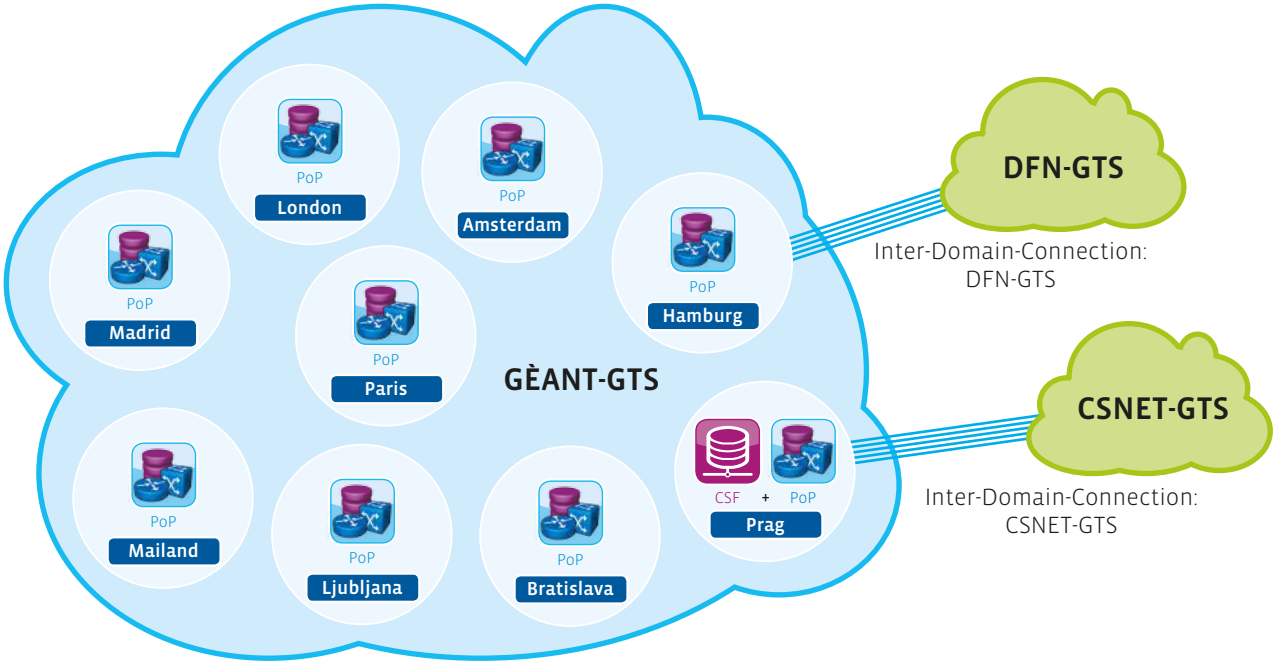


Abbildung 2: Struktur der GÉANT-GTS-Domain mit ausgewählten NREN-Erweiterungen (siehe Teil 2 des Artikels).

ches in diversen Hardwareumgebungen bereits implementiert ist. Auch im GÉANT-GTS stehen OpenFlow Hardware-Switches zur Verfügung, die in individuellen Testbedumgebungen eingesetzt werden können.

Beschreibung des GÉANT-GTS

Seit April 2013 wird der neue GÉANT Service – GTS (GÉANT Testbeds Service, [3], [4], [5], [6]) entwickelt. Dieser Service (http://services.geant.net/gts/) stellt den Benutzern individuelle Testbedumgebungen zur Verfügung. Das Besondere an diesem Service ist, dass diese Testbeds mit Hilfe eines automatischen Provisionierungssytems in Sekundenschnelle vom Benutzer selbst zusammengestellt und aufgebaut werden können. Jedes Testbed ist dabei von anderen Testbeds völlig isoliert, sodass auch kritische und unerprobte Neuanwendungen problemlos im Experiment durchgeführt werden können, ohne dass Beeinträchtigungen von anderen Benutzern befürchtet werden müssen. Genau das ist die Stärke und Besonderheit dieses neuen Service: Er ermöglicht flexibles Experimentieren, das auch ein Anpassen der zugrunde liegenden Netztopologie erlaubt. Eine weitere Besonderheit von GTS ist, dass diese automatisch provisionierten virtuellen Testbeds – im Gegensatz zu einer Simulation – Anteile der physischen Infrastruktur buchen können und der Wissenschaftler so über ein reales Netz seine Forschung betreiben und realistische Aussagen für das Netzverhalten und den Netzverkehr treffen kann. Da die im GÉANT zur Verfügung stehende physische Infrastruktur über ganz Europa verteilt ist (siehe Abbildung 4) sind auch Tests im Wide Area Network Bereich möglich.

Um ein Testbed in GTS aufzubauen, beschreibt ein Benutzer zunächst, wie das Testbed genau aussehen und welche Ressourcen es enthalten soll. Dies geschieht mit Hilfe eines Dokumentes, welches über ein Web-Interface hochgeladen werden kann. Dort nimmt ein Ressourcen-Manager das Dokument in Empfang, prüft es auf Syntax und Verfügbarkeit bezüglich der geforderten Ressourcen und stellt dann dem Benutzer im Falle einer positiven Bewertung des Dokumentes die Ressourcen-Kennungen der Testbed-Komponenten zur Verfügung, sodass der Benutzer diese Ressourcen kontrollieren kann und in seinem Testbed damit arbeiten kann.

Das oben genannte Dokument für die Beschreibung eines Testbeds enthält Domain Specific Language (DSL) Code, der auf Groovy (einer Objekt-orientierten Sprache für die Java-Plattform) basiert. Für fortgeschrittene Benutzer hat dies den Vorteil, dass mit Schleifenbildung schnell und unkompliziert sehr komplexe und große Netze konstruiert werden können. Um den Einstieg zu erleichtern, ist geplant, in Zukunft auch ein „Drag&Drop“ basiertes, graphisches User Interface (GUI) zur Verfügung zu stellen, in dem durch Anklicken auf und Ziehen von Icons Testbeds entworfen und Ressourcen verbunden werden können. Der DSL Code wird dabei automatisch im Hintergrund generiert. Ein Prototyp für dieses erweiterte „jFED-GUI“ wurde bereits von iMinds (http://jfed.iminds.be/) entwickelt und wird im Laufe des Jahres 2016 zum Einsatz kommen. Derzeit können in GTS virtuelle Maschinen (VMs), virtuelle Links (VCs) und OpenFlow Instanzen als Netzressourcen im Testbed reserviert, aktiviert, deaktiviert und wieder frei gegeben werden. Die Architektur von GTS ist aber skalierbar und kann jederzeit mit neuen Ressourcen erweitert werden. Dazu ist es nur notwendig, fünf Kontrollmodule für die neue Ressource zu entwickeln, d. h. die neue Ressource muss wie oben beschrieben (1) reserviert, (2) aktiviert, (3) deaktiviert und (4) freigegeben werden können; des Weiteren muss eine (5) Statusabfrage möglich sein. Dadurch sind beliebige Arten von Ressourcen integrierbar, denkbar wären z. B. auch Ressourcen wie öffentliche IP-Adressen, Zeitstempel oder LTE-Komponenten, usw. Außer den bereits angebotenen Ressourcen werden in Kürze auch Hardware/Bare Metal Servers (BMS), virtuelle Maschinen mit mehr RAM/CPU Leistung oder OS-Flavors im GÉANT Testbeds Service zur Verfügung stehen. Damit ist GTS eine Beispielarchitektur für isolierte virtuelle Netze, die automatisch provisioniert werden können und die beliebige Ressourcen verfügbar machen können.

Durch diese Flexibilität bezüglich Netzprovisionierung kann ein GTS Testbed auch jederzeit so konstruiert werden, dass z. B. Laboreinrichtungen von zwei oder mehreren wissenschaftlichen Instituten und Partnern über ein GTS Testbed miteinander verschaltet werden: Das GTS Testbed fungiert in diesem Fall nicht nur als Verbindungsstruktur zwischen den Laboreinrichtungen, sondern kann auch zusätzliche Ressourcen einbinden. Um eine solche Koppelung an ein GTS Testbed nach außen zu vereinfachen, wurde als weitere Ressource ein „External Domain Interface“ entwickelt. Damit kann bereits im DSL Code der Anbindungspunkt nach außen beschrieben werden (siehe Abbildung 3).

```
ExternalDomain {
id = "ex1"
location = "prg"
port { id = "ep1"
}
```

Abbildung 3: DSL code für die Anbindung externer Domains

Die Anbindung von GTS an eine Partnereinrichtung muss jedoch derzeit noch vom GÉANT NOC manuell geschaltet werden. In der Praxis hat sich gezeigt, dass diese Möglichkeit besonders auch für Demos auf Konferenzen und Tagungen interessant ist, weil der Tagungsort somit leicht in bereits bestehende Testumgebungen mit eingeschlossen und angebunden werden kann. Vorgeführt wurde dies bereits auf der Super Computing Conference SC14

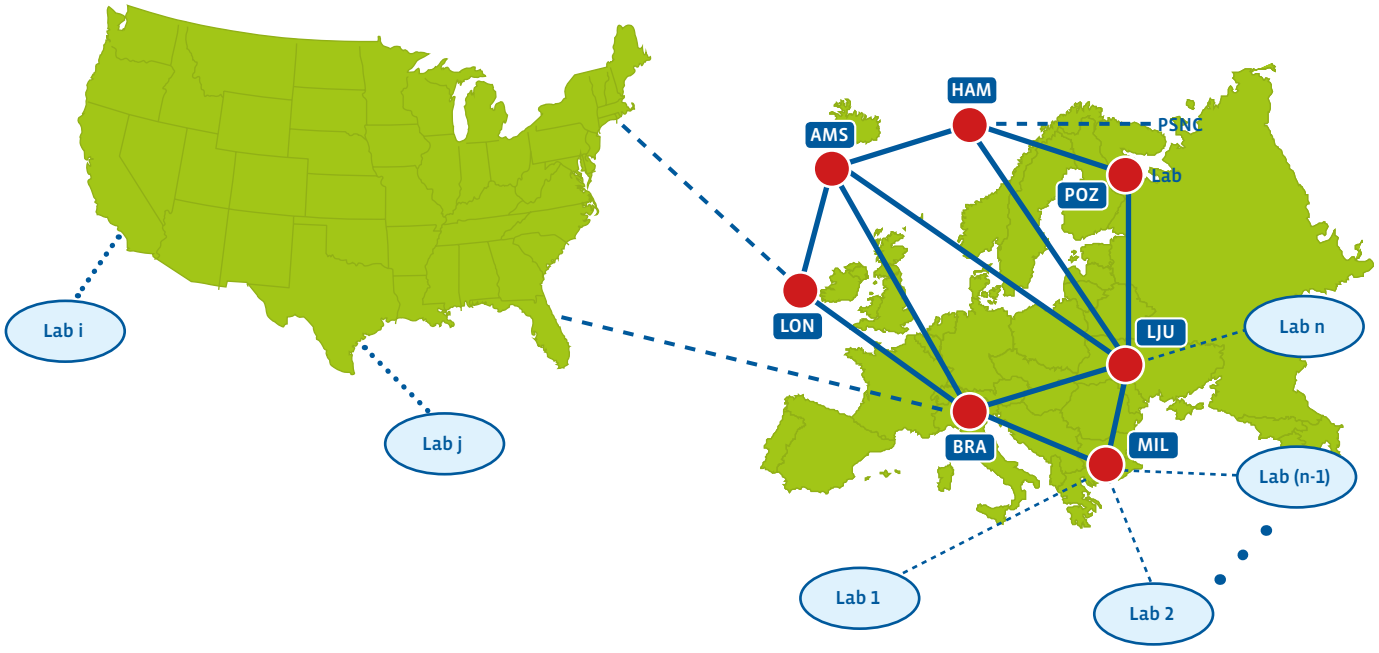


Abbildung 4: Der GÉANT GTS als Vermittlungsstruktur zwischen Laboratorien und anderen SDN-Testbeds (hier: USA).

in New Orleans, auf der ONS (Open Networking Summit) 2015 in San José und der ONS 2016 in Santa Clara. Durch diese Funktion dient das GÉANT-GTS als Software Defined Exchange (SDX), also als software-basierte Vermittlungszentrale (siehe Abbildung 4), die zusätzliche Netzressourcen zur Verfügung stellen kann.

Obwohl GÉANT-GTS OpenFlow-Testbeds ermöglicht, ist der Service selbst nicht OpenFlow basiert. Die Software, die den Service steuert, ist nicht proprietär, sondern setzt auf Standardtechnologien wie OpenStack und NSI. Auch die Service-Architektur ist herstellerunabhängig, was die zum Einsatz kommende Hardware betrifft.

Der GÉANT-GTS wird gegenwärtig durch neun GÉANT-GTS-PoPs in Amsterdam, Prag, Ljubjana, Bratislava, London, Mailand, Paris, Madrid und Hamburg bereitgestellt (siehe Abbildung 2). Die GÉANT-GTS-PoPs sind mit 10-Gb-Kanälen untereinander vollvermascht.

Neben den PoPs muss in jeder Domain eine Managementumgebung (Central Server Facility, CSF) für die Netzbetreiber und die Nutzer installiert werden. Sie besteht aus drei Servern (CSF0, CSF1, CSF2) mit speziellen Funktionen.

Beide technischen Umgebungen (PoPs und CSF) werden zusammen mit der geplanten DFN-GTS-Domain im zweiten Teil des Artikels beschrieben. ◆

References

[1] Peter Kaufmann, The FEDERICA virtual environment testbed, DFN-Mitteilungen Nr. 76, Mai 2009
[2] Susanne Naegele-Jackson, Peter Kaufmann, NOVI:Virtuelle Netze koppeln, DFN-Mitteilungen Nr. 82, Mai 2012
[3] GTS services.geant.net/gts
[4] M. Hazlinsky, B. Pietrzak, P. Szegedi, F. Farina, J. Sobieski, SDNI: The GÉANT Testbeds Service – Virtual Network Environments for Advanced Network and Applications Research, Science and Technology Conference (Modern Networking Technologies) (MoNeTeC), 2014 International, IEEE, Moscow, Russia, 28-29 Oct. 2014, p. 62-67, ISBN: 978-1-4799-7593-8, DOI: 10.1109/MoNeTeC.2014.6995585, available from http://sdiconf.com/files/SDI_Proceedings_2014.pdf
[5] Jerry Sobieski, Susanne Naegele-Jackson, Blazej Pietrzak, Michal Hazlinsky, Fabio Farina and Kim Kramaric, GÉANT Testbeds Service (GTS) - GÉANT Testbed Service - External Domain Ports: A demo on multiple domain connectivity, European Workshop on Software Defined Networks (EWSDN), Bilbao, Sept. 30 - Oct. 2, 2015
[6] Jerry Sobieski, Susanne Naegele-Jackson, Blazej Pietrzak, Michal Hazlinsky, Peter Szegedi and Fabio Farina, GÉANT Testbeds Service - Virtual Network Environments for Advanced Network Research, TERENA Networking Conference TNC15, Porto, Portugal, June 14-18, 2015, https://tnc15.terena.org/core/poster/4

Kurzmeldungen

Intensivierung der Zusammenarbeit zwischen GÉANT und dem indischen Forschungsnetz NKN

Die Region Asien-Pazifik bildet einen der Schwerpunkte der Zusammenarbeit des DFN mit dem europäischen Netzwerk GÉANT im Bereich International Business Development. Thema hier ist vor allem die Intensivierung der bestehenden Verbindungen als Basis für Kooperationen zwischen Forschungseinrichtungen in Europa und Ländern der Asien-Pazifik Region.

Asien stellt nicht nur über 60% der Weltbevölkerung dar und beinhaltet 1/3 der Landmasse der Erde, die Region verfügt außerdem über das zweitgrößte regionale Bruttoinlandsprodukt (GDP). Etwa 1,6 Milliarden Asiaten hatten bis Ende 2014 ein Mobiltelefon und etwa 3 Milliarden nutzen das Internet. So besitzt z. B. Indien, als einer der BRICS-Staaten, ein großes Potential im Forschungsbereich.

In Horizon 2020, dem aktuellen europäischen Forschungsrahmenprogramm, ist Indien als Partner anerkannt, erhält jedoch keine Fördergelder im Rahmen von Kooperationsprojekten. Dadurch sank die Beteiligung indischer Partner an Forschungsprojekten im Vergleich zum vorhergehenden Rahmenprogramm FP7 drastisch. Momentan besteht keine nennenswerte Beteiligung indischer Partner an europäischen Forschungsprojekten. Es existiert jedoch eine deutsche Initiative in Form des Indo-German Science und Technology Centres (IGSTC), welches jährlich Ausschreibungen für Kooperationsprojekte durchführt und Fördergelder bereitstellt. Das IGSTC (**) wird gefördert durch das Bundesministerium für Bildung und Forschung (BMBF) und dem Indischen Department of Science und Technology (DST).

Indien ist durch zwei NRENs in der Forschungsnetz-Community vertreten, dem National Knowledge Network (NKN) und dem India Education and Research Network (ERNET).

Bei der jährlich stattfindenden Konferenz des indischen NRENs National Knowledge Network (NKN) im Januar diesen Jahres, präsentierte DFN-Mitarbeiterin Léonie Schäfer das europäische Netzwerk GÉANT, sowie den aktuellen Stand der Kooperationen zwischen GÉANT und NKN. Die Konferenz fand vom 21.–22. Januar in Hyderabad im indischen Bundesland Telangana statt.

Das bereits 1986 gegründete indische ERNET betreibt ein terrestrisches und ein satellitengestütztes Netzwerk für ganz Indien und ist u. a. Anbieter für eduroam. Das NKN wurde 2010 von der indischen Regierung durch das Cabinet Committee on Infrastructure (CCI) gegründet. Es betreibt ein 10G-Backbone und vernetzt ca. 4 Millionen Nutzer an über 1500 Standorten miteinander. Bis zur Gründung von NKN arbeitete GÉANT ausschließlich mit ERNET zusammen. Jedoch soll nun, nach den Plänen der indischen Regierung, das seit 2010 bestehende Forschungsnetz NKN das kleinere ERNET übernehmen und damit zum alleinigen Forschungsnetz für Indien werden.

Die Konnektivität von NKN zu GÉANT besteht aktuell durch eine 2,5 Gbit/s Verbindung über TEIN4(*), welche in Kürze auf 10 Gbit/s ausgebaut werden soll, um den internationalen Standard zu halten.

In Vorbereitung sind des Weiteren 2 x 5 Gbit/s Verbindungen zu GÉANT über Netherlight in Amsterdam. Ein Memorandum of Understanding über die Grundsätze der Zusammenarbeit von NKN mit GÉANT ist in Vorbereitung.

Der DFN wird über GÉANT seine Kontakte zu NKN weiter intensivieren und bestehende, sowie zukünftige Kooperationsprojekte zwischen DFN-Mitgliedern und indischen Partnern gerne unterstützen. ◆

(*) Trans-Eurasia Information Network (TEIN) – www.tein.net
(**) IGSTC http://www.igstc.org/

Neuer Vorstand der GÉANT Association gewählt

Die Mitgliederversammlung der GÉANT Association hat auf ihrem 6. Treffen am 26. November 2015 in Luxemburg einen neuen Vorstand gewählt. Repräsentanten von 36 europäischen Forschungsnetzen wählten DFN-Geschäftsführer Christian Grimm zum neuen Vorstandsvorsitzenden der GÉANT Association für die kommenden drei Jahre. Zu den neuen Mitgliedern des Vorstandes wurden Erik Huizer von SurfNET, Valter Nordh vom schwedischen SUNET sowie Raimundas Tuminauskas vom litauischen LITNET gewählt. Da ihre Amtszeit noch ein weiteres Jahr oder mehr beträgt, verbleiben Sabine Jaume-Rajaonia vom französischen Forschungsnetz RENATER, Ivan Maric vom kroatischen CARNet, Marko Bonač vom slowenischen ARNES, Alberto Pérez Gomez vom spanischen RedIRIS sowie Dorte Olesen aus Dänemark als Mitglieder des Vorstandes im Amt. ◆

Sieben Jahre DNSSEC in der Praxis – ein Erfahrungsbericht

Das Leibniz-Rechenzentrum setzt DNSSEC mit validierenden Resolvern seit 2008 im Münchner Wissenschaftsnetz (MWN) ein, seit 2010 werden eigene Domains auch aktiv signiert. Dieser Artikel fasst die gewonnenen praktischen Erfahrungen zusammen, zeigt die erst durch DNSSEC ermöglichten funktionalen Neuerungen für SSH- und E-Mail-Server auf und gibt einige Tipps, was bei der Umsetzung beachtet werden sollte. Da Software und Infrastruktur inzwischen ausgereift sind, wird ein baldiger Einstieg in das Thema uneingeschränkt empfohlen.

Text: **Bernhard Schmidt, Daniel Feuchtinger, Dr. Wolfgang Hommel, Prof. Dr. Helmut Reiser** (Leibniz-Rechenzentrum - LRZ)

Foto © Peter de Kievith/fotolia.de

Einleitung

Angesichts der ständigen technologischen Weiterentwicklung des Internets ist klar, dass man sich einigen Themen nicht langfristig entziehen kann und dies unter dem Aspekt der Sicherheit auch nicht tun sollte. DNSSEC fällt in diese Kategorie: Bedarf, Mehrwert und Unvermeidbarkeit sind schnell erkennbar, dennoch wird eine Auseinandersetzung mit der Materie gerne vertagt, bis eine kritische Masse durch andere gebildet wurde. Eine frühzeitige Beschäftigung mit neuen Technologien bietet aber die Möglichkeit, umfassendes Know-How ohne Zeitdruck aufzubauen, Designkonzepte aufgrund der historischen Entwicklung zu verstehen und den optimalen Zeitpunkt für die praktische Umsetzung selbst zu wählen.

Erste praktische Gehversuche mit DNSSEC für mehr als 130.000 Benutzer im Münchner Wissenschaftsnetz (MWN), hat das Leibniz-Rechenzentrum (LRZ) mit der Umstellung seines primären Resolvers auf DNSSEC-Validierung bereits 2008 unternommen. Nach der Teilnahme an DNSSEC-Testbeds und erfolgreichem Signieren kleinerer Domains seit 2010, gibt es inzwischen kein Zurück mehr. Seit März 2014 werden alle LRZ-Resolver DNSSEC-validiert betrieben und innerhalb von drei Monaten wurden bis Januar 2015 auch die großen Hauptdomains lrz.de, tum.de (Technische Universität München) und lmu.de (Ludwig-Maximilians-Universität München) signiert. Im Laufe des Jahres 2015 kamen 40 weitere Domains dazu. Dank der guten Vorbereitung sind dabei keine Probleme aufgetreten.

Das Ergebnis motiviert dazu, auch anderen Einrichtungen die Umstellung auf DNSSEC vorbehaltlos zu empfehlen. Dieser Artikel zeigt die abgestufte Vorgehensweise auf, zunächst den rekursiven DNS-Resolver-Dienst und anschließend die autoritativen DNS-Server umzustellen, gibt Empfehlungen zum externen Monitoring für das frühzeitige Erkennen potentieller Fehler und zeigt mit SSHFP und DANE/TLSA zwei DNSSEC-Anwendungen auf, von denen die eigene Server- und E-Mail-Infrastruktur ohne großen Zusatzaufwand profitieren kann.

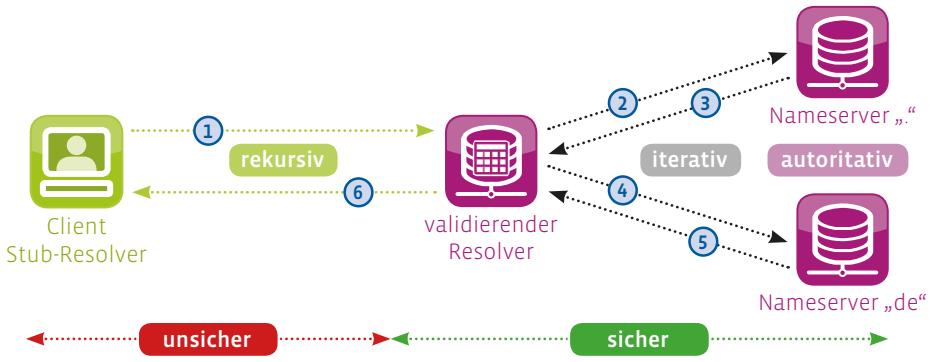


Abbildung 1: Rekursive Namensauflösung mit validierendem Resolver

DNSSEC-Resolver

Das LRZ betreibt für alle Server und Clients im MWN eine zur Sicherstellung der Ausfallsicherheit redundante DNS-Resolver-Infrastruktur auf Basis der ISC-Referenzimplementierung BIND. Die Umstellung auf DNSSEC-Validierung birgt das Risiko, dass Einträge aus fehlerhaft DNSSEC-signierten Zonen gar nicht mehr aufgelöst werden können und diese Zonen damit für alle Clients validierender Resolver nicht mehr erreichbar sind. Fehler in Signaturen und Signaturketten traten, bedingt durch die höhere Komplexität und nicht ausgereifte Software, zu Beginn noch häufiger auf und fielen aus Nutzersicht, oft zu unrecht, auf die Betreiber der validierenden Resolver zurück. Daher hat das LRZ zunächst nur einen seiner Resolver entsprechend konfiguriert, um die Systemreife beurteilen zu können, ohne die Dienstnutzung durch angebundene Endgeräte zu gefährden. Seit der Umstellung sämtlicher Resolver auf DNSSEC-Validierung vor über zwei Jahren sind am LRZ jedoch trotz der relativ großen Anzahl an versorgten Benutzern nur fünf Störungsmeldungen eingegangen, die peripher durch DNSSEC hervorgerufen wurden und immer durch die jeweilige Gegenseite verursacht waren. Trotz dieser Zwangsbeglückung aller Anwender mit DNSSEC sind somit keine nennenswerten Probleme aufgetreten.

Erwähnenswert bleiben zwei Schwierigkeiten: Zum einen können DNSSEC-validierende Resolver auch weiterhin kein DNS-Spoofing auf dem Weg zwischen Endgerät und DNS-Resolver verhindern. Das Problem ist dann gelöst, wenn man dem Netz zwischen Endgerät und Resolver vertraut, im Idealfall läuft der Resolver also auf dem Endgerät.

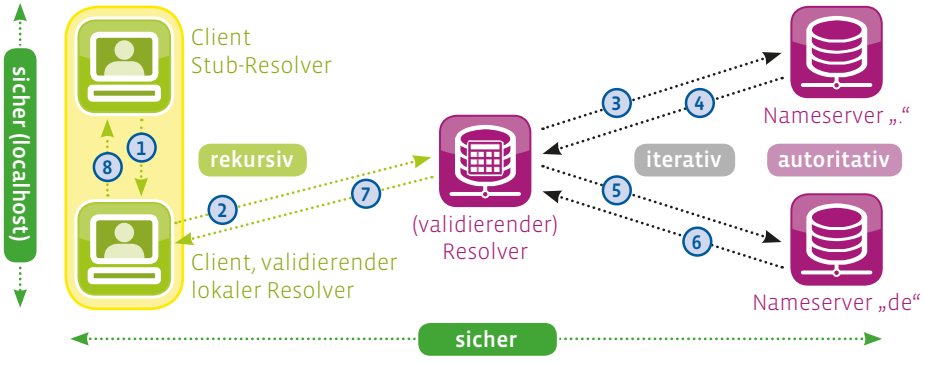


Abbildung 2: Rekursive Namensauflösung mit validierendem lokalen Resolver

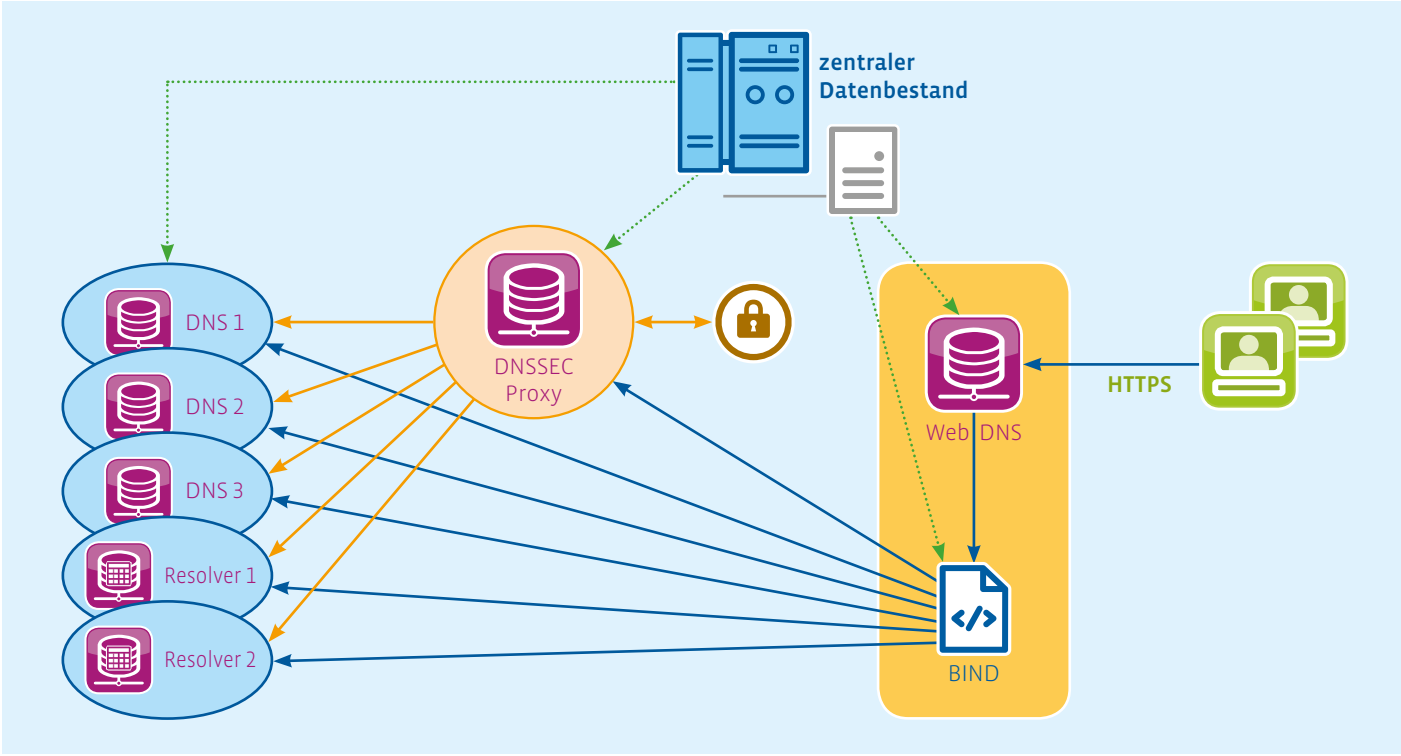


Abbildung 3: DNS-Infrastruktur mit einem Signing Proxy

Im LRZ kommt auf einigen Produktiv-Systemen als lokaler validierender Resolver die OpenSource-Software Unbound zum Einsatz. Zum anderen werden lokale DNS-Zonen, für die der Resolver als Slave fungiert, von ISC BIND nicht DNSSEC-validiert. Um dieses Problem zu umgehen, müssten die Resolver ihren Slave-Status verlieren, das ist bei den LRZ-Resolvern noch nicht der Fall, da DNS-Änderungen damit nicht sofort wirksam würden.

Autoritative DNS-Server

Das Signieren eigener DNS-Zonen ist mit deutlich mehr Aufwand verbunden als die Umstellung von DNS-Resolvern. Alle beteiligten autoritativen Server, also auch die Slaves, müssen DNSSEC-fähig sein. Die Aussicht darauf, durch eine Fehlkonfiguration die Namensauflösung durch DNSSEC-validierende Resolver weltweit für alle eigenen Systeme zu unterbinden, wirkt sich positiv auf den Adrenalinspiegel aller Beteiligten aus und ist zugleich Schlüssel zu den unten beschriebenen funktionalen Neuerungen für andere Dienste. Da ein erneutes Signieren der Zone bei jeder Änderung erforderlich ist und die manuelle Vorgehensweise, z. B. mit dem Tool dnssec-signzone, durchaus fehleranfällig ist, sollte von Anfang an auf eine durchgängige Automatisierung der Abläufe hingearbeitet werden.

Die ISC BIND Software hat seit Version 9.8 ein als auto-dnssec maintain bezeichnetes Feature, bei der sich BIND automatisch um das Re-Signing kümmert. Das LRZ nutzt das mit BIND 9.9 eingeführte Inline-Signing, das nicht mehr mit lokalen Zonenfiles, sondern auf Basis von Zonentransfers (AXFR) arbeitet und dadurch die Einrichtung so genannter Signing Proxies ermöglicht. Vom LRZ wurden für die Einrichtungen im MWN bereits über 700 Domains und 2.000 Subdomains registriert, die mandantenfähig per Web-Frontend auf Basis des Produkts Nixu (jetzt FusionLayer, Inc.) NameSurfer verwaltet werden. DNSSEC-relevante Zonen werden an den Inline-Signing-Proxy transferiert, mit dessen Ergebnissen wiederum die autoritativen LRZ-DNS-Server und die Resolver gespeist werden. Der Signing-Proxy kann netzseitig geschützt werden, da Zugriff nur auf den Master und von den autoritativen Servern nötig ist. Die Keys sind damit besser vor unberechtigtem Zugriff geschützt (Abbildung 3).

Diese Implementierung integriert sich nahtlos in die am LRZ schon vorhandene BIND-Infrastruktur und wurde deshalb Alternativen wie OpenDNSSEC vorgezogen. Tests haben ergeben, dass OpenDNSSEC zwar durchaus interessant wäre, da es z. B. auch Key-Rollovers automatisieren kann, dafür ist das Setup mit MySQL und SoftHSM als Abhängigkeiten aber deutlich komplexer und im MWN benötigte Funktionen wie dynamische DNS-Updates fehlen bislang.

Monitoring eigener DNSSEC-signierter Zonen

Fehler in den eigenen DNSSEC-Daten (z. B. Ablauf der Gültigkeitsdauer von Signaturen u.ä.) führen dazu, dass Dienste in der entsprechenden Domain von Clients validierender Resolver faktisch nicht mehr erreichbar sind. Falls zur Behebung des Fehlers eine Änderung des Eintrages in der da-

rüber liegenden Domain (z. B. DS-Record .de-Zone) notwendig wird, bedeutet dies, dass die gesamte Domain im schlechtesten Fall bis zum Ablauf der TTL der darüberliegenden Domain (24 Stunden im Fall der de-Domain) nicht mehr auflösbar ist. Da solche Fehlkonfigurationen je nach lokaler Resolverstruktur nicht auffallen, kommt dem Monitoring auch unter Einbezug externer Systeme eine essenzielle Bedeutung zu.

Am LRZ findet deshalb eine automatisierte, tägliche Prüfung jeder DNSSEC-Zone statt. Zunächst werden die signierten Zonen lokal mit den Tools ldns-verify-zone (Open Source) und dnssec-verify (Bestandteil von BIND) untersucht, die das NSEC-Chaining, die Keys und die RRSIG-Validity überprüfen. Bei identifizierten Fehlern oder wenn die verbleibende RRSIG-Gültigkeit unter 30 Tage fällt, wird automatisch per E-Mail alarmiert. Anschließend werden die SOA-Records über bislang sehr zuverlässige externe Dienste, nämlich die Google DNS-Server und den OARC Open DNSSEC Validating Resolver, abgefragt, wobei auf sichere Delegation (ad-Flag) und Funktionsfähigkeit aus Nutzersicht geprüft wird. Die Gültigkeitsdauer der Signaturen wurde so gewählt, dass den Administratoren auch im Urlaubsfall genügend Zeit bleibt, auf Fehler bei der Signaturerneuerung zu reagieren.

Mehrwert für andere Dienste

DNSSEC ist notwendig, um DNS-Spoofing zuverlässig zu verhindern. Da dieses Risiko für die meisten im Tagesgeschäft aber eher hypothetisch ist, ergeben sich die Vorteile von DNSSEC derzeit primär im Zusammenspiel neuer RTYPEs mit anderen Diensten. Am LRZ werden diesbezüglich bereits SSHFP und DANE/TLSA genutzt.

SSHFP (RFC 4255) ermöglicht es, die Fingerprints der Hostkeys von SSH-Servern in DNS Resource Records zu hinterlegen. SSH-Clients können die Hostkeys dann per DNSSEC verifizieren. Relevant ist dies z. B. für Benutzer, die sich das erste Mal mit einem SSH-Server verbinden (wer prüft den angezeigten Hostkey bislang wirklich manuell?), oder wenn sich die Hostkeys eines Servers aus guten Gründen geändert haben (und sonst jeder Benutzer auf diesen Umstand hingewiesen und dadurch verunsichert wird). In der Praxis hilfreich ist diese Automatisierung insbesondere für externe Nutzer, die z. B. auf Git-Server über SSH oder auf Login-Knoten von High Performance Computing Systemen zugreifen, da die entsprechenden Fingerprints nur in den seltensten Fällen anderweitig, z. B. auf einem Webserver, veröffentlicht sind und somit Man-in-the-Middle-Angriffe einfach und benutzerfreundlich ausgeschlossen werden können. Das Erzeugen der benötigten SSHFP-Einträge ist mit dem OpenSSH-Standardwerkzeug ssh-keygen unter Verwendung der Option -r ‹hostname› trivial.

DANE/TLSA (RFC 6698) bietet die Funktion, Zertifikatsinformationen wie das zu benutzende CA-Zertifikat (Trust Anchor) oder unmittelbar das Serverzertifikat für Verbindungsendpunkte (Hostname und TCP/UDP Port) zu hinterlegen. Dieser Ansatz hat das Potential, herkömmliche Public-Key-Infrastrukturen bzw. die kommerziellen SSL-CAs überflüssig zu machen, findet bislang bei den großen Browserherstellern aber noch kein großes Interesse. Überaus praxisrelevant ist es jedoch bei der Transportverschlüsselung zwischen E-Mail-Servern, da hier sehr häufig nicht-validierbare Serverzertifikate, die z. B. selbstsigniert oder längst abgelaufen sind, eingesetzt werden und eine manuelle Validierung durch einen Administrator weder technisch möglich, noch praktikabel ist. Durch das Hinterlegen von Mailserver-Zertifikaten in TLSA-Records wird das durch Zertifikats-Pinning bekannte Sicherheitsniveau erreicht, so dass eine Validierung der Gegenseite Man-in-the-Middle-Angriffe verhindert; zudem stellt TLSA sicher, dass keine TLS-Downgrade-Angriffe mehr möglich sind. Von dem am LRZ eingesetzten MTA Postfix wird DANE/TLSA seit Version 2.11 unterstützt. Angesichts der noch fehlenden flächendeckenden Verbreitung von DNSSEC werden zwar nur 2 % der ausgehenden TLS-Verbindungen mit DANE gesichert, aber, obwohl bislang weniger als 2 % aller vom LRZ verwalteten Zonen signiert sind, könnten bereits mehr als 70 % des eingehenden Mailverkehrs über LRZ-Mailserver mit DANE geschützt werden. Da es beim Empfang von E-Mails allerdings prinzipbedingt keine Signalisierung der TLSA-Nutzung durch den Sender gibt, lassen sich keine konkreten Statistiken erstellen.

Weitere, sich aktuell im Draft-Status befindliche IETF-Standards werden das Hinterlegen von PGP-Keys (OPENPGPKEY) und S/MIME-Zertifikaten (SMIMEA) ermöglichen und so hoffentlich die bestehenden Usability-Probleme z. B. von PGP-Keyservern und dem häufig praktizierten manuellen Austausch von S/MIME-Zertifikaten per signierter Initial-E-Mail lösen. Noch wichtiger als bei SSHFP-Einträgen müssen dafür aber noch geeignete Management-Schnittstellen geschaffen werden, die einen massentauglichen Betrieb ohne manuelles Eingreifen der DNS-Server-Administratoren ermöglichen.

Fazit

DNSSEC ist reif für die Praxis. Nachdem das LRZ die Anfänge samt den Höhen und Tiefen der DNSSEC-Testbeds und eingesetzten Software mitgemacht hat, lässt sich guten Gewissens festhalten, dass ein stabiler Produktivbetrieb inzwischen uneingeschränkt möglich ist. Die bayerischen Universitäten und Hochschulen haben Anfang 2016 beschlossen, DNSSEC und DANE zur Steigerung der E-Mail Sicherheit im Rahmen eines gemeinsamen Projektes in Bayern einzuführen. Die neuen Möglichkeiten zur Erhöhung des Sicherheitsniveaus angebundener Dienste sind keine „must-have Killer-Features“ und nicht nur subjektiver Anreiz, sondern objektiver Mehrwert. Nach Einschätzung der Autoren führt langfristig kein Weg an DNSSEC vorbei. Jetzt ist die Gelegenheit, ohne Termindruck von außen und ohne unüberblickbare Risiken einzusteigen. ◆

25 Jahre DFN-Nutzergruppe Hochschulverwaltung

Dieses Jahr im November feiert die DFN-Nutzergruppe Hochschulverwaltung ihr 25-jähriges Bestehen. Aus diesem Anlass hier ein kurzer Rück- und Ausblick.

Text: **Prof. Dr. Gerhard Peter** (Leiter der DFN-Nutzergruppe Hochschulverwaltung)

DFN-Nutzergruppentagung „Dienste, Dienste, Dienste…“ in Leipzig 2009

Die DFN-Nutzergruppe

Zunächst stellt sich die Frage was eine Nutzergruppe ist. Ende der 80er Jahre des letzten Jahrhunderts wurde eine große Zahl von DFN-Nutzergruppen gegründet. Mit Unterstützung des Deutschen Forschungsnetzes organisierten sich diese zu spezifischen Themen aus dem Umfeld von Wissenschaft und Forschung. Nutzer mit vergleichbaren Aufgabengebieten oder gleichen Interessen schlossen sich zusammen und formulierten ihre Anforderungen an den Netzbetreiber DFN. Daraus resultierten gruppenspezifische Nutzergruppen, die die Interessen der Fachhochschulen, oder die der Studierenden vertraten. Neben den gruppenspezifischen Nutzergruppen gab es auch Gruppen, die sich an Fachinteressen ausrichteten. So z. B. die Nutzergruppe der *Wissenschaftsjournalisten* oder die Gruppe *Chemie*.

Alle hatten ihre speziellen Anforderungen an den DFN-Verein und formulierten ihre Wünsche und Fragen.

Die Dynamik des Anfangs

Die DFN-Nutzergruppe Hochschulverwaltung war somit eine von vielen ähnlichen Gruppen. Die Gruppe wurde am 10. November 1991 in Berlin gegründet. Ihre Aufgabe war es, die Nutzung des Wissenschaftsnetzes für Verwaltungszwecke und durch Verwaltungspersonal zu unterstützen.

Um die Leistungsfähigkeit der Gruppe zu steigern, bildeten sich gleich zu Beginn vier eigenständige Arbeitskreise heraus.

AK 1: Realisierung
AK 2: Zukünftige Entwicklungen
AK 3: Sicherheit
AK 4: Recht

Als Dach der vier Arbeitskreise fungierte die Nutzergruppe. Die Lebensdauer der Arbeitskreise *Zukünftige Entwicklungen*, *Sicherheit* und *Recht* war jedoch begrenzt und so blieb nur der Arbeitskreis *Realisierung* übrig und die Unterscheidung zwischen Arbeitskreis und Nutzergruppe wurde aufgehoben. Die jeweiligen Leiter definierten sich als Sprecher und Stellvertreter.

Sehr schnell stellte sich heraus, dass die Mitglieder der Nutzergruppe aus zwei Gruppen bestanden, zum einen aus Mitarbeitern der Rechenzentren und zum anderen aus Mitarbeitern der Hochschulverwaltung.

Jede dieser Gruppen hatte ihren eigenen fachlichen Hintergrund und ihren eigenen Sprachgebrauch. So kam es zu einem regen Erfahrungs- und Wissensaustausch. Die Verwaltungsmitarbeiter eigneten sich IT-Kompetenzen und Verständnis für die Vernetzung an, die RZ-nahen Gruppenmitglieder lernten die komplexen Aufgaben der Verwaltung kennen. Das wechselseitige Wissen wurde in einem DFN-Bericht ausformuiert.

(von links nach rechts): Herby Roebke, Ingrid Duda, Peter Leinen; Nutzergruppensitzung in Hamburg 2014

Themen waren bereits damals aktuelle Netztechnologien, Datenschutz und Datensicherheit, Infrastruktur und Anwendungsmöglichkeiten.

Ziel war es, den Nutzen und die potentiellen Gefahren der Materie in der Sprache für die Hochschulverwaltungen zu formulieren, um sie den Hochschulleitungen und Verwaltungsmitarbeitern näher bringen zu können.

Wie wir erfolgreich arbeiten

Die gewonnenen Erkenntnisse wurden bald einem breiten Kreis an Interessierten in Form einer Tagung zugänglich gemacht. Diese Tagungen finden in einem zweijährigen Rhythmus statt. Das erste Jahr nach einer Tagung dient der Orientierung und Weiterbildung der Gruppenmitglieder. Vermutlich ist auch dies der Grund für den Erfolg der Nutzergruppe. Fragen werden intern gestellt und die Lösung gemeinsam ermittelt. Jedes Mitglied kann Fragen einbringen und profitiert von der internen Kompetenz. Zusätzlich bringen externe Referenten ihr Wissen auf den Sitzungen mit ein.

Im zweiten Jahr wird die nächste Tagung explizit vorbereitet. Es werden Schwerpunktthemen festgelegt und in eine feste Grundstruktur eingebunden. Die Vortragsthemen am Eröffnungstag sind den Grundlagen und den Perspektiven gewidmet. Der zweite Tag widmet sich den fachspezifischen Themen und der Dritte konzentriert sich auf die Anwendungen der Verwaltungs-IT.

Unsere Themen

So haben bereits viele erfolgreiche Tagungen stattgefunden. Interessant ist der Vergleich der jeweiligen Schwerpunktthemen. Folgende Tagungen haben mit den genannten Schwerpunkten stattgefunden:

1994	Merseburg „DV- Kommunikation für die Verwaltung der Hochschulen über WiN“
1995	Kaiserslautern „Sichere Datenübertragung in offenen Netzen“
1997	München „WWW und Hochschulverwaltung“
1999	Leipzig „Verwaltungsnetze/ Verwaltung im Netz“
2001	Kassel „Service mit Sicherheit“
2003	Potsdam „Verwaltung@eUniversity“
2005	Braunschweig „Auflösung von Verwaltungsgrenzen“
2007	Halle „Bologna online“
2009	Leipzig „Dienste, Dienste, Dienste…“
2011	Berlin „Hochschule mit links und Recht“

Jupp Hötte, Gründungsmitglied

Inga Scheler, Sprecherin ab Januar 2016

Bochum Mai 2015: Peter Leinen, damaliger Sprecher

2013 Mannheim „Mobiler Campus“
2015 Bochum „Sicherheit trotz(t) IT“

An der Themensetzung ist die sich entwickelnde Aufgabenstellung erkennbar. Zunächst gab es eine Konzentration auf technische Aspekte, um den Einsatz der Kommunikationstechnik im Verwaltungsbereich überhaupt zu ermöglichen. Die Vorteile, die sich dadurch öffnen, wurden nicht durchgängig gesehen. Relativ schnell zeigte sich daher auch der Sicherheitsbereich als zentrales Thema. Anfänglich waren die Bedenken gegen eine Öffnung der Verwaltung so groß, dass für ein eigenes, physisch getrenntes Netz plädiert wurde. Überzeugungsarbeit musste geleistet werden. Einzelne Tagungen standen wieder unter einem aktuellen Thema, das alle Verwaltungen betraf, wie beispielsweise die Folgen der Umstellung auf den Bolognaprozess oder die Auswirkung des Einsatzes mobiler Geräte. Auch für 2017 werden wir wieder ein passendes und zeitbezogenes Motto finden.

Ein Ausblick

Die nächste Tagung findet 2017 an der Westfälischen Wilhelms-Universität in Münster statt. Der Monat Mai hat sich als Termin als konkretes Merkmal herausgestellt. Die Arbeitstreffen zwischen den Tagungen finden ca. viermal im Jahr an wechselnden Orten statt. Das 110. Arbeitstreffen fand im April 2016 in Konstanz statt.

Bis zum Herbst werden dann die Vorträge, sowie das Schwerpunktthema und die Referenten festgelegt. Bei allen Beiträgen handelt es sich um eingeladene Vorträge. Diese werden aufeinander abgestimmt und die Referenten über die Zielsetzung und die benachbarten Vorträge informiert. Die Nutzergruppenmitglieder sind aufgefordert, Vorträge zu übernehmen und die Sitzungsleitungen zu stellen.

So stehen sich bewährte Strukturen mit immer wieder neuen und aktualisierten Themen gegenüber.

Wir feiern 25 erfolgreiche Jahre!

Mit einer 25-Jahrfeier werden wir die gemeinsamen Jahre und das erfolgreiche Arbeiten begehen. Dafür findet am 7. Oktober 2016 eine Vortragsveranstaltung zum Thema Nutzergruppe Hochschulverwaltung statt, auf der es sowohl einen Rückblick als auch einen Ausblick geben wird: Wie ist die Nutzergruppe entstanden, was stellt sie jetzt dar und was werden ihre zukünftigen Aufgaben und Zielsetzungen sein. ◆

Nutzergruppensitzung auf dem Dach der Geschäftsstelle des DFN in Berlin 2016

Frage & Antwort zum Thema PKI und Zertifikate

Jürgen Brauckmann, Leiter des PKI-Teams (Public Key Infrastructure) am DFN-CERT (Computer Emergency Response Team des Deutschen Forschungsnetzes) steht Prof. Andreas Hanemann Rede und Antwort.

Text: **Prof. Andreas Hanemann** (FH Lübeck)

Der Professor für Rechnernetze und Webtechnologien an der FH Lübeck, Andreas Hanemann, befragte den Experten des DFN-CERT im Rahmen seines MOOC (Massive Open Online Course) zum Thema Netzwerksicherheit. Das DFN-CERT beschäftigt sich insgesamt mit Sicherheitsthemen, die für das DFN-Netz und die angeschlossenen Hochschulen und Forschungseinrichtungen relevant sind. Das PKI-Team betreibt dabei eine Zertifizierungsstelle als Basis für die Zertifizierung in den Mitgliedseinrichtungen des DFN-Vereins. Da das Thema PKI auf allgemeines Interesse stößt, wollen wir Ihnen dieses Interview nun auch hier zugänglich machen.

Für welchen Zweck können Zertifikate aus einer PKI eingesetzt werden?

Obwohl die technische Basis von PKIs immer sehr ähnlich ist (asymmetrische Kryptographie, Zertifikate), können sehr unterschiedliche Einsatzszenarien abgebildet werden:

- Server können mit Zertifikaten beweisen, dass sie authentisch sind, und die Verschlüsselung von Verbindungen zu Clients ermöglichen. Diese TLS Serverauthentisierung ist z. B. großflächig im Einsatz bei Webservern mit dem Protokoll HTTPS und bei der sicheren Kommunikation zwischen Mail-Programmen und dem Mail-Provider über STARTTLS in SMTP/IMAP/POP.
- Personen oder Geräte können sich an einem Server anmelden (TLS Client-Authentisierung, z. B. verwendet im Webbrowser, oder 802.1X Geräteanmeldung im Netzwerk).
- E-Mails können mit S/MIME direkt Ende-zu-Ende, zwischen den Mailprogrammen der Kommunikationspartner, verschlüsselt werden.

Wie können Zertifikate für die Authentifizierung einer Person, eines Gerätes oder eines Servers verwendet werden?

Zertifikate verknüpfen einen Namen, z. B. eine E-Mail-Adresse oder eine Serveradresse, mit einem kryptographischen Schlüssel. Für eine erfolgreiche Authentisierung muss der Zertifikatinhaber zunächst nachweisen, dass er den zum präsentierten Zertifikat gehörenden geheimen kryptographischen Schlüssel besitzt. Nach diesem Nachweis muss der Prüfer untersuchen, ob der Name im präsentierten Zertifikat seinen Erwartungen entspricht (also z. B. dass der Server www.example.org tatsächlich ein Zertifikat mit dem Namen www.example.org übermittelt hat), und ob er dem Zertifikat und der ausgebenden Zertifizierungsstelle vertraut.

Wie wird das Vertrauen in Zertifikate geprüft?

Hierzu werden Root-CAs verwendet (von Microsoft „Vertrauenswürdige Stammzertifizierungsstellen“ genannt, von Mozilla einfach nur „Zertifizierungsstellen“). In der

prüfenden Software sind diese Root-CAs konfiguriert, normalerweise über eine vom Hersteller vorbereitete Liste, oder manuell ergänzt durch den Nutzer. Beim Prüfvorgang wird getestet, dass das zu untersuchende Zertifikat von einer Zertifizierungsstelle unterhalb einer bekannten Root ausgestellt wurde. Falls ja, wird dem Zertifikat vertraut.

Bevor ein Hersteller eine Root-CA in seine Software aufnimmt, muss der Betreiber der Root-CA die Einhaltung von formalen Kriterien nachweisen. Für Zertifikate für TLS gibt es herstellerübergreifende Kriterien, die sogenannten Baseline Requirements des CA/Browser Forums. Für andere Zertifikattypen gibt es nur herstellereigene Regeln.

Damit die Vertrauenswürdigkeit einer PKI sichergestellt wird, werden regelmäßig Audits durchgeführt. Wer führt diese durch und wie ist der Ablauf?

Für PKIs, die über eine Root-CA in Softwareprodukten von Microsoft, Apple, Oracle, Google oder Mozilla direkt vertrauenswürdig sind, ist ein jährliches Audit Pflicht. Hierfür gibt es verschiedene zulässige Audit-Standards, von denen die am häufigsten verwendeten „WebTrust for Certification Authorities“ und „ETSI TS 102 042“ sind. Eine Prüfung nach diesen Standards kann nur durch eine anerkannte Stelle durchgeführt werden, die bei einer nationalen oder internationalen Akkreditierungsstelle für Auditoren registriert ist. In Deutschland vergibt beispielsweise die DakkS GmbH die Berechtigung für Audits nach ETSI TS 102 042. Für WebTrust ist die zuständige Akkreditierungsstelle das American Institute of Certified Public Accountants und CPA Canada.

Bei einem Audit wird zunächst der Dokumentationsstand des Gesamtsystems geprüft: Ist die Dokumentation der baulichen, organisatorischen und technischen Gegebenheiten vollständig und aktuell? Sind die dokumentierten technischen Maßnahmen ausreichend und entsprechen sie dem Stand der Technik?

Im Anschluss wird geprüft, dass die dokumentierten Maßnahmen nicht nur auf dem Papier stehen, sondern auch tatsächlich umgesetzt werden. Dies geschieht durch eine Vor-Ort-Inspektion, die von der räumlichen Situation bis hin zu einzelnen Firewall-Regeln alle Aspekte des Gesamtsystems umfasst. Der Auditor selbst wird übrigens auch noch einmal überprüft: Der Prüfbericht wird durch eine unabhängige Stelle innerhalb der Organisation des Auditors auf Schwachstellen und Mängel untersucht.

Welche Schritte sind notwendig, wenn ein Benutzer oder ein Serveradministrator ein Zertifikat der DFN-PKI erhalten möchte?

Je nach Einsatzszenario werden unterschiedliche Verfahren zur Ausgabe von Zertifikaten verwendet.

Ein Weg ist die Beantragung über den Webbrowser. Für Nutzerzertifikate wird ein Webformular ausgefüllt, bei dessen Übermittlung direkt im Browser des Nutzers ein geheimer kryptographischer Schlüssel erzeugt wird. Der Nutzer erstellt dann ein Antragsformular und meldet sich mit diesem Formular bei dem Teilnehmerservice seiner Einrichtung.

Für Serveradministratoren, die ein Zertifikat für einen Server nutzen möchten, ist der Weg ähnlich: Sie müssen in ihrer Serversoftware einen Zertifikatrequest erzeugen, diesen in einem Webformular eintragen und sich wiederum mit einem Antragsformular an den Teilnehmerservice der Einrichtung wenden.

Verfahren mit einem höheren Automatisierungsgrad, bei denen die Zertifikaterstellung z. B. in eine Chipkartenproduktion eingebunden ist, sind in der DFN-PKI aber auch schon seit vielen Jahren im Einsatz. Diese Verfahren müssen aber immer stark auf die jeweilige Einrichtung zugeschnitten sein.

Wichtig: Bei Nutzerzertifikaten ist in der DFN-PKI im Sicherheitsniveau „Global“ stets eine persönliche Identifizierung notwendig, da mit dem Zertifikat beispielsweise Prüfungsanmeldungen zuverlässig durchgeführt werden können sollen.

Zertifikate haben eine begrenzte Lebensdauer. Wie lange sind die Zertifikate üblicherweise gültig? Wie läuft die Erneuerung ab?

Zertifikate werden mit einem Ablaufdatum versehen, da die in ihnen enthaltenen Daten regelmäßig überprüft werden müssen. Nutzerzertifikate sind in der DFN-PKI im Sicherheitsniveau „Global“ aktuell 3 Jahre, Serverzertifikate 39 Monate gültig. Die Laufzeit richtet sich dabei nach Vorgaben aus internationalen Richtlinien für Serverzertifikate.

Für die Erneuerung hat es sich als zweckmäßig erwiesen, denselben Ablauf wie für die Erst-Beantragung durchzuführen.

Zertifikate müssen manchmal für ungültig erklärt werden, z. B. wenn der private Schlüssel entwendet wurde. Welche Mechanismen gibt es dafür?

Um ein Zertifikat für ungültig zu erklären, muss es zunächst bei der Zertifizierungsstelle (CA) als gesperrt markiert werden. Im nächsten Schritt muss diese Sperrinformation durch geeignete Protokolle an diejenigen übermittelt werden, die die Zertifikate prüfen. Hierfür stehen grundsätzlich drei verschiedene Mechanismen zur Verfügung:

- Eine Certificate Revocation List (CRL) ist eine komplette Liste aller gesperrten Zertifikate einer CA. Sie wird von der CA zum Download angeboten, und kann automatisiert durch die Aufnahme der URL in die Zertifikate bezogen werden. CRL können sehr groß werden (einige Megabyte), sodass der Abruf z. B. nicht bei jedem Aufruf einer sicheren Webseite durchgeführt werden kann.
- Online Certificate Status Protocol (OCSP) ist ein Protokoll, bei dem eine Software die CA über eine Einzelabfrage nach dem Gültigkeitszustand eines einzelnen Zertifikates befragen kann. OCSP ist in den meisten Situationen besser geeignet als CRLs, wird von den Browserherstellern aber trotzdem kritisiert. OCSP weist zum einen typischerweise eine Latenz von bis zu 300ms auf, was Softwarehersteller als großes Hindernis für schnelles Webbrowsen betrachten, und kann zum anderen nicht in allen Situationen zuverlässig genutzt werden, z. B. hinter Captive Portals.
- Als dritten Mechanismus, der eine wachsende Bedeutung hat, sind herstellerabhängige Verfahren zu nennen, bei denen Softwarehersteller gezielt einzelne Zertifikate auf eine eigene Blacklist setzen. Google hat hierfür vor einigen Jahren ein Verfahren namens CRL-Set entwickelt, Mozilla arbeitet an einem ähnlichen Verfahren. Größtes Problem ist hierbei, dass nur die vom Hersteller als „relevant“ erachteten Zertifikate auf die Blacklist gesetzt werden.

Bietet die DFN-PKI CRL und/oder OCSP an?

In der DFN-PKI ist für alle Zertifikate CRL und OCSP verfügbar.

Sind nach der Erfahrung des DFN-CERT die Überprüfungen durch Browser bei ungültigen Zertifikaten ausreichend (man liest hier, dass als Default-Einstellung bei Zertifikaten mit nicht ermittelbarem Status von vertrauenswürdigen Zertifikaten ausgegangen wird)?

Tatsächlich prüfen einige Browser inzwischen gar nicht mehr selbst den Sperrzustand von Serverzertifikaten über OCSP/CRL, z. B. Google Chrome und viele mobile Browser. Die meisten Browser versuchen eine Sperrprüfung per OCSP durchzuführen, stellen bei Nicht-Erreichbarkeit des OCSP-Responders aber trotzdem eine Verbindung her. Der DFN-Verein stellt eine Testseite zur Verfügung, mit der man testen kann, inwieweit Software die Prüfung von Sperrzuständen durchführt.

Der Hash-Algorithmus SHA-1 wurde in den vergangenen Jahren als immer unsicherer eingestuft, so dass ein Wechsel auf SHA-2 erfolgen muss. Wie wird ein solcher Übergang organisiert?

Hierbei muss man berücksichtigen, dass ein Hash-Algorithmus in vielen verschiedenen Kontexten verwendet wird. Ein Anwendungsfall ist z. B. die Signatur von E-Mails: Von der E-Mail wird mit dem Hash-Algorithmus ein wenige Byte großer Fingerabdruck erzeugt, der dann mit einem Signaturverfahren wie RSA-PKCS#1 signiert wird. Hier wäre ein Update des Mail-Programms von Sender und Empfänger notwendig, um SHA-2 zu nutzen.

Ein anderer Anwendungsfall betrifft die PKI-Betreiber: Die Signaturen unter Zertifikaten werden ebenfalls mit Hilfe eines Hash-Algorithmus erzeugt. Hier müssen dann zunächst neu ausgegebene Zertifikate mit dem neuen Algorithmus signiert werden. Je nach Anwendung müssen gegebenenfalls auch bereits im Einsatz befindliche Zertifikate ausgetauscht werden. Das betrifft insbesondere Webserver, da viele Webbrowser inzwischen mehr oder weniger deutliche Warnmeldungen bei SHA-1-Zertifikaten darstellen. Ab 2017 werden viele Webbrowser voraussichtlich gar keinen Zugriff

mehr auf Webserver erlauben, die noch mit einem SHA-1-Zertifikat ausgestattet sind.

Ein großes Problem ist immer die Rückwärtskompatibilität: Während Webbrowser durch Autoupdate-Funktionen inzwischen eine hohe Agilität aufweisen, gibt es viele Geräte, die jahrelang im Einsatz bleiben sollen und nicht unbedingt jeden Algorithmus unterstützen. Das betrifft sehr hochpreisige Systeme wie Load-Balancer oder VPN-Konzentratoren, die aus Kostengründen natürlich jeweils so spät wie möglich ersetzt werden sollen. Aber auch die Kompatibilität mit Geräten, die viel in Entwicklungsländern verwendet werden, ist immer ein Thema. Wenn dort große Teile der Bevölkerung mit nicht-aktuellen Devices auf das Internet zugreifen, stellen sich bestimmte Fragen nach technischem Fortschritt ganz anders. Wäre es z. B. vertretbar, dass ein Anbieter eines sozialen Netzwerkes seine Verschlüsselungsalgorithmen so umstellt, das große Teile der Bevölkerung aus Entwicklungsländern nicht mehr an dem Dienst teilnehmen können? Diese Frage veranlasst zur Zeit Facebook, über ein System nachzudenken, bei dem Verbindungen zu alten Geräten noch mit SHA-1 signierten Zertifikate abgesichert werden, neue Geräte aber sicherere SHA-2-Zertifikate nutzen.

E-Mail-Verschlüsselung mittels PGP gilt als relativ schwer bedienbar. In einem Artikel forderte J. Schmidt vom Heise-Verlag beispielsweise dieses nicht weiter zu nutzen und durch Alternativen zu ersetzen. Wie sieht man beim DFN-CERT die Situation?

Die klassische E-Mail-Verschlüsselung, die Ende-zu-Ende mit eigenen Schlüsseln von Absender und Empfänger arbeitet, gibt es seit fast 25 Jahren. In dieser Zeit konnte die Usability nicht so gesteigert werden, dass sie von „Normal-Benutzern“ mit für sie erträglichem Aufwand freiwillig verwendet wird. Das betrifft sowohl PGP als auch S/MIME.

Dessen ungeachtet können beide Verfahren sehr gut in relativ homogenen Benutzergruppen verwendet werden, wenn entweder eine genügend große Motivation der Teilnehmer da ist, oder aber Support, z. B. von einem Rechenzentrum, vorhanden ist. Damit sind sowohl PGP als auch S/MIME nach wie vor unabdingbar für sichere und verlässliche Kommunikation.

Wo Jürgen Schmidt Recht hat: PGP und S/MIME sichern normalerweise keine Alltagskommunikation ab und schützen keine Personen, die keine eigene große Motivation zur sicheren Nachrichtenübermittlung haben. Wie der großflächige erfolgreiche Einsatz von Verschlüsselungsverfahren bei diversen Instant Messenger Diensten (z. B. dem von Jürgen Schmidt angeführten iMessage von Apple) gezeigt hat, kann man Nutzern aber durchaus Kryptographie und sichere Kommunikation quasi „unterschieben“, ohne dass man sie zu dem relativ hohen Aufwand von S/MIME und PGP zwingt.

Dazu braucht es aber einen neuen Denkansatz ohne ständige Verweise auf die bestehenden, für diesen Einsatzzweck gescheiterten Verfahren. Leider hat noch niemand gezeigt, wie neue sichere Verfahren herstellerübergreifend und interoperabel eingeführt werden können. ◆

Sicherheit

Der CAOS Stick – Crash Any OS

Die Gefahren durch Angriffe auf IT-Systeme mittels bösartiger USB-Hardware sind in den letzten Jahren wiederholt aufgezeigt worden. Eine umfassende systematische Suche entsprechender Schwachstellen war bisher sehr aufwendig und ihre Demonstration fast unmöglich. Das in diesem Artikel vorgestellte Framework ermöglicht ein systematisches und hoch performantes Fuzzing von USB-Treibern durch massiven parallelen Einsatz von virtuellen Maschinen.

Text: **Sergej Schumilo, Hendrik Schwartke, Ralf Spenneberg** (OpenSource Security)

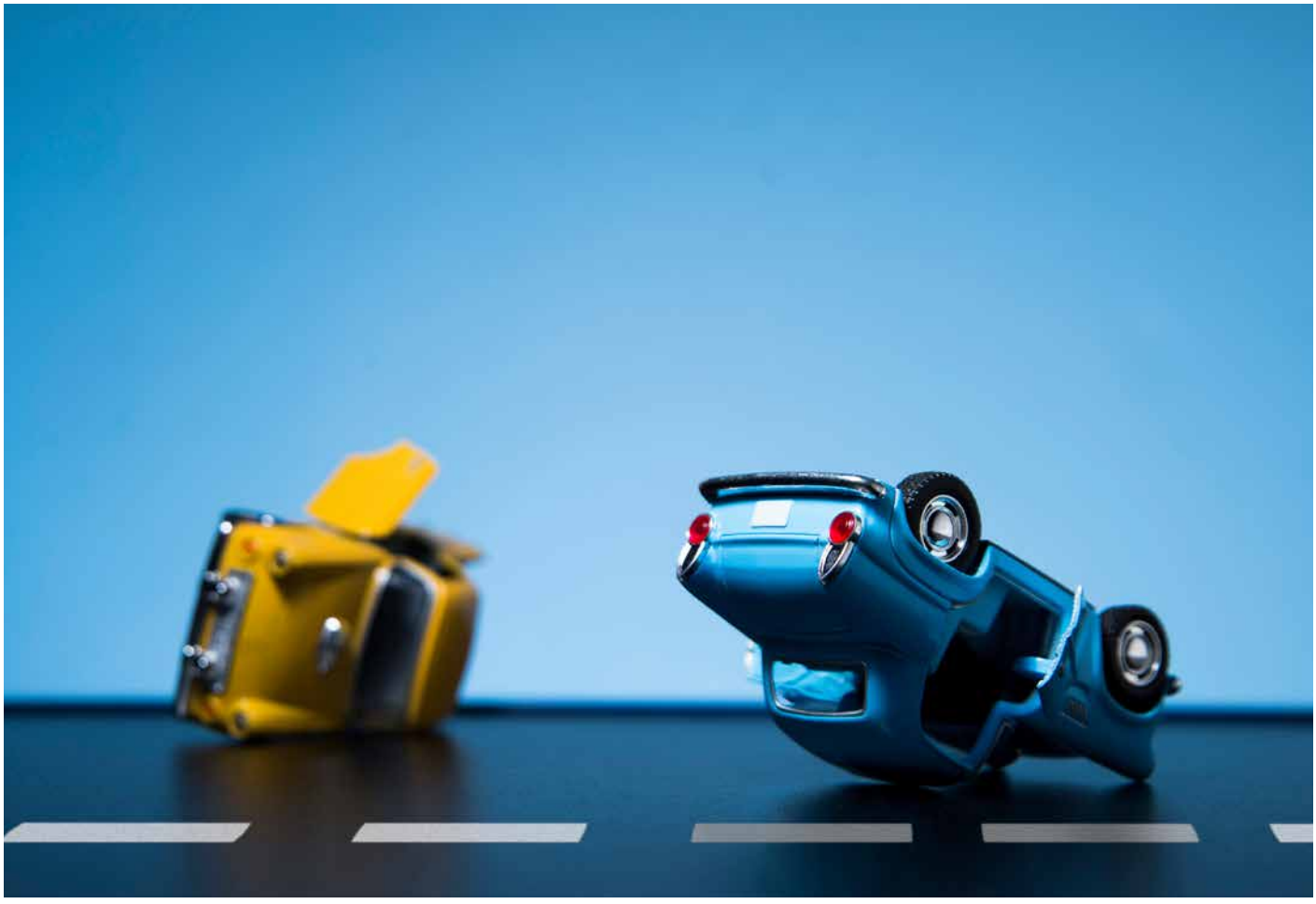


Foto © arda savacıoulları / iStockphoto.de

Der Universal Serial Bus (USB) ist ein serielles Bussystem und ein Standard für die Kommunikation zwischen verschiedensten Peripheriegeräten und dem Host. Anschlüsse für USB-Geräte finden sich in allen Bereichen der Technik. Ob am Computer, der Spielkonsole, dem Drucker oder in der automobilen Unterhaltungselektronik, überall findet der USB-Standard Anwendung. Umso wichtiger ist es, die Frage zu stellen, ob die USB-Implementierungen in diesen Systemen den erwarteten Sicherheitsanforderungen genügen.

Die Gefahren durch Angriffe mittels bösartiger USB-Hardware sind in den letzten Jahren wiederholt aufgezeigt worden. Der USB stellt schon seit Jahren ein attraktives Ziel für Angreifer und ihre Exploits dar. Bekannte Angriffsvektoren waren in der Vergangenheit die Ausnutzung der Auto-Run Funktionalität älterer Windows-Versionen [autorun] oder das automatisierte Absetzen von bösartigen Kommandos über die Emulation eines USB-Eingabegeräts (Human Interface Device, HID) [teensy]. Spätestens seit der Veröffentlichung von BadUSB [badUSB], findet eine Sensibilisierung für Sicherheitsschwachstellen statt. Einige Sicherheitsforscher, wie z. B. Andy Greenberg [usbbroken], bezeichnen das Sicherheitskonzept des USB-Standards als komplett unzureichend.

Neben den genannten Angriffsvektoren existiert jedoch noch ein weiterer Weg, Systeme mittels USB zu kompromittieren. Dieser basiert auf der Ausnutzbarkeit von Implementierungsschwachstellen der durch das Betriebssystem oder Drittthersteller bereitgestellten Treiber. Da der USB Hot-Plug unterstützt, wählt das jeweilige Betriebssystem nach dem Einstecken und der anfänglichen Initialisierung des USB-Geräts einen generischen USB-Treiber anhand einer USB-Klasse (Eingabegeräte, Drucker, etc.) oder einen gerätespezifischen Treiber. Das Betriebssystem übergibt nach der anfänglichen Initialisierung die Kontrolle an den ausgewählten USB-Treiber. Das Sicherheitsmodell impliziert jedoch, dass die Implementierung des geladenen Treibers über keine Sicherheitsschwachstellen verfügt. Dass diese Anforderung bei etlichen USB-Treibern verschiedenster Betriebssysteme nicht erfüllt ist, zeigen verschiedenste Forschungen und Treiber-Untersuchungen. Problematisch ist hierbei, dass im Falle einer Kompromittierung des angegriffenen Systems, der Angreifer die Möglichkeit hat, Schadcode im Kernel-Space auszuführen. Damit stehen ihm wesentlich mehr Privilegien als bei den anderen oben aufgezeigten Vektoren zur Verfügung.

Für die Untersuchung der Treiber von USB-Geräten auf Sicherheitslücken hat sich in der Vergangenheit die Fuzzing-Methode bewährt [davis]. Beim USB-Fuzzing wird mit Hilfe eines Man-In-The-Middle-Ansatzes der USB-Verkehr gezielt verändert. Alternativ kann durch die Implementierung eines USB-Emulators ein Gerät bereitgestellt werden, welches an ein Zielsystem unerwartete oder (teilweise) veränderte Daten schickt, um Abstürze oder Fehlverhalten des Zielsystems zu provozieren.

vUSBf-Framework

Anforderungen an das Fuzzing-Framework sind die hohe Ausführgeschwindigkeit, eine hohe Reproduzierbarkeit und eine möglichst lückenlose Protokollierung der Auswirkungen verschiedener USB-Payloads. Darüber hinaus soll das Framework möglichst einfach erweiterbar sein. Die folgenden Lösungsansätze dienen der Implementierung eines USB-Fuzzing-Frameworks, welche diese Anforderungen erfüllt.

Das Framework setzt für die Realisierung der gegebenen Anforderungen auf die im Linux-Kernel integrierte Virtualisierungsinfrastruktur KVM, um damit die zu überprüfenden Systeme zu virtualisieren. KVM wird mit QEMU kombiniert, welches die Peripherie emuliert. Diese Virtualisierungslösung ist, im Gegensatz zu anderen kommerziellen Lösungen, unter verschiedenen GPL-Versionen lizensiert und bietet somit größtmögliche Flexibilität bzgl. Verwendung und Erweiterbarkeit.

Architektur

Das vUSBf-Framework ist in der Programmiersprache Python entwickelt. Die Software-Architektur entspricht der nachfolgenden Grafik (Abbildung 1, s. S. 46):

Ein Hauptbestandteil des Frameworks stellt das Modul namens QEMU-Controller dar. Mit Hilfe von diesem Modul wird unter anderem der QEMU-Prozess gestartet. Auch die Überwachung der Standard-Datenströme erfolgt durch dieses Modul. Ferner erlaubt das Modul die Steuerung des QEMU-Prozesses, wie beispielsweise das Laden von Snapshots oder das Beenden der virtuellen Maschine. Das Modul untersucht des Weiteren die Ausgaben der virtuellen Maschine auf Fehlermeldungen.

Die USB-Emulation verfügt über eine erweiterbare API. Als Datenkanal wird ein hierfür erstellter Unix-Socket pro laufender QEMU-Instanz verwendet. Hierarchisch gesehen wird erst ein Emulator für den Verbindungsaufbau des USB-Redirection-Protokolls gestartet, welcher danach die Kontrolle an einen speziellen USB-Emulator übergibt und sich danach um alle Anfragen des zu überprüfenden, virtualisierten Systems kümmert.

Jeder USB-Emulator übergibt ausgehende Pakete vor dem Senden an das Fuzzing-Modul, welches dabei einen Wrapper für die Send-Funktion darstellt. Das Fuzzing-Modul bezieht aus dem Testcase-Pool einen Testcase und wendet alle darin definierten Fuzzing-Instruktionen auf das ausgehende Paket an und übergibt das permutierte Paket in Form eines Byte-Arrays per Rückgabewert an die eigentliche Send-Routine. Die Permutation von eingehenden Daten an den USB-Emulator ist nicht erforderlich. Außerdem ermöglicht der Emulator auch das Permutieren von USB-Datenstrukturen, die als Teil des USB-Protokolls verschickt werden.

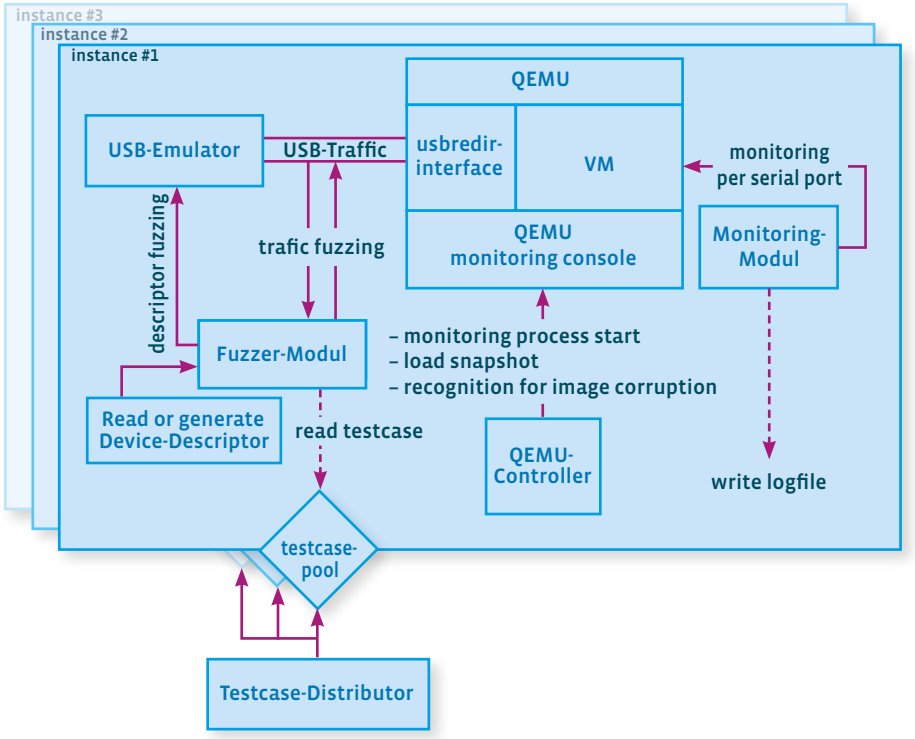


Abbildung 1: Software-Architektur

Für die Überwachung des zu überprüfenden Betriebssystems werden austauschbare Monitoring-Module verwendet. Der Grund hierfür liegt in den verschiedenen Möglichkeiten und Gegebenheiten, in Abhängigkeit des emulierten bzw. virtualisierten Betriebssystems. Das Linux- und FreeBSD-Monitoring-Modul überwacht ein serielles TTY-Terminal für die Erkennung von Abstürzen. Für die Überwachung ist somit keine direkte Interaktion zwischen dem Monitoring-Modul und dem Kernel bzw. einem hierfür entwickelten Treibers erforderlich, es genügt ein Parser für Kernel-Meldungen. Um den Informationsgehalt der Kernel-Ausgaben von unixoiden Betriebssystemen zu steigern, wird die Kernel-Verbosity auf den höchstmöglichen Wert eingestellt. Alternativ können auch permanent die Kernel-Logdateien gelesen werden. Abstürze lassen sich typischerweise anhand von entsprechenden Stack-Traces oder ähnlichen Ausgaben erkennen.

Falls ein Absturz erkannt wurde, wird der QEMU-Controller benachrichtigt, welcher dann die virtuelle Maschine auf ihren Anfangszustand zurücksetzt. Das Geschehen wird ferner zur späteren Analyse protokolliert.

Das Windows-Monitoring-Modul ist aktuell noch in der Entwicklung und erfordert mehr Aufwand, da ohne weiteres keine Möglichkeit besteht, die Kernel-Ausgaben auf den seriellen Port zu projizieren. Aktuell nutzt das Framework eine VNC-Verbindung für jede Instanz, über die dann per Farbwert eines aufgenommenen Bildschirmfotos auf einen möglichen Absturz geschlossen wird.

Das Framework erlaubt Multiprocessing und Clustering. Mit Hilfe von mehreren parallel arbeitenden Instanzen kann die Ausführgeschwindigkeit gesteigert werden. Die modulare Architektur erlaubt es, einzelne Instanzen autonom arbeiten zu lassen. Ein zusätzlicher Testcase-Distributor sorgt für die gleichmäßige Verteilung der Testcases an die einzelnen Instanzen. Der Testcase-Distributor kommuniziert mit den anderen Prozessen über verschiedene IPC-Schnittstellen. In der aktuellen Version verwenden wir eine MySQL-Datenbank für die Verteilung von Tasks in Netzwerken. Hierfür wird die Datenbank zu Beginn mit Tasks gefüllt und die konfigurierten Worker arbeiten diese dann verteilt ab.

Das vUSBf-Framework ermöglicht eine signifikante Steigerung der Ausführgeschwindigkeit, im Vergleich zu anderen USB-Fuzzing-Lösungen.

Das Framework bietet zwei Modi: Der Modus Reload, stellt nach jedem virtuellen Einstecken eines virtuellen USB-Gerätes den Zustand der virtuellen Maschine durch einen Snapshot wieder her. Der Vorteil bei dieser Variante ist, dass damit Testcases und deren Wirkung auf das zu untersuchende System isoliert werden. Dieser Modus erkennt Testcases, die alleine ohne weitere Mitwirkung eine Reaktion auslösen.

Die zweite Variante ist der Modus Non-Reload, welcher dem Facedancer-artigen Fuzzing nachempfunden ist. Bei diesem Modus wird der Zustand der virtuellen Maschine nur im Fehlerfall wiederhergestellt. Das heißt, falls der USB-Stack nicht mehr auf ein virtuelles Einstecken reagiert, wird der definierte Zustand, mithilfe eines Snapshots, wiederhergestellt. Dies hat unter anderem den Vorteil, dass mit diesem Modus Fehler oder Schwachstellen gefunden werden können, welche nur dann zu Abstürzen oder anderen fehlerhaften Reaktionen führen, falls eine Sequenz von bösartigen USB-Geräten eingesteckt wird. Gleichzeitig ist dieser Modus schneller.

Durch Multiprocessing auf mehreren CPUs eines Systems und Clustering über mehrere Systeme konnte beispielhaft die Berechnungszeit für 1 Million Testfälle von ca. 23 Tagen bei der sequenziellen Ausführung auf wenige Stunden (Multiprocessing über 16 CPU-Kerne) bis auf 50 Minuten (Multiprocessing + Clustering über drei Systeme) gesenkt werden. Die dargestellten Laufzeiten verdeutlichen den Nutzen des vUSBf-Frameworks und die Möglichkeit, eine systematische Untersuchung von mehreren

Gerätetreibern zu realisieren. Der limitierende Faktor entspricht hierbei nur der zur Verfügung stehenden Anzahl der Rechner bzw. der gegebenen Rechenleistung.

CAOS-Stick

Für Demonstrationszwecke und einfache Penetrationstests wurde der CAOS-Stick entwickelt. Diese Erweiterung des vUSBf-Framework erlaubt es, die gefundenen USB-Payloads, welche in Abstürzen der entsprechenden Betriebssysteme resultieren, mit einem Klick als Emulationsfirmware zu exportieren. Durch dieses Feature lassen sich gefundene Payloads nicht nur in virtuellen Umgebungen testen, sondern auch Bugs anhand von physikalischen Systemen verifizieren und somit Artefakte der verwendeten Virtualisierungslösung ausschließen. Da wir zum aktuellen Zeitpunkt Payloads für fast alle Server- bzw. Desktop-Betriebssysteme gefunden haben, die sich mindestens als Denial-of-Service Angriff ausnutzen lassen, wurde dieses Feature CAOS-Stick bzw. CAOS-Firmware genannt. Dabei steht der Name CAOS für das Akronym Crash Any OS.

Als Basis für den CAOS-Stick dient der Arduino Leonardo. Dieses Microcontroller-Board basiert auf dem Atmel ATmega32u4, welcher mit 16 Mhz getaktet ist. Der Microcontroller erlaubt es, den USB-Port, der gleichzeitig auch für die Stromversorgung verwendet werden kann, vollständig als USB-Device zu programmieren. Außerdem lässt sich der Microcontroller mit Hilfe des JTAG- und UART-Interface einfach debuggen.

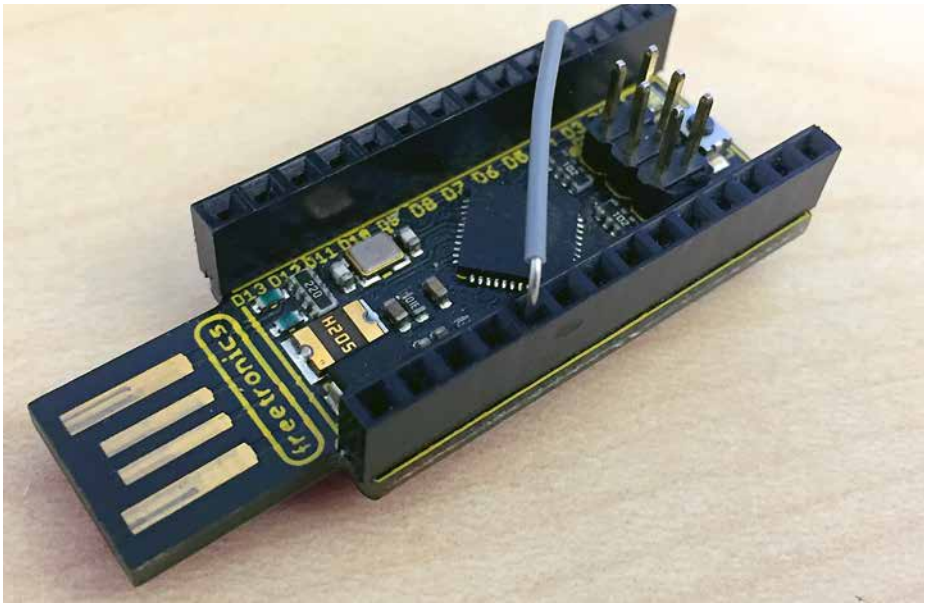
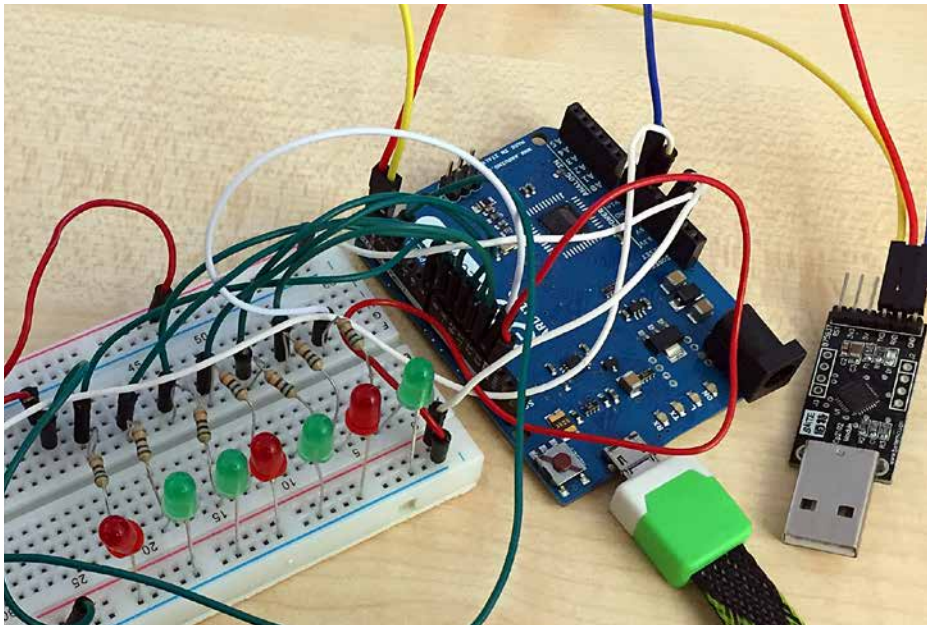


Abbildung 3: LeoStick-Hardware

Abbildung 2: Arduino Leonardo mit einem angeschlossenen UART-USB-Converter und einer Debug-Schaltung



Während der Entwicklung der ersten CAOS-Firmwares, verwendeten wir den üblichen Arduino Leonardo. Für Debug-Zwecke wurde außerdem eine minimalistische Schaltung und ein UART-USB-Controller an diesen angeschlossen.

Die finale Version des CAOS-Stick wird durch den LeoStick repräsentiert. Hierbei handelt es sich um ein zum Arduino Leonardo kompatibles Microcontroller-Board im Formfaktor eines USB-Sticks. Die CAOS-Firmwares lassen sich sowohl auf den LeoStick als auch auf den Arduino Leonardo flashen.

Die CAOS-Firmware basiert auf einer stark modifizierten Version des Arduino Leonardo SDKs. Dabei wurden Teile des USB-Codes modifiziert und an die entsprechenden Anforderungen angepasst. Hierfür werden Deskriptor-Informationen in Form von Strukturen automatisch generiert, in den Code integriert und durch modifizierte USB-Funktionsaufrufe innerhalb des Arduino-Codes ausgeführt. Die Payloads werden hierbei aus dem Flash-Speicher, welcher 32 Kilobytes groß ist, in den SRAM geladen. Dies ist erforderlich, da es sich um eine Harvard-Architektur-CPU handelt und die relativ geringe SRAM-Größe von 2,5 Kilobytes ansonsten ein Problem

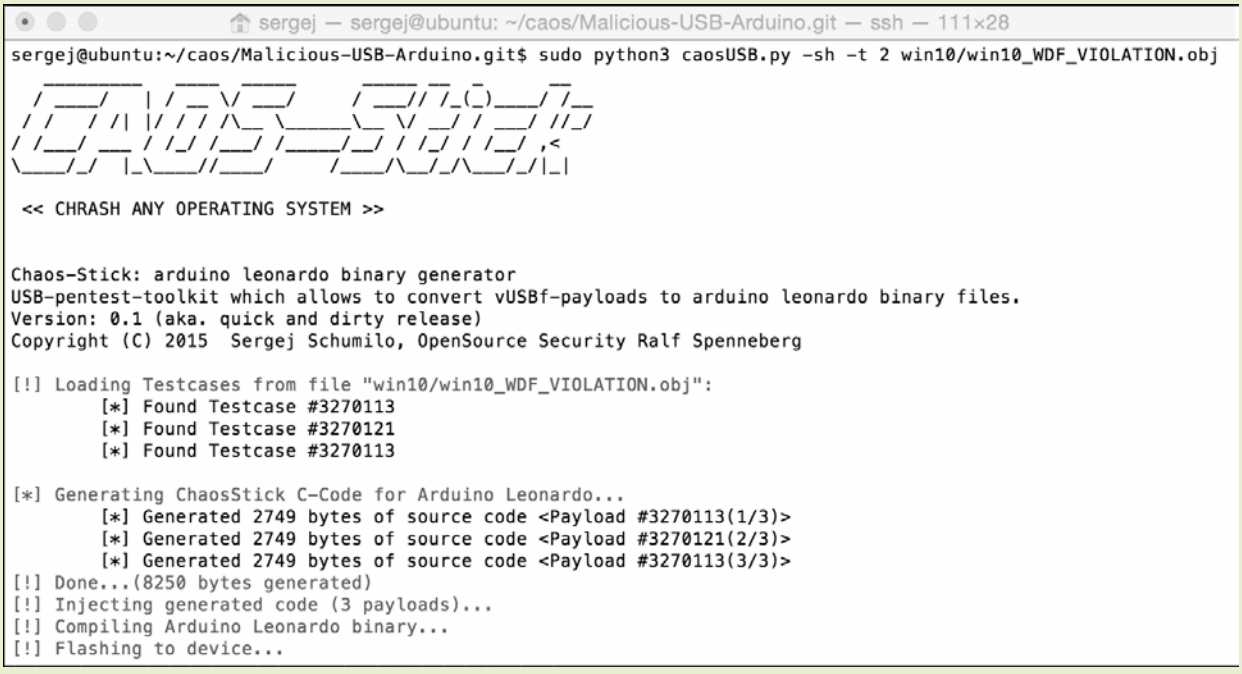


Abbildung 4: Generierung einer Microsoft Windows 10 CAOS-Firmware

darstellen würde. Nach der Generierung der entsprechenden Strukturen und des passenden Gluecodes, wird der Quelltext mit dem GCC-AVR kompiliert und in Form einer Hex-Datei bereitgestellt.

Mit Hilfe von Tools, wie zum Beispiel avrdude, lassen sich die generierten Hex-Dateien auf einen ATmega32u4 bestückten Microcontroller flashen.

Die CAOS-Firmware unterstützt auch Sequenzen mehrerer Payloads in einer Firmware. Diese Sequenzen lassen sich auch beliebig mit einstellbaren Timeouts konfigurieren. Außerdem lassen sich die übertragenen USB-Payloads mit Hilfe des UART-Ausgabe jederzeit nachvollziehen und für Debug-Zwecke ausgeben.

Um die automatische Übertragung von USB-Payloads zu unterbinden, wurde eine Prüfung der GPIO-Pins D3 und 5V eingebaut. Die CAOS-Firmware prüft zur Laufzeit, ob diese Kontakte verbunden sind und überträgt dann keine USB-Payloads. Dieser Modus wird benötigt um den Microcontroller nach dem Aufspielen einer CAOS-Firmware neu flashen zu können und um das Host-System bei einem Flash-Vorgang nicht zu einem Absturz zu bringen.

Gefundene Schwachstellen

Die bisher gefundenen Schwachstellen wurden gruppiert und analysiert. Anschließend wurden die erkannten Probleme an die Linux Maintainer gemeldet. Fast alle gefundenen Schwachstellen beziehen sich auf gerätespezifische Treiber, und somit nicht auf Treiber für generische USB-Klassen. Ein erstes Advisory wurde bereits veröffentlicht [secadv]. Die weiteren Schwachstellen werden in Zukunft ebenfalls veröffentlicht.

Betroffen sind etliche Kernel-Module in aktuellen Linux-Kernel Versionen. Zu dem größten Teil der gefundenen Fehlern zählen Nullpointer-Dereferenzierungen und Kernel-Paging-Requests. Die meisten gefundenen Fehler führen nur zu einer Kernel Oops. Kritisch ist aber die Tatsache, dass der Linux-Kernel eine Build-Option namens Panic-on-Oops hat, welche bei jeder auftretenden Kernel Oops zu einer Kernel Panic führt und das System somit zum Absturz bringt. Unter anderem verwendet RedHat Enterprise Linux diese Kernel-Option. Es ist somit anfällig für eine Vielzahl von Denial of Service-Attacken.

Des Weiteren wurden bereits Fehler in FreeBSD gefunden. Auch unter OS X gab es einen Fehler in einem Dritthersteller-Treiber. Ferner wurden etliche Sicherheitslücken in Windows Dritthersteller-Treiber, die automatisch beim Einstecken des CAOS-Stick mit Hilfe von Windows Update nachinstalliert werden, gefunden. Dazu zählen auch kritische und theoretisch sogar ausnutzbare Fehler, wie zum Beispiel stackbasierte Bufferoverflows.

Fazit

In der Vergangenheit wurden bereits mehrfach fehlende Sicherheitskonzepte und Gefahren bei der Verwendung des USB

aufgezeigt. Spätestens seit der BadUSB-Veröffentlichung fand eine umfassende Sensibilisierung für konzeptionelle Sicherheitsschwachstellen, auch in der Öffentlichkeit, statt. Darüber hinaus wurden immer wieder neue Schwachstellen in den Implementierungen der USB-Gerätetreiber gefunden, welche in Einzelfällen schwerwiegende Kompromittierungen erlauben. Bewährt hat sich für die Suche nach neuen Fehlern die USB-Fuzzing-Methode. Hierfür werden unerwartete oder ungültige Daten an den entsprechenden USB-Treiber geschickt, um Fehlverhalten oder Abstürze zu provozieren, wodurch dann auf Fehler in der Implementierung geschlossen und durch nachträgliche Untersuchungen die Ausnutzbarkeit bestimmt werden kann. Leider ist die Suche mit Hardware-basierten Lösungen sehr zeitaufwendig.

Das entwickelte USB-Fuzzing-Framework vUSBf ermöglicht eine automatisierte Suche nach solchen Schwachstellen und erlaubt eine Steigerung der Ausführgeschwindigkeit um fast drei Größenordnungen, im Vergleich zu sequenziell arbeitenden USB-Fuzzing Lösungen. Realisiert wird dies durch den Einsatz von etlichen parallel arbeitenden virtuellen Maschinen und die Verwendung von USB-Emulatoren, welche die benötigten USB-Daten bereitstellen, ohne physikalische Hardware vorauszusetzen. Durch das Clustering ist die Ausführgeschwindigkeit beliebig skalierbar. Des Weiteren werden gefundene Fehler in virtuellen Umgebungen umfassend dokumentiert und sind reproduzierbar. Mit dem CAOS-Stick lassen sich die gefundenen Abstürze auch auf physikalische Systeme übertragen und verifizieren. Dadurch können mögliche Artefakte der Virtualisierung ausgeschlossen werden.

Das entwickelte vUSBf-Framework bietet eine umfassende, automatisierte und systematische Untersuchung von USB-Gerätetreibern auf Implementierungsschwachstellen und ermöglicht auch die Entdeckung bisher unbekannter Fehler in deren Implementierung. Das vUSBf-Framework ist darüber hinaus vielseitig einsetzbar, wie zum Beispiel für Regressionstests bei der Treiberentwicklung oder für die Suche nach neuen Schwachstellen. Ferner lässt es sich durch die zur Verfügung gestellten Schnittstellen um weitere Funktionalitäten erweitern. Dank des automatischen Datei-Exportes von Testcases und CAOS-Firmwares, wird auch der Debug-Prozess für Kernel- oder Treiber-Entwickler erleichtert bzw. der Fehler-Report nachvollziehbar. ◆

References

[autorun] AutoRun changes in Windows 7. http://blogs.technet.com/b/srd/archive/2009/04/28/autorun-changes-in-windows-7.aspx

[teensy] Adrian Crenshaw. Programmable HID USB Keystroke Dongle, DEF CON 18. https://www.defcon.org/images/defcon-18/dc-18-presentations/Crenshaw/DEFCON-18-Crenshaw-PHID-USB-Device.pdf, 2010

[badUSB] Karsten Nohl, Sascha Krißler and Jakob Lell. BadUSB — On accessoriesthat turn evil. https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf, 2014

[usbbroken] Andy Greenberg. Why the Security of USB Is Fundamentally Broken. http://www.wired.com/2014/07/usb-security/.8 american fuzzy lop (http://lcamtuf.coredump.cx/afl/)
A-16 23. DFN-Konferenz „Sicherheit in vernetzten Systemen“

[davis] NCC Group Andy Davis. Lessons learned from 50 bugs: Common USB driver vulnerabilities. https://www.nccgroup.com/media/190706/usb_driver_vulnerabilities_whitepaper_january_2013.pdf

[secadv] Sergej Schumilo, Hendrik Schwartke, Ralf Spenneberg. OS-S Security Advisory 2015–04 (usbvision driver). http://os-s.net/advisories/DOS-KernelCrashesOnInvalidUSBDeviceDescriptors-UsbvisionDriver.pdf

Sicherheit aktuell

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

Neue CA-Hierarchie in der DFN-PKI

Das Wurzelzertifikat „Deutsche Telekom Root CA 2“, der bisherigen DFN-PKI im Sicherheitsniveau „Global“, läuft 2019 ab. Da 39 Monate lang gültige Zertifikate unter dieser Root ab Mai 2016 nicht länger ausgestellt werden können, muss eine neue Hierarchie eingesetzt werden. Der DFN-Verein setzt die erfolgreiche Zusammenarbeit mit T-Systems fort und bleibt zur Sicherstellung der Browserverankerung unter einer Root-CA von T-Systems. Diese neue Root-CA heißt „T-TeleSec GlobalRoot Class 2“. Mit dieser neuen Root-CA kann die DFN-PKI auch nach 2019 weiter eingesetzt werden. Die alte Hierarchie bleibt bis zum Ablauf des Root-Zertifikats weiter nutzbar – nach Ablauf jedoch mit sukzessive kürzeren Laufzeiten der neu ausgestellten Zertifikate. Die DFN-PCA informiert die Teilnehmer an der DFN-PKI rechtzeitig über die notwendigen Schritte zur Umstellung. ◆

Neues Zertifikatprofil „Must Staple“

OCSP-Stapling ist ein sinnvoller Weg, Sperrinformationen für Zertifikate von Webservern an Browser auszuliefern. OCSP-Stapling erhöht nicht nur die Geschwindigkeit von Webseitenaufrufen, sondern schützt auch die Privatsphäre des Besuchers der Webseite. Um dieses Verfahren weiter zu unterstützen, bietet die DFN-PKI ab Ende März 2016 ein Zertifikatsprofil an, in dem die Erweiterung „Must Staple“ gesetzt ist. Dies verhindert, dass Angreifer auf Webserver mit einer Man-In-The-Middle-Position die Sperrinformation unterdrücken, um dem Besucher fälschlicherweise ein ungesperrtes Zertifikat vorzutäuschen. Dieses Profil wird automatisch verfügbar sein und kann beim Ausstellen des Zertifikats vom Teilnehmerservice-Mitarbeiter optional ausgewählt werden. ◆
https://blog.pki.dfn.de/2015/03/mehr-privacy-fuer-den-nutzer-ocsp-stapling/

ETSI Audit 2015 abgeschlossen

Im November 2015 wurde das jährliche Audit der DFN-PKI (Global) nach ETSI TS 102 042 durchgeführt und nach erfolgreichem Abschluss das entsprechende Zertifikat erneut ausgestellt. Das Audit besteht aus zwei Teilen: Der Hauptteil findet bei der DFN-PCA in Hamburg statt. Zusätzlich gibt es angekündigte und vorbereitete Besuche bei Teilnehmern der DFN-PKI, bei der die Arbeit des Teilnehmerservice stichprobenartig untersucht wird. Vielen Dank an alle Einrichtungen, die auch dieses Jahr ein erfolgreiches Audit der DFN-PKI ermöglicht haben! ◆

DDoS-Abwehr im X-WiN

Derzeit baut der DFN-Verein eine DDoS-Abwehrplattform im XWiN auf. Diese Plattform besteht aus zwei Hauptkomponenten: Zum einen der Analysekomponente (NeMo), welche dem NOC und dem DFN-CERT Anomalien im X-WiN meldet und zur Analyse aufbereitet. Zum anderen der Komponente zur DDoS-Mitigation. Diese kann direkt aus NeMo gesteuert werden und setzt die Maßnahmen zur Abwehr von schädlichem Verkehr um. Sie besteht aus derzeit vier virtuellen Maschinen, die auf speziellen Einschüben (VSM – Virtualized Service Module) direkt in den inneren SuperCore-Routern des X-WiN laufen. Die Software auf diesen Maschinen steuert über BGP-Flowspec das Routing des Schadverkehrs. Darüber hinaus kann entsprechender Verkehr auf den VMs feingranular gefiltert werden. Die DDoS-Abwehrplattform wird vom NOC zum Schutz des X-WiN eingesetzt. Ein entsprechender Dienst, um auch Ressourcen von Teilnehmern am X-WiN schützen zu können, befindet sich derzeit in der Vorbereitung und wird voraussichtlich noch 2016 in Betrieb gehen. ◆

Lieber sicher ins eduroam

eduroam ist der Kommunikationsdienst des DFN-Vereins, der reisenden Wissenschaftler(inne)n den unbeschwerten Zugang zum X-WiN ermöglicht. Der Dienst wurde 2003 erstmals den Einrichtungen im DFN angeboten und erfreut sich seither steigender Beliebtheit. Aktuell (Stand Frühjahr 2016) nehmen am Dienst eduroam ca. 380 Einrichtungen teil. Zusätzlich zu den über 1000 eduroam Standorten (s. www.eduroam.de), gibt es in mehreren Deutschen Städten im Rahmen des „eduroam off campus“ sogenannte eduroam Service Provider, die den Dienst in Hotels, Gaststätten, Restaurants und in Bussen und Bahnen anbieten. International ist eduroam ebenfalls bestens aufgestellt, so können eduroam Nutzer(innen) mittlerweile in ca. 80 Territorien weltweit den Dienst eduroam nutzen.

Schon längst ist eduroam keine Domäne der Informatik mehr, so nutzen Wissenschaftler(innen) aus allen Fachdisziplinen den Dienst eduroam.

Zur Authentifizierung der Nutzer in eduroam kommen Standardprotokolle zum Einsatz, die ein hohes Maß an Sicherheit bieten. eduroam zählt weltweit zu den sichersten Authentifizierungsinfrastrukturen. Voraussetzung dafür ist die korrekte Konfiguration der jeweiligen Geräte, die in eduroam genutzt werden sollen.

Die Authentifizierung in eduroam erfolgt in der Regel mit der Eingabe der Kennungen und des Passwortes. Damit Kennungen und Passwörter sicher übertragen werden, bietet die DFN-Geschäftsstelle einen Konfigurationsassistenten an, der Profile für die gängigen Betriebssysteme (ANDROID 4.3+, Mac OS X, MS Windows Vista, 7, 8, 8.1, 10 und Linux) bereitstellt.

Der Konfigurationsassistent, der im Rahmen des Projekte GN3, GN3plus, und GN4 entwickelt und von der DFN-Geschäftsstelle angepasst wurde, ist unter der URL https://cat.eduroam.de erreichbar.

Den Konfigurationsassistenten kann jeder eduroam Identity Provider, also Einrichtungen, die Nutzer ins eduroam bringen, nutzen. Für die Teilnahme ist eine Registrierung mit einem gültigen Nutzerzertifikat der DFN-PKI (Global) erforderlich. Nach Kontaktaufnahme erhält man ein Einladungstoken, mit dem die Registrierung abgeschlossen werden kann. Die Konfiguration des Konfigurationsassistenten ist einfach gestaltet und richtet sich nach dem jeweiligen Authentifizierungsverfahren, welches der Administrator für seine Einrichtung gewählt hat. Die Profile werden dann gemäß den Vorgaben des Administrators automatisch generiert. Zur Kontaktaufnahme und bei Fragen schickt man eine E-Mail an roaming@dfn.de. ◆

Kontakt

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

Second Hand Software im Paket

Bundesgerichtshof geht weiteren Schritt zur Liberalisierung des Handels mit „Gebrauchtsoftware“

Mit der Frage der Zulässigkeit des Handels mit sogenannten „Gebrauchtlizenzen“ von Software haben sich die Gerichte in der Vergangenheit bereits mehrfach befassen müssen (vgl. Försterling in DFN-Infobrief Recht 5/2012, S. 8 ff.). In einem Urteil des Bundesgerichtshofs (BGH) vom 11. Dezember 2014, dessen Begründung seit dem 16. Juni 2015 vorliegt (BGH, I ZR 8/13 – UsedSoft III), führt der BGH seine bisherige Rechtsprechung fort und erweitert die Voraussetzung zugunsten eines wirksamen Erwerbs gebrauchter Software. Er bejaht eine Erschöpfung des Verbreitungsrechts nunmehr nicht nur hinsichtlich der heruntergeladenen Kopie des Ersterwerbers, sondern darüber hinaus – und das war bislang ungeklärt – auch hinsichtlich derjenigen Kopie, die der Ersterwerber selbst zum Zwecke der Weitergabe an einen Zweiterwerber anfertigt. Die Entscheidung öffnet damit dem Gebrauchtsoftwarehandel die Türen für die Aufspaltung sog. Volumenlizenzen – dies sind Lizenzen, die als gebündeltes Paket veräußert werden und die die Nutzung einer bestimmten Anzahl eigenständiger Kopien des Computerprogramms erlauben.

Text: **Clara Ochsenfeld** (Forschungsstelle Recht im DFN)

Foto © benstevens/iStockphoto.de

Einordnung der Problematik

Das deutsche und europäische Recht schützt die Erfinder und Hersteller von Computerprogrammen grundsätzlich dahingehend, dass dem Rechtsinhaber gem. § 69c Nr. 3 S. 1 Urheberrechtsgesetz (UrhG) das ausschließliche Recht der Verbreitung und Vervielfältigung seines Computerprogramms zusteht. Der Schutz findet jedoch seine Grenzen, wenn ein Vervielfältigungsstück des Programmes mit Zustimmung des Rechtsinhabers im Gebiet der Europäischen Union […] im Wege der Veräußerung in den Verkehr gebracht worden ist (sog. Erschöpfungsgrundsatz). In diesem Fall erschöpft sich gem. § 69c Nr. 3 S. 2 UrhG das Verbreitungsrecht in Bezug auf dieses Vervielfältigungsstück. Das bedeutet, dass in diesem Fall der urheberrechtliche Schutz zugunsten eines der Allgemeinheit dienenden freien Warenverkehrs zurücktreten muss, soweit der Rechteinhaber eine entsprechende Vergütung für das Vervielfältigungsstück erhalten hat. Sinn und Zweck dieser Regelung ist es demnach, die Verbreitung rechtmäßig veräußerter Werkstücke zu erleichtern, diese nicht durch daran fortbestehende Rechte zu beschränken und letztlich klare und übersichtliche Verhältnisse im Rechtsverkehr zu schaffen. Die Wirkung der Erschöpfung entfaltet sich grundsätzlich gegenüber jedermann und führt dazu, dass die in Verkehr gebrachten Werkstücke im Interesse der Verwerter und der Allgemeinheit an einem freien Warenverkehr für jede Weiterverbreitung frei werden.

Durch die Rechtsprechung des EuGH (Urteil vom 3. 7. 2012 – C-128/11 – Oracle/UsedSoft) und anschließend des BGH (Urteil vom 17.7.2013 - I ZR 129/08 - UsedSoft II) war die grundsätzliche Problematik der sog. „Online-Erschöpfung“ gebrauchter Software bereits gelöst worden (vgl. Försterling in DFN-Infobrief Recht 5/2012 S. 8 ff.). Der EuGH stellte in seiner Entscheidung die Online-Übermittlung (z. B. durch einen Download) der körperlichen Weitergabe (z. B. auf einem Datenträger) unter der Voraussetzung gleich, dass dem Ersterwerber ein unbegrenztes Nutzungsrecht eingeräumt wurde und dieser seine eigene Programmkopie löscht. Die Löschung der eigenen Programmkopie ist insoweit erforderlich, als die sog. „Online-Erschöpfung“ gerade nicht dazu führen soll, dass sich die Anzahl der berechtigten Nutzer erhöht, sondern lediglich sichergestellt werden soll, dass ebenso wie im analogen Bereich die Verkehrsfähigkeit und damit die Weitergabe eines geschützten Werkes ermöglicht wird. Lediglich am Rande ging der BGH hier auf die Frage ein, wann ein ausreichender Nachweis für das Löschen der eigenen Programmkopie vorliegt und ließ sie letztlich offen. Allerdings ließ er durchdringen, dass eine notarielle Bestätigung über die Erklärung des Ersterwerbers darüber, die Kopien entfernt zu haben, nicht genüge.

Bislang durch die höchstrichterliche Rechtsprechung noch ungeklärt war die Frage, ob das Verbreitungsrecht sich auch hinsichtlich einer Zweitkopie, also einer Kopie, die durch den Ersterwerber für den Zweiterwerber angefertigt wird, erschöpft. Dies hat der BGH mit seiner Entscheidung nun bejaht und damit den Weg für den Handel mit Gebrauchtsoftware, die durch den Ersterwerber im Rahmen von Volumenlizenzverträgen erworben wurde, geebnet.

Sachverhalt der Entscheidung

In dem der Entscheidung zugrundeliegenden Sachverhalt erwarb eine Bildungseinrichtung 40 zeitlich unbegrenzte Softwarelizenzen von einem Softwareunternehmen, welches die ausschließlichen urheberrechtlichen Nutzungsrechte an der veräußerten Software hält. Die Einrichtung erhielt die Software aufgrund der Teilnahme an einem Vertragslizenzprogramm für Bildungseinrichtungen vom veräußernden Unternehmen zu vergünstigten Konditionen. Eine Vertragsklausel bestimmte, dass die erworbenen Lizenzen nicht übertragbar sind und ausschließlich zum Zweck der internen Verteilung innerhalb der Bildungseinrichtung genutzt werden dürfen. Die Bildungseinrichtung erhielt das für die Installation der Software notwendige sog. Enduser-License-Agreement (EULA) sowie eine Seriennummer, mittels derer sie sich die entsprechende Software im Internet vom Kundenportal des Herstellers herunterlud und auf Installationsdatenträgern (sog. „Media-Kit-Datenträgern“) speicherte. Im Anschluss an den Erwerb veräußerte die Einrichtung die Software – ohne diese zuvor auf ihren Rechnern installiert zu haben – dann zu einem höheren Preis an einen Händler für sog. „Gebrauchtsoftware“, der zwei der Lizenzen nebst einem Media-Kit-Datenträger mit dem darauf gespeicherten EULA seinerseits an einen Dritten weiterveräußerte. Das Softwareunternehmen sah in der Weiterveräußerung eine Verletzung seines urheberrechtlichen Verbreitungsrechts und verklagte den Händler für Gebrauchtsoftware auf Unterlassung und Schadensersatz.

Entscheidung des BGH

Der BGH hat die Revision des Softwareunternehmens als unbegründet zurückgewiesen. Begründet wurde dies damit, dass das klagende Softwareunternehmen dem Herunterladen einer Kopie des Computerprogramms zugestimmt hatte und der erwerbenden Bildungseinrichtung 40 Lizenzen einräumte. Somit gestattete es die Herstellung von insgesamt 40 einzelnen Kopien zur Installation an 40 eigenständigen Arbeitsplätzen. Die Zustimmung des klagenden Softwareunternehmens belief sich somit nicht nur auf das Herunterladen einer Kopie der Computerprogramme, sondern erstreckte sich auch darauf, 40 eigenständige Kopien herzustellen. Der BGH bejaht eine Erschöpfung nunmehr auch hinsichtlich dieser weiteren vom Ersterwerber angefertigten Kopien. Dies begründet er vornehmlich damit, dass eine wirtschaftliche Betrachtungsweise, aufgrund der aufgestellten Grundsätze des EuGH zur Online-Erschöpfung, geboten sei. Der BGH geht davon aus, dass der Fall, in dem der Rechtsinhaber dem Herunterladen des Com-

puterprogramms und der Anfertigung einer weiteren Kopie zustimmt, hinsichtlich der Erschöpfung des Verbreitungsrechts nicht anders zu beurteilen sei als der Fall, dass der Rechtsinhaber der Veräußerung in einer entsprechenden Anzahl körperlichen Datenträger zustimmt. Die Erschöpfung trete unabhängig davon ein, dass sich das Softwareunternehmen nur mit einer Nutzung des Programms durch Bildungseinrichtungen einverstanden erklärt hat. Der Erschöpfungsgrundsatz könne nicht vertraglich abbedungen werden, sodass sich das Softwareunternehmen gerade nicht auf eine vertragliche Vereinbarung mit dem Ersterwerber berufen könne, die die Zustimmung der Nutzung durch Bildungseinrichtungen begrenzt. Der weitere Vertrieb eines Werkstücks, das mit Zustimmung des Rechteinhabers im Wege der Veräußerung in den Verkehr gebracht wurde, ist vom Berechtigten im Anschluss laut BGH nämlich nicht mehr kontrollierbar. Eine wirksame Beschränkung gegenüber dem Ersterwerber wirke demnach nicht dahingehend, dass auch der weitere Vertrieb auf diese Beschränkung hin überprüft werden könne.

Das klagende Softwareunternehmen konnte darüber hinaus nicht mit dem Argument durchdringen, das durch die Bildungseinrichtung gezahlte Entgelt für die Softwarelizenzen sei allein zur Nutzung nichtkommerzieller Zwecke angemessen gewesen. Denn bereits der EuGH hatte in seiner Entscheidung festgelegt, dass es grundsätzlich ausreicht, wenn der Rechtsinhaber die Möglichkeit hatte beim Erstverkauf der betreffenden Kopie eine angemessene Vergütung zu erzielen. Das Softwareunternehmen habe hier die Möglichkeit gehabt, die Zustimmung zum Herunterladen der Kopie von der Zahlung eines Entgeltes abhängig zu machen und eine angemessene Vergütung zu erzielen. Es komme demnach nicht darauf an, ob dieses Entgelt lediglich unter der Voraussetzung einer beschränkten Nutzergruppe für angemessen gehalten wurde.

Der BGH hat in seiner Entscheidung jedoch darüber hinaus klargestellt, dass eine Aufspaltung nur dann möglich ist, wenn es sich um sog. Volumenlizenzen über Einzelplatzsoftware handelt und die Kopien in entsprechender Anzahl der Veräußerung beim Ersterwerber unbrauchbar gemacht wurden. Bei den einzelnen Lizenzen handele es sich demnach um eigenständige Nutzungsrechte, die eigenständig übertragen werden können. Dies gilt jedoch nicht im Falle sog. Client-Server-Lizenzen, also Software, die auf einem Server gespeichert wird und die Nutzung des Programms durch mehrere Personen gestattet wird, ohne dass einzelne Kopien angefertigt werden. In diesem Fall liegt die Voraussetzung der Löschung insofern nicht vor, als diese nach wie vor auf dem Server des Ersterwerbers liegt. Der Nacherwerber kann sich folglich nur dann auf den Erschöpfungsgrundsatz berufen, wenn die Kopien in entsprechender Anzahl seines Erwerbs beim Ersterwerber unbrauchbar gemacht wurden.

Fazit und Hinweise für die Hochschulen

Für die Hochschulen und Bildungseinrichtungen kann die Entscheidung des BGH sowohl positive als auch negative Auswirkungen hervorrufen. Positiv insoweit, als die weitere Öffnung eines Gebrauchtmarktes für Software auch ihnen die Möglichkeit gibt, Software vergünstigt aus zweiter Hand zu beziehen. Hierbei sollte jedoch beachtet werden, dass die Anforderungen an die Darlegungs- und Beweislast des Zweiterwerbers, der sich auf die Löschung der Kopie beim Ersterwerber beruft, noch nicht abschließend geklärt sind. Im Falle des Erwerbes von Gebrauchtsoftware sollten die Hochschulen demnach insbesondere auf geeignete Nachweise bezüglich des Entfernens der jeweiligen Kopien beim Ersterwerber achten und insoweit ihre Rechtsabteilung in den Erwerbsvorgang miteinbeziehen. Negative Auswirkung kann die Entscheidung insoweit haben, als die Softwareunternehmen die finanzielle Begünstigung und Gewährung von Rabatten beim Erwerb von Volumenlizenzen in Zukunft einschränken könnten, da für sie nicht gewährleistet werden kann, dass die Software nur für die vereinbarten Zwecke von einem bestimmten Nutzerkreis verwendet wird.

Darüber hinaus ist insbesondere bei der Veräußerung von Software durch die Hochschulen und Forschungsinstitute an einen Gebrauchthändler äußerste Vorsicht geboten. Bei der Veräußerung von Software ist nämlich stets zwischen der schuldrechtlichen und urheberrechtlichen Ebene zu unterscheiden. Schuldrechtliche Absprachen bestehen und wirken grundsätzlich nur zwischen den jeweiligen Vertragsparteien. Das Urheberrecht hingegen beinhaltet dingliche Rechte, die gegenüber jedermann wirken. Das dargestellte Urteil betrifft nur das Verhältnis Softwarehersteller (bzw. Rechteinhaber) und Zweiterwerber (Gebrauchtsoftwarehändler). Zu unterscheiden ist demnach das Verhältnis zwischen Softwarehersteller und Ersterwerber. Die Softwareüberlassungsverträge zwischen Hersteller und Ersterwerber enthalten nämlich oftmals schuldrechtliche Klauseln, die einer Weiterveräußerung an Dritte entgegenstehen und Schadensersatz- sowie Unterlassungsansprüche des Softwareunternehmens nach sich ziehen können, soweit sie Wirksamkeit entfalten. Im Falle einer Veräußerung der Software ist demnach ebenfalls immer die Rechtsabteilung der Institution miteinzubeziehen, die die entsprechenden Klauseln genau prüfen kann. ◆

Was lange währt … muss nicht immer gut sein

Rechtliche Probleme bei dem Angebot und der Nutzung einer automatischen E-Mail-Weiterleitung an Hochschulen

Die Nutzung einer automatischen E-Mail-Weiterleitung von der universitären E-Mail-Adresse auf eine private E-Mail-Adresse erfreut sich unter Hochschulmitgliedern seit Jahren großer Beliebtheit. Rechtlicher Risiken war man sich dabei meistens überhaupt nicht bewusst, sodass diese Praxis lange bedenkenlos Bestand hatte. Dass dieses Verhalten jedoch keineswegs ohne Weiteres rechtlich zulässig ist, soll in diesem Beitrag aufgezeigt werden, um Hochschulen zu animieren, die Aufrechterhaltung einer solchen Service-Option kritisch zu überdenken.

Text: **Florian Klein** (DFN-Verein)

Foto © BastianDietz/photocase.com

I. Hintergrund

Zu dem Service-Angebot einer Hochschule gehört es in aller Regel, dass Studierenden und Mitarbeitern ein eigener E-Mail-Dienst mit speziellen Hochschul-Mail-Adressen zur Verfügung gestellt wird, der über hochschuleigene Server betrieben wird. Einigen Hochschulmitgliedern ist die Nutzung eines solchen Dienstes jedoch zu unkomfortabel, weil sie bereits eine eigene private E-Mail-Adresse besitzen und ihre Kommunikation deshalb bevorzugt darüber abwickeln möchten. Um dies zu ermöglichen, bieten Hochschulen zusätzlich meist die Option an, im System eine private E-Mail-Adresse zu hinterlegen, auf die sämtliche E-Mails, die an die Hochschul-Mail-Adresse des jeweiligen Nutzers adressiert sind, automatisch weitergeleitet werden. Zum Teil kann dabei auch ausgewählt werden, ob im Hochschulpostfach zumindest eine Kopie der eingehenden und automatisch weitergeleiteten E-Mails abgelegt werden soll. Ist diese Einstellung einmal aktiviert, endet die Weiterleitung erst, wenn man diese manuell deaktiviert. Bis zu diesem Zeitpunkt werden alle E-Mails ohne jegliche menschliche Kontrolle des Inhalts an einen externen E-Mail-Provider weitergereicht, der dem Nutzer seine private E-Mail-Adresse zur Verfügung stellt. Dies kann in vielen Fällen dazu führen, dass kritische Informationen und Daten die Einflusssphäre der Hochschule verlassen und auf Servern landen, die keiner Kontrolle der Hochschule mehr unterliegen. Führt man sich dies vor Augen, drängen sich in Zeiten einer steigenden Bedeutung des Datenschutzes unweigerlich Zweifel auf, ob dies im Hinblick auf dienstliche Daten tatsächlich mit den geltenden Gesetzen vereinbar ist.

II. Rechtliche Betrachtung

Aus rechtlicher Sicht gibt es bei einer automatischen E-Mail-Weiterleitung in erster Linie vier Problemfelder: das Datenschutzrecht, den strafrechtlichen Geheimnisschutz, das Arbeitsrecht und das Informationsfreiheitsrecht. Vorab ist aber darauf hinzuweisen, dass viele rechtliche Fragen in diesem Zusammenhang kein Spezifikum der automatischen E-Mail-Weiterleitung sind, sondern sich durchaus auch bei einer manuellen, individuellen Weiterleitung stellen können. Eine Besonderheit ergibt sich allerdings aus der fehlenden inhaltlichen Kontrollmöglichkeit bei einer automatischen E-Mail-Weiterleitung, da diese sich ja gerade dadurch auszeichnet, dass jede Mail unterschiedslos weitergeleitet wird. Kann im Einzelfall deshalb überhaupt nicht festgestellt werden, welche Daten und Inhalte weitergeleitet werden, ist für die Beurteilung der rechtlichen Zulässigkeit im Zweifel davon auszugehen, dass darunter auch kritische Inhalte sind, für deren Weitergabe spezielle rechtliche Anforderungen bestehen, zumal E-Mails sehr häufig Daten beinhalten, die dem Datenschutzrecht unterliegen.

Um den verschiedenen rechtlichen Fragen in hinreichendem Maße gerecht werden zu können, befasst sich dieser Beitrag zunächst nur mit dem Datenschutzrecht. Der zweite Teil befindet sich im DFN-Infobrief Recht vom Juli 2015.

1. Rechtliche Beurteilung bei Mitarbeitern

Hochschulen sind in vielen Fällen als Körperschaften des öffentlichen Rechts organisiert. In Nordrhein-Westfalen legt dies beispielsweise § 2 Abs. 1 S. 1 Hochschulgesetz NRW (HG NRW) fest. Insofern ergibt sich, dass die jeweiligen Landesdatenschutzgesetze für staatliche Hochschulen als öffentliche Stellen zur Anwendung kommen und Datenverarbeitungen der Hochschulen deshalb an deren Maßstab zu messen sind. Da jedes Bundesland ein eigenes Landesdatenschutzgesetz erlassen hat, erfolgt die Darstellung hier exemplarisch anhand des nordrhein-westfälischen Datenschutzgesetzes. Die meisten Ausführungen lassen sich jedoch auf die anderen Bundesländer übertragen, da die wesentlichen Grundsätze in allen Bundesländern sehr ähnlich sind.

Die erste Differenzierung, die bei der rechtlichen Betrachtung vorzunehmen ist, ist die zwischen Mitarbeitern der Hochschule und Studierenden, da insofern unterschiedliche Regelungen zu beachten sind. Mitarbeiter sind Teil der Hochschule und ihr Verhalten wird dieser zugerechnet, soweit sie zur Erfüllung ihrer Aufgaben tätig werden und in einem Arbeits- bzw. Beamtenverhältnis zu ihr stehen. Insofern ergeben sich aus dem Status als Beamter oder Angestellter im öffentlichen Dienst keine Unterschiede. Dienstliche Tätigkeiten der Mitarbeiter werden somit nach dem für die Hochschule geltenden Datenschutzrecht beurteilt, wobei die Hochschule nach außen die für diese Datenverarbeitungen verantwortliche Stelle ist.

Relevante Datenverarbeitung

Ausgangspunkt jeder datenschutzrechtlichen Betrachtung ist die Feststellung, ob personenbezogene Daten in einer Weise verarbeitet werden, die vom Datenschutzgesetz erfasst ist. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 DSG NRW). In Bezug auf die Daten, die typischerweise in einer E-Mail enthalten sind, sind dies beispielsweise (personalisierte) E-Mail-Adressen, Namen, Kontaktdaten und Ähnliches. Werden also E-Mails automatisch an eine andere Adresse weitergeleitet, sind in aller Regel auch personenbezogene Daten betroffen.

Problematisch ist dies dann, wenn in der Weiterleitung der E-Mails eine Datenverarbeitung zu sehen ist. Zu denken ist vorrangig an eine Datenübermittlung. Als Übermitteln definiert das Gesetz das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die verantwortliche Stelle weitergegeben oder

zur Einsichtnahme bereitgehalten werden […]. Dabei soll eine Übermittlung nicht nur dann vorliegen, wenn der Empfänger die personenbezogenen Daten tatsächlich zur Kenntnis nimmt, sondern auch schon dann, wenn er nur die faktische Möglichkeit hat, die Daten tatsächlich zur Kenntnis zu nehmen. Warum diesem Übermittlungsbegriff ein derart weites Verständnis zugrunde gelegt wird, erschließt sich bei einem Blick auf den Sinn und Zweck der Regelungen zur Datenübermittlung: es geht nämlich primär darum, jegliche gezielte Ausweitung des Personenkreises, dem die personenbezogenen Daten zugänglich sind, zu verhindern und eine solche droht schon dann, wenn nur die faktische Möglichkeit der Kenntnisnahme besteht.

Dritter ist im Fall der automatischen E-Mail-Weiterleitung, bei der ein Mitarbeiter seine eingehenden E-Mails an eine private E-Mail-Adresse weiterleiten lässt, nicht der Mitarbeiter als Inhaber der E-Mail-Adresse, sondern dessen Mail-Provider. Sofern es nicht um hochschulinterne Weiterleitungen geht, bei denen diese Problematik nicht besteht, ist der Anbieter des Mailing-Dienstes weder Teil der Hochschule noch steht er in einem besonderen Verhältnis zu ihr, sodass er sich außerhalb der verantwortlichen Stelle befindet.

Damit eine datenschutzrechtlich relevante Übermittlung vorliegt, müssten die jeweiligen Daten also auch durch die Hochschule an den Mail-Provider weitergegeben werden. Der Begriff der Weitergabe erfasst jede Handlung, durch die die in den Daten enthaltenen Informationen in den Bereich des Empfängers gelangen. Auch wenn der Zweck der E-Mail-Weiterleitung nicht darin liegt, seinem privaten E-Mail-Provider Informationen zu verschaffen, gelangen dadurch die Daten aus allen dienstlichen E-Mails in dessen Machtbereich und können theoretisch von diesem eingesehen werden, solange die Inhalte nicht verschlüsselt sind. Schon auf dem Transportweg werden E-Mails häufig mit Postkarten verglichen, da sie leicht abgefangen und die Inhalte ausgelesen werden können. Sind sie aber erst auf dem fremden Mail-Server eingegangen, kann der Mail-Provider erst recht faktisch ohne Probleme auf sie zugreifen.

Selbst wenn zum Teil gefordert wird, dass eine tatsächliche Kenntnisnahme der Daten durch den Dritten erfolgt, ist eine solche Kenntnisnahme nicht immer auszuschließen, da beispielsweise Anbieter wie Google tatsächlich E-Mail-Inhalte scannen und – mindestens zu Werbezwecken – automatisiert auswerten. Als Gegenpol dazu stehen unter anderem die deutschen Anbieter, die an das Fernmeldegeheimnis gebunden sind und die deshalb nicht auf die E-Mail-Inhalte zugreifen dürfen. Dies schließt einen Zugriff allerdings nur rechtlich und keineswegs faktisch aus. Auch diese haben also die tatsächliche Möglichkeit einer Kenntnisnahme, sodass im Zweifel selbst bei diesen eine Weitergabe zu bejahen sein dürfte.

Dass diese Weitergabe auch durch die Hochschule als verantwortliche Stelle erfolgt, ergibt sich daraus, dass der jeweilige Hochschulmitarbeiter die automatische E-Mail-Weiterleitung aktiviert und damit die Weitergabe der Daten sämtlicher eingehender E-Mails veranlasst hat. Dieses Verhalten muss sich die Hochschule zurechnen lassen.

Es ist allerdings darauf hinzuweisen, dass diese Konstellation einer automatischen E-Mail-Weiterleitung in der Rechtswissenschaft bisher kaum diskutiert wurde. Dennoch lässt sich als weiteres Argument für die Einordnung als Datenübermittlung eine Parallele zum Cloud-Computing anführen. Zwar gibt es dieses in verschiedensten Ausprägungen, doch ist eine davon die Bereitstellung von Speicherplatz auf Servern des externen Diensteanbieters für den Cloud-Nutzer. Nimmt jemand einen solchen Dienst in Anspruch und verlagert seine Daten in den Cloud-Speicher, erfolgt dies nicht mit der Intention, dass der Cloud-Anbieter diese zur Kenntnis nehmen soll, sondern dient vorwiegend der Arbeitserleichterung, da die Daten von überall über das Internet abrufbar sind und man sich das Vorhalten eigener großer Speichermedien ersparen kann. Dennoch ist der Cloud-Anbieter faktisch in der Lage, die gespeicherten Daten zur Kenntnis zu nehmen. Hier besteht also eine Konstellation, die der E-Mail-Weiterleitung sehr ähnlich ist, da in beiden Fällen externe Diensteanbieter faktisch Zugriffsmöglichkeiten auf fremde Daten erhalten, auch wenn die Ausnutzung dieser Zugriffsmöglichkeiten vom Nutzer nicht gewollt ist.

Im Hinblick auf das Cloud-Computing mithilfe externer Diensteanbieter besteht weitgehend Einigkeit, dass dieses als sogenannte Auftragsdatenverarbeitung zu qualifizieren ist. Die Auftragsdatenverarbeitung (§ 11 DSG NRW) ist ein rechtliches Konstrukt, das es datenverarbeitenden Stellen erleichtern soll, sich bei der Datenverarbeitung der Unterstützung externer Stellen zu bedienen. Das funktioniert dadurch, dass das Gesetz einen externen Datenverarbeiter nicht als Dritten ansieht, wenn eine wirksame Vereinbarung über die Auftragsdatenverarbeitung geschlossen wurde. Dies führt dazu, dass eine Weitergabe von Daten an ihn im Rechtssinne keine Übermittlung von Daten darstellt und deshalb unter erleichterten Voraussetzungen zulässig ist. Verantwortlich bleibt bei dieser Konstruktion stets der Auftraggeber, der verpflichtet ist, sich im Rahmen der Vereinbarung Kontroll- und Weisungsrechte von dem externen Dienstleister einräumen zu lassen und die Umstände der Datenverarbeitung zu regeln. Zugleich bedeutet dies aber auch, dass bei einer unwirksamen oder einer nicht vorhandenen Vereinbarung über die Durchführung einer Auftragsdatenverarbeitung die gesetzliche Privilegierung der Datenweitergabe nicht eingreifen kann und dann eine Datenübermittlung vorliegen muss. Denn wenn die Weitergabe der Daten an den Cloud-Anbieter als solche keine Datenübermittlung im Sinne des Datenschutzgesetzes darstel-

len würde, bräuchte man gar keine Auftragsdatenverarbeitung. Nimmt man also diese Parallele des Cloud-Computings zu Hilfe, ergibt sich auch für die automatische E-Mail-Weiterleitung, dass in der Weiterleitung der E-Mails an eine private E-Mail-Adresse eine Übermittlung der darin enthaltenen Daten an den E-Mail-Provider zu sehen ist.

Doch selbst wenn man dies ungeachtet der oben stehenden Argumente bestreiten möchte, verbleibt immer noch eine datenschutzrechtlich relevante Nutzung von Daten (§ 3 Abs. 2 Nr. 7 DSG NRW), da dies als Auffangtatbestand jede sonstige Verwendung personenbezogener Daten erfasst.

Datenschutzrechtliche Erlaubnistatbestände

Ist also das Vorliegen einer datenschutzrechtlich relevanten Verwendung festgestellt, ist für deren Zulässigkeit erforderlich, dass eine Einwilligung des Betroffenen vorliegt oder eine gesetzliche Vorschrift dieses Verhalten erlaubt (§ 4 DSG NRW).

Von einer Einwilligung des Betroffenen wird man bei einer automatischen E-Mail-Weiterleitung indes nicht ohne Weiteres ausgehen können. Zum einen weiß der Absender überhaupt nicht, dass seine E-Mails, die er an eine Hochschuladresse sendet, an einen anderen Mail-Provider weitergeleitet werden und muss damit auch nicht zwingend rechnen, sodass allein der Versand einer E-Mail, die personenbezogene Daten enthält, noch nicht als Einwilligung durch schlüssiges Verhalten eingestuft werden kann. Zum anderen könnte der Absender ohnehin nur in die Verwendung der eigenen Daten einwilligen. Im Hinblick auf die Daten Dritter, die potentiell per E-Mail verschickt werden, wäre die Einwilligung des jeweiligen Dritten erforderlich, die naturgemäß nicht vom Absender der E-Mail erteilt werden kann.

Dass das DSG NRW oder eine andere Rechtsvorschrift eine solche Datenverwendung erlaubt, kann ebenfalls nicht pauschal unterstellt werden. Insbesondere ist nicht ersichtlich, inwiefern eine automatische E-Mail-Weiterleitung zur Aufgabenerfüllung der Hochschule erforderlich ist, da in aller Regel auch mit den Hochschul-Mail-Adressen gearbeitet werden kann und ein potentiell geringfügig verringerter Komfort gegenüber privaten Mail-Adressen nicht ausreichend ist, um die strengen Anforderungen des Erforderlichkeitskriteriums zu erfüllen. Da also keineswegs

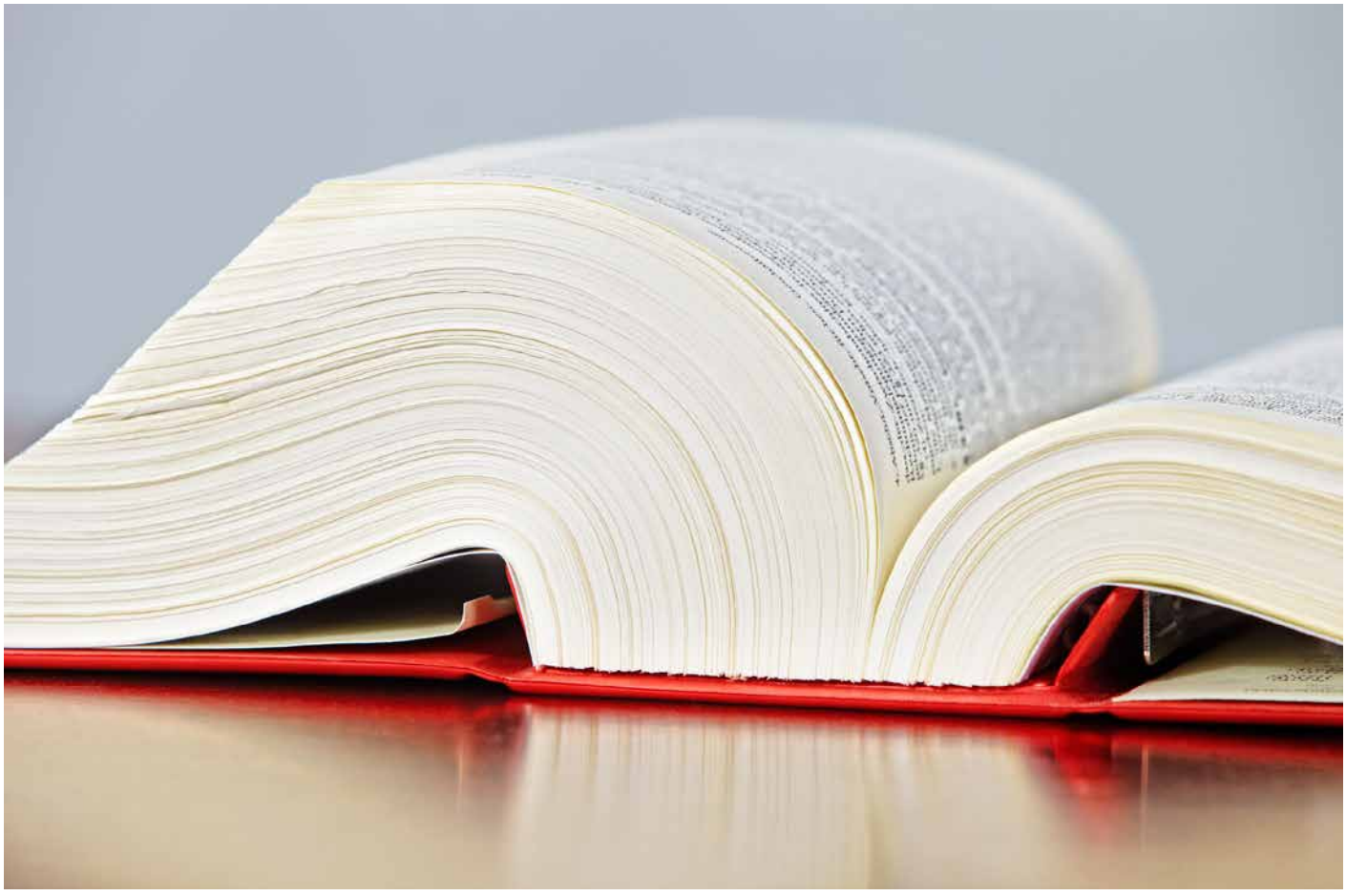


Foto © Ingo Bartussek / fotolia.de

für alle Fälle sichergestellt ist, dass ein Erlaubnistatbestand eingreift, bestehen nicht unerhebliche datenschutzrechtliche Bedenken gegenüber einer automatischen E-Mail-Weiterleitung.

Dies gilt umso mehr, als bei Datenübermittlungen an E-Mail-Provider, die ihren Sitz außerhalb der EU-Mitgliedstaaten haben, wie dies z. B. bei den US-amerikanischen Anbietern der Fall ist, noch höhere Anforderungen gelten. So muss im Normalfall nämlich, zusätzlich zu den üblichen Zulässigkeitsvoraussetzungen, ein angemessenes Datenschutzniveau gewährleistet werden (§ 17 DSG NRW), welches in den meisten Fällen nicht vorliegt und nur durch besondere Vorkehrungen geschaffen werden kann (z. B. durch die Vereinbarung sogenannter Standardvertragsklauseln).

Datenschutz durch technische und organisatorische Maßnahmen

Außerdem ist zu berücksichtigen, dass die Landesdatenschutzgesetze die verantwortlichen Stellen dazu verpflichten, die Ausführung und Einhaltung der datenschutzrechtlichen Vorschriften durch technische und organisatorische Maßnahmen sicherzustellen (z. B. § 10 DSG NRW). Zur Konkretisierung dieser Verpflichtung enthalten die Gesetze eine Auflistung bestimmter Maßnahmen, die der Gewährleistung verschiedener datenschutzrechtlicher Schutzstandards dienen sollen. Dazu gehört beispielsweise, dass die Vertraulichkeit und Verfügbarkeit der Daten sichergestellt werden müssen, indem Maßnahmen getroffen werden, die garantieren, dass die Daten nur von Befugten zur Kenntnis genommen werden können, zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Bei der Nutzung einer automatischen E-Mail-Weiterleitung gelangen geschützte Daten in die Hände eines Dritten, bei dem nicht sichergestellt ist, dass er seinerseits die erforderlichen Schutzmaßnahmen getroffen hat. Dazu kommt, dass die Hochschulen auf die externen Mail-Provider überhaupt keinen Einfluss und deshalb keine Kontroll- oder Steuerungsmöglichkeit zur Einführung der erforderlichen technischen und organisatorischen Maßnahmen haben. Darüber hinaus dürfte man zu den erforderlichen organisatorischen Maßnahmen der Hochschule in einem solchen Fall zählen können, dass sie ihren Mitarbeitern untersagt, solche automatischen E-Mail-Weiterleitungen einzurichten und dies auch technisch verhindert oder zumindest erschwert, indem entsprechende Funktionen gar nicht erst angeboten werden. Die allgemeine Pflicht der Hochschule, ihren Betrieb so zu organisieren, dass geltende Gesetze Beachtung finden und möglichst keine Rechtsverletzungen begangen werden („Compliance"), ist hier im Hinblick auf den Datenschutz spezialgesetzlich konkretisiert. Das Service-Angebot einer automatischen E-Mail-Weiterleitung für dienstliche E-Mail-Konten, welches sich technisch relativ leicht verhindern lässt, wird man deshalb als Verstoß gegen § 10 DSG NRW ansehen müssen.

Pflichten gegenüber der Datenschutzaufsicht

Problematisch ist die automatische E-Mail-Weiterleitung zudem im Hinblick auf die Verpflichtungen, die der Hochschule gegenüber der Datenschutzaufsicht obliegen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) hat eine Aufsichtsfunktion gegenüber den öffentlichen Stellen, da das Gesetz vorsieht, dass er die Einhaltung der datenschutzrechtlichen Vorschriften bei diesen überwacht (§ 22 DSG NRW). Um diese Aufgabe erfüllen zu können, sind die Hochschulen als öffentliche Stellen generell verpflichtet, den LDI bei seiner Aufgabe zu unterstützen und erforderlichenfalls Amtshilfe zu leisten. Insbesondere sind ihm Auskünfte über Fragen zur Datenverarbeitung zu erteilen, Einsicht in alle Datenverarbeitungsvorgänge, Dokumentationen und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, jederzeit Zutritt zu allen Diensträumen und Zugriff auf elektronische Dienste zu ermöglichen und ggf. auch Kopien von Unterlagen zur Verfügung zu stellen. Im Einzelfall kann dies auch bedeuten, dass bestimmte dienstliche E-Mails vorzulegen sind. Wenn nun aber die E-Mails nur noch in privaten Postfächern auf fremden Servern liegen, weil sie ohne Speicherung einer Kopie im Postfach der Hochschul-Mail-Adresse automatisch weitergeleitet werden, ist der Hochschule die Erfüllung dieser Verpflichtung faktisch oft nicht mehr möglich. Dieses Problem stellt sich in ähnlicher Hinsicht auch noch unter zwei anderen rechtlichen Aspekten (Arbeitsrecht und Informationsfreiheitsrecht), die allerdings erst im zweiten Teil dieses Beitrags dargelegt werden.

Löschungspflichten

Zu guter Letzt ist noch zu bedenken, dass das Datenschutzrecht Löschungspflichten in Bezug auf solche personenbezogenen Daten vorsieht, deren Speicherung unzulässig ist oder deren Kenntnis nicht mehr zur Aufgabenerfüllung der verarbeitenden Stelle erforderlich ist. Dies ist Ausfluss des Grundsatzes der Datensparsamkeit und der Datenvermeidung, wonach möglichst wenige personenbezogene Daten erhoben und verarbeitet werden sollen und dies auch nur solange wie nötig. Die Einhaltung dieser Löschungspflichten kann nicht mehr effektiv durch die Hochschule kontrolliert werden, wenn die E-Mails mit entsprechenden Daten nicht mehr in ihrem Einflussbereich gespeichert sind, sondern auf den Servern externer Mail-Provider liegen.

Rechtsfolgen

Für datenschutzrechtliche Verstöße bestehen in verschiedenem Maße gesetzliche Sanktionen. So erklärt § 34 DSG NRW die rechtswidrige Weitergabe nicht offenkundiger personenbezogener Daten zur Ordnungswidrigkeit, die mit einer Geldbuße bis zu 50.000 € geahndet werden kann. Diese ordnungsrechtliche Verantwort-

lichkeit ist zuvorderst eine persönliche und trifft deshalb denjenigen Mitarbeiter, der die automatische E-Mail-Weiterleitung eingestellt und genutzt hat. Im Einzelfall kann jedoch unter den hier nicht näher zu erörternden Voraussetzungen des § 30 Ordnungswidrigkeitengesetz (OWiG) auch eine Geldbuße gegen die Hochschule verhängt werden. Dies kann relevant werden, wenn der Leitungsebene eine Aufsichtspflichtverletzung dergestalt vorzuwerfen ist, dass unzureichende organisatorische Vorkehrungen zur Sicherstellung der Einhaltung datenschutzrechtlicher Regelungen getroffen wurden.

Darüber hinaus kann jeglicher Verstoß gegen datenschutzrechtliche Vorschriften gemäß § 24 DSG NRW zu einer Beanstandung durch den LDI führen, der insofern eine Aufsichtsaufgabe hat. Eine solche Beanstandung müsste gegenüber dem Rektor erfolgen und ist mit einer Aufforderung zur Abgabe einer Stellungnahme verbunden, welcher innerhalb einer bestimmten Frist nachgekommen werden muss. Gleichzeitig unterrichtet der LDI auch die Aufsichtsbehörde. Dies ist unter anderem deshalb notwendig, weil der LDI selbst – zumindest in einigen Bundesländern – keine Durchsetzungsbefugnisse hat. Verweigert die Hochschule trotz Beanstandung durch den LDI eine Anpassung des Verhaltens und teilt die Aufsichtsbehörde die Ansicht des LDI, kann diese (im Fall der nordrhein-westfälischen Hochschulen ist dies das Ministerium für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen) dann gegebenenfalls die Durchsetzung erzwingen. Im Hinblick auf die konkrete Vorgehensweise in anderen Bundesländern ist auf die entsprechenden Normen der jeweiligen Landesdatenschutzgesetze zu verweisen.

Schließlich ist noch zu beachten, dass § 20 DSG NRW einen Schadensersatzanspruch des Betroffenen vorsieht, wenn dieser einen Schaden durch eine unrichtige oder unzulässige Datenverarbeitung erleidet. In schweren Fällen kann der Betroffene sogar einen Anspruch auf Ersatz seiner immateriellen Schäden haben („Schmerzensgeld“). Das erforderliche Verschulden der verantwortlichen Stelle wird dabei vermutet, kann aber widerlegt werden, sofern es tatsächlich an einem fahrlässigen oder vorsätzlichen Handeln fehlte. Erfolgte die Datenverarbeitung in einer automatisierten Datei, ist der Schadensersatzanspruch sogar verschuldensunabhängig, dafür allerdings in der Höhe auf einen bestimmten Betrag gedeckelt. Anspruchsgegner ist insofern in jedem Fall die Hochschule als Träger der verantwortlichen Stelle.

2. Rechtliche Beurteilung für Studierende

Für Studierende sind gesonderte Erwägungen anzustellen. Selbst wenn diese nach dem jeweiligen Hochschulgesetz als Mitglieder der Hochschule qualifiziert werden (so z. B. für eingeschriebene Studierende § 9 Abs. 1 S. 1 HG NRW) und damit in einem Sonderrechtsverhältnis zur Hochschule stehen, muss die Hochschule sich deren Verhalten nicht ohne Weiteres zurechnen lassen. Sie sind deshalb datenschutzrechtlich nicht Teil der öffentlichen Stelle „Hochschule“, sodass ihr Handeln auch nicht nach dem Landesdatenschutzgesetz zu beurteilen ist. Vielmehr unterliegen sie als Private dem Bundesdatenschutzgesetz (BDSG) und sind dessen Terminologie folgend sogenannte „nicht-öffentliche Stellen“. Das BDSG wiederum legt in § 1 Abs. 2 Nr. 3 fest, dass es dann nicht anwendbar ist, wenn solche nicht-öffentlichen Stellen eine Datenverarbeitung ausschließlich für persönliche oder familiäre Tätigkeiten vornehmen. Hiermit will der Gesetzgeber Privatleute in einem engen Kreis von den Restriktionen des Datenschutzrechts befreien, um ihr privates Handeln nicht unverhältnismäßig zu erschweren. Zu diesem engen persönlichen Bereich sollen auch Tätigkeiten im Rahmen der Aus- und Fortbildung gehören, wozu man auch das Studium zählen können wird, solange die jeweiligen Tätigkeiten nicht über den üblichen persönlichen Kreis hinausreichen. Richten sich Studierende also eine automatische E-Mail-Weiterleitung von ihrer Hochschul-Mail-Adresse auf eine private E-Mail-Adresse ein und nutzen diese für Zwecke des Studiums und andere private Angelegenheiten, sind die Voraussetzungen dieses speziellen Anwendungsbereichsausschlusses erfüllt und das Datenschutzrecht deshalb nicht anwendbar. Daraus folgt zugleich, dass insoweit anders als bei den Mitarbeitern datenschutzrechtliche Bedenken nicht bestehen und zahlreiche Fälle denkbar sind, in denen die Nutzung einer automatischen E-Mail-Weiterleitung durch Studierende rechtmäßig möglich ist.

Dieser Rahmen einer Datenverarbeitung zu ausschließlich persönlichen Zwecken wird jedoch überschritten, sobald Studierende bestimmte Selbstverwaltungsaufgaben der Hochschule wahrnehmen, indem sie beispielsweise in Gremien, Ausschüssen, Fachschaften oder Ähnlichem tätig werden und dabei personenbezogene Daten verarbeiten. Insoweit kommt das Datenschutzrecht also auch für Studierende zur Anwendung. Das Gleiche gilt für eine sonstige Nutzung der E-Mail-Adresse für Tätigkeiten, die über den persönlichen Bereich hinausgehen. Obwohl dies keine seltenen Konstellationen sind, dürfte es unverhältnismäßig sein, allein deshalb ein pauschales Verbot des Angebots einer automatischen E-Mail-Weiterleitung für alle Studierenden zu fordern. Stattdessen rückt hier die Eigenverantwortung der jeweiligen Studierenden in den Vordergrund, die zunächst selbst dafür Sorge tragen müssen, dass sie gesetzeskonform handeln. Aufgrund der allgemeinen Pflicht der Hochschule zur Organisation des Hochschulbetriebs in der Form, dass gesetzliche Verbote eingehalten werden und insbesondere auch das Datenschutzrecht Beachtung findet, könnte man von ihr aber unter Umständen verlangen, dass sie Studierende, die in Hochschulgremien tätig sind, darauf hinweist, dass die Nutzung einer automatischen E-Mail-Weiterleitung datenschutzrechtlich nicht risikolos und potentiell rechtswidrig ist. Deshalb bietet es sich an, im Rahmen des Aktivierungsprozesses der automatischen E-Mail-Weiterleitung für Studierende einen entsprechenden Warnhinweis

aufzunehmen, dessen Kenntnisnahme bestätigt werden muss, sofern dieses Service-Angebot für Studierende überhaupt aufrechterhalten werden soll.

Darüber hinaus verpflichtet § 11 Abs. 3 HG NRW die Mitglieder der Hochschule ohnehin in allen Angelegenheiten zur Verschwiegenheit, die ihnen als Träger eines Amtes oder einer Funktion bekannt geworden sind und deren Vertraulichkeit sich aus Rechtsvorschriften, auf Grund besonderer Beschlussfassung des zuständigen Gremiums oder aus der Natur des Gegenstandes ergibt. Verstöße gegen diese Verschwiegenheitspflicht können durch Maßnahmen zur Wiederherstellung der Ordnung geahndet werden, welche allerdings von der Hochschule entsprechend geregelt sein müssen (§ 11 Abs. 5 HG NRW). Ob diese Verschwiegenheitspflicht bei der Nutzung einer automatischen E-Mail-Weiterleitung eingehalten wird, bei der potentiell solche geheimen Inhalte in den Machtbereich des externen E-Mail-Providers gelangen, ist zumindest zweifelhaft.

III. Fazit

Schon die datenschutzrechtliche Betrachtung hat gezeigt, dass das Service-Angebot einer automatischen E-Mail-Weiterleitung durch Hochschulen jedenfalls für ihre Mitarbeiter rechtliche Risiken mit sich bringt, denen nur durch die Abschaffung dieses Angebots sicher vorgebeugt werden kann. Festzuhalten sind aber auch zwei andere Fakten: zum einen stellen sich diese Probleme in der Regel nicht bei Weiterleitungen an eine andere hochschulinterne E-Mail-Adresse desselben Nutzers, da der Herrschaftsbereich der verantwortlichen Stelle dabei nicht verlassen wird und die Daten nicht in die Hände eines Dritten gelangen. Zum anderen ist darauf hinzuweisen, dass bisher – soweit ersichtlich – weder Gerichtsentscheidungen zu dieser Fragestellung ergangen sind noch sonstige Fälle einer Ahndung eines solchen Angebots bekannt geworden sind. Auch die rechtswissenschaftliche Literatur setzt sich so gut wie gar nicht mit diesem Problem auseinander. Ganz vereinzelt finden sich jedoch ebenfalls kritische Einschätzungen. Dennoch ist zu berücksichtigen, dass die Sensibilität für datenschutzrechtliche Fragestellungen und Standards angesichts fortwährender Diskussionen über Vorratsdatenspeicherung und scheinbar allgegenwärtige Überwachung durch Geheimdienste in der Bevölkerung zunimmt. Ferner sind öffentliche Stellen schon durch das Grundgesetz an Gesetz und Recht gebunden und haben eine gewisse Vorbildfunktion. Insofern sollte es nicht zum Maßstab des Handelns gemacht werden, dass dieses Angebot teils schon jahrelang Bestand hatte, ohne dass es Beanstandungen gab. Generell rechtfertigt eine lange Ausübung eines rechtswidrigen Verhaltens keine Fortführung dieser Zustände in der Zukunft. Vielmehr gehört die automatische E-Mail-Weiterleitung auf den Prüfstand der Hochschulen.

Für Studierende dagegen dürfte die automatische E-Mail-Weiterleitung aus datenschutzrechtlicher Perspektive in der Regel deutlich weniger kritisch einzustufen sein. Soweit einige Studierende im Rahmen der Aufgabenerfüllung der Hochschule in Gremien tätig werden und insoweit auch an das Datenschutzrecht gebunden sind, dürfte es unter dem Blickwinkel der Verhältnismäßigkeit vertretbar sein, dieses Service-Angebot für Studierende nicht generell abzuschaffen, sondern dessen Inanspruchnahme nur mit einer Aufklärung und einem entsprechenden Warnhinweis zu versehen. Denn es verbleibt immer noch ein großer Kreis von Studierenden, für die eine Nutzung der automatischen E-Mail-Weiterleitung datenschutzrechtlich zulässig sein dürfte. ◆

Übersicht über die Mitgliedseinrichtungen und Organe des DFN-Vereins

(Stand: 05/2016)

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

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

Die Organe des DFN-Vereins sind:

die Mitgliederversammlung
der Verwaltungsrat
der Vorstand

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

Verwaltungsrat
Der Verwaltungsrat beschließt alle wesentlichen Aktivitäten des Vereins, insbesondere die technisch-wissenschaftlichen Arbeiten und berät den Jahreswirtschaftsplan. Für die 11. Wahlperiode sind Mitglieder des Verwaltungsrates:

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

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

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

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

Prof. Dr. Ulrike Gutheil
(Technische Universität Berlin)

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

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

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

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

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

Prof. Dr. Horst Stenzel
(Fachhochschule Köln)

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

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

Der Verwaltungsrat hat als ständige Gäste

einen Vertreter der Hochschulrektorenkonferenz:

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

einen Vertreter der Hochschulkanzler:

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

einen Vertreter der Kultusministerkonferenz:

Jürgen Grothe
(SMWK Dresden)

den Vorsitzenden der jeweils letzten Mitgliederversammlung:

Prof. Dr. Gerhard Peter
(Hochschule Heilbronn)

den Vorsitzenden des ZKI:

Martin Wimmer
(Universität Regensburg)

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

Prof. Dr. Hans-Joachim Bungartz
Vorsitz

Prof. Dr. Ulrike Gutheil
Stellv. Vorsitzende

Dr. Rainer Bockholt
Stellv. Vorsitzender

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

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

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Albstadt	Hochschule Albstadt-Sigmaringen (FH)
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Hochschule Aschaffenburg
Augsburg	Hochschule für angewandte Wissenschaften, Fachhochschule Augsburg
	Universität Augsburg
Bad Homburg	Dimension Data Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	BBB Management GmbH
	Berliner Institut für Gesundheitsforschung/Berlin Institut of Health
	Beuth Hochschule für Technik Berlin – University of Applied Sciences
	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
	Bundesanstalt für Materialforschung und -prüfung
	Bundesinstitut für Risikobewertung
	Deutsche Telekom AG Laboratories
	Deutsches Herzzentrum Berlin
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin (FUB)
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hochschule für Technik und Wirtschaft – University of Applied Sciences
	Hochschule für Wirtschaft und Recht
	Humboldt-Universität zu Berlin (HUB)
	International Psychoanalytic University Berlin
	IT-Dienstleistungszentrum
	Konrad-Zuse-Zentrum für Informationstechnik (ZIB)
	Museum für Naturkunde
	Robert Koch-Institut
	Stanford University in Berlin
	Stiftung Deutsches Historisches Museum
	Stiftung Preußischer Kulturbesitz
	Technische Universität Berlin (TUB)
	T-Systems International GmbH
	Umweltbundesamt
	Universität der Künste Berlin
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum Berlin für Sozialforschung gGmbH (WZB)
Biberach	Hochschule Biberach
Bielefeld	Fachhochschule Bielefeld
	Universität Bielefeld
Bingen	Fachhochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Fachhochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Fachhochschule Georg Agricola für Rohstoff, Energie und Umwelt zu Bochum
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern
	Bundesministerium für Umwelt, Naturschutz, Bau u. Reaktorsicherheit
	Deutsche Forschungsgemeinschaft (DFG)
	Deutscher Akademischer Austauschdienst e. V. (DAAD)
	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	Rheinische Friedrich-Wilhelms-Universität Bonn
	Zentrum für Informationsverarbeitung und Informationstechnik
Borstel	FZB, Leibniz-Zentrum für Medizin und Biowissenschaften
Brandenburg	Technische Hochschule Brandenburg
Braunschweig	DSMZ – Deutsche Sammlung von Mikroorganismen und Zellkulturen GmbH
	Helmholtz-Zentrum für Infektionsforschung GmbH
	Hochschule für Bildende Künste Braunschweig
	Johann-Heinrich von Thünen-Institut, Bundesforschungs-institut für Ländliche Räume, Wald und Fischerei
	Julius Kühn-Institut Bundesforschungsinstitut für Kulturpflanzen
	Physikalisch-Technische Bundesanstalt (PTB)
	Technische Universität Carolo-Wilhelmina zu Braunschweig
Bremen	Hochschule Bremen
	Hochschule für Künste Bremen
	Jacobs University Bremen gGmbH
	Universität Bremen
Bremerhaven	Alfred-Wegener-Institut, Helmholtz-Zentrum für Polar- und Meeresforschung (AWI)
	Hochschule Bremerhaven
	Stadtbildstelle Bremerhaven
Chemnitz	Technische Universität Chemnitz
	TUCed – Institut für Weiterbildung GmbH
Clausthal	Clausthaler Umwelttechnik-Institut GmbH (CUTEC)
	Technische Universität Clausthal-Zellerfeld
Coburg	Hochschule für angewandte Wissenschaften, Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus-Senftenberg
Darmstadt	European Space Agency (ESA)
	Evangelische Hochschule Darmstadt
	GSI Helmholtzzentrum für Schwerionenforschung GmbH
	Hochschule Darmstadt
	Merck KGaA
	Technische Universität Darmstadt
	T-Systems International GmbH
Deggendorf	Hochschule für angewandte Wissenschaften, Fachhochschule Deggendorf
Dortmund	Fachhochschule Dortmund
	Technische Universität Dortmund
Dresden	Evangelische Hochschule Dresden
	Helmholtz-Zentrum Dresden-Rossendorf e. V.
	Hannah-Arendt-Institut für Totalitarismusforschung e. V.
	Hochschule für Bildende Künste Dresden
	Hochschule für Technik und Wirtschaft
	Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden e. V.
	Leibniz-Institut für Polymerforschung Dresden e. V.
	Sächsische Landesbibliothek – Staats- und Universitätsbibliothek
	Technische Universität Dresden
Düsseldorf	Fachhochschule Düsseldorf
	Heinrich-Heine-Universität Düsseldorf
	Information und Technik Nordrhein-Westfalen (IT.NRW)
	Kunstakademie Düsseldorf

Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Hochschule Emden/Leer
Erfurt	Fachhochschule Erfurt
	Universität Erfurt
Erlangen	Friedrich-Alexander-Universität Erlangen-Nürnberg
Essen	Rheinisch-Westfälisches Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Europa-Universität Flensburg
	Fachhochschule Flensburg
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Deutsche Nationalbibliothek
	Deutsches Institut für Internationale Pädagogische Forschung
	Frankfurt University of Applied Science
	Johann Wolfgang Goethe-Universität Frankfurt am Main
	Philosophisch-Theologische Hochschule St. Georgen e.V.
	Senckenberg Gesellschaft für Naturforschung
Frankfurt/O.	IHP GmbH – Institut für innovative Mikroelektronik
	Stiftung Europa-Universität Viadrina
Freiberg	Technische Universität Bergakademie Freiberg
Freiburg	Albert-Ludwigs-Universität Freiburg
	Evangelische Hochschule Freiburg
	Katholische Hochschule Freiburg
Freising	Hochschule Weihenstephan
Friedrichshafen	Zeppelin Universität gGmbH
Fulda	Hochschule Fulda
Furtwangen	Hochschule Furtwangen – Informatik, Technik, Wirtschaft, Medien
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH
	Leibniz-Rechenzentrum d. Bayerischen Akademie der Wissenschaften
Gatersleben	Leibniz-Institut für Pflanzengenetik und Kulturpflanzenforschung (IPK)
Geesthacht	Helmholtz-Zentrum Geesthacht Zentrum für Material- und Küstenforschung GmbH
Gelsenkirchen	Westfälische Hochschule
Gießen	Technische Hochschule Mittelhessen
	Justus-Liebig-Universität Gießen
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GwDG)
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	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 e. V.
	Martin-Luther-Universität Halle-Wittenberg
Hamburg	Bundesamt für Seeschifffahrt und Hydrographie
	Deutsches Elektronen-Synchrotron (DESY)
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	DFN – CERT Services GmbH
	HafenCity Universität Hamburg
	Helmut-Schmidt-Universität, Universität der Bundeswehr
	Hochschule für Angewandte Wissenschaften Hamburg
	Hochschule für Bildende Künste Hamburg
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg-Harburg
	Universität Hamburg
	Xantaro Deutschland GmbH
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
Idstein	Hochschule Fresenius gGmbH
Ilmenau	Bundesanstalt für IT-Dienstleistungen im Geschäftsbereich des BMVBS
	Technische Universität Ilmenau
Ingolstadt	DiZ – Zentrum für Hochschuldidaktik d. bayerischen Fachhochschulen
	Hochschule für angewandte Wissenschaften FH Ingolstadt
Jena	Ernst-Abbe-Hochschule Jena
	Friedrich-Schiller-Universität Jena
	Leibniz-Institut für Photonische Technologien e. V.
	Leibniz-Institut für Altersforschung – Fritz-Lipmann-Institut e. V. (FLI)
Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Fachhochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	Fachinformationszentrum Karlsruhe (FIZ)
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe – Technik und Wirtschaft
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Hochschule für angewandte Wissenschaften, Fachhochschule Kempten
Kiel	Christian-Albrechts-Universität zu Kiel
	Fachhochschule Kiel
	Institut für Weltwirtschaft an der Universität Kiel
	Helmholtz-Zentrum für Ozeanforschung Kiel (GEOMAR)
	ZBW – Deutsche Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft
Koblenz	Hochschule Koblenz
Köln	Deutsche Sporthochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Katholische Hochschule Nordrhein-Westfalen
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln gGmbH
	Technische Hochschule Köln
	Universität zu Köln

Konstanz	Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)
	Universität Konstanz
Köthen	Hochschule Anhalt
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e. V.
Landshut	Hochschule Landshut - Hochschule für angewandte Wissenschaften
Leipzig	Deutsche Telekom, Hochschule für Telekommunikation Leipzig
	Helmholtz-Zentrum für Umweltforschung – UFZ GmbH
	Hochschule für Grafik und Buchkunst Leipzig
	Hochschule für Musik und Theater „Felix Mendelssohn Bartholdy“
	Hochschule für Technik, Wirtschaft und Kultur Leipzig
	Leibniz-Institut für Troposphärenforschung e. V.
	Mitteldeutscher Rundfunk
	Universität Leipzig
Lemgo	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	Hochschule 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 für Philosophie München
	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.
	Katholische Stiftungsfachhochschule München
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft
	Technische Universität München
	Universität der Bundeswehr München
Münster	Fachhochschule Münster
	Westfälische Wilhelms-Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neu-Ulm	Hochschule für Angewandte Wissenschaften, Fachhochschule Neu-Ulm
Nordhausen	Hochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
Nürtingen	Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen
Nuthetal	Deutsches Institut für Ernährungsforschung Potsdam-Rehbrücke
Oberwolfach	Mathematisches Forschungsinstitut Oberwolfach gGmbH
Offenbach/M.	Deutscher Wetterdienst (DWD)
Offenburg	Hochschule Offenburg, Fachhochschule
Oldenburg	Carl von Ossietzky Universität Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück (FH)
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Deutsche Gesellschaft zum Bau und Betrieb von Endlagern für Abfallstoffe mbH
Pforzheim	Hochschule Pforzheim - Gestaltung, Technik, Wirtschaft und Recht
Potsdam	Fachhochschule Potsdam
	Helmholtz-Zentrum, Deutsches GeoForschungsZentrum – GFZ
	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam-Institut für Klimafolgenforschung (PIK)
	Universität Potsdam
Regensburg	Ostbayerische Technische Hochschule Regensburg
	Universität Regensburg
Rosenheim	Hochschule für angewandte Wissenschaften – Fachhochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn Rhein-Sieg
Schmalkalden	Hochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Siegen	Universität Siegen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Fachhochschule Stralsund
Stuttgart	Cisco Systems GmbH
	Duale Hochschule Baden-Württemberg
	Hochschule der Medien Stuttgart
	Hochschule für Technik Stuttgart
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte Tautenburg
Trier	Hochschule Trier
	Universität Trier
Tübingen	Eberhard Karls Universität Tübingen
	Leibniz-Institut für Wissensmedien
Ulm	Hochschule Ulm
	Universität Ulm
Vechta	Universität Vechta
	Private Hochschule für Wirtschaft und Technik
Wadern	Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH (LZI)
Weimar	Bauhaus-Universität Weimar
	Hochschule für Musik FRANZ LISZT Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz

Weßling	T-Systems Solutions for Research GmbH
Wiesbaden	Hochschule RheinMain
	Statistisches Bundesamt
Wildau	Technische Hochschule Wildau (FH)
Wilhelmshaven	Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth
Wismar	Hochschule Wismar
Witten	Private Universität Witten/Herdecke gGmbH
Wolfenbüttel	Ostfalia Hochschule für angewandte Wissenschaften
	Herzog August Bibliothek
Worms	Hochschule Worms
Wuppertal	Bergische Universität Wuppertal
Würzburg	Hochschule für angewandte Wissenschaften – Fachhochschule Würzburg-Schweinfurt
	Julius-Maximilians-Universität Würzburg
Zittau	Hochschule Zittau/Görlitz
Zwickau	Westsächsische Hochschule Zwickau