DFN mitteilungen

25 Jahre DFN-CERT

... mehr als nur Sicherheit für uns

DFN-MailSupport erfolgreich zertifiziert
Von gemeinsamen Sicherheits-standards profitieren

Virtuelle Netze für die DFN-Community
Generalized-Virtualization-Service ist jetzt verfügbar

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, Maimona Id
Gestaltung: Labor3 | www.labor3.com
Druck: Druckerei Rüss, Potsdam

Fotonachweis:
Titel: Grafik © Matthias Stümpke
Seite 6/7 © fermate / iStock
Seite 34/35 © G. Brammer / ESO

Prof. Dr. Klaus-Peter Kossakowski
Geschäftsführer der DFN-CERT Services GmbH

Vor über 25 Jahren wurde das Computer Emergency and Response Team (CERT) im Deutschen Forschungsnetz, kurz DFN-CERT, gegründet. Es entstand aus der Erkenntnis, dass auch ein Netz wie das DFN, damals fast das einzige und ebenso wie heute das schnellste Internet in Deutschland, ein eigenes Sicherheitsteam haben muss. Dieses Team steht den Anwendern bei Sicherheitsproblemen zur Seite, leistet Unterstützung, koordiniert Aktivitäten und sorgt für die Nachsorge bei kritischen Hinweisen auf gestohlene digitale Identitäten oder befallene Systeme.

Das Deutsche Forschungsnetz sowie seine angeschlossenen Anwender sind ein attraktives Ziel. Es gibt interessante Dinge zu holen, relevante Forschungsergebnisse ein paar Jahre früher als vor der offiziellen Veröffentlichung verfügbar zu machen oder die schnelleren Leitungen des DFN mit ihren viel größeren Kapazitäten für DDoS-Angriffe zu nutzen. Und ja, auch in Forschungsnetzen werden manchmal Festplatten so verschlüsselt, dass niemand sie wieder entschlüsseln kann, selbst wenn die Bitcoins eingezahlt werden. Warum sollte es auch anders sein als im restlichen Internet? Lehrende, Forschende und Studierende sind eben nicht „tabu“ für die Angreifer und schon lange nicht „immun“ gegenüber Bedrohungen.

Für viele, die sich heute mit Cyber-Security befassen, gehört „Incident Management“ zu den ganz elementaren Aufgaben: Die Fähigkeit, zugesagte Dienste auch bei und trotz Angriffen aufrecht zu erhalten, Angriffe schnell zu analysieren und sie dann zu stoppen. Die Vertraulichkeit sensitiver Informationen sicherzustellen und zu verhindern, dass Manipulationen an Daten oder Systemen die Reputation oder auch Leib und Leben von Menschen gefährden, ist anerkannte – quasi lebensnotwendige – Voraussetzung für jedwede Digitalisierung unserer Gesellschaft. Das DFN-CERT ist mit diesen kritischen Funktionen unverzichtbar.

Damals aber, 1993 bei der Gründung, war dies eben keine Selbstverständlichkeit, sondern eine Pioniertat und die Voraussicht des Vereins, dieses Thema zu institutionalisieren und ihm eine nachhaltige Struktur zu geben. Ich bin deswegen sehr stolz, dass wir es in all diesen Jahren geschafft haben, uns selbst, unserer besonderen Rolle und der Vision, die am Anfang stand, treu zu bleiben: Wir sind ein wertorientierter Dienstleister mit eingespielten Teams und viel individuellem Know-how, der sich immer wieder neu orientiert, um Trends aufzunehmen oder auf Herausforderungen zu reagieren. Für den DFN, seine Anwender und unsere weiteren Kunden sind wir der verlässliche Partner für mehr Sicherheit und Datenschutz.

Danke an die, die das alles möglich gemacht haben!
Danke an die, die das durch Ihre Arbeit jeden Tag möglich machen!

Prof. Dr. Klaus-Peter Kossakowski

Unsere Autoren dieser Ausgabe im Überblick

1 Michael Röder, DFN-Verein (roeder@dfn.de); **o. Abb.** Christine Kahl, DFN-CERT (kahl@dfn.de); **o. Abb.** Stefan Kelm, DFN-CERT Services GmbH (kelm@dfn-cert.de); **2** Rogier Spoor, SURFnet (rogier.spoor@SURFnet.nl); **3** Tangui Coulouarn, DeiC (tangui.coulouarn@deic.dk); **o. Abb.** François Kooman, SURFnet (françois.kooman@SURFnet.nl); **4** Dr. Peter Kaufmann, DFN-Verein (kaufmann@dfn.de); **5** Dr.-Ing. Susanne Naegele-Jackson, Regionales Rechenzentrum Erlangen, RRZE (susanne.naegele-jackson@fau.de); **6** Sascha Schweiger, RRZE (sascha.schweiger@fau.de); **7** Philipp Seyerlein, RRZE (philipp.seyerlein@fau.de); **8** Nina Bark, DFN-Verein (bark@dfn.de); **9** Maimona Id, DFN-Verein (id@dfn.de); **10** Dr. Volker Hammerr, Secorvo Security Consulting GmbH (volker.hammer@secorvo.de); **11** Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **12** Dr. Ralf Gröper, DFN-Verein (groeper@dfn.de); **13** Jule Anna Ziegler, Leibniz-Rechenzentrum (LRZ) der Ludwig-Maximilians-Universität München (LMU) (jule.ziegler@lrz.de); **14** Bastian Kemmler, LRZ der LMU (bastian.kemmler@lrz.de), **15** Michael Brenner, LRZ der LMU (michael.brenner@lrz.de); **o. abb.** Thomas Schaaf, LRZ der LMU (schaaf@nm.ifi.lmu.de); **16** Charlotte Röttgen, Forschungsstelle Recht im DFN (roettgen@dfn.de); **17** Armin Strobel, Forschungsstelle Recht im DFN (strobel@dfn.de)

Inhalt

Wissenschaftsnetz

Vertrauen ist gut, Prüfen ist Pflicht

Erfolgreich zertifiziert: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verleiht DFN-MailSupport im Januar 2018 ein Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz. Es bestätigt damit, dass die Infrastruktur und Prozesse des E-Mail-Dienstes für die fachgerechte Verarbeitung sensibler Informationen geeignet sind. Die Anerkennung des Zertifikates entlastet teilnehmende Einrichtungen bei der Ausübung ihrer eigenen Prüfpflicht im Rahmen der Auftragsdatenverarbeitung.

Text: **Michael Röder** (DFN-Verein)

Foto © Pincio/iStock

771 Milliarden E-Mails[1] wurden im vergangenen Jahr in Deutschland versandt und empfangen. Mittlerweile gehört die E-Mail zu den meist genutzten Kommunikationskanälen weltweit. Das haben auch Angreifer erkannt und missbrauchen E-Mails für ihre geschickten Täuschungsversuche. So sorgen Phishingmails und virulente Anhänge für ein erhebliches Sicherheitsrisiko. Laut Statistik (Abbildung 1) übertrifft die Anzahl unerwünschter E-Mails die Menge an erwünschten Nachrichten um ein Vielfaches. Ein vertrauenswürdiger und rechtlich einwandfreier E-Mail-Dienst ist die Grundlage für das reibungslose Funktionieren vieler Prozesse in Forschung und Lehre. Jede funktionale Beeinträchtigung dieses hochsensiblen Dienstes macht sich in der Regel schnell in allen Geschäftsbereichen bemerkbar.

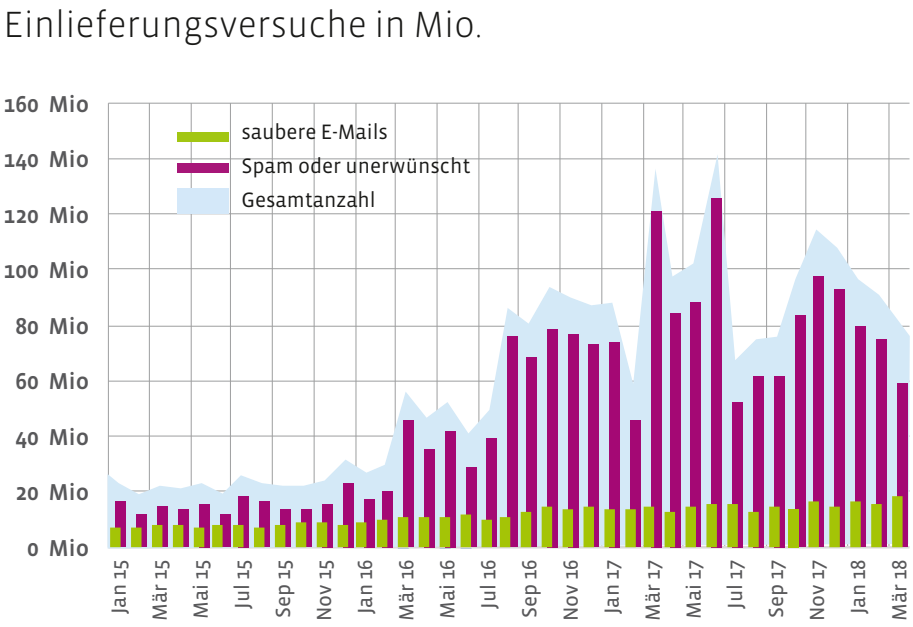


Abbildung 1: Monatliche Anzahl eingelieferter E-Mails über alle DFN-MailSupport-Teilnehmer

Für jeden Betreiber einer Mailinfrastruktur ist es deshalb zwingend notwendig, seine Endnutzer beim Herausfiltern potenziell unerwünschter E-Mails zu unterstützen. Darum haben sich die Einrichtungen, die am Wissenschaftsnetz teilnehmen, gemeinsam mit dem DFN-Verein dazu entschieden, ein weitestgehend automatisiertes Verfahren zu entwickeln. Das Ergebnis dieser Zusammenarbeit ist der Dienst DFN-MailSupport. Seit seiner Überführung in den Regelbetrieb (2014) trägt er zum hohen Sicherheitsniveau im X-WiN und in den Einrichtungen bei. Mit DFN-MailSupport können teilnehmende Einrichtungen selbst bestimmen, anhand welcher Kriterien und Schwellwerte der Schadgehalt ihrer E-Mails gemessen werden soll und welchen weiteren Verlauf die Nachricht nimmt.

Gemeinsam mit der Community wird der DFN-Dienst entlang seiner Bedürfnisse kontinuierlich weiterentwickelt. So ist der Funktionsumfang vor Kurzem beispielsweise um das Scannen ausgehender E-Mails erweitert worden. Aktuell nutzen 92 Einrichtungen den Dienst und versorgen damit über 650.000 Endnutzer.

Verarbeitung personenbezogener Daten im Auftrag

Um potenzielle Risiken zu benennen und sich in der Folge auf geeignete technische und organisatorische Gegenmaßnahmen zu einigen, schreibt der Gesetzgeber den Parteien, die am Verarbeitungsprozess personenbezogener Daten beteiligt sind, das Schließen einer Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag (kurz: ADV) vor. Aus dieser ADV ergeben sich diverse Rechte und Pflichten, die sich Auftraggeber (hier: teilnehmende Einrichtung) und Auftragnehmer (hier: DFN-Verein) gegenseitig zusichern. Ein wesentlicher Bestandteil der ADV ist das Kontrollrecht des Auftraggebers gegenüber dem Auftragnehmer. Tatsächlich ergibt sich daraus eine Pflicht des Auftraggebers, sich regelmäßig von der Umsetzung der definierten Gegenmaßnahmen zu überzeugen. Die Kontrolle der technischen Maßnahmen geschieht in der Regel durch eine Begehung der Standorte, an denen relevante Daten verarbeitet werden. Eine Kontrolle organisatorischer Maßnahmen ist beispielsweise möglich, indem Einsicht in die Dokumentation des Dienstes genommen werden kann. Zu den Dokumentationsunterlagen gehören neben Netz- und Notfallplänen unter anderem ein Sicherheitskonzept, Risikoanalysen und daraus abgeleitete Richtlinien.

Bis zum Erhalt des Zertifikates nach ISO 27001 auf der Basis von IT-Grundschutz war es allerdings ein langer Weg für alle Beteiligten. Grundsätzlich gehen Administratoren und Rechenzentrumsverantwortliche mit aller gebotenen Sorgfalt ans Werk, wenn es darum geht, sensible Daten zu verarbeiten. Um davon aber einen externen Auditor zu überzeugen, bedarf es verschiedener sorgfältiger Vorbereitungen. Die Frage, warum ausgerechnet diese ISO-Norm als Grundlage für das Audit genutzt wurde, soll gemeinsam mit einigen anderen Aspekten im Folgenden beleuchtet werden.

[1] laut einer Analyse der E-Mail-Dienstleister Web.de und GMX.

Von gemeinsamen Sicherheitsstandards profitieren

Das BSI hat einen Maßnahmenkatalog entwickelt, der die Prüfpflicht des Auftraggebers einer ADV angemessen abbildet. Dieser Maßnahmenkatalog ist vom BSI in Anlehnung an den internationalen ISO 27001-Standard erarbeitet worden. Zusätzlich sind weitere Maßnahmen aus dem BSI-Standard „IT-Grundschutz“ eingeflossen. Deshalb trägt der daraus resultierende Standard den Namen „ISO 27001 auf der Basis von IT-Grundschutz“.

Der Auftragnehmer der ADV kann einen vom BSI zertifizierten Auditor damit beauftragen, die genutzte Infrastruktur entsprechend zu auditieren. Im Falle eines positiven Auditorenvotums erstellt der Auditor einen umfassenden Zertifizierungsbericht, der anschließend dem BSI zur Prüfung vorgelegt wird. Sofern seitens des BSI keine weiteren Auflagen erteilt werden, wird dem Auditgegenstand als Resultat ein Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz verliehen. Dieses Zertifikat in Verbindung mit dem Zertifizierungsbericht des Auditors können Einrichtungen, die am Dienst DFN-MailSupport teilnehmen, anerkennen und damit stellvertretend ihrer aus der ADV resultierenden Verpflichtung gerecht werden. Zusätzlich kann sich jede Einrichtung bei Bedarf im Rahmen einer persönlichen Kontrolle von der fachlich korrekten Umsetzung überzeugen.

Gegenstand des Audits

Eine Reihe von Prüfungen ist bei den Begehungen der Standorte, an denen Daten von DFN-MailSupport verarbeitet werden, vorgeschrieben. Unter anderem sind dabei technische Maßnahmen relevant, die im Betrieb vor Ausfällen schützen sollen, wie beispielsweise redundante Stromzuführungen und Netzanschlüsse sowie Netzersatzanlagen der genutzten Infrastruktur. Zum Schutz vor Beeinträchtigung zählen aber auch Frühwarnsysteme wie Brand- und Leckagemeldeanlagen, deren ordnungsgemäße Kennzeichnung sowie die zentrale Auswertung eintreffender Ereignisse bzw. eine automatisierte Alarmierung. Auch eine zu klein dimensionierte Klimaanlage entgeht dem geschulten Auditorenauge nicht. Entdeckt der Auditor eine mangelhafte Umsetzung, formuliert er schriftlich eine Auflage und versieht diese mit einem Zeitfenster für die Behebung. Ein positives Votum ist erst dann möglich, wenn alle Auflagen angemessen bearbeitet wurden.

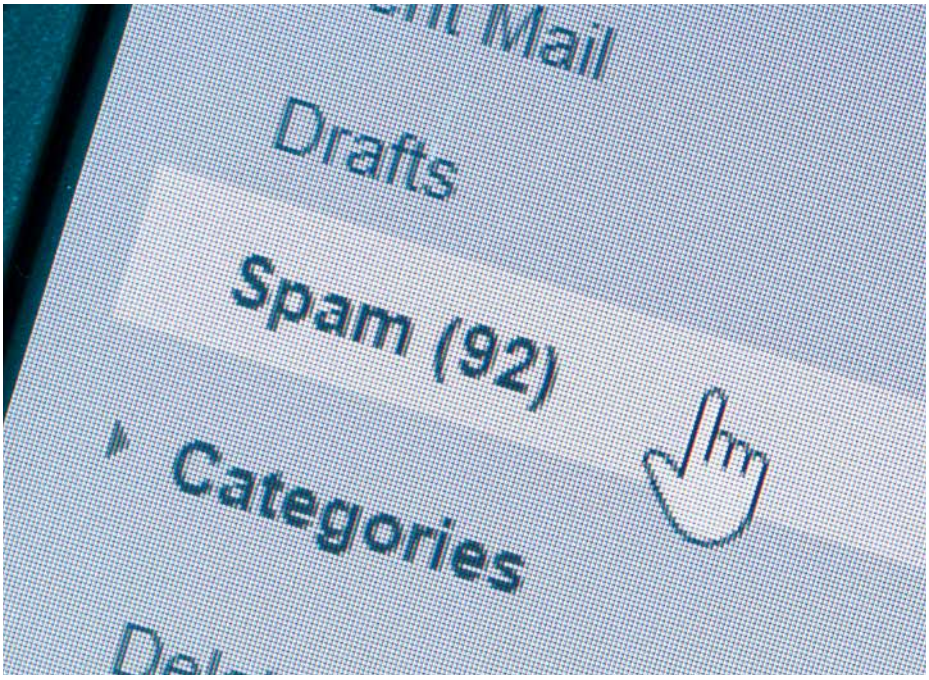


Foto © Kenishirotie / iStock

Neben den technischen Maßnahmen wird ebenfalls die Umsetzung organisatorischer Maßnahmen überprüft, dazu zählen beispielsweise konkrete Zugangs- und Zutrittsberechtigungen. Diese stellen sicher, dass ausschließlich ein definierter Personenkreis berechtigt ist, Zugang zu den Daten zu erhalten. Integrale Bestandteile jeder Standortprüfung sind, neben Prozessen des Changemanagements wie etwa Wartung und Reinigung, Maßnahmen zur Gebäudeüberwachung. Ebenso gehört dazu die Überprüfung von Feuerlöschanlagen und Wartungsprotokollen. Auch Notfallkonzepte, Informationen zu Ersthelfern und definierte Abläufe im Havariefall müssen dokumentiert, regelmäßig überprüft und leicht zugänglich aufbewahrt werden. Mitunter verlaufen die Grenzen zwischen technischen und organisatorischen Maßnahmen fließend. Gelegentlich machte der Auditor auf die Entfernung von Brandlasten wie beispielsweise Lieferkartons etc. aufmerksam. Deren Beseitigung ist mit wenig Aufwand verbunden, der entstehende Mehrwert ist aus Sicht des präventiven Brandschutzes ungleich größer. Auch den Schutz von Mitarbeitern und Besuchern des Rechenzentrums berücksichtigt das Audit. Maßnahmen zur Beschilderung von Fluchtwegen und Sammelplätzen werden genauso überprüft wie die regelmäßige Durchführung von Brandschutzübungen einschließlich ihrer Protokollierung.

Auch die tatsächliche technische Implementierung muss sich an die Vorgaben des Standards halten. So zählt beispielsweise ein ausgereiftes Firewallkonzept genauso zu den Prüfbausteinen des Audits wie eine funktionierende Rollentrennung unter den Administratoren. Im Zuge dessen müssen nachvollziehbare Vertretungsregelungen existieren, die allerdings gleichzeitig unterschiedliche Tätigkeitsgebiete

DATENSCHUTZ UND IT-SICHERHEIT GEWÄHRLEISTEN

Die Verarbeitung von E-Mails ist in vielen Fällen eng mit der Verarbeitung personenbezogener Daten verbunden. Vereinfacht dargestellt sind personenbezogene Daten alle Informationen, die mit wenig oder mittelbarem Aufwand eindeutig auf eine real existierende Person schließen lassen. Das Bundesdatenschutzgesetz stellt – auch in seiner neuen Fassung – hohe Anforderungen an einen Verarbeiter personenbezogener Daten. Einrichtungen, die das Abuse-Management ihrer E-Mails an DFN-MailSupport auslagern möchten, müssen deshalb im Namen ihrer Anwender sicherstellen, dass der Verarbeitungsprozess mit der notwendigen Sorgfalt geschieht. Neben dem Schutz der Personendaten sind auch die Integrität der transportierten Information und der Schutz vor unerlaubtem Zugriff von allerhöchstem Interesse. Zur IT-Sicherheit zählen aber auch Maßnahmen, die dem Ausfallschutz dienen.

nicht ausschließen dürfen. Denn die restriktive Vergabe von Rechten ist eines der oberen Gebote der IT-Sicherheit. Interne Richtlinien müssen glaubhaft in der Umsetzung Anwendung finden und regelmäßig auf Aktualität überprüft werden.

Und ganz zum Schluss gilt für jeden einzelnen Auditgegenstand: Eine gute Dokumentation ist bereits die halbe Miete. Denn während des Audits hat der Auditor wenig Zeit zur Verfügung. Jedes Detail, das sich ihm schnell erschließt, sorgt für Transparenz und stärkt das Vertrauen in den Zertifizierungsprobanden.

Abbildung 2: Zertifizierungsbuttons zum ISO 27001-Zertifikat auf der Basis von IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik für den Untersuchungsgegenstand „DFN-MailSupport“

DFN-MailSupport ist zertifiziert nach ISO 27001 auf der Basis von IT-Grundschutz

Ist der Auditor schließlich nach allen Auditvorbereitungen, Reviews der Dokumentation sowie diversen Admin-Interviews von der standardkonformen Umsetzung aller Maßnahmen überzeugt, wird der Zertifizierungsbericht beim BSI eingereicht. Mit dem Empfang des schriftlichen Einverständnisses des BSI, ist der Dienst DFN-MailSupport nun seit Januar 2018 nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert. Ein solches Zertifikat wird grundsätzlich für eine begrenzte Laufzeit von drei Jahren vergeben. Zwischendurch finden in Abständen von zwölf Monaten regelmäßige Überwachungsaudits statt.

Ein großes Dankeschön

An dieser Stelle bedankt sich der DFN-Verein bei allen Kolleginnen und Kollegen vor Ort, die den Auditor sowie unseren Beauftragten für IT-Sicherheit und unsere Datenschutzbeauftragte bei den Standortbesichtigungen so tatkräftig unterstützt haben. Sowohl der wohlwollende Umgang mit Optimierungsvorschlägen des Auditors als auch die Bereitschaft, Einsicht in die Dokumentenlage zu gewähren, sind Zeichen des besonderen Vertrauens, das uns entgegengebracht wurde. Die beispielhafte Vorbereitung an allen Standorten war maßgeblich dafür verantwortlich, dass der gesamte Zertifizierungsprozess termingerecht und mit einem positiven Auditorenvotum abgeschlossen werden konnte. ◆

Am Anfang war der Wurm: 25 Jahre DFN-CERT

Vor mehr als 25 Jahren gründete der DFN-Verein das Computer Emergency and Response Team (CERT) als eines der ersten CERTs in Deutschland. Seitdem unterstützt und berät das CERT-Team die Teilnehmer am DFN bei Sicherheitsproblemen. Zu seinen Kernaufgaben zählen die Koordination von präventiven Maßnahmen sowie das Sammeln und Verteilen von Hinweisen auf kompromittierte Rechner. Inzwischen sind weitere Teams für allgemeine Beratungsleistungen, den Betrieb von Public Key Infrastrukturen und für Softwareentwicklungen hinzugekommen.

Text: **Stefan Kelm, Christine Kahl** (DFN-CERT)

die Sicherheit im Chaos zu gewährleisten.

„Wir sind so etwas wie die Netz-Feuerwehr. Wenn es brennt, kommen wir

Alles im (Tasten-)Griff: Dr. Klaus-Joachim Mück (links) und Klaus-Peter Kossakowski sorgen für Sicherheit im Computernetz Internet.
Foto: LÜTTGEN

und versuchen, den Schaden zu begrenzen", sagt Klaus-Peter Kossakowski, Chef des Computer Emergency Response Teams (CERT) des Deutschen Forschungsnetzes. Der In-

im Namen des US-Präsidenten Bill Clinton e-Mails im Netz zu versenden. Als Absender der Post erschien die Internet-Adresse des Weißen Hauses in Washington. „Der Versuch ging als Angriff von Hakkern auf das Weiße Haus durch die Medien. Tatsächlich haben die Leute aber nur die Möglichkeiten des ‚sendmail'-Programms genutzt, das für die Übertragungen von Briefen im ganzen Netz verwendet wird", sagt Kossakowski.

Auslöser der vermeintlichen Attacke war ausgerechnet ein Artikel über Datensicherheit in der Computerzeitschrift „c't". Nur ein Zufall machte es möglich, daß die falschen Briefe überhaupt auffielen.

Da in dem in der Computerzeitschrift abgedruckten Programm eine entscheidende Zeile fehlte, benutzten viele Leser den falschen Dienst für die

Hier war es ein leichtes, die Nutzer zu ermitteln", sagt Kossakowski. „Viele waren sich gar nicht bewußt, etwas Unrechtes getan zu haben. Schließlich hatten sie ja nur die Anweisung in der Zeitschrift befolgt."

Eine wirksame Methode, das Fälschen von Absendern zu verhindern, gibt es nach den Worten des Sicherheits-Experten nicht.

Schützen läßt sich allerdings der Inhalt der Post. Geplagte Briefschreiber können entsprechende Verschlüsselungs-Software beim CERT erhalten. Nur wer den richtigen Schlüssel auf seinem Rechner gespeichert hat, kann die Nachricht lesen.

Bei diesen Schlüsseln handelt es sich allerdings nicht um simple Paßwörter. „Die sind viel zu leicht zu knacken", sagt Kossakowski. „Mein Schlüssel ist eine Primzahl mit 1024 Stellen. Je länger, desto sicherer."

Internet: Weltweit ein Netz mit 30 Millionen Rechnern

Das Internet verbindet Computer auf der ganzen Welt. Schätzungen gehen von 30 Millionen Rechnern aus, die genaue Zahl kennt niemand.

tische Diskussionen oder Klatsch- und Tratsch-Runden einschalten. Mit einer e-Mail-Adresse kann man Post aus der ganzen Welt empfangen.

Ausschnitt aus einer Reportage zur CERT-Gründung aus dem Hamburger Abendblatt vom 25. August 1993

Am 2. November 1988 brach das Internet zusammen. Nun, nicht das gesamte Internet, welches zu diesem Zeitpunkt aus ca. 70.000 überwiegend in den USA laufenden Rechnern bestand, aber immerhin geschätzte fünf bis zehn Prozent aller Rechner waren außer Betrieb. Heute würde man dies einen erfolgreichen Denial-of-Service (DoS) Angriff nennen. Verantwortlich dafür war der Student Robert T. Morris, Sohn von Robert H. Morris, seines Zeichens Informatiker an dem zur NSA (National Security Agency) gehörenden NCSC (National Computer Security Center). Morris Jr. hatte einen Wurm geschrieben, wie derartige Malware damals genannt wurde. Diese Schadsoftware kann sich selbst verbreiten und ist dabei nicht auf Dinge wie zu öffnende E-Mail Anhänge, zu besuchende Webseiten oder klickende User angewiesen. Dieser Wurm, ursprünglich als simples Experiment zum Zählen von Rechnern gedacht, nutzte Schwachstellen und Konfigurationsprobleme in weit verbreiteten Anwendungen wie „rexec/rsh“, „sendmail“ oder „fingerd“ aus.

Der Wurm geriet jedoch völlig außer Kontrolle. Eigentlich hatte Morris Jr. eine Routine programmiert, die verhindern sollte, dass ein einmal infiziertes System erneut infiziert wird. Diese Routine war jedoch fehlerhaft. Ein „Bug“ sorgte dafür, dass bereits infizierte Systeme über den sogenannten „sendmail Debug-Modus“ immer und immer wieder infiziert wurden. Auf den betroffenen Systemen wurde dadurch eine derartig hohe Last erzeugt, dass diese nicht mehr benutzbar und damit unerreichbar waren. Außerdem schalteten etliche überforderte Administratoren infizierte Systeme einfach ab, um die Schäden zu begrenzen.

Experten verschiedener betroffener Institutionen gelang es recht schnell, den Wurm zu analysieren und die Systeme entsprechend zu bereinigen, jedoch wusste kaum jemand von den Bemühungen der Anderen. Während also die technische Analyse sowie die Behebung der Schwachstellen auf lokaler Ebene problemlos erfolgte, fehlte eine Institutionen übergreifende Koordination des Vorfalls komplett, nicht zuletzt in Ermangelung einer funktionierenden Kommunikationsinfrastruktur, da der Wurm die E-Mail-Kommunikation verhinderte.

Tatsächlich erfolgte jedoch zeitnah eine Aufarbeitung des Vorfalls auf übergeordneter Ebene. Nur knapp vier Wochen nach dem Vorfall lud die verantwortliche US-Behörde DARPA (Defense Advanced Research Projects Agency) zu einer Krisensitzung ein. Bereits wenige Wochen später wurden Projektmittel für die Etablierung eines Computer-Notfallteams an der Carnegie Mellon University in Pittsburgh zur Verfügung gestellt – das erste Computer Emergency Response Team (CERT) der Welt war geboren. Schon der Name dieses Teams sollte als Aufgabenfeld nicht nur die Reaktion auf Vorfälle („Emergency Response“) verdeutlichen, sondern auch deren übergreifende Koordination – das Team nannte sich offiziell CERT/CC (für „Coordination Center“).

Die Anfänge

Zügig gründeten sich auch in anderen Ländern weitere CERTs und mit der Gründung von FIRST – dem „Forum of Incident Response and Security Teams“ – existierte ab 1990 außerdem ein weltweiter Dachverband. Aus den anfänglich 11 Gründungsmitgliedern sind inzwischen über 400 CERTs geworden. Auch außerhalb der USA gab es nun zahlreiche Aktivitäten. Die europäischen Forschungsnetze hatten bereits eine Arbeitsgruppe zum Thema „Security“ etabliert, an der auch der DFN-Verein aktiv beteiligt war.

Im Jahr 1992 schrieb der DFN-Verein ein Forschungsprojekt zum Aufbau eines CERTs aus, welches der Fachbereich Informatik der Universität Hamburg für sich gewinnen konnte. Das Projekt stellte sich in den DFN Mitteilungen, Heft 31, vor:

> *Mit der Ausschreibung des Projekts „CERT im DFN - Aufbau und Betrieb eines Computer Emergency Response Teams (CERT) für das Deutsche Forschungsnetz" trug der DFN-Verein dem starken Interesse an einer Unterstützung bei der Lösung sicherheitsrelevanter Probleme Rechnung. Im Herbst 1992 schloss der DFN-Verein einen Vertrag mit der Universität Hamburg. […] Die Arbeit des Projektteams, das aus zwei wissenschaftlichen Mitarbeitern besteht, begann am 1. Januar 1993 und verläuft über eine Dauer von 18 Monaten. Für unterstützende Arbeiten werden zwei Studenten eingesetzt. […] Die Aufgaben des Projekts sind:*
>
> - *Zusammenarbeit mit anderen CERTs*
> - *Untersuchungen und Forschungen*
> - *Betreuung und Unterstützung*

Ein Grund dafür, dass das neue DFN-CERT am Fachbereich Informatik der Universität Hamburg etabliert wurde, war die Historie des Fachbereichs. Bereits seit den 1980er Jahren wurde unter der Leitung von Prof. Dr. Klaus Brunnstein zum Thema Sicherheit geforscht. Mit dem 4-semestrigen Vorlesungszyklus „IT Security and Safety“ war die Universität deutschlandweit Vorreiter in Sachen IT-Sicherheit. Im Sommer 1988 schließlich, also noch vor dem Ausbruch des Morris-Wurms, wurde das Virus Test Center (VTC) gegründet, ein über viele Jahre laufendes, sehr praxisnahes Projektseminar. Hier konnten die Studierenden unter anderem Computer-Viren disassemblieren und die bereits damals existierenden Antiviren-Programme testen. Und tatsächlich gehörten einige der VTC-Studierenden 1993 dann zu den ersten Mitarbeitern des DFN-CERTs.

„Damit das DFN-CERT seine Aufgaben erfolgreich wahrnehmen kann, steht der Aufbau notwendiger Kooperationen und Verbindungen mit nationalen und internationalen Gruppen im Mittelpunkt der ersten Monate. Hilfreich ist dabei die Zusammenarbeit mit der RARE CERT Task Force. Diese Projektgruppe der Dachorganisation der europäischen Netzorganisationen hat das Ziel, die Mitgliedsorganisationen bei der Gründung eigener CERTs zu unterstützen. Auch der direkte Anschluss an das amerikanische FIRST-System und die Kooperation mit Herstellern und nationalen Gruppen ist geplant.

Ein großer Teil der praktischen Tätigkeit des DFN-CERTs wird darauf ausgerichtet sein, Kontakt mit den DFN-Teilnehmern aufzunehmen und sie zu betreuen. Dazu sollen die Anwender gezielt angesprochen und zur Mitarbeit aufgefordert werden."

Das Zitat aus Heft 31 der DFN Mitteilungen gibt auch aus heutiger Sicht sehr gut wieder, welches die Schwerpunkte der DFN-CERT Mitarbeiter in den folgenden Jahren werden sollten. Die konkrete Ausrichtung auf den betreuten Anwenderkreis, also die DFN-Mitgliedseinrichtungen, und die Kooperation mit vergleichbaren Organisationen und Verbänden, gehören noch heute zu den wichtigsten Aufgaben des DFN-CERT. Tatsächlich ist das DFN-CERT nicht nur Mitglied in etlichen Verbänden, sondern gestaltet diese auch aktiv mit, z. B.

- FIRST (seit 1994)
- Deutscher CERT-Verbund
- Task Force (TF) CSIRT
- Trusted Introducer.

Zu den weiteren Meilensteinen gehörten ab 1996 der Aufbau und Betrieb der damals noch DFN-PCA genannten DFN-PKI sowie der Übergang von einem Forschungsprojekt in eine (zunächst gemeinnützige) GmbH im Jahr 1999.

Nach 25 Jahren ist aus dem mit vier Mitarbeitern ins Leben gerufenen Computer-Emergency-Response-Team für die Anwender des DFN ein hochspezialisierter Dienstleister für IT-Sicherheit mit gut 50 Mitarbeitern geworden. Dieses Wachstum war stets organisch und an den Bedarf des Hauptkunden, den DFN-Verein, ausgerichtet.

Fünf Teams, fünf Schwerpunkte

Das DFN-CERT strukturiert sich aktuell in fünf Teams, unterstützt durch eine Organisations-Gruppe, die unter anderem für den reibungslosen Ablauf der DFN-Konferenz für Sicherheit in vernetzten Systemen, die im Februar 2018 zum 25igsten Mal stattgefunden hat, verantwortlich zeichnet. Von den fünf Teams beschäftigt sich das **Incident Response-Team (IRT)** mit den Aufgaben, die ursprünglich für das Unternehmen namensgebend waren.

Das IRT erbringt mittels der Erstellung von Schwachstellenmeldungen, inklusive der Information zu verfügbaren Patches, eine präventive Dienstleistung zur Vorbeugung von Sicherheitsvorfällen. Es unterstützt bei der Aufdeckung und Analyse von akuten Sicherheitsvorfällen (Incident Handling), erstellt automatisierte Warnmeldungen über Auffälligkeiten im Netz des DFN und hilft bei der Analyse und Quellenbekämpfung von DoS-Angriffen. Schwachstellenmeldungen sowie automatische Warnmeldungen stehen den DFN-Anwendern über ein mittlerweile in zweiter Generation existierendes Sicherheitsportal zur Verfügung. Das Portal verfügt zusätzlich über einen Netzwerkprüfer, zur proaktiven Kontrolle der Konfiguration des eigenen Netzwerks.

Ein Hauptaspekt für die erfolgreiche Arbeit des IRT stellt die Beschaffung von Daten, deren Verifikation und Aggregation dar. Nicht zuletzt aufgrund der zu verarbeitenden Volumina ist hierfür eine automatisierte Verarbeitung durch spezialisierte Softwaresysteme erforderlich. Derartige Software ist nicht auf dem Markt verfügbar, sondern wird vom **Projekt und Entwicklungs-Team (PET)** des DFN-CERT entwickelt.

Das PET erstellt sowohl Software für die interne Nutzung, zu der u. a. das Autorensystem für die Erstellung und Verwaltung von Schwachstellenmeldungen zählt, als auch Software für Projekt- und Kooperationspartner. Diese Software wird dabei vor allem im Rahmen von internationalen Projekten entwickelt, die den Austausch von Vorfallsdaten und die Bereitstellung technischer Plattformen unter Einhaltung der nationalen und europäischen Datenschutzanforderungen und Gesetze zum Ziel haben. Durch derartige Projekte leistet das PET einen essenziellen Beitrag zur internationalen Vernetzung des DFN-CERT und der Beschaffung einer nutzbringenden Datenbasis zur Versorgung der DFN-Anwender mit Vorfallsdaten.

Neben einigen Projekten im Bereich der Sensorik ist das ACDC-Projekt (http://www.acdc-project.eu) besonders erwähnenswert. In diesem Projekt wurden erstmals europaweit rechtliche und technische Grundlagen für einen einfachen Datenaustausch gelegt. Im Nachgang des Projektes hat das DFN-CERT den Betrieb und die Verwaltung der zentralen Datenaustauschkomponente (ACDC-CCH) übernommen und arbeitet kontinuierlich an der

Aufrechterhaltung und Ausweitung des etablierten Datenaustauschs.

Zusätzlich werden in Hamburg auch Komponenten entwickelt, die für einen sicheren Netzbetrieb notwendig und speziell auf die Anforderungen des DFN ausgerichtet sind. So ist eine auf die im DFN eingesetzten Router zugeschnittene Messplattform entstanden, sowie auch eine Unterstützung der Peering-Planung. Außerdem wurde „NeMo“ entwickelt, eine Software für den DoS-Basis-Dienst und den Selbstschutz des X-WiN gegen DoS-Angriffe. Datenschutzaspekte und das Ziel, minimalinvasiv in den Netzwerkverkehr des Forschungsnetzes einzugreifen, machten hier eine eigene Entwicklung notwendig. Die entstandene Software stieß auf nachhaltiges Interesse auch bei anderen Forschungsnetzen und wird jetzt vom DFN-Verein diesen Forschungsnetzen bereitgestellt.

Die Erbringung der Dienste, der internationale Datenaustausch und die Kooperation in Projekten erfordern auch den sicheren und stabilen Betrieb von Informationstechnologie. Dafür ist das **IT-Service (ITS) Team** verantwortlich.

Das ITS-Team stellt die Netzwerk- und Basis-IT-Infrastruktur für das DFN-CERT bereit. Außerdem betreibt und überwacht es Dienste wie z. B. das Sicherheitsportal. Darüber hinaus ist es für die Bereitstellung sämtlicher Endgeräte, IT-Dienste und der technischen Basisinfrastruktur für die Mitarbeiter des DFN-CERT zuständig. Aufgrund der Sensitivität der verarbeiteten und bereitgestellten Daten gehört die Absicherung der Systeme zu den Kernkompetenzen des Teams.

Das ITS-Team setzt das Wissen über den Betrieb von IT-Infrastrukturen nicht nur im Tagesgeschäft ein, sondern nutzt dieses auch zur Unterstützung von Entwicklungsprojekten, wie zum Beispiel der bereits erwähnten DoS-Abwehrplattform oder dem Aufbau von Sensorik.

25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ *Foto © Nina Bark / DFN-Verein*

Ein aktueller Themenschwerpunkt ist die Auswertung der durch die Sensorik erfassten Daten für ein mögliches DFN-SOC (Security Operations Center). Darüber hinaus unterstützt das ITS-Team Kunden und Projektpartner bei der Installation und Inbetriebnahme von Softwaresystemen, die durch das PET entwickelt wurden und außerhalb des DFN-CERT Rechenzentrums betrieben werden sollen.

Seit 1996 bietet das DFN-CERT auch Nutzer- und Geräte-Authentifizierung als Dienstleistung an. Lag der Schwerpunkt anfangs noch auf Forschungsaktivitäten, so hat sich inzwischen die Bereitstellung von Zertifikaten im X.509 Standard als Hauptaufgabe eines eigenen Teams herauskristallisiert. Die sichere Authentifizierung von Nutzern und Geräten ist ein Kernbaustein von vernetzten Diensten, Public-Key-Infrastrukturen (PKI) mit X.509-Zertifikaten liefern hierfür in vielen Szenarien eine geeignete Lösung. Das **PKI-Team** passt das Angebot weiterhin kontinuierlich an sich ändernde Rahmenbedingungen, wie die vom Gesetzgeber vorgegebene eIDAS-Verordnung oder das IT-Sicherheitsgesetz und an die Bedürfnisse der Nutzer an.

Die DFN-PKI ist mit über 1,8 Millionen ausgestellten Zertifikaten (seit 2005) die größte vom CERT betriebene PKI. Sie bietet den Anwendern die Möglichkeit, Nutzer- und Server-Zertifikate zu beziehen, die mit einem Vertrauensanker direkt in den Betriebssystemen und Browsern als vertrauenswürdig eingestuft werden. Hierfür muss die DFN-PKI die Baseline Requirements des CA/Browserforums und die Sonderregeln der Root-Programme von Mozilla und Microsoft einhalten sowie ein jährliches Audit nach dem Standard ETSI EN 319 411-1 durch den TÜViT bestehen.

Neben der Pflege und Erweiterung der Software sowie der Bereitstellung der Validierungsdienste (CRL und OCSP) übernimmt das PKI-Team auch Aufgaben im Rahmen des Teilnehmer-Enrollments. So auch die Verifikation von Organisationsnamen, Domains und IP-Adressbereichen. Außerdem berät das Team Anwender rund um den Einsatz und die Erzeugung von Zertifikaten auf verschiedensten Geräten.

Anforderungen des Gesetzgebers sowohl an die IT-Sicherheit als auch den Datenschutz stehen in besonderem Fokus des fünften Teams, das zugleich das jüngste Team im DFN-CERT ist. Das **CAT-Team (Consulting, Analysis und Training)** unterstützt Anwender beim Aufbau eigener CERTs und SOCs sowie bei der Planung und Implementierung von Informationssicherheits- (ISMS) und Datenschutzmanagementsystemen (DSMS). Das Beratungsteam findet auch Antworten auf Einzelfragen der Sicherheit und der Umsetzung datenschutzrechtlicher Anforderungen in die Praxis.

Aufgrund der interdisziplinären Besetzung und der langjährigen Erfahrung im Hochschul- und Forschungsbereich können dabei alle rechtlichen, technischen und organisatorischen Anforderungen berücksichtigt werden. Das CAT-Team führt im Auftrag von Anwendern auch Überprüfungen von bereits ergriffenen Sicherheitsmaßnahmen mit Penetrationstests oder umfassenden Risikoanalysen durch. Das erworbene Know-How gibt das Team im Rahmen von Konferenzen, Workshops und Tutorien weiter. Wesentliche Schwerpunkte der gegenwärtigen Beratung sind die Umsetzung der Anforderungen zum Datenschutz aus der EU-Datenschutzgrundverordnung (EU-DSGVO), der Aufbau von CERTs und SOCs an Hochschulen und Forschungseinrichtungen und die sichere und datenschutzgerechte Implementierung von modernen Campus-Managementsystemen mit einem hohen Grad der Digitalisierung von Arbeitsprozessen. Aufgrund der fortschreitenden Digitalisierung der Verwaltungsprozesse in Lehre und Forschung werden diese Themen zusammen mit der sicheren und datenschutzgerechten Implementierung von Prozessen in den nächsten Jahren auch weiter einen Schwerpunkt des CAT-Teams bilden.

Danke für 25 Jahre erfolgreiche Zusammenarbeit

An den verschiedenen Ausrichtungen der Teams innerhalb des DFN-CERT lässt sich ablesen, wie vielfältig heutzutage der Bedarf im IT-Security-Bereich geworden ist. Bei aller Differenzierung geht es dem DFN-CERT aber auch 25 Jahre nach der Gründung darum, Sicherheit in einer vernetzten Welt zu fördern.

Diese Leidenschaft für Sicherheit kanalisieren wir in Dienste und Services, die Ihnen, unseren Anwendern, die tägliche Arbeit im Umgang mit IT-Sicherheit leichter machen sollen. Das planen wir auch für die nächsten Jahrzehnte! ◆

Der Blick durch die Kanzlerbrille

Die Digitalisierung ist für ihn Chefsache: Christian Zens, Kanzler an der Friedrich-Alexander-Universität Erlangen-Nürnberg. *Foto © Frank Homann*

Seit Ende 2017 ist Christian Zens stellvertretender Vorstandsvorsitzender im DFN-Verein. Zuvor gehörte er schon als Gast dem Verwaltungsrat an und vertrat dort als Universitätskanzler die Belange deutscher Hochschulleitungen. 12 Jahre Kanzlerschaft haben ihn eines gelehrt: Grundneugier, Empathie und Kommunikationstalent gehören zum Rüstzeug eines Hochschulkanzlers. Welche Herausforderungen er bei seiner Arbeit zu meistern hat, erzählt er im Interview.

Herr Zens, seit Ende 2017 sind Sie Mitglied im DFN-Vorstand. Sie und der DFN-Verein, sind das gute alte Bekannte?

Es fühlt sich auf jeden Fall so an. Bei meinen ersten Schritten als Kanzler war der DFN-Verein von Anfang an dabei. 2007 wurde ich zum Kanzler der Europa-Universität Viadrina Frankfurt (Oder) ernannt. Als Quereinsteiger kam ich aus einer klassischen hierarchisch aufgebauten Bundesverwaltung in eine Universitätsverwaltung mit komplexen Organisationsstrukturen. Das war eine ganz schöne Umstellung – und auch ein Lernprozess. Hochschulen ticken einfach anders. Von Hause aus Jurist, hatte ich einige Lücken zu schließen bei meiner neuen Tätigkeit. Ich wusste zwar, was der DFN-Verein macht, aber mein erster Zugang war die Forschungsstelle Recht im DFN mit ihren tollen umfangreichen Dienstleistungen und Rechtsberatungen. Ich nahm damals an einer Reihe von Seminaren teil, die mir bei meiner täglichen Arbeit als Verwaltungschef sehr geholfen haben. Später vertrat ich im Verwaltungsrat des DFN die Belange der Kanzlerinnen und Kanzler und war direkter Mitgliedsvertreter der Viadrina. Den DFN-Verein und mich verbindet bis heute ein gemeinsamer produktiver Weg.

„Es geht nicht darum, auf jeden Zug der Digitalisierung aufzuspringen."

Sie sind seit 2014 Leiter des Arbeitskreises Hochschul-IT der Vereinigung der Kanzlerinnen und Kanzler der Universitäten Deutschlands. Was hat ein Kanzler mit IT und Digitalisierung zu schaffen?

Das Thema Digitalisierung liegt nicht erst seit gestern auf meinem Tisch, es ist seit mindestens 15 Jahren prominent. Die nachhaltige Einbindung von Informations- und Kommunikationstechnologien (IuK-Technologien) hat für eine Hochschule eine zukunftsweisende Bedeutung und entscheidet auch über ihre Wettbewerbsfähigkeit. Das betrifft nicht nur Wissenschaftlerinnen und Wissenschaftler, sondern auch die Verwaltung als modernen Dienstleister. Als Kanzler trage ich die Verantwortung für die administrative Steuerung universitärer Kernprozesse in Forschung und Lehre. Als Beauftragter für den Haushalt ist es mein Job, die finanziellen und personellen Mittel bereitzustellen, damit eine funktionierende digitale Infrastruktur umgesetzt

Foto © Maimona Id / DFN-Verein

werden kann. Es geht nicht darum, einzelne Lösungen zu finden oder auf jeden Zug der Digitalisierung aufzuspringen. Die Umsetzung großer IT-Projekte zieht viele Changemanagementprozesse nach sich. Sie haben in der Regel sehr viel Bedarf an Customizing, der Anpassung bestehender Systeme an die hochschuleigenen Bedürfnisse. Kern meiner Arbeit ist ein maßgeschneidertes funktionierendes Projektmanagement. Ich blicke dabei durch die Brille eines Organisationsentwicklers.

Welche Rolle spielt der Arbeitskreis Hochschul-IT?

Im Arbeitskreis Hochschul-IT geht es um Themen von strategischer Relevanz wie etwa Personal, Finanzen oder Rechtsfragen. Das Thema Digitalisierung ist viel zu komplex, um es allein auf das Technische zu reduzieren. Eine strategische ganzheitliche Sicht ist mindestens genauso wichtig. Wir Kanzlerinnen und Kanzler sind Generalisten, keine Spezialisten! Die Spezialisten sind die Chief Information Officer (CIO) und die Kolleginnen und Kollegen aus den Rechenzentren oder dem DFN-Verein. Deren fachliche Expertise benötigen wir, damit wir Informationen zu aktuellen Tendenzen und Entwicklungen in der Kommunikationstechnologie erhalten und zu einer umfassenden Bewertung gelangen können. Darum habe ich unter anderem angeregt, dass wir einen regelmäßigen Austausch mit den Kolleginnen und Kollegen des Vereins „Zentren für Kommunikationsverarbeitung in Forschung und Lehre“ (ZKI e. V.) – der Vereinigung der IT-Servicezentren der Hochschulen, Universitäten und Forschungseinrichtungen in Deutschland – pflegen. Deren Ziele sind vielleicht nicht immer deckungsgleich mit den Zielen der Kanzlerinnen und Kanzler. Aber im Sinne eines guten Netzwerks versuchen wir, die Themenschwerpunkte wie Big Data oder digitale Bildungsangebote zu diskutieren und aufeinander abzustimmen.

> „Das Thema Digitalisierung ist viel zu komplex, um es allein auf das Technische zu reduzieren.“

Was sind die Voraussetzungen für die Umsetzung der Digitalisierungsprozesse?

Ein hochschulweites IT-Konzept ist aus meiner Sicht für das Gelingen zwingend notwendig. Darum habe ich seinerzeit an der Viadrina einen Chief Information Officer (CIO) eingesetzt. CIO haben den Vorteil, dass sie als Beauftragte der Präsidenten oder Kanzler unmittelbaren Zugang zu den Universitätsleitungen haben. An der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) gab es bereits diese Position sowie ein CIO-Gremium. Mit dem CIO-Gremium arbeite ich sehr eng zusammen. Die Aufgabe dieses Gremiums ist es, auf Grundlage unserer hochschulpolitischen Ziele eine IuK (Informations- und Kommunikation)-Strategie zu entwickeln und in die Gesamtstrategie der Hochschule einzupassen. Unser Rechenzentrum ist ein wichtiger Baustein unserer Gesamtstrategie. Leider wird die IT an den Hochschulen manchmal so ähnlich behandelt wie der Strom aus der Steckdose. Er ist existenziell, aber keiner fragt sich, wo er herkommt. Wir nehmen mittlerweile einen hohen Service-Level im IT-Bereich als selbstverständlich in Anspruch. Ich schaffe es vielleicht nicht, jeden dafür sensibilisieren, aber es wäre schön zu verdeutlichen, welche Herausforderungen die Rechenzentren im Allgemeinen zu meistern haben und wie viel Know-how, Technik und kluge Personen dahinter stecken.

> „Hochschulen sind hochfragmentierte Organisationen.“

Welche Herausforderungen meinen Sie?

Hochschulen sind hochfragmentierte Organisationen. Das heißt, die einzelnen sehr verschieden geprägten Fakultäten verfolgen ihre berechtigten Eigeninteressen. Arbeitsweisen und Anforderungen in Bezug auf IuK-Bedarfe sind in den verschiedenen Disziplinen einer großen Universität äußerst heterogen. Da sind Fliehkräfte am Werk, die nicht so einfach einzufangen sind. Letztendlich geht es darum, gemeinsam zu entscheiden, welche technischen Entwicklungen oder

Themenschwerpunkte für die gesamte Institution künftig richtungsweisend sind. Das ist eine Frage der Priorisierung. Darum sind in unserem CIO-Gremium auch verschiedene Interessensgruppen wie Studierende oder Kolleginnen und Kollegen aus der Bibliothek vertreten. Mir ist es wichtig, gemeinsam mit unserem Rechenzentrum die relativ stark dezentralisierte Struktur zu konsolidieren, also zu einer Dienstleistung aus einer Hand zu kommen.

Wissen denn die Endnutzer, welche Dienstleistungen – unter anderem die des DFN – ihr Rechenzentrum vorhält?

Je weiter entfernt die einzelnen Nutzer vom Rechenzentrum sind, umso weniger weiß man übereinander Bescheid. Wenn ich unsere Lehrstuhlarbeit betrachte, gibt es durchaus – wenn die Kapazitäten und Fähigkeiten es hergeben – Eigenentwicklungen bei den einzelnen Fakultäten. Das führt in der Summe zu einer Heterogenität der einzelnen Systeme. Die Fachgebiete haben teilweise gar nicht auf dem Schirm, welche guten Beratungsmöglichkeiten und Dienstleistungen das eigene Rechenzentrum anbietet. Das beinhaltet auch die DFN-Dienste. Ich finde, das ist ein Stück weit die Bringschuld der Hochschulverwaltung darauf hinzuweisen, dass der DFN-Verein im Einzelfall weit bessere Alternativen bietet. Von meiner Ebene aus kann ich die Fakultätsverwaltungen und Dekanate mit einbeziehen. Rechenzentren wiederum kommen mit Endnutzern persönlich in Kontakt, wenn es beispielsweise darum geht, einen Computerarbeitsplatz einzurichten. Dabei könnten sie gleich über die DFN-Dienste informieren. Wir müssen da, glaube ich, über mehrere Kanäle parallel tätig werden.

Foto © Maimona Id / DFN-Verein

Beschweren sich die Rechenzentren über zu wenig Unterstützung?

Ich sehe das nicht als Beschwerde. Selbstverständlich versuchen sie, auf die Folgen fehlender Ressourcen hinzuweisen. Der technologische Wandel geht mit der Einführung neuer Dienste einher und führt auch zu neuen Organisationsabläufen. Dafür benötigt man in aller Regel ausreichendes Personal. Das fordern die Rechenzentren ein – und das auch zu Recht. Für Kanzlerinnen und Kanzler ist es allerdings schwierig abzuschätzen, was tatsächlich jenseits aller Technik an Personalbedarf dahintersteckt. Einfach weil wir in den Abläufen wie etwa 24-Stunden-Bereitschaftsdiensten viel zu wenig drinstecken. Um das beurteilen zu können, müssen wir tiefer ins Detail gehen. Das sind letztendlich Infrastrukturfragen, die ich als Kanzler im Blick haben muss. Ich habe immer einen sehr engen Kontakt zu meinen Rechenzentrumsleitern gepflegt und für deren Interessen gekämpft. Das setze ich auch an der FAU fort. Was man nicht vergessen darf: Wir reden im Endeffekt über sehr viel Geld. Im High Performance Computing (HPC) etwa sind das Summen, die Hochschulen in ihre Kalkulationen mit einbeziehen müssen. Alles, was wir hier an Geld zusätzlich benötigen, müssen wir in der Regel an anderer Stelle kürzen.

> „Wir reden hier über Gesamthaushalte einzelner Universitäten im Bereich einer halben Milliarde Euro pro Jahr."

Das hört sich schwierig an.

Das ist ein stetiger Aushandelsprozess – und Teil meiner Arbeit. Da gibt es durchaus sehr unterschiedliche Interessenslagen an einer Universität. Heutzutage sind Hochschulen nicht nur hoheitlich unterwegs. Im wirtschaftlichen Bereich legen sie immer mehr zu. Wir reden hier über Gesamthaushalte einzelner Universitäten im Bereich einer halben Milliarde Euro oder mehr pro Jahr. Das funktioniert nicht ohne professionelles Finanzmanagement. Das Einwerben von Drittmitteln ist ein wichtiger Bestandteil der Hochschulfinanzierung. Im vergangenen Jahr hat zum Beispiel die FAU zum ersten Mal die 200-Millionen-Marke geknackt. Dieser Erfolg ist auch und vor allem auch der Exzellenz unserer Wissenschaftlerinnen und Wissenschaftlern geschuldet, die die Fördermittelgeber mit ihrer Expertise und ihrem Renommee überzeugen können. Das zeigt, wie wichtig es ist, im Wettbewerb um die besten Köpfe vorne zu liegen.

CHRISTIAN ZENS, STELLVERTRETENDER VORSTANDSVORSITZENDER DES DFN-VEREINS

Studium der Rechtswissenschaften an der Ludwig-Maximilians-Universität München | nach dem Referendariat 1991 Eintritt in die Bundesfinanzverwaltung, tätig als langjähriger Leiter des Bundesvermögensamtes Frankfurt (Oder), aber auch als Referent im Bundesfinanzministerium | von 2007-01/2017 Kanzler der Europa-Universität Viadrina Frankfurt (Oder), zugleich Geschäftsführer der universitätseigenen Weiterbildungsgesellschaft VSM Viadrina School of Management gGmbH | Seit 2014 Leiter des Arbeitskreises Hochschul-IT im Bundesarbeitskreis der Kanzlerinnen und Kanzler der Universitäten Deutschlands | Seit Februar 2017 Kanzler der Friedrich-Alexander-Universität Erlangen-Nürnberg

Apropos Wettbewerbsfähigkeit: wie sieht es denn mit der Internationalisierung aus?

An der FAU wurde die Internationalisierung schon früh getriggert. Neben den Studierenden geht es an der FAU maßgeblich um die Internationalisierung unserer Professorenschaft und des akademischen Mittelbaus. Das betrifft mittlerweile ebenso den Bereich des wissenschaftsunterstützenden Personals. Unsere Forscher sind international stark vernetzt. Da können sie als Verwaltung nicht sagen, bei uns ist die Amtssprache aber ausschließlich Deutsch. Da geht es darum, eine Willkommenskultur und Serviceorientierung zu schaffen. Das ist nicht einfach ein „nice to have“, sondern heutzutage eine Notwendigkeit. Wir wollen, dass fähige Senior- und Nachwuchswissenschaftler einen Grund haben, zu uns zu kommen. Denn – um wieder auf die Wettbewerbsfähigkeit zu kommen – wir stehen nicht nur national, sondern auch international mit anderen Arbeitgebern im Wettbewerb um gute Arbeitskräfte. In einem Bundesland, das eine extrem niedrige Arbeitslosenquote hat, ist es sehr schwierig, qualifiziertes Fachpersonal zu finden. Wir merken ganz deutlich die aktuelle Hochkonjunkturphase.

Womit können Sie letztendlich punkten?

Eine ideale Forschungs-Infrastruktur gehört heute zu einem attraktiven Gesamtpaket für Forscherinnen und Forscher dazu. Mit seinem Hochleistungsnetz X-WiN, den entsprechenden Bandbreiten und Dienstleistungen stellt der DFN-Verein das notwendige Gerüst zur Verfügung. Mithilfe der digitalen Kommunikationstechnologien können sich unsere Wissenschaftler mit ihren Kollegen im Ausland vernetzen und große Datenmengen in einem sicheren Umfeld austauschen. Ohne diese Möglichkeiten wären internationale Kooperationen heute nicht mehr möglich.

Kommen wir auf Ihre ehrenamtliche Tätigkeit im Vorstand zu sprechen. Wie möchten Sie sich neben ihren Schwerpunkten der rechtlichen und sicherheitsrelevanten Fragen rund um den DFN-Verein noch einbringen?

Am DFN-Verein, den ich als sehr professionell erachte, schätze ich besonders, dass er stark mitgliederbezogen ist. Es sind häufig die Kolleginnen und Kollegen aus den Rechenzentren, die die Mitgliedsrechte der Einrichtungen wahrnehmen. Sie haben sich bisher auch etwas deutlicher eingebracht als die Universitätsleitungen. Die Viadrina habe ich lange Zeit persönlich vertreten in den Mitgliederversammlungen. Daher war ich immer sehr gut auf dem Laufenden. Als stellvertretender Vorstandsvorsitzender möchte ich die Anliegen der Kanzlerinnen und Kanzler in den DFN-Verein immer wieder einbringen und mich dafür einsetzen, dass die Informationen, Dienste und Entwicklungen des DFN in den Universitätsleitungen stärker wahrgenommen werden.

Sie stehen in Ihrem 12. Jahr als Hochschulkanzler. Ist das ein Traumjob für Sie?

Also nicht Traumjob in dem Sinne, dass ich schon als Student davon geträumt hätte, Kanzler zu werden. Aber ja, vom Aufgabenfeld her ist es ein Traumjob, weil es eine sehr erfüllende Tätigkeit ist. Ich habe jeden Tag mit Menschen zu tun. Empathie und Kommunikationstalent spielen eine große Rolle. Aber auch Widerstandsfähigkeit und ein gutes Bauchgefühl sind hilfreich. Was mir aber bei meiner Arbeit immer geholfen hat, das ist eine gewisse Grundneugierde. Ich finde es extrem spannend, mit welchen Fragestellungen sich unsere Forscherinnen und Forscher beschäftigen, auch wenn ich es oft nicht verstehe. Mit welcher intrinsischen Motivation sie sich auf ihre Forschung konzentrieren, das empfinde ich persönlich als sehr befriedigend und bereichernd.

> „Empathie und Kommunikationstalent spielen eine große Rolle.“

Das Interview führte **Maimona Id** (DFN-Verein).

eduVPN - securing your privacy when you are out and about

eduVPN enables employees, researchers and students on untrusted Internet connections to easily and securely connect to the Internet or gain access to their institutes protected systems.

Text: **Rogier Spoor** (SURFnet), **Tangui Coulouarn** (DeiC), **François Kooman** (SURFnet)

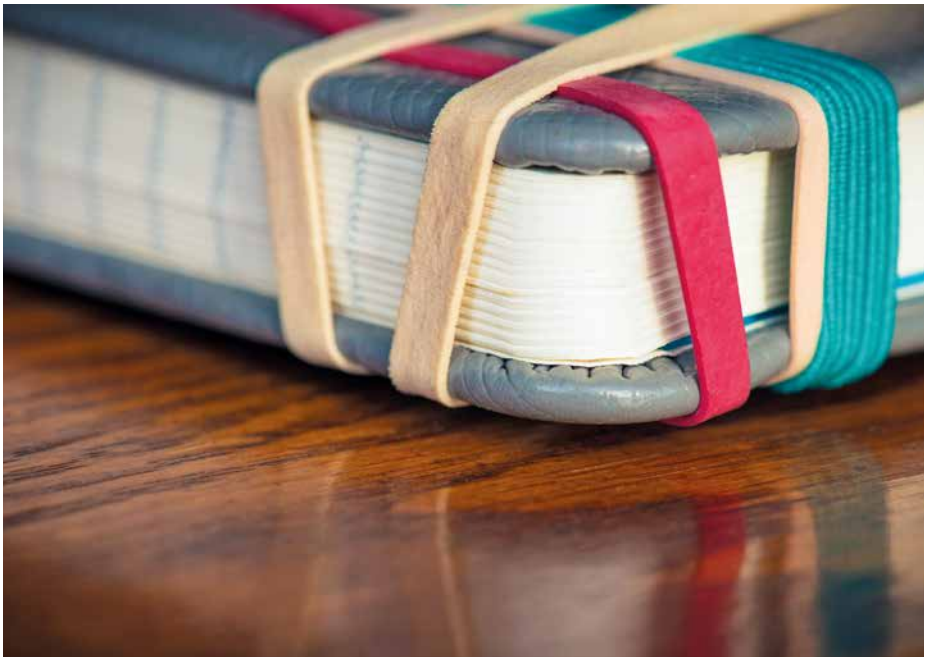


Foto © georgeclerk/iStock

Many public Wi-Fi networks, for example on the train, in the library or in restaurants are insecure, but your home network is not always safe either. Some crucial parts of your Internet traffic may be intercepted despite transport encryption. Malicious people can also divert you to a phishing-website in order to intercept your password. Not a comforting thought, especially if you are processing sensitive information.

The eduVPN service solves this by setting up a so-called Virtual Private Network (VPN), an encrypted connection between your computer or smartphone and a trusted end-point, which carries your entire Internet traffic securely through the untrusted Internet access. This end-point may be operated by your home institution, the National Research Network (NREN) of your country, or the NREN of the country you are currently in. This will allow you to connect securely to the Internet without the fear of prying eyes.

Background

As hinted at by its name, eduVPN is a software-based VPN solution tailored specifically for the research and education community. It is based on the OpenVPN protocol and it contains a series of extra features, (e.g. support of SAML for authentication) as well as client apps for most common platforms.

eduVPN started at SURFnet as a proof-of-concept in 2013, but has grown into a full-fledged production service in 2018. As the interest grew in the NREN community, eduVPN was established as a programme under the Commons Conservancy foundation[1]. In January 2018, it was introduced in the GÉANT project for maturing and governance.

Who is eduVPN for?

- For students, researchers and employees: an easy to use VPN app.
- For NRENs and institutes: Secure and privacy friendly VPN software one can deploy themselves.

What are the key strengths of eduVPN?

- focus on security and strong cryptography;
- Integrate seamlessly with existing Identity Management Systems
- completely open-source, both server and clients;
- focus on privacy and GDPR compliance.

1 https://commonsconservancy.org/programmes/

Inspired by eduroam

The eduVPN project has been inspired by eduroam. From the start, with a handful of European universities, the eduroam service has grown to cover over 70 countries and tens of thousands of WiFi hotspots on every continent around the globe.

The strengths of eduroam:

- a solid technical design (802.1x),
- trust framework for authenticating users, cross country and domain,
- any educational/research institute can join,
- governance and policies are in place,
- allow for guest access,
- governance under GÉANT auspices.

How have we applied the eduroam strengths to eduVPN?

- a solid VPN software design based on OpenVPN combined with SAML support and apps for Windows, Linux, iOS, macOS and Android,
- eduVPN supports eduGAIN for authentication,
- all eduVPN software has been open-sourced and will be audited. This empowers any institute to start running their own eduVPN server,
- eduVPN supports guest access. This means it is possible to connect to an eduVPN server in another country,
- governance will be put under GÉANT auspices.

In the GÉANT project, which was started in January 2018, we are working on the governance and policies of eduVPN.

Connect to other countries

Like eduroam, which allows guest Wi-Fi access at non home institutes, eduVPN allows guest VPN access for foreign eduVPN servers. On the authorisation-layer a trust has been created between the eduVPN servers run by different institutes. Why is this useful? When you are abroad, for example in Brazil, connecting to an eduVPN server in Europe will result in high latency. Service like video conferencing and web browsing will likely be affected by this. This is worsened by the fact that DNS services are also tunnelled, which adds even more latency. User experience significantly improves by using a nearby eduVPN server. That is why we have chosen to implement the same kind of guest access functionality that eduroam has. This basically means that users can – as a guest – use the eduVPN servers in other countries for simple secure Internet access.

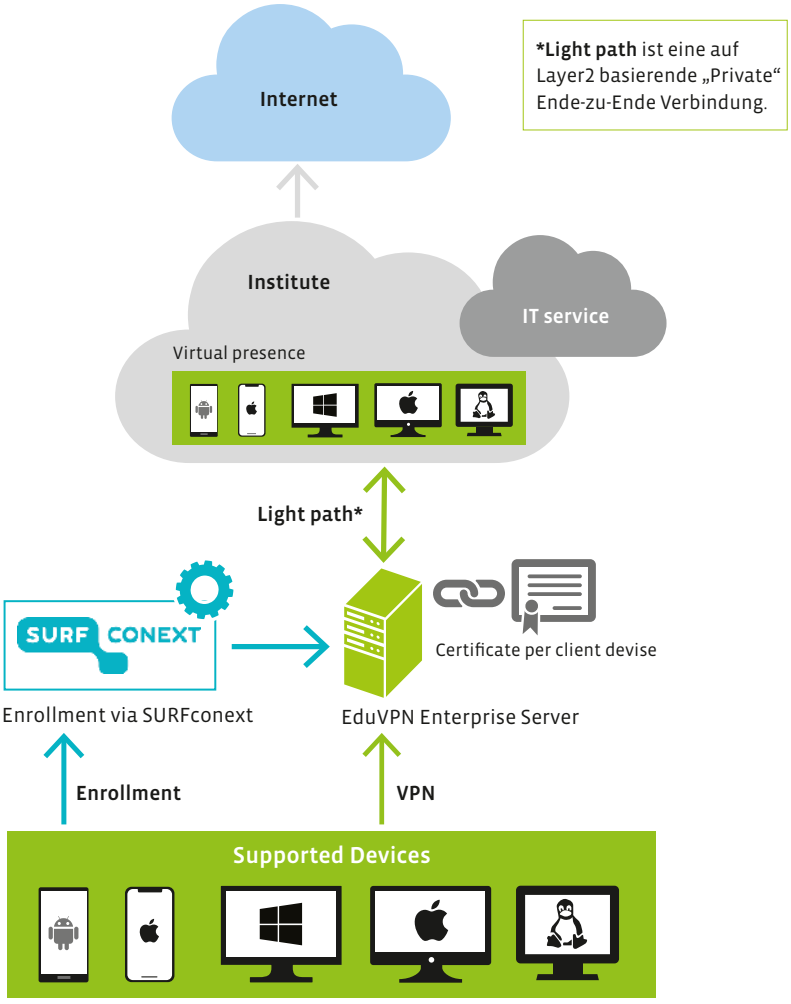


Figure 1: "Institute Access" technical design via lightpath @SURFnet

Security aspect

A VPN service should be in itself very secure. In the last years, we have seen large security vulnerabilities in commercial VPN solutions from big hardware vendors such as Cisco ASA and Juniper Netscreen. In order to improve the security of VPN services Security researchers stress the importance of:

- open standards,
- open source software,
- keep it simple,
- regular audits,
- proven cryptography.

In eduVPN project we have focussed on applying these best practices as much as possible. OpenVPN was chosen as "core" VPN technology because it is open source and has been audited by an international community. OpenVPN also works better than for example IPsec in restricted environments, such as firewalled networks,

Sucht man im Internet nach VPN-Diensten, so findet man viele Links, die auf kommerzielle Anbieter hinweisen, z. B. die zehn besten VPN-Dienste. Viele Einrichtungen im DFN betreiben entweder selber einen VPN-Dienst oder nutzen einen kommerziellen Anbieter, dass Bedarf für ein VPN-Dienst in den Einrichtungen im DFN besteht, ist daher offensichtlich. Problematisch kann jedoch sein, dass jede Einrichtung im DFN unterschiedliche VPN-Protokolle einsetzt, manche Einrichtungen setzen auf OpenVPN, andere auf IP-Sec und wieder andere Einrichtungen setzen auf kommerzielle VPN-Anbieter. Dabei kann es im Roaming-Fall vorkommen, z. B. in einem öffentlichen Netz, dass gerade diese oder jene VPN-Protokolle mit den entsprechenden Kommunikations-Ports vor Ort gar nicht unterstützt werden und der Nutzer seinen VPN-Dienst nicht nutzen kann.

Vor allem an dieser Stelle kann eduVPN die Lösung sein. Der Dienst verwendet ein vordefiniertes VPN-Standard Protokoll (openVPN). Durch dieses ist es möglich, ein einheitliches, funktionierendes VPN-Verfahren einzuführen, welches kombiniert mit einer AAI wie z. B. der DFN-AAI weltweit eingesetzt werden kann, genau wie in eduroam durch das 802.1X Verfahren. Auch die DFN-Geschäftsstelle plant daher, genau wie NORDUnet, DeiC, AARnet und UNINETT, eduVPN zu pilotieren. Sollten Sie Interesse haben, am Piloten teilzunehmen, so nehmen Sie bitte Kontakt mit uns auf: eduVPN@dfn.de.

because it is able to hide the VPN traffic. Currently OpenVPN isn't an open standard but there is work in progress. OpenVPN supports a variety of cryptography ciphers and after consultation of crypto experts AES-256-GCM was chosen.

Privacy

Privacy is fundamental but unfortunately also increasingly scarce on the Internet. eduVPN strengthens the user's security and privacy by enabling institutions, students, teachers, employees and researchers to connect securely to the Internet and their institution network wherever they are. eduVPN has been developed with privacy and security in mind from the very beginning of the project.

Privacy by design: A differentiator between eduVPN and commercial solutions lies in the use of federated identity, which de facto separates the authentication of users and the delivery of VPNs. It is possible to identify the user in case of abuse, but even in case of a full security breach of the eduVPN server no personal data can be retrieved from the server.

eduVPN collects, stores and logs information. The information is used for providing the eduVPN service, auditing and analysis in order to maintain, protect and improve eduVPN. Main principles regarding data collection are:

- don't collect personal information or data when it is not necessary,
- never use personal data for other purposes than those for which the personal data were initially collected.

How to deploy eduVPN

We determined two use cases for eduVPN:

- Secure Internet: go online safely at public hotspots,
- Institute Access: access to the institute's network.

The "Secure Internet" use case provides VPN protection for users who go online on public WiFi hotspots. These WiFi hotspots are generally not encrypted, so basically the traffic between the device and the access point is not protected by the access point. When using eduVPN the traffic between the device and the eduVPN server will be fully encrypted. Local eavesdropping or injecting data is impossible.

The "Institute Access" use case concerns the use of eduVPN for private network access. In this use case, authorised end-users (students, researchers or employees of higher education) are enabled to have access to some protected resources/networks in their home institutions or other institutions. In practice, end-users can use the same apps as for the Secure Internet scenario by choosing another profile, the difference lies in the network they have access to behind the server.

SURFnet has decided to offer "Institute Access" like a typical cloud service. The eduVPN servers are centrally located in a twin-datacenter and via a layer-2 link a connection into the institute has been created. This is shown in the figure 1.

eduVPN is open-source software and has been put on GitHub2. The GitHub repositories also include documentation regarding the technical design and deployment. Installing and deploying an eduVPN for the use case "Secure Internet" is easy.

Interested?

At this moment SURFnet is offering eduVPN as an official supported service in the Netherlands. NRENs NORDUnet, DeiC, AARnet and UNINETT are currently piloting and testing the eduVPN concept. Other institutes willing to pilot the eduVPN are welcome. For more information, please contact via email: eduVPN@SURFnet.nl ◆

2 https://www.github.com/eduvpn

Virtuelle Netze leicht gemacht

Im europäischen Wissenschaftsnetz GÉANT ist ein Generalized-Virtualization-Service (GVS) aufgebaut worden. Die GVS-Architektur stellt voneinander isolierte virtuelle Netze zur Verfügung. Nutzer können sich virtuelle Ressourcen (z. B. Rechnerkapazität, Speicherplatz oder Switching-/Routingkapazitäten) und virtuelle Netzstrukturen selbstständig zusammenstellen und damit eine eigene virtuelle Netzumgebung für betriebliche oder experimentelle Zwecke erzeugen. In den DFN Mitteilungen Nr. 89 und Nr. 90 wurden bereits wichtige Eigenschaften des GÉANT-Testbeds-Services (GTS) beschrieben; dieser ist nun als festes Dienstangebot nutzbar und wurde dafür in Generalized-Virtualization-Service (GVS) umbenannt.

Text: **Dr. Peter Kaufmann** (DFN-Verein), **Dr.-Ing. Susanne Naegele-Jackson, Sascha Schweiger, Philipp Seyerlein** (RRZE)

Foto © RioPatuca Images/fotolia

Flexible Experimente auf individuellen Netzen

Der GVS [2, 3] stellt den Benutzern aufbauend auf einer physischen Netzinfrastruktur „Virtual Networks“ (GVS-VN) zur Verfügung. Diese GVS-VN können mithilfe eines automatischen Provisionierungssystems in Minutenschnelle vom Benutzer selbst zusammengestellt und aufgebaut werden. Jedes GVS-VN ist dabei von anderen Teilnetzen isoliert, sodass neben **betrieblichorientierten** GVS-VN 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 Dienstes: Er ermöglicht den Aufbau flexibler Datennetze für unterschiedliche Zwecke, in denen dem Nutzer auch ein Anpassen der zugrundeliegenden (virtuellen) Netztopologie erlaubt ist.

Eine weitere Besonderheit von GVS für experimentelle Untersuchungen ist, dass diese automatisch provisionierten GVS-VN spezifische Anteile der physischen Infrastruktur buchen können und der Wissenschaftler so seine Forschung über ein reales Netz betreiben kann 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 1), sind auch Experimente im Wide Area Network Bereich möglich.

Um ein GVS-VN aufzubauen, beschreibt ein Benutzer zunächst, wie sein Teilnetz genau aussehen soll und welche Ressourcen es enthalten soll. Das geschieht mithilfe eines Dokumentes (Domain Specific Language (DSL) Code), das 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 virtuellen Teilnetz-Komponenten zur Verfügung. Der Benutzer kann diese Ressourcen kontrollieren und in seinem GVS-VN damit arbeiten.

Für die Kopplung eines GVS-VN an eine „fremde“ Netzumgebung wurde als weitere Ressource ein „External Domain Interface“ entwickelt. Dadurch kann ein GVS-VN auch jederzeit so konstruiert werden, dass z. B. Laboreinrichtungen von zwei oder mehreren wissenschaftlichen Instituten und Partnern über ein GVS-VN miteinander verschaltet werden: Das GVS-VN fungiert in diesem Fall nicht nur als Verbindungsstruktur zwischen den Laboreinrichtungen, sondern kann auch zusätzliche Ressourcen einbinden. In der Praxis hat sich gezeigt, dass diese Möglichkeit besonders für Demos auf

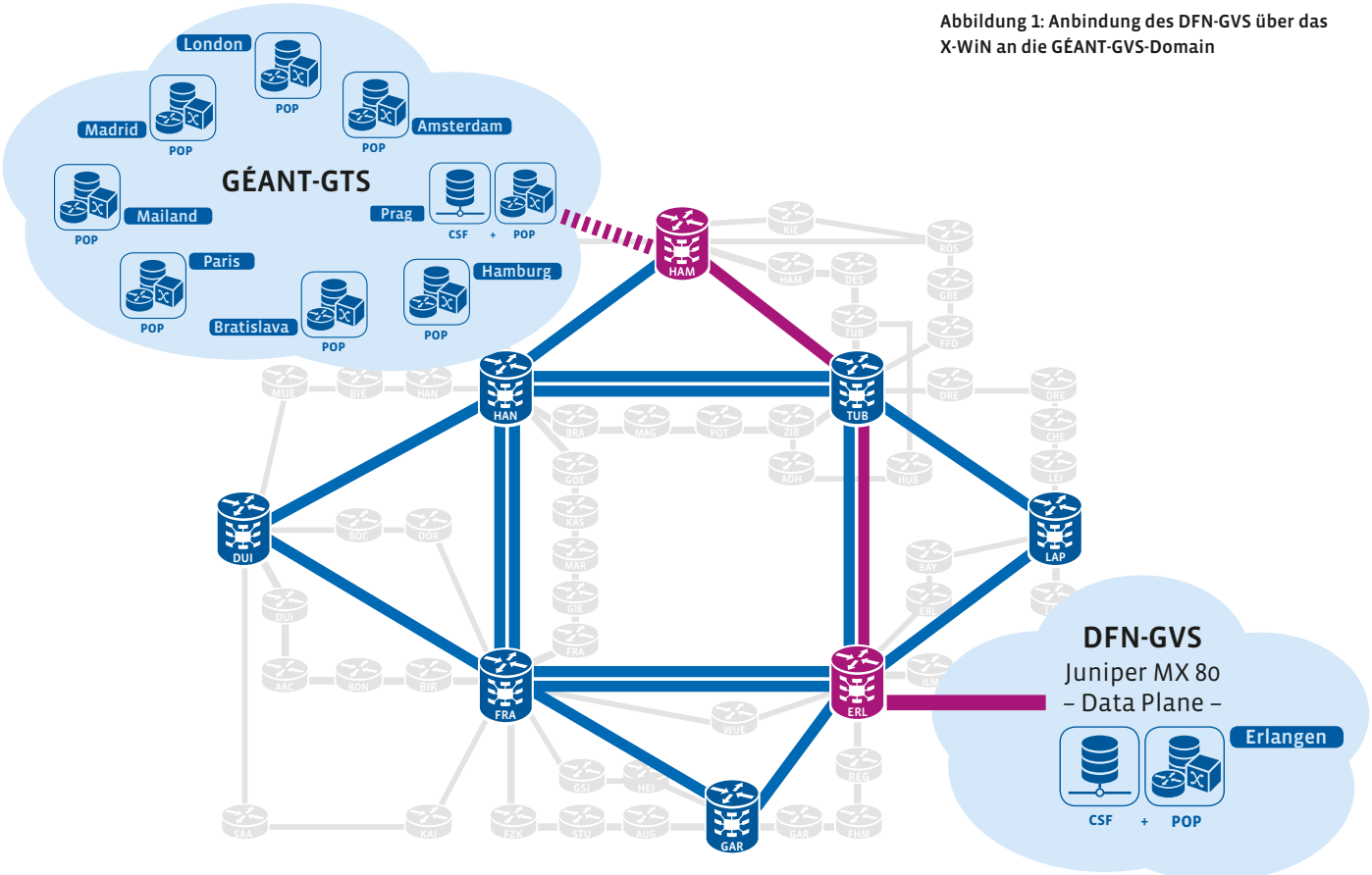


Abbildung 1: Anbindung des DFN-GVS über das X-WiN an die GÉANT-GVS-Domain

Konferenzen und Tagungen interessant ist, weil der Tagungsort somit leicht in bereits bestehende Testumgebungen mit eingeschlossen und angebunden werden kann. Mit dieser Funktionalität dient der GVS als Software Defined Exchange (SDX). Das ist eine software-basierte Vermittlungszentrale, die zusätzliche Netzressourcen zur Verfügung stellen kann.

Neue Möglichkeiten in Version 5.0

GÉANT-GVS wird mittlerweile in der Version 5.0 betrieben. Die Vorgänger-Version 4 führte als Neuerung Bare Metal Server (BMS) ein, die Nutzer als Hardware Ressource nun in ihre Netzumgebung einbauen können (neben den bereits verfügbaren Ressourcen wie Virtual Machines (VMs), Virtual Circuits (VCs) und OpenFlow Switch Instanzen). Die OpenFlow Switch Instanzen wurden in Version 4 ebenfalls erneuert und stehen jetzt komplett virtualisiert auf CORSA DP2100 Hardware zum Abruf bereit. Für Version 4 wurden alle diese Ressourcen komplett neu mit 10 GE Interfaces für die Dataplane direkt in den Backbone von GÉANT integriert.

Die neue Version 5 bietet eine public API sowie einen neuen zweistufigen Registrierungsprozess. Darüber hinaus wurde eine zusätzliche Benutzerrolle eingeführt, mit der es einem „Projektmanager“ nun auch selbst möglich ist, neue User für sein eigenes Projekt anzulegen. Version 6 ist für Sommer 2018 geplant. Ein Highlight soll hier unter anderem der neue DragnDrEd Editor sein, mit dem sich dann auch grafisch neue Netzumgebungen durch einfache Mausklick- und Ziehoperationen zusammenstellen lassen. Der dazugehörige DSL Code zur Beschreibung des Netzes wird dabei automatisch im Hintergrund generiert. In der Entwicklungsplanung für Version 7 sind Checkpoint/Restart Mechanismen (samt zugehöriger Speicherlösung) vorgesehen.

Multi-Domain-Fähigkeit und internationale Kooperation

Die GVS-Architektur ist Multi-Domain fähig. Dafür ist der GÉANT-GVS durch analoge Installationen in mehreren Forschungsnetzen zu einem Multi-Domain-GVS erweitert worden. Die Anbindung der NREN-GVS an den GÉANT-GVS erfolgt mit 10 GE-Verbindungen.

Die Nutzung der Multi-Domain-Struktur ist vergleichsweise einfach, da auch der Ressourcen Manager im GVS Multi-Domain fähig ist. Das bedeutet, dass der Ressourcen Manager einer GVS-Domain auch bei externen GVS-Domains Ressourcen für ein GVS-VN anfragen kann. Für den Benutzer hat dies den Vorteil, dass er sein GVS-VN in einem „One-Stop-Shopping“ (OSS) Verfahren bucht, auch wenn seine Ressourcen möglicherweise im Moment nicht alle komplett in der eigenen GVS-Domain zur Verfügung stehen, sondern ergänzungsweise bei anderen GVS-Providern reserviert bzw. ausgeliehen werden müssen. Für den Benutzer ist dieser Prozess transparent, d. h. er kontaktiert lediglich „seinen“ GVS vor Ort und bekommt dann über diesen Service auch seinen Ressourcenzugang. Dadurch sind auch internationale Netze umsetzbar, je nachdem, wo die GVS-Betreiber ihre Standorte eingerichtet haben. Es gibt GVS-Erweiterungen bei CESNET, HEAnet, NORDUnet, RENAM (im Aufbau), bei Ciena (Canada, über OTN Equipment) und seit Anfang 2018 auch im DFN.

Die DFN-GVS-Domain

Generell besteht die DFN-GVS-Domain ebenso wie das GÉANT-GVS-Pendant aus der GVS-Central-Server-Facility (GVS-CSF) und beliebig vielen Knoten-Standorten, den Points-of-Presence (GVS-PoP). Die GVS-CSF ist für das zentrale Management der GVS-Domain zuständig, die GVS-PoP werden für die Bereitstellung der Ressourcen benötigt. Der Standort des GVS-CFS muss ebenfalls mindestens einen GVS-PoP aufweisen. Die DFN-GVS-Domain, welche zur Zeit aus der CSF und einem PoP besteht, wird aktuell am X-WiN-Kernnetzknoten der Friedrich-Alexander-Universität Erlangen-Nürnberg installiert und mit dem Kernnetzknoten in Hamburg verbunden. Dort befindet sich bereits ein GÉANT-GVS-PoP, welcher sich für ein Multi-Domain-Peering mit dem DFN-GVS eignet.

Die DFN-Installation stellt funktional folgende Eigenschaften zur Verfügung:

- Datentransport-Ressourcen,
- Routing/Switching-Komponenten,
- Compute-Ressourcen (VMs),
- Bare-Metal-Server (BMS),
- Speicherplatz,
- Managementkomponenten für die DFN-GVS-Domain,
- Managementkomponenten für die Projekte/Netzwerke der Nutzer.

Für die Umsetzung der funktionalen Anforderungen umfasst der DFN-GVS-PoP die folgenden Hardwarekomponenten (siehe Abbildung 2):

- drei Dell 530 Server (Compute Nodes, 1 GE- und 10 GE-NICs) für die Bereitstellung von virtuellen Maschinen,
- einen Juniper MX-80 Router (48*1GE, 4*10GE) für Data-Plane Verbindungen,
- zwei Juniper EX-4300 Switche (48*1GE, 4*10GE, 4*40GE) für das Management der Control-Plane,
- einen CORSA-Switch DP2100 (arbeitet u. a. als OpenFlow Switch),
- 18 Bare-Metal-Server,
- Speicherplatz (file systems, virtual disks, usw.).

Die Einrichtung der Benutzerteilnetze (GVS-VN) erfolgt auf der Hardware und den Servern der DFN-GVS-PoPs und nicht auf dem System der DFN-CSF, welche ausschließlich für die Kontrolle und das Management des DFN-GVS-Dienstes zuständig ist und somit auch die PoPs steuert und verwaltet.

Die CSF selbst besteht aus der gleichen Dell-Hardware, welche auch für die Compute Nodes des PoP verwendet wird und erstreckt sich über drei Hardwareserver. Allgemein unterteilt sich die CSF in einen Orchestration-Teil (CSF0), einen Teil für die Internet Access Gateways (IAGW) der Benutzer (CSF1) und einem Teil, der als Storage (CSF2) dient. Vor allem CSF0 gliedert sich jedoch in weitere logische Teile:

- CSF0 (Orchestration):
  - CSF0.0: virtueller Server, welcher GVS Core Services übernimmt,
  - CSF0.1: virtueller Server für den OpenStack Controller,
  - CSF0.2: virtueller Server für OpenNSA ,
  - CSF0.3: virtueller Server für den Betrieb von OpenStack Network (Neutron),
- CSF1 (Gateway Server) für die IAGW für Benutzerzugänge ins DFN-GVS,
- CSF2 (Storage Server) verwaltet Konfigurationen von Benutzerexperimenten, Input- und Output-Daten.

Da die Provisionierung von virtuellen Maschinen im GVS auf OpenStack basiert, müssen mehrere OpenStack Komponenten installiert und konfiguriert werden (siehe Kasten). Alle CSF-SW-Komponenten, die auf den CSF0/1/2 laufen, konnten vom GÉANT-GVS übernommen werden.

Im DFN-GVS wird ein Corsa Switch für OpenFlow Testbeds eingesetzt, um es Benutzern zu ermöglichen, ihre eigenen Flowspecs mit virtuellen Ports für ihre Testbedumgebung festzulegen – unabhängig von der physischen Portbelegung auf dem Switch. Das bedeutet, dass eine Benutzerinstanz mit virtuellen Ports auf dem Switch auf andere physische Ports umgezogen werden kann, (z. B. bei Maintenance) ohne dass der Benutzer seine Flowspecs und seine Topologie ändern muss.

OPENSTACK KOMPONENTEN AUF DER DFN-CSF

Keystone: der OpenStack Authentifizierungs- und Authorisierungsservice regelt die interne Kontenzuordnung zwischen GVS und OpenStack internen Referenzen

Nova: verwaltet die VM in den PoPs

Glance und Cinder: verwalten die Boot Images mit OS der VM und ermöglichen Snapshots von laufenden Instanzen

Neutron: wird in GVS dazu verwendet, einfache Konnektivität zwischen den VM herzustellen

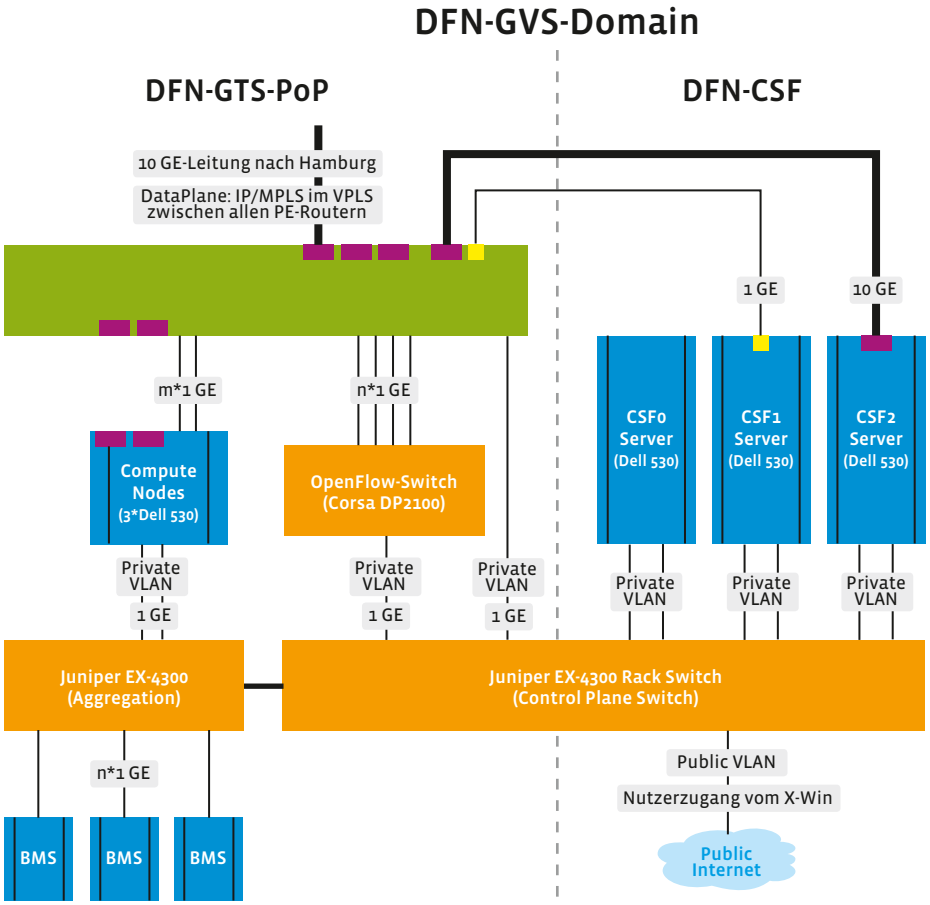


Abbildung 2: Komponenten des DFN-GVS-PoP mit Managementsystem

CSF0 Server:
Management des DFN-GTS
CSF1 Server:
Internet Access Gateway für Benutzerzugänge ins DFN-GTS
CSF2 Server:
Storage Server für Nutzerkonfigurationen

Maßgeschneiderte Netze für eine Vielzahl von Nutzern

Nutzer des DFN-GVS können den Service über eine Webseite auf dem DFN-CSF-Server erreichen und dort ihre Beschreibung für die gewünschte Netztopologie hochladen. Ist die Beschreibung syntaktisch korrekt und können die aufgelisteten Ressourcen reserviert werden, bekommt man den Zugang zu seinen VM im GVS-VN über einen Konsolenlink sobald die VM vom Nutzer aktiviert wurden. Die Nutzer können so die VM einrichten und über ein Internet Access Gateway (IAGW) auch Software von außen in ihr GVS-VN hochladen. Die Einbindung externer Labore oder VPN in das eigene GVS-VN kann über das „External Domain Interface“ erfolgen (Abbildung 2, S. 27).

Durch die flexiblen Netzbausteine, mit denen ein minutenschneller Aufbau eines virtuellen Netzes möglich ist, ist GVS nicht nur für die Forschung interessant. Auch vielfältige betriebliche Anwendungen für Netzbetreiber und Administratoren sind denkbar. So kann z. B. die Skalierbarkeit getestet und das Netzverhalten im WAN-Umfeld verfolgt werden. Darüber hinaus können auch unterschiedliche Linkmerkmale im Hinblick auf Quality of Service (QoS) oder Queuing Mechanismen betrachtet werden. Besonders geeignet sind solche maßgeschneiderten virtuellen Netze auch für Untersuchungen zur Netzsicherheit, DDoS Flooding Attacken, Penetrationstests und VM-basierten Honeynet Deployments. Bereits bekannte Attacken und deren Abwehr können gezielt reproduziert, beobachtet und die Wirkung von Abwehrmechanismen nachverfolgt werden.

Abbildung 3: Bisherige GÉANT-GVS Domains

Als typische Nutzer von GÉANT-GVS haben sich bisher folgende Gruppen erwiesen:

- Wissenschaftler, die eine Netzinfrastruktur für ein Forschungsprojekt benötigen und möglichst schnell mit ihrer eigentlichen Forschungsarbeit über dieses Netz beginnen möchten ohne lange und mühsame Aufbauphase;
- Wissenschaftler, die am GÉANT Projekt selbst beteiligt sind und durch diesen anpassungsfähigen Service die Möglichkeit haben, Innovationen schnell testen und umsetzen zu können;
- Doktoranden und Absolventen, die eine Netzumgebung für eine prototypische Umsetzung einer Entwicklung für ihre Abschlussarbeit benötigen;
- Professoren, die für Seminare den praxisnahen Umgang mit Netzen zeigen möchten (über eine reine Simulation hinaus);
- Netzforscher, die für ihre Untersuchungen eine lange Laufzeit (z. B. für Performanzmessungen) benötigen und auf realitätsnahe Netzbedingungen über echte Hardware angewiesen sind;
- Forschungsprojekte, die z. B. für Demos auf Konferenzen schnell ein Netz benötigen, das über ihre Laborumgebung hinausgeht und zusätzliche Ressourcen zur Verfügung stellt;
- Projektmitarbeiter oder Administratoren, die Sicherheitskonzepte testen möchten (DDoS Mitigation, etc.), die sie im eigenen Produktionsnetz so nicht durchführen können oder dürfen;
- Netzadministratoren, die aus Provider Sicht generell beobachten und prüfen wollen, wie stabil sich virtuelle Netze automatisch provisionieren, zuweisen und gegeneinander isolieren lassen;
- Forschungsprojekte, die Projektteilnehmer mit eigenen Laboren „in Streulagen“ haben und mit GVS als Verbindungsstruktur ihre Partner anbinden möchten.

In der Funktion als Software Defined Exchange (SDX), also als software-basierte automatische Vermittlungszentrale (siehe Abbildung 3), die zusätzliche Netzressourcen zur Verfügung stellen kann, ist GÉANT-GVS hauptsächlich für Netzbetreiber hochinteressant. Die darunterliegende Architektur lässt außerdem die

REFERENZEN

[1] https://www.geant.org/Services/Connectivity_and_network/Pages/GEANT_Testbeds_Service.aspx
[2] 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
[3] Susanne Naegele-Jackson, Jerry Sobieski, Michal Hazlinski, Jakub Gutkowski, Creating Automated Wide-Area Virtual Networks with GTS - Overview and Future Developments, accepted for publication at the 8th IEEE International Conference on Cloud Computing Technology and Science, NetCloud 2016, Luxembourg, Dec 12 - 15, 2016.
[4] Sonja Filiposka, Possibilities for using GTS as a practical tool in higher education courses on networking, GTS workshop, Utrecht, The Netherlands, Feb 28th & March 1st 2017.

individuelle Umsetzung einer GVS Instanz zu, d. h. ein Betreiber kann selbst entscheiden, welche Hardware er anbieten möchte (z. B. nur VM und VC). Aber auch andere spezielle Hardware kann problemlos zum Einsatz kommen. Dafür ist es nur erforderlich, für eine neue Hardware-Ressource ein sogenanntes Remote Control Agent (RCA) Modul zu entwickeln, mit dem der GVS Ressourcen Manager dann die darunterliegende Hardware als einzelne Slice einem Benutzer zur Verfügung stellen kann.

Dadurch haben Benutzer nicht nur mehr Ressourcen zur Verfügung, sondern durch die leicht erweiterbare Architektur ist es auch möglich, dass NRENs sich auf bestimmte neue Ressourcen spezialisieren. Es ist außerdem denkbar, dass NRENs nur ausgewählte Ressourcen anbieten, ihre Nutzer aber durch die Multi-Domainfähigkeit auch Zugang zu anderen nicht lokal vorhandenen Ressourcen bekommen. Ein solches maßgeschneidertes Betriebskonzept ermöglicht es einem Netzbetreiber, ein effizientes und ausgewogenes Angebot an Ressourcen zu bieten, und darüber hinaus ohne großen Aufwand auch einen kurzfristigen sprunghaften Anstieg der Nachfrage bzgl. einer Ressource zu meistern.

Zusammenfassung

In GÉANT ist ein General-Virtualization-Service (GVS) basierend auf dem SDN-Konzept aufgebaut worden, der europäischen Nutzern eine stabile Betriebs- und Experimentierumgebung zur Verfügung stellt. Die GVS-Architektur erlaubt auch die (statische) Einbindung andersartiger Netzinseln, sodass der GÉANT-GVS als Software Defined Exchange (SDX), also als software-basierte Vermittlungszentrale, arbeiten kann. In mehreren NRENs ist eine analoge GVS-Umgebung aufgebaut worden, die zusammen mit dem GÉANT-GVS eine GVS-Multi-Domain-Umgebung bildet.

Der DFN-Verein hat Anfang 2018 eine eigene GVS-Domain implementiert. Interessenten aus der DFN-Community können ab sofort ihre Nutzungsszenarien im DFN-GVS konfigurieren. ◆

Technik, die Musik verbindet

Text: **Nina Bark** (DFN-Verein)

Die weltweiten Forschungsnetze können viel mehr als nur wissenschaftliche Daten übertragen. Ein Beispiel für die interdisziplinäre Arbeit der weltweiten Forschungsnetz-Community ist das Projekt LoLa (Low Latency audio visual streaming system). Vom italienischen Forschungsnetz GARR entwickelt, ermöglicht LoLa Musikern auf der ganzen Welt miteinander zu arbeiten und in Echtzeit gemeinsam Konzerte zu geben, ohne sich physisch auch nur auf demselben Kontinent zu befinden.

Spezialisierte Hardware für LoLa Anwendungen *Foto © Nina Bark, DFN-Verein*

Eine außergewöhnliche Probe

Der australische Bratscher, Dirigent und Komponist Brett Dean besuchte im November 2017 die Geschäftsstelle des DFN-Vereins in seiner ehemaligen Wahlheimat Berlin. Anlass war die Generalprobe zwei seiner Stücke. Im großen Konferenzraum des DFN-Vereins erwarteten Dean neben der neuesten LoLa Technik auch einige Musiker des New World Symphony Orchestra – nicht vor Ort, sondern direkt zugeschaltet aus dem fast 8.000 Kilometer entfernten Miami. Möglich machte dies das Projekt LoLa. Das Audio/Video-Streaming System für musikalische, interaktive Performances und Unterricht erlaubt eine unkomprimierte und dadurch nur minimal verzögerte Übertragung über größere Distanzen. Zusammen mit den Forschungsnetzen GARR (Italien) als Initiator des Projekts sowie GÉANT und Internet2 (USA) konnte der DFN-Verein LoLa ein erstes Mal testen.

Brett Dean siedelte 1984 nach seinem Studium in Brisbane nach Deutschland über, wo er 15 Jahre lang Bratschist bei den Berliner Philharmonikern war. Im Jahr 2.000 kehrte er nach Australien zurück, um sich stärker dem Komponieren zu widmen. Heute erfreuen sich seine Werke großer Aufmerksamkeit, und er gehört zu den international meistaufgeführten Komponisten seiner Generation.

Das Sextett Old Kings in Exile, das die jungen Musiker unter anderem mit Dean probten, handelt von der Demenzerkrankung seines Vaters. Trotz der großen Entfernung gelang es Dean während der Probe, den jungen Musikern seine Gefühle und Erlebnisse hinter den Noten zu vermitteln und ihnen so einen besseren Zugang zu seinem Stück zu verschaffen.

Der Komponist hatte bereits einige Jahre zuvor über LoLa mit der America's Orchestral Academy zusammengearbeitet. Damals war es auch das erste Mal für die Academy. Die 1987 gegründete Orchesterakademie bereitet junge Musikerinnen und Musiker auf eine professionelle Karriere in der klassischen Musik vor. „Der technische Fortschritt ist immens“ betonte Dean. Beim ersten Mal gab es noch viele Unterbrechungen, jetzt kann er alles gut hören, auch wenn manches Instrument ein bisschen lauter oder leiser ist. Sowohl der Kom-

ponist als auch die Musiker freuten sich sehr, die Feinheiten ihres Spiels noch weiter vertiefen zu können.

Was ist LoLa genau?

Das LoLa-Projekt ermöglicht Musikdarbietungen in Echtzeit, bei denen die Musiker durch fortschrittliche Netzwerkdienste verbunden sind, wie sie von den Forschungsnetzen und anderen internationalen Backbones bereitgestellt werden. Die Idee zu dem Projekt kam von Musikern, die an vielen geografisch verteilten Aktivitäten beteiligt sind und damit viel Zeit in Reisen investieren müssen. Ihnen stellt LoLa ein Werkzeug zur Verfügung, damit sie gemeinsam mit Kolleginnen und Kollegen vor einem Konzert Proben durchführen können, auch wenn die Musiker sich nicht am selben Ort befinden. Des Weiteren können sich Musiker z. B. an Master Classes beteiligen, um Studenten auf der ganzen Welt zu unterrichten. Hierbei ist es sogar möglich, gemeinsam mit dem Schüler während des Unterrichts aufzutreten. Aber LoLa bietet auch die Möglichkeit, Konzerte vor Publikum zu geben, mit verteilten Darstellern aber auch mit verteilten Zuschauern. Das Projekt ermöglicht dadurch ein innovatives, bisher unerforschtes Performance-Szenario mit neuen Herausforderungen und Möglichkeiten.

Das Projekt wurde vom Musikkonservatorium Giuseppe Tartini aus Triest (Italien) in Zusammenarbeit mit GARR entwickelt. Es entstand 2005 nach einer Demonstration der ersten interkontinentalen Viola MasterClass zwischen der GARR National User's Conference in Pisa (Italien) und der New World Symphony Music Academy in Miami (USA). Im Jahr 2010 wurde es erstmals öffentlich vorgeführt mit einem Klavierduokonzert zwischen dem Musikkonservatorium Tartini und dem Forschungsinstitut für Akustik/Musik in Paris. Heute wird LoLa in einer Vielzahl von Institutionen auf der ganzen Welt eingesetzt, die alle an ihr nationales Forschungs- und Bildungsnetzwerk angeschlossen sind.

Komponist Brett Dean und Musiker des New World Symphony Orchestra
Foto © Christian Meyer, DFN-Verein

Wie kann das gehen?

LoLa ist ein Audio-Visual-Streaming-System, also ein Werkzeug für eine IP-basierte Echtzeitkommunikation (Voice und Video) mit dem Ziel, eine „natürliche" Distanz zwischen Mensch und Maschine zur Verfügung zu stellen. Es ist für Distanzmusikaufführungen konzipiert, kann aber auch für jedes andere Szenario, bei dem Echtzeit-Interaktion erforderlich ist, verwendet werden.

Besonderes Augenmerk wurde auf die Optimierung der Signalverarbeitung und -übertragung gelegt, um die Systemlatenzzeit so gering wie möglich zu halten und so niedrig wie möglich unterhalb der menschlichen Verzögerungswahrnehmungsschwelle zu bleiben. Sowohl Standard Definition Videos (SD) und High Definition Video (HD) Modi werden ab Version 1.4.x unterstützt. Das System basiert auf einer leistungsfähigen Audio-/Video-Erfassungshardware und auf der Integration und Optimierung der Erfassung, Präsentation und Übertragung von Audio- und Videoströmen. Das LoLa-System erfordert auch eine sehr hohe Leistung der Wide Area und Local Area Networks – eine ein Gigabit pro Sekunde Ende-zu-Ende-Verbindung ist die minimale empfohlene Konfiguration, wenn das System mit unkomprimierten Videosignalen genutzt wird. Bei einer geringeren Bandbreite kann das System mit eingeschalteter Videokompression genutzt werden.

LoLa ist eine Spezialsoftware, die auch eine sehr spezialisierte Hardware erfordert. Die LoLa-Community bietet in ihren zahlreichen Best-Practice-Vorlagen Tipps, welche Produkte verwendet werden können. Seit November 2017 gibt es eine Partnerschaft mit dem Kamerahersteller XIMEA. Die XIMEA USB3 Videokameras haben sich auf dem Feld der IP-basierten Echtzeitkommunikation als die technisch beste, kostengünstigste und zuverlässigste Videohardware erwiesen, die mit LoLa kompatibel ist. Die lizenzierte Software LoLa steht für alle akademischen und nicht-kommerziellen Zwecke kostenlos zur Verfügung. In allen anderen Fällen kann eine Shareware-Lizenz angefordert werden, um das Projekt zu unterstützen. ◆

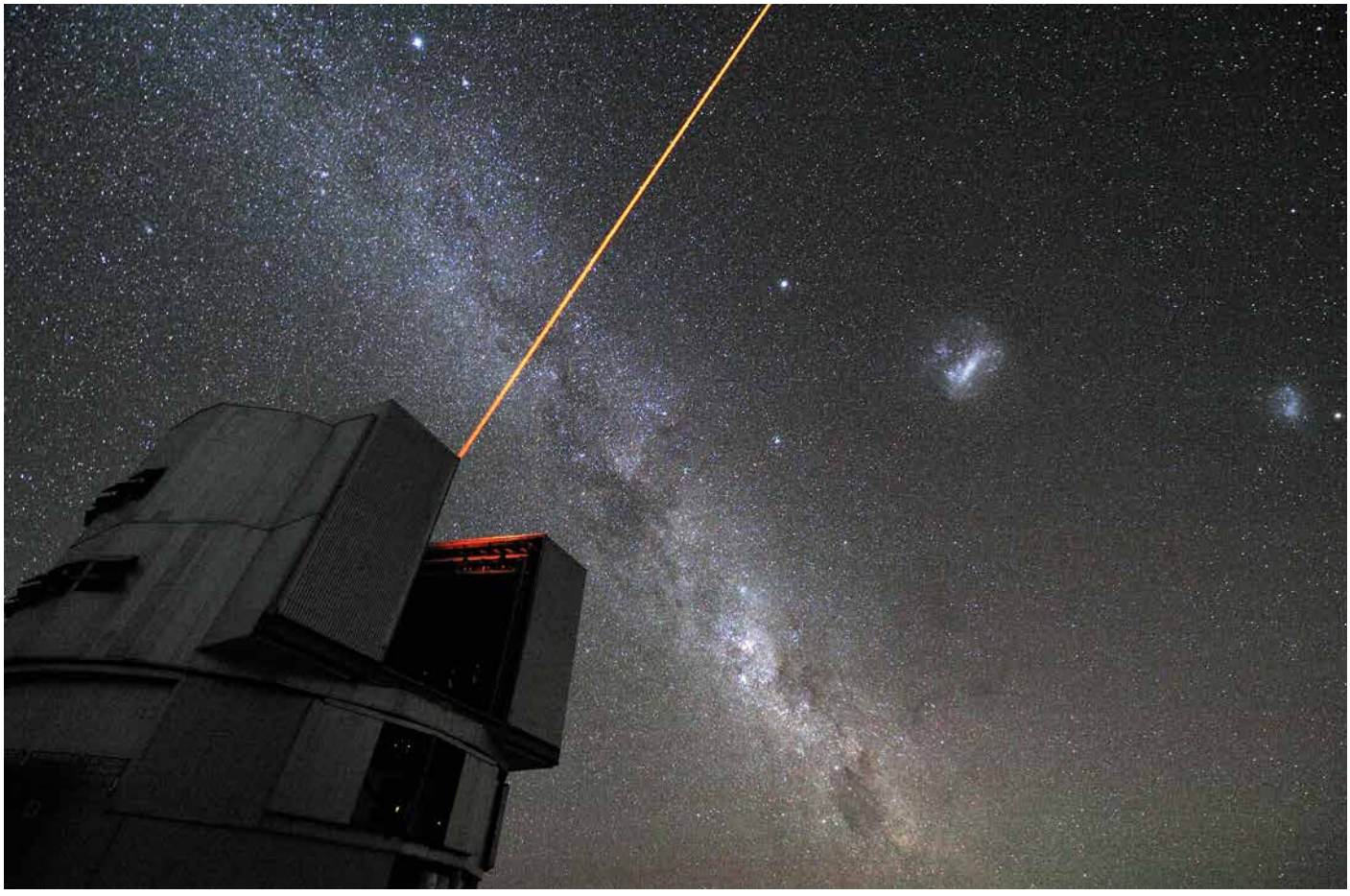
Forschung

Mit vereinten Kräften – das Zeitalter der Multi-Messenger-Astronomie
von Maimona Id

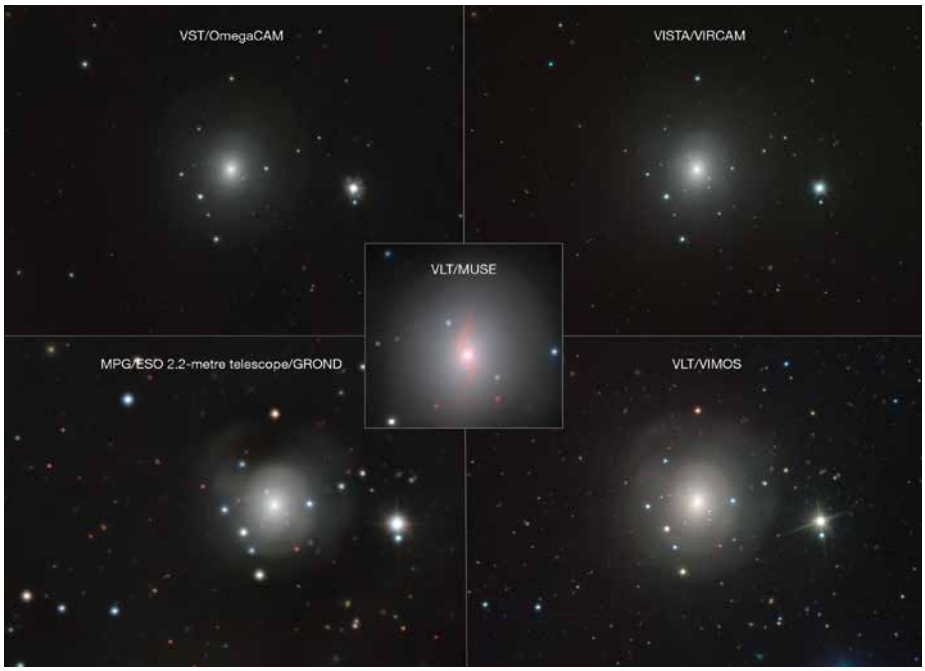
Mit vereinten Kräften – das Zeitalter der Multi-Messenger-Astronomie

Zum ersten Mal gelingt es Wissenschaftlern, die gemeinsame Quelle von Gravitationswellen und elektromagnetischer Strahlung zu identifizieren. In einer der größten „Target of Opportunity“-Kampagnen lüften sie das Geheimnis um die Verschmelzung zweier Neutronensterne. Einen großen Anteil an diesem Erfolg haben auch die nationalen und länderübergreifenden Forschungsnetze, ohne deren engagierte Zusammenarbeit eine solche Entdeckung wohl noch auf sich warten lassen würde.

Text: **Maimona Id** (DFN-Verein)



ESO's Very Large Telescope (VLT) at Paranal Observatory, Chile *Foto © ESO/G. Hüdepohl, atacamaphoto.com*



Multi-Messenger-Astronomie: Verschiedene ESO-Teleskope und Instrumente zeigen die Galaxie NGC 4993. Bei der schwachen Lichtquelle in der Nähe des Zentrums handelt es sich um eine Kilonova, eine Explosion aus der Verschmelzung zweier Neutronensterne. Diese Verschmelzung führte zu Gravitationswellen, die von LIGOVirgo detektiert wurden sowie zu Gammastrahlen, die von Fermi und INTEGRAL im Weltraum aufgezeichnet wurden.

Quelle: VLT/VIMOS. VLT/MUSE, MPG/ESO 2.2-metre telescope/GROND, VISTA/VIRCAM, VST/OmegaCAM

Katastrophe im Weltall: Zwei Neutronensterne umkreisen einander mit hoher Geschwindigkeit. Je näher sie sich kommen, desto schneller werden sie. Die Schwerkraft zwingt die Kolosse – extrem dichte Überreste kollabierter massereicher Sterne – auf einen unausweichlichen Kollisionskurs. So extrem ist die Beschleunigung dieser Himmelskörper, dass sie eine Krümmung der Raumzeit verursachen und Energie in Form von Gravitationswellen emittieren. Etwa 130 Millionen Jahre später am 17. August 2017 erreichen die Gravitationswellen auf ihrer Reise durch das All die Erde und treffen auf die hochempfindlichen bis zu vier Kilometer langen Messinstrumente des Laser Interferometer Gravitational-Wave Observatory (LIGO) in Hanford in den USA. Fast zwei Minuten dauern die Signale an. Dank des Virgo-Interferometers des European Gravitational Observatory (EGO) in Santo Stefano a Macerata in Italien kann der Ursprung des Signals exakter eingegrenzt werden – auf die rund 130 Millionen Lichtjahre von der Erde entfernte Galaxie NGC 4993 im Sternbild Hydra. Fast zeitgleich detektieren zwei Weltraumteleskope, das Fermi Gamma-ray Space Telescope der NASA und das INTErnational Gamma Ray Astrophysics Laboratory (INTEGRAL) der ESA, eine kurze aber energiereiche Gammastrahlenexplosion in derselben Sternenregion. An einen Zufall glauben die Forscher jetzt nicht mehr. Alles deutet darauf hin, dass die beiden Signale aus ein und derselben Quelle stammen – einer gewaltigen Kilonova, verursacht durch die explosive Verschmelzung zweier Neutronensterne.

„Ich wusste sofort, dass hier etwas sehr Ungewöhnliches passiert."

Am selben Tag befindet sich Marina Rejkuba an ihrem Arbeitsplatz am Paranal-Observatorium in der Atacamawüste, im Norden Chiles. Einen Großteil des Jahres arbeitet die Astrophysikerin im Hauptquartier ihres Arbeitgebers, der Europäischen Südsternwarte (ESO), in Garching. Mit seinen erdgebundenen leistungsstarken Teleskopen ist das internationale Observatorium in der Lage, elektromagnetische Strahlung im gesamten Wellenlängenbereich zu messen. Rejkuba erhält an diesem Nachmittag ungewöhnlich viele spontane Observationsanfragen für das VISTA (Visible and Infrared Survey Telescope for Astronomy)-Teleskop, dem größten Durchmusterungsteleskop der Welt im nahen Infrarotbereich. Mit nur einer Observation kann es die dreifache Fläche des Mondes scannen. Es folgen weitere Anträge, denselben Bereich neben der Galaxie NGC 4993 mit allen vier Teleskopen des Very Large Telescope (VLT) – einem der höchstentwickelten optischen Instrumente der Welt – zu scannen, um noch präzisere Informationen zu erhalten. „Die Community der Astrophysiker ist unglaublich gut vernetzt. Ich wusste sofort, dass hier etwas sehr Ungewöhnliches passiert.", erinnert sich die 45-Jährige. Sie ist alarmiert. Jede Sekunde zählt bei der Erforschung eines Ereignisses, auf das die Wissenschaft Schätzungen zufolge 80.000 Jahre warten muss, bis es sich so nah an der Erde wiederholt. Als die Dunkelheit anbricht, richtet die Fachwelt sämtliche zur Verfügung stehenden Teleskope und Detektoren geschlossen auf einen hellen Punkt am Firmament. Sie ist endgültig angekommen im Zeitalter der Multi-Messenger-Astronomie.

Start einer der größten „Target of Opportunity (ToO)“-Kampagnen

Um das Rätsel der Kilonova zu lösen, startet die ESO nun eine ihrer größten „Target of Opportunity (ToO)“-Kampagnen. Gemeint sind damit kurzfristig außer der Reihe angesetzte Observationen. Für diese existiert ein strenges Regelwerk, das es der ESO erlaubt, bei außergewöhnlichen Vorkommnissen von den festgesetzten Terminen abzusehen. Denn jedes Jahr gehen bei der ESO rund 2.000 Anträge auf Beobachtungszeit ein. Ihre Teleskope sind 365 Tage im Jahr im Einsatz, sie sind permanent um den Faktor vier bis sechs überbucht. Ziel der Beobachtungskampagne ist, das spektakuläre Ereignis von Anfang bis Ende zu erforschen. Dafür werden zahlreiche unterschiedliche Teleskope und Messinstrumente der ESO und ihrer Partner simultan eingesetzt, um sämtliche Wellenlängenbereiche der Kilonova von Ultraviolett bis Infrarot sowie Röntgenstrahlung und Radiowellen einzufangen und so einen möglichst vollständigen Datensatz des historischen Ereignisses zu erhalten. „Die Prioritäten für die ToO-Kampagnen werden im Voraus festgelegt, denn schließlich müssen dafür wichtige lang geplante Messungen unterbrochen werden“, erklärt die Leiterin des ESO User Support Departments (USD). Ihr Job ist es, die weltweiten Messanfragen der Forscher zu koordinieren und die simultanen Observationen sowohl vorzubereiten als auch umzusetzen – eine Herkulesaufgabe. Und ein Wettlauf mit der Zeit: „Die Intensität und Helligkeit der elektromagnetischen Signale sowie das Wellenlängenspektrum veränderten sich innerhalb von Stunden rapide. Das hatten wir in unseren theoretischen Modellen zwar vorausgesehen, die Herausforderung bestand aber darin, adhoc Entscheidungen zu treffen, mit welcher Observationsstrategie, welchen Instrumenten und in welcher Wellenlänge wir die umfassendsten und genauesten Messergebnisse erreichen“, erklärt sie. Um diese gewichtigen Entscheidungen treffen zu können, müssen die von den Teleskopen in Chile erzeugten Messdaten so schnell wie möglich im ESO-Hauptsitz ausgewertet und der weltweiten Forschercommunity für weitere Berechnungen und Analysen zur Verfügung gestellt werden.

Das weltweit größte und modernste Wissenschaftsnetz

Letztendlich sind an der Beobachtung der Kilonova weltweit mehr als 70 Observatorien und Teleskope auf der Erde und im All sowie etwa 3.500 Forscher von über 900 Institutionen beteiligt. Ob die Entdeckung des Elementarteilchens Higgs-Boson oder aber die vollständige Sequenzierung des menschlichen Genoms vor rund 17 Jahren – bedeutende Forschungserfolge werden mittlerweile häufig in großen disziplinübergreifenden Kooperationen erreicht. Globale Konsortien von mehreren Tausend Wissenschaftlern sind längst keine Seltenheit mehr. Dabei entstehen gewaltige Mengen an Forschungsdaten. „Mithilfe von automatisierten elektronischen Kommunikations-Tools erhalten wir regelmäßig Alerts und Informationen zu den aktuellen Messungen. Die Systeme dokumentieren wer, was, in welcher Zeit und in welcher Qualität gemessen hat“, erklärt Rejkuba. Darüber hinaus verfügt die ESO über webbasierte Programme, die fast in Echtzeit Reporte für die Forscher sowie den automatischen Datentransfer von Chile nach Deutschland bereitstellen. Möglich machen das die Hochleistungsdatennetze für Forschung und Bildung. Nationale Wissenschaftsnetze wie das Deutsche Forschungsnetz X-WiN sind über das europäische Wissenschaftsnetz GÉANT mit weiteren nationalen Forschungsnetzen (NREN) verbunden. Zusammen bilden sie das weltweit größte und modernste Wissenschaftsnetz mit über 50 Millionen Nutzern in 10.000 Institutionen in ganz Europa. Das Backbone-Netzwerk arbeitet mit Geschwindigkeiten von bis zu 500 Gbit/s und erreicht weltweit über 100 nationale Forschungsnetze. Mussten vor einigen Jahren die Daten noch aufgrund ihrer Größe von Chile aus auf Datenträgern per Luftpost verschickt werden, was einige Tage Verzögerung zur Folge hatte, gelangen sie nun mittels einer Hochgeschwindigkeits-Standleitung des chilenischen Forschungsnetzes REUNA über die Gemeinschaft der lateinamerikanischen Forschungsnetze RedCLARA, das europäische Netz GÉANT sowie die Leitungen des DFN an

Foto © ESO/G. Hüdepohl, atacamaphoto.com, kleines Foto © Marina Rejkuba

Kleines Wunder in der Atacamawüste: Marina Rejkuba, Leiterin des ESO User Support Departments (USD) hat Glück. Wenige Tage zuvor verdecken Schnee und Wolken das Firmament über Paranal. Just am 17. August zieht der Himmel auf und gibt den Blick frei auf die spektakuläre Kilonova.

das Zentralarchiv der ESO in Garching. Damit ist eine sichere und vor allem schnelle Datenübertragung ohne Datenstaus garantiert. Die Vielzahl an Messdaten aus aktuellen Forschungsereignissen wie der Kilonova können so nahezu in Echtzeit an die Kooperationspartner großer Forschungsverbunde übermittelt werden. Und so hängen der Erfolg der Observationskampagne und der wissenschaftliche Durchbruch nicht zuletzt von modernster Datenkommunikation und -infrastruktur ab. Die nationalen Forschungsnetze fungieren jedoch nicht nur als Datenprovider, sondern bieten auch noch eine umfangreiche Kommunikationsinfrastruktur mit verschiedenen Zusatzdiensten an. So betreibt beispielsweise der DFN-Verein eine Authentifizierung- und Autorisierungs-Infrastruktur (DFN-AAI), um Mitarbeiterinnen und Mitarbeitern von Forschungs- und Bildungseinrichtungen einen geschützten Zugang zu sensiblen Daten zu ermöglichen und damit Kooperationen zu vereinfachen. Dafür müssen sie sich einfach bei ihrer Heimateinrichtung authentifizieren. Für die länderübergreifende Zusammenarbeit großer Forschergruppen wurde der Dienst eduGAIN „trust and identity infrastructure“ entwickelt. Er steht neben den europäischen Teilnehmern auch außereuropäischen Teilnehmern zur Verfügung. Wie sehr moderne Forschung mittlerweile vom Zugang und Austausch von Daten abhängig ist, zeigt auch der Zuwachs bei der Nutzung dieser Dienste.

„Eine neue Ära der Zusammenarbeit und Koordination“

Nach ihrer Rückkehr ins Hauptquartier in Garching ist Marina Rejkuba weiterhin in die Wochen und Monate andauernden Follow up-Beobachtungen der Kilonova eingebunden. Sie ist glücklich darüber, dass die ToO-Kampagne so erfolgreich verlaufen ist. „Es war eine unglaublich ereignisreiche Zeit, stressig, weil ich von jetzt auf gleich folgenschwere Entscheidungen zu treffen hatte, und aufregend, weil wir zum ersten Mal die Verschmelzung zweier Neutronensterne erleben durften“, schwärmt die gebürtige Kroatin. „Es war klar, dass wir eine neue Ära beschreiten, in der wir weitere fächerübergreifende Zusammenarbeit und Koordination zwischen Forscherteams auf der ganzen Welt benötigen, um solche historischen Entdeckungen entschlüsseln zu können“, sagt sie. Dieses eine bahnbrechende Ereignis hat auf einen Schlag viele wissenschaftliche Rätsel gelöst, für deren Annahme es bisher nur theoretische Modelle gab: Unter anderem, dass schwere Metalle wie Gold und Platin nicht von dieser Erde sind, sondern im All beim Crash zweier Neutronensterne entstehen. ◆

Löschen nach Konzept

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) verpflichtet ab Ende Mai 2018 mit neuem Nachdruck zum Löschen personenbezogener Daten. Diese Herausforderung rückt für viele Organisationen derzeit in den Fokus ihrer Datenschutz-Projekte. Was aber muss gelöscht werden und wie gestaltet man ein durchgängiges Löschkonzept sinnvoll? Die DIN 66398 macht Vorschläge für ein effizientes Vorgehen.

Text: **Volker Hammer** (Secorvo Security Consulting GmbH)

Was und warum Löschen

Das Löschen personenbezogener Daten wird bereits seit den 1990er Jahren vom Bundesdatenschutzgesetz (BDSG) und auch von der DSGVO gefordert. Die DSGVO ist ab Ende Mai 2018 anzuwenden und löst dann viele nationale Datenschutzvorschriften ab. Sie enthält unter anderem wesentlich höhere Bußgelder, die bis zum Maximum von 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes einer Organisation betragen können. In vielen Organisationen hat die Umsetzung der DSGVO daher die Aufmerksamkeit der Geschäftsführung.

Foto © sebra/fotolia

Personenbezogene Daten sind nach der DSGVO alle Informationen, die sich auf eine identifizierbare natürliche Person (betroffene Person) beziehen. Identifizierbar ist eine Person auch, wenn Daten über beliebige Indirektheitsstufen und beliebige Merkmale zugeordnet werden können. Dabei sind alle Merkmale und Merkmalskombinationen für die Identifizierung zu berücksichtigen, die der verantwortlichen Stelle zugänglich sind, beispielsweise Personalnummern, Kontonummern, E-Mail-Adressen oder auch IP-Adressen oder eindeutige Bewegungsmuster. Für das Kriterium der Identifizierbarkeit sind auch Informationen außerhalb der verantwortlichen Stelle zu berücksichtigen, beispielsweise im Internet, zumindest wenn sie legal zugänglich sind. Nach dieser Definition sind sehr viele Datenbestände in Organisationen personenbezogen und deshalb der Löschung zu unterwerfen. Dazu gehören Daten von Probanden in Projekten, Daten in der Personalverwaltung in Forschungsinstituten, Daten der Berechtigungsverwaltung oder in Log-Protokollen im IT-Betrieb, oder auch Daten der Ansprechpartner von Lieferanten. Zum Löschen gleichwertig ist Anonymisieren, weil die Daten danach nicht mehr unter das Regime des Datenschutzes fallen. Allerdings ist eine echte Anonymisierung gefordert – und diese gelingt oft nur mit erheblichem Aufwand. Es darf nämlich **keine Möglichkeit** mehr bestehen, auf die Person zurückzuschließen. Löschen ist meist die viel einfachere Alternative.

Das Datenschutzrecht fordert, dass personenbezogene Daten nur verarbeitet werden, solange die Organisation, die sie verarbeitet (Verantwortlicher), einen rechtmäßigen Zweck nachweisen kann. Die Zulässigkeitsgrundlagen legt Art. 6 DSGVO fest. Dazu gehören insbesondere gesetz-

liche Vorschriften für die Verarbeitung von Daten, Pflichten für die Abwicklung eines Vertrages oder Einwilligungen. Sind die Zwecke erledigt, müssen die Daten gelöscht werden (Art. 5: Datenminimierung und Speicherbegrenzung). Dies begründet die Pflicht zur Regellöschung.

Daneben besteht nach Art. 17 DSGVO die Möglichkeit, dass die betroffene Person eine frühere Löschung im Einzelfall beantragt. Dem Antrag muss stattgegeben werden, wenn bestimmte Bedingungen erfüllt sind. Außerdem kann die betroffene Person per Antrag auch verlangen, dass die Löschung im Einzelfall ausgesetzt wird. Auch dafür müssen bestimmte Bedingungen erfüllt sein.

Neben diesen Vorschriften, die für das technische Löschen relevant sind, definieren weitere Artikel der DSGVO verschiedene Dokumentations-, Informations- oder Meldepflichten.

Ausgangssituation in der Praxis

In der Praxis gibt es große Umsetzungsdefizite beim Löschen. Das hat zwei Ursachen: Die Löschregeln sind nicht definiert und es fehlen Löschmechanismen in Anwendungen. Insgesamt zeigt sich schnell, dass das Löschen personenbezogener Daten keine einmalige Aktion sein kann, sondern ein systematisches Vorgehen erfordert. Sinnvoll ist ein Löschkonzept, das die Aufgabe gut strukturiert und dauerhaft gepflegt werden kann. Wie aber kann ein solches Löschkonzept aufgebaut sein und erstellt werden? Eine bewährte Vorgehensweise wäre für die Projektplanung sehr hilfreich.

Seit April 2016 liegt mit der DIN 66398 eine „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ vor. Auch eine englische Sprachfassung steht zur Verfügung. Die Norm geht auf ein Industrieprojekt zum Löschen personenbezogener Daten zurück und stellt einen praxistauglichen, effizienten und systematischen Weg vor, wie Löschkonzepte in Organisationen etabliert werden können. Derzeit greifen Organisationen diese Vorgehensweise auf, um mit Blick auf die DSGVO ihre Löschkonzepte aufzusetzen.

Inhalte der Norm

Die Norm bietet umfangreiche Hilfestellungen, um ein Löschkonzept zu erstellen und in Organisationen zu etablieren, insbesondere:

- bietet sie bewährte Begriffe für Löschprojekte,
- beschreibt sie Vorgehensweisen, durch die Löschregeln festgelegt werden,
- gibt sie Vorschläge für die Umsetzung der Löschregeln,
- empfiehlt sie eine Struktur für die Dokumente des Löschkonzepts,
- gibt sie Empfehlungen, wie das Löschkonzept etabliert und fortgeschrieben werden kann.

Die Norm schlägt eine **Struktur für die Dokumente** des Löschkonzepts in drei Ebenen vor (Abb. 1). Im Dokument zur Vorgehensweise beschreibt die jeweilige Organisation unter anderem, welche Datenbestände sie mit ihrem Löschkonzept abdeckt und welche Vorgehensweise sie anwendet. Außerdem werden die Verantwortlichen für die einzelnen Dokumente und Prozesse festgelegt. Den Kern des Löschkonzepts bildet der Katalog der Löschregeln. Schließlich muss beschrieben werden, wie die Löschregeln in der Praxis anzuwenden sind. Dazu dienen die sogenannten Umsetzungsvorgaben, die diese Festlegungen jeweils für einen Bereich treffen. Die Norm empfiehlt, mit Ausnahme des Regelkatalogs, die Dokumentation zum Löschkonzept in vorhandene Dokumente zu integrieren, soweit dies sinnvoll erscheint.

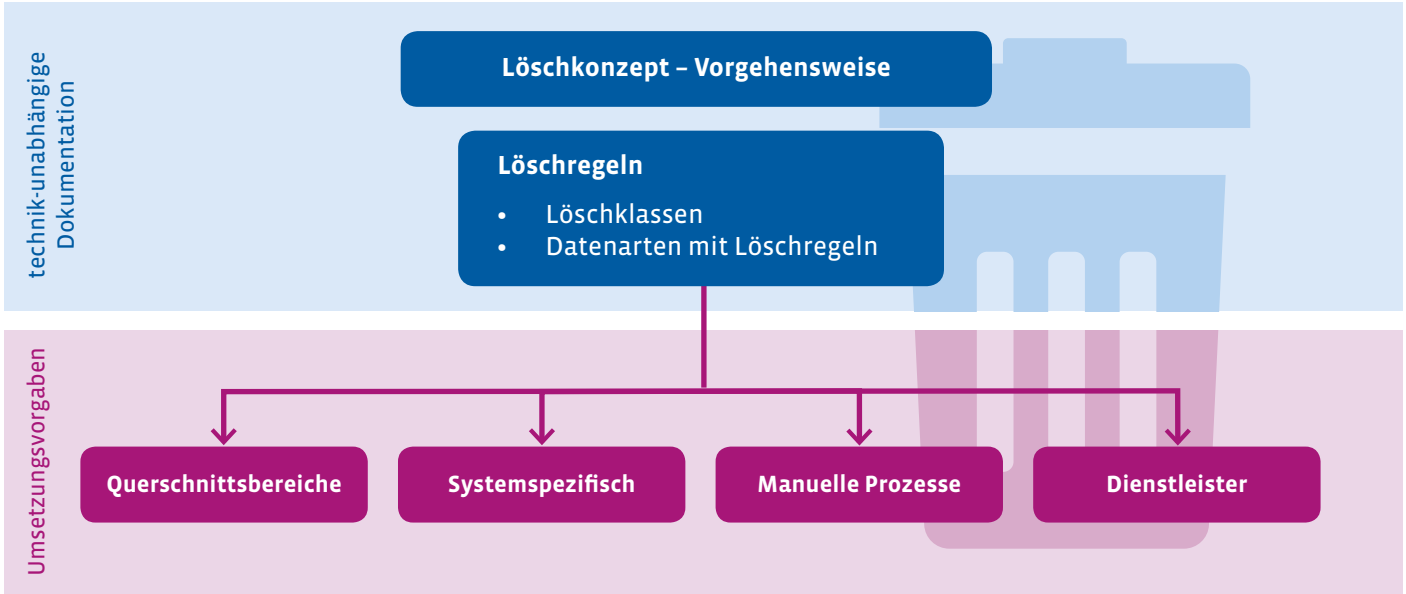


Abbildung 1: Dokumentationsstruktur eines Löschkonzepts in Anlehnung an DIN 66398

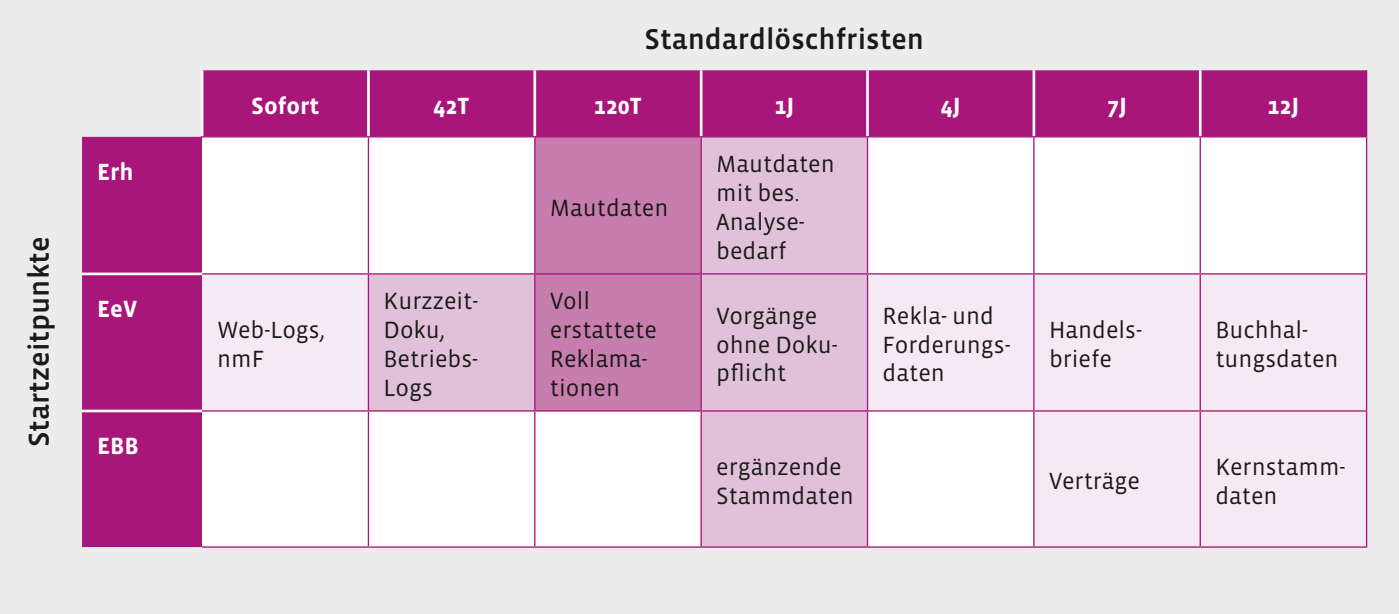


Abbildung 2: Matrix der Löschklasse der Toll Collect GmbH in Anlehnung an DIN 66398 (Legende im Text)

Die Löschregeln

Die größte Hürde für die Löschung personenbezogener Daten ist das Fehlen von Löschregeln. Ohne Löschregeln können keine Mechanismen implementiert werden. Der Kern der Norm ist deshalb eine Vorgehensweise, um Löschregeln zu definieren. Der Datenbestand der verantwortlichen Stelle wird dazu nach datenschutzrechtlichen Zwecken in sogenannte Datenarten unterteilt. Für jede Datenart wird genau eine Löschregel definiert. Sie besteht aus einem Startzeitpunkt und einer Regellöschfrist.

Um die Komplexität der Regelbildung und der Implementierung zu reduzieren, schlägt die DIN 66398 vor, Standardlöschfristen zu verwenden, um Löschfristen, die vergleichsweise nahe beieinanderliegen, in einer Frist zusammenzufassen. In Abbildung 2 werden sieben Fristen nach Tagen (T) und Jahren (J) unterschieden. Solche Standardfristen ergeben sich insbesondere aus Gesetzen, die übergreifend für alle Verantwortlichen gelten (in Abb. 2 hell), spezifische Rechtsvorschriften für den Anwendungsbereich (dunkel) und die frei gewählten Fristen (mittel). Es zeigt sich außerdem, dass sich die Startzeitpunkte nach drei wesentlichen Typen einteilen lassen: der Erhebung (Erh), einem Ereignis in einem Vorgang (EeV) oder dem Ende der Beziehung zum Betroffenen (EBB). Diese Typen von Startzeitpunkten abstrahieren von konkreten Ereignissen und werden in der Norm verwendet, um mit den Standardlöschfristen die sogenannten Löschklassen zu bilden (Abbildung 2). Diese Matrix ist ein ausgezeichnetes Hilfsmittel, um Löschregeln für Datenarten zu identifizieren und einen Überblick über die Datenarten und ihre Einordnung zu behalten. Die Datenarten müssen allerdings so eingeordnet werden, dass die Löschung der Datenobjekte datenschutzrechtlich nicht unangemessen lange verzögert wird.

Im Katalog werden Datenarten und Löschregeln technikunabhängig formuliert, also unabhängig von der Art ihrer Repräsentation oder von Speicherorten und Verarbeitungsprozessen. Für die Löschregel zur Datenart „Rechnung“ ist es deshalb unerheblich, ob sie in einer Datenbank, als PDF oder in einem Aktenordner vorliegt. Als Begründung für die Regeln sind im Katalog die datenschutzrechtlichen Zwecke aufzuführen.

Umsetzung

Die Übertragung und technische Umsetzung für konkrete Systeme und andere Bereiche wird für den Regelbetrieb über sogenannte **Umsetzungsvorgaben** gesteuert. Eine Umsetzungsvorgabe legt dann für die Datenarten des jeweiligen Bereichs fest, wie die Löschregeln angewandt werden. Dadurch wird beispielsweise in Systemlöschkonzepten für das System geregelt, welche Mechanismen mit welchen Konfigurationsparametern die Löschung ausführen, von wem sie gesteuert werden und welche Nachweise für Löschläufe erzeugt werden müssen.

Neben dem Löschen im Regelbetrieb muss ein Löschkonzept in der Praxis aber auch Sondersituationen abdecken. Die Norm gibt auch dafür Hinweise.

Um Backups und Wiederherstellung abzudecken, muss klar unterschieden werden zwischen Produktion und Archiven einerseits, in denen die Regellöschfristen zur Anwendung kommen, und Backups andererseits, die löschfällige Daten datenschutzrechtlich angemessen kurz über die Regellöschfrist hinaus vorhalten dürfen und dann überschrieben werden müssen.

Die Umsetzungsvorgaben müssen festlegen, wie die löschfälligen Daten nach einer Wiederherstellung behandelt werden. Andere Sonderfälle behandeln beispielsweise Beweismittel für einen Rechtsstreit, Störungen in einem IT-Prozess oder Fehler in Datenbeständen. Dazu können beispielsweise Kennzeichen zum Aussetzen der Löschung für einzelne Datenobjekte verwendet werden oder Löschmechanismen insgesamt befristet gestoppt werden.

Etablieren eines Löschkonzepts

Die Norm fasst Erfahrungen aus sieben Jahren Projektarbeit zusammen. Sie bietet ein praxistaugliches und systematisches Vorgehen für Löschkonzepte. Die DIN 66398 macht auch einen Vorschlag zur Organisation eines Löschprojekts, mit dem ein solches Konzept in der Organisation etabliert werden kann. Die klare Struktur der Dokumentation legt ein entsprechendes Vorgehen im Projekt nahe: Zunächst wird ein Katalog der Löschregeln erstellt. Danach werden die Umsetzungsvorgaben definiert und implementiert. Bereits zu Beginn eines Projekts „Löschkonzept“ besteht damit eine klare Strategie und es stehen einheitliche Begriffe zur Verfügung. Fehlschläge und lange Lernkurven können vermieden werden.

Im Rahmen des Projekts muss aber auch erreicht werden, dass Löschen nicht nur als eine einmalige Projektaufgabe, sondern als kontinuierlicher Prozess verstanden wird. Das Löschen von nicht mehr aufbewahrungspflichtigen oder obsoleten Daten soll als eine „übliche Anforderung“ an IT-Systeme verstanden werden. Die Aufgabe muss daher Bestandteil von Beschaffungs- und Entwicklungsprojekten sein und in Projektprozesse integriert werden.

Die DIN 66398 fordert, dass ein einmal erstelltes Löschkonzept gemäß der Entwicklung von Recht, Fachprozessen und IT-Systemen fortgeschrieben wird. Die Norm benennt deshalb Aufgaben, für die die Verantwortlichkeiten festgelegt werden müssen. Dazu gehören die Pflege des Katalogs der Löschregeln und die Entwicklung und Fortschreibung von Umsetzungsvorgaben. In der Norm werden außerdem Informationspflichten und Freigabebeteiligungen empfohlen, damit die datenschutzrechtliche Zulässigkeit von Löschregeln durch den Datenschutzbeauftragten geprüft werden kann, z. B. bei Dokumentänderungen, einigen Aktivitäten des Changemanagements oder bei Systembeschaffungen.

Vielfältiger Nutzen

Motiviert werden Löschkonzepte derzeit über die Datenschutz-Anforderungen der DSGVO. Es ist naheliegend, dass daher auch der Nutzen für den Datenschutz zunächst in den Fokus rückt. Bereits die Gewinne für den Datenschutz sind überraschend breit: Zunächst können die Vorgaben zum generellen Löschen und zum Löschen im Einzelfall erfüllt werden. Die Maßnahmen können auch gegenüber der Aufsichtsbehörde nachgewiesen werden. Für die Datenschützer der Organisation wird aber auch die Informationsbasis für andere Aufgaben wesentlich verbessert. Durch den Katalog der Löschregeln und die Umsetzungsvorgaben werden Datenbestände, Verantwortliche und Fachprozesse umfassend dokumentiert. Eine solche Dokumentation ist gleichzeitig die Voraussetzung, um die Rechtsansprüche der betroffenen Personen auf Auskunft, Sperrung oder Löschung überhaupt erfüllen zu können. Für die Dokumentation der Löschregeln sind die Zulässigkeitsgrundlagen zu erheben. Damit werden gleichzeitig die datenschutzrechtlichen Grundlagen aller Fachprozesse geprüft. Und schließlich kann durch das Löschprojekt und die Integration der Löschanforderungen in Projektprozesse die Einbettung des Datenschutzes in die Organisation deutlich verbessert werden.

Neben den positiven Effekten für den Datenschutz tritt vielfach weiterer Nutzen für die Organisation ein: Mit dem Blick auf das Löschen von Daten können Geschäftsprozesse manchmal präzisiert und optimiert werden. Es werden klarere Vorgaben für die Datenhaltung getroffen und überflüssige Bestände abgebaut. Durch eine bessere Übersicht über (zu schützende) Datenbestände können überflüssige Angriffsziele reduziert und Maßnahmen der Informationssicherheit besser gesteuert werden.

Im Zuge der Umsetzung von Löschregeln bietet es sich in manchen Fällen an, Systeme und IT-Prozesse zu entkoppeln, zu konsolidieren oder rückzubauen. Für den IT-Betrieb können sich dadurch Performance-Gewinne und eine verbesserte Stabilität ergeben. Bereinigte Datenbestände reduzieren auch die Kosten künftiger System-Migrationen. Ein Löschkonzept mit seinen Dokumenten nach DIN 66398 ist schließlich auch in Mitbestimmungsverfahren hilfreich. ◆

WEITERFÜHRENDE MATERIALIEN

- DIN 66398:2016-05: Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth-Verlag, 2016.
- Hammer, V. (2016): DIN 66398 - Die Leitlinie Löschkonzept als Norm, DuD 8/2016, 528 ff.; Download unter www.secorvo.de › Publikationen › Fachaufsätze › 2016.
- Hammer, V., Schuler, K. (2012): Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, 2012, Download unter: www.secorvo.de › Publikationen › Fachartikel › 2012.
Dieses Dokument ist eine Vorversion zur Norm.

Eine Übersicht zu den Inhalten der DIN 66398 und weiterführende Informationen gibt auch die Webseite DIN-66398.de.

Sicherheit aktuell

Text: **Wolfgang Pempe, Ralf Gröper** (DFN-Verein)

Unter dem Schlagwort „Trusted Identity“ rücken die entsprechenden DFN-Dienste enger zusammen: DFN-AAI, eduroam und DFN-PKI werden enger miteinander verzahnt, um sich optimal zu ergänzen. So können die steigenden Anforderungen an eine vertrauenswürdige und manipulationssichere Authentifizierung und Autorisierung im DFN und bei seinen teilnehmenden Einrichtungen besser berücksichtigt werden. Neben den bekannten Kurzbeiträgen aus den Diensten DFN-CERT und DFN-PKI werden hier zukünftig auch Beiträge zu den Themen eduroam und DFN-AAI veröffentlicht.

Foto © wonry/iStock

Incident Response in der DFN-AAI

Über die letzten Jahre hat die Bedeutung der AAI stark zugenommen, was einerseits mit der fortschreitenden Föderierung von Online-Diensten, der starken internationalen Vernetzung im Bereich E-Research und andererseits mit der flächendeckenden Implementierung von Identity Providern an den Heimateinrichtungen zusammenhängt. So ist die DFN-AAI mittlerweile die – je nach Zählweise – dritt- oder viertgrößte Identity Federation weltweit. Mit der Anzahl der verfügbaren Dienste (Service Provider) und teilnehmenden Einrichtungen hat sich auch die Angriffsfläche für Attacken aller Art vergrößert. Auf Seiten der Identity Provider ist dies typischerweise Identitätsdiebstahl und der damit verbundene illegale Zugriff auf geschützte Daten beim Service Provider, z. B. Genomdatenbanken. Bei Service Providern besteht die Gefahr, dass im Falle eines Angriffs unberechtigte Dritte Zugriff auf personenbezogene oder sonstige Nutzerdaten erlangen. In beiden Fällen ist es wichtig, die jeweilige(n) Gegenstelle(n) rechtzeitig zu informieren.

Derzeit arbeiten DFN-AAI und DFN-CERT gemeinsam daran, die bei Sicherheitsvorfällen mit AAI-Bezug zu befolgenden Prozeduren und die hierfür erforderlichen Kommunikationskanäle zu spezifizieren und zu dokumentieren. In diesem Kontext kommen u. a. auch die Empfehlungen des Security Incident Response Trust Framework for Federated Identity (Sirtfi) zum Tragen. Aktuelle Informationen zu diesem Thema werden unter https://doku.tid.dfn.de/de:aai:incidentresponse bereitgestellt. ◆

Umstellung der Verfahren zur Freischaltung von Domains

Anfang Februar hat das für Web-PKIs zuständige Standardisierungsgremium „CA/Browser Forum“ festgelegt, dass die Verfahren zur Prüfung von berechtigten Domains in Serverzertifikaten umgestellt werden müssen. Dies betrifft auch die DFN-PKI. Im Gegensatz zum bisherigen ausschließlich WhoIs-basierten Verfahren wird zukünftig ein Challenge-Response-Verfahren per E-Mail an eine konstruierte E-Mail-Adresse mit der beantragten Domain oder an den Zonenverwalter verschickt. Die E-Mail-Adresse des Zonenverwalters ist im SOA Resource Record zu der zu validierenden Domain im DNS hinterlegt. Welches der beiden Verfahren genutzt werden soll, kann der Teilnehmerservice der DFN-PKI in den Einrichtungen pro Domain entscheiden. Durch diese Maßnahme stellt der DFN sicher, dass auch weiterhin standardkonforme Serverzertifikate in der DFN-PKI ausgestellt werden können. Weitere Informationen finden Sie unter https://blog.pki.dfn.de/2018/03/ausblick-umstellung-der-verfahren-zur-freischaltung-von-domains/ ◆

Certificate Transparency in der DFN-PKI

Als Konsequenz aus Problemen mit den Zertifizierungsprozessen bei einigen CAs, die in den letzten Jahren offenbar wurden, haben Forscher u. a. von Google ein System namens Certificate Transparency (CT) entwickelt. Hierbei handelt es sich um einen Mechanismus, mit dem ausgestellte Serverzertifikate von einer oder mehreren Sammelpunkten öffentlich einsehbar gehalten werden. Ziel ist die Erhöhung der Transparenz der Browser-PKI durch die komplette Überprüfbarkeit der CAs durch die Öffentlichkeit. Über kryptografische Beweise (Consistency Proofs über Merkle Hash Trees) ist sichergestellt, dass unbemerkte nachträgliche Manipulationen des CT-Logs unmöglich sind. Google hat angekündigt, dass sein Browser Chrome ab Frühjahr 2018 erzwingen wird, dass neu ausgestellte Serverzertifikate der öffentlichen Browser-PKI in CT-Logs veröffentlicht werden. Neben der rein technischen Anbindung, die von der DFN-PKI in den letzten Monaten umgesetzt worden ist, ergibt sich eine Änderung für Antragssteller: Wird ein Serverzertifikat in der DFN-PKI im Sicherheitsniveau Global beantragt, so muss der Antragssteller der Veröffentlichung zustimmen. Ohne diese Zustimmung wird kein Serverzertifikat mehr erstellt. So stellen wir sicher, dass die gewohnte Nutzererfahrung mit Servern mit Zertifikaten aus der DFN-PKI erhalten bleibt und für Endnutzer kaum korrekt zu interpretierende Warnmeldungen im Browser verhindert werden. Weitere Informationen finden Sie unter https://blog.pki.dfn.de/2018/01/certificate-transparency-in-der-dfn-pki/ ◆

DFN-Dienst DoS-Basisschutz

Der DFN-Dienst zum Schutz von Einrichtungen vor Denial-of-Service-Angriffen, DFN DoS-Basisschutz, wird seit einem Jahr angeboten. Dieser kann aufgrund rechtlicher Rahmenbedingungen nur in Anspruch genommen werden, wenn vorab eine entsprechende Dienstvereinbarung durch den Teilnehmer und den DFN unterzeichnet wurde. Hierfür fällt kein zusätzliches Entgelt an. Für 15 % der DFNInternet-Dienste ist dies bisher erfolgt und im Falle eines Angriffes kann das Network Operations Center des DFN in Absprache mit dem betroffenen Teilnehmer Gegenmaßnahmen einleiten. Umgekehrt können aber 85 % der DFNInternet-Dienste im Falle eines Angriffes derzeit vom DFN nicht unmittelbar geschützt werden. Es ist daher wichtig, dass möglichst alle Teilnehmer am DFN die Dienstvereinbarung unterzeichnen. Informationen zum DoS-Basisschutz und zur Dienstvereinbarung erhalten Sie unter dos-schutz@dfn.de/ ◆

KONTAKT

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

Anwenderfreundlich und kompakt – Security Incident und Event Management light

Ein prozessorientiertes Informationssicherheitsmanagement (ISMS) zum Schutz von Informationswerten ist für Unternehmen heute unverzichtbar. Wegen umfangreicher möglicher Richtlinien ist die Umsetzung oft zeit- und ressourcenintensiv – insbesondere für kleinere und mittlere Unternehmen (KMU). Darum bietet sich für den ISMS-Teilprozess Security Incident und Event Management (SIEM) ein leichtgewichtiges Modell an. Ziel ist, die Prozessbausteine auf das Notwendigste zu reduzieren. Der Vorteil: neben der kompakten Darstellung ist der Prozess einfach anzuwenden. Er bleibt trotzdem kompatibel mit etablierten Rahmenwerken und erfüllt weiterhin komplexe Sicherheitsanforderungen. Die Preisträger des X-WINner-Awards 2017 über ihr Konzept eines leichtgewichtigen SIEM-Prozesses.

Text: **Jule Anna Ziegler, Bastian Kemmler, Michael Brenner, Thomas Schaaf**
(Leibniz-Rechenzentrum (LRZ), Ludwig-Maximilians-Universität München (LMU))

Ob Malware, Trojaner oder Computerwürmer – der Schaden, den gezielte IT-Sicherheitsvorfälle beispielsweise in öffentlichen Einrichtungen wie Krankenhäusern anrichten können, ist erschreckend. Dementsprechend nehmen die gesetzlichen Anforderungen und rechtlichen Rahmenbedingungen zur Informationssicherheit rapide zu. So verlangt das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz von Betreibern sogenannter kritischer Infrastrukturen, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer in-

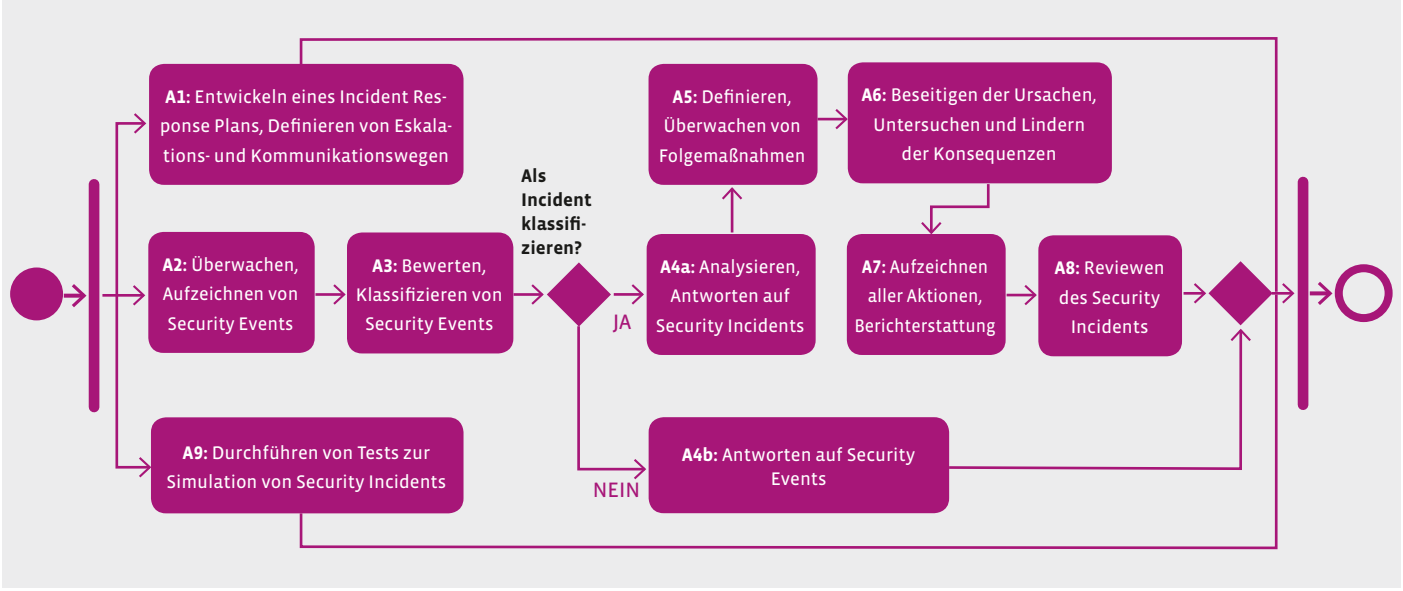


Abbildung 1: allgemeiner SIEM-Prozess

formationstechnischen Systeme, Komponenten oder Prozesse zu treffen“ [Bu15].

Am Thema Informationssicherheit kommt mittlerweile kein Unternehmen mehr vorbei. Das betrifft auch kleinere und mittlere Unternehmen (KMU) sowie IT-Organisationen im Hochschulumfeld. Der Aufwand, ein Informationssicherheitsmanagementsystem (ISMS) zu etablieren – sei es eigenständig, oder als Teil eines bereits bestehenden prozessorientierten Service-Managementsystems (SMS) – ist wegen der unterschiedlichen Rahmenwerke wie ISO/IEC 27000 oder IT-Grundschutz gerade für kleine Nutzer und ihre Ressourcen erheblich. Dazu kommen weitere erschwerende Faktoren: Viele Beschäftigte nehmen die Einführung eines Managementsystems als Verlust von Entscheidungsfreiheit und Flexibilität wahr.

Dementsprechend können die Reaktionen auf die Umsetzung negativ ausfallen. Je tiefgreifender die Veränderung ist und je schlechter sie vermittelt wird, desto größer sind die zu erwartenden Widerstände. Darum ist eine für die Beschäftigten einfache Anwendbarkeit und Verständlichkeit des ISMS-Teilprozesses Security Incident und Event Management (SIEM) ein entscheidender Erfolgsfaktor für eine erfolgreiche und nachhaltige Einführung.

Der allgemeine SIEM-Prozess: Von den Anforderungen zu den Aktivitäten und Outputs

Aus allgemeinen Rahmenwerken abgeleitete Anforderungen dienen als Grundlage für die Entwicklung des späteren leichtgewichtigen SIEM-Prozesses. Nach der Strukturierung und Harmonisierung bedeutungsgleicher Begriffe ergeben sich die für den allgemeinen SIEM-Prozess (vgl. Abbildung 1) notwendigen Prozessbausteine: die Aktivitäten (Inputs) und Outputs (Tabelle 1). Damit können die einzelnen Arbeitsschritte und ihre Ergebnisse später miteinander verglichen und die Vorgehensweise auf beliebige Prozesse oder Themengebiete angewendet werden. Abbildung 1 veranschaulicht mit einem UML (Unified Modeling Language)-Aktivitätsdiagramm des allgemeinen SIEM-Prozesses die Aktivitäten innerhalb des Prozesses.

RELEVANTE RAHMENWERKE FÜR DAS INFORMATIONSSICHERHEITSMANAGEMENT

Die folgenden kurz vorgestellten Rahmenwerke beinhalten grundlegende Anforderungen für einen allgemeinen SIEM-Prozess. Wesentlich für alle Rahmenwerke ist das Prinzip des Deming-Zyklus [De86], auch PDCA -Zyklus (Plan-Do-Check-Act) genannt, der die kontinuierliche Verbesserung der Abläufe und Prozesse eines Managementsystems zum Ziel hat.

ISO/IEC 27000 [IS13b]: Die Standardfamilie zum Informationssicherheitsmanagement bietet die Möglichkeit zur Zertifizierung. Innerhalb dieser Standardfamilie beschreibt die ISO/IEC 27001 [IS13b] die Anforderungen an ein ISMS sowie die Maßnahmen, die für die Etablierung eines SIEM relevant sind.

Information Security Management Toolkit [UC 1] der Universities and Colleges Information Systems Association (UCISA): Das Toolkit behandelt ebenso das Thema SIEM und setzt auf der ISO/IEC 27001 [IS13b] und 27002 [IS13a] auf.

IT-Grundschutz [Bu16]: Das durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschriebene Rahmenwerk zum Informationssicherheitsmanagement ist ebenfalls kompatibel mit der ISO/IEC 27000 und besteht aus einem vierteiligen Standard sowie modular aufgebauten IT-Grundschutz-Katalogen mit bereits identifizierten Bausteinen, Maßnahmen sowie Gefährdungen.

Die IT Infrastructure Library (ITIL) [Ax11]: Die Büchersammlung mit „Good Practices“ für ein Servicemanagementsystem (SMS) gilt momentan als der De-facto-Standard im IT-Service Management (ITSM) [Br11]. Der Fokus von ITIL liegt auf 25 Prozessen, die einem Service Lifecycle zugeordnet sind. Dazu zählt auch das Informationssicherheitsmanagement.

FitSM [Fi16]: Eine Standardfamilie für ein leichtgewichtiges SMS ist durch FitSM beschrieben, die aus sieben Teilen besteht und ebenfalls Ziele sowie Aktivitäten, unter anderem zum Informationssicherheitsmanagement, festlegt.

COBIT 5 [IS12b]: Die mehrteilige Dokumentenfamilie rückt die Governance und das Management der Unternehmens-IT in den Vordergrund. Die Anforderungen zum SIEM sind im Handbuch COBIT 5: Enabling Processes [IS12a] innerhalb der Domäne der Managementprozesse beschrieben.

Der leichtgewichtige SIEM-Prozess: die Prozessbausteine auf dem Prüfstand

Zur Gestaltung eines einfach anwendbaren und leicht verständlichen Modells – abgeleitet aus dem allgemeinen SIEM-Pro-

zess (Abb. 1) – werden die zuvor identifizierten Aktivitäten und Outputs überprüft. Ziel ist es, Prozessbausteine sinnvoll zusammenzufassen oder aber auch komplett zu streichen, ohne die Wirksamkeit des SIEM-Prozesses zu gefährden.

Ausgehend von den Outputs, die den Aktivitäten zugeordnet sind, lassen sich beispielsweise O1, O2 und O3 in der Richtlinie O5 (Management von Security Incidents) und der zugehörigen Prozessbeschreibung für alle Security Incidents und Events auf einem gemeinsamen Niveau festhalten. Denkbar sind hier verschiedene Verfahren für unterschiedliche Typen von Incidents bzw. Events, sodass je nach Klassifizierung in Aktivität A3 unterschieden werden kann. Jedoch sollte bei dieser Variante die Anzahl und Variabilität der Verfahren auf ein Minimum beschränkt werden. Somit werden beispielsweise Response Pläne, Eskalations- und Kommunikationswege, Bewertungs- und Entscheidungskriterien nur noch nach Typ des Incidents bzw. Events definiert. Abweichungen werden an den Information Security Risk Manager eskaliert. Mit ähnlicher Argumentation lässt sich die Aktivität A1 ebenfalls in dieselbe Richtlinie aufnehmen.

Weiter vereinfachend wirkt eine Zusammenfassung der Aktivitäten A5 und A6, da kleinere und mittlere Organisationen die Definition der Folgemaßnahmen und die damit einhergehende Durchführung und Beseitigung der Störung meist in einem Arbeitsschritt erledigen. Verzichten kann man hingegen auf die Aktionen A7 und A8. Relevante Aufzeichnungen werden aufgrund der hohen Verbreitung von SMS-Tools meist ohnehin automatisch erstellt. Ein entsprechendes Erfolgs- oder Nicht-Erfolgs-Review wird üblicherweise im Rahmen der Aktivitäten A5 und A6 implizit durchgeführt. Auch die Aktion A9 ist vernachlässigbar, da die Simulation von Security Incidents bei den KMU meist nicht organisationsintern, sondern von entsprechend spezialisierten Unternehmen extern durchgeführt wird. Als Koordinator dient

	ISO/IEC 27001	UCISA Toolkit	IT-Grundschutz	ITIL	FitSM	COBIT 5	Leichtgewichtiges Modell
Aktivitäten/Inputs							
A1: Entwickeln eines Incident Response Plans, Definieren von Eskalations- und Kommunikationswegen		✓	✓			✓	**R**
A2: Überwachen und Aufzeichnen von Security Events	✓	✓	✓	✓	✓	(✓)	✓
A3: Bewerten und Klassifizieren von Security Events	✓	✓	(✓)		✓	✓	✓
A4: Analysieren und Antworten auf Security Incidents und Events	✓	✓	✓	✓	✓	✓	✓
A5: Definieren und Überwachen von Folgemaßnahmen			x	x	x		✓
A6: Beseitigen der Ursachen, Untersuchen und Lindern der Konsequenzen	(✓)	✓	✓	✓		✓	✓
A7: Aufzeichnen aller Aktionen und Berichterstattung	(✓)	✓	(✓)	✓	(✓)	✓	(✓)
A8: Durchführen eines Reviews nach einem Security Incident	✓	✓	(✓)	(✓)	(✓)	(✓)	(✓)
A9: Durchführen von Tests zur Simulation von Security Incidents und deren Dokumentation			✓				
Outputs							
O1: Dokumentierter Incident Response Plan zum Umgang mit Security Incidents		✓				✓	**R**
O2: Definierte Eskalations- und Kommunikationswege		✓	✓			✓	**R**
O3: Bewertungs- und Entscheidungskriterien	(✓)	(✓)			(✓)		**R**
O4: Berichte und Aufzeichnungen über Security Incidents und Events sowie Folgemaßnahmen	✓	✓	✓	✓	✓	✓	✓
O5: Richtlinie für das Management von Security Incidents (oder beschreibende Dokumentation)	✓	✓	✓	✓	✓	✓	✓

Tabelle 1: Aktivitäten und Outputs abgeleitet aus den Anforderungen der unterschiedlichen Rahmenwerke:
✓ = explizit, **(✓)** = implizit, **R** = als Verfahren in der Richtlinie enthalten

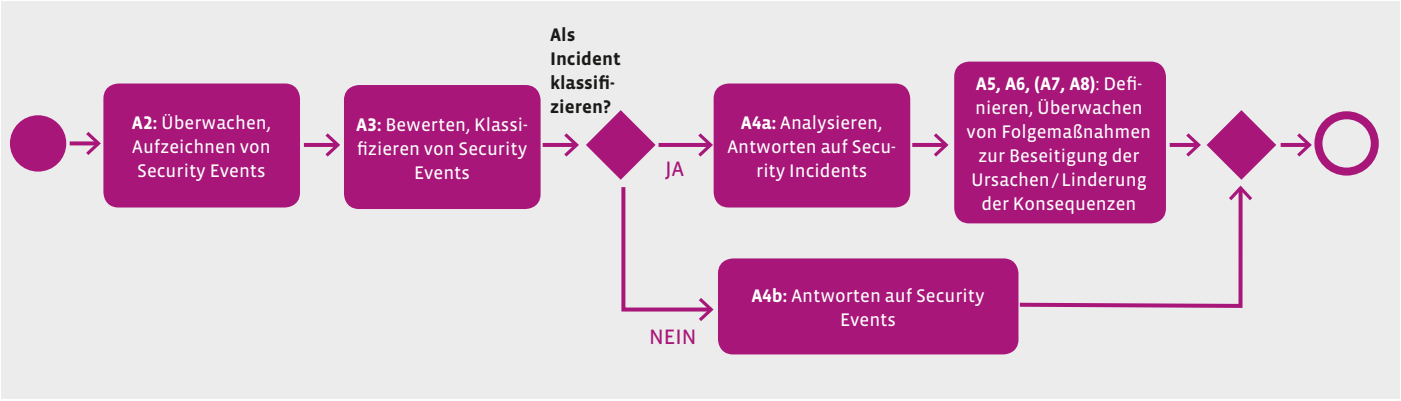


Abbildung 2: leichtgewichtiger SIEM-Prozess

hier ebenfalls der Information Security Risk Manager. Damit kann A9 ebenfalls als Eskalationszustand betrachtet werden. Die Zusammenfassungen und Kürzungen ergeben nun den leichtgewichtigen SIEM-Prozess (Abbildung 2).

Experten-Evaluation und Ausblick

Zur Validierung des Modells beurteilten acht Experten aus Hochschulumfeld und Industrie (Berater/Trainer, Auditoren, Datenschutzbeauftragte) die Kritikalität und Relevanz der einzelnen Prozessaktivitäten und -outputs mithilfe eines Online-Fragebogens – ohne zuvor Einsicht in das vorgestellte leichtgewichtige Modell bekommen zu haben. Die unvoreingenommene Fragestellung diente dazu, ein fundiertes Feedback über die Relevanz der Prozessbausteine zu erhalten. In der Gesamtbetrachtung aller Prozessbausteine bestätigen die Experten die Anwendbarkeit des leichtgewichtigen SIEM-Prozesses. Zur weiteren Bewertung des Modells ist im nächsten Schritt die praktische Umsetzung des Prozesses geplant. Ebenso können analog zu dem hier beschriebenen Vorgehen weitere beispielhafte, leichtgewichtige Verfahrensbeschreibungen zur Unterstützung der Umsetzung eines leichtgewichtigen Service Management Ansatzes entwickelt werden. ◆

LITERATUR

- B[Ax11] Axelos, Hrsg. ITIL service design. TSO The Stationery Office, London, 2nd ed. Auflage, 2011.
- [Br11] Brenner, Michael; Gentschen Felde, Nils; Hommel, Wolfgang; Metzger, Stefan; Reiser, Helmut; Schaaf, Thomas: Praxisbuch ISO-IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung; [mit 80 Prüfungsfragen zur Vorbereitung auf die Foundation-Zertifizierung]. Hanser, München, 2011.
- [Bu15] Bundestag: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 17.07.2015.
- [Bu16] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz: www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, Version: 2016. Abruf: 24. Mrz.2016.
- [De86] Deming, William Edwards: Out of the Crisis. Massachusetts Institute of Technology Center for Advances Engineering Study, Cambridge, Massachusetts, 1986.
- [Fi16] FitSM: FitSM-Standards for lightweight IT service management. http://fitsm.itemo.org/ , Version: 2016. Abruf: 1.Apr.2016
- [IS12a] ISACA: COBIT 5 – Enabling Processes. ISACA, Illinois, 2012
- [IS12b] ISACA: COBIT 5 – Rahmenwerk für Governance und Management der Unternehmens-IT. ISACA, Illinois 2012.
- [IS13a] ISO/IEC: Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013). 2013.
- [IS13b] ISO/IEC: Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013). 2013.
- [UC 1] UCISA: UCISA Information Security Management Toolkit. www.ucisa.ac.uk/~/media/Files/members/activities/ismt/Complete%20with%20covers, Edition 1.0 Volume 1. Abruf: 20.Feb.2016.

Das vollständige Paper „Leichtgewichtiges Security Incident und Event Management im Hochschulumfeld“ ist bei der Gesellschaft für Informatik e.V. (GI) unter folgendem Link veröffentlicht: https://dl.gi.de/handle/20.500.12116/482.

Alles unter Kontrolle?

Die EU-DSGVO und ihre Auswirkungen auf die Rolle des Datenschutzbeauftragten

Die Europäische Datenschutzgrundverordnung (EU-DSGVO), die am 25. Mai 2018 in allen europäischen Mitgliedstaaten wirksam werden wird, bringt neben den Veränderungen in der datenschutzrechtlichen Regelungssystematik auch einige Neuerungen im Bereich der datenschutzrechtlichen Kontrollorgane mit sich. Insbesondere das Anforderungs- und Aufgabenprofil des Datenschutzbeauftragten erfährt Änderungen, die es bis zum Wirksamwerden der DSGVO in die internen Abläufe der Hochschulen und Forschungseinrichtungen zu integrieren gilt. Der folgende Beitrag zeigt einige wesentliche Unterschiede von bestehendem und künftigem Recht auf. Sofern der Gesetzgeber zwischen öffentlichen und nicht-öffentlichen Stellen unterscheidet, wird diesen Unterschieden im Folgenden Rechnung getragen; im Übrigen liegt ein regulatorischer Gleichklang vor.

Text: **Charlotte Röttgen** (Forschungsstelle Recht im DFN)

Foto © yoh4nn / iStock

I. Einleitung

Nach bisherigem Datenschutzrecht gibt es vor allem zwei entscheidende datenschutzrechtliche Institutionen, die Aufsichtsbehörde als obere datenschutzrechtliche Kontrollinstanz sowie den Datenschutzbeauftragten. Während die Aufgabe der Aufsichtsbehörde im Wesentlichen darin besteht, die Einhaltung datenschutzrechtlicher Vorschriften bei der Verarbeitung personenbezogener Daten durch datenverarbeitende Stellen zu überwachen und bei Verstößen einzuschreiten, war es bislang die Aufgabe des im Zentrum dieses Beitrags stehenden Datenschutzbeauftragten, auf die Einhaltung datenschutzrechtlicher Vorgaben bei der Verarbeitung personenbezogener Daten innerhalb der eigenen Behörde oder der nicht-öffentlichen Stelle hinzuwirken.

Mit Wirksamwerden der DSGVO innerhalb der europäischen Mitgliedstaaten gehen hinsichtlich der Rolle des Datenschutzbeauftragten einige Neuerungen einher. Wird sich an Art und Anzahl der datenschutzrechtlichen Institutionen nichts ändern, gibt es aber bei der Bestellpflicht sowie beim Aufgaben- und Anforderungsprofil einige Punkte, die es nach der DSGVO zukünftig zu beachten gilt.

Die geänderten Vorschriften der DSGVO haben auch zur Folge, dass sich das Verhältnis von Personalrat bzw. Betriebsrat und Datenschutzbeauftragtem voraussichtlich verändern wird. Unterliegen Personal- und Betriebsrat in ihrer Tätigkeit – soweit sie

die Verarbeitung personenbezogener Daten zum Gegenstand hat – bislang nicht der Kontrolle durch den Datenschutzbeauftragten, könnte sich dies ab Mai nächsten Jahres ändern.

II. Der Datenschutzbeauftragte im öffentlichen und nicht-öffentlichen Bereich

Der Datenschutzbeauftragte ist und bleibt auch nach der DSGVO das Kontrollorgan innerhalb einer öffentlichen oder nicht-öffentlichen Stelle. Er ist Ansprechpartner für die Behördenleitung, die Geschäftsführung und die Beschäftigten in allen, den Datenschutz betreffenden Angelegenheiten und ist in alle datenschutzrelevanten Abläufe der datenverarbeitenden Stelle einzubinden, um die Einhaltung der Datenschutzgesetze zu überprüfen. Die Aufgaben, die Anforderungen und das Verfahren der Bestellung des Datenschutzbeauftragten sind in der DSGVO abschließend in Art. 37-39 DSGVO geregelt.

1. Die Pflicht zur Bestellung eines Beauftragten für den Datenschutz

Nach bisherigem Recht auf Bundes- und Landesebene ist die Bestellung eines Datenschutzbeauftragten für öffentliche Stellen und Behörden bereits verpflichtend. Auf Bundesebene beispielsweise findet sich die Regelung zur Bestellpflicht des behördlichen Beauftragten für den Datenschutz im aktuell bestehenden Recht in § 4f Abs. 1 S. 1 BDSG, im nordrhein-westfälischen Datenschutzgesetz in § 32a Abs. 1 S. 1 DSG NRW und im Datenschutzgesetz von Berlin in § 19a Abs. 1 S. 1 Bln DSG. Teilweise hängt die Pflicht zur Bestellung des behördlichen Datenschutzbeauftragten davon ab, ob die Verarbeitung personenbezogener Daten automatisiert erfolgt.

Letzteres ist in der DSGVO nicht mehr der Fall; im Bereich der Bestellpflicht des Datenschutzbeauftragten wird eine Differenzierung zwischen automatisierter und nicht automatisierter Datenverarbeitung zukünftig nicht mehr vorgenommen. Mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln, sieht die DSGVO eine solche Bestellpflicht für öffentliche Stellen und Behörden, die personenbezogene Daten verarbeiten, nun verbindlich vor. Das heißt, beruhte die Einführung einer Bestellpflicht eines behördlichen Datenschutzbeauftragten bisher auf dem Willen des jeweiligen Bundes- oder Landesgesetzgebers, gibt es hier künftig keinen Abweichungsspielraum mehr und es besteht gem. Art. 37 Abs. 1 lit. a DSGVO in allen Ländern sowie im Bund die unmittelbare Pflicht, einen behördlichen Datenschutzbeauftragten zu bestellen.

Für öffentliche Hochschulen und Forschungseinrichtungen wird sich also nur dann etwas ändern, wenn in dem jeweiligen Datenschutzrecht ihres Landes eine solche Bestellpflicht bislang nicht existierte.

Im nicht-öffentlichen Bereich stellt sich die Rechtslage folgendermaßen dar: Werden personenbezogene Daten automatisiert verarbeitet und sind mit dieser Datenverarbeitung mehr als neun Personen betraut, besteht nach derzeit geltendem Recht auch für nicht-öffentliche Stellen die Pflicht zur Bestellung eines Datenschutzbeauftragten (§ 4f Abs. 1 S. 3 BDSG). Im Falle der nicht-automatisierten Datenverarbeitung liegt die Schwelle der hiermit betrauten Personen bei 20 (§ 4f Abs. 1 S. 2 BDSG). Wird die Mindestanzahl an Personen, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, nicht überschritten, besteht nach noch geltendem Recht somit keine Pflicht zur Bestellung eines Datenschutzbeauftragten im nicht-öffentlichen Bereich. Ausnahmsweise besteht aber unabhängig von der Anzahl der Beschäftigten eine generelle Bestellpflicht für nicht-öffentliche Stellen, sofern sie „automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten“ (§ 4f Abs. 1 S. 6 BDSG).

Ab dem 25. Mai 2018, wenn die DSGVO wirksam wird, ergibt sich die Pflicht zur Bestellung eines Datenschutzbeauftragten im nicht-öffentlichen Bereich aus Art. 37 Abs. 1 lit. b und c DSGVO. Hiernach wird es für die Frage nach einer Bestellpflicht wesentlich auf die Kerntätigkeit des Verantwortlichen ankommen. Besteht diese nämlich in der Durchführung von Verarbeitungsvorgängen, die „aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen“ (Art. 37 Abs. 1 lit. b DSGVO) oder besteht diese in der „umfangreichen Verarbeitung besonderer Kategorien von Daten“ (Art. 37 Abs. 1 lit. c DSGVO), trifft nicht-öffentliche Stellen die Pflicht zur Bestellung eines Datenschutzbeauftragten. Der Begriff Kerntätigkeit ist so zu verstehen, dass es sich um die Haupt- und nicht nur eine Nebentätigkeit handeln muss. Das bedeutet, dass die konkrete Datenverarbeitung für die Geschäftsabläufe erforderlich ist.

2. Interner, externer und gemeinsamer Datenschutzbeauftragter

Gem. Art. 37 Abs. 6 DSGVO besteht – wie auch schon nach altem Recht – die Möglichkeit, einen Datenschutzbeauftragten aus dem Kreis der Beschäftigten des Verantwortlichen zu wählen oder alternativ einen externen Beauftragten für den Datenschutz auf Grundlage eines Dienstleistungsvertrags zu verpflichten.

Außerdem können nach bisher geltendem Recht auf Bundes- und Landesebene die Behörden und öffentlichen Stellen für mehrere Einrichtungen einen gemeinsamen Datenschutzbeauftragten bestellen (vgl. § 5 Abs. 3 S. 2 HDSG; § 32a Abs. 1 S. 3 DSG NRW). Das aktuelle Bundesdatenschutzgesetz sieht hier eine Einschränkung insoweit vor, als dass der Datenschutzbeauftragte nur dann für mehrere Stellen gleichzeitig ernannt werden darf, wenn dies auf-

grund der Struktur der Stellen bzw. Behörden erforderlich ist (§ 4f Abs. 1 S. 5 BDSG).

Auch zukünftig werden mehrere öffentliche Stellen oder mehrere Behörden gem. Art. 37 Abs. 3 DSGVO einen gemeinsamen Datenschutzbeauftragten bestellen können. Hierbei haben sie künftig allerdings ihrer jeweiligen Organisationsstruktur und -größe Rechnung zu tragen. Die Anzahl der öffentlichen Stellen und Behörden, für die ein Datenschutzbeauftragter bestellt werden kann, darf nicht so groß sein, dass er nicht mehr in der Lage ist, seine ihm obliegenden Aufgaben angemessen in dem gebotenen Rahmen wahrzunehmen.

Hinsichtlich der nicht-öffentlichen Stellen ist im aktuellen BDSG keine ausdrückliche Regelung dazu enthalten, unter welchen Voraussetzungen und Rahmenbedingungen ein Datenschutzbeauftragter für eine Unternehmensgruppe bestellt werden kann. Die DSGVO schafft diesbezüglich in Art. 37 Abs. 2 DSGVO Klarheit. Nach künftigem Recht wird die Bestellung eines gemeinsamen Datenschutzbeauftragten einer Unternehmensgruppe dann zulässig sein, wenn dieser von jeder Niederlassung aus leicht erreicht werden kann. Ob es sich bei der geforderten Erreichbarkeit um eine solche via Kommunikationsmittel oder eine örtliche Erreichbarkeit handelt, geht aus der Norm nicht hervor. Da eine Erreichbarkeit über Kommunikationsmittel de facto keine Einschränkung in einer Unternehmensstruktur darstellen würde, ist es wahrscheinlicher, dass der Gesetzgeber hier auf die örtliche Erreichbarkeit abstellen wollte.

3. Anforderungsprofil

Eine Neuerung stellen die erhöhten Anforderungen an die fachliche Qualifikation des Datenschutzbeauftragten nach der DSGVO dar. Wird bisher die „erforderliche Fachkunde und Zuverlässigkeit“ verlangt (bspw. § 4f Abs. 2 S. 1 BDSG; § 32a Abs. 1 S. 2 DSG NRW; § 19a Abs. 2 S. 1 Bln DSG), enthält Art. 37 Abs. 5 DSGVO zu dem Anforderungsprofil des Datenschutzbeauftragten nun ausdrückliche Vorgaben. Zukünftig wird der Datenschutzbeauftragte sowohl im öffentlichen, als auch im nicht-öffentlichen Bereich „auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt […].“ Mit der ausdrücklichen Betonung von Fachwissen im Bereich des Datenschutzrechts und der Datenschutzpraxis macht der Unionsgesetzgeber deutlich, dass sowohl eine rechtliche als auch eine spezielle technische Vorbildung bei der Person vorhanden sein sollten, die in das Amt des Datenschutzbeauftragten berufen wird. Inwieweit sich dies in der Praxis umsetzen lassen wird, ist fraglich, da längst nicht jede Behörde oder nicht-öffentliche Stelle über Personal verfügt, das die verlangten Kenntnisse vorweisen kann.

Von der DSGVO abweichende Auswahlkriterien, wie sie in der Vergangenheit in Behörden und Unternehmen entwickelt worden sind, um die erforderliche Fachkunde des Datenschutzbeauftragten feststellen zu können, werden mit Wirksamwerden der DSGVO nicht mehr anwendbar sein, da die Regelungen diesbezüglich abschließend sind und so die bisherige nationale Rechtspraxis verdrängen. Darüber hinaus verlangt Art. 37 Abs. 5 DSGVO, dass der Datenschutzbeauftragte die erforderlichen Fähigkeiten besitzt, um die in Art. 39 genannten Aufgaben erfüllen zu können. Neben der Aufgabe, die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen, muss er etwa auch die fachliche Qualifikation zur Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten besitzen (Art. 39 Abs. 1 lit. a DSGVO) und den Verantwortlichen im Zusammenhang mit der Datenschutz-Folgenabschätzung beraten können (Abs. 1 lit. c).

4. Das Aufgabenprofil des Datenschutzbeauftragten

Dass der Datenschutzbeauftragte vertiefte fachliche Kenntnisse besitzen sollte, kommt nicht von ungefähr. Abhängig davon, in welchem Umfang die jeweilige Einrichtung Daten verarbeitet, kann sich der Tätigkeitsaufwand des Datenschutzbeauftragten durch die DSGVO deutlich erweitern. Der in Art. 39 Abs. 1 DSGVO enthaltene Aufgabenkatalog des Datenschutzbeauftragten reicht von der Unterrichtung und Beratung der verantwortlichen datenverarbeitenden Stelle sowie der Beschäftigten (lit. a), über die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften (lit. b) bis hin zu der Beratung des Verantwortlichen im Zusammenhang mit der Datenschutz-Folgenabschätzung (lit. c). Die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften dürfte verglichen mit der alten Rechtslage voraussichtlich die größte Änderung im Aufgabenprofil des Datenschutzbeauftragten darstellen.

a) Überwachungsaufgabe

Infolge der sprachlichen Neuformulierung der Aufsichtsfunktion wird sich voraussichtlich eine wesentliche Änderung in der Tätigkeit des Datenschutzbeauftragten ergeben. Gem. Art. 39 Abs. 1 lit. b DSGVO „überwacht“ der Datenschutzbeauftragte die Einhaltung der DSGVO und anderer Datenschutzvorschriften. Vergleicht man diese Formulierung mit denen der alten Datenschutzgesetze, offenbart sich eine deutliche Verschärfung der Verantwortlichkeit. Nach dem alten Recht „unterstützt“ der Datenschutzbeauftragte bislang die verantwortliche Stelle bei der Sicherstellung des Datenschutzes (§ 32a Abs. 1 S. 5 DSG NRW) oder „wirkt“ auf die Einhaltung datenschutzrechtlicher Vorschriften „hin“(§ 4g Abs. 1 S. 1 BDSG). Sowohl das „Unterstützen“ bei der Einhaltung von Datenschutzgesetzen als auch das „Hinwirken“ darauf implizieren eine helfende aber zugleich untergeordnete Rolle. Mit Wirksamwerden der DSGVO wird der Datenschutzbeauftragte nunmehr für die „Überwachung der Einhaltung“ verantwortlich. Indem er zukünftig die Einhaltung der Datenschutzgesetze zu überprüfen hat, wird er voraussichtlich in die Rolle eines Letztverantwortlichen kommen;

seine Verantwortung im Bereich der Datenschutz-Compliance wird dadurch deutlich erhöht werden.

b) Unterrichtungs- und Beratungstätigkeit

Die Unterrichtungs- und Beratungsfunktion kann etwa die Durchführung regelmäßiger Schulungen der Verantwortlichen sowie der Beschäftigten durch den Datenschutzbeauftragten erfordern, in denen der Datenschutzbeauftragte hinreichende Kenntnisse im Bereich des Datenschutzrechts und insbesondere für die konkret durchzuführenden Datenverarbeitungen vermitteln soll. In Wahrnehmung dieser Aufgaben dient der Datenschutzbeauftragte hierbei als Ansprechpartner sowohl der verantwortlichen Stelle, als auch den Beschäftigten gegenüber. Dieses Aufgabenfeld gehört auch nach bisherigem Recht zu einer der Haupttätigkeiten eines Datenschutzbeauftragten. Durch die DSGVO wird es hier zu keinen gravierenden Änderungen kommen.

c) Datenschutz-Folgenabschätzung

Ist es bislang noch die Aufgabe des Datenschutzbeauftragten, eine Vorabkontrolle in etwaige risikobehafteten Verarbeitungsverfahren durchzuführen (bspw. § 4d Abs. 5, 6 BDSG; § 32a Abs. 1 DSG NRW), bringt die DSGVO in diesem Bereich eine Änderung mit sich. Zukünftig wird es keine Vorabkontrolle mehr geben, sondern eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO), die inhaltlich aber im Wesentlichen der Vorabkontrolle entspricht. Die Datenschutz-Folgenabschätzung ist eine Risikobewertung, die vorzunehmen ist, wenn bei der Verarbeitung personenbezogener Daten voraussichtlich ein erhöhtes Risiko für Rechte und Freiheiten natürlicher Personen bestehen könnte. Ein solches Risiko gilt es, im Rahmen der Folgenabschätzung zu erkennen und zu bewerten. Gehörte die Durchführung der Vorabkontrolle bislang gänzlich in den Aufgabenbereich des Datenschutzbeauftragten, wird die Datenschutz-Folgenabschätzung nach der DSGVO von dem für die Datenverarbeitung Verantwortlichen selbst durchzuführen sein. Der Datenschutzbeauftragte soll den Verantwortlichen bei der Datenschutz-Folgenabschätzung nur noch beraten.

III. Die Aufsichtsfunktion des Datenschutzbeauftragten im Verhältnis zu Personal- und Betriebsrat

Im datenschutzrelevanten Tätigkeitsbereich des Personal- und des Betriebsrats wird es ab dem 25. Mai 2018 eine wesentliche Änderung geben. Zukünftig dürften nämlich beide der Kontrolle durch den Datenschutzbeauftragten unterliegen. Das würde bedeuten, soweit ihre Tätigkeit den Umgang mit und die Verarbeitung von personenbezogenen Daten zum Gegenstand hat, dürfte der Datenschutzbeauftragte diese Arbeitsabläufe im Hinblick auf ihre Konformität mit den Vorgaben des Datenschutzrechts überprüfen. Dies ergibt sich aus Art. 38 Abs. 2 DSGVO, der vorschreibt, dass dem Datenschutzbeauftragten in Wahrnehmung seiner Aufgaben ausnahmslos Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zu gewähren ist. Eine Einschränkung im Hinblick auf den Personal- und/oder den Betriebsrat ist in der Norm nicht enthalten.

Nach der bisherigen Rechtsprechung der deutschen Gerichte stellt sich die Rechtslage – sowohl auf Bundes-, als auch auf Landesebene – derzeit noch so dar, dass Personalrat und Betriebsrat keiner Kontrolle durch den Datenschutzbeauftragten unterliegen. Diese Rechtspraxis wird mit großer Wahrscheinlichkeit zukünftig, unter Geltung der DSGVO, nicht aufrechterhalten bleiben können. Grund hierfür ist, dass diese richterrechtliche Regelung nicht mit den Vorgaben der DSGVO im Einklang steht.

IV. Zusammenfassung und Ausblick

Die europäische Datenschutzreform, die ab dem 25. Mai 2018 ihre Wirksamkeit entfalten wird, hat auch Auswirkungen auf die Rolle des Datenschutzbeauftragten. Während es hinsichtlich der Pflicht zur Bestellung eines Beauftragten für den Datenschutz im öffentlichen Bereich nur marginale Änderungen geben wird, werden vor allem nicht-öffentliche Einrichtungen durch den Wegfall des Schwellenwerts von der Gesetzesänderung betroffen sein. Bei dem Anforderungs- und Aufgabenprofil des Datenschutzbeauftragten kommt es schließlich zu mehreren wesentlichen Neuerungen. Insbesondere weist Art. 39 DSGVO dem Datenschutzbeauftragten einen erweiterten und stärker ausdifferenzierten Aufgabenbereich zu, der mit gesteigerten Qualifikationsanforderungen an seine Person im Zeitpunkt der Bestellung korrespondiert. Die Aufgabe der Überwachung der Einhaltung datenschutzrechtlicher Vorschriften dürfte hierbei die wichtigste Neuerung und diejenige mit dem größten Verantwortungszuwachs darstellen.

Es ist den Datenschutzbeauftragten von Hochschulen und Forschungseinrichtungen daher angeraten, sich bis zum Wirksamwerden der DSGVO auf die inhaltlichen Neuerungen ihrer Tätigkeit vorzubereiten. Insbesondere die zukünftige Überwachungsaufgabe verlangt eingehende Kenntnisse der Vorgaben der DSGVO und der datenschutzrechtlichen Spezialvorschriften. Da die Aufsichtsbehörde im Falle von Verstößen des Datenschutzbeauftragten gegen Art. 37-39 DSGVO die Hochschulen und Forschungseinrichtungen mit Sanktionen belegen kann, ist es auch im Interesse der Verantwortlichen, eine zeitnahe Weiterbildung ihrer Datenschutzbeauftragten zu fördern. Ob und wie sich das Verhältnis von Datenschutzbeauftragtem und Personalrat bzw. Betriebsrat aufgrund des neuen Hierarchieverhältnisses zwischen den beiden Akteuren in der Praxis ändern wird, bleibt abzuwarten. ◆

Ist Internet nicht gleich Internet?

BGH legt dem EuGH eine Vorlagefrage zur urheberrechtlichen Beurteilung der Übernahme eines Bildes auf die eigene Homepage vor.

Mit seinen Entscheidungen zur urheberrechtlichen Beurteilung von sogenannten Hyperlinks und Framelinks auf geschützte Werke, die mit Erlaubnis des Rechteinhabers veröffentlicht wurden, hat der Europäische Gerichtshof (EuGH) wesentliche Grundsätze aufgestellt, die es bei urheberrechtlichen Fragestellungen im digitalen Raum zu beachten gilt. Mit der Frage, inwiefern diese Grundsätze auch auf andere Sachverhaltskonstellationen übertragbar sind, musste sich nun der Bundesgerichtshof (BGH) auseinandersetzen. Mit seinen Vorlagefragen an den EuGH vom 23.02.2017 (Az. I ZR 267/15) bittet er den EuGH die Frage abschließend zu beantworten, ob die aufgestellten Grundsätze auf diejenigen Situationen übertragbar sind, in denen ein frei zugängliches Bild, das mit Erlaubnis des Rechteinhabers auf einer Internetseite veröffentlicht wurde, kopiert und auf einer anderen Internetseite veröffentlicht wird. Der BGH deutet an, dass er eine Übertragbarkeit in diesem Zusammenhang ablehne.

Text: **Armin Strobel** (Forschungsstelle Recht im DFN)

Foto © Odem1970/iStock

I. Hintergrund

Mit der voranschreitenden Digitalisierung werden das Urheberrecht und die Betroffenen vor immer neue Fragen gestellt. Die Vielfalt und die damit verbundenen Möglichkeiten des Internets führen regelmäßig zu neuen Fallkonstellationen, die es mithilfe des Urheberrechts interessengerecht zu lösen gilt. Im Fokus steht dabei immer wieder die Nutzung eines im Internet frei zugänglichen Werks für eigene Zwecke. Die freie Zugänglichkeit der Werke führt jedoch nicht automatisch dazu, dass die Werke auch ohne Weiteres genutzt werden dürfen. Sowohl nationale als auch europäische Urheberrechtsbestimmungen gilt es zu beachten, um eine Haftung für eigene Handlungen zu verhindern.

In der Vergangenheit hat sich der EuGH bereits mit Fragen der Haftung für sogenannte Hyperlinks beschäftigt. Die dort aufgestellten Grundsätze haben bei der rechtlichen Beurteilung von urheberrechtlichen Fallgestaltungen im digitalen Raum wesentliche Bedeutung gewonnen. Es stellt sich nun die Frage, ob diese Grundsätze auch auf andere, vergleichbare Sachverhaltskonstellationen übertragen werden können.

Im Zentrum dieser Fragestellungen steht dabei das Recht der öffentlichen Zugänglichmachung nach § 19a Urheberrechtsgesetz (UrhG). Es handelt sich hierbei um eine besondere Form der öffentlichen Wiedergabe im Sinne des § 15 Abs. 2 und 3 UrhG, nach welchem es dem Rechteinhaber vorbehalten ist, ein urheberrechtlich geschütztes Werk drahtgebunden oder drahtlos der Öffentlichkeit in einer Weise zugänglich zu machen, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist. Da die Vorschrift auf einer europäischen Richtlinie beruht, ist bei der Anwendung der Vorschriften auf eine richtlinienkonforme Auslegung zu achten. Die abschließende Auslegungskompetenz des europäischen Rechts obliegt dabei dem EuGH. Aus diesem Grund besteht für Gerichte die Möglichkeit, ein Gerichtsverfahren auszusetzen und Fragen dem EuGH vorzulegen, wenn es die Auslegung von europarechtlichen Vorschriften für den konkreten Fall als erforderlich ansieht und die Fragen nicht unter Berücksichtigung vorheriger Rechtsprechung des EuGH beantwortet werden können (vgl. Art. 267 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)).

II. Sachverhalt

Von dieser Möglichkeit hat im vorliegenden Fall auch der BGH Gebrauch gemacht. In dem zugrundeliegenden Rechtsstreit macht ein Fotograf (Kläger) sein Recht der öffentlichen Zugänglichmachung geltend, das er durch ein online veröffentlichtes Referat auf einer Schulhomepage als verletzt ansieht.

Als Rechteinhaber einer Fotografie der Stadt Cordoba hat der Kläger einzig einem Online-Reisemagazin ein einfaches Nutzungsrecht für die Veröffentlichung im Internet eingeräumt. Eine Schülerin hat dieses Bild kopiert und in ein Referat eingefügt. Das Schülerreferat wurde anschließend auf dem Server der Schule gespeichert und zusätzlich auf der Schulhomepage veröffentlicht. Durch die Einstellung des Referats mit der Fotografie sieht der Kläger sein Recht der öffentlichen Zugänglichmachung verletzt und verlangt die Entfernung des Referats von der Homepage sowie Schadensersatz. Hiergegen wehrt sich die Beklagte (Bundesland, das die Schulaufsicht ausübt). Sie ist der Ansicht, dass keine Urheberrechtsverletzung vorliege, da die Fotografie durch die Veröffentlichung in dem Online-Reisemagazin bereits für jedermann frei zugänglich war und somit keine Verletzung des Rechts der öffentlichen Zugänglichmachung anzunehmen sei.

III. Vorlagefrage des BGH

Nachdem die vorinstanzlichen Gerichte eine Urheberrechtsverletzung durch das Einstellen des Referats mit der Fotografie bejahten, muss sich nun auch der BGH mit dieser Frage auseinandersetzen. Wie bereits angedeutet, geht es auch hier um die Frage, ob durch die Veröffentlichung des Referats das Recht der öffentlichen Zugänglichmachung des Klägers bezüglich der Fotografie von Cordoba verletzt wird. Von zentraler Bedeutung ist dabei, ob die vom EuGH aufgestellten Grundsätze zur Linkhaftung auf die hier vorliegende Situation übertragen werden können.

Eine öffentliche Zugänglichmachung ist anzunehmen, wenn die beiden Tatbestandsvoraussetzungen – Handlung der Wiedergabe und Öffentlichkeit dieser Wiedergabe – erfüllt sind.

Die Handlung der Wiedergabe ist nach dem BGH weit zu verstehen, um ein hohes Schutzniveau des Urheberrechts zu gewährleisten. Entscheidend ist, dass einem Dritten absichtlich und gezielt der Zugang zu einem urheberrechtlich geschützten Werk verschafft wird, den dieser ohne diese Handlung nicht hätte. Das eingesetzte technische Mittel oder Verfahren ist nicht erheblich. Im vorliegenden Fall bejaht das Gericht diese Voraussetzung. Durch das Einstellen des Referats auf der Schulhomepage werde die Fotografie von Cordoba den Besuchern der Schulhomepage zugänglich gemacht. Es schade insofern nicht, dass die Besucher der Schulhomepage das Bild auch über die Internetseite des Online-Reisemagazins hätten abrufen können, weil ihnen durch die Veröffentlichung auf der Schulhomepage zumindest ein weiterer Zugang ermöglicht wurde, der ohne die Einstellung nicht bestanden hätte.

Der BGH stellt außerdem fest, dass sich die Veröffentlichung des Referats auf der Internetseite der Schule grundsätzlich an die Öffentlichkeit richtet, da das Referat für jeden Internetnutzer

zugänglich ist und sich damit an eine unbestimmte Zahl potenzieller Adressaten richtet. Um eine öffentliche Zugänglichmachung im Sinne des Urheberrechts annehmen zu können, ist darüber hinaus jedoch erforderlich, dass die Veröffentlichung unter Verwendung eines anderen technischen Verfahrens als bei der Erstveröffentlichung erfolgt oder zumindest für ein neues Publikum wiedergegeben wird.

Ein anderes technisches Verfahren der Veröffentlichung verneint der BGH in diesem Fall mit dem Hinweis, dass sowohl bei der Erstveröffentlichung in dem Online-Reisemagazin als auch bei der Veröffentlichung auf der Schulhomepage eine Wiedergabe im Internet erfolgte und sich damit die Verfahren der Veröffentlichung nicht unterscheiden.

Zweifel äußert der BGH aber hinsichtlich der Wiedergabe gegenüber einem neuen Publikum. Ein solches kann grundsätzlich angenommen werden, wenn durch die zweite Veröffentlichung ein Publikum angesprochen wird, an das der Rechteinhaber bei der ersten Veröffentlichung nicht dachte. Die Zweifel sind darin begründet, dass die Beklagte geltend macht, dass die Grundsätze des EuGH zur Linkhaftung auf die vorliegende Fallkonstellation übertragen werden könnten. Der EuGH verneint eine Wiedergabe gegenüber einem neuen Publikum, wenn ein Link zu einem urheberrechtlich geschützten Werk führt, das auf der anderen Internetseite mit Erlaubnis des Rechteinhabers veröffentlicht wurde und ohne Zugangsbeschränkungen für jedermann zugänglich ist. Nach Auffassung des EuGH richtet sich sowohl die erste Veröffentlichung als auch der Link an jeden potenziellen Internetnutzer, sodass in beiden Fällen jedermann als Adressat der jeweiligen Handlung angesehen werden kann. Da sich die Adressatenkreise somit überschneiden und die Erstveröffentlichung auch bewusst an jeden Internetnutzer adressiert war, kann für diesen Fall kein neues Publikum angenommen werden.

Bundesgerichtshof in Karlsruhe
Foto © Nikolay Kazakov

Diese Grundsätze möchte die Beklagte auf die hier zugrundeliegende Sachverhaltskonstellation übertragen wissen. Auch hier sei es so, dass die Fotografie in dem Online-Reisemagazin ohne jegliche Zugangsbeschränkung veröffentlicht wurde. Dadurch richte sich diese Veröffentlichung an alle potenziellen Internetnutzer. Eine erneute Veröffentlichung auf der Schulhomepage könne sich dann nicht an ein neues Publikum richten. Die Situation sei mit der bei der Linksetzung vergleichbar, sodass auch die Grundsätze übertragbar seien.

Der BGH teilt die Argumentation und Ansicht der Beklagten hingegen nicht. Die Entscheidung des EuGH bei der Linksetzung basiere auf der Abwägung zwischen den Interessen des Urhebers und denen der Nutzer von urheberrechtlich geschützten Werken. Für das Funktionieren des Internets seien dabei elektronische Verweise in Form der Hyperlinks von besonderer Bedeutung, um sich in dem Medium zurechtzufinden und zu bewegen. Das Interesse auf einen funktionierenden Meinungs- und Informationsaustauschs übersteige daher das Interesse des Rechteinhabers, das Werk nach seinem Ermessen zu nutzen. Eine vergleichbare Sachlage sei hier jedoch nicht zu erkennen. Für das Funktionieren des Internets und einen regen Meinungs- und Informationsaustausch sei das Kopieren eines Werks auf den eigenen Server und das Einstellen auf eine andere Internetseite nicht erforderlich. Die Interessenabwägung ginge vielmehr zugunsten des Urhebers aus, der sein Werk verwerten wolle und von einem hohen Urheberrechtsschutz profitieren möchte.

Außerdem stellt der BGH die zentrale Rolle des Nutzers eines urheberrechtlich geschützten Werks heraus. Bei der Linksetzung habe der Linksetzende keine abschließende Kontrolle über das verlinkte Werk. Allein der Betreiber der ersten Internetseite – der mit Erlaubnis des Rechteinhabers agiere – könne darüber entscheiden, ob das Werk im Internet abrufbar sei oder nicht. Werde das Werk von der ersten Internetseite gelöscht, gehe der Link

ins Leere und der Linksetzende könne das Werk keinem mehr zugänglich machen. Im hier zu entscheidenden Fall nehme die Beklagte hingegen eine zentrale Rolle bei der öffentlichen Zugänglichmachung ein. Durch das Kopieren der Fotografie auf den Server und das Einstellen auf der Schulhomepage könne sie alleine darüber entscheiden, ob die Fotografie Dritten zugänglich gemacht werde. Auch bei einer Löschung des Bildes von der Internetseite des Online-Reisemagazins wäre es weiterhin auf der Schulhomepage abrufbar. Der Rechteinhaber könne somit nicht mehr alleine entscheiden, ob das Bild abrufbar ist. Das Gericht sieht in der Handlung der Beklagten daher vielmehr eine eigenständige Verwertungshandlung, die der Erlaubnis des Rechteinhabers bedürfe.

Aus diesen Gründen lehnt der BGH eine Übertragung der Grundsätze zur Linkhaftung des EuGH auf diese Fallkonstellation ab. Zugleich stellt der BGH jedoch fest, dass die Frage auch unter Berücksichtigung der bisherigen Rechtsprechung des EuGH nicht zweifelsfrei abschließend beantwortet werden könne. Da die Regelung zum Recht der öffentlichen Zugänglichmachung auf einer europäischen Richtlinie beruht, obliege es daher dem EuGH die Frage abschließend zu beantworten. Deshalb legt das Gericht die Frage der Übertragbarkeit der Grundsätze dem EuGH vor und unterlässt eine abschließende Entscheidung zu diesem Zeitpunkt.

IV. Fazit und Konsequenzen für die Hochschulen

Die Vorlage des BGH an den EuGH ist die Fortsetzung einer Reihe höchstrichterlicher Entscheidungen auf nationaler und europäischer Ebene zum Urheberrecht im digitalen Umfeld. Die Entscheidung des BGH zur Vorlage ist dabei im Ergebnis zu begrüßen. Eine endgültige Entscheidung hat – unabhängig in welche Richtung sie geht – weitreichende Auswirkungen, die es nicht zu unterschätzen gilt.

Auch wenn das Interesse der Beklagten auf Übertragung der Grundsätze auf die vorliegende Konstellation nachvollziehbar ist, erscheinen die vom BGH angeführten Argumente gegen eine solche Übertragbarkeit überzeugend. Die Kopie eines Bildes auf dem eigenen Server mit der anschließenden Veröffentlichung auf der eigenen Homepage ist nicht vergleichbar mit einem Link zu einem urheberrechtlich geschützten Werk. Vor allem der Kontrollverlust des Rechteinhabers über sein Werk führt zu einer Situation, die eine andere rechtliche Beurteilung erfordert. Eine Übertragung der genannten Grundsätze würde die Position des Rechteinhabers erheblich schwächen und zu einem Absenken des Schutzniveaus des Urheberrechts führen. Gerade bei der stetig wachsenden und schon jetzt erheblichen Bedeutung des Internets würde das quasi zu einem Schutzverlust des Urhebers führen, sobald das urheberrechtlich geschützte Werk einmal mit Erlaubnis veröffentlicht wurde. Ein gerechter Interessenausgleich würde durch eine so weitreichende Konsequenz gefährdet.

WEITERFÜHRENDE HINWEISE

Bei der Frage, ob die vom EuGH aufgestellten Grundsätze auf die vorliegende Fallkonstellation übertragen werden könne, beziehen sich sowohl die Beklagte im Rahmen ihrer Argumentation als auch der BGH in seiner Begründung auf die Entscheidungen des EuGH zu Hyperlinks und zum sogenannten Framing. Zu Zwecken der einfacheren Lesbarkeit wird in diesem Infobrief aber nur auf die Entscheidung zu den Hyperlinks ausdrücklich Bezug genommen.

Zur Rechtsprechung des EuGH zur Haftung für Hyperlinks siehe Strobel, „Links, Links, Links und immer noch nicht der rechte Weg?“, in: DFN-Infobrief Recht 11/2016.

Zur Rechtsprechung des EuGH zur Haftung für Framelinks siehe Hinrichsen, „Alles bleibt im Rahmen!“, in: DFN-Infobrief Recht 12/2014.

Für die Hochschulpraxis haben die Vorlagefragen des BGH zunächst einmal keine direkten Auswirkungen. An der Rechtslage ändert sich durch sie erst einmal nichts. Es gilt der Grundsatz der Vorsicht bei der Verwendung von Werken, die aus dem Internet beschafft werden. Ohne eine explizite Erlaubnis des Rechteinhabers sollten Bilder oder andere Werke nicht vorschnell kopiert und für eigene Zwecke auf Internetseiten veröffentlicht werden. Zumindest eine sorgfältige Klärung der Rechtslage an dem Werk sollte in jedem Fall erfolgen. Dennoch sollten die Hochschulen die Entwicklung in dieser Rechtssache verfolgen. Es geht hierbei um eine Fragestellung, die sich der eine oder andere Mitarbeiter schon einmal gestellt haben dürfte und die auch nicht gänzlich von der Hand zu weisen ist. Eine Entscheidung durch den EuGH führt daher zu Rechtssicherheit in einer Frage, die aufgrund der Vielfältigkeit des Internets und den daraus resultierenden Möglichkeiten nicht unerheblich ist. Der BGH hat mit seinen Ausführungen zwar angedeutet, welche Rechtsauffassung er vertritt, die abschließende Klärung erfolgt jedoch erst durch den EuGH und darf mit Spannung erwartet werden. ◆

DFN-Kanzlerforum am Müggelsee

Zum Thema „Wettbewerbsfaktor Digitalisierung“ trafen sich die Kanzlerinnen und Kanzler deutscher Universitäten und Hochschulen dieses Jahr am Müggelsee. Ein wichtiges Ziel des DFN-Kanzlerforums ist es, den Hochschulleitungen eine Diskussionsplattform zu aktuellen Themen der Informationsverarbeitung und datentechnischen Kommunikation zu bieten und sie über innovative Entwicklungen und Dienste innerhalb des Deutschen Forschungsnetzes zu informieren.

Text: **Maimona Id** (DFN-Verein)

Der DFN-Verein rief und die deutschen Kanzlerinnen und Kanzler kamen. Aus dem ganzen Bundesgebiet waren die Verwaltungschefs von Universitäten und Hochschulen der Einladung zum DFN-Kanzlerforum am 23. und 24. April an den Müggelsee gefolgt. Die „Badewanne der Berliner“ – so wird der größte der Hauptstadtseen auch genannt – bot eine angenehme Kulisse für den angeregten Austausch zu den aktuellen Herausforderungen der Digitalisierung für Forschung, Lehre und Verwaltung.

Das Kanzlerforum startete am Nachmittag mit einem Überblick zum Verein sowie den Aktivitäten der DFN-Geschäftsstelle. In verschiedenen Kurzvorträgen erhielten die Teilnehmerinnen und Teilnehmer Informationen zu den aktuellen Entwicklungen und Diensten rund um das Wissenschaftsnetz X-WiN sowie den internationalen Kooperationen und Forschungsprojekten des DFN. Der Abend bot den Gästen ausreichend Gelegenheit, sich auszutauschen.

„Quo vadis, DFN?“ hieß es am zweiten Tag des Kanzlerforums. Als advocatus diaboli betätigte sich dabei der Vorstandsvorsitzende des DFN-Vereins Hans-Joachim Bungartz: „Jedes Ding hat seine Zeit. Braucht es so etwas wie den DFN-Verein überhaupt noch?“, fragte er provokativ. Die Antwort lieferte er gleich nach.

Hotel Müggelsee Berlin: direkt am Seeufer gelegen *Foto © 2018, GCH Hotel Group, Germany*

Der DFN sei nicht nur der Betreiber des X-WiN, Interessenvertreter auf globaler Ebene oder aber Entwickler netzgestützter Dienste in Forschung, Lehre und Verwaltung, sondern ihm komme sogar eine Schlüsselrolle zu bei der Bewältigung der künftigen Herausforderungen und Aufgaben im Zuge der Digitalisierung. Denn eine funktionierende IT-Infrastruktur bilde das Rückgrat einer im Wandel befindlichen Wissenschaft. Besonders am Herzen lag dem Vorsitzenden die Rolle des DFN-Vereins als starke Interessengemeinschaft der großen wie auch kleinen Institutionen. Er forderte die Anwesenden zum Mitmachen und Mitgestalten auf. Mathias Neukirchen, Kanzler der Technischen Universität Berlin (TU Berlin) meldete sich daraufhin zu Wort: „Ich habe gestern und heute viel Spannendes zum DFN gehört. Es ist beruhigend, dass es Fachleute gibt, die unsere Themen so vorbereiten."

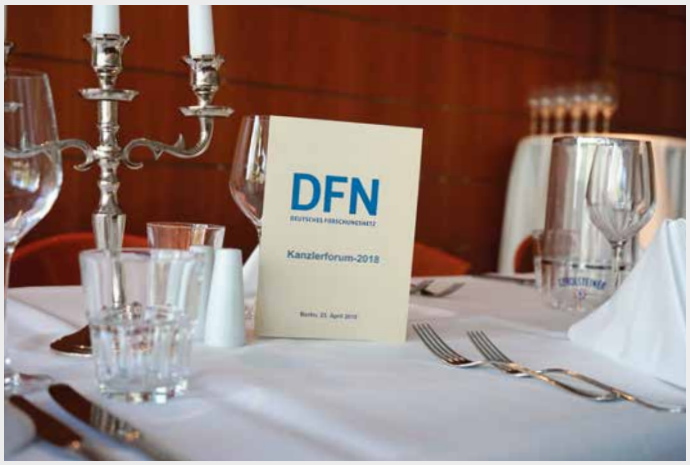
Auf sehr großes Interesse stieß das Thema Cloud-Services: Auf dem Podium, das vom stellvertretenden DFN-Vorstandsvorsitzenden Rainer Bockholt moderiert wurde, diskutierten Hartmut Hotzel, Leiter des Servicezentrums für Computersysteme und Computerkommunikation der Bauhaus-Universität Weimar und Odej Kao, Chief Information Officer (CIO) der TU Berlin über die Chancen und Herausforderungen bei der Nutzung von kommerziellen oder föderierten Cloud-Diensten. „Cloud-Dienste sind heutzutage Standard. Gewinnen wir zusätzliche Bewerberinnen und Bewerber an einer Hochschule, wenn wir Cloudlösungen anbieten? Die Antwort ist Nein. Verlieren wir umgekehrt welche, wenn wir keine Cloud haben? Die Antwort ist ja", betonte Odej Kao. Er gab jedoch zu bedenken, dass es nicht ausschließlich um rein technische Fragen geht, sondern auch um betriebswirtschaftliche und rechtliche. Darum sei eine starke strategische Governance in den Universitäten und Hochschulen gefragt, um die Mitarbeiter bei der Umsetzung der Cloud-Lösungen zu unterstützen. Dass das Thema bei den Kanzlerinnen und Kanzlern präsent ist und diese vor schwierige Aufgaben stellt, zeigte die rege Beteiligung an der nachfolgenden Diskussion.

Die letzte Session bestritt die Forschungsstelle Recht im DFN. Ihre Vortragsthemen Reform des Urheberrechts, aktuelle Rechtsfragen, aus der Hochschulpraxis und arbeitsrechtliche Fragestellungen hatten die Kolleginnen und Kollegen aus Münster ganz auf die Bedarfe der Kanzlerinnen und Kanzler abgestimmt.

Das Schlusswort hatte Christian Zens, stellvertretender Vorstandsvorsitzender: „Auch die Kanzlerinnen und Kanzler sind wichtige Entscheider, wenn es um die Herausforderungen der Digitalisierung geht. Bleiben Sie am Ball, halten Sie engen Kontakt zu Ihrem Rechenzentrum und vor allem: Bringen Sie sich ein im DFN-Verein. Diese Solidargemeinschaft ist wichtig und nützt letztendlich uns allen." ◆

Sorgte für großes Interesse: die Podiumsdiskussion zu den Cloud-Services
Fotos auf dieser Seite © Maimona Id, Nina Bark / DFN-Verein

Intensive Gespräche und fachlicher Austausch: das DFN-Kanzlerforum macht es möglich



Nicht nur der Geist, auch der Magen kam auf seine Kosten

DFN Live: Wissen weitergeben, Erfahrungen teilen

Der DFN-Verein lebt von der Expertise und Erfahrung seiner Mitglieder und Nutzer des Deutschen Forschungsnetzes. Mit zahlreichen Veranstaltungen, Tutorien, Tagungen und Workshops bietet der DFN-Verein ein Forum für einen lebendigen Austausch und Wissenstransfer.

Mitgliederversammlung

Eine unserer Stärken ist das breite Mandat unserer Mitglieder. Mit über 300 institutionellen Mitgliedern engagiert sich die überwiegende Mehrzahl der deutschen Hochschulen und Forschungseinrichtungen sowie forschungsnaher Unternehmen der gewerblichen Wirtschaft im DFN-Verein. Auf der 75. Mitgliederversammlung am 5. und 6. Dezember 2017 im Wissenschaftszentrum Bonn, wählten die Vertreter der Mitgliedseinrichtungen einen neuen Verwaltungsrat. Im Anschluss bestimmte das dreizehnköpfige Gremium aus seinen Reihen den Vorstand für den DFN-Verein für die bis 2020 dauernde XII. Wahlperiode. Hierbei wurden Prof. Dr. Hans-Joachim Bungartz (TU München) als Vorstandsvorsitzender des DFN-Vereins und Dr. Rainer Bockholt (Universität Bonn) als stellvertretender Vorstandsvorsitzender bestätigt. Als weiterer stellvertretender Vorstandsvorsitzender wurde Christian Zens (Friedrich-Alexander-Universität Erlangen-Nürnberg) neu in den Vorstand gewählt, er ersetzt Dr. Ulrike Gutheil.

Dem Verwaltungsrat des DFN-Vereins werden außer den drei Vorstandsmitgliedern auch Prof. Dr. Gabi Dreo Rodosek (Universität der Bundeswehr München), Prof. Dr. Rainer W. Gerling (Max-Planck-Gesellschaft), Dr.-Ing. habil. Carlos Härtel (General Electric), Prof. Dr. Odej Kao (TU Berlin), Prof. Dr.-Ing. Ulrich Lang (Universität zu Köln), Prof. Dr. Joachim Mnich (DESY), Dr. Karl Molter (Hochschule Trier), Dr.-Ing. Christa Radloff (Universität Rostock), Prof. Dr.-Ing. Ramin Yahyapour (Universität Göttingen und GWDG) sowie Dr. Harald Ziegler (Friedrich-Schiller-Universität Jena) angehören.

Die Vertreter der Mitglieder treffen sich zweimal jährlich, um gemeinsam die Zukunft des DFN-Vereins zu gestalten. Nach der Eröffnung der Vorabendveranstaltung nahm der leitende Oberstaatsanwalt der Generalstaatsanwaltschaft Bamberg, Lukas Knorr, die Teilnehmer mit in die dubiose Welt des Cybercrime. Er berichtete über seine spannende Arbeit, über neue Möglichkeiten und die technischen sowie bürokratischen Hürden, die er und sein Team dabei überwinden müssen. Danach reisten wir mit

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

Dr. Moritz Helmstädter durch das menschliche Gehirn. Er zeigte, wie er mit seiner Karte des Denkens den Geheimnissen des Organs auf die Schliche kommen will. Ein gemeinsames Abendessen rundete den Abend ab.

TERMIN

Die nächste Mitgliederversammlung findet am **4./5. Juni 2018** in Berlin statt.

Betriebstagungen

Zur Unterstützung der Betriebsverantwortlichen in den Mitgliedseinrichtungen findet zweimal jährlich für je zwei Tage unsere Betriebstagung statt. Hier treffen sich mit Betriebsfragen beauftragte Mitarbeiterinnen und Mitarbeiter, Vertreter der Mitgliedsorganisationen und interessiertes Fachpublikum zum Erfahrungsaustausch und zur Weiterbildung. Dabei sollen Fragen rund um den Einsatz von DFN-Diensten beantwortet, die Netzverantwortlichen über neue Entwicklungen informiert und Einsteiger geschult werden.

Mit 280 Teilnehmerinnen und Teilnehmern gehörte die Frühjahrstagung zu einer der bisher am besten besuchten Betriebstagungen. Ob Neuigkeiten aus der DFN-Cloud oder Aktuelles zum Thema eduroam, die Entwicklungen der DFN-Dienste stießen in den einzelnen Foren auf großes Interesse. Aber auch einen Blick in die Vergangenheit bot die Tagung: anlässlich des 25-jährigen Jubiläums des DFN-CERT berichteten die CERTlinge ausführlich über ihre Tätigkeiten: von den Anfängen als eines der ersten Computer-Notfallteams in Deutschland bis zum heutigen hochspezialisierten Dienstleister für Sicherheit im Internet.

Seminaris CampusHotel Berlin *Foto © Nina Bark / DFN-Verein*

TERMIN

Die nächste DFN-Betriebstagung findet am **25./26. September 2018** im Seminaris CampusHotel Berlin statt.

Tagungsraum im Grand Elysée Hotel Hamburg *Foto © Nina Bark / DFN-Verein*

TERMIN

Die nächste DFN-Konferenz „Sicherheit in vernetzten Systemen“ findet am **6./7. Februar 2019** im Grand Elysée Hotel Hamburg statt.

25 Jahre DFN-Konferenz „Sicherheit in vernetzten Systemen“

Das DFN-CERT veranstaltet im Auftrag des DFN-Vereins seit mehr als 25 Jahren die DFN-Konferenz „Sicherheit in vernetzten Systemen“ im Grand Elysée Hotel Hamburg. Diese im Sicherheitsbereich etablierte Veranstaltung beinhaltet eine große Vielfalt an Beiträgen und Diskussionen zum Thema Informationssicherheit. Mit ihrer betont technischen und wissenschaftlichen Ausrichtung und im Schnitt 350 Teilnehmern hat sich die DFN-Konferenz als eine der größten deutschen Sicherheitstagungen etabliert.

Die Veranstaltung, die traditionell den Blick in die Zukunft richtet, startete anlässlich ihres Jubiläums in diesem Jahr mit einem kurzen Ausflug in die Vergangenheit und zeigte einmal mehr den rasant wachsenden Einfluss der Digitalisierung auf nahezu alle Bereiche der Gesellschaft. Wie wichtig die Gestaltung menschengerechter IT-Sicherheit dadurch in Zukunft wird, zeigte nicht nur die thematisch passende Keynote, auch in den weiteren Beiträgen kam das Thema zur Sprache.

Die Veranstaltung findet in den Tagungsräumen des Grand Elysée Hotel Hamburg statt

RA Dr. J. K. Köcher, DFN-CERT führte durch die Veranstaltung

Fotos © Nina Bark/DFN-Verein

DFN-Konferenz „Datenschutz“

Das Thema Datenschutz hat in den vergangenen Jahren zunehmend an Gewicht gewonnen. Im Auftrag des DFN-Vereins veranstaltet das DFN-CERT deshalb seit 2012 jährlich eine DFN-Konferenz „Datenschutz“. Mit der Veranstaltung kommt der DFN-Verein dem Bedarf von Forschungs- und Wissenschaftseinrichtungen an rechtlicher Unterstützung bei der praktischen Umsetzung von Datenschutz nach. Die DFN-Konferenz „Datenschutz“ richtet sich ausdrücklich, aber nicht ausschließlich an Hochschulen sowie Forschungs- und Wissenschaftseinrichtungen.

Am 28. und 29. November 2017 fand die 6. DFN-Konferenz „Datenschutz“ im Grand Elysée Hotel Hamburg statt. Die Konferenz mit 170 Teilnehmern stand dabei ganz im Zeichen der kommenden Veränderungen durch die EU-Datenschutzgrundverordnung, die ab dem 25.05.2018 in allen Mitgliedstaaten der Europäischen Union unmittelbar gelten wird.

TERMIN

Die 7. DFN-Konferenz „Datenschutz“ findet am **20./21. November 2018** im Grand Elysée Hotel Hamburg statt.

Aktuelle Informationen rund um das Deutsche Forschungsnetz und seine Veranstaltungen erhalten Sie auch regelmäßig in unserem Newsletter.
Den DFN-Newsletter können Sie unter **www.dfn.de** abonnieren.

Überblick DFN-Verein

(Stand: 06/2018)

Fotos © jackijack/fotolia

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

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

Die Geschäftsstellen

Geschäftsstelle Berlin (Sitz des Vereins)
DFN-Verein e. V.
Alexanderplatz 1
D-10178 Berlin
Telefon: +49 (0)30 884299-0

Geschäftsstelle Stuttgart
DFN-Verein e. V.
Lindenspürstraße 32
D-70176 Stuttgart
Telefon: +49 (0)711 63314-0

Die Organe

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

Verwaltungsrat
Der Verwaltungsrat beschließt alle wesentlichen Aktivitäten des Vereins, insbesondere die technisch-wissenschaftlichen Arbeiten und berät den Jahreswirtschaftsplan. Für die 12. Wahlperiode sind Mitglieder des Verwaltungsrates:

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

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

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

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

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

Prof. Dr. Odej Kao
(Technische Universität Berlin)

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

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

Dr. Karl Molter
(Hochschule Trier)

Dr.-Ing. Christa Radloff
(Universität Rostock)

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

Christian Zens
(Friedrich-Alexander-Universität Erlangen-Nürnberg)

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

Der Verwaltungsrat hat als ständige Gäste

einen Vertreter der Hochschulrektorenkonferenz:

Prof. Dr. Monika Gross
(Präsidentin der Beuth Hochschule für Technik Berlin)

einen Vertreter der Hochschulkanzler:

Christian Zens
(Kanzler der Friedrich-Alexander-Universität Erlangen-Nürnberg)

einen Vertreter der Kultusministerkonferenz:

Jürgen Grothe
(SMWK Dresden)

den Vorsitzenden der jeweils letzten Mitgliederversammlung:

Prof. Dr. Gerhard Peter
(Hochschule Heilbronn)

den Vorsitzenden des ZKI:

Hartmut Hotzel
(Bauhaus-Universität Weimar)

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

Prof. Dr. Hans-Joachim Bungartz
Vorsitz

Dr. Rainer Bockholt
Stellv. Vorsitzender

Christian Zens
Stellv. Vorsitzender

Der Vorstand wird beraten von einem Technologie-Ausschuss (TA), einem Betriebsausschuss (BA) und einem Ausschuss für Recht und Sicherheit (ARuS).

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

Die Mitgliedereinrichtungen

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	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
	Deutsche Telekom IT GmbH
	Deutsches Herzzentrum Berlin
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin (FUB)
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hochschule für Technik und Wirtschaft – University of Applied Sciences
	Hochschule für Wirtschaft und Recht
	Humboldt-Universität zu Berlin (HUB)
	International Psychoanalytic University Berlin
	IT-Dienstleistungszentrum
	Konrad-Zuse-Zentrum für Informationstechnik (ZIB)
	Museum für Naturkunde
	Robert Koch-Institut
	Stanford University in Berlin
	Stiftung Deutsches Historisches Museum
	Stiftung Preußischer Kulturbesitz
	Technische Universität Berlin (TUB)
	Umweltbundesamt
	Universität der Künste Berlin
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum Berlin für Sozialforschung gGmbH (WZB)
Biberach	Hochschule Biberach
Bielefeld	Fachhochschule Bielefeld
	Universität Bielefeld
Bingen	Technische Hochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Hochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Hochschule für Gesundheit
	Ruhr-Universität Bochum
	Technische Hochschule Georg Agricola
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern
	Bundesministerium für Umwelt, Naturschutz, Bau u. Reaktorsicherheit
	Deutsche Forschungsgemeinschaft (DFG)
	Deutscher Akademischer Austauschdienst e. V. (DAAD)
	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
	Deutsches Zentrum für Neurodegenerative Erkrankungen e. V.
	Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.
	ITZ Bund
	Rheinische Friedrich-Wilhelms-Universität Bonn
Borstel	FZB, 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	Technische Universität Clausthal-Zellerfeld
Coburg	Hochschule für angewandte Wissenschaften, Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus-Senftenberg
Darmstadt	Deutsche Telekom IT GmbH
	European Space Agency (ESA)
	Evangelische Hochschule Darmstadt
	GSI Helmholtzzentrum für Schwerionenforschung GmbH
	Hochschule Darmstadt
	Merck KGaA
	Technische Universität Darmstadt
Deggendorf	Technische Hochschule
Dortmund	Fachhochschule Dortmund
	Technische Universität Dortmund

Dresden	Evangelische Hochschule Dresden
	Helmholtz-Zentrum Dresden-Rossendorf e. V.
	Hannah-Arendt-Institut für Totalitarismusforschung e. V.
	Hochschule für Bildende Künste Dresden
	Hochschule für Technik und Wirtschaft
	Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden e. V.
	Leibniz-Institut für Polymerforschung Dresden e. V.
	Sächsische Landesbibliothek – Staats- und Universitätsbibliothek
	Technische Universität Dresden
Dummersdorf	Leibniz – Institut für Nutztierbiologie (FBN)
Düsseldorf	Hochschule Düsseldorf
	Heinrich-Heine-Universität Düsseldorf
	Information und Technik Nordrhein-Westfalen (IT.NRW)
	Kunstakademie Düsseldorf
	Robert-Schumann-Hochschule
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Hochschule Emden/Leer
Erfurt	Fachhochschule Erfurt
	Universität Erfurt
Erlangen	Friedrich-Alexander-Universität Erlangen-Nürnberg
Essen	RWI – Leibniz-Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Europa-Universität Flensburg
	Hochschule Flensburg
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Deutsche Nationalbibliothek
	Deutsches Institut für Internationale Pädagogische Forschung
	Frankfurt University of Applied Science
	Johann Wolfgang Goethe-Universität Frankfurt am Main
	Philosophisch-Theologische Hochschule St. Georgen e. V.
	Senckenberg Gesellschaft für Naturforschung
Frankfurt/O.	IHP GmbH – Institut für innovative Mikroelektronik
	Stiftung Europa-Universität Viadrina
Freiberg	Technische Universität Bergakademie Freiberg
Freiburg	Albert-Ludwigs-Universität Freiburg
	Evangelische Hochschule Freiburg
	Katholische Hochschule Freiburg
Freising	Hochschule Weihenstephan
Friedrichshafen	Zeppelin Universität gGmbH
Fulda	Hochschule Fulda
Furtwangen	Hochschule Furtwangen – Informatik, Technik, Wirtschaft, Medien
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH
	Leibniz-Rechenzentrum d. Bayerischen Akademie der Wissenschaften
Gatersleben	Leibniz-Institut für Pflanzengenetik und Kulturpflanzenforschung (IPK)
Geesthacht	Helmholtz-Zentrum Geesthacht Zentrum für Material- und Küstenforschung GmbH
Gelsenkirchen	Westfälische Hochschule
Gießen	Technische Hochschule Mittelhessen
	Justus-Liebig-Universität Gießen
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GwDG)
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	Ernst-Moritz-Arndt-Universität Greifswald
	Friedrich-Loeffler-Institut, Bundesforschungsinstitut für Tiergesundheit
Hagen	Fachhochschule Südwestfalen, Hochschule für Technik und Wirtschaft
	FernUniversität in Hagen
Halle/Saale	Leibniz-Institut für Wirtschaftsforschung Halle e. V.
	Martin-Luther-Universität Halle-Wittenberg
Hamburg	Bundesamt für Seeschifffahrt und Hydrographie
	Deutsches Elektronen-Synchrotron (DESY)
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	DFN – CERT Services GmbH
	HafenCity Universität Hamburg
	Helmut-Schmidt-Universität, Universität der Bundeswehr
	Hochschule für Angewandte Wissenschaften Hamburg
	Hochschule für Bildende Künste Hamburg
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg-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)
	NEC Laboratories Europe GmbH
	Ruprecht-Karls-Universität Heidelberg
Heilbronn	Hochschule für Technik, Wirtschaft und Informatik Heilbronn
Hildesheim	Hochschule für angewandte Wissenschaft und Kunst Fachhochschule Hildesheim/Holzminden/Göttingen
	Stiftung Universität Hildesheim
Hof	Hochschule für angewandte Wissenschaften Hof – FH
Idstein	Hochschule Fresenius gGmbH
Ilmenau	Technische Universität Ilmenau
Ingolstadt	DiZ – Zentrum für Hochschuldidaktik d. bayerischen Fachhochschulen
	Hochschule für angewandte Wissenschaften FH Ingolstadt
Jena	Ernst-Abbe-Hochschule Jena
	Friedrich-Schiller-Universität Jena
	Leibniz-Institut für Photonische Technologien e. V.

	Leibniz-Institut für Alternsforschung – Fritz-Lipmann-Institut e. V. (FLI)
Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Hochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	FIZ Karlsruhe - Leibnitz-Institut für Informationsinfrastruktur
	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
	Katholische Hochschule Mainz
	Universität Koblenz-Landau
Mannheim	Hochschule Mannheim
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	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 angewandte Wissenschaften München
	Hochschule für Philosophie München
	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e. V.
	Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt GmbH
	ifo Institut – Leibniz-Institut für Wirtschaftsforschung e. V.
	Katholische Stiftungshochschule München
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft
	Technische Universität München
	Universität der Bundeswehr München
Münster	Fachhochschule Münster
	Westfälische Wilhelms-Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neu-Ulm	Hochschule für Angewandte Wissenschaften, Fachhochschule Neu-Ulm
Nordhausen	Hochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
Nürtingen	Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen
Nuthetal	Deutsches Institut für Ernährungsforschung Potsdam-Rehbrücke
Oberwolfach	Mathematisches Forschungsinstitut Oberwolfach gGmbH
Offenbach/M.	Deutscher Wetterdienst (DWD)
Offenburg	Hochschule Offenburg
Oldenburg	Carl von Ossietzky Universität Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Bundesgesellschaft für Endlagerung mbH (BGE)
Pforzheim	Hochschule Pforzheim – Gestaltung, Technik, Wirtschaft und Recht
Potsdam	Fachhochschule Potsdam
	Helmholtz-Zentrum, Deutsches GeoForschungsZentrum – GFZ

	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam-Institut für Klimafolgenforschung (PIK)
	Universität Potsdam
Regensburg	Ostbayerische Technische Hochschule Regensburg
	Universität Regensburg
Reutlingen	Hochschule Reutlingen
Rosenheim	Hochschule für angewandte Wissenschaften – Fachhochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	Cispa Helmholtz-Zentrum i.G.
	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn Rhein-Sieg
Schenefeld	European X-Ray Free-Electron Laser Facility GmbH
Schmalkalden	Hochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Siegen	Universität Siegen
Sigmaringen	Hochschule Albstadt-Sigmaringen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Hochschule Stralsund
Stuttgart	Cisco Systems GmbH
	Duale Hochschule Baden-Württemberg
	Hochschule der Medien Stuttgart
	Hochschule für Technik Stuttgart
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte Tautenburg
Trier	Hochschule Trier
	Universität Trier
Tübingen	Eberhard Karls Universität Tübingen
	Leibniz-Institut für Wissensmedien
Ulm	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