Deutsches Forschungsnetz | DFN Mitteilungen Ausgabe 87 | November 2014
www.dfn.de

DFN Mitteilungen

DFNFernsprechen:
Neu aufgelegt!

Bibliothek 2.0:
Alles digital oder was?

Join the GÉANT Association!

Europas Netzwerkorganisationen DANTE und TERENA unter einem Dach vereint.

9 770177 689001

Impressum

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

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

ISSN 0177-6894

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

Fotonachweis:
Titelfoto © Jodi Jacobson/iStock
Seite 6/7 © Downunderphoto/fotolia
Seite 30/31 © zettberlin/photocase

Dr. Wolfgang A. Slaby
von 1985 bis 2013 Leiter des Universitätsrechenzentrums der Katholischen Universität Eichstätt-Ingolstadt und Mitglied des Verwaltungsrates des DFN-Vereins in seiner V., VI., VII. sowie in seiner IX. und X. Wahlperiode

Im Juni diesen Jahres haben sich die Mitglieder, Freunde und Mitarbeiter des Vereins zur Förderung eines Deutschen Forschungsnetzes zusammengefunden, um das 30-jährige Gründungsjubiläum ihres DFN-Vereins zu feiern. Mitstreiter aus verschiedenen Epochen kamen zusammen, um sich gemeinsam an Geschaffenes und Erlebtes zu erinnern und zugleich den Blick auf aktuelle und künftige Vorhaben und Herausforderungen zu richten. Neben dem Wiedersehen mit vielen Freunden und Kollegen und den gemeinsamen Erinnerungen war das Schönste an dieser Feier, dass 2014 - wieder einmal - ein äußerst ereignisreiches und produktives Jahr war, das reichlich Anlass bot, mehr über Künftiges zu sprechen denn über Vergangenes.

Gleich zu Beginn des Jahres hatte das DFN mit dem DFN-Terabit-Testbed erstmals die Terabit/s-Schwelle bei der Datenübertragung durchstoßen und damit die Weichen gestellt für eine technologische Weiterentwicklung der Netz-Plattform, die weit über dieses Jahrzehnt hinaus weisen wird. Zugleich wurde mit der Migration der optischen Plattform des DFN der Schritt in ein neues technisches Paradigma gewagt, das ein Vielfaches an Flexibilität und Leistungsskalierung im Wissenschaftsnetz ermöglicht.

Parallel dazu stand die Föderierung von Diensten auf der Agenda des DFN. Was in den vergangenen Monaten unter dem Stichwort DFN-Cloud in der Community diskutiert wurde, ist nichts anderes als die Möglichkeit zur gegenseitigen Erbringung von Diensten innerhalb der Gemeinschaft der DFN-Mitglieder und -Nutzer. Der DFN-Verein hat in diesem Zusammenhang wieder einmal seine besondere Fähigkeit unter Beweis gestellt, Gemeinschaft zu bilden und die Interessen seiner Mitglieder dort zu bündeln, wo ohne den DFN-Verein kein gemeinsames Wirken möglich gewesen wäre.

Auf der kommenden Mitgliederversammlung am 3. Dezember 2014 geht der Verwaltungsrat in seine XI. Wahlperiode. Einige Verwaltungsratsmitglieder – mich eingeschlossen – werden in der nächsten Wahlperiode nicht mehr zur Verfügung stehen und den Platz frei machen für neue Kräfte. Andere können erneut kandidieren und werden möglicherweise für weitere drei Jahre in ihrem Amt bestätigt. Ich möchte mich an dieser Stelle im Namen aller Mitglieder des aktuellen Verwaltungsrates für das Vertrauen bedanken, dass uns die Mitglieder des DFN-Vereins in der zurückliegenden Wahlperiode geschenkt haben.

Zugleich möchte ich allen Mitgliedern danken, die sich im DFN-Verein engagiert haben und jene Anwender, die bislang auf eine Mitgliedschaft verzichtet haben, ermutigen, ebenfalls im DFN-Verein aktiv zu werden. Selten wird Mitarbeit durch so viele Erfolge belohnt wie hier. Denn so, wie mit jedem Nutzer der Nutzen eines Wissenschaftsnetzes wächst, so wächst die Innovationskraft des DFN und der Gewinn der Wissenschaft insgesamt durch die aktive Mitarbeit in unserer Community.


















Unsere Autoren dieser Ausgabe im Überblick

1 Christian Meyer, DFN-Verein (hoelzner@dfn.de); **2** Bettina Kauth, DFN-Verein (kauth@dfn.de); **3** Dr. Malte Armbruster, DFN-Verein (armbruster@dfn.de); **4** Florian Eilers, DFN-Verein (eilers@dfn.de); **5** Gerrit Gragert, Staatsbibliothek zu Berlin (gerrit.gragert@sbb.spk-berlin.de); **6** Wolfgang Pempe, DFN-Verein (pempe@dfn.de); **7** Kai Hoelzner, DFN-Verein (hoelzner@dfn.de); **8** Dr. Leonie Schäfer, DFN-Verein (schaefer@dfn.de); **9** Kennedy Aseda, KENET (kaseda@kenet.or.ke); **10** Felix von Eye, Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften (felix.voneye@lrz.de); **11** Dr. Wolfgang Hommel, LRZ (wolfgang.hommel@lrz.de); **12** Prof. Dr. Helmut Reiser, LRZ (helmut.reiser@lrz.de); **13** Prof. Dr. Marcel Waldvogel, Universität Konstanz (marcel.waldvogel@uni-konstanz.de); **14** Jürgen Kollek, Universität Konstanz (juergen.kollek@uni-konstanz.de); **15** Dr. Ralf Gröper, DFN-Verein (groeper@dfn.de); **16** Jürgen Brauckmann, DFN-CERT (brauckmann@dfn-cert.de); **17** Dr. Dankmar Lauter, DFN-CERT (lauter@dfn-cert.de); **18** Philipp Roos, Forschungsstelle Recht im DFN (recht@dfn.de); **19** Florian Klein, Forschungsstelle Recht im DFN (recht@dfn.de)

Inhalt

Wissenschaftsnetz

International

Campus

Sicherheit

Recht

DFN-Verein

Wissenschaftsnetz

DFNFernsprechen: Neu aufgelegt!

Ab kommenden Jahr wird DFNFernsprechen für die Nutzer in neuem Gewand angeboten. Mit VoIP-Centrex, einem zukünftig noch verbessertem Angebot für pauschaliertes Abrechnen und einer Reihe von handlicheren und leistungsfähigen Dienstmodulen unterstützt der DFN-Verein die Anwender beim Aufbau einer maßgeschneiderten und leicht zu verwaltenden Kommunikationsinfrastruktur in ihren Einrichtungen.

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

Foto: © Eli K Hayasaka

Neue Dienste für DFNFernsprechen

Die Entwicklung der rechnergestützten Informations- und Kommunikationssysteme wird von der Idee einer Konvergenz bisher unterschiedlicher Kommunikationssysteme und -netze bestimmt (Datennetze, Fernsprechnetze, Mobilfunknetze usw.). Als ein wichtiger Integrationsfaktor erscheint dabei das Internetprotokoll, weil es global verbreitet ist und – zumindest prinzipiell – in allen Netzen und für nahezu alle Dienste und Anwendungen genutzt werden kann.

Als Enabler von netzgestützten F&L-Prozessen bietet der DFN-Verein den Anwendern im Wissenschaftsnetz mit DFNFernsprechen einen Dienst an, der klassische Telefonie und Voice-over-IP-Lösungen vereint und entsprechende Übergänge zwischen beiden Technologien ermöglicht.

Innerhalb seines Fernsprechdienstes hat der DFN-Verein eine europaweite Ausschreibung seines Dienstangebotes durchgeführt und im August dieses Jahres per Zuschlagserteilung erfolgreich beendet. Ziel war es, innovative Entwicklungen in den Dienst zu integrieren und die Konvergenz von Daten- und Sprachdiensten weiter voranzutreiben. Gegenstand der Ausschreibung war an erster Stelle die Telefonie aus dem Festnetz über IP-basierte Netze und klassische ISDN- bzw. analoge Anschlüsse, wobei an die IP-basierte Kommunikation (sog. Voice-over-IP, kurz VoIP) im Vergleich zum bisherigen Dienstangebot höhere Anforderungen gestellt wurden, da hiermit auch das höhere Innovationspotential erschlossen wird. Die klassische leitungsvermittelte Telefonie über ISDN oder analoge Leitungen wird als etabliertes Kommunikationsmedium weiterhin unverändert im Fernsprechdienst angeboten.

Sowohl die paketvermittelte VoIP-Telefonie als auch die leitungsvermittelte klassische Telefonie erforderten bisher immer den Betrieb einer Telekommunikationsanlage (kurz TK-Anlage) auf Seite der Teilnehmer. Oftmals scheuen kleine und mittelgroße Einrichtungen diesen Eigenbetrieb aber, sei es aus Budgetgründen oder Personalgründen, und versuchen als Mitnutzer bei Partnereinrichtungen den TK-Betrieb auszulagern. Künftig wird hierfür ein neues Dienstmodul VoIP-Centrex angeboten, welches ein umfangreiches Angebot von Funktionalitäten moderner VoIP-Telefonanlagen in das Wissenschaftsnetz integriert. Dabei soll auch schrittweise das große Potential an zusätzlichen Funktionalitäten und Innovationen einer solchen Integration ausgeschöpft werden. Teilnehmer des VoIP-Centrex-Dienstes können nicht nur auf ihre lokalen Telefonanlage zurückgreifen, sondern profitieren auch von künftigen Innovationen in der VoIP-Technologie und genießen dank der doppelten Anbindung der VoIP-Centrex-Plattform an das Wissenschaftsnetz eine weitaus höhere Verfügbarkeit als herkömmliche ISDN-Anlagen.

Als weiteres Dienstmodul bietet DFNFernsprechen neben VoIP-Centrex künftig auch ein SMS-Gateway. Eine nicht geringe Anzahl von Einrichtungen nutzen SMS-Nachrichten für die Abwicklung ihrer Arbeitsprozesse. An erster Stelle sind hier Bibliotheken zu nennen, die Nutzer z. B. über fällige Medien oder abgelaufene Leihfristen informieren müssen. Aber auch im Campus-Management oder in der IT-Überwachung kann der Einsatz von SMS-Benachrichtigungen sinnvoll sein. Speziell für diese Anwender bietet DFNFernsprechen in seiner künftigen Gestalt einen SMS-Gateway-Dienst, der ermöglicht, E-Mail-Textnachrichten als SMS über ein Mobilfunknetz zu versenden.

Die vierte Säule des Dienstes DFNFernsprechen stellt ein auf die Bedürfnisse von Hochschulen und Forschungseinrichtungen zugeschnittener Mobilfunkrahmenvertrag dar, der es teilnehmenden Einrichtungen erlaubt, für die Wissenschaft maß-

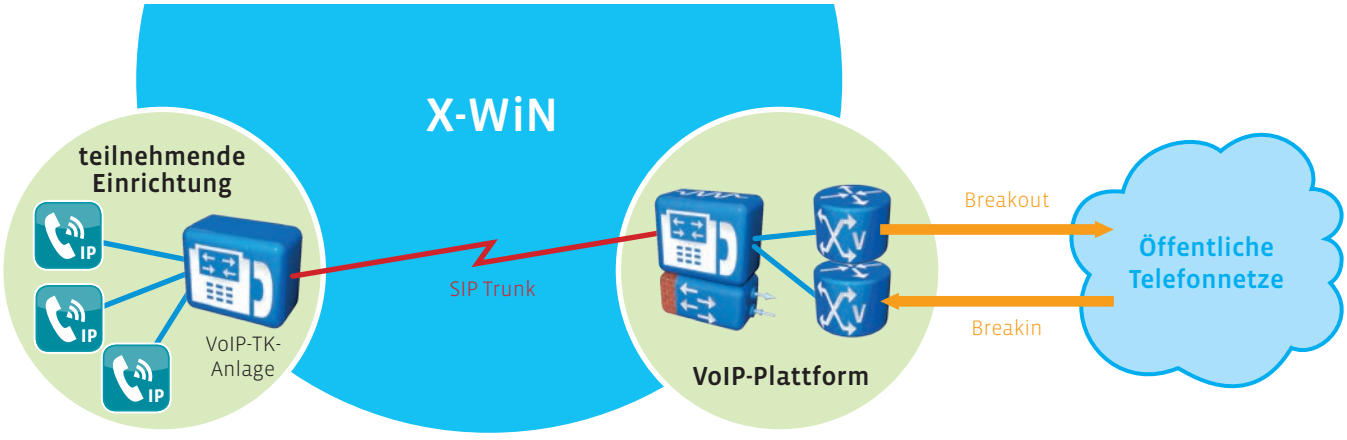


Abbildung 1: Die VoIP-TK-Anlage einer teilnehmenden Einrichtung wird über einen SIP-Trunk mit der VoIP-Plattform verbunden.

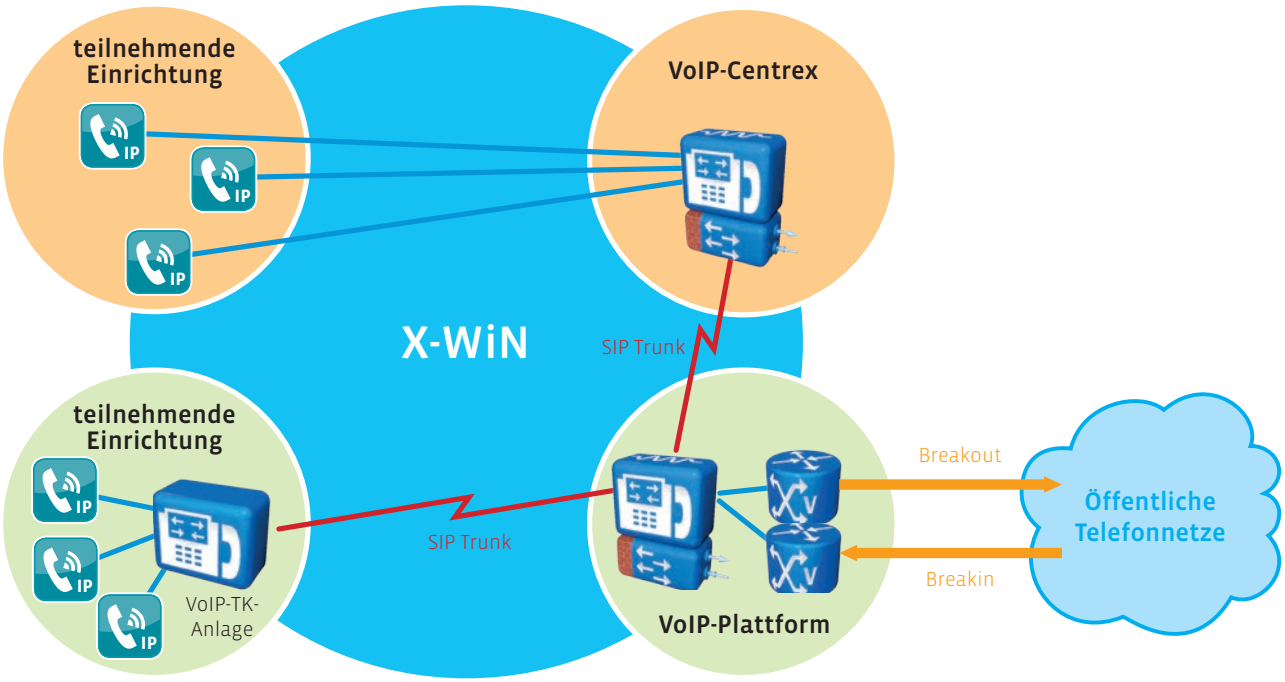


Abbildung 2: Teilnehmende Einrichtungen müssen keine VoIP-TK-Anlage betreiben. Die Endgeräte der am VoIP-Centrex-Dienst teilnehmenden Einrichtungen verbinden sich direkt mit der VoIP-Centrex-Plattform, welche wiederum über einen SIP-Trunk mit dem öffentlichen Telefonnetz verbunden ist.

geschneiderte Verträge zur Nutzung von mobiler Sprach-, Nachrichten- und Datenübertragung einzugehen.

Telefonie aus dem Festnetz

Im Fernsprechdienst des DFN-Vereins wird es weiterhin die Möglichkeit geben, klassische Anschlüsse mit dem bisherigen Funktionsspektrum zu beauftragen. Dazu gehören analoge Anschlüsse, ISDN-Basisanschlüsse sowie ISDN-Primärmultiplexanschlüsse. In der VoIP-Telefonie konnten wichtige infrastrukturelle und qualitative Verbesserungen umgesetzt werden.

Einrichtungen, die eine eigene VoIP-TK-Anlage betreiben möchten oder bereits betreiben, können dies auch weiterhin tun. Zwischen solchen Teilnehmer-TK-Anlagen und der zentralen VoIP-Plattform im X-WiN wird ein sogenannter SIP-Trunk aufgebaut, um die Konnektivität in das öffentliche Telefonnetz herzustellen (vgl. Abbildung 1). Die Kommunikation über einen SIP-Trunk kann bei Bedarf auch verschlüsselt werden. Das Verschlüsselungskonzept sieht dabei vor, dass die Signalisierung einer Verbindung zertifikatbasiert per Transport Layer Security (TLS) verschlüsselt und der eigentliche Medienstrom mit dem Secure Real-Time Transport Protocol (SRTP) verschlüsselt werden.

Die VoIP-Plattform ist die zentrale Komponente des VoIP-Dienstes und dient der Vermittlung der IP-basierten Kommunikation innerhalb der teilnehmenden Einrichtungen und durch Gateways auch in alle öffentlichen Telefonnetze. In Zukunft wird hier ein optimiertes Redundanzkonzept eingesetzt. Die VoIP-Plattform ist nun an zwei Standorten (Frankfurt und Hannover) mit jeweils zwei trassendisjunkten redundanten Zugangsleitungen in das Wissenschaftsnetz eingebunden. Darüber hinaus ist die Infrastruktur an jedem Standort ebenfalls redundant aufgebaut. Mit diesen Maßnahmen wird eine den Anforderungen der Wissenschaft entsprechende Ausfallsicherheit gewährleistet.

Zur Vermeidung von Angriffen auf VoIP-TK-Anlagen und zur Minimierung der Auswirkungen von Toll-Fraud-Vorfällen (Gebührenbetrug) wird ein sogenanntes Fraud Detection and Prevention System in die VoIP-Plattform integriert. Damit ist eine nahezu in Echtzeit wirkende Betrugserkennung aktiv, die Vorfälle dieser Art sowohl über dynamisch selbstlernendes Monitoring als auch über Blacklisting schon in der frühen Wirkphase erkennen und unterbinden kann. Das System nutzt dabei verschiedene Metriken, um grundlegende Attribute wie Gesprächsdauer, Tageszeit, simultan hergestellte Verbindungen, ungewöhnliche Rufziele oder ungewöhnliche Quell-IP-Adressen zu messen.

Weitere Fortschritte konnten auch in der über VoIP erreichbaren Übertragungsqualität erreicht werden. So kann neben den Sprach-Codecs G.711 und G.729 nun auch

der breitbandige Sprach-Codec G.722 verwendet werden.

Die Ergebnisse der Ausschreibung haben auch den Raum für zukünftige Innovationen geschaffen, um den Dienst DFNFernsprechen immer dem aktuellen Stand der Technik anzupassen. Eine erste Weiterentwicklung wird die Integration von Video in die VoIP-Plattform sein, um auf den SIP-Trunks zusätzlich zur Sprachübertragung auch die Videoübertragung zu ermöglichen.

VoIP-Centrex

Der DFN-Verein bietet mit dem Dienst VoIP-Centrex die Möglichkeit, alle Funktionen einer VoIP-TK-Anlage zu nutzen, ohne selbst eine Anlage dafür betreiben zu müssen. Teilnehmer benötigen hierfür lediglich entsprechende VoIP-Endgeräte. Diese Endgeräte benötigen einen Zugang zum Wissenschaftsnetz und werden bei Erstnutzung automatisch provisioniert, indem die Geräte an der VoIP-Centrex-Plattform registriert und aktiviert werden. Jedes angeschlossene Endgerät wird als ein aktiver Port gezählt und in einem monatlichen Portpreis abgerechnet.

Wie in Abbildung 2 dargestellt, wird die VoIP-Centrex-Plattform per SIP-Trunking mit der zentralen VoIP-Plattform verbunden, um die Konnektivität innerhalb des Forschungsnetzes als auch in die öffentlichen Telefonnetze sicherzustellen. Dieser SIP-Trunk ist gesichert, alle Verbindungen werden TLS/SRTP verschlüsselt. Auch die Verbindung der Endgeräte mit der VoIP-Centrex-Plattform erfolgt mit dieser Verschlüsselung. Die Infrastruktur der VoIP-Centrex-Plattform wird redundant an zwei Standorten betrieben und ist über zwei Kernnetzknoten an das Wissenschaftsnetz angebunden.

Die Verwaltung der Endgeräte erfolgt über eine Webschnittstelle. Hier können alle Endgeräte und Nebenstellen administriert, neue Endgeräte eingetragen oder alte ausgetragen, Rufnummern zugewiesen und zentrale Adressbücher gepflegt werden. Jede Nebenstelle kann zusätzlich noch durch den entsprechenden Nutzer verwaltet werden, um beispielsweise Voicemail einzurichten, Rufumleitungen zu konfigurieren oder nutzerspezifische Adressbücher zu pflegen.

SMS-Gateway

Der zweite durch die Ausschreibung neu organisierte Dienst ist ein SMS-Gateway. Teilnehmende Einrichtungen können Nutzer per Mobilfunk-SMS erreichen, indem die gewünschte Textnachricht per E-Mail an das SMS-Gateway geschickt wird. Das SMS-Gateway nimmt die E-Mail entgegen, wandelt sie nach Prüfung der Nutzungsberechtigung in das SMS-Format um, wobei die Rufnummer des Empfängers aus der Betreffzeile der E-Mail entnommen wird, und sendet sie in das Mobilfunknetz der Empfängernummer. Das SMS-Gateway nimmt dabei auch Quittungs- und Fehlermeldungen aus dem Mobilfunknetz entgegen und leitet sie an den E-Mail-Absender weiter. ◆

Fazit

Durch die Konvergenzstrategie des DFN-Vereins im Bereich der Kommunikationsnetze und die damit einhergehende Vereinfachung der Organisationsprozesse, profitieren alle Teilnehmer des DFNFernsprechdienstes und zwar sowohl von den Möglichkeiten einer Konvergenz von Sprach- und Datendiensten als auch von verbesserten wirtschaftlichen Konditionen. So wird auch weiterhin die DFN-interne Telefonie und somit alle Verbindungen zwischen Anschlüssen des Dienstes DFNFernsprechen und allen Anschlüssen innerhalb des Mobilfunkrahmenvertrages entgeltfrei sein.

X-WiN – maßgeschneidert

Text: **Bettina Kauth** (DFN-Verein)

Foto: © emanoo / photocase.de

Der DFN-Verein bietet neben dem Anschluss an die IP-Infrastruktur des X-WiNs auch ein breites Spektrum von VPN-Lösungen an, um damit dem Bedarf verteilter Organisationen oder Netzverbünden nach exklusiv nutzbaren Weitverkehrs-Infrastrukturen zu entsprechen.

Generell werden zwei Typen von Virtuellen Privaten Netzen (VPNs) nachgefragt: Zum einen Punkt-zu-Punkt Verbindungen zwischen Standorten, zum anderen Infrastrukturen, die den Zusammenschluss mehrerer verteilter Standorte erlauben. Mögliche Lösungen können entweder auf der Optischen- oder auf der Routing-Infrastruktur des X-WiNs umgesetzt werden.

Allen im folgenden beschriebenen Lösungen ist gemein, dass sie in das Monitoring- und Servicekonzept des DFNs eingebunden sind. So sind alle Typen von VPN-Anschlüssen und Infrastrukturen in die 24x7-Monitoring und Entstörungsbehandlung integriert und profitieren vom Klima, Strom und Standort-Management an den DFN-Kernnetzstandorten.

Optische VPN

Schon seit langem gehört die Bereitstellung exklusiver physikalischer Links und Wellenlängen für die Verbindung zwischen Einrichtungen zum Portfolio des DFN-Vereins. In früheren Netzgenerationen waren solche Lösungen jedoch mit erheblichen Kosten und technischen Beschränkungen verbunden. Seit der DFN-Verein die optische Plattform des X-WiNs selbst betreibt, ergeben sich flexible und insbesondere auch wirtschaftliche Lösungen zum Aufbau optischer VPNs. Neben Punkt-zu-Punkt-Verbindungen zwischen zwei Standorten ist die Implementierung beliebig komplexer Topologien zwischen mehreren Standorten möglich. Dabei können Link-Bandbreiten von einem , zehn oder hundert Gigabit pro Sekunde umgesetzt werden. Die Zugangsleitungen der Anwender terminieren an vom DFN-Verein betriebenen Wellenlängen-Multiplexern in den jeweils nächstgelegenen Kernnetzstandorten. Die implementierte Topologie steht den Nutzern eines optischen VPNs exklusiv zur Verfügung. Diese Exklusivität bringt verschiedene Vorteile mit sich, z. B. sind optische VPNs komplett aus dem globalen Internet losgelöst. Allerdings erfordern sie auch eine gute Planung hinsichtlich benötigter Kapazitäten und eine Bewertung der Ausfallsicherheit der Komponenten (Multiplexer und Links). Auf dem optischen Layer können die Pfade im VPN mit Protection versehen werden.

Die optischen VPNs stellen einen nicht unerheblichen Teil der Nutzung der optischen Plattform des Wissenschaftsnetzes dar. So sind neben den 148 Kernnetz-Verbindungen, die für die IP-Plattform des X-WiNs eingesetzt werden, noch einmal 61 Verbindungen für Virtuelle Private Netze geschaltet. Große nationale VPNs wie das des Deutschen Wetterdienstes verfügen dabei über eine Vielzahl von Standorten, die über ganz Deutschland verteilt und mit Gigabit-Kapazität untereinander verbunden sind.

MPLS basierte VPN

Neben optischen VPNs bietet der DFN-Verein auch Lösungen an, die über die Routing-Infrastruktur des Wissenschaftsnetzes realisiert werden. Diese basieren auf IP/MPLS (Multiprotocol LabelSwitching). Der MPLS-Layer wird hierbei aber nur im X-WIN-Backbone benötigt und muss nicht in den Anwendernetzen implementiert werden. Der VPN-Verkehr nutzt in aller Regel die Links des IP-Backbones, wobei die Switching-Pfade analog zu den IP-Routing-Pfaden verlaufen. Kommt es zu Ausfällen von Kernnetzkomponenten wie Links oder Routern, wird ein Pfad automatisch neu berechnet. Damit

profitieren die IP/MPLS-basierten Lösungen von der redundanten Auslegung des X-WiN-Backbones und von den dort vorhandenen Link-Kapazitäten. Anwender können ihre schon vorhandenen Zugangsleitungen an das X-WiN für die Implementierung von VPN-Lösungen nutzen. Dies erfolgt über die Definition von virtuellen LANs (VLANs), die eine Zuordnung des Verkehrs zum jeweiligen Dienst ermöglichen. Die auf dem Anwenderlink insgesamt verfügbare Bandbreite kann den VLANs entweder explizit zugeteilt werden, oder sie nutzen die vorhandene Bandbreite gemeinsam. Damit sind die MPLS basierten VPNs mit vergleichsweise geringem Aufwand zu implementieren.

Natürlich ist es auch möglich, eine dedizierte Zugangsleitung für den VPN-Anschluss zu schalten. Anschlüsse, die einem VPN zugeordnet sind, sind aus dem globalen Routing nicht mehr erreichbar und somit vor äußeren Angriffen, etwa in Form von DoS- oder Intrusion-Attacken geschützt. Im X-WiN können mittels IP/MPLS Layer-2-basierte Punkt-zu-Punkt Verbindungen (L2VC) oder virtuelle Routing-Infrastrukturen (VRF) aufgebaut werden.

Layer2 Virtual Circuit (L2VC)

Ein Layer2 Virtual Circuit (L2VC) wird klassischerweise eingerichtet, wenn eine Punkt-zu-Punkt Verbindung zwischen zwei Standorten benötigt wird. So wurde für die TU Chemnitz zur Unterstützung eines Projektes mit „E-Plus“ ein L2VC zwischen der TU Chemnitz und der TU Braunschweig bereitgestellt. Der Anwender erhält eine Layer-2 Schnittstelle, die sich wie eine LAN Schnittstelle verhält. Allerdings gibt es auch Anwendungsbeispiele, bei denen über L2VC eine komplexere Infrastruktur aufgebaut wird, weil die Anwender die L2-Funktionalität benötigen.

Layer3 VPN:

Bei einem Layer3 VPN (L3VPN) erhalten die Teilnehmer einen Anschluss an eine IP-Infrastruktur. Dabei wird innerhalb des X-WiNs eine Virtual Routing and Forwarding Instanz (VRF) definiert, die die Routinginformation für dieses L3VPN enthält und keinen Übergang zu der globalen X-WiN-Routingtable hat. L3VPN-Routen werden also einzig in dieser VRF-Instanz gehalten und sind vom globalen Routing losgelöst. Damit ist es den angeschlossenen Einrichtungen möglich, auch Adressbereiche aus dem privaten Adressraum (RFC 1918) in ihrer VRF zu verteilen. Der Austausch der Routinginformation zwischen Anwender und VRF erfolgt per Border Gateway Protocol (BGP) zwischen dem Anwender und dem X-WiN-Router, an dem die Anschlussleitung mündet. Das Verteilen der Routinginformation erfolgt über die X-WiN-VRF-Konfiguration und ist für den Teilnehmer transparent. Dabei werden auch IPv4/IPv6 dual-stack Lösungen unterstützt.

L3VPNs werden häufig von Organisationen mit räumlich weit verteilten Instituten genutzt, wie z. B. der Fraunhofer-Gesellschaft oder dem Deutschen Zentrum für Neurodegenerative Erkrankungen (DZNE).

Hybride aus Optik und MPLS

Im X-WiN haben sich auch einige „hybride“ VPN-Strukturen herausgebildet, bei denen optische und MPLS-basierte VPNs miteinander kombiniert werden. So wurde für das VPN-Netz des LOFAR-Radiointerferometers, das eine Vielzahl von Antennenfeldern in den Niederlanden und in Deutschland sowie in Frankreich, Großbritannien und in Schweden zu einem riesigen virtuellen Radioteleskop zusammenschaltet, im X-WIN eine Infrastruktur aus optischen Kanälen und L2VC implementiert.

Das wohl bekannteste L3VPN in der Wissenschaft dürfte derzeit das „LHCONE“ für den Large Hadron Collider am Genfer CERN sein, das sich über ganz Europa bis in die USA und nach Ost-Asien erstreckt. Innerhalb des X-WiNs nutzt dieses VPN dedizierte optische 10-Gigabit-Ethernet-Verbindungen, die einen virtuellen Backbone zwischen dem Karlsruher Institut für Technologie (KIT), der Darmstädter Gesellschaft für Schwerionenforschung (GSI), dem Deutschen Elektronen-Synchrotron (DESY), der RWTH-Aachen und der Universität Wuppertal aufspannen und auf den X-WiN Routern terminieren und dort als L3VPN implementiert sind. Für die internationale Anbindung wird die Anbindung des X-WiN an den europäischen Forschungsbackbone GÉANT genutzt.

Internationale VPNs

In der Regel haben alle Teilnehmer eines VPNs einen Anschluss an das X-WiN. Wie aber schon das Beispiel LHCONE zeigt, gibt es vermehrt internationale Kooperationen in der Wissenschaft, die ebenfalls einen Bedarf an VPNs haben. Um dies weiter zu unterstützen, war der DFN-Verein maßgeblich an der Entwicklung eines europäischen Multi-Domain-VPN-Dienstes (MD-VPN) im Rahmen des europäischen Forschungsbackbones GÉANT beteiligt. Bereits mehr als die Hälfte der europäische Forschungsnetze nehmen an dem Dienst, der es ermöglicht, MPLS-basierte VPN-Lösungen zwischen Instituten mit Anschluss an unterschiedliche europäische Forschungsnetze zu etablieren, teil. ◆

Fazit

Die Implementierungen im X-WiN sind so heterogen wie die Anforderungen, die die Anwender stellen. Deshalb gibt es *den* VPN-Dienst nicht, sondern immer nur individuelle Lösungen, die der DFN-Verein gemeinsam mit den Anwendern entwickelt. Dabei werden neben den technischen Anforderungen die administrativen Möglichkeiten und natürlich auch die finanziellen Rahmenbedingungen der Nutzer berücksichtigt.

DFN-Portale als Mittelpunkt des Dienstnutzungs-Lifecycles

Seit Herbst 2013 steht den Anwendern des DFN-MailSupport-Dienstes das DFN-Mail-Support-Dienst-Portal im Pilotbetrieb zur Verfügung. Damit markiert der DFN-Verein den Beginn einer Umstellung seiner bisherigen heterogenen Dienst-Portale in ein neues homogenes Portal-Konzept

Text: **Dr. Malte Armbruster** (DFN-Verein), **Florian Eilers** (DFN-Verein)

Foto: © Christian Lagereek

Dienst- und Konfigurationsportale des DFN

Unter „Portal“ wird eine bidirektionale Daten-Schnittstelle zwischen den administrativen Domänen des DFN-Vereins und seiner Anwender für die Durchführung von verteilten F&L-Prozessen verstanden. Mit dieser Definition beschränken sich Portale nicht nur auf die F&L-Prozesse zu einzelnen DFN-Diensten oder einer bestimmten technischen Realisierung (z. B. als www-Seite), sondern können ein genereller Ansatz zur Durchführung von F&L-Prozessen sein.

Im DFN-Verein werden seit langem bereits für mehrere Dienste Teile der oben genannten Funktionen in Portalen umgesetzt. Es zeigt sich, dass die Portale von den Anwendern und Nutzern gut angenommen werden und zur Integration der Dienste in die F&L-Prozesse der Anwender einen sehr wertvollen Beitrag leisten. Insgesamt ist festzustellen, dass hier aus dem konkreten Bedarf heraus schon mehrere Portale entstanden sind.

Die bereits heute realisierten Portale zu Diensten des DFN sind häufig als www-Seiten implementiert, die funktional auf bestimmte F&L-Prozesse der Anwender mit dem DFN (zum Beispiel die Suche nach dem nächsten eduroam-Hotspot) ausgeprägt sind und in denen ein bidirektionaler und ggf. auch zeitnah zu verarbeitender Fluss von Daten möglich ist. Aufgrund eines fehlenden gemeinsamen konzeptionellen Rahmens aber unterscheiden sich die heutigen Portale voneinander u. a. im Informationsgehalt, in der Benutzungsstrategie und im Leistungsumfang. Auch fehlte bislang eine einheitliche Strategie zur Abgrenzung des Informationsinhaltes von Portalen zu den allgemeinen Inhalten unter www.dfn.de.

Um die Heterogenität der bestehenden Portal-Landschaft im DFN-Verein zu verringern und eine Konvergenz auf informationeller und funktionaler Ebene zu befördern, arbeitet der DFN-Verein derzeit an einer grundlegenden Revision seiner Portale. Ziel ist es, mittels einer intuitiven Nutzerführung und eines prozessorientierten Gestaltungskonzeptes ein möglichst hohes Maß an Benutzbarkeit zur Verfügung zu stellen. Bevor nun allerdings konkret auf die Umsetzung der Portale eingegangen wird, soll das der Architektur der Portale zugrunde liegende Konzept des „Lifecycle“-Gedankens erläutert werden.

Das Lifecycle-Konzept

Beim Lifecycle-Konzept steht die Überlegung im Mittelpunkt, dass jede Dienstnutzung in vier distinkt voneinander zu unterscheidende Phasen unterteilt werden kann und der DFN-Verein seinen Anwendern in allen diesen Phasen unterstützend zur Seite steht. Die vier Phasen sind wie folgt aufgeteilt:

1. Informieren – ein Anwender möchte sich über einen bestimmten Dienst informieren um herauszufinden, ob die Nutzung dessen von Vorteil sein könnte.
2. Aktivieren – ein Anwender möchte einen Dienst für sich nutzbar machen, entscheidet sich also für die Aktivierung des Dienstes.
3. Nutzen – ein Anwender nutzt den Dienst und muss ihn gegebenenfalls an seine individuellen Bedürfnisse anpassen (i.e. Konfigurationsmöglichkeit).
4. Beenden – der Anwender möchte den Dienst nicht weiter in Anspruch nehmen und dementsprechend die Dienstnutzung beenden.

In jeder der vier Phasen entstehen unterschiedliche Bedürfnisse des Anwenders, denen sich der Dienstanbieter annehmen muss. So entstehen in der ersten Phase häufig Fragen wie „was genau bietet dieser Dienst?“, „was kostet mich die Nutzung?“, „gibt es besondere Nutzungsrichtlinien?“, „kann ich den Dienst zunächst testen?“. In der zweiten Phase stehen hingegen Fragen zur Installation und gegebenenfalls notwendigen Umstellung bestehender Infrastrukturen im Mittelpunkt. In der dritten Phase sollen dann eventuell notwendige Konfigurationen angepasst oder durch die Dienstaktivierung bereitgestellte Inhalte abgerufen werden können. In der abschließenden Phase dann müssen vertragliche und technische Fragen zu der Beendigung des Dienstes beantwortet werden. Ebenfalls soll der Anwender bei der Umstellung unterstützt werden, da eventuell diverse System-Konfigurationen wieder angepasst werden müssen.

Dem DFN-Verein ist es hierbei ein wichtiges Anliegen, seinen Anwendern in allen vier Phasen bestmöglich zur Seite zu stehen und sie so gut wie möglich zu unterstützen. Auch bei der bei anderen Dienstanbietern gerne vernachlässigten vierten Phase sollen sich die Anwender der DFN-Dienste nicht „im Stich“ gelassen fühlen, sondern ebenfalls sorgfältig unterstützt werden.

Dieses Modell der Aufteilung einer Dienstnutzung in vier Phasen liegt der Architektur der DFN-Portale zugrunde. Die vom DFN-Verein entwickelten Portale sollen also eine erste Anlaufstelle darstellen, die den Anwender in seiner jeweiligen Nutzungsphase abholen und ihm dabei assistieren, die für ihn aktuell anstehenden Fragen zu klären und Bedürfnisse zu bedienen.

Zusätzlich bieten Portale insbesondere bei Diensten mit großem individuellen Konfigurationsbedarf – wie dem DFN-MailSupport-Dienst – sowohl für den DFN-Verein als Anbieter eines Dienstes als auch für den Anwender mehrere Vorteile.

Vorteile der Portale

Ein sofort offensichtlicher Vorteil eines Portals zur Konfiguration eines Dienstes liegt sicherlich in der grundsätzlich ständigen Erreichbarkeit des selbigen. Völlig losgelöst von der Erreichbarkeit der Mitarbeiter des DFN-Vereins kann sich der autorisierte Anwender zu jeder Tages- und Nachtzeit am Portal anmelden

und die dort angebotenen Parameter den Bedürfnissen seiner Einrichtung anpassen. Ebenfalls kann ein Anwender durch diese Autonomie beliebig oft seine Konfiguration anpassen, testen und abändern.

Direkt mit der zeitlichen Erreichbarkeit eines Portals verbunden ist die ortsunabhängige Erreichbarkeit. Denn mittels eines webbasierten Portals ist es dem Anwender nicht nur jederzeit, sondern prinzipiell von jedem Ort aus möglich, beispielsweise mittels Smartphone auf das Portal zuzugreifen und Veränderungen vorzunehmen.

Ein vielleicht nicht ganz so offensichtlicher Vorteil liegt in der Dokumentations-Eigenschaft eines Portals. So liegen dem Anwender alle möglichen Konfigurationsmöglichkeiten direkt vor und sind durch Pop-Up-Hilfen – oder gegebenenfalls mittels eigenständiger Webseiten – erklärt. Somit erhöht sich für den Anwender die Zugänglichkeit der Konfigurationsmöglichkeiten, was wiederum zu einer besseren Nutzbarkeit und Anpassungsmöglichkeit seitens des Anwenders beiträgt. Ein Portal stellt somit nicht nur die Schnittstelle zur Konfiguration oder Nutzung von Diensten dar, sondern ermöglicht dem Nutzer durch seine übersichtliche und klare Struktur intuitives Arbeiten. Insofern hat es neben seiner Funktion als Werkzeug auch den Charakter eines Leitfadens für den jeweiligen Dienst des DFN-Vereins. Auch wird die Sichtbarkeit eventuell neu implementierter Features erheblich erhöht, da sie in den Portalen direkt sichtbar sind und dem Anwender somit im Kontext der dokumentierten Portalumgebung verfügbar gemacht werden.

Spezifische Herausforderungen

Eines der Ziele der zu entwickelnden Dienst-Portale ist die Bereitstellung einer möglichst homogenen Bedienbarkeit. Dafür war eine Benutzungs-Struktur zu entwerfen, die sich in allen denkbaren Dienst-Portalen umsetzen lässt. Ziel ist also eine Architektur, die so allgemein wie möglich und so speziell wie nötig konzipiert ist, um den Anwendern ein höchstmögliches Maß an Wiedererkennung bereits verinnerlichter Abläufe zu bieten.

Gerade das oben erwähnte Lifecycle-Modell bietet sich hierfür als grundlegende Struktur idealerweise an, da sich damit eben alle Dienste grundlegend strukturieren lassen. Daraus lässt sich dann bereits eine sinnvolle, grundsätzliche Oberflächenstrukturierung ableiten, die ein einheitliches Bedienungs-Paradigma unterstützt.

Dabei werden die Geschäftsprozesse der einzelnen Dienste in den Dienst-Portalen klar strukturiert und direkt zugreifbar abgebildet, um die Anwender bei ihren Abläufen optimal zu unterstützen. Dies stellt einen erheblichen Mehrwert gegenüber der vereinzelt noch vorhandenen „Verwaltung per Telefonanruf oder E-Mail“ dar. Natürlich bleibt die telefonische und schriftliche Erreichbarkeit der entsprechenden Ansprechpartner in den Geschäftsstellen dabei auch zukünftig in vollem Umfang erhalten.

Und auch wenn es selbstverständlich ist, soll nicht unerwähnt bleiben, dass auch nach Inbetriebnahme von Dienst-Portalen selbstverständlich auch wie bisher ein Mitarbeiter des DFN mit Rat und Tat zur Seite steht und immer nur einen Anruf oder eine E-Mail weit entfernt ist. Die Wahl liegt nun allerdings beim Anwender, der seine Konfigurations- und Nutzungsparameter mit einem Dienst-Portal nun auch selbst in die Hand nehmen kann.

Technisches Framework

Bei der technischen Lösung der Dienst-Portale für das Wissenschaftsnetz lag der Fokus auf höchster Zuverlässigkeit und Verfügbarkeit. Ein weiterer wichtiger Aspekt bei der Arbeit mit Dienst-Portalen ist ihre plattformunabhängige Erreichbarkeit und Kompatibilität mit einer größtmöglichen Zahl von Endgeräten.

Eine ideale Grundlage hierfür bietet die unter der GNU-Lizenz veröffentliche „Liferay“-Plattform. Durch die sehr aktive Community verfügt es über eine große Anzahl von Funktionen und Möglichkeiten, die von den Entwicklern laufend erweitert werden. Unter anderem sind die mit ‚Liferay’ realisierten Dienst-Portale dezentral erreichbar und erfordern vom Anwender keine Installation und bieten die Möglichkeit mehrsprachiger Nutzeroberflächen.

Um dem hohen Bedürfnis nach Sicherheit und getesteter Stabilität zu entsprechen, wurde eine Enterprise-Lösung dieser Plattform ausgewählt, welche die vielen Vorzüge der OpenSource-Entwicklung mit den Vorteilen einer hochgradig anwenderorientierten Betreuung der Software kombiniert. ◆

Ausblick

Als nächster Schritt ist die Einbindung der Dienst-Portale in die DFN Authentifikations- und Autorisierungs-Infrastruktur (DFN-AAI) geplant. Dazu wird derzeit ein spezielles Portal für die Rechteverwaltung implementiert. Als Meta-Portal können damit die Zugriffsrechte von Dienst-Administratoren für sämtliche DFN-Portale vergeben und verwaltet werden.

Mit verteilten Rollen: Attribute Authorities in der DFN-AAI

Im Bereich des Web-basierten Single Sign-On (Web-SSO) bieten Attribute Authorities eine einfache, standardkonforme Möglichkeit, Informationen über Nutzer von Ressourcen zu speichern und abrufbar zu halten, die nicht von der jeweiligen Heimateinrichtung gepflegt werden – zum Beispiel Zugriffsrechte auf bestimmte Dienste.

Text: **Gerrit Gragert** (Staatsbibliothek zu Berlin), **Wolfgang Pempe** (DFN-Verein)

Komponenten des Web-SSO

Web-basiertes Single Sign-On (Web-SSO) erlaubt es Anwendern, sich mit Nutzernamen und Passwort, mit denen sie bei ihrer Heimateinrichtung registriert sind, bei internen und externen Diensten anzumelden (Authentifizierung) und – entsprechende Berechtigungen vorausgesetzt (Autorisierung) – diese zu nutzen. Ohne auf den Aspekt des „Single“ in „Single Sign-On“ eingehen zu wollen, betrachten wir zunächst die beteiligten Akteure bzw. Komponenten:

- Der Nutzer, der versucht, sich über einen Web-Browser bei einem Dienst anzumelden.
- Die Heimateinrichtung bzw. das von ihr betriebene Identity Management System (IdM), in dem die Nutzerdaten liegen.
- Der Dienst, der als Web-Anwendung über Inter-/Intranet erreichbar ist.

Damit die Kommunikation innerhalb der Dreiecksbeziehung IdM – Browser – Web-Anwendung zustande kommt, müssen bestimmte Standards unterstützt werden. Auf HTTP-Ebene ist dies SAML2 (Security Assertion Markup Language)[1]. Um das IdM der Heimateinrichtung und die Web-Anwendung in die Lage zu versetzen, einander zu verstehen, müssen beide SAML 2 sprechen. In aller Regel ist hierzu die Installation von Software erforderlich, die SAML-Support bietet, gleichsam also als Adapter dient. Auf Seite des IdM der Heimateinrichtung spricht man von einem Identity Provider (IdP), auf Seiten der Anwendung vom Service Provider (SP).

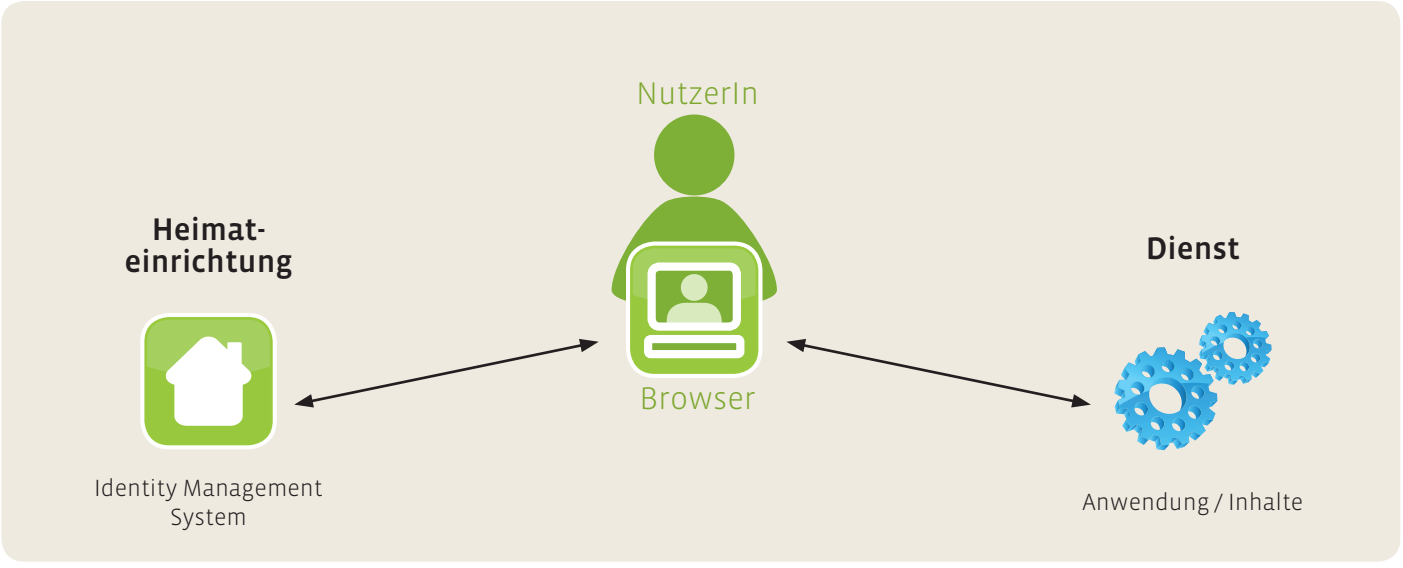


Abb. 1: Beziehung IdM – Nutzer – Dienst

Attribute und Autorisierung

Neben der Information, dass sich ein Nutzer erfolgreich beim IdP der jeweiligen Heimateinrichtung anmelden konnte, sind zur erfolgreichen Anmeldung bei einem Dienst in aller Regel zusätzliche Angaben erforderlich, die als sog. Attribute an den SP übertragen werden, der diese als (CGI-)Variablen an den jeweiligen Dienst weiterreicht. Attribute werden üblicherweise (SAML2) zusammen mit der Anmeldeinformation via Redirect in einer sog. SAML Assertion über den Browser des Nutzers an den SP übertragen. Daneben gibt es auch Szenarien, in denen der SP direkt über eine sog. Attribute Query auf den IdP zugreift, um Nutzerattribute abzuholen. Eine Reihe von Diensten stehen prinzipiell allen Nutzern und Einrichtungen offen, allerdings sind sie in der Regel nur personalisiert nutzbar, d.h. vom IdP müssen personenbezogene Angaben wie bspw. E-Mail-Adresse, Personenname und/oder ein eindeutiger Identifier übertragen werden. Sehr viele Dienste sind jedoch nur für Angehörige bestimmter Einrichtungen oder Projekte verfügbar, d.h. der Zugang zu bestimmten Ressourcen wird aufgrund von Lizenzbestimmungen, Projektbeteiligungen, Gruppenzugehörigkeiten o.Ä. auf einen bestimmten Personenkreis beschränkt.

Als Beispiel für diese Art von Diensten seien die klassischen Bibliotheksdienste genannt, also Inhaltsanbieter (Content Providers), auf deren Ressourcen nur Angehörige von Einrichtungen zugreifen können, mit denen ein kostenpflichtiger Lizenzvertrag abgeschlossen wurde. Normalerweise sind gemäß den Lizenzbestimmungen nur bestimmte Nutzergruppen berechtigt, auf die jeweiligen Inhalte zuzugreifen, d.h. hier ist eine Autorisierung anhand bestimmter Attribute erforderlich. Bei den berechtigten Nutzergruppen handelt es sich in aller Regel um Angehörige der jeweiligen Einrichtung gemäß des jeweiligen Landeshochschulgesetzes und fallweise um Bibliotheksnutzer, die von Bibliotheksterminals aus auf lizenzierte Inhalte zugreifen (Library Walk-In). Zur Autorisierung werden wahlweise die Attribute eduPersonScopedAffiliation mit den anonymen Werten „member@...“ bzw. „library-walk-in@...“ oder eduPersonEntitlement mit „urn:mace:dir:entitlement:common-lib-terms“ ausgewertet. (siehe Abb. 2)

Service-seitiges Rechtemanagement

Im Fall der Bibliotheksdienste stellt es für Heimateinrichtungen in der Regel kein Problem dar, die für die Autorisierung benötigten Attribute IdP-seitig zu generieren und auszuliefern. Es existieren aber auch Situationen, in denen dies nicht der Fall ist:

- Die Entscheidung über Zugriffrechte soll nicht durch die Heimateinrichtung sondern alleine durch den Dienstanbieter bzw. ein Projekt oder eine Forschungsinfrastruktur erfolgen.
- Die Berechtigungen sind nur für einen begrenzten (z. B. fest gebuchten) Zeitraum gültig.
- Es ist nur ein kleiner, u.U. schlecht überschaubarer Personenkreis innerhalb einer Einrichtung betroffen – z. B. die Angehörigen nur eines Instituts der Universität – die zugreifen dürfen. Hier fehlen den Einrichtungen vielfach solch feingranulare Informationen in ihren Identity Management Systemen.

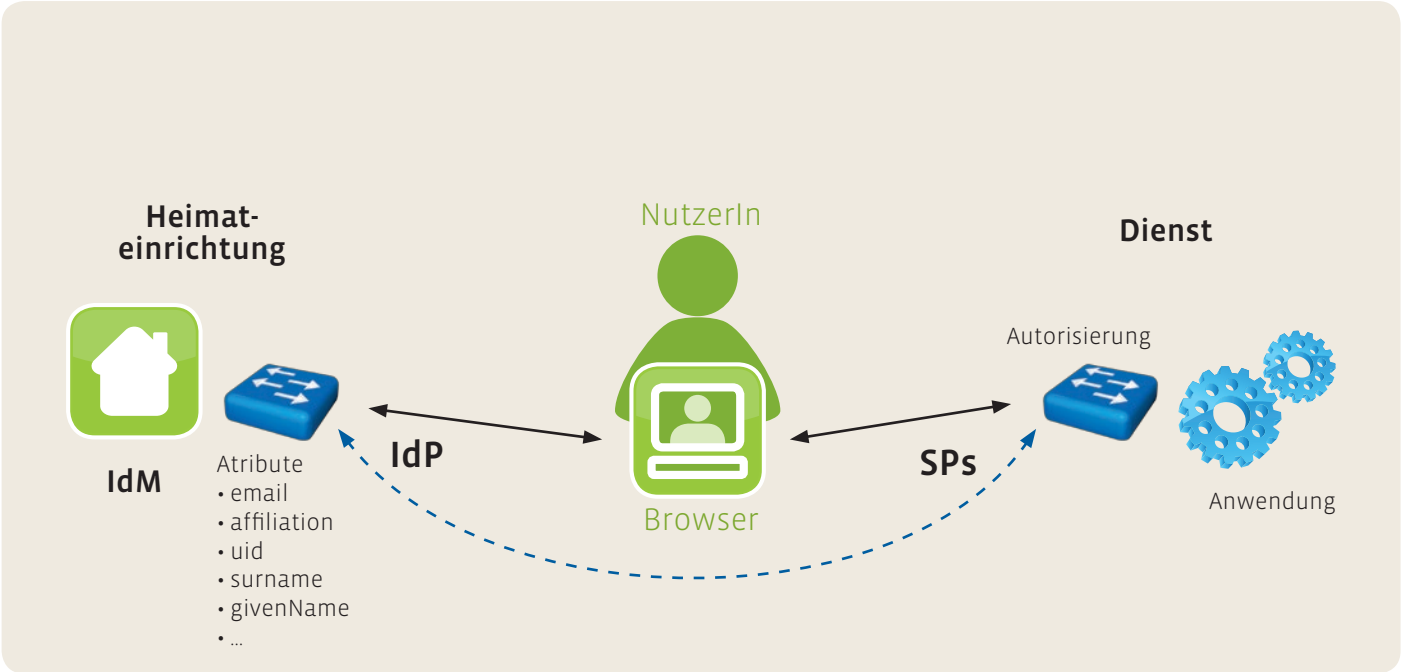


Abb 2.: Attribute und Autorisierung

In den beiden letztgenannten Fällen macht es wenig Sinn bzw. muss unverhältnismäßig hoher Aufwand betrieben werden, um die erforderlichen Informationen IdM-/IdP-seitig zu pflegen.

In solchen Situationen bieten sich sog. Attribute Authorities als zusätzliche, externe Attributquellen an, in denen unabhängig vom IdP der jeweiligen Heimateinrichtung Dienst- bzw. projektspezifische Nutzerdaten und Berechtigungen gepflegt werden können. Selbstverständlich kann auch die hinter dem jeweiligen SP liegende Anwendung eine entsprechende Datenbank anbinden. Falls die betreffende Anwendung dies nicht von Haus aus unterstützt oder die Betreiber den hohen Aufwand zur Vermeidung von Inkonsistenzen der Nutzerdaten vermeiden wollen, ist es einfacher, dem SP die Aufgabe zu übertragen, der diese standardkonform (SAML2) wahrnimmt, indem er Attribute Queries an eine oder mehrere Attribute Authorities richtet.

Technisch gesehen handelt es sich bei einer Attribute Authority um einen üblicherweise funktionsreduzierten IdP, der als einziges Profil Attribute Queries unterstützen muss. Hierzu ist es erforderlich, dass der IdP der Heimateinrichtung ein Attribut liefert (z. B. uid, E-Mail, eduPersonPrincipalName, eduPersonUniqueId)[2], das den / die jeweilige(n) Nutzer(in) eindeutig identifiziert und anhand dessen die Attribute Query bei einer oder mehreren Attribute Authorities erfolgt.

Wie das konkret aussieht, zeigt das folgende Beispiel eines vom DFN betriebenen Projekt-Wikis, auf das ausgewählte Nutzer bestimmter Einrichtungen zugreifen – darunter auch einige, deren Heimateinrichtung noch keinen IdP betreibt. Diese werden zu diesem Zweck in einem Homeless IdP registriert.

Um auf das Wiki zugreifen zu können, müssen sich die Nutzer zunächst beim IdP ihrer jeweiligen Heimateinrichtung (bzw. Homeless IdP) authentisieren. Der IdP überträgt neben der Anmeldeinformation u. a. ein Attribut zur Identifizierung des jeweiligen Nutzers, in diesem Fall eduPersonPrincipialName (ePPN). Anhand dieses Attributs führt der SP, der den Zugriff auf das Wiki kontrolliert, eine Attribute Query gegen die Attribute Authority durch. Findet sich dort ein passender Eintrag, wird die Zugriffsberechtigung anhand eines weiteren Attributs, eduPersonEntitlement (ePE), an den SP übertragen, der diese Information in eine Gruppenmitgliedschaft / Rolle übersetzt und an das Wiki weiterreicht. Eine ähnliche Lösung wird auch beim Mailsupport-Portal implementiert, wobei der Komplexitätsgrad jedoch höher liegt, da hier hierarchische Zugriffrechte vergeben werden.

Implementierung in der DFN-AAI

Da beim Betrieb von Attribute Authorities auch die Qualität und Verlässlichkeit der hinterlegten (Personen)Daten eine Rolle spielen, kommen wie beim IdP die Verlässlichkeitsklassen der DFN-AAI[3] zur Anwendung. Daher ist für den Betrieb einer oder mehrerer Attribute Authorities eine Dienstvereinbarung für die DFN-AAI erforderlich. Heimateinrichtungen, die bereits einen IdP betreiben, müssen also keine weiteren Verträge unterzeichnen.

In der Metadatenverwaltung der DFN-AAI werden seit Anfang 2014 Attribute Autho-

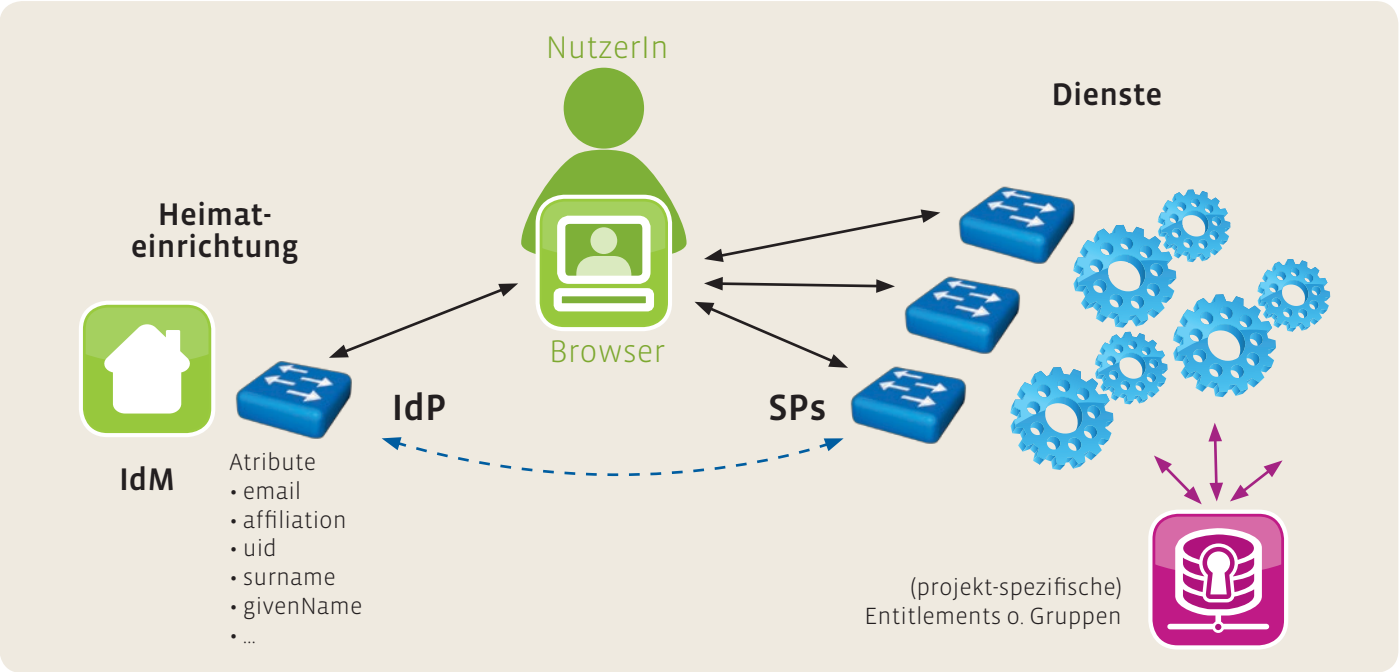


Abb. 3: Attribute Authority als externe Attributquelle

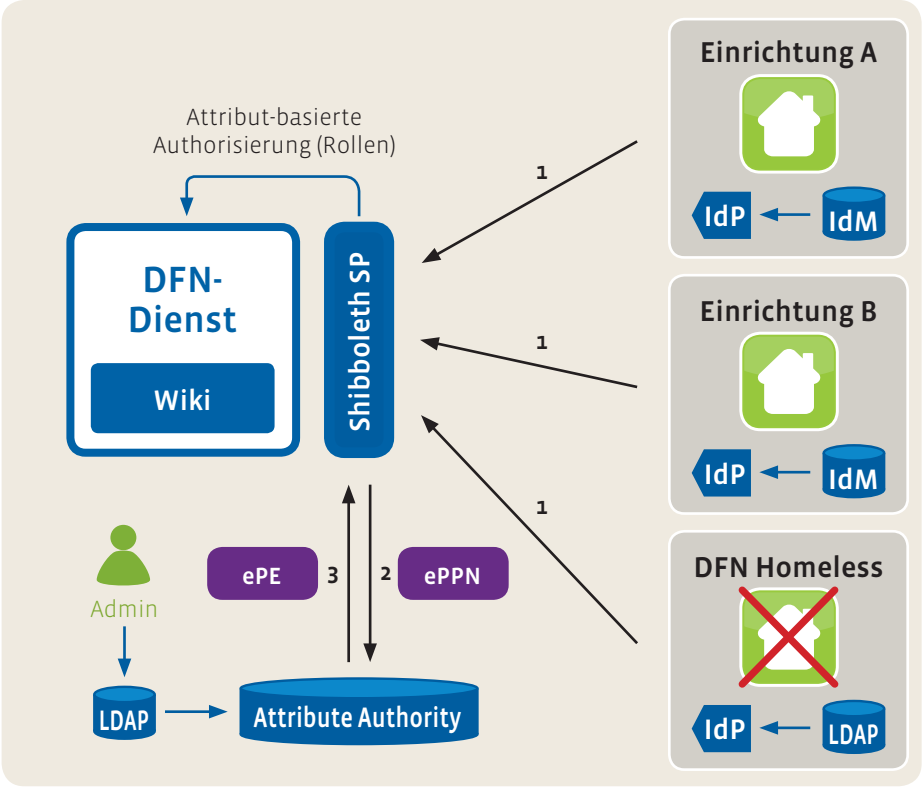


Abb. 4: Beispiel DFN Projekt-Wiki

rities als eigener Providertyp neben IdPs und SPs unterstützt, siehe Abb. 5. Dies hat folgende Vorteile:

1. Üblicherweise darf pro Einrichtung nur ein IdP in der DFN-AAI registriert sein – diese Einschränkung gilt nicht für Attribute Authorities.
2. Metadatentechnisch muss nur ein Teilbereich der sonstigen IdP-Metadaten registriert werden (AttributeAuthorityDescriptor), d.h. die Föderationsmetadaten werden nicht unnötig aufgebläht.
3. Bei der Generierung der Konfiguration der zentralen Discovery Services (WAYF) können Attribute Authorities von IdPs unterschieden und somit effektiv ausgeschlossen werden.

Anwendungsbeispiel: Fachinformationsdienste

Nicht nur bei den aufgeführten Webdiensten können Attribute Authorities zum Tragen kommen, sondern auch bei der Informationsversorgung von Wissenschaft und Forschung. Zwar versorgen heutzutage die Universitätsbibliotheken die Institute und Einrichtungen ihrer Alma Mater mit einer Vielzahl an sogenannten elektronischen Ressourcen wie Online-Fachdatenbanken, E-Journals oder E-Books, aber aufgrund endlicher Etats und zum Teil hoher Lizenzkosten für die genannten Informationsquellen kann nicht jede Bibliothek für jedes Fachgebiet allumfassend diese zur Verfügung stellen.

Dieses Problem bestand schon in früheren Jahren, als sich die Literaturversorgung durch Bibliotheken vor allem noch auf den gedruckten Bereich beschränkte. Deswegen förderte die Deutsche Forschungsgemeinschaft (DFG) mit den sogenannten Sondersammelgebieten (SSG) seit langem Bibliotheken, damit diese für ein jeweiliges Fachgebiet alle relevante Literatur beschaffen konnten, mit dem Ziel, jedes wichtige Buch mindesten einmal in Deutschland für die Fernleihe zur Verfügung zu haben. Mittlerweile ändert die DFG jedoch ihre Förderpolitik und transformiert die SSGs zu Fachinformationsdiensten (FIDs), die für eine klar umrissene deutschlandweite Fachcommunity elektronische Ressourcen lizenzieren und zugänglich machen sollen.

Ein Beispiel für eine solche Dienstleistung ist die Plattform CrossAsia (http://crossasia.org) der Staatsbibliothek zu Berlin. Angehörige der Fachcommunity können sich dort registrieren und nach schriftlicher Bestätigung ihrer Institutionszugehörigkeit auf die lizenzierten Datenbanken zugreifen. Die Plattform - wie alle künftigen FIDs - ist somit ein Mittler zwischen einem lizenzierten und somit geschützten Angebot bei einem Informationsanbieter und den Nutzern unabhängig von deren Heimateinrichtungen. Soll also ein Zugriff über die DFN-AAI erfolgen, ist das bisherige duale System von IdP, bei welchem abhängig von der Zugehörigkeit zur Heimateinrichtung Rechte vergeben werden, und SP, der den Zugriff anhand dieser Rechte gewährt oder verweigert, nicht mehr ausreichend, denn Nutzer erhalten nach ihrer Registrierung bei CrossAsia von dort weitere Rechte, die mit ihren bestehenden Rechten kumuliert werden müssen, damit ein echtes Single-Sign-On mit der Identität ihrer Heimateinrichtung realisiert werden kann. Hier kann eine Attribute Authority im Rahmen von CrossAsia zur Bereitstellung der zusätzlichen Zugriffsrechte genutzt werden.

Im Gegensatz zu den beschriebenen DFN-Diensten besteht hier jedoch das Problem, dass sich SP und AA nicht in einer Hand befinden, sondern dass die Attribute Authority von CrossAsia als weiterer Dienst föderationsweit angeboten wird und von den SPs abgefragt werden muss. Auch wenn die technischen Hürden dafür nicht sehr hoch sind, erfordert dies einige Überzeugungsarbeit bei den entsprechenden Anbietern. Grundsätzlich wirft es jedoch zwei Prob-

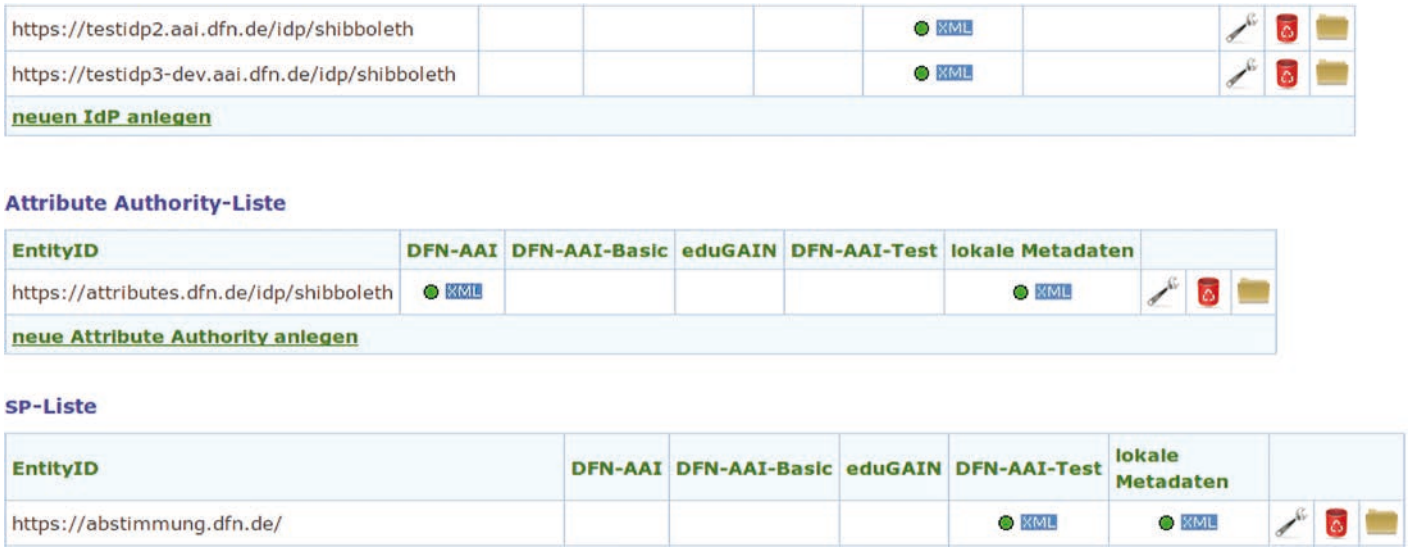


Abb. 5: Metadatenverwaltung der DFN-AAI

leme auf, die bei den oben beschriebenen DFN-Diensten so nicht zum Tragen kommen: zum einen muss die Shibboleth-Implementierung auf Anbieterseite dazu in der Lage sein, eine Attribute Authority einzubinden. Wenn dies den selbst entwickelten Plattformen der Anbieter nicht möglich ist, behilft sich CrossAsia hier mit einem Shibbolethfähigen Proxy. Zum anderen muss der Nutzer föderationsweit mit einer eindeutigen ID erkennbar sein, damit in der Attribute Authority die entsprechenden Rechte zugeordnet werden können. Da die SPs, auf die zugegriffen werden soll, im Regelfall von dritten betrieben werden, ist die Verwendung der eduPersonPrincipalNames (ePPN), der oftmals die User ID als ersten Bestandteil enthält, nicht empfehlenswert. Als geeigneter hat sich die Verwendung der eduPersonUniqueId (ePUID) herausgestellt, welche die für diesen Anwendungsfall größtmögliche Anonymität gewährt.

Der beschriebene Anwendungsfall im Rahmen von CrossAsia wurde bereits erfolgreich getestet und wird momentan in den produktiven Betrieb überführt, der in dieser Form voraussichtlich Ende des Jahres beginnen wird.

Offene Punkte und Probleme

Soll eine Attribute Authority föderationsweit betrieben werden, ist dafür wie beim Betrieb eines IdPs der Abschluss der Dienstvereinbarung für die DFN-AAI notwendig, auch wenn die Daten in der Attribute Authority durch ihre Verknüpfung über einen Identifier mit den Daten beim IdP der jeweiligen Heimateinrichtung zusammenhängen. Ist bei der Heimateinrichtung kein Login mehr möglich, sind auch die zusätzlichen Attribute in der Attribute Authority nutzlos. Hier muss der Betreiber der Attribute Authority Sorge tragen, dass kein Datengrab entsteht, d.h. ohne entsprechende Datenpflege kommt eine Attribute Authority nicht aus, weshalb die in der DFN-AAI festgelegten Verlässlichkeitsklassen auch hier zur Anwendung kommen, siehe oben. Für eine Attributverwaltung gibt es kaum Standardlösungen, so dass neben dem organisatorischen Aufwand auch ein gewisses Maß an technischer Eigenentwicklung notwendig ist. Allerdings beschäftigen sich derzeit auf europäischer Ebene einige Projekte mit dem Thema, so dass in absehbarer Zeit mit entsprechenden Softwaretools zu rechnen ist.

Vornehmlichstes Problem bleibt jedoch die Frage nach dem eindeutigen Identifier für die Nutzer, gerade wenn eine Attribute Authority Berechtigungen für mehrere Dienste bereitstellt, wie es im Rahmen der oben beschriebenen Fachinformationsdienste denkbar ist. Da ein SP eine Attribute Query nur anhand eines Schlüsselattributs durchführen kann (also z. B. entweder ePPN oder ePUID), muss hier zunächst festgelegt werden, welche ID zur Anwendung kommt. Dann muss diese ID dauerhaft eindeutig und für alle SPs gleich sein, damit in einer zentralen Attribute Authority eine Verwaltung von verschiedenen Nutzern für verschiedene SPs überhaupt handhabbar ist.

Wir stehen also, was den Betrieb von Attribute Authorities angeht, erst am Anfang. In der föderativen Bildungs-, Universitäts- und Informationsversorgungslandschaft gibt es aber kaum eine Alternative, wenn bundesweit ein Diensteangebot bzw. Informationsversorgung mit einem Web-SSO auf Basis von Shibboleth erfolgen soll. ◆

[1] https://www.oasis-open.org/standards#samlv2.0
[2] Zu den Attributen des eduPerson-Schemas siehe die Übersicht unter http://macedir.org/specs/internet2-mace-dir-eduperson-201310.html
[3] https://www.aai.dfn.de/der-dienst/verlaesslichkeitsklassen/

Kurzmeldungen

1000ster Roaming-Standort in Sichtweite

An den zuletzt 336 Hochschulen und Forschungseinrichtungen, die DFN-Roaming/eduroam für Mitarbeiter und Studierende anbieten, authentifizieren sich täglich zwischen 70.000 und 150.000 Endgeräte. Da viele Einrichtungen mehrere Campusse unterhalten, zählte der Dienst zuletzt fast 1000 Roaming-Standorte.

Auch international nimmt die Verbreitung von eduroam immer mehr zu. Inzwischen wird der WLAN-Dienst nicht nur in der gesamten GÉANT-Community Europas angeboten, sondern ebenso an vielen Hochschulen in Nord- und Südamerika, in verschiedenen mittel- und ostasiatischen Forschungsnetzen, in Südafrika und ebenfalls im noch jungen kenianischen Forschungsnetz KENET.

Eduroam zeigt auch, wie mobil Studierende und Wissenschaftler heute arbeiten: Ganze 17 Prozent der Nutzer in Deutschland sind ursprünglich an einer Hochschule außerhalb Deutschlands authentifiziert und nutzen eduroam während eines Gastsemesters oder eines Reiseaufenthalts in Deutschland. Der von der GÉANT Association organisierte Dienst zählt damit zu den erfolgreichsten Exporten der europäischen Forschungsnetzorganisation, der international zu einem Standard geworden ist.

Verbreitung findet eduroam mittlerweile auch außerhalb von Hochschulinstituten. Nach München, Würzburg und Ingolstadt bietet Augsburg seit kurzem als vierte Stadt in Deutschland eduroam auch in den städtisch organisierten WLANs an. ◆

12. Tagung der DFN-Nutzergruppe: „Sicherheit trotz(t) IT“

Unter dem Thema „Sicherheit trotz(t) IT“ findet vom 18. bis 20. Mai 2015 die Tagung der DFN-Nutzergruppe Hochschulverwaltung im Veranstaltungszentrum der Ruhr-Universität Bochum statt. Organisiert wird sie durch den DFN-Verein in Zusammenarbeit mit dem Dezernat für Informations- und Kommunikationsdienste der RUB. Vortragende aus Forschung, Verwaltung und Wirtschaft beschäftigen sich bereits zum 12. Mal mit hochaktuellen Fragen zu Informationssicherheit, Datenaufbewahrung und Softwarebeschaffung/-management.

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

Weitere Informationen zur Arbeit der Nutzergruppe und zu den Tagungen finden Sie unter: www.hochschulverwaltung.de. ◆

Neue Kernnetzknoten im X-WiN

Das Wissenschaftsnetz X-WiN ist im Jahr 2014 um fünf Kernnetz-Standorte reicher geworden. Bereits Anfang des Jahres 2014 wurde ein neu eingerichteter Kernnetzknoten an der TU Bergakademie Freiberg in Betrieb genommen. Im Juli wurde zusätzlich zum bestehenden Leipziger X-WiN-Knoten in der Ritterstraße ein zweiter Knoten am Augustusplatz in Betrieb genommen. Ebenfalls im Juli erfolgte die Anbindung des European Commercial Internet Exchange (ECIX), dem nach dem DE-CIX zweitgrößten Internet Exchange Point Deutschlands. Bis Ende des Jahres in Betrieb gegangen sein werden ebenfalls der generalüberholte Kernnetzknoten in Frankfurt/Oder, der von seinem Standort im alten Rechenzentrum der Europa-Universität Viadrina in der Großen Scharrnstraße in das neu errichtete Rechenzentrum in der Logenstraße verlegt und bei dieser Gelegenheit technisch erneuert wird. Direkt im Anschluss erfolgt auch die Installation eines zweiten Kernnetzknotens in Dresden. Das „Lehmann Zentrum“ der Technischen Universität Dresden, das mit einem nagelneuen Petaflop-Rechner ausgestattet, die bisherigen Institute für Hochleistungsrechnen, für wissenschaftliches Rechnen, für virtuellen Maschinenbau sowie das Medienzentrum und das Center for Advanced Modelling unter einem Dach vereint, wird ab 2015 zugleich Heimat des zweiten Dresdner X-WiN-Knotens. Erwähnenswert ist in diesem Zusammenhang auch, dass die TU Dresden zu den ersten Einrichtungen in Deutschland gehört, die mit 100 Gigabit/s an das Wissenschaftsnetz angeschlossen sind. ◆

Join the GÉANT Association!

Europas Netzwerkorganisationen DANTE und TERENA haben am 7. Oktober in Berlin die formalen Schritte eingeleitet, um künftig als eine gemeinsame Organisation die Vernetzung der Wissenschaften in Europa voranzutreiben. Die Fusion, die bereits seit einigen Jahren von den nationalen Netzwerkorganisationen in Europa diskutiert wurde, vereinigt DANTE und TERENA unter dem gemeinsamen Dach der „GÉANT Association". Die Mitgliedervertreter von TERENA und die Anteilsinhaber von DANTE einigten sich bei diesem Treffen auf ein gemeinsames Vorgehen und brachten damit eine neue Phase nach fast 30-jährigem Wirken für die Vernetzung und kooperative Forschung und Entwicklung in Europa auf den Weg.

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

Illustration: © FrankRamspott/iStock

Der Beschluss, die dreißigjährige Geschichte parallelen Wirkens künftig unter einem gemeinsamen Dach für beide Organisationen fortzuschreiben, geht nicht zuletzt auch auf die GÉANT Expert Group zurück, einer im Jahr 2010 von der Europäischen Kommission eingesetzten Expertengruppe, die eine Strategie für den weiteren Ausbau des europäischen Forschungsnetzes entwickeln sollte. Der im Oktober 2011 vorgelegte Ergebnisbericht „Knowledge without Borders – GÉANT 2020 as the European Communications Commons" wurde zunächst mit großem Interesse von Forschungsnetzen und der Europäischen Kommission ausgewertet. Anlässlich der TERENA Networking Conference 2012 auf Island einigte man sich, die Leiter von ausgewählten Forschungsnetzen in der so genannten „Reykjavik-Gruppe" zusammenzurufen, um die Umsetzung der Empfehlungen auch sicherzustellen und geordnet voranzutreiben. Angeführt von Andreas Dudler, dem Geschäftsführer des schweizerischen Forschungsnetzes SWITCH, stellte die „Reykjavik-Gruppe" die Machbarkeit der Zusammenführung von DANTE und TERENA fest und erhielt einstimmige Unterstützung aller europäischen Forschungsnetze. Auf dieser Grundlage konnten endlich die konkreten Herausforderungen angegangen werden. Nach über einem Jahr intensiver Planung, unter anderem unterstützt auch durch externen Rat zu unerlässlichen Details aus Arbeits- und Steuerrecht nach englischer und niederländischer Gesetzgebung, war schließlich ein formal einwandfreier und weitgehend reibungsloser Weg gezeichnet.

DFN traditionell eng verknüpft mit DANTE und TERENA

Der DFN-Verein war seit deren Gründung sowohl Mitglied von TERENA als auch Anteilseigner von DANTE. Besonders engagiert war der DFN-Verein bei DANTE in seiner Rolle als Mitbegründer. Seit vielen Jahren war der DFN-Verein hier in verschiedenen Funktionen auch personell engagiert. So zählte der langjährige Geschäftsführer des DFN-Vereins Klaus Ullmann zu den früheren Direktoren von DANTE, bekleidete dort für Jahre das Amt des Chairmans und war ebenfalls in den Führungsgremien der von DANTE verantworteten Projekte zum Ausbau des GÉANT-Netzes aktiv. Aktuell ist DFN-Geschäftsführer Christian Grimm in diesen Positionen aktiv, seit der Gründung auch als Direktor in der GÉANT Association.

Mehr Synergien für Europas Wissenschaft

Einer der Gründe für die Vereinigung beider Organisationen lag darin, dass die Rechtsform von DANTE als „haftungsbegrenzte nicht börsennotierte Kapitalgesellschaft" (company limited by shares) nur begrenzte Mitwirkungsmöglichkeiten für die „jüngeren" nationalen Forschungsnetze bot, die in den vergangenen zwanzig Jahren vor allem in Ost- und Südost-Europa gegründet wurden. Ein weiterer Motor war auch das Bedürfnis, die parallel arbeitenden Organisationen unter einem Dach zu vereinen sowie mehr Synergien zwischen DANTE auf der einen und der TERENA Association auf der anderen Seite zu erreichen. DANTE agierte bislang vor allem als Organisator und Betreiber des europäischen Forschungsbackbones GÉANT sowie als Koordinator der zugehörigen EU-Projekte und beteiligte sich an globalen Vernetzungsinitiativen, die zum Teil ebenfalls durch EU-geförderte Projekte unterstützt wurden.

Die Vereinigung beider Organisationen unter dem gemeinsamen Dach der GÉANT Associaton birgt große Potenziale für die Wissenschaft in Europa. Insbesondere, weil die Kompetenzen und Zuständigkeiten beider Organisationen in der Vergangenheit stets klar gegeneinander abgegrenzt waren, verhalten sich beide Partner zueinander wie perfekt ineinander passende Puzzle-Teile. Beide Organisationen haben sich über Jahrzehnte ein eigenes Profil erarbeitet, ohne in die Kompetenzen der Schwesterorganisation einzugreifen.

TERENA vertrat die Interessen von mehr als vierzig nationalen Forschungsnetzen und war Garant dafür, dass Dienste, Services und Architekturen auf nationaler Ebene bereits in ihrer Entstehung Teil der internationalen Strategien einzelner Länder bildeten. Mit jährlichen Konferenzen, Seminaren, Trainings und einer intensiven Kommunikationsarbeit versorgte TERENA die europäischen Netzwerke viele Jahre verlässlich mit Informationen und trug wesentlich dazu bei, dass nationale Vorhaben im Netzbereich bereits in der Phase der Konzeption international diskutiert und abgestimmt werden konnten.

DANTE wiederum betrieb mit GÉANT das größte und leistungsfähigste Forschungsnetz der Welt, das über ein breites Portfolio an international synchronisierten Diensten verfügt. Durch leistungsstarke Übergänge in die Netze Nordamerikas und Ost-Asiens und eine Reihe eigener und assoziierter Netz-Infrastrukturen in Afrika, Südamerika, Zentral- und Ost-Asien hat sich der europäischen Forschungsbackbone zu einem globalen Forschungsnetz entwickelt.

Zwei Organisationen – eine gemeinsame Geschichte

Blickt man in der Geschichte beider Organisationen zurück, wird deutlich, wie eng die Arbeit und die Ziele beider Organisationen seit langem miteinander verzahnt waren. TERENA wurde 1986 unter dem damaligen Namen RARE (Réseaux Associés pour la Recherche Européenne) aus dem Kreis der nationalen europäischen Forschungsnetze heraus gegründet, auch um den damals in Europa favorisierten Standard OSI mit seinen Protokollen zu promoten. TERENA zählte zu den Mit-Initiatoren des ersten paneuropäischen Forschungsnetzes „IXI" (International X.25 Infrastructure Backbone Service), welches auf dem OSI-orientieren Technologie-Standard X.25 basierte.

Die DANTE Ltd. war 1993 als Kapitalgesellschaft eigens zu dem Zweck gegründet worden, eine europaweite Infrastruktur aus Mitteln der öffentlichen Hand wie aus den nationalen Forschungsnetzen zu etablieren. Ausschlaggebend für die Grün-

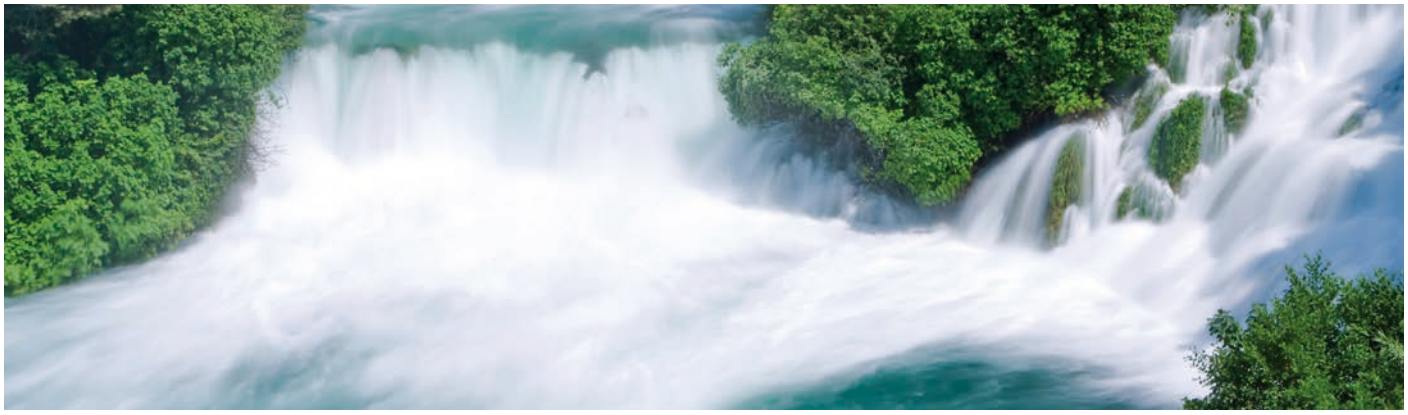


Foto: © Bartosz Hadyniak / iStock

dung war, dass die bereits bestehende TERENA Association als Verein wenig geeignet erschien, Mittel zu empfangen und wirtschaftlich zu agieren.

Nicht wenige Akteure begriffen DANTE in den Anfangsjahren noch als „operational unit" von TERENA, wobei bereits in den ersten Jahren einige Differenzen in der strategischen Ausrichtung beider Organisationen zu erkennen waren. DANTE war als Mittelempfänger der Europäischen Kommission zu Anfang ganz auf die in Europa politisch geförderten OSI-Protokolle verpflichtet, während sich TERENA – frei von der Verantwortung für einen eigenständigen Netzbetrieb – bald an der IP-Welt orientierte.

Dieses Schisma zwischen Netzbetreiber auf der einen Seite und Interessenvertreter nationaler Forschungsnetzorganisationen auf der anderen Seite verschwand auch dann nicht, als der europäische Forschungsbackbone mit dem TEN-34 auf IP umgestellt wurde. Dies änderte sich, als sich die nationalen Forschungsnetzorganisationen ebenso wie DANTE in Folge der Liberalisierung der Telekommunikationsmärkte vom Einkäufer fertig konfektionierter Netze zum Betreiber selbstgemanagter Infrastrukturen wandelten.

Gleichzeitig nahm auch die Bedeutung von TERENA für die nationalen Netzwerke immer weiter zu. Die fortschreitende europaweite Synchronisierung von Diensten und Services wie eduroam oder eduGAIN und ein immer breiteres und professionelleres Dienste-Portfolio steigerten den Bedarf an internationaler Abstimmung mit den europäischen Partnernetzen deutlich. Und dabei verwischten sich auch immer mehr die alten Grenzen zwischen DANTE und TERENA. Die Frage, wer einen bestimmten Dienst technisch aufsetzt und administriert war für die zum Dienste-Anbieter aufgestiegenen Forschungsnetze mindestens ebenso wichtig wie die Frage, wie sich nationale Vorhaben bereits in der Entstehungsphase international verknüpfen lassen. Dies führte in den vergangenen Jahren dazu, dass die alten Grenzen zwischen DANTE und TERENA zwar auf organisatorischer Ebene noch Bestand hatten, auf technischer und operationaler Ebene aber längst antiquiert wirkten.

Die Verschmelzung beider Organisationen, die am 7. Oktober 2014 in Berlin endlich auch formal begonnen wurde, markiert dabei einen Schritt, der in der Praxis an vielen Stellen längst vollzogen war.

Aufbruch in die Zukunft

Erster Präsident der GÉANT Association ist Pierre Bruyère, Direktor des belgischen Forschungsnetzes BELNET und bisher Präsident von TERENA. Bob Day, Executive Director des britischen Forschungsnetzes Janet und bisheriger Chairman von DANTE, wird als erster CEO der GÉANT Association in den kommenden Monaten die äußerst verantwortungsvolle Aufgabe übernehmen, die operativen Geschäfte und die Mitarbeiter von DANTE und TERENA zusammenzuführen. Die Suche nach einem „permanenten" CEO hat bereits begonnen, mit der Ernennung ist jedoch nicht vor Mitte 2015 zu rechnen.

Der Fahrplan für die Zusammenführung beider Organisationen wird dadurch geprägt sein, dass „von außen" keine Störungen während des Integrationsprozess wahrgenommen werden, aber möglichst bald die Vorteile einer vereinfachten Governance, eines effizienteren Managements und einer flexibleren Nutzung der Ressourcen spürbar werden sollen.

Die Chancen dafür stehen mehr als gut. Unter dem gemeinsamen Dach der GÉANT Association vereinen sich mit DANTE und TERENA eine effektive, innovative und mitgliederreiche Interessenorganisation und der weltweit mächtigste Netzbetreiber der Wissenschaft. Die europäischen Netze aber rücken durch die Vereinigung beider Organisationen noch dichter an ihre User-Communities heran wie die nationalen Entwickler von Diensten, Services und Netzen dichter an „ihre", europäische Infrastruktur heran rücken. Vor allem aber bedeutet die Vereinigung von DANTE und TERENA eine Stärkung der europäischen Forschung und Bildung und eine technische wie politische Vernetzung der Wissenschaften in Europa als Ganzes. ◆

Global Liaison – Twinning Between Kenia and Germany

Over several years the twinning arrangement between DFN, the German NREN and KENET, the Kenya Education Network has developed and intensified. Two staff members of DFN have visited the KENET headquarters in Kenya and four engineers from KENET come to Germany to learn about DFN. Furthermore, there is a lively exchange of information between the KENET NOC in Nairobi and the DFN NOC in Stuttgart. This year Kennedy Aseda, Lead Networks Operations Engineer at KENET, visited DFN at its different sites.

An Interview with **Kennedy Aseda** (KENET) by **Leonie Schäfer** (DFN-Verein)

How did KENET start? How is it positioned today?

KENET is one of the first NRENs founded in Africa. It started in 1999 and by June 2008 had 4 engineers as employees and 12 campuses connected. Today KENET has over 30 employees, mainly engineers, and employs 5 additional graduate trainees. The number of connected member campuses increased from 12 in 2008 to 150 today. 70% of the staff members are working in at the main offices in Nairobi, 30% outside at the USIU NOC offices. The USIU NOC office is situated about 25km outside of Nairobi. Main users of KENET's network are public and private universities, furthermore some research institutes, technical colleges and governmental affiliates. Newly added to the circle of members are schools and hospitals.

What are the major projects KENET is currently involved in?

Our major project currently is to bring Kenyan schools online. The "Schools Fiber Connectivity and FREE Internet Project" runs in the city of Nairobi. 245 schools will be connected as part of this pilot. Based on the results of the pilot 2700 schools in total will be connected. Our main challenge within this project is to manage this huge amount of "clients". For this large number of clients, individual solutions are not possible. Our approach therefore is to provide solutions to communities instead of individuals. The pilot project will run in Nairobi for one year and then the concept will be transferred to other cities.

Another important project for KENET is eduroam. Currently there are 18 eduroam campuses implemented at Kenyan universities which offer over 1 Gbps connectivity. The schools connectivity project will also have a pilot installation of eduroam.

What do you see as Future Work for KENET?

The development of a concept for sharing research infrastructures would be a challenging task. Up to now infrastructure facilities are simply shut up after use or after the end of the project. Our objective is to try to get the infrastructure back online for the use of the community. The problem is that researchers tend to see research instruments and the corresponding infrastructure as "their" belonging. One of the major goals of the project would be to collect research instruments at a more centralised location which would allow continuous access by the researchers.

How is your cooperation with DFN and DANTE/GEANT?

The cooperation with DFN is a well-established working relationship. DFN advised the initial set-up of the Kenyan NREN and offered counseling during the subsequent years. Furthermore, DFN actively supported the installation of eduroam in our country. In recent years, several of my colleagues came to visit the DFN headquarter and its NOC to learn from the day-to-day operation of the DFN network. We always implemented something spe-

cial after our return from DFN and we appreciate DFN's support in engineering matters.

With GEANT / DANTE we cooperate as part of the AfricaConnect project. Myself, I am a member of the Global eduroam Governance Committee (GeGC). The GeGC has the objective to ensure interoperability between eduroam regions, and to define technological and administrative improvements for the operation of eduroam at the global level.

What will you take back from your visit to DFN?

We discussed many, many things. Videoconferencing Infrastructure is in principle available in Kenya but up to now much too expensive for our universities. Our lecturers would like to take videos from the lectures, but not with a webcam. We therefore need to test new VC solutions. Now we have an idea of how to install a camera for the recording of lectures and are confident to have a new VC solution within the next 3 months.

We also discussed how to improve the performance of the network in a cost effective manner. The people at the DFN NOC were very helpful in that respect. We furthermore discussed security issues – we aim to install an Update-Service on a subscription base – and PKI and Certification solutions. PKI in Kenya is set up but not yet alive. The DFN PKI provided useful ideas for its further development.

The biggest lesson I learned, however, is that „Everything is built in a progressive way" and „Everything needs time". This became evident while following the 30 years DFN celebrations end of May in Berlin.

What is your job profile at KENET?

I am the Lead Network Operations Engineer. I am supervising the operations team and ensure that Network Operations works correctly. Furthermore, I influence decisions about the selection of equipment and technical devices. My tasks include team coordination, risk management and working with our partners. In short, I have to „to put out the fire" in case of trouble.

What do you enjoy most about your work?

I enjoy most that there are new challenges every day. I enjoy the satisfaction to meet and accomplish these challenges. In Network operations, all challenges are different. I like problem solving, to meet the challenges, and to learn something new every day. ◆

Rechnerraum der Universität Mombasa *Foto © Thomas Schmid, DFN-Verein*

UbuntuNet High Speed R&E Network Commissioned

Text reproduced from the GÉANT CONNECT magazine

UbuntuNet Alliance, the research and education network for Eastern and Southern Africa; and DANTE, the operator of GÉANT, the pan-European research and education network, announced the commissioning of the UbuntuNet network, the regional high-speed Internet network connecting researchers, educators and students in Eastern and Southern Africa to their peers in the region and to Europe.

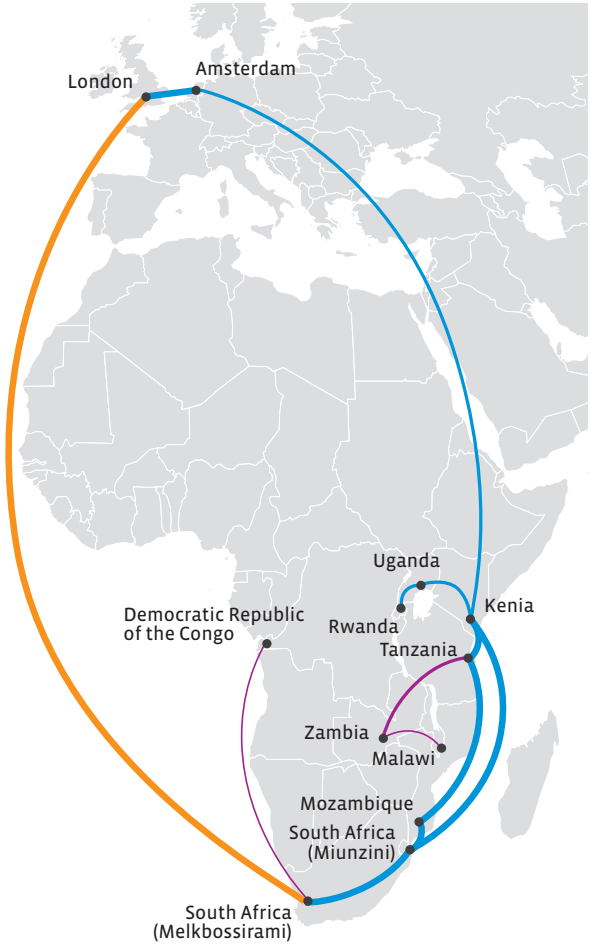
The African research and education community has for far too long carried the burden of slow Internet connectivity which has consequently widened the gap between the continent's researchers and their peers globally. The establishment of national research and education networks (NRENs), the regional UbuntuNet Alliance, and the kick off of the AfricaConnect are milestones transforming the research and education landscape on the continent.

The rollout of the UbuntuNet network has been implemented in two phases based on country readiness to connect to the regional network. Block A, which was completed in February 2014, procured equipment to establish Points of Presence (PoPs) in Mtunzini, Maputo, Dar es Salaam, Nairobi, Kampala and Kigali, and to upgrade the Ubuntunet Alliance PoP in London. High capacity cross border links interconnecting these PoPs to create a regional research network were also procured under this phase, as well as a transcontinental link between Nairobi and the Ubuntunet Alliance's PoP in Amsterdam. The first phase serves a total of six NRENs namely TENET (south Africa), MoRENet (Mozambique), TERNET (Tanzania), KENET (Kenya), RENU (Uganda) and RwEdNet (Rwanda), and forms the backbone on which the network to serve the entire Alliance region will be created.

Block B included procurement of equipment and installation of high capacity cross-border links connecting the NRENs including; Eb@le (Democratic Republic of Congo), MAREN (Malawi) and ZAMREN (Zambia). The link between Dar es Salaam in Tanzania and Lusaka in Zambia was completed at the end of May 2014 drastically reducing connectivity costs to nearly nothing for the Zambian research and education community. Links from Lusaka to Blantyre in Malawi, and from Cape Town to Moanda in DRC will be completed in the near future.

A major immediate impact of the network is that connectivity costs have dropped from a regional average of $4000 per megabit per second per month to $135per megabit per second per month indicating a 97 percent price reduction in just four years.

For more information, visit:
UbuntuNet Alliance, www.ubuntunet.net
AfricaConnect, www.africaconnect.eu



Rollout of the UBUNTU-Network:

Partner NREN-Links
completed in February 2014
completed in May 2014

GÉANT Extends ESnet's Transatlantic Connectivity

Author: **Paul Maurice** (GÉANT Ltd.)

The U.S. Department of Energy's (DOE) Energy Sciences Network, otherwise known as ESnet, is extending its reach using the state-of-the-art GÉANT network and the services of GÉANT's operator, GÉANT Ltd., to deploy a resilient high speed network ring across Europe.

Together with the ESnet and GÉANT infrastructure, the three 100Gbps European links and associated routing equipment will greatly improve collaboration opportunities between US and European research and education facilities, thanks to the superfast connectivity and resilience vital for such big data uses.

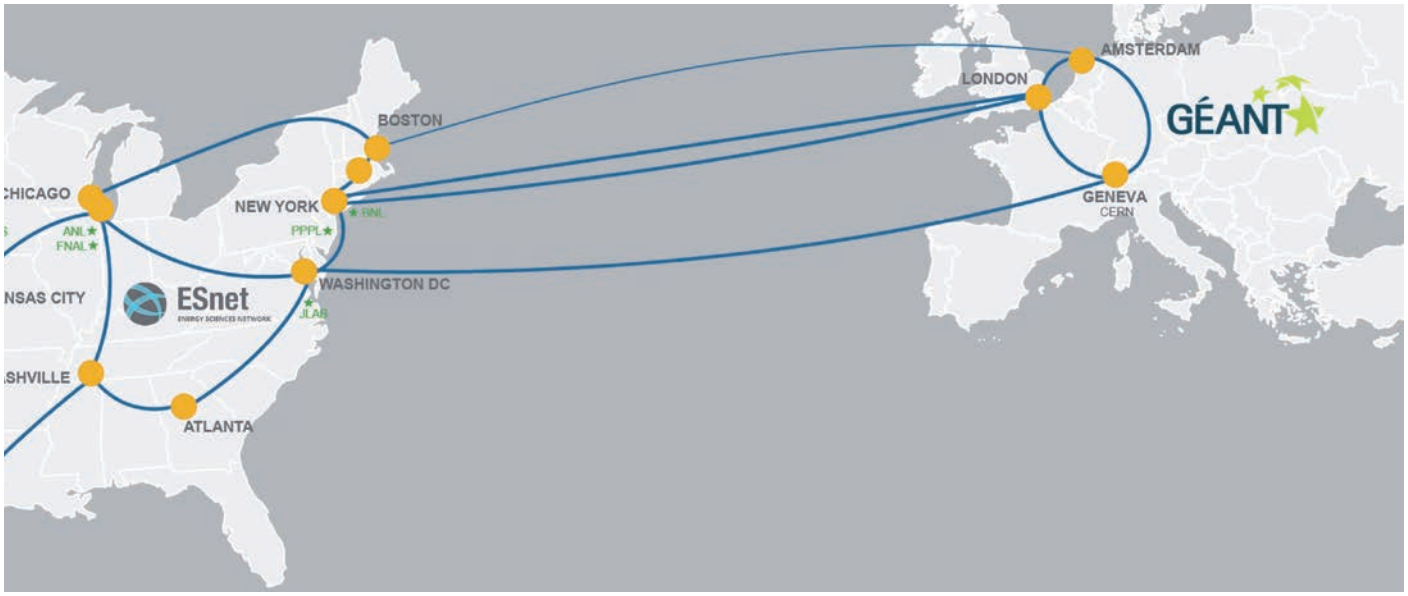
ESnet is connecting to GÉANT at three locations: London, Amsterdam and Geneva. GÉANT will provide the three 100Gbps links to move data between these locations, as well as the GÉANT Open service, which will enable ESnet to quickly manage multiple interconnections with international networks. GÉANT Ltd. is also responsible for the provision and installation of the four ESnet points-of-presence across Europe.

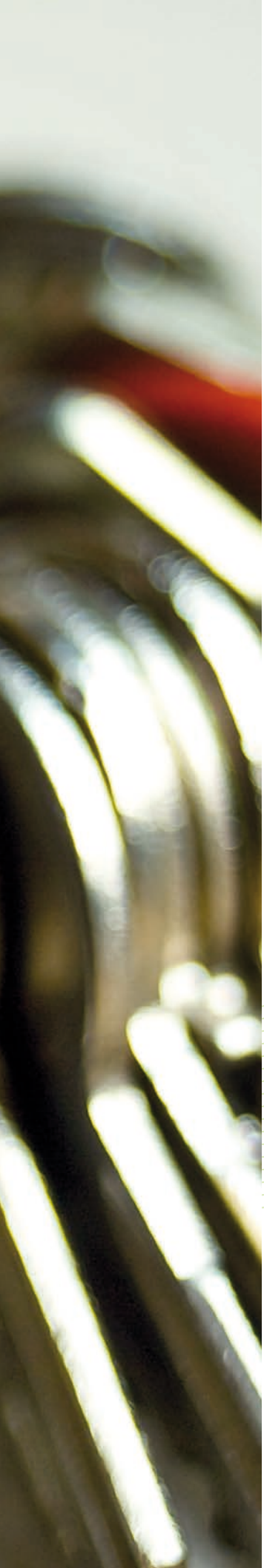
GÉANT Ltd installed ESnet's first European network node at CERN in mid-September. The first link is planned to become operational in November. The plan is for all links to be commissioned and in production by January 2015. The timing is important, because the LHC is undergoing upgrades and expected to resume operations next spring, at which point it will be generating significantly more scientific data every day.

All ESnet equipment housing, power and installation within Europe is being managed by the GÉANT Ltd.

ESnet

ESnet provides the high-bandwidth, reliable connections linking scientists at national laboratories, universities and other research institutions, and enabling them to collaborate on some of the world's most important scientific challenges including energy, climate science, and the origins of the universe. Funded by the U.S. Department of Energy's (DOE) Office of Science and managed by the Scientific Networking Division at Lawrence Berkeley National Laboratory, ESnet provides scientists with access to unique DOE research facilities and computing resources.





Campus

Herausforderungen und Anforderungen für ein organisationsweites Notfall-Passwortmanagement
von Felix von Eye, Dr. Wolfgang Hommel, Prof. Dr. Helmut Reiser

Herausforderungen und Anforderungen für ein organisationsweites Notfall-Passwortmanagement

Das Hinterlegen von Passwörtern ist ein notwendiges Übel, wenn in Ausnahmesituationen auch solche Personen auf Systeme und Dienste zugreifen können sollen, die im regulären Betrieb nicht damit befasst sind. Bei einer großen Anzahl verwalteter Passwörter, die zudem häufig geändert werden müssen, skalieren herkömmliche Ansätze wie versiegelte Passwortzettel im Tresor nicht ausreichend. Dedizierte Softwarelösungen bieten Chancen, bergen aber auch Sicherheitsrisiken. Am Beispiel des Leibniz-Rechenzentrums stellen wir Herausforderungen, Anforderungen, Lösungsansätze, bisherige Betriebserfahrungen und offene Wünsche vor.

Text: **Felix von Eye, Dr. Wolfgang Hommel, Prof. Dr. Helmut Reiser** (Leibniz-Rechenzentrum – LRZ)

1 Einleitung

Die Eingabe einer Kombination aus Loginname und zugehörigem Passwort stellt in IT-Umgebungen mit normalem Schutzbedarf seit langer Zeit die am häufigsten eingesetzte Form der Authentisierung dar. Trotz Alternativen wie Tokens, Smartcards, elektronischen Ausweisen und verschiedensten Varianten der Biometrie, deren Vor- und Nachteile gegenüber der Passwort-Authentifizierung schon oft und lange diskutiert wurden (z. B. in [RZ06] oder [Mau08]), führt im Hochschulumfeld fast kein Weg an Passwörtern vorbei: Relativ geringe Implementierungskosten, ausreichend hohe Nutzerakzeptanz und die Seltenheit signifikanter Sicherheitsvorfälle legen nahe, dass Passwörter auch in Zukunft ein fester Bestandteil des täglichen Umgangs mit IT-Diensten sein werden.

Etwas vereinfacht dargestellt muss bei Passwörtern unterschieden werden, ob sie

- persönliche Zugangsdaten darstellen, beispielsweise zum Login an PCs, zum Zugriff auf die eigene Mailbox oder zur Anmeldung bei einem webbasierten Dienst, oder
- mehreren Personen bekannt sein sollen, z. B. root- bzw. Administrator-Passwörter für Server bzw. für das Management von IT-Diensten.

Für den ersten dieser beiden Fälle wird aus guten Gründen empfohlen, für unterschiedliche Dienste bzw. Dienstleister verschiedene Passwörter zu verwenden (siehe z. B. [Bun11]). Die recht große Anzahl insbesondere an Webdiensten – durchschnittlich verwaltet jeder Nutzer im beruflichen wie auch im privaten Umfeld 25 verschiedene Accounts [FH07] –, motiviert den Einsatz von Passwortmanagement-Werkzeugen, die sich vom Passwortzettel in der Brieftasche über das Speichern im Browser bis hin zum Einsatz dedizierter Software erstrecken, wobei die Sicherheit dieser Lösungen regelmäßig geprüft werden sollte [BS12].

Auch für die System- und Dienstadministration empfiehlt sich generell die Verwendung persönlicher Zugangsdaten, also beispielsweise der Einsatz mehrerer personalisierter Kennungen mit root- bzw. Administratorenberechtigung auf Servern, wenn mehrköpfige Betriebsgruppen Zugriff haben sollen – alleine schon, um im Zweifelsfall einfacher nachvollziehen zu können, wer eine bestimmte Änderung an einem System vorgenommen hat. Dieser Teilaspekt der Benutzer- und Berechtigungsver-

waltung wird gemeinhin als Privileged Account Management bezeichnet.

Das Notfall-Passwortmanagement deckt hingegen Situationen ab, in denen am Dienstbetrieb nicht direkt beteiligte Dritte in Ausnahmesituationen Zugriff auf Systeme erhalten sollen, um größeren Schaden abzuwenden. Beispielsweise kann es ein Ziel sein, dass ein rund um die Uhr besetztes Security-Team Zugriff auf möglicherweise kompromittierte Server erhält, auch wenn der zuständige Systemadministrator und z. B. seine Urlaubsvertretung längere Zeit nicht erreichbar sind. Zu den klassischen Lösungsansätzen für dieses Problemfeld gehören z. B. auf Zetteln notierte Passwörter in versiegelten Kuverts, die in einem Tresor deponiert und beim Eintreten eines Notfalls einem dazu Berechtigten ausgehändigt werden.

Solche Lösungen, die auf einer physischen Absicherung basieren, skalieren allerdings nur unzureichend: Anders als früher müssen nicht mehr nur einige Handvoll, sondern Dutzende von Passwörtern geeignet hinterlegt werden. Passwortrichtlinien sehen nicht nur regelmäßige Passwortänderungen vor, sondern erfordern diese auch beispielsweise bei Personalfluktuation – diese ist aufgrund der vielen befristeten Stellen im Hochschulumfeld inzwischen eher die Regel als die Ausnahme. Das Pflegen hinterlegter Passwortzettel entwickelt sich dadurch von der subjektiv lästigen Pflichtübung hin zum objektiven Zeitfresser.

Die Umstellung des Notfall-Passwortmanagements auf eine zentrale, serverbasierte Software-Lösung, die von jedem Administrator-Arbeitsplatz aus genutzt werden kann, birgt viele Chancen, aber auch viele (Sicherheits-) Risiken und will aufgrund ihrer Tragweite gut überlegt sein. In diesem Artikel stellen wir die Ergebnisse eines rund einjährigen Projekts am Leibniz-Rechenzentrum (LRZ) vor, in dem zunächst eine umfassende Bedarfs- und Anforderungsanalyse durchgeführt wurde, die in Abschnitt 2 zusammengefasst ist und zum Teil auf Vorarbeiten einer an der Ludwig-Maximilians-Universität München erstellten Bachelorarbeit [Gem12] basiert und auf deren Basis mehrere kommerzielle Softwarelösungen evaluiert wurden. In Abschnitt 3 beschreiben wir die implementierte Lösung, unsere Vorgehensweise bei der Einführung und Migration sowie die bisherigen Praxiserfahrungen. Abschließend fassen wir in Abschnitt 4 das bislang Erreichte zusammen, skizzieren noch offene Punkte für die Weiterentwicklung und

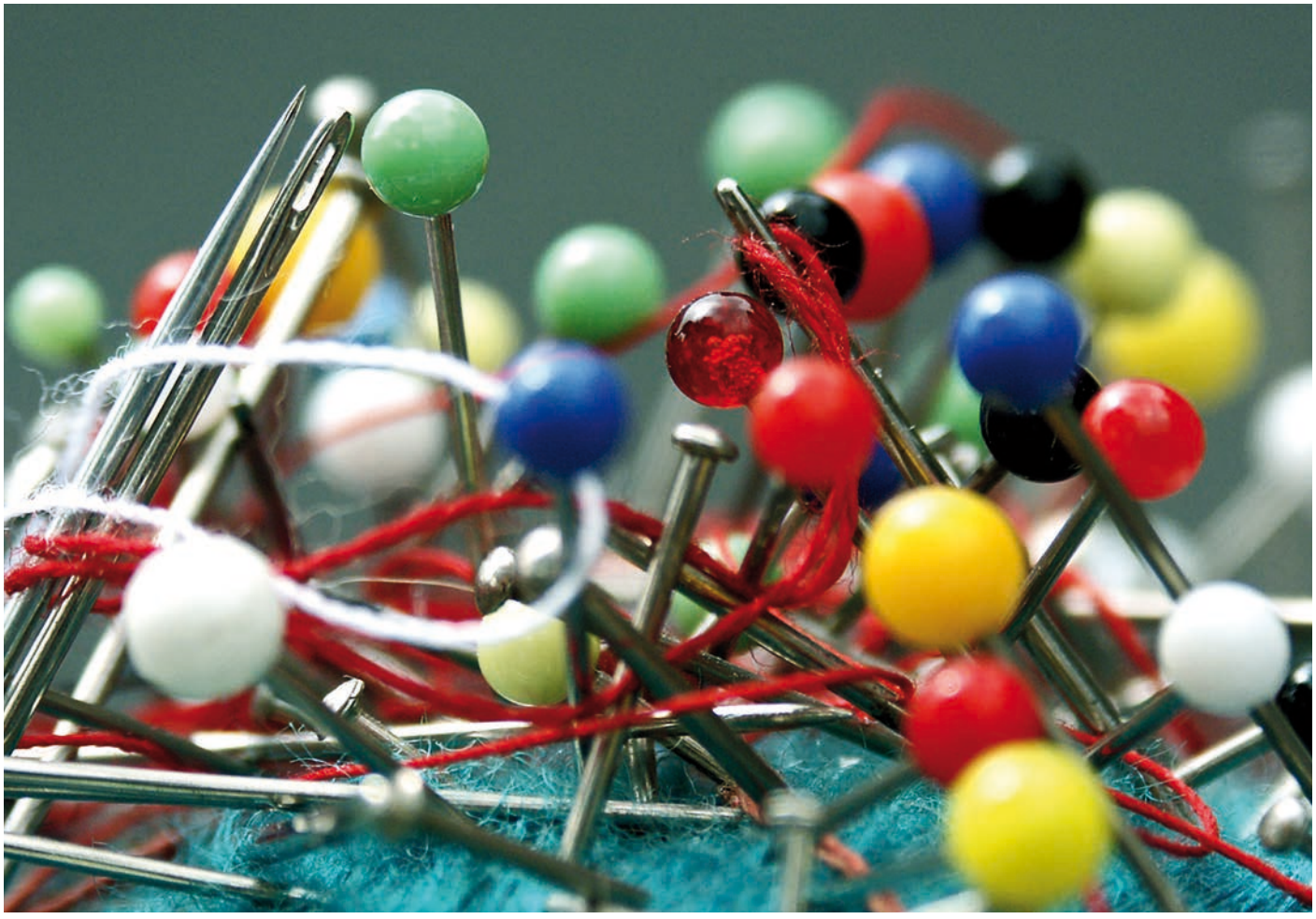


Foto © Gerti G./photocase.de

beurteilen die Übertragbarkeit auf andere Hochschulrechenzentren.

2 Entwicklung eines Kriterienkatalogs

Die zentrale Anforderung an eine Passwortmanagement-Lösung ist, dass Passwörter, die der Lösung anvertraut werden, sicher und jederzeit abrufbar abspeichert werden, wobei sicher bedeutet, dass zu jedem Zeitpunkt sichergestellt sein muss, dass Unberechtigte nicht in der Lage sind, mit vertretbarem Aufwand die Passwörter im Klartext zu erhalten. Beim Notfall-Passwortmanagement wird die zentrale Anforderung des Passwortmanagements dahingegen erweitert, dass der Kreis der zum Einsehen eines Passworteintrags berechtigten Personen temporär vergrößert wird. Dabei besteht jedoch die Herausforderung, dass ein potentieller Missbrauch einer Notfall-Berechtigung weitestgehend ausgeschlossen wird oder wenigstens eine zeitnahe Alarmierung stattfindet.

Die Kriterien, nach denen man eine Notfall-Passwortmanagement-Lösung bewerten kann, kann man grob in die Kategorien Architektur, Passworterstellung, Notfallautorisierung, Auditierung und Sicherheitsanforderungen einteilen. Im Folgenden werden diese Kategorien beschrieben und die darin enthaltenen Kriterien erläutert.

2.1 Architektur

Ein organisationsweites Notfall-Passwortmanagement sollte, wenn organisatorisch möglich, so viele der insgesamt eingesetzten und nicht nur persönlich genutzten Passwörter wie möglich enthalten. Dies dient dazu, dass in einer Notfallsituation keine unnötigen Verzögerungen entstehen, da zu jedem Passworteintrag bekannt sein sollte, wo er zu finden ist. In vielen Fällen bietet es sich daher an, die Passwörter in einer zentralen Passwortmanagement-Instanz abzulegen und die Autorisierung innerhalb dieser vorzunehmen; es ist jedoch ebenso möglich, dass mehrere Instanzen parallel oder hierarchisch betrieben werden.

Vor Einführung eines Notfall-Passwortmanagements ist somit zunächst zu ermitteln, welche zentrale Struktur man für das Speichern von Passwörtern vorsieht. Erst wenn es eine einheitliche Struktur gibt, können Passworteinträge von Personen aufgefunden werden, die diese Passworteinträge nicht angelegt haben, vor allem, wenn sich die Passwörter über mehrere Datenbanken oder Instanzen erstrecken.

Damit man eine wirksame Autorisierung und Authentifizierung durchführen kann, ist es notwendig, dass eine organisationsweite Passwortmanagement-Lösung mehrbenutzerfähig ist. Die populären und meist für den privaten Einsatz konzipierten Passwortmanager wie KeePass, KWallet oder die in modernen Browsern integrierten Passwortmanager sind üblicherweise nicht in der Lage, mehrere voneinander unterschiedliche Nutzer mit zwar unterschiedlichen Berechtigungen, aber einem gemeinsamen Datenbestand zu unterstützen. Da das Anlegen und Verwalten von Benutzern jedoch kein Teil des Passwort- sondern des Identity-Managements ist, ist eine Integration mit Verzeichnisdiensten wie LDAP oder Active Directory erforderlich.

Ebenfalls für den Aufbau des Passwortmanagement-Systems ist von Interesse, wie die Absicherung gegen diverse mögliche Ausfälle oder Fehler realisiert ist. Da ein Notfall-Passwortmanagement als Spezialfall des normalen Passwortmanagements aber genau für diese Fälle eingesetzt werden soll und man somit nicht davon ausgehen kann, dass die hauptamtlichen Administratoren zur Verfügung stehen – beispielsweise könnte dies während einer Rufbereitschaft außerhalb der üblichen Bürozeiten sein – ist die Zugänglichkeit des Systems von entscheidender Bedeutung. Üblicherweise ist jedoch die Ausfallsicherung weniger eine Problemstellung des technischen als eher des organisatorischen Systems. Wenn beispielsweise das Notfall-Passwortmanagement von der Existenz und Funktionsfähigkeit anderer Systeme abhängt, so wird es nach dem Ausfall eben dieser Systeme nicht mehr funktionieren. Unabhängig davon muss jedoch eine gewisse Redundanz unterstützt werden.

Ferner sollte ein Notfall-Passwortmanagement-System so in der Infrastruktur platziert werden, dass dieses über klar definierte Zugriffswege erreichbar ist. Weiterhin hat jegliche Kommunikation und jeglicher Eintrag innerhalb des Systems verschlüsselt zu erfolgen, so dass selbst im Falle der (ggf. auch physischen) Kompromittierung des Systems die gespeicherten Passwörter nicht ohne zusätzlichen Aufwand in falsche Hände gelangen können.

Was ein Notfall-Passwortmanagement-System noch abrundet, aber nur in wenigen auf dem Markt erhältlichen Produkten zu finden ist, ist die Möglichkeit, dass das Notfall-Passwortmanagement-System Passwörter automatisch auf Zielsystemen ändert und diese dann in der eigenen Datenbank aktualisiert. Zwar ist diese Funktion nicht unproblematisch, da durch eine falsch konfigurierte Befehlsfolge schnell aus einer harmlosen Passwortänderung eine Systemstörung wird, aber es eröffnet die Möglichkeit, dass ein Missbrauch der Notfall-Berechtigung durch eine zeitliche Einschränkung verringert wird. Diese automatisierte Passwortänderung wäre somit einer Forderung nach einer regelmäßigen Änderung von Passwörtern, wie dies beispielsweise der BSI Grundschutz [Bun] vorsieht, gleichzusetzen.

2.2 Erstellen der Passwörter

Die Nutzung einer Passwortmanagement-Lösung bringt für Administratoren den Vorteil, dass nicht mehr jedes einzelne Passwort für jeden einzelnen Dienst individuell gewählt, anhand einer möglicherweise vorhandenen Passwortrichtline verifiziert und manuell an eine Passwortänderung gedacht werden muss. Diese Arbeitserleichterung setzt jedoch voraus, dass Passwort-

generatoren zur Verfügung stehen, die beliebige Passwortrichtlinien unterstützen und ausreichend zufällige Passwörter erstellen können.

Eine beliebte Möglichkeit, sich einer regelmäßigen Änderung von Passwörtern zu widersetzen von Administratoren ist, zwei Passwörter zu haben, die immer im Wechsel verwendet werden. Sind diese Passwörter genügend unterschiedlich, so überlisten sie ein einfaches Prüfsystem, das im Allgemeinen nur das aktuelle mit dem neuen Passwort vergleicht und bewertet, ob das neue Passwort genügend Unterschiede aufweist, um als „neues" Passwort zu gelten. Somit sollte eine Passwortmanagement-Lösung ein Log der bisher verwendeten Passwörter enthalten, die bei solch einer Prüfung herangezogen werden kann. Diese History der bereits verwendeten Passwörter muss jedoch genauso gut abgesichert sein wie das aktuelle Passwort, um mögliche Sicherheitsrisiken auszuschließen.

Auch an anderer Stelle ist eine solche History der Passworteinträge interessant. Im Fall eines Restore eines älteren Backups kann es vorkommen, dass die regelmäßige Passwortänderung des Systems bereits auf Grund einer oder mehrerer Passwortänderungen ein neues Passwort gespeichert hat. Ist eine solche History nicht vorhanden, würde sich der Zugriff auf das Backup als schwierig erweisen bzw. es wäre nötig, bei jedem Backup darauf zu achten, dass wichtige Systempasswörter in einzelnen Passworteinträgen von Hand ergänzt oder extern gespeichert werden.

Weiterhin muss es einem Nutzer des Passwortmanagements möglich sein zu bestimmen, wer seinen Passworteintrag einsehen darf und wer nicht. Vor allem beim Notfall-Passwortmanagement muss diese Berechtigungsverwaltung noch feingranularer sein als dies beim normalen Passwortmanagement möglich ist. So ist eine einfache „Lesen"-Freigabe für ein Notfall-Passwortmanagement nicht ausreichend, da unterschieden werden muss, ob ein lesender Zugriff im Rahmen der täglichen Arbeit oder ob dieser lesende Zugriff im Rahmen einer temporären Notfall-Berechtigung stattfindet. Üblicherweise sollen Personen, die über eine temporäre Notfall-Berechtigung verfügen, nicht in der Lage sein, die Einträge außerhalb fest vorgegebener Umstände einzusehen, deren Eintreten zu dokumentieren ist.

Foto © Dagmar Fischer / photocase.de

Neben dem Einsehen eines Passworteintrages sollte ein Nutzer auch in der Lage sein, zu bestimmen, welche Einträge im Ganzen für wen sichtbar sind und welche anderen Benutzern verborgen bleiben. Gerade wenn Einträge, für die man überhaupt keine Berechtigung hat, ausgeblendet werden, wird die Übersichtlichkeit und Nutzbarkeit des Systems erhöht.

2.3 Autorisierung einer temporären Zugriffsberechtigung

Zentraler Punkt eines Notfall-Passwortmanagements ist das Bereitstellen von temporären Zugriffsberechtigungen für den Fall, dass ein Zugriff auf ein System von jemanden durchgeführt werden muss, der ansonsten nicht zum Kreis der Administratoren des Systems gehört. Da diesem im Allgemeinen das Passwort für den Zugriff nicht bekannt sein sollte, ist für ein erfolgreiches Anmelden eine aktuelle Zugriffsberechtigung nötig.

Wie ein solches Ausweiten der normalen Berechtigung technisch und organisatorisch umgesetzt werden sollte, ist von Organisation zu Organisation unterschiedlich. Denkbar wären beispielsweise versiegelte Passworteinträge, die nicht unbemerkt zu öffnen sind. Erst wenn der Fall eintritt, dass eine temporäre Zugriffsberechtigung benötigt wird, wird das Siegel gebrochen und der Zugriff auf das Passwort ist möglich. Selbstverständlich muss in diesem Fall eine Benachrichtigung an den jeweils zuständigen Administrator gesandt werden, wobei sich dafür beispielsweise E-Mails, SMS oder automatisierte Sprachanrufe eignen.

Da sich diese Art der Privilegieneskalation weder für alle Einsatzszenarien noch für alle Organisationsformen eignet, da es sich hierbei um eine Tätigkeit handelt, die viel mit Vertrauen und wenig mit Kontrolle zu tun hat, bietet es sich an, auch andere Formen der temporären Zugriffsberechtigung zu fordern wie beispielsweise Mehr-Augen-Prinzip oder explizite Berechtigungspfade, das heißt, dass es explizit genannte Personen gibt, die nacheinander ihr Einverständnis zur Privilegieneskalation geben müssen. Diese Methoden eignen sich, um einen potentiellen Missbrauch der temporären Zugriffsberechtigung wirksam zu unterbinden, da ein Mitarbeiter alleine dazu nicht die Berechtigung besitzt. Ist jedoch in einer Notfallsituation nur eine der nötigen Personen, die ihr Einverständnis geben müssen, nicht verfügbar, so kann in einer solchen Situation auf den Passworteintrag nicht zugegriffen werden, so dass organisatorisch immer sichergestellt werden muss, dass jederzeit ausreichend viele verantwortlichen Entscheider verfügbar sind.

Ein wichtiger Punkt bei einer temporären Zugriffsberechtigung ist, dass sie temporär ist, das heißt, dass eine einmalig gewährte Zugriffsberechtigung nicht dauerhaft gültig sein sollte, sondern nach einer fest oder dynamisch vorgegebenen Zeit wieder entzogen wird. Dabei ist es wichtig, dass dieser Vorgang durch die Notfall-Passwortmanagement-Lösung durch einen Automatismus oder wenigstens durch einen Teilautomatismus unterstützt wird, da ansonsten im täglichen Betrieb untergeht, dass beispielsweise ein Passworteintrag entsiegelt wurde. Ebenfalls denkbar, aber technisch viel aufwändiger, ist die schon oben erwähnte automatische Passwortänderung nach dem Gewähren einer temporären Zugriffsberechtigung. Dies verhindert, dass man das Wissen um ein Passwort auch nach dem Entzug der Zugriffsberechtigung weiter nutzen kann.

2.4 Audit

Gerade im Hinblick auf die temporäre Zugriffsberechtigung ist es nötig, je nach Schutzbedarf der Einträge mitzuprotokollieren, wer welche Passworteinträge einsieht bzw. welche Aktionen mit einem Passworteintrag durchgeführt wurden. Dabei sollte, soweit dies möglich ist, das Log auditsicher, d.h. resistent gegenüber Manipulationen sein, so dass im Idealfall nicht einmal Tool-Administratoren die Möglichkeit haben, alte Logeinträge zu manipulieren.

In vielen Einsatzszenarien ist es weiterhin hilfreich, wenn Logeinträge nicht nur innerhalb der Notfall-Passwortmanagement-Lösung zu finden sind, sondern wenn es einen automatischen Versand von Benachrichtigungen gibt, der die zuständigen Administratoren über wichtige Ereignisse informiert. Neben der temporären Zugriffsberechtigung kann es allgemein für das Monitoring eines Systems interessant sein, zu ermitteln, wer sich zu welchem Zeitpunkt einen Passworteintrag ansieht, um im Anschluss auf das System zuzugreifen.

2.5 Sicherheitsanforderungen

Gerade bei der zentralen Sammlung und Verwaltung von Passwörtern für administrative Zugänge auf Systeme muss man sensibel auf die Sicherheitsbedenken der Administratoren eingehen, da diese sich sehr stark auf die Bereitschaft der Administratoren auswirken, dem Notfall-Passwortmanagement-System Zugangsdaten anzuvertrauen. Aber neben den subjektiven Sicherheitsbedenken einzelner Administratoren muss man sich jedoch vor Einführung eines Notfall-Passwortmanagements durchaus bewusst sein, dass ein zentraler Ort, an dem ein Großteil der Passwörter und sonstigen Zugriffsberechtigungen einer Organisation abgelegt ist, bei Bekanntwerden tatsächlich ein attraktives Ziel für potentielle Angreifer darstellt. Aus diesem Grund ist es wichtig, im Vorfeld zu untersuchen, ob die gewählte Softwarelösung und das System, auf der diese betrieben wird, den eigenen Sicherheitsanforderungen genügt oder ob es möglich bzw. nötig ist, zusätzliches dediziertes Sicherheitsmonitoring zu installieren.

Viele Hersteller versprechen in ihren Produktbeschreibungen, dass jegliche Einträge mit den besten und sichersten kryptographischen Algorithmen verschlüsselt in der Datenbank abgespeichert werden. Der Nachweis dieser Behauptung ist jedoch

selbst in einer Evaluation von Software-Lösungen nur sehr schwer bis gar nicht zu erbringen und auch bei Open-Source-Lösungen nur mit unverhältnismäßigem Aufwand nachweisbar, dass keine Bugs oder Backdoors vorhanden sind. Zudem sollte berücksichtigt werden, dass die verschlüsselte Speicherung der Passworteinträge nur einer von mehreren wichtigen Sicherheitsbausteinen ist. Mindestens genauso wichtig sind die zuverlässige Implementierung des Berechtigungsmanagements und dem Schutzbedarf angemessene Authentifizierungsmöglichkeiten – beispielsweise beugt eine Zwei-Faktor-Authentifizierung dem Problem vor, dass ein vom Angreifer ausgespähtes Benutzerpasswort den Zugriff auf alle seine Passworteinträge ermöglicht.

3 Inbetriebnahme eines Notfall-Passwortmanagements

Bei der Einführung einer neuen Software-Lösung beginnt man im Allgemeinen nicht auf der grünen Wiese, sondern hat schon eine vorhandene Infrastruktur, in die sich die neue Software-Lösung integrieren muss. Auch am LRZ wurden in der Vergangenheit Notfall-Passwörter in verschiedenen Arten und Weisen aufbewahrt, wobei sich die Aufbewahrung von Fall zu Fall unterschieden hat, jedoch waren die gewählten Lösungen zueinander inkompatibel und zumeist offline. Aus diesem Grund wurde vor etwa eineinhalb Jahren beschlossen, dass ein hausweites Notfall-Passwortmanagement eingeführt werden soll.

Zu diesem Zweck wurden einige Tools und Konzepte evaluiert, die anhand des oben genannten Kriterienkatalogs bewertet wurden. Dabei hat sich herausgestellt, dass alle (Personal) Passwortmanager für ein Notfall-Passwortmanagement ungeeignet sind, da die dafür nötige Freigabe von Berechtigungen nicht zeitnah und ohne weiteres umgesetzt werden kann. Da dies am LRZ die grundlegende Anforderung war, wurden diese Produkte aus der weiteren Betrachtung gestrichen. Unter den übrig gebliebenen Tools ist besonders das Tool Password Manager Pro [Man14] hervorgestochen, das die oben genannten Kriterien in fast allen Punkten unterstützt. Dieses Tool ist jedoch für einen Unternehmenseinsatz ausgelegt, bei dem wenige Administratoren vielen Nutzern gegenüberstehen. Im alltäglichen Umfeld eines Hochschul-Rechenzentrums ist dies jedoch nicht der Fall, so dass die Lizenzkosten für diese Lösung oberhalb des am LRZ vertretbaren Maßes lagen.

Aufgrund positiver Erfahrung einer Gruppe des LRZ und einer hausweiten Testphase wurde schließlich die Entscheidung für das Tool Password Safe Enterprise Edition (PSE) der Mateso GmbH [Mat14, vEH13] getroffen, um damit ein Notfall-Passwortmanagement am LRZ aufzubauen. Diese Software bietet eine zentrale Datenbank, die mit Hilfe von Windows-Desktop-Clients angesprochen werden kann. Durch eine Synchronisation mit dem Active Directory ist die Authentifizierung einfach auf Mitarbeiter einschränkbar und durch die Möglichkeit der Versiegelung ist ein Notfall-Passwortmanagement mit dieser Software möglich. Zwar werden mit dieser Software einige der oben genannten Kriterien nicht

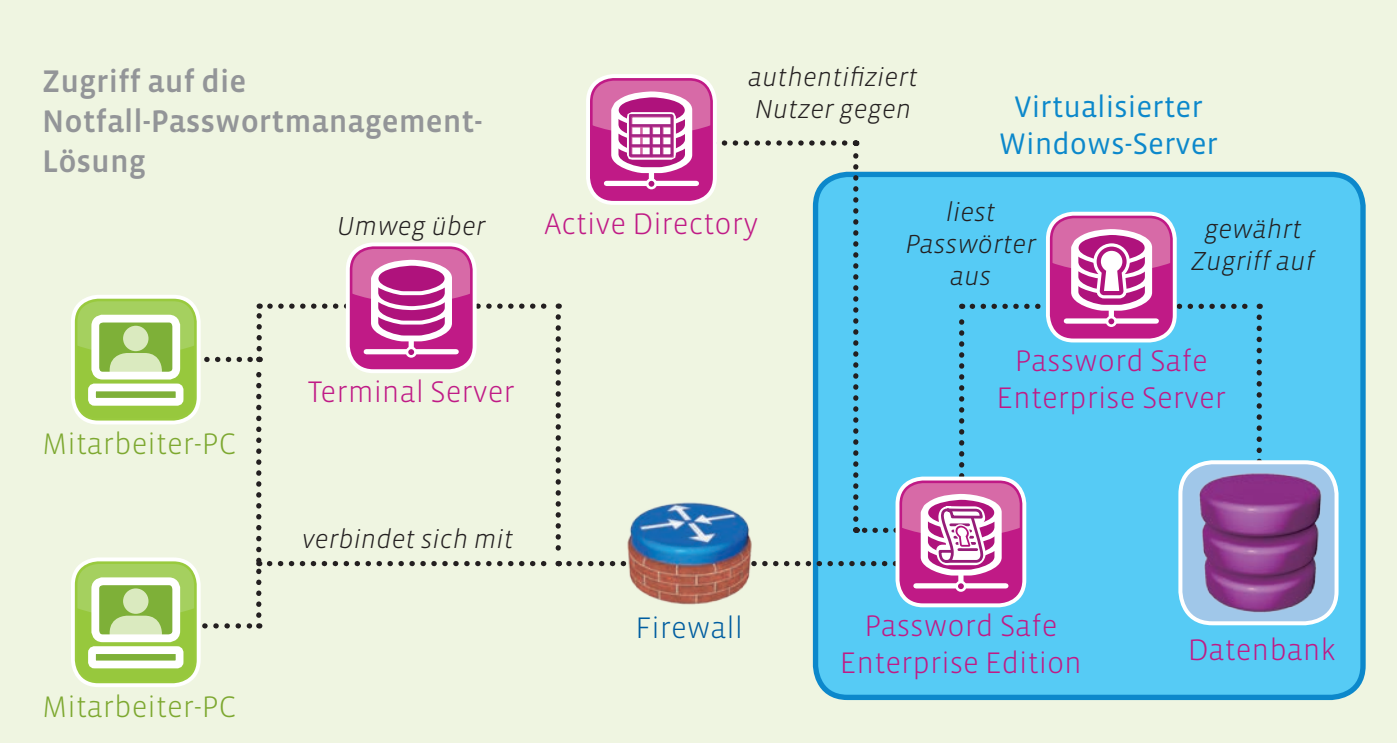


Abb. 1: Zugriff auf die Notfall-Passwortmanagement-Lösung

(vollumfänglich) erfüllt, jedoch wurden diese Punkte als nicht betriebskritisch für eine Einführung gesehen.

Die Nachteile von PSE für den konkreten Einsatz am LRZ sind unter anderem:

- Das Ändern von Passwörtern auf dem Zielsystem wird nicht unterstützt. Dies bedeutet zwar einen erhöhten Mehraufwand für die Administratoren, erleichtert jedoch die Einführung eines Passwortmanagement-Tools, da die Administratoren keine Kontrolle aus der Hand geben müssen.
- Das Tool prüft nicht, ob Passwörter bereits verwendet wurden. Diese Einschränkung ist bisher am LRZ nicht von hoher Relevanz, da auch andere passwortverarbeitende Systeme dieser Einschränkung unterliegen.
- Falls auf ein Passwort im Notfall zugegriffen und dabei das angebrachte Siegel gebrochen wurde, ist der Zugriff auf das Passwort von Dritten gesperrt. Erst muss von einem berechtigten Benutzer das Siegel wieder hergestellt bzw. entfernt werden, bevor eine weitere Verwendung des Eintrags möglich ist.
- Eine temporäre Freigabe, wie oben gefordert, ist nur in dem Maß möglich, dass das wiederhergestellte Siegel erneut als Zugriffsbarriere besteht. Da es nicht möglich ist, Passwörter auf dem Zielsystem automatisch ändern zu lassen, ist es nicht möglich, weitere temporäre Einschränkungen einzubauen.

Was vor der Inbetriebnahme nur unzureichend bedacht wurde, ist, dass in der Einrichtungsphase schon vorhandene Passwörter geeignet in die Passwortmanagement-Lösung importiert werden müssen. Zwar bietet PSE, wie im Allgemeinen alle Lösungen, die Möglichkeit, dass Passwörter in einer einfachen Form wie CSV-Dateien importiert werden können, jedoch ist durch vielfältige Berechtigungsvergaben, Sichtbarkeitseinstellungen und Versiegelungsoptionen der manuelle Aufwand für jedes einzelne Passwort so hoch, dass ein einfaches Copy & Paste des Passworts in die Datenbank zeitlich nicht relevant ist. Der langfristige Vorteil liegt jedoch auf der Hand: Während man bei einer Offline-Lösung, wie beispielsweise den Passwortzetteln im Tresor, bei jeder Änderung des Passworts der organisatorische Aufwand nahezu gleich groß ist, ist bei der hier vorgestellten Lösung der initiale Aufwand zwar sehr hoch, wird jedoch nur das Passwort in einem Eintrag geändert, so bleiben alle anderen Eigenschaften wie eingestellte Berechtigungen bestehen und müssen nicht zwangsweise neu bearbeitet werden.

Somit wird den Administratoren ein praktisches Werkzeug in die Hand gegeben, das hilft, das tägliche Chaos mit Zugriffsberechtigungen zu bändigen. Die Akzeptanz des Programms unter den Administratoren entsprach jedoch zunächst nicht den hoch gesteckten Zielen während der Einführung. So haben zum aktuellen Zeitpunkt etwa 70 % aller Administratoren einen Zugriff auf das Passwortmanagement-Tool und es wird eine knapp vierstellige Anzahl von Passwörtern darin verwaltet. Zwar ist diese Zahl, verglichen mit den am LRZ erbrachten Diensten noch recht bescheiden, aber aus Sicht der Administratoren wird die Datenbank im Wesentlichen für die kritischen Zugänge verwendet, die im Notfall bekannt sein müssen. Kleinere, unwichtige Systeme, deren Abschalten im Notfall keinen größeren Schaden verursacht, werden somit nicht über das Notfall-Passwortmanagement verwaltet sondern weiterhin über die dezentralen Lösungen. Die Gründe dafür sind sehr unterschiedlich. Neben einigen Unzulänglichkeiten des verwendeten Tools, wie beispielsweise einiger beschränkt aussagekräftiger Benachrichtigungen, die versendet werden, wenn ein versiegeltes Passwort angezeigt wird, und dem strategischen Fehler, in einer sehr heterogenen Umgebung auf eine damals rein Windows-basierte Lösung zu setzen, spielen die oben bereits angesprochenen Sicherheitsbedenken der Administratoren eine große Rolle.

Zwar wurde zur Absicherung der Passwort-Datenbank und des zentralen Servers eine Reihe von Maßnahmen ergriffen, wie beispielsweise die sehr strikte Einschränkung der Netz-basierten Erreichbarkeit des Servers, so ist, wie in Abbildung 1 zu sehen, im LRZ der Zugriff auf das Tool nur von Mitarbeiter-PCs oder über einen Terminalserver aus möglich, jedoch ist die generelle Ablehnung von Closed Source Software gerade im wissenschaftlichen Bereich auf einem hohen Niveau. Innerhalb der Datenbank wird jedoch in regelmäßigen Audits überprüft, ob die Administratoren die Berechtigungen und Sichtbarkeiten ihrer Passworteinträge korrekt gesetzt haben, so dass auf der einen Seite die Passwörter vor neugierigen Augen geschützt sind, auf der anderen Seite aber berechtigte Personen in Notfällen auf die Einträge zugreifen können.

Zusammenfassend kann man sagen, dass die Inbetriebnahme des Notfall-Passwortmanagements ein Erfolg war. Zwar sind auch nach gut einem Jahr Betrieb des Notfall-Passwortmanagements noch eine Reihe von Passwörtern nicht in das Tool eingetragen. Die Zahl der Passworteinträge ist jedoch kontinuierlich steigend und auch die Nutzung des Tools zur Erleichterung der täglichen Arbeit – da man sich das Merken oder anderweitige Notieren von Passwörtern sparen kann – wird von immer mehr Administratoren genutzt. Diese Akzeptanzsteigerung wurde insbesondere auch durch begleitende Schulungsmaßnahmen, einer ausführlichen FAQ und nicht zuletzt durch eine persönliche Betreuung der Administratoren erreicht.

4 Fazit

Organisationsweit zentrales Notfall-Passwortmanagement hat zahlreiche Vorteile, stößt bei seiner Einführung aber häufig auf die Skepsis der Administratoren, die

ihre Zugangsdaten darin hinterlegen sollen. Die Anzahl von Passwörtern, die mehreren Personen zugänglich sein müssen, kann zwar minimiert, aber in der Praxis nur sehr selten auf null gesenkt werden. Die Umstellung von rein persönlichem Passwortmanagement oder Offline-Verfahren wie verschlossenen Kuverts im Tresor auf ein organisationsweites Notfall-Passwortmanagement-Tool muss entsprechend gut geplant werden. Der größte Vorteil serverbasierter Lösungen ist die zuverlässige Alarmierung der zuständigen Administratoren, wenn sich jemand z. B. im Notfall einen temporären Zugriff auf einen Passworteintrag verschafft. Der Aufwand, beispielsweise die Ordnerstruktur, Default-Berechtigungen und E-Mail-Alarmierung zu konfigurieren, darf hierbei aber nicht unterschätzt werden.

Danksagungen

Teile dieser Arbeit wurden durch das Bundesministerium für Bildung und Forschung gefördert (FKZ: 16BP12309). Die Autoren danken den Mitgliedern des Munich Network Management Teams (MNM-Team) für wertvolle Kommentare zu früheren Versionen dieses Artikels. Das MNM-Team ist eine Forschungsgruppe der Münchener Universitäten und des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften unter der Leitung von Prof. Dr. Dieter Kranzlmüller und Prof. Dr. Heinz-Gerd Hegering. ◆

References

[BS12] Andrey Belenko und Dmitry Sklyarov. "Secure Password Managers" and "Military-Grade Encryption" on Smartphones: Oh, Really? Blackhat Europe, 2012.

[Bun] Bundesamt für Sicherheit in der Informationstechnik. BSI-Grundschutzkataloge – Regelung des Passwortgebrauchs. https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02011.html.

[Bun11] Bundesamt für Sicherheit in der Informationstechnik. BSI gibt Tipps für sichere Passwörter. https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit_27012011.html, 2011.

[FH07] Dinei Florencio und Cormac Herley. A Large-scale Study of Web Password Habits. In Proceedings of the 16th International Conference on World Wide Web, WWW '07, Seiten 657–666, New York, NY, USA, 2007. ACM.

[Gem12] Eva Gembler. Erarbeitung eines kryptografischen Modells organisationsweiter Passwortverwaltung am Beispiel des Leibniz-Rechenzentrums. Bachelorarbeit, Ludwig-Maximilians-Universität München, München, September 2012.

[Man14] ManageEngine. Password Manager Pro. http://www.manageengine.com/products/passwordmanagerpro/, 2014.

[Mat14] Mateso GmbH. Password Safe Enterprise Edition. http://www.passwordsafe.de/, 2014.

[Mau08] Thomas Maus. Das Passwort ist tot – lang lebe das Passwort! Datenschutz und Datensicherheit - DuD, 32(8):537–542, 2008.

[RZ06] Heiko Roßnagel und Jan Zibuschka. Single Sign On mit Signaturen. Datenschutz und Datensicherheit - DuD, 30(12):773–777, 2006.

[vEH13] Felix von Eye und Wolfgang Hommel. Gut gesichert? – Anforderungen an ein zentralisiertes Passwortmanagement. In ADMIN-Magazin, Jgg. 03, Seiten 96–101, München, Deutschland, Mai 2013. Linux New Media AG.

SIEGE: Service-Independent Enterprise-GradE protection against password scans

Security is one of the main challenges today, complicated significantly by the heterogeneous and open academic networks with thousands of different applications. Botnet-based brute-force password scans are a common security threat against the open academic networks. Common defenses are hard to maintain, error-prone and do not reliably discriminate between user error and coordinated attack. In this paper, we present a novel approach, which allows to secure many network services at once. By combining in-app tracking, local and global crowdsourcing, geographic information, and probabilistic user-bot distinction through differential password analysis, our PAM-based detection module can provide higher accuracy and faster blocking of botnets. In the future, we aim to make the mechanism even more generic and thus provide a distributed defense for our infrastructure against one of the strongest threats.

Text: **Prof. Dr. Marcel Waldvogel, Jürgen Kollek** (University of Konstanz)

1 Introduction

Account information is in high demand among crooks. Hacked accounts are used (1) as stepping stones to hide their tracks, (2) to abuse legitimate web sites for phishing and distribution of malware and copyrighted material, (3) to send spam without being filtered, (4) (5) for installing keyloggers to obtain more data, including banking information, and (5) to add machines to global botnets for later automated large-scale malfeasance.

One of the favorite uses of botnets is to farm more accounts to increase the power (and rental value) of the botnet [Pur03]. This is generally done by trying to authenticate against a service with (username, password) tuples based on dictionaries. These dictionaries are frequently enhanced by formation rules to e.g. append a few digits to words or replace the letter e by the digit *3*.

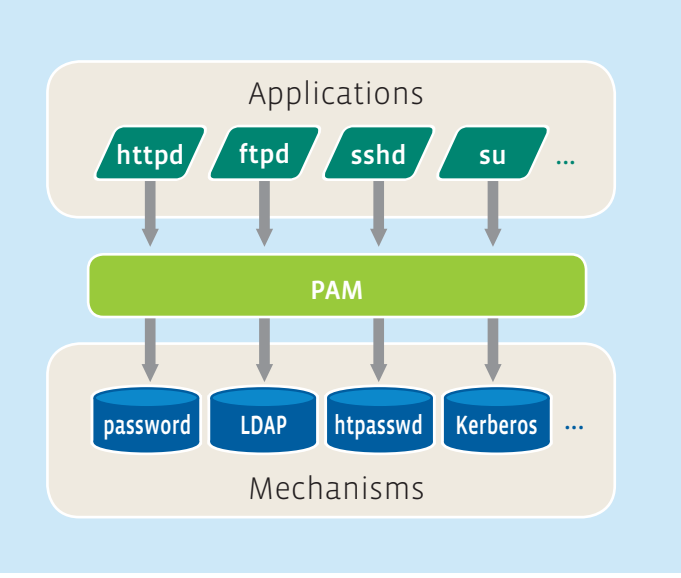


Figure 1: Flexibility of Pluggable Authentication Modules (PAM)

In the beginning, these (username, password) pairs were fired at the target as quickly as possible. However, tools such as DenyHosts [Den] and Fail2ban [Fai] made it easy to defend against these types of attacks by blacklisting the IP address of the assailant.

Nowadays, the attacks happen much more subtly. A large set of bots, often several hundred thousand, jointly and covertly go stalking potential victims: Each of them only uses a few shy attempts, hoping this will not alert the subject. Later, another member of the hunting party will tickle the prey, while the first attacker approaches the next target.

As it is necessary to allow a user to mistype her password or switch to the correct password for the system, a single failed attempt cannot be used as a direct indication of an attack. Identifying user-generated typos helps distinguishing between botnet attacks and failed user logins.

Our PAM[SS95]-based approach includes several firsts:

1. Retaining the power of PAM, allowing arbitrary authentication and authorization mechanisms to be used (Section 3)
2. Allowing geographical risk differentiation (GRID, Section 4.2)
3. Hierarchical risk grouping (Section 4.2)
4. Coordinated organisation-wide defense (CROWD, Section 4.1)
5. Dictionary-attack defense (Section 4.3)
6. Secure typo detection for user-bot differentiation (Section 4.4)

Based on flexible, realtime in-app tracking and combined with the use of DNS-based black lists, SIEGE provides low-maintenance, high-impact defense against password-guessing attacks.

2 Related work

Around 1990, it dawned to administrators and system programmers that the traditional `/etc/passwd`-based login approach was not flexible enough. Kerberos [KN03], LDAP [WHK97] and derivatives such as Microsoft's Active Directory started coming of age in the following decade. The Open Software Foundation came up with Pluggable Authentication Modules (PAM) [SS95] as the way of making authentication more flexible (Figure 1).

For each application, the system administrator can individually specify which authentication mechanisms to allow as part of the module chain (Figure 2 (b)). In addition to authentication, other account-specific functions, session management and change of authentication token (mostly passwords) can be controlled (Figure 2 (a)). Common functions include limiting access by date and time; creating and populating home directories on the first login; mounting special volumes such as encrypted homes (and securely unmounting them on logout) and many more (Figure 3).

Due to its versatility, PAM has become the de facto authentication mechanism for most Unix-like desktop and server systems [Mor97].

For more than a decade, brute force account/password guessing attacks against SSH (and other services requiring authentication) have been going on [Cid13]. In the early days, a single host attacked its target with a large set of login attempts. This was simple to mitigate: Specialized host-based intrusion detection systems (IDS) like Fail2ban or DenyHosts [Fai, Den] started scanning log files for IP addresses which exceeded a given failed

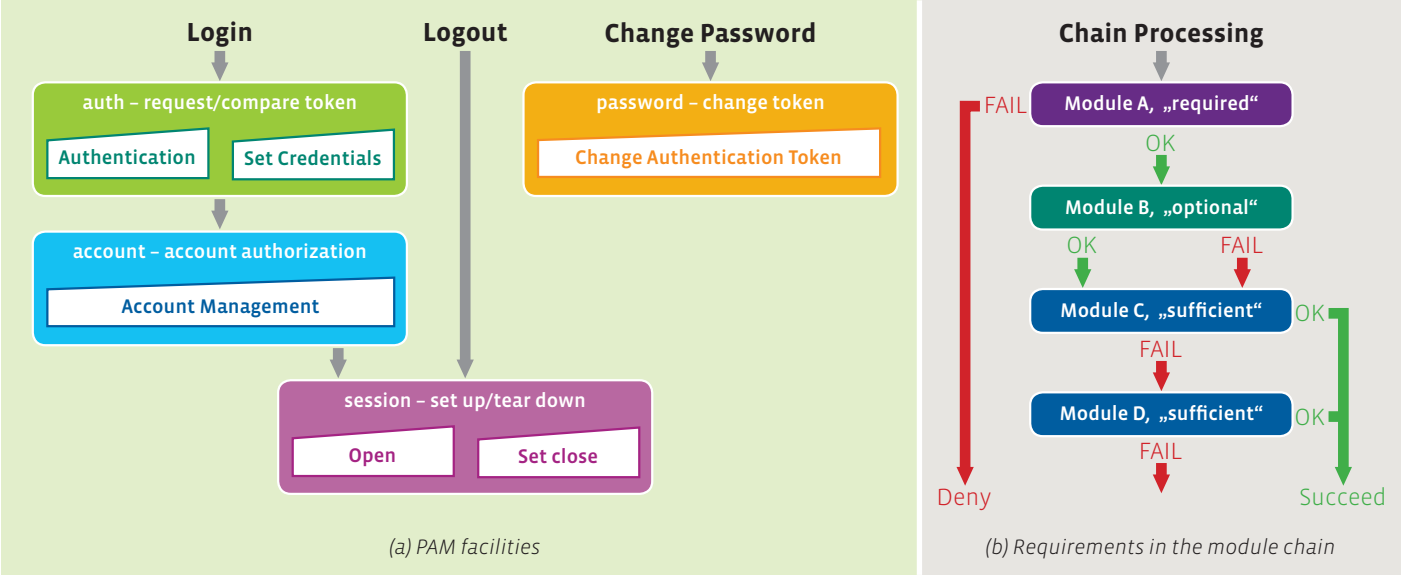


Figure 2: PAM architecture

login rate threshold. The culprits were blocked from further attempts for a specified length of time.

Even though these are still not standard practice when setting up new hosts, the attackers moved away from individual source hosts to entire botnets. This helped them also to cover their tracks. Nowadays, each of the several ten or hundred thousands members of a botnet only probes a small set of username/password combinations before focusing on the next victim. This renders source-based limits essentially useless. Furthermore, log file analysis has several drawbacks: It must be flexible enough to cope with changes of the authentication software, but it must not be fooled into misinterpreting log entries.

For example, an SSH error message documenting a failed attempt for user might look as follows

```
Jan 08 13:39:55 testhost sshd[555]: Invalid user test from 111.222.33.44
```

Malicious users can try to lock out users from a different address, say, 22.33.44.55, by trying to authenticate with the non-existant user test from 22.33.44.55 . The resulting message

```
Jan 08 13:39:59 testhost sshd[559]: Invalid user test from 22.33.44.55
from 111.222.33.44
```

and its relatives were misinterpreted by many earlier versions of most software packages, as they did not have the benefit of the differing background colors.

`pam_abl` [ABL] provides a similar function, but implements it as part of the PAM chain.
Therefore, it does not need to parse log files and thus is not vulnerable to the above log injection attacks. However, a host with pam abl still fights alone in a steep uphill battle against a fierce horde of coordinated botnet members.

In more restricted environments (stronger rules, fewer services, or fewer users) than in academia, it is also possible to limit the hosts which may login or use certificate-based logins (including SSH keys). However, the diverse student and staff body of most universities makes the necessary education and support problems look like an unsurmountable problem, especially as this diverse group of 'locals,' together with many academic guests, make traditional security perimeters impossible: *inside* is the same as *outside*.

Intrusion Detection Systems (IDS) can try and limit logins, e.g. based on IP-based blacklists [Cis09]. However, due to the encrypted nature of SSH traffic, it is impossible to distinguish failed logins from short successful logins, which occur e.g. in remote management. Neither is it possible to differentiate between 'good' and 'bad' users at this level.

3 Operation

SIEGE brackets the actual authentication modules (Figure 3 (b)).[1] With this trick, it can remain mechanism-agnostic while learning as much as possible about successful and failed authentications: A successful authentication will be visible to both module parts, while a failed attempt will only call the top half.

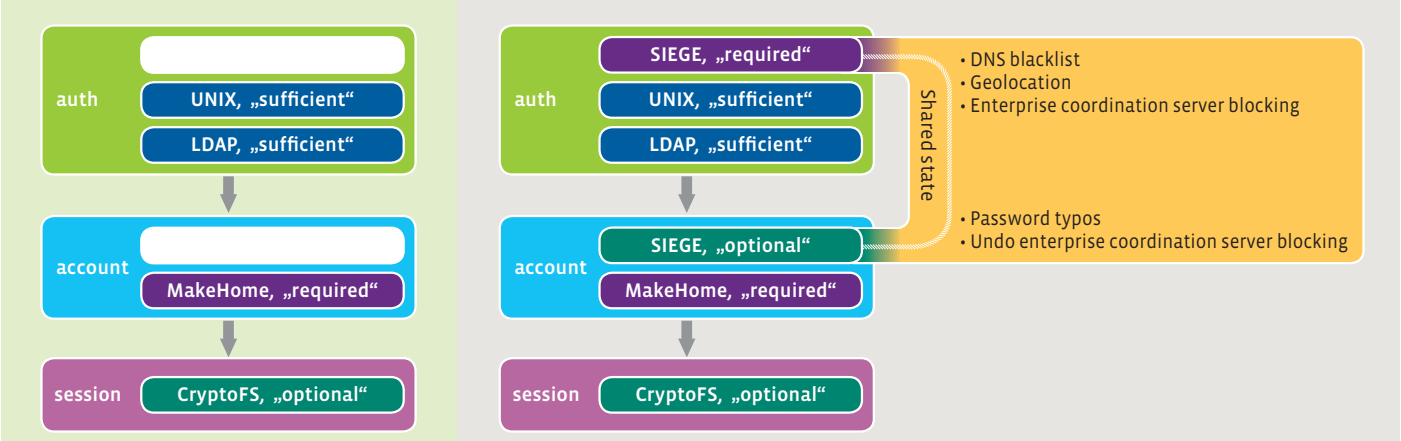


Figure 3: PAM protection

The functions are divided into top and bottom halves as follows.

Top half

1. Check whether the remote host is known to third-party DNS-based blacklists, such as Spamhaus XBL [Spa]. Fail immediately on match.
2. Compare the password against a dictionary of common passwords (Section 4.3)
3. 3Determine remaining number of failed attempts for this address:
   (a) Look up source address in the CROWD (CooRdinaated Organization-WiDe, Section 4.1) server. If unreachable, use local cache. Return this information, if any. Otherwise:
   (b) Determine geographic origin of the connection. Use administrator-set likelihood for legitimate login attempts modified with optional user preferences to determine maximum number of login attempts (Section 4.2).
4. Decrease the number of remaining login attempts, indicating that a (so far unsuccessful) attempt is in progress. The amount of reduction is tuned by the likelihood of a user password mistake (Section 4.4).
5. Perform hierarchical blocking propagation (Section 4.2).
6. Store this information in the local cache and update the CROWD.

To simplify the process of writing back local results if the CROWD has been temporarily unavailable, the minimum of the remaining attempts of CROWD and the local cache can be used.

Bottom half

1. Undo the attempted reduction and update cache and CROWD accordingly.

This unique three-level approach of (1) global, long-term DNS blacklist, (2) organization-wide CROWD, and (3) local system information, is able to strike an excellent balance between security, manageability, reliability, control, and privacy. The local level can react quickly and provides defense even when the higher levels are unreachable, e.g. because of denial of service, while CROWD helps to react even to slow attacks. The DNS blacklists help identify the long-time perpetrators, even if they have been inactive for some days. These functions cannot all be bundled into one global system, as this itself would become a security risk. In our design, the global level never sees usernameinformation. Password-related information does not leave the local host and even there it is only stored for a very short period of time. Details about the implementation can be found in [Kol13].

4 Defense mechanisms

The challenge in the defense against password-guessing attacks gets in balance between

1. locking out as many of the attackers as possible in order to reduce their guessing rate as much as possible, and
2. allowing legitimate users to log in even when an attack is ongoing.

Our approach at achieving this is described in the remainder of this section.

4.1 Coordinated organization-wide defense

In the spirit of Indra [JWZ03], CROWD uses the wisdom of the (cooperating) masses within an organization to coordinate their defense against the seemingly unsurpassable superiority of the botnet. Each host contains a local secret, which is used to authenticate against the central CROWD server through a secure connection.

The race conditions in the protocol are hard to exploit, as the problem windows are very short-lived. This approach still allows the clients to remain in full control, keep the server simple (get, put, expire) and close gaping accounting loopholes in other approaches. For example, pam abl (and, depending on the configuration, also the other mechanisms) allow a single-source attacker to open a large number of connections simultaneously. When they are open and ready to receive the password, hundreds or thousands of parallel guesses can be made before the source is blacklisted. Due to the pre-decrementing used in SIEGE, even with some decrements missing due to the race condition, only the first few attempts will be evaluated before the attacker is stopped.

4.2 Geographical risk differentiation

Even at a university with global outreach, the services requiring authentication have a local user base: Most requests will be from within the campus, the city, state, or country. Therefore, remote locations are less likely to be the source of legitimate logins, making password mismatches from other locations more likely to be from attackers. As a result, the threshold to block a given source for exceeding the number of bad password attempts can be set smaller while maintaining a high probability that legitimate users will not be locked out.

SIEGE uses this property to differentiate failure thresholds and their effects. A sample set of parameters is given in Table 1: For the university's home country, after 10 failed attempts within a defined period (typically 10 minutes), the host is blocked for a configurable time (10 minutes as well). As soon as 10 hosts within the

Class	Failure thresholds				Blocking periods (minutes)			
	Host	Subnet	Net	Country	Host	Subnet	Net	Country
Home	10	10	10	∞	10	20	30	—
Neighbors	5	5	5	20	10	20	30	60
Others	2	2	2	10	10	20	30	60

Table 1: Example escalation parameters for password failures

same subnet (/24 in the case of IPv4) are blocked, the entire subnet is blocked for 20 minutes. When the blocked subnets in a /16 network reaches 10, the entire /16 network is blocked for 30 minutes. Even when many networks in the home country are blocked, the country itself is never completely blocked. For neighbor and other countries, entire countries can be blocked.

This mechanism can be too aggressive for a member of the university visiting a country where a large number of bots are operating. Therefore, we allow individual users to list countries they are visiting.[2] For those users, the login threshold will be set to 2 (or the minimum of the country) and they will be exempt from network size escalation.

This allows to trade the small risk of user accounts being attacked against the convenience of the user. Because this has to be a user-driven step, the user can also be educated about security precautions at this time.

With this adaptive combination of reactions, the GRID component of SIEGE can ensure a very high level of security without compromising user experience.

4.3 Dictionary-based botnet identification

As a rule of thumb (and often as part of the security policy), passwords should not be derived from dictionary words or well-known frequently-used passwords. This can be enforced by the CrackLib PAM module [Gaf] or other similar tools. Conversely, this also means that users are unlikely to use a dictionary word as their password. SIEGE includes a simple test whether a password tried is known to CrackLib and immediately classifies a host trying to use such a word as an attacker, putting it on a temporary blacklist. This significantly increases the efficiency of the defense perimeter.

4.4 User-/bot password differentiation

For processes supporting manual password entry, users may mistype the password. Common typing mistakes include:

Transposing two keys on the keyboard: Two adjacent characters in the password are swapped.
Duplicating. Bouncing a key on the keyboard: A character is in the password twice instead of once.
Missing. Not hitting a key strong enough: The resulting password is missing a character.

It is unlikely that an attacker will try the correct password modified by one of these rules early in the process. Thus, seeing a password modified by one of these rules is likely to come from a user. When we detect mistakes like that, the try will not count as much as a full incorrect password attempt, thus reducing the chance of a legitimate user being locked out incorrectly.

As the above error-generating processes can all be reversed, this is easy even when the passwords are encrypted (which they should be):

Transposing. All possible single transpositions can be tried in (L– 1). A password encryption attempts locally on the machine, where L is the length of the password just received.
Duplicating. All sequences of duplicate successive characters can be eliminated each in D. Password encryption attempts locally on the machine, where D is the number of duplicate successive characters (D < L).
Missing. All possible missing characters can be tried in (L + 1). A password encryption attempts locally on the machine, where A is the size of the likely alphabet.

The first two mechanisms are very cheap, the third can be rather costly if an expensive encryption function was chosen for the password. In some environments this costly step might be undesirable and can thus be deactivated.

Mechanisms which perform weak matches against the password open up new attack vectors. One prominent mechanism are timing attacks, where a shorter password verification time would indicate that the correct password has been found after only a subset of the operations. To thwart such timing attacks, all the configured operations must be performed for an incorrect input

password. As the number of password verification options then only depend on the input password, the timing leaks no information about the proximity of the input to the actual password.

As the weak matching does not directly return information whether the password was a close match or not, this information is very hard to abuse. Therefore we believe that this option only strengthens the defense, not weakens it, as it allows for significantly narrower limits before blacklisting.

5 Evaluation

We built a simulator of the GRID and hierarchical blocking propagation logic to show the large-scale effects (Table 2). For this simulation, we assumed three botnet sizes, ranging from 10 thousand to 100 million hosts. The botnets are following either of two goals: A targeted attack against single host, or a sweeping attack, which only tries to collect accounts. We also estimate that due to protocol overhead and built-in backoff timers, each bot can try a single password per second per target host.

For unprotected hosts, this means that the total number of password attempts is the product of botnet size and number of target hosts, resulting in up to stunning 10^{11} password attempts per second! Fail2ban and DenyHosts are assumed to block a host after 10 failures for the following 10 minutes, so the effective trial rate is 10 attempts every 610 s improving on the unprotected hosts by a factor of 61.

SIEGE uses the parameters from Table 1. We assume that there are 256 countries, one home country, five neighbors, and the remaining 250 in the 'other' class. Each country consists of 256 /16 nets, subdivided into /24s. Attacking hosts are uniformly distributed about the resulting 232 addresses. This is actually the worst case for SIEGE, as any clustering will greatly increase the impact of the hierarchical blocking. We also assume that the attackers will carefully avoid all passwords found in the targets' dictionary, to avoid multiplying SIEGE blocking rate (and thus significantly reducing attack rate).

The results are impressive: SIEGE limits background-type scans to a few dozen password attempts per second. But even under heavy attack, no more than 7k attempts are successful, while still offering service to most legitimate users. GRID and CROWD combined offer 7 orders of magnitude protection over vanilla systems and more than 5 magnitudes compared to Fail2ban/DenyHosts-style.

6 Conclusions

Even a small campus without any specific protection can be subject to roughly 1017 password scans per day, especially on the weekend, when monitoring is not as close. This is equivalent to trying all(!) twelve-digit lowercase passwords, ten-digit alphabetic passwords or nine-digit passwords perfectly chosen from all 95 ASCII printable characters. With a large number of unprotected hosts, you no longer should assume that even excellent passwords are safe. Therefore, alternate mechanisms are needed. GRID and CROWD mechanisms of SIEGE provide several orders of magnitude improvement to current approaches. When you know that your campus is free of dictionary-derived passwords, the attacker identification can be significantly sped up providing even stronger protection.

We are currently working on putting the code into a releasable format to make the SIEGE benefits available to the community ◆

Target hosts	single			1k		
Botnet hosts	10k	1,000k	100,000k	10k	1,000k	100,000k
Unprotected	10k	1,000k	100,000k	10,000k	1,000,000k	100,000,000k
Fail2ban/DenyHosts	0.2k	16k	1,630k	163k	16,300k	1,630,000k
SIEGE, 1 home	0.0k	0.1k	5k	0.0k	0.1k	5k
SIEGE, 5 neighbors	0.0k	0.2k	**0.5k**	0.0k	0.2k	**0.5k**
SIEGE, 250 others	0.0k	**0.4k**	**0.4k**	0.0k	**0.4**k	**0.4k**
SIEGE, total	0.0k	0.7k	6.5k	0.0k	0.7k	6.5k

Table 2: Password trial rate [s−1] (bold numbers indicate country blocking)

References

[ABL] PAM ABL: Automatic defense against brute force attacks. http://pam-abl. sourceforge.net, accessed 2014-04-08.

[Cid13] Daniel Cid. SSH brute force – The 10 year old attack that still persists. Sucuri Blog, July 2013. http://blog.sucuri.net/2013/07/ssh-brute-force-the-10-year-old-attack-that-still-persists.html, accessed 2014-04-08.

[Cis09] Combating Botnets Using the Cisco ASA Botnet Traffic Filter. white paper, Cisco, 2009. http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/white_paper_c11-532091.pdf.

[Den] DenyHosts. http://denyhosts.sourceforge.net. [Fai] Fail2ban. http://www.fail2ban.org.

[Gaf] Cristian Gafton. pam cracklib - checks the password against dictionary words. http://www.linux-pam.org/Linux-PAM-html/sag-pam_cracklib.html, accessed 2014-04-08.

[JWZ03] Ramaprabhu Janakiraman, Marcel Waldvogel, and Qi Zhang. Indra: A Peer-to-Peer Approach to Network Intrusion Detection and Prevention. In Proceedings of IEEE WETICE 2003, Linz, Austria, 2003.

[KN03] J. Kohl and C. Neumann. The Kerberos Network Authentication Service (V5). RFC 1510, Internet Engineering Task Force (IETF), September 2003. http://tools.ietf.org/html/rfc1510.

[Kol13] Jürgen Kollek. Ein verbesserter PAM-basierter Ansatz um "brute force"-Passwort- Angriffe auf den "secure shell"-Service zu erkennen und zu verhindern. Bachelor's thesis, University of Konstanz, 2013. http://kops.ub.uni-konstanz.de/handle/urn:nbn:de:bsz:352-259480.

[Mor97] Andrew G. Morgan. Pluggable Authentication Modules for Linux. Linux Journal, December 1997.

[Pur03] Ramneek Puri. Bots & Botnet: An Overview. SANS Institute InfoSec Reading Room, August 2003. http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299, accessed 2014-04-08.

[Spa] Spamhaus. XBL – Exploit and Botnet filter. http://www.spamhaus.org/xbl/.

[SS95] V. Samar and R. Schemers. Unified Login with Pluggable Authentication Modules (PAM). Request for Comments 86.0, Open Software Foundation, October 1995. Archived at http://www.kernel.org/pub/linux/libs/pam/pre/doc/rfc86.0.txt.gz, accessed 2014-04-08.

[WHK97] M. Wahl, T. Howes, and S. Kille. Lightweight Directory Access Protocol (v3). RFC 2251, Internet Engineering Task Force (IETF), December 1997. http://tools.ietf.org/html/rfc2251.

[1] In a future version, we might consider bracketing it inside the authentication facility, between the Authentication and Set Credentials functions, similar to pam abl

[2] This is best done before leaving the home country, to avoid a lockout in the case of an acute attack.

Sicherheit aktuell

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

Austausch des DFN-PCA-Zertifikats

Für die Umstellung der DFN-PKI auf SHA-2 wurde eine Neu-Signierung des DFN-PCA-Zertifikats mit SHA-2 durch die Deutsche Telekom Root CA 2 notwendig. Am 11.2.2014 führte die T-Systems diese Neu-Signierung des DFN-PCA Zertifikats durch, und erzeugte ein neues Zertifikat mit „CN=DFN-Verein PCA Global – G01“, gültig ab 11. Februar 2014. In der DFN-PKI wurde dieses DFN-PCA-Zertifikat schrittweise ab Mitte Mai 2014 in den Anwender-CAs zur Verfügung gestellt. Die Parameter dieses DFN-PCA-Zertifikats sind so gewählt, dass es vollständig kompatibel und austauschbar mit dem DFN-PCA-Zertifikat von 2006 ist. Anfang Juli 2014 forderte der Auditor von T-Systems dann leider den Austausch dieses Zertifikats, da bei der Ausstellung von T-Systems eine bestimmte Zertifikaterweiterung (certificatePolicies) nicht aufgenommen wurde. T-Systems stellte daraufhin am 22.7.2014 ein weiteres, drittes DFN-PCA-Zertifikat aus, in dem die Mängel behoben sind. Auch dieses dritte DFN-PCA-Zertifikat ist kompatibel und austauschbar mit den beiden anderen. Daher gibt es durch die SHA-2-Umstellung und den erzwungenen Austausch drei DFN-PCA-Zertifikate. Das DFN-PCA-Zertifikat von Februar 2014 wird gesperrt werden, und darf daher nicht mehr verwendet werden. Im DFN-PKI Blog finden Sie ein kleines Shellskript, welches einen HTTPS-Webserver darauf testet, ob alle ausgelieferten Zertifikate mit SHA-2 signiert sind und ob das korrekte neue DFN-PCA-Zertifikat eingesetzt wird. ◆

Foto © Jo3-Hannes/photocase.de

SHA-2 in der DFN-PKI

In den vergangenen Ausgaben der DFN-Mitteilungen wurde bereits mehrfach über die Migration der DFN-PKI auf den SHA-2 Hashing-Algorithmus berichtet. Die Umstellung wurde inzwischen abgeschlossen und alle neu ausgestellten Zertifikate in der DFN-PKI werden standardmäßig mit SHA-2 signiert. Nachdem die Firma Microsoft als erster Browserhersteller einen Migrationsplan zur Abschaffung von SHA-1 vorgelegt hatte, sind inzwischen auch Google und Mozilla auf den Zug aufgesprungen. Besonders Google hat einen aggressiven Zeitplan vorgelegt und beginnt bereits in der kommenden Chrome-Version 39 (geplante Veröffentlichung im November 2014), Webseiten zu bestrafen, die ein Serverzertifikat mit SHA-1 verwenden, indem das Schloss neben der URL mit einem gelben Dreieck versehen wird. Die kommenden Chrome-Versionen werden dann sukzessive stärkere optische Warnungen anzeigen. Wichtig ist hierbei zu beachten, dass nicht nur die Serverzertifikate betroffen sind, sondern auch alle Sub-CAs in der Zertfizierungskette. Die vom Server ausgelieferte CA-Kette muss somit auch gegebenenfalls angepasst werden. Die Root-CAs (im Falle der DFN-PKI also die Deutsche Telekom Root CA 2) sind nicht betroffen, da ihre Integrität nicht durch Prüfen der Signatur erfolgt. Im DFN-PKI Blog haben wir weiterführende Informationen zusammengestellt, die den Anwendern im DFN insbesondere helfen, ihre Server auf korrekte Zertifikate und Konfigurationen zu testen und so eine reibungslose Migration zu SHA-2 sicherzustellen. Darüber hinaus findet sich hier eine Liste von Software, die noch nicht kompatibel mit SHA-2 ist mit Hinweisen zu entsprechenden Informationen bei den Herstellern. ◆

DFN-PKI Blog

In den vergangenen Jahren ist seit den Sicherheitsvorfällen bei großen kommerziellen CAs (Comodo, DigiNotar ...) und einigen katastrophalen Sicherheitslücken in Standardsoftware (Goto Fail, Heartbleed) viel passiert. Die DFN-PKI unterzieht sich einem jährlichen externen Audit, um die Browserverankerung sicherzustellen und die Browserhersteller geben in immer kürzeren Zyklen Anforderungen an CAs weiter. Diese Informationsflut ist über die Mailinglisten der DFN-PKI nicht mehr in einer Form unterzubringen, die allen Wünschen gerecht wird: Während der eine nur absolut betriebskritische Informationen erhalten möchte, interessieren sich andere für Hintergründe und Einschätzungen der Vorgänge durch die Mitarbeiter der DFN-PKI. Daher gibt es seit kurzen den DFN-PKI Blog, in dem regelmäßig ausführlich über Entwicklungen in der PKI-Welt berichtet wird, Tipps und Tricks zum Umgang mit den sich ändernden Anforderungen bereitgestellt werden und der es überdies besser als eine E-Mail erlaubt, die Informationen auch mit Kollegen zu teilen, die nicht die E-Mails der DFN-PKI Mailingliste erhalten. Den Blog finden Sie unter https://blog.pki.dfn.de. ◆

SSL 3.0 abschalten

Aus Rückwärtskompatibilitätsgründen werden viele HTTPS-Server noch mit Unterstützung von SSL 3.0 zusätzlich zum moderneren TLS 1.0, 1.1 und 1.2 betrieben. SSL 3.0 wird seit langem als deutlich unsicherer als TLS bewertet. Am 14.10.2014 wurde ein weiterer Angriff auf SSL 3.0 veröffentlicht. Für Serverbetreiber sollte dieser neue Angriff Anlass sein, SSL 3.0 endgültig abzuschalten. Uns ist aktuell nur eine Software bekannt, die auf SSL 3.0 angewiesen ist: Der alt-ehrwürdige Internet Explorer 6, für dessen Einsatz es keinerlei Rechtfertigung mehr gibt. Hinweise zum Test von eigenen Webservern auf SSL 3.0 sowie zu empfohlenen Konfigurationen für gängige Webserver finden Sie im DFN-PKI Blog. ◆

Sicherheitslücke in GNU Bash: Shellshock

Nachdem dieses Jahr bereits der Fehler in OpenSSL namens „Heartbleed“ vielen Systemadministratoren Kopfzerbrechen und reichlich Arbeit beschert hat, kommt nun eine vermutlich noch schwerwiegendere Sicherheitslücke in der GNU-Bash-Shell ans Tageslicht. Aufgrund der hohen Verbreitung der GNU Bash und der Möglichkeit, einen beliebigen Programmcode aus der Ferne ohne Authentifizierung auszuführen, wurde die Sicherheitslücke CVE-2014-6271 entsprechend „Shellshock“ getauft. Ein erster Patch zur Fehlerbehebung wurde nur kurze Zeit später als unzureichend erkannt, so dass eine weitere Identifizierung der verbliebenen Schwachstelle mit der National Vulnerability Database ID CVE-2014-7169 notwendig wurde. Für letztere Schwachstelle wurden von den meisten Linux-Distributionen bereits Patches bereitgestellt, die möglicherweise aber die Kompatibilität von bestehenden Shell-Skripten beeinträchtigen können. Nur wenige Tage später wurden weitere Probleme identifiziert, die unter den Bezeichnungen CVE-2014-6277, CVE-2014-6278, CVE-2014-7186, CVE-2014-7187 erfasst wurden und weitere Patches notwendig machen. Die DFN-Anwender wurden von uns umgehend durch das Advisory DFN-CERT-2014-1258 über die Sicherheitslücken und die jeweils verfügbaren Sicherheitsupdates informiert. Weitere Hintergrundinformationen sowie Hinweise zur Identifizierung betroffener Systeme finden Sie auf den Webseiten des DFN-CERT. ◆

Google Android: eduroam-Zugangsdaten gefährdet

Google Android gilt als eines der beliebtesten Betriebssysteme für mobile Endgeräte, wie Smartphones und Tablets, und naturgemäß werden auch von DFN-Anwendern in großem Umfang WLAN-Verbindungen, unter anderem über eduroam, genutzt, um mit ihren Geräten in das Internet zu gelangen. Mit großer Wahrscheinlichkeit sind zahlreiche DFN-Anwender jetzt erneut von einer alarmierenden Sicherheitslücke betroffen, die bei Verwendung der Default-Konfiguration für die WLAN-Einstellungen besteht. Bei mobilen Geräten mit Android-Betriebssystem ist die Default-Konfiguration für die Option CA-Zertifikat für WLAN-Verbindungen „keine Angabe". Konkret bedeutet dieses als normal dokumentierte Verhalten, dass die Prüfung der Zertifikatskette komplett deaktiviert ist, d.h. jedes beliebige Zertifikat wird ohne weitere Warnung akzeptiert. Erschwerend kommt hinzu, dass Benutzer nicht, wie sonst bei TLS/SSL-Verbindungen zu Servern üblich, darüber informiert werden, falls ein Serverzertifikat von einer unbekannten oder als nicht vertrauenswürdig angesehenen Root-CA (Wurzelzertifikat) ausgestellt wurde. Falls die Default-Konfiguration für Option CA-Zertifikat „keine Angabe" verwendet wird, verbindet sich das Gerät (Client) mit jedem Server, der ein beliebiges Zertifikat vorweisen kann. Anschließend werden die Zugangsdaten des Nutzers (Benutzerkennung, Passwort, Challenge Response) bei den Authentifizierungsverfahren EAP-TTLS (PAP, MSCHAPv2) und PEAP (MSCHAPv2) an den Server übermittelt. Das bedeutet, dass mit minimalen Aufwand ein bösartiger Access-Point konfiguriert werden kann, der eduroam-Zugangsdaten im Klartext sammelt. Besonders problematisch ist dies, wenn die Zugangsdaten für weitere Dienste wie E-Mail oder den VPN-Zugang zur Heimateinrichtung verwendet werden. Weitere Informationen finden Sie auf den Webseiten des DFN-CERT. ◆

Kontakt

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

Foto © Giorgio Magini/iStockphoto

Bibliothek 2.0: Alles digital, oder was?

Schlussanträge des Generalanwalts des Europäischen Gerichtshofs (EuGH) zur Auslegung der „Bibliotheksschranke“

Die Bibliothek der Zukunft: Bildschirme, Tablets und Smartphones – aber keine Bücher mehr? Hiervon sind heutige Bibliotheken noch weit entfernt. Zumindest existieren in einigen Bibliotheken bereits digitale Leseplätze, von denen aus Bücher aus dem Bestand der Bibliothek aufgerufen werden können. Das beruht darauf, dass der Gesetzgeber am 1. Januar 2008 mehrere urheberrechtliche Normen einführte, die es sich zum Ziel setzten, die Medienkompetenz der Bevölkerung und die öffentliche Bildung zu stärken. Eine dieser Normen befasst sich mit der urheberrechtlichen Zulässigkeit digitaler Leseplätze in Bibliotheken und anderen öffentlichen Einrichtungen. Dabei war lange Zeit unklar, wie die einzelnen Merkmale der Norm auszulegen sind. Hierzu äußerte sich nun der Generalanwalt des EuGH (Schlussanträge des Generalanwalts Niilo Jääskinen v. 5.6.2014 in der Rechtssache C-117/13).

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

I. Hintergrund

Mit § 52b Urheberrechtsgesetz (UrhG), der sog. Bibliotheksschranke, hat der deutsche Gesetzgeber im Jahr 2008 europäische Vorgaben zum Urheberrecht im Zuge des sog. Zweiten Korbs („Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“) in deutsches Recht transformiert. Die Norm gibt vor, dass es unter bestimmten Umständen urheberrechtlich zulässig sein kann, wenn öffentlich zugängliche Bibliotheken, Museen oder Archive den Nutzern veröffentlichte Werke aus ihrem Bestand an elektronischen Leseplätzen zugänglich machen. Das kann für die Nutzer erhebliche Vorteile mit sich bringen: So können sie am elektronischen Leseplatz ein Werk bequem suchen und von dort aus ihre Recherchen durchführen. Nervenaufreibende und zeitintensive Suchen nach dem physischen Werkexemplar würden überflüssig werden. Auch die inhaltliche Recherche könnte mittels Stichwortsuche vereinfacht werden.

Bei all diesen euphorischen Vorstellungen von einer „Bibliothek 2.0“ darf jedoch das Urheberrecht nicht in Vergessenheit geraten, das der Einrichtung von elektronischen Leseplätzen Grenzen setzen kann. Handelt es sich um ein urheberrechtlich geschütztes Werk, stellen sowohl das regelmäßig erforderliche Einscannen der Seiten als auch die Bereithaltung des digitalisierten Werkes urheberrechtliche Nutzungshandlungen dar. Derartige Nutzungshandlungen sind grundsätzlich nur dem Urheber oder aber dem Inhaber entsprechender Nutzungsrechte – bei einem Buch also einem Verlag – vorbehalten. Daraus folgt, dass eine Übereinkunft mit dem Rechteinhaber erforderlich ist. Ausnahmsweise ist eine Übereinkunft jedoch entbehrlich, wenn eine urheberrechtliche Schrankenregelung greift – am bekanntesten ist hier die in § 53 UrhG normierte Privatkopierfreiheit. Hintergrund solcher Schranken ist das Interesse der Allgemeinheit an geisti-

gen Leistungen, die insoweit einer Sozialbindung unterliegen. Bei § 52b UrhG handelt es sich um eine solche – noch recht junge – Schrankenregelung, die nach intensiven Diskussionen zwischen den Verfechtern von Ausschließlichkeitsrechten des Urhebers und den bildungspolitischen Vertretern aller Fraktionen in ihrer derzeitigen Form Einzug in das UrhG erhalten hat. Die Diskussionen basierten vornehmlich auf der Befürchtung der Rechteinhaber, dass ihnen wirtschaftliche Werte genommen würden.

Schon die heftigen Diskussionen während des Gesetzgebungsprozesses ließen erahnen, dass sich die Gerichte alsbald mit der Auslegung der Bibliotheksschranke zu beschäftigen haben würden. Ein Musterprozess zwischen der TU Darmstadt und dem Eugen Ulmer Verlag wurde im Jahr 2012 schließlich vor dem Bundesgerichtshof (BGH) verhandelt (Beschluss vom 20.9.2012, Az. I 69/11). Finanziert wurden die Parteien des Rechtsstreits vom European Bureau of Library, Information and Documentation (Eblida) auf Seiten der TU Darmstadt bzw. dem Börsenverein des deutschen Buchhandels auf Seiten des Eugen Ulmer Verlags. Daran lässt sich die hohe Bedeutung des Verfahrens erkennen.

Während der Verhandlungen kristallisierten sich drei besonders dringliche Fragen heraus. Da es sich bei § 52b UrhG jedoch um die Umsetzung einer europäischen Richtlinie handelt („Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft“) blieb den Karlsruher Richtern die Möglichkeit, dem EuGH sog. Vorlagefragen zu stellen. Durch solche Vorlagefragen können die nationalen Gerichte sicherstellen, dass die nationale Auslegung bestimmter Vorschriften im Sinne der europäischen Vorgaben erfolgt. Der BGH machte von dieser Möglichkeit Gebrauch und stellte dem EuGH drei Vorlagefragen, die die Bibliotheksschranke betreffen. Nun hat der Generalanwalt Niilo Jääskinen seine Schlussanträge gestellt. Den Schlussanträgen eines Generalanwalts leistet der EuGH in der Regel Folge, sodass sich ein Blick auf die Ausführungen lohnt.

II. Die Schlussanträge des Generalanwalts

Die Schlussanträge des Generalanwalts beziehen sich auf die Auslegung der einzelnen Tatbestandsmerkmale der Bibliotheksschranke. Hervorzuheben ist, dass der Generalanwalt die Bedeutung des § 52b UrhG in dem wichtigen Punkt stärkt, dass die Regelung auch dann zur Anwendung kommt, wenn der Verlag das Buch in digitaler Form zu angemessenen Bedingungen anbietet. Ferner soll die erforderliche Digitalisierung, die neben der

Foto © Creativeye99/iStock.

Foto © .marqs/photocase.de

Wiedergabe eine weitere Nutzungshandlung darstellt, von § 52b UrhG erfasst sein. Allerdings erlaube die Norm den Nutzern nicht, Seiten in digitaler Form – etwa auf USB-Sticks – abzuspeichern.

1.Sachverhalt

Den vom EuGH zu beantwortenden Auslegungsfragen liegt ein Rechtsstreit zwischen der TU Darmstadt und dem Eugen Ulmer Verlag zugrunde. Die öffentlich zugängliche Universitäts- und Landesbibliothek der TU Darmstadt stellte (und stellt) ihren Nutzern seit 2009 bestimmte Werke aus ihrem Bestand an Terminals auch in elektronischer Form zur Verfügung. Zu diesen Werken gehörte u. a. das im Eugen Ulmer Verlag erschienene Lehrbuch „Einführung in die neuere Geschichte".

Die TU Darmstadt hatte das Lehrbuch zunächst digitalisiert und sodann in die von den Terminals aus abrufbare Datenbank hochgeladen. Es war den Nutzern der Leseplätze nicht möglich, gleichzeitig mehr Exemplare des Werkes aufzurufen, als im Bibliotheksbestand vorhanden waren. Über die bloße Wiedergabe hinaus wurde es den Nutzern der Leseplätze ermöglicht, das Lehrbuch auf Papier auszudrucken und auf einem USB-Stick abzuspeichern, sodass es auch zu Hause wiedergegeben werden konnte. Die TU Darmstadt wies jedoch mittels eines Hinweisschildes, das an den Leseplätzen angebracht war, darauf hin, dass eine Nutzung nur zu Forschungszwecken und für private Studien zulässig sei. Bei der Anfertigung der Kopien sollten ferner die Grenzen der Privatkopierfreiheit Beachtung finden. Ein Angebot des Eugen Ulmer Verlages, das Lehrbuch in elektronischer Form zu erwerben, schlug die TU Darmstadt aus.

2. Schlussanträge

Der Generalanwalt antwortet in seinen Schlussanträgen auf die drei dem EuGH vom BGH vorgelegten Auslegungsfragen.

Auswirkung von Lizenzangeboten

Mit der ersten Frage begehrte der BGH darüber Auskunft, ob bereits das bloße Angebot eines angemessenen Lizenzvertrags über den Erwerb eines Werks in digitalisierter Form ausreicht, damit § 52b UrhG als die Bibliotheken begünstigende Schranke ausscheidet. So spricht § 52b UrhG, der wiederum auf einer ähnlichen Formulierung in der Richtlinie basiert, davon, dass die Schrankenregelung nicht eingreift, wenn „vertragliche Regelungen" entgegenstehen.

Der Generalanwalt legt die entsprechenden Erwägungsgründe in der Richtlinie zunächst wörtlich aus: In diesen heißt es, dass „vertragliche Beziehungen" und der „Abschluss von Vereinbarungen" dazu führen können, dass die Schrankenregelung nicht eingreift. Insofern seien bestehende vertragliche Beziehungen zu verlangen, wohingegen bloße Lizenzaussichten nicht ausreichen könnten.

Doch auch systematische und mit Blick auf den Sinn und Zweck der Norm gerichtete Überlegungen ergeben für den Generalanwalt kein anderes Ergebnis. Zwar müsse eine Schrankenregelung wie die Bibliotheksschranke eng ausgelegt werden. Allerdings gehe es hier nicht um die Schranke selber, sondern nur um eine Ausnahme, wann sie nicht eingreife. Zudem würde ein gegenteiliges Verständnis dazu führen, dass der Rechteinhaber die gesamte Regelung mit bloßen Angeboten torpedie-

ren und die Norm jeglicher praktischer Bedeutung berauben könnte. Daher spreche auch das Telos der Norm – die Verbreitung von Wissen und Förderung von Kultur – für dieses Verständnis.

Vorherige Digitalisierung

Die Empfehlung des Generalanwalts auf die zweite Vorlagefrage des BGH erscheint im Ergebnis wenig überraschend. So fragte der BGH, ob die für die Nutzung von Werken an elektronischen Leseplätzen unentbehrliche Digitalisierung des Werkes auch von der Bibliotheksschranke erfasst ist (sog. Annexkompetenz) oder sich aus einer anderen Vorschrift der Richtlinie (Art. 5 Abs. 2 lit. c) herleite. Könnte sie weder aus der Bibliotheksschranke selbst noch aus der betreffenden anderen Vorschrift der Richtlinie hergleitet werden, würde dies den Anwendungsbereich der Bibliotheksschranke erheblich minimieren.

Dementsprechend kommt auch der Generalanwalt in Übereinstimmung mit den Erwägungen, die schon der BGH angestellt hatte, zu dem Schluss, dass die Digitalisierung der Werke zulässig ist. Allerdings müsse einschränkend beachtet werden, dass die Bestimmungen der Richtlinie nicht erlauben würden, ganze Bestände zu digitalisieren, sondern sich vielmehr auf einzelne Werke bezögen. Es sei unzulässig, wenn die Schrankenregelung dazu missbraucht würde, den Kauf ausreichend vieler physischer Vervielfältigungsstücke zu umgehen. Der Generalanwalt plädiert dafür, dass eine Erforderlichkeit für die Digitalisierung gegeben sein müsse und nennt als Beispiel die mögliche übermäßige Abnutzung durch eine Vielzahl von Kopien.

Ausdrucken und Speicherungsmöglichkeit auf USB-Sticks

In seiner Antwort auf die dritte Vorlagefrage beschäftigt sich der Generalanwalt mit der Frage, ob die Bibliotheksschranke so weit reicht, dass die Nutzer der elektronischen Leseplätze die dort zugänglich gemachten Werke ganz oder teilweise auf Papier ausdrucken oder auf einem USB-Stick abspeichern dürfen. Das bisherige Meinungsspektrum zu dieser Frage reichte von einer Differenzierung zwischen Ausdruck und Abspeicherung (so etwa die Ansicht des BGH) bis hin zu der Meinung, dass die spezifische Vorschrift in der Richtlinie überhaupt keine Antwort auf diese Frage gebe (Bundesregierung).

Nach den Erwägungen des Generalanwalts erlaubt die Bibliotheksschranke weder das Ausdrucken noch die Speicherungsmöglichkeit auf einem USB-Stick. Das ergebe sich daraus, dass die Bibliotheksschranke eine Einschränkung des Wiedergaberechts enthalte. Die Nutzung an den Leseterminals setze lediglich eine auf die Räumlichkeiten der Bibliothek beschränkte Wahrnehmung voraus. Bei einem Ausdruck und einer Speicherung handele es sich allerdings jeweils um Vervielfältigungshandlungen, die nicht erforderlich, sondern allenfalls dem Nutzer dienlich seien. Zugleich betont der Generalanwalt, dass sich die Möglichkeit eines Ausdrucks aber aus anderen Schrankenregelungen EU-rechtskonform ableiten könne. So finde ja auch bei Fotokopien zuerst eine Digitalisierung des Originals statt, bevor die analoge Kopie des Werks auf Papier erscheine.

III. Fazit und Konsequenzen für die Hochschulpraxis

Den Schlussanträgen des Generalanwalts zufolge ist der Weg für elektronische Leseplätze geebnet. Das beruht im Wesentlichen darauf, dass die Verlage die Bibliotheksschranke nicht durch das bloße Angebot eines Werks als E-Book außer Kraft setzen können. Dass das Angebot eines elektronischen Leseplatzes auch die vorherige Digitalisierung umfassen muss, erscheint logisch und notwendig. In diesen Punkten stellen sich die Schlussanträge des Generalanwalts als Sieg der Verfechter digitaler Leseplätze heraus. Die Interessen der Verlage werden allerdings in dem Punkt gewahrt, dass eine digitale Speicherungsmöglichkeit für Nutzer deutlich abgelehnt wird. Physische Vervielfältigungen, die gerechtfertigt werden können, lassen sich von einem digitalen Leseplatz aus zwar einfacher anfertigen, stellen jedoch keine wirklich „neue“ Rechteeinschränkung und wirtschaftliche Beeinträchtigung dar. Zu beachten ist überdies der Hinweis des Generalanwalts, dass sich die Vervielfältigung als notwendig erweisen muss. Beispiele für eine solche Notwendigkeit sind das Alter, die Zerbrechlichkeit, die Seltenheit oder aber auch die Häufigkeit der Nutzung des Werkes.

Aus Hochschulsicht können die Schlussanträge des Generalanwalts nur begrüßt werden. Erfreulich ist zudem, dass die Schlussanträge endlich für Rechtssicherheit sorgen können. Bevor nun aber mit einer raschen Umsetzung begonnen wird, sollte zumindest noch abgewartet werden, ob der EuGH den Schlussanträgen auch tatsächlich Folge leistet. Das ist in aller Regel der Fall – zumal die Ausführungen des Generalanwalts schlüssig sind und überzeugen können. Es deutet also alles darauf hin, dass auch die Bibliotheken – rechtssicher – in der digitalen Welt ankommen können. ◆

Anmerkungen:

Ebenfalls zu § 52b UrhG bereits: Wörheide, DFN-Infobrief Recht 6/2012, S. 2 f.
Bröckers, DFN-Infobrief Recht 6/2009, S. 7 f.

Das mach' ich doch mit Links!

Oberlandesgericht Köln verneint Zueigenmachen fremder Inhalte allein durch Link mit empfehlender Ankündigung

Die Haftung eines Linksetzers für verlinkte fremde Inhalte im Internet hängt im Wesentlichen davon ab, ob der Linksetzer sich die fremden Inhalte zu eigen gemacht hat und sie deshalb wie eigene Inhalte behandelt werden müssen, für die keinerlei Haftungsprivilegierungen bestehen. Das Oberlandesgericht (OLG) Köln hat nun im Hinblick auf eine wettbewerbsrechtliche Streitigkeit mit Urteil vom 19.02.2014 (Az. 6 U 49/13) entschieden, dass das Setzen eines Links auf der eigenen Internetseite zur Startseite eines fremden Internetauftritts auch bei einer empfehlenden Ankündigung regelmäßig nicht genügt, um darin schon ein Zueigenmachen bestimmter rechtswidriger Inhalte auf Unterseiten des fremden Internetauftritts zu sehen.

Text: **Florian Klein** (Forschungsstelle Recht im DFN)

Hintergrund

Elektronische Verweise (Links) auf fremde Informationen sind im Internet ein sehr beliebtes und praktisches Hilfsmittel, um Nutzern einer Webseite weitergehende Informationen zukommen zu lassen oder sie auf ähnliche Informationsangebote hinzuweisen. Für den Linksetzer hat dies den Vorteil, dass er sich eigene Recherchen oder Erläuterungen ersparen kann, ohne dass dadurch ein Informationsdefizit beim Nutzer entstünde. Letzterer wiederum kann sich ohne großen Aufwand von einer Quelle zur anderen durchklicken und ist nicht auf das Angebot eines einzigen Informanten beschränkt. Rechtlich brisant wird das Setzen eines Links potentiell dann, wenn die verlinkten fremden Inhalte in irgendeiner Weise rechtsverletzend sind. Hier stellt sich nämlich stets die Frage, inwiefern neben dem unmittelbaren Anbieter der rechtswidrigen Inhalte auch der Linksetzer für die Rechtsverletzung einzustehen hat. Da der Gesetzgeber diese Problematik ganz bewusst nicht spezialgesetzlich geregelt hat, sind die Gerichte berufen, diese Frage anhand der allgemeinen Haftungsgrundsätze zu beantworten.

Insofern gilt zunächst, dass stets an die Möglichkeit einer Haftung als Störer auf Unterlassen bzw. Beseitigung der Rechtsverletzung zu denken ist, die jedoch von der Verletzung zumutbarer Prüfungspflichten abhängig ist (s. hierzu vertiefend den DFN-Rechtsguide unter III. 3. b), https://www.dfn.de/rechtimdfn/rgwb/rechtsguide/rg-kapitel3/#c11723).

Darüber hinaus kommt allerdings auch eine weitergehende, täterschaftliche Haftung in Betracht, die neben Unterlassungs- und Beseitigungsansprüchen nicht nur Schadensersatzansprüche auslösen, sondern – je nach betroffenem Inhalt – unter Umständen auch strafrechtliche Konsequenzen haben kann. Eine so weitgehende Haftung ist jedoch nur möglich, wenn die fremden rechtswidrigen Inhalte durch das Setzen des Links „zu eigen gemacht“ werden. Wann dies allerdings gegeben ist, hängt von sämtlichen Umständen des Einzelfalls ab und kann mitunter nur schwierig beurteilt werden. Aus der Rechtsprechung lassen sich insofern bisher allenfalls Indizien entnehmen, ohne dass es eine sichere Beurteilungsgrundlage gäbe.

Die Entscheidung des Gerichts

Für einen Link mit empfehlender Ankündigung, der auf die Startseite eines fremden Internetauftritts verweist, auf dessen Un-

Foto © .marqs/photocase.de

terseite sich rechtswidrige Inhalte befinden, hat das OLG Köln in seinem Urteil ein Zueigenmachen abgelehnt.

1. Sachverhalt

Der Entscheidung des OLG Köln lag ein wettbewerbsrechtlicher Sachverhalt zugrunde, in dem es konkret um die Zulässigkeit bestimmter Werbemaßnahmen für Heilmittel ging. Der beklagte Orthopäde hatte auf seiner Internetseite für eine von ihm angebotene spezielle Akupunkturbehandlung geworben. Am Ende des entsprechenden Werbe- und Informationstextes hatte er die Ankündigung „Weitere Informationen auch über die Studienlage finden Sie unter …“ eingefügt und einen Link eingesetzt. Dieser Link führte zur Startseite der Internetpräsenz eines Forschungsverbandes zur Implantatakupunktur. Erst auf Unterseiten dieser Internetpräsenz des Forschungsverbandes befanden sich die streitgegenständlichen, als irreführend beanstandeten Werbeaussagen über Anwendungsgebiet und Wirkung der Therapie. Allein wegen dieser Verlinkung auf die Startseite mahnte die Klägerin (ein Wettbewerbsverein) den Orthopäden ab, der daraufhin den Link entfernte, aber die Abgabe einer Unterlassungserklärung verweigerte. Aus diesem Grund beschritt die Klägerin nachfolgend den Rechtsweg und forderte Unterlassung bestimmter Werbeaussagen sowie Ersatz der Abmahnkosten.

2. Urteil

Das OLG Köln gab jedoch dem Beklagten Recht und lehnte sowohl einen Anspruch auf Unterlassung als auch auf Ersatz der Abmahnkosten ab, weil die vermeintlich irreführenden Werbeaussagen auf der verlinkten Internetseite des Forschungsverbandes Implantatakupunktur dem Orthopäden nicht zuzurechnen seien.

Vorliegen einer geschäftlichen Handlung/Werbung

Die Aussagen auf dieser Internetseite und der auf diese verweisende Link auf der Webseite des Orthopäden seien als geschäftliche Handlung und als Werbung für eine von ihm angebotene Behandlungsmethode anzusehen, was Grundvoraussetzung für das Bestehen eines wettbewerbsrechtlichen Unterlassungsanspruchs ist. Denn es sei klar ersichtlich, dass diese Veröffentlichung objektiv (auch) dem Zweck diene, Internetnutzern das Dienstleistungsangebot des Beklagten nahe zu bringen und dafür zu werben. Insofern könne der Link auch nicht isoliert von der Werbehandlung betrachtet werden. Selbst wenn die verlinkte Seite gar nicht der Förderung geschäftlicher Interessen, sondern bloß der Information oder Meinungsbildung diene, verliere der Link nicht seinen werblichen Charakter, weil sich der beklagte Orthopäde durch Setzung des Links weiterführende Darstellungen erspart und den Verweis auf die fremde Webseite mit den dort vorgehaltenen Informationen für seinen eigenen werblichen Auftritt nutzbar gemacht habe.

Zueigenmachen als Zurechnungsvoraussetzung

Allerdings folge allein daraus noch nicht, dass der beklagte Orthopäde für sämtliche Informationen auf der verlinkten Webseite des Forschungsverbandes einzustehen habe. Insofern fehlt es den Richtern nämlich an einem Zueigenmachen der fremden Inhalte durch das Setzen des Links, welches es rechtfertigen würde, die fremden Inhalte wie eigene Werbeaussagen zu betrachten.

Zunächst stellt das Gericht fest, dass die Link-Haftung vom Gesetzgeber bewusst nicht geregelt worden sei und sie sich deshalb nach den allgemeinen Vorschriften richte. Demnach hafte derjenige, der sich fremde Informationen zu eigen macht, auf die er mittels eines Hyperlinks verweist, dafür wie für selbst geschaffene Inhalte. Ob ein solches Zueigenmachen vorliege, sei aus der objektiven Sicht eines verständigen Durchschnittsnutzers auf der Grundlage einer Gesamtbetrachtung aller relevanten Umstände zu beurteilen.

Zusammenfassung der höchstrichterlichen Rechtsprechung zum Zueigenmachen

Um die Frage auch im konkreten Fall beantworten zu können, fassen die Richter im Folgenden die höchstrichterlichen Entscheidungen der letzten Jahre zu diesem Thema zusammen und ermitteln daraus, welche Umstände für das Zueigenmachen als relevant anzusehen seien und wo die Grenze zwischen einem bloßen Verweis auf fremde Äußerungen und einer Übernahme von Verantwortung für ihren Inhalt verlaufe.

Im Grundsatzurteil „Schöner Wetten“ (Az. I ZR 317/01) hat der Bundesgerichtshof (BGH) eine Störerhaftung des Linksetzers verneint, weil der dort gesetzte Link auf die Internetseite eines Anbieters von (illegalen) Glücksspielen nur der Ergänzung eines Online-Presseartikels über die hinter diesem Angebot stehende Unternehmerin und deren Model-Karriere diene und damit die Einholung weiterer Informationen ermögliche. Da sich die Rechtswidrigkeit der fremden Inhalte in diesem Fall nicht aufgedrängt habe, seien keine Prüfpflichten verletzt worden. Außerdem habe sich der Linksetzer die Inhalte weder zu eigen gemacht noch die Internetnutzer außerhalb des redaktionellen Beitrags zur Kontaktaufnahme mit dem Unternehmen oder gar zur Glücksspielteilnahme angeregt. Besonders zu berücksichtigen sei auch, dass im Interesse der Meinungs- und Pressefreiheit keine zu strengen Anforderungen an das Setzen von Links gestellt werden dürften, die den Zugang zu allgemein zugänglichen Quellen erleichtern. Denn erst durch den Einsatz von Links könne die enorme Informationsfülle des Internets sinnvoll erschlossen werden.

In einem anderen Fall, in dem es um einen Anbieter von Altersverifikationssystemen ging, der auf seiner Webseite Links zu Seiten mit pornographischen Inhalten gesetzt hatte, hat der BGH

(Az. I ZR 102/05) dagegen ein Zueigenmachen und damit eine Zurechnung bejaht, weil die Links elementarer Bestandteil der Geschäftsidee seien und es dem Anbieter gerade darauf angekommen sei, seinen Nutzern einen gebündelten Zugang zu den pornographischen Webseiten seiner Kunden anzubieten.

In einer dritten Entscheidung urteilte der BGH (Az. VI ZR 210/08), dass der Verbreiter einer fremden Äußerung sich diese nur dann zu eigen mache, wenn er sich so mit ihr identifiziere, dass sie als seine eigene erscheine, wobei Zurückhaltung bei der Bejahung einer solchen Identifizierung geboten sei. So reiche dafür beispielsweise die Wiedergabe einer Domain auf dem Titelblatt eines Printmagazins nicht aus, wenn dadurch dem Leser nur aufgezeigt werden solle, unter welcher Domain die dort erschienenen Artikel online abrufbar seien.

Im Fall „marions-kochbuch.de“ (Az. I ZR 166/07) hatten Nutzer der Konkurrenzseite „chefkoch.de“ Fotos von zubereiteten Gerichten aus der Online-Rezeptsammlung „marions-kochbuch.de“ kopiert und hochgeladen. Für den darin liegenden Urheberrechtsverstoß musste der Betreiber von „chefkoch.de“ haften, weil der BGH ein Zueigenmachen der von den Nutzern hochgeladenen Inhalte durch ihn bejaht hatte. Entscheidend für diese Beurteilung war, dass der Betreiber tatsächlich und nach außen sichtbar die inhaltliche Verantwortung für die auf seiner Seite veröffentlichten Rezepte und Abbildungen übernommen hatte, indem er die Bilder unter anderem mit seinem Kochmützen-Emblem versehen und sie als Kerngehalte seiner Seite nur nach redaktioneller Kontrolle zugänglich gemacht hatte.

Große Bedeutung kommt überdies dem BGH-Urteil „AnyDVD“ (Az. I ZR 191/08) aus dem Jahr 2010 zu. Darin sei klargestellt worden, dass bei der Linkhaftung immer eine umfassende Interessenabwägung im Einzelfall erforderlich sei, bei der nicht künstlich zwischen der technischen Funktion und der inhaltlichen Dimension eines Links unterschieden werden dürfe. Eine Haftung des Linksetzers sei immer dann ausgeschlossen, wenn es zulässig war, über das als rechtswidrig erkannte Angebot der verlinkten fremden Seite zu berichten (im konkreten Fall ging es um Software zur Umgehung von Kopierschutz auf DVDs) und die Berichterstattung des Linksetzers in distanzierter Weise erfolgte, was gerade kein Zueigenmachen darstelle. Quintessenz aus diesem Urteil ist nach Ansicht von Vertretern des Schrifttums, dass die bloße Empfehlung eines Beitrags per Link noch kein hinreichendes Indiz für eine Identifikation mit der rechtsverletzenden Äußerung dergestalt sein könne, dass der Linksetzer auch die Verantwortung für die fremden Inhalte übernehmen wolle. Dementsprechend könne allein aus dem Setzen eines Links, der für die eigene Veröffentlichung von inhaltlicher Bedeutung ist, noch nicht auf ein Zueigenmachen geschlossen werden.

In einem letzten Fall ging es vor dem BGH (Az. I ZR 147/09) schließlich um einen Link in einem Newsletter, der auf redaktionelle Artikel eines Dritten verwies, in denen sich wettbewerbsrechtsverletzende (da herabsetzende) Äußerungen fanden. Der Ersteller des Newsletters habe den Link ersichtlich als Beleg und Ergänzung für von ihm geäußerte eigene Ansichten verwendet. Ziel der Linksetzung sei nicht nur die technische Erleichterung des Abrufs der betreffenden Internetseiten gewesen, sondern die unmittelbare Erschließung zusätzlicher Informationsquellen für die Leser des Newsletters, die für das weitergehende Verständnis der vom Newsletter-Ersteller geäußerten Meinung erkennbar von Bedeutung gewesen seien. Die beanstandete allgemeine Herabsetzung anderer Wettbewerber wurde nämlich erst durch die verlinkten Artikel auf einzelne Wettbewerber konkretisiert. Insofern sei mit der Setzung der Links gerade auch bezweckt worden, dass die Leser die verlinkten Artikel zur Kenntnis nehmen, wodurch der Inhalt der Artikel Bestandteil der Stellungnahme des beklagten Newsletter-Erstellers geworden sei.

Anwendung im konkreten Fall

Für den konkreten Fall leiten die Kölner Richter aus dieser Synopse der höchstrichterlichen Rechtsprechung den Grundsatz ab, dass das Setzen eines Links auf die Startseite eines fremden Internetauftritts unabhängig vom empfehlenden Charakter des Links noch nicht ausreiche, um annehmen zu können, dass sich der Linksetzer mit einem irreführenden und daher (wettbewerbs-) rechtsverletzenden Inhalt identifiziere. Insofern sei auch ein Zueigenmachen nicht gegeben.

Zwar habe durch den Hinweis „Weitere Informationen auch über die Studienlage finden Sie unter [Link]“ keine eindeutige Distanzierung von den dort befindlichen Angaben stattgefunden. Aus objektiver Sicht eines verständigen Durchschnittsnutzers habe es der Orthopäde aber erst recht nicht darauf angelegt, die Besucher seiner Seite über den Link gerade zu den inkriminierten Aussagen weiterzuleiten. Weder erschienen seine eigenen Werbeaussagen ohne Nutzung des Links unvollständig oder unverständlich noch seien die verlinkten Inhalte insgesamt oder in konkret abgrenzbarem Umfang als wesentlich für die objektive Zwecksetzung seines eigenen Internetauftritts anzusehen, welche darin bestehe, die Nutzer für die von ihm angebotenen besonderen Akupunkturbehandlungen zu interessieren.

Die Richter sehen den Link mit der vorangestellten Ankündigung eher wie einen abschließenden Hinweis auf weiterführende Literatur am Ende eines Zeitschriftenartikels, durch welchen der Verfasser genauso wenig seine ungeteilte Zustimmung zu allen in der angegebenen Literatur vertretenen Auffassungen ausdrücke. Selbst angesichts der Tatsache, dass der Link auch in gewis-

ser Hinsicht empfehlend wirke, könne man ihm keine so starke Identifikation mit bestimmten Inhalten entnehmen, dass allein daraus auf eine Übernahme der Verantwortung für diese Inhalte geschlossen werden könnte.

Darüber hinaus sei schließlich noch zu berücksichtigen, dass der Link gerade nicht unmittelbar zu den beanstandeten, rechtswidrigen Äußerungen führte, sondern nur zu der als solchen unbedenklichen Startseite des Internetauftritts des Forschungsverbandes, von welcher aus auch andere (rechtmäßige) Inhalte abgerufen werden konnten. Fernliegend sei dabei die Ansicht, dass der Orthopäde durch seinen Link die volle Verantwortung für den gesamten Inhalt der Webpräsenz einschließlich all ihrer Unterseiten übernommen habe.

Im Übrigen habe der Orthopäde den Link unmittelbar nach der Abmahnung von seiner Internetseite entfernt, sodass ihm auch insoweit keine weitergehende Rechtsverletzung zur Last gelegt werden könne.

Fazit und Konsequenzen für die Hochschulpraxis

Positiv hervorzuheben ist, dass das Urteil des OLG Köln zunächst eine übersichtliche Zusammenfassung der bisherigen höchstrichterlichen Urteile zu den verschiedenen Konstellationen gibt, in denen ein Zueigenmachen thematisiert wurde. Auf einen Blick kann man sich dadurch über die verschiedenen Ansätze des BGH informieren.

Erfreulich ist auch, dass die Haftung für Links nicht über Gebühr ausgeweitet wurde. Denn es besteht ein erhebliches praktisches Bedürfnis dafür, beim Einsatz von Links nicht sämtliche Unterseiten eines verlinkten Internetauftritts auf Rechtsverletzungen überprüfen zu müssen. Gerade beim geplanten Einsatz mehrerer elektronischer Verweise oder bei der Verlinkung sehr umfangreicher Internetpräsenzen wäre damit ein Aufwand verbunden, der praktisch kaum zu tragen wäre. Würde deshalb teilweise auf den Einsatz von Links verzichtet, wäre der freie Informationsfluss im Internet nicht unerheblich behindert. Hier zeigt das OLG Köln also das nötige Fingerspitzengefühl.

Foto © Superbass

Letztlich darf die Entscheidung des OLG Köln jedoch auch nicht überbewertet werden, da gerade bei der Frage des Zueigenmachens stets eine Einzelfallbetrachtung angezeigt ist, die schon bei geringfügig anderen Umständen des Falles zu einem gegenteiligen Ergebnis führen kann. Ein größeres Maß an Rechtssicherheit für Linksetzer wäre hier durchaus wünschenswert.

In der Praxis sollte man grundsätzlich darauf achten, bei der Verwendung von Links möglichst den objektiven Eindruck hervorzurufen, dass man sich von den verlinkten Inhalten distanziert bzw. keine Verantwortung für diese tragen möchte. Eine Überprüfung der gesamten verlinkten Webpräsenz kann in Konstellationen wie der des vorliegenden Falles unter Umständen verzichtbar sein. Disclaimern kommt insofern aber allenfalls geringe Indizwirkung zu, ein Allheilmittel stellen sie keinesfalls dar. Besondere Vorsicht ist geboten, wenn die eigenen Ausführungen unvollständig oder unverständlich sind und sich das Gesamtbild nur mithilfe der verlinkten Inhalte erschließt. Hier liegt die Annahme eines Zueigenmachens sehr nahe, sodass in einem solchen Fall eine Rechtmäßigkeitsprüfung der verlinkten Inhalte erfolgen sollte. Führt ein Link dagegen zu einer Seite, auf der sich ausschließlich weiterführende Informationen finden, die für die eigenen Aussagen zunächst ohne Belang sind, die den dargestellten Sachverhalt aus anderer Perspektive beleuchten und bei denen klar ist, dass sie die Ansicht eines Dritten darstellen, dürfte ein Zueigenmachen eher selten bejaht werden.

Darüber hinaus wird wohl auch bei Deep Links, die direkt zu der Unterseite mit den relevanten Informationen führen, eher von einem Zueigenmachen auszugehen sein, zumal eine Überprüfung der konkret verlinkten Unterseite regelmäßig zumutbar ist.

Zumindest im Rahmen journalistisch-redaktioneller Angebote gewährt die Rechtsprechung Linksetzern aber einen größeren Handlungsspielraum, da insofern die Meinungs- oder Pressefreiheit für den Linksetzer streitet.

Unabhängig von der Frage des Zueigenmachens beim Setzen eines Links sollte spätestens bei einem Hinweis auf die potentielle Rechtswidrigkeit verlinkter Inhalte unverzüglich überprüft werden, ob der jeweilige Hinweis zu Recht eine Beanstandung der Inhalte vornimmt, und dann umgehend durch Entfernung des Links reagiert werden. ◆

Übersicht über die Mitgliedseinrichtungen und Organe des DFN-Vereins

(Stand: 11/2014)

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

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

Die Organe des DFN-Vereins sind:

die Mitgliederversammlung
der Verwaltungsrat
der Vorstand

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

Verwaltungsrat
Der Verwaltungsrat beschließt alle wesentlichen Aktivitäten des Vereins, insbesondere die technisch-wissenschaftlichen Arbeiten und berät den Jahreswirtschaftsplan. Für die 10. Wahlperiode sind Mitglieder des Verwaltungsrates:
Prof. Dr. Hans-Joachim Bungartz (TU München)
Prof. Dr. Rainer W. Gerling (MPG München)
Prof. Dr. Ulrike Gutheil (TU Berlin)
Dir. u. Prof. Dr. Siegfried Hackel (PTB Braunschweig)
Dr.-Ing.habil. Carlos Härtel (GE Global Research)
Prof. Dr.-Ing. Ulrich Lang (Univ. zu Köln)
Prof. Dr. Joachim Mnich (DESY)
Prof. Dr. Wolfgang E. Nagel (TU Dresden)
Prof. Dr. Bernhard Neumair (KIT)
Dr.-Ing. Christa Radloff (Univ. Rostock)
Prof. Dr. Peter Schirmbacher (HU zu Berlin)
Dr. Wolfgang A. Slaby (Kath. Univ. Eichstätt-Ingolstadt)
Prof. Dr. Horst Stenzel (FH Köln)

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

einen Vertreter der HRK:
gegenwärtig Herr Prof. Dr. Andreas Bertram (Präsident der Hochschule Osnabrück)

einen Vertreter der Hochschulkanzler:
Herr Christian Zens (Kanzler der Stiftung Europa-Universität Viadrina)

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

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

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

Prof. Dr. Hans-Joachim Bungartz, Vorsitz
Prof. Dr. Ulrike Gutheil
Prof. Dr. Bernhard Neumair

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

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

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

Erlangen	Friedrich-Alexander-Universität Erlangen-Nürnberg
Essen	Rheinisch-Westfälisches Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Fachhochschule Flensburg
	Universität Flensburg
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Deutsche Nationalbibliothek
	Deutsches Institut für Internationale Pädagogische Forschung
	Frankfurt University of Applied Science
	Johann Wolfgang Goethe-Universität Frankfurt am Main
	KPN EuroRings B.V.
	Philosophisch-Theologische Hochschule St. Georgen e.V.
	Senckenberg Gesellschaft für Naturforschung
	Stonesoft Germany GmbH
Frankfurt/O.	IHP GmbH – Institut für innovative Mikroelektronik
	Stiftung Europa-Universität Viadrina
Freiberg	Technische Universität Bergakademie Freiberg
Freiburg	Albert-Ludwigs-Universität Freiburg
Freising	Hochschule Weihenstephan
Friedrichshafen	Zeppelin Universität gGmbH
Fulda	Hochschule Fulda
Furtwangen	Hochschule Furtwangen – Informatik, Technik, Wirtschaft, Medien
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit mbH
	Leibniz-Rechenzentrum d. Bayerischen Akademie der Wissenschaften
Gatersleben	Leibniz-Institut für Pflanzengenetik und Kulturpflanzenforschung (IPK)
Geesthacht	Helmholtz-Zentrum Geesthacht Zentrum für Material- und Küstenforschung GmbH
Gelsenkirchen	Westfälische Hochschule
Gießen	Technische Hochschule Mittelhessen
	Justus-Liebig-Universität Gießen
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GwDG)
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	Ernst-Moritz-Arndt-Universität Greifswald
	Friedrich-Loeffler-Institut, Bundesforschungsinstitut für Tiergesundheit
Hagen	Fachhochschule Südwestfalen, Hochschule für Technik und Wirtschaft
	FernUniversität in Hagen
Halle/Saale	Institut für Wirtschaftsforschung Halle
	Martin-Luther-Universität Halle-Wittenberg
Hamburg	Bundesamt für Seeschifffahrt und Hydrographie
	Datenlotsen Informationssysteme GmbH
	Deutsches Elektronen-Synchrotron (DESY)
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	DFN – CERT Services GmbH
	HafenCity Universität Hamburg
	Helmut-Schmidt-Universität, Universität der Bundeswehr
	Hochschule für Angewandte Wissenschaften Hamburg
	Hochschule für Bildende Künste Hamburg
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg-Harburg
	Universität Hamburg
Hameln	Hochschule Weserbergland
Hamm	SRH Hochschule für Logistik und Wirtschaft Hamm
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe
	Hochschule Hannover
	Gottfried Wilhelm Leibniz Bibliothek – Niedersächsische Landesbibliothek
	Gottfried Wilhelm Leibniz Universität Hannover
	HIS Hochschul-Informations-System GmbH
	Hochschule für Musik, Theater und Medien
	Landesamt für Bergbau, Energie und Geologie
	Medizinische Hochschule Hannover
	Technische Informationsbibliothek und Universitätsbibliothek
	Stiftung Tierärztliche Hochschule
Heide	Fachhochschule Westküste, Hochschule für Wirtschaft und Technik
Heidelberg	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	Network Laboratories NEC Europe Ltd.
	Ruprecht-Karls-Universität Heidelberg
Heilbronn	Hochschule für Technik, Wirtschaft und Informatik Heilbronn
Hildesheim	Hochschule für angewandte Wissenschaft und Kunst Fachhochschule Hildesheim/Holzminden/Göttingen
	Stiftung Universität Hildesheim
Hof	Hochschule für angewandte Wissenschaften Hof – FH
Ilmenau	Bundesanstalt für IT-Dienstleistungen im Geschäftsbereich des BMVBS
	Technische Universität Ilmenau
Ingolstadt	DiZ – Zentrum für Hochschuldidaktik d. bayerischen Fachhochschulen
	Hochschule für angewandte Wissenschaften FH Ingolstadt
Jena	Ernst-Abbe-Hochschule Jena
	Friedrich-Schiller-Universität Jena
	Leibniz-Institut für Photonische Technologien e. V.
	Leibniz-Institut für Altersforschung – Fritz-Lipmann-Institut e. V. (FLI)
Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Fachhochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	Fachinformationszentrum Karlsruhe (FIZ)
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe – Technik und Wirtschaft
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Hochschule für angewandte Wissenschaften, Fachhochschule Kempten
Kiel	Christian-Albrechts-Universität zu Kiel
	Fachhochschule Kiel
	Institut für Weltwirtschaft an der Universität Kiel
	Helmholtz-Zentrum für Ozeanforschung Kiel (GEOMAR)
	ZBW – Deutsche Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft
Koblenz	Hochschule Koblenz
Köln	Deutsche Sporthochschule Köln
	Fachhochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Katholische Hochschule Nordrhein-Westfalen
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln gGmbH
	Universität zu Köln
Konstanz	Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)
	Universität Konstanz
Köthen	Hochschule Anhalt
Krefeld	Hochschule Niederrhein

Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e. V.
Landshut	Hochschule Landshut - Hochschule für angewandte Wissenschaften
Leipzig	Deutsche Telekom, Hochschule für Telekommunikation Leipzig
	Helmholtz-Zentrum für Umweltforschung – UFZ GmbH
	Hochschule für Grafik und Buchkunst Leipzig
	Hochschule für Musik und Theater „Felix Mendelssohn Bartholdy“
	Hochschule für Technik, Wirtschaft und Kultur Leipzig
	Leibniz-Institut für Troposphärenforschung e. V.
	Mitteldeutscher Rundfunk
	Universität Leipzig
Lemgo	Hochschule Ostwestfalen-Lippe
Lübeck	Fachhochschule Lübeck
	Universität zu Lübeck
Ludwigsburg	Evangelische Hochschule Ludwigsburg
Ludwigshafen	Fachhochschule Ludwigshafen am Rhein
Lüneburg	Leuphana Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Leibniz-Institut für Neurobiologie Magdeburg
Mainz	Fachhochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Universität Koblenz-Landau
Mannheim	Hochschule Mannheim
	TÜV SÜD Energietechnik GmbH Baden-Württemberg
	Universität Mannheim
	Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW)
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Philipps-Universität Marburg
Merseburg	Hochschule Merseburg (FH)
Mittweida	Hochschule Mittweida
Mülheim an der Ruhr	Hochschule Ruhr West
Müncheberg	Leibniz-Zentrum für Agrarlandschafts- u. Landnutzungsforschung e. V.
München	Bayerische Staatsbibliothek
	Hochschule München (FH)
	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.
	Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt GmbH
	ifo Institut – Leibniz-Institut für Wirtschaftsforschung e. V.
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft
	Technische Universität München
	Universität der Bundeswehr München
Münster	Fachhochschule Münster
	Westfälische Wilhelms-Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neu-Ulm	Hochschule für Angewandte Wissenschaften, Fachhochschule Neu-Ulm
Nordhausen	Fachhochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
Nürtingen	Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen
Nuthetal	Deutsches Institut für Ernährungsforschung Potsdam-Rehbrücke
Oberwolfach	Mathematisches Forschungsinstitut Oberwolfach gGmbH
Offenbach/M.	Deutscher Wetterdienst (DWD)
Offenburg	Hochschule Offenburg, Fachhochschule
Oldenburg	Carl von Ossietzky Universität Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück (FH)
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Deutsche Gesellschaft zum Bau und Betrieb von Endlagern für Abfallstoffe mbH
Potsdam	Fachhochschule Potsdam
	Helmholtz-Zentrum, Deutsches GeoForschungsZentrum – GFZ
	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam-Institut für Klimafolgenforschung (PIK)
	Universität Potsdam
Regensburg	Ostbayerische Technische Hochschule Regensburg
	Universität Regensburg
Rosenheim	Hochschule für angewandte Wissenschaften – Fachhochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn Rhein-Sieg
Schmalkalden	Fachhochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Siegen	Universität Siegen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Fachhochschule Stralsund
Stuttgart	Cisco Systems GmbH
	Duale Hochschule Baden-Württemberg
	Hochschule der Medien Stuttgart
	Hochschule für Technik Stuttgart
	NextiraOne Deutschland GmbH
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte Tautenburg
Trier	Hochschule Trier
	Universität Trier
Tübingen	Eberhard Karls Universität Tübingen
	Leibniz-Institut für Wissensmedien
Ulm	Hochschule Ulm
	Universität Ulm
Vechta	Universität Vechta
	Private Fachhochschule für Wirtschaft und Technik
Wadern	Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH (LZI)
Weimar	Bauhaus-Universität Weimar
	Hochschule für Musik FRANZ LISZT Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz
Weßling	T-Systems Solutions for Research GmbH
Wiesbaden	Hochschule RheinMain
	Statistisches Bundesamt
Wildau	Technische Hochschule Wildau (FH)
Wilhelmshaven	Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth

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