IT-Dienstleistung

An jedem Ort, zu jeder Zeit: Mobilität im „Netz“

Wissenschaftler und Studierende sind heute weltweit unterwegs, schicken binnen Sekunden Daten auf andere Kontinente, lehren und lernen per Video und Livestream. Dazu benötigen sie eine professionelle Infrastruktur. Das Leibniz-Rechenzentrum sorgt dafür, dass im Münchner Wissenschaftsnetz (MWN) und darüber hinaus alles reibungslos und auch mobil funktioniert.

Von Helmut Reiser

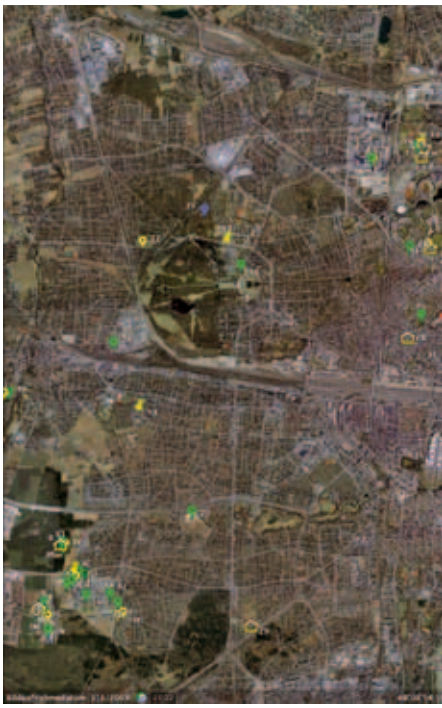

ABB.: GOOGLE EARTH

DAS „NETZ“ IST heute eine unverzichtbare Basisinfrastruktur für jeden Wissenschaftler, Studierenden und Mitarbeiter, ob an einer Hochschule oder einer außeruniversitären Forschungseinrichtung. Und genau so wird es auch wahrgenommen: Das „Netz“ ist einfach da, es funktioniert immer und am besten überall. Parallel dazu ist die sog. pervasive Universität entstanden, also eine Universität, die didaktisch, technisch und organisatorisch pervasive Lehr- und Lernumgebungen unterstützt (s. H.-G. Hegering et al. 2009 im Literaturverzeichnis S. 33). Lernen und Lehren sind dabei nicht mehr nur auf Hörsäle, Seminarräume oder Bibliotheken beschränkt, sondern finden überall und potentiell zu jeder Zeit statt. So gibt es heute z. B. bereits viele Vorlesungen, die per Video aufgezeichnet und über einen Streaming-Server abgerufen werden können. Pervasives Lernen und Lehren werden auch durch neue, leistungsfähige und einfach zu benutzende mobile Geräte unterstützt und stark gefördert. Viele dieser Geräte (Smartphones, Tablet-Computer, MP3-Player, etc.) gelten als schick und „trendy“, was in den letzten Jahren sicher auch zur extrem großen Verbreitung beigetragen hat. Diese Geräteklasse lässt sich in der Regel gar nicht mehr ans Festnetz anschließen. Eine Kommunikation bzw. Verbindung mit dem Internet ist ausschließlich über Funk möglich.

Auch in der europäischen Universitäts- und Forschungslandschaft wird eine wachsende Bedeutung der Mobilität, sowohl bei den Netzen als auch den Anwendungen, festgestellt. Die Europäische Kommission spricht im Strategiepapier „GÉANT 2020“ gar von einer Welt allgegenwärtiger Konnektivität.

Diese Entwicklungen führen dazu, dass Lernende und Lehrende gleichermaßen hohe Anforderungen an die mobile Nutzung von Kommunikationsnetzen und Diensten stellen. Dies verlangt von dem Betreiber einer Kommunikationsinfrastruktur sowohl technische als auch administrative Unterstützung. Grundbaustein dieser Vernetzung, für Wissenschaftler und Studenten im Großraum München, ist das Münchner Wissenschaftsnetz (MWN).

Münchner Wissenschaftsnetz

Das Münchner Wissenschaftsnetz versorgt alle Münchner Universitäten, Hochschulen und viele weitere Forschungseinrichtungen. Es wird zwar weiterhin als Münchner Wissenschaftsnetz bezeichnet, geht aber heute in seiner räumlichen Ausdehnung weit über die Stadt München hinaus. Derzeit werden gut 120.000 Nutzer in mehr als 540 Gebäudekomplexen über das MWN erschlossen. Neben einer hohen Bandbreite (derzeit 10 Gbit/s im Backbone und zum DFN/Internet) und einer flächendeckenden Versorgung wird der ausfallsichere Betrieb immer wichtiger. Zusätzlich zu dem primären Internetzugang über das Deutsche Forschungsnetz (DFN) gibt es einen redundanten Anschluss an den lokalen Provider M-net. Das Backbone-Netz wird von 12 Routern gebildet, an denen über kaskadierte Switches und über eine strukturierte Verkabelung die Nutzer versorgt werden. Gegenwärtig betreibt das LRZ knapp 1.300 Switches mit ins-

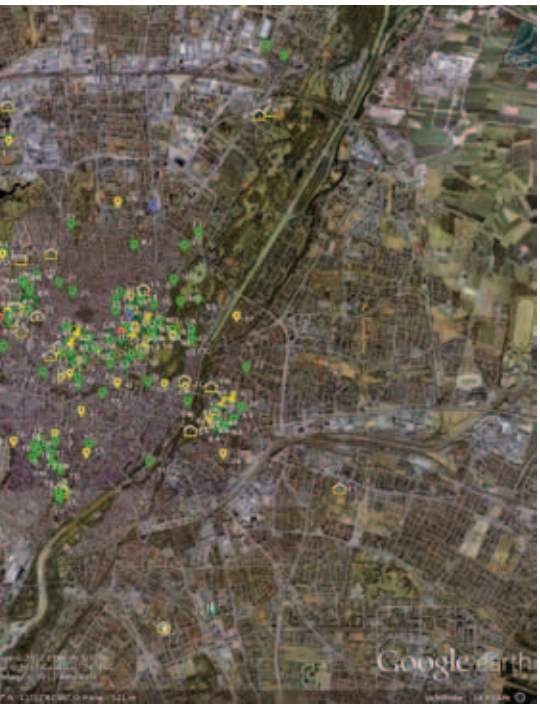

Abb. 1: Unkomplizierter Internetzugang: Standorte im Münchner Wissenschaftsnetz mit WLAN im Münchner Stadtgebiet.

gesamt fast 90.000 Ports. Diese Basisinfrastruktur bildet das Fundament, auf dem die mobile Nutzung aufsetzen kann.

Mobile Nutzung von IT-Diensten

Die mobile Nutzung von IT-Diensten lässt sich durch die vier primären Mobilitätsformen, also Endgeräte-, Personen-, Dienst- und Sitzungsmobilität, charakterisieren.

Die Endgerätemobilität ist die Form, an die man primär denkt: Ein Nutzer ist in der Lage, sein Endgerät an verschiedenen Orten zu bewegen, aber auch ganz einfach „unterwegs" zu nutzen. Ein klassisches Beispiel hierfür ist die Nutzung eines Smartphones, Tablet-Computers oder Laptops.

Die Personenmobilität umfasst die Möglichkeit eines Nutzers, seine Endgeräte zu wechseln, gleichzeitig aber seine Identität im Netz aufrechtzuerhalten. Es werden also die verschiedenen Geräte eines Nutzers unterstützt. Daraus leiten sich Fragen des Identitätsmanagements sowie Authentisierungsmechanismen ab, aber auch die technische Unterstützung für verschiedenste Gerätetypen und Betriebssysteme.

Die Dienstmobilität bedeutet, dass Dienste netz-, betreiber- und geräteübergreifend angeboten werden. Um beim Beispiel der Vorlesungsaufzeichnung zu bleiben, bedeutet dies, dass das Video (z. B. dessen Auflösung) an das gerade verwendete Gerät (z. B. Smartphone, Tablet oder Laptop) angepasst wird und aus verschiedenen Netzen und über verschiedene Provider erreichbar ist.

Sitzungsmobilität ist dann gegeben, wenn der Zustand eines Dienstes „eingefroren" und auf andere Systeme verlagert werden kann. Um weiter beim Beispiel zu bleiben, könnte der Nutzer das Video auf seinem stationären Rechner starten, irgendwann dort anhalten und zur U-Bahn gehen, um es auf der Fahrt an genau der selben Stelle auf seinem Tablet fortzusetzen.

Das Leibniz-Rechenzentrum (LRZ) als Betreiber des Münchner Wissenschaftsnetzes unterstützt primär die Personen- und Gerätemobilität. Auf den ersten Blick erscheint dies sehr einfach; die technischen und administrativen Implikationen werden im Folgenden kurz beschrieben. Die beiden anderen primären Mobilitätsformen (Dienst- und Sitzungsmobilität) sind originär von den konkret genutzten IT-Diensten bestimmt und können dementsprechend nur vom Dienstbetreiber (i. d. R. den Hochschulen) unterstützt werden.

Gerätemobilität mit WLAN und Mobilfunk

Endgeräte mobil zu nutzen, ist technisch nur durch eine drahtlose Verbindung realisierbar, denn nur dann lässt sich das Gerät auch über nennenswerte Strecken bewegen. Hierzu betreibt das LRZ eine sehr große WLAN-Infrastruktur mit knapp 2.000 WLAN Access Points (APs) in gut 350 Gebäuden (Abb. 1). Während des Semesters sind auf den APs heute bis zu 7.700 Nutzer gleichzeitig aktiv (zum Vergleich: 2009 waren es 3.000, 2010 in der Spitze 4.500 Nutzer).

Auch bei den Geräten zeigt sich ein massiver Zuwachs: Während des Semesters sind innerhalb einer Woche mehr als 55.000 verschiedene Geräte im WLAN. Obwohl das LRZ damit innerhalb von Deutschland eine der größten WLAN-Installationen betreibt, gibt es bei weitem keine flächendeckende Versorgung. Derzeit können nur öffentliche Bereiche wie Hörsäle, Seminarräume, studentische Arbeitsräume, Bibliotheken, Cafeterien etc. mit WLAN versorgt werden. Bei den vielen Standorten und den teilweise schwierigen Gebäudestrukturen (Altbauten) müsste die Anzahl der Access Points um ein Vielfaches höher sein, um eine Vollversorgung anzubieten.

Neben WLAN unterstützen viele Geräte auch diverse Mobilfunk-Protokolle. Für seine Nutzer betreibt das LRZ daher einen Zugangspunkt, der

Abb. 2: Weltweit mobil: Übersicht über die Anzahl der Einrichtungen, die eduroam unterstützen.

ABB.: WWW.EDUROAM.ORG

als Corporate Data Access (CDA) bezeichnet wird. Geräte, die sich über Mobilfunk einbuchen, erhalten normalerweise eine Adresse aus dem Netz des entsprechenden Mobilfunkproviders. Eine Abschottung zu anderen Kunden oder dem Internet erfolgt in der Regel nicht. Wenn die Geräte jedoch über den CDA ins Netz gehen, erhalten sie, egal wo sie sich ins Mobilfunknetz einbuchen, eine private Adresse aus dem MWN, d. h. logisch befindet sich das Gerät innerhalb des MWN. Dies hat zwei Vorteile: erhöhte Sicherheit und die komfortablere Nutzung von Diensten. Die Geräte sind aus dem öffentlichen Internet oder von anderen mobilen Geräten im selben Mobilfunknetz nicht erreichbar; dies bedeutet einen Sicherheitsgewinn. Außerdem sind so Dienste, die auf das MWN beschränkt sind (z. B. bestimmte Vorlesungsaufzeichnungen), nutzbar und alle Datenverbindungen werden über die Sicherheitssysteme (Intrusion Prevention Systeme) des LRZ geführt und abgesichert.

Personenmobilität und Gerätevielfalt

Die Personenmobilität, also die Möglichkeit eines Nutzers, seine Geräte zu wechseln bzw. mehrere (und verschiedene) Geräte gleichzeitig zu nutzen, ist heute die Regel. Für den Betreiber eines großen Netzes bedeutet dies, dass nach Möglichkeit und Kundenwunsch auch alle diese Geräte netztechnisch unterstützt werden sollen. Dies umfasst u. a. die Unterstützung bei der Client Software (z. B. VPN-Client), die Konfiguration (z. B. über vordefinierte Profile) sowie die Unterstützung der Nutzer im Rahmen des Servicedesks. Im konkreten Fall werden im MWN weit über 20 verschiedene Systeme unterstützt. Bei Laptops mit den diversen Betriebssystemen ist die Unterstützung drahtloser Netze sehr gut, auch gut dokumentiert und in gewissem Sinn ähnlich. Anders sieht es bei den Mobiltelefonen mit WLAN-Unterstützung aus. Hier hat fast jede Geräteklasse ein eigenes Betriebssystem, das sich völlig von anderen unterscheidet. Hierfür Unterstützung zu bieten, ist auch im Hinblick auf die Gerätevielfalt mit großem Aufwand verbunden. Zum Teil wird dann in enger Abstimmung mit Nutzern eine Dokumentation erstellt. So gibt es derzeit beispielsweise Dokumentationen für folgende Smartphones: Android, Bada, Blackberry, iOS-Geräte, Symbian, Windows Mobile und Windows Phone. Sobald ein neuer Gerätetyp auf dem Markt erhältlich ist, taucht er auch im MWN auf, und kurz darauf gibt es die ersten Kundenanfragen zur Netznutzung mit diesem neuen Gerät.

Weltweit ins Internet: Education Roaming (eduroam)

Neben den oben beschriebenen Mobilitätsformen gibt es eine weitere Dimension: die inter- sowie die intraorganisationale Mobilität. Letztere bezeichnet die Mobilität innerhalb einer Organisation, die mit Hilfe der oben genannten Techniken gut realisierbar ist. Unter interorganisationaler Mobilität wird die Mobilität zwischen verschiedenen Organisationen verstanden. Insbesondere in Wissenschaft und Forschung ist dies eine sehr wichtige Nutzungsform. Hierfür gibt es im Rahmen einer internationalen Kooperation, dem so genannten eduroam, einen sehr eleganten Ansatz, der es Wissenschaftlern, Studierenden und Hochschulangehörigen erlaubt, an anderen (teilnehmenden) Hochschulen und Wissenschaftseinrichtungen das WLAN zu nutzen. Eduroam steht für Education Roaming. Ein Nutzer im eduroam-Verbund authentisiert sich, egal wo er sich befindet, immer bei seiner Heimatorganisation mit seiner Heimatkennung und seinem Passwort. Die dafür notwendige Netzverbindung zur Heimatorganisation erfolgt verschlüsselt, d. h. eine potentiell böswillige Gastorganisation ist nicht in der Lage, Kennung oder Passwort mitzulesen. Bei einer erfolgreichen Authentisierung benachrichtigt die Heimateinrichtung die Gastorganisation, und diese schaltet daraufhin den Netzzugang für das entsprechende Gerät frei. Das LRZ beteiligt sich mit dem MWN flächendeckend und mit allen APs am eduroam-Verbund; reisende Wissenschaftler aus anderen Universitäten können das MWN also für den Zugang ins Internet nutzen.

Diese Möglichkeit besteht umgekehrt natürlich auch für Münchner Nutzer, die andere Universitäten im In- und Ausland besuchen. Derzeit sind allein in Deutschland über 300 Standorte mit mehr als 40.000 Access Points im eduroam-Verbund vertreten. Ursprünglich als europäische Initiative gestartet, ist eduroam mittlerweile weltweit im Einsatz und nutzbar. Einen Überblick über die Anzahl der weltweit teilnehmenden Organisationen gibt Abbildung 2.

Sicherheitsmanagement für mobile Nutzung

Eduroam ist für den Nutzer eine echte Erleichterung. Er konfiguriert eduroam einmal auf seinem Gerät und kann dann bei jedem eduroam-Partner seinen Laptop aufklappen und ist unmittelbar im Netz. Die Vorteile dieser mobilen Nutzung (sehr einfacher und problemloser Netzzugang auch bei verschiedenen Organisationen) können sich für den Betreiber jedoch schnell zum Problem entwickeln. Bei privaten Geräten und Geräten von Gästen ist nicht bekannt, welches Sicherheitsniveau sie haben und wie sie gepflegt und aktualisiert werden. Das bedeutet: Als Betreiber muss man damit leben können, immer einen gewissen Anteil infizierter Systeme oder Schadsoftware im Netz zu haben. Dies hat Auswirkungen auf die Bearbeitung von Missbrauchsfällen (Abuse-Bearbeitung) und es bedarf spezifischer Sicherheitssysteme. Mit Schadsoftware infizierte Rechner versuchen oft automatisch, weitere Systeme im selben Netz oder im Internet anzugreifen. Nachdem Gäste im eduroam eine Adresse aus dem MWN erhalten, wird der Angreifer auch dem MWN zugordnet, denn die für den Angriff verwendete Adresse ist auf das LRZ registriert. Die Administratoren der fremden angegriffenen Systeme melden den Vorfall entsprechend über eine Mailingliste (abuse@lrz.de). Im MWN wird dann ein Sicherheitssystem benötigt, um Angriffe aus dem MWN heraus möglichst effektiv zu erkennen und im Normalfall vollautomatisch zu verhindern.

Zu diesem Zweck hat das LRZ ein Intrusion Prevention System (IPS) mit der Bezeichnung Secomat entwickelt. Der Verkehr aus den eduroam- und WLAN-Netzen wird, für den Nutzer nicht erkennbar, über den Secomat geleitet und dort analysiert. Auf Basis verschiedener Heuristiken ist das System in der Lage, Angriffe zu erkennen, und kann den verursachenden Verkehr automatisch sperren. Der Verursacher wird auf eine Webseite umgeleitet, auf der ihm erklärt wird, warum er gesperrt wurde und wo er sich z. B. einen Virenscanner laden kann. Der redundant und ausfallsicher ausgelegte Secomat ist ein sehr erfolgreiches Sicherheitssystem. So kommt es oft vor, dass gesperrte Nutzer erst durch diesen Hinweis bemerkt haben, dass ihr System infiziert war, und sich bedanken.

Sollte trotzdem ein Angriff aus dem MWN ins Internet erfolgreich sein, muss der Verursacher im Rahmen der Abuse-Bearbeitung ermittelbar sein. Im Fall von eduroam geschieht dies über eine enge Kooperation mit der Heimatorganisation des eduroam-Benutzers, der den Angriff verursacht hat.

Zusammenfassung und Ausblick

Die mobile Nutzung im MWN hat in den letzten Jahren sehr stark zugenommen und wird in der näheren Zukunft sicher noch weiter zunehmen. Das MWN unterstützt die mobile Nutzung technisch durch ein sehr großes WLAN-Netz und den Betrieb eines CDA. Mit WLAN werden die öffentlichen Bereiche versorgt. Auch wenn der Wunsch nach einer flächendeckenden Versorgung immer wieder geäußert wird, ist dies bei der Gebäudestruktur der Universitäten und der großen Ausdehnung des MWN derzeit nicht finanzierbar. Für die mit der Mobilitätsunterstützung zusammenhängenden betrieblichen Herausforderungen und Sicherheitsfragen wurden adäquate Lösungen gefunden und umgesetzt. Durch Teilnahme am eduroam-Verbund ist für reisende Wissenschaftler oder Hochschulangehörige eine Netznutzung bei anderen eduroam-Partnern weltweit problem- und kostenlos möglich. ■

DER AUTOR

PD Dr. Helmut Reiser leitet die Abteilung Kommunikationsnetze am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften.

Literatur und WWW

H.-G. Hegering, A. Läpple, H. Reiser: Kommunikationsstrukturen in einer pervasiven Lehr- und Lernumgebung. In: it – Information Technology 51, 1 (Februar 2009), S. 24–31

European Commission: Knowledge without Borders – GÉANT 2020 as the European Communication Commons; Report of the GÉANT Expert Group, Brussels, October 2011, http://cordis.europa.eu/fp7/ict/e-infrastructure/docs/geg-report.pdf

Wie funktioniert WLAN im Münchner Wissenschaftsnetz? www.lrz.de/services/netz/mobil/wireless/

Was ist eduroam? www.eduroam.org/

eduroam in Deutschland: http://airoserv4.dfn.de/

eduroam weltweit: www.eduroam.org/?p=where

Wie kann ich eduroam einrichten? www.lrz.de/services/netz/mobil/eduroam/