IT-Sicherheit

Grenzenlose Dienstvielfalt

Supercomputer, Wissenschaftsnetze und viele weitere IT-Dienste für Forschung und Lehre sind Sachwerte, die vor missbräuchlicher Verwendung geschützt werden müssen. Das Leibniz-Rechenzentrum (LRZ) gewährleistet als Betreiber einer hochwertigen IT-Infrastruktur die Sicherheit der ihm von Nutzern anvertrauten Daten – etwa mit Hilfe des Föderierten Identitäts-Managements.

Von Wolfgang Hommel

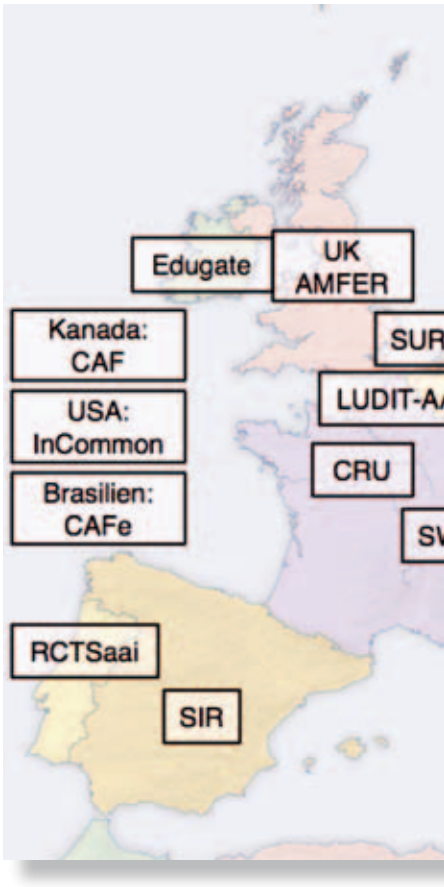


Abb. 1: Nationale Hochschulföderationen im Überblick.

EINE ESSENTIELLE Teilaufgabe des Sicherheitsmanagements ist es, nur bekannten und berechtigten Nutzern Zugriff auf Dienste und Daten zu gewähren. Um bei seinen über 120.000 Nutzern nicht den Überblick zu verlieren, betreibt das LRZ ein Identity & Access Management (I&AM) System, in dem alle Nutzer und deren Berechtigungen, LRZ-Dienste in Anspruch zu nehmen, verzeichnet sind. Bei jedem Versuch, z. B. E-Mails abzurufen, auf Speichersysteme zuzugreifen oder den SuperMUC zu verwenden, wird der Nutzer zunächst authentifiziert – üblicherweise, indem er seine LRZ-Kennung und sein Passwort eingeben muss. In einem zweiten Schritt prüft das I&AM-System, ob er für den gewünschten Dienst autorisiert ist. Den dafür notwendigen Datenbestand zu pflegen, ist überaus anspruchsvoll. Einige Abläufe werden aber nach und nach durch Datenaustausch mit den Studenten- und Personalverwaltungssystemen der Münchner Universitäten automatisiert. Zugleich wird so sichergestellt, dass Berechtigungen zeitnah zugewiesen und beim Verlassen der Hochschule wieder entzogen werden.

Überregionale Dienstangebote

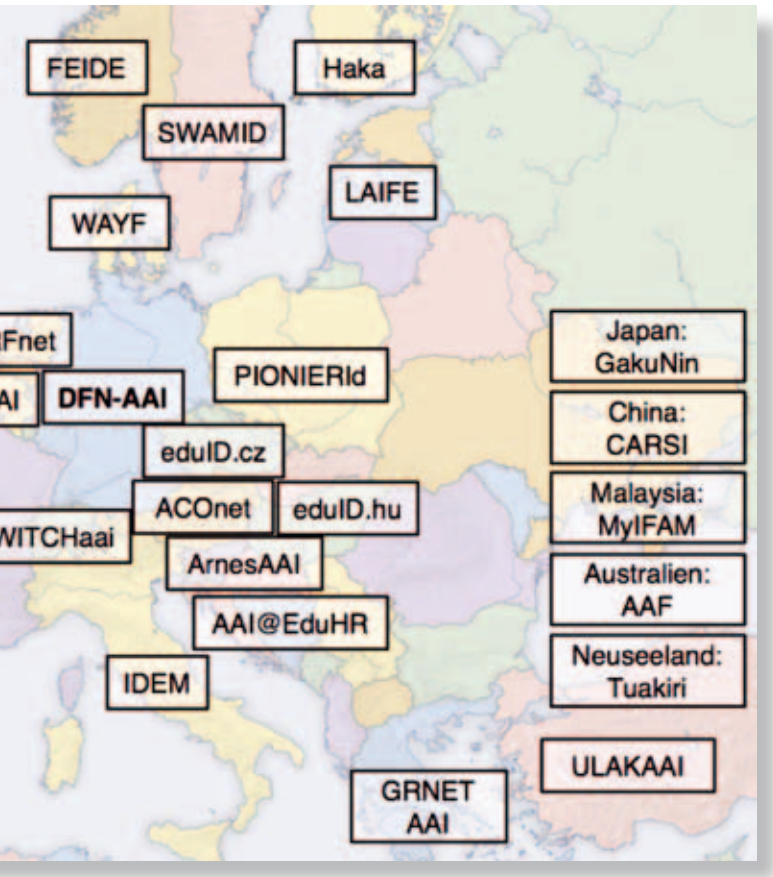
Nutzer mit einer Münchner Alma Mater sind jedoch im Rahmen ihrer Arbeiten auch an Diensten interessiert, die nicht das LRZ erbringt. Hierzu gehören u. a. wissenschaftliche Datenbanken und Zeitschriften, E-Learning über das iTunes-University-Programm von Apple, Softwareangebote mit Sonderkonditionen für Hochschulangehörige und Dienste des Deutschen Forschungsnetzes (DFN) wie Videokonferenzen.

Auch diese Dienste sollen nur ausgewählten Nutzern zugänglich sein: Sonderkonditionen für Studenten beim Softwarekauf dürfen ausschließlich von Studenten, E-Book-Downloads bei Verlagen nur von Angehörigen von Hochschulen mit entsprechenden Lizenzen genutzt werden. Herkömmliche Autorisierungsnachweise wie das postalische Einsenden von Immatrikulationsbescheinigungen sind mit hohem Aufwand und langen Laufzeiten behaftet.

Föderiertes Identitäts-Management

Als Lösung bietet sich deshalb eine selektive, organisationsübergreifende Kopplung von I&AM-Systemen an. Beim Föderierten Identitäts-Management (Federated Identity Management, FIM) fungiert die Heimateinrichtung eines Nutzers als Identity Provider (IDP). Dieser stellt dem Dienst die erforderlichen Nutzerinformationen zur Verfügung. Für alle im I&AM-System erfassten Angehörigen der Münchner Universitäten betreibt das LRZ den Identity Provider. Zur deutschlandweit vom Deutschen Forschungsnetz aufgebauten Authentifizierungs- und Autorisierungsinfrastruktur (DFN-AAI) haben sich schon mehr als 80 IDPs zusammengeschlossen, die eine hochschulübergreifende Nutzung von bereits rund 100 Diensten ermöglichen. Zu

ALLE ABB.: LRZ/W. HOMMEL



diesen gehören auch die vom LRZ betriebenen E-Learning-Systeme der Münchner Universitäten, die über Kurse der Virtuellen Hochschule Bayern auch von Studenten anderer bayerischer Universitäten genutzt werden können.

Datenschutz

Ein großer Vorteil beim Einsatz von FIM ist die einfache Möglichkeit zur Umsetzung von Datenschutzprinzipien wie der Datensparsamkeit: Falls die Berechtigung zur Dienstnutzung nur von der Hochschulzugehörigkeit oder der Eigenschaft des Nutzers, Mitarbeiter einer bestimmten Fakultät zu sein, abhängt, übermittelt der Identity Provider nur genau diese Information an den Dienst. Weiterführende Auskünfte wie Name oder E-Mail-Adresse werden in diesem Fall nicht erteilt.

Welche personenbezogenen Daten der Identity Provider jeweils herausgeben würde, wird dem Nutzer vorab in Form einer Visitenkarte angezeigt (Abb. 2). Nur wenn er damit einverstanden ist, werden die Daten tatsächlich zum Dienst übertragen.

Benutzerfreundlichkeit

Die zu beobachtende große Beliebtheit des FIM-basierten Zugangs zu Diensten geht auch mit dessen Benutzerfreundlichkeit einher. Neben intuitiver Bedienung und transparenten Datenflüssen ist das vom Identity Provider realisierte Single Sign-On ausschlaggebend: Nutzer müssen ihr Passwort nur bei ihrem Identity Provider eingeben und sich keine separaten Zugangsdaten pro Dienst merken. Zudem hält der Identity Provider einige Zeit Informationen darüber vor, welcher Nutzer sich bereits angemeldet hat. Dadurch können verschiedenste Dienste genutzt werden, ohne dass die Arbeit immer wieder durch Passwortabfragen unterbrochen wird.

Zukünftige Entwicklung

Der europäische Forschungsnetzverbund GÉANT schafft unter dem Namen eduGAIN derzeit die organisatorischen und technischen Randbedingungen für länderübergreifendes FIM. Nutzern und Dienstanbietern aus Deutschland erschließen sich so mit der DFN-AAI vergleichbare Föderationen in über einem Dutzend anderer europäischer Länder (Abb. 1). Seit Anfang 2012 werden auch interkontinentale Verbünde aufgebaut, um entsprechende Forschungsvorhaben zu unterstützen.

DER AUTOR

Dr. Wolfgang Hommel ist Informationssicherheitsbeauftragter des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften und leitet die Gruppe Planung Kommunikationsnetze. Seit 2004 hält er Lehrveranstaltungen zur IT-Sicherheit an der LMU München.

Abb. 2: Anmeldung bei Diensten über den Identity Provider.