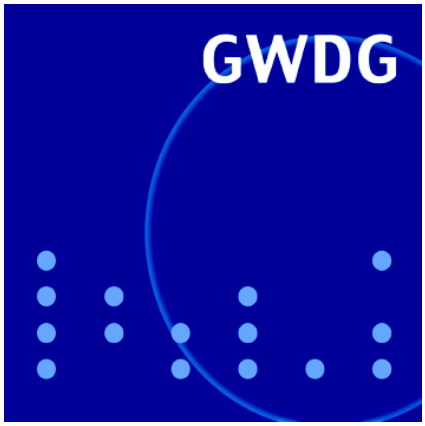


Digitale Langzeitarchivierung

Identity Management

Intrusion Detection und Prevention im GÖNET

GWDG Nachrichten

7 / 2006

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Inhaltsverzeichnis

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

29. Jahrgang, Ausgabe 7 / 2006

http://www.gwdg.de/GWDG-Nachrichten

Herausgeber: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Fassberg, 37077 Göttingen-Nikolausberg

Redaktion und Herstellung: Dr. Thomas Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de

1. Digitale Langzeitarchivierung bei der GWDG – neue technische Infrastruktur

1.1 Einleitung

Digitale Daten der Max-Planck-Gesellschaft und der Universität Göttingen werden bereits seit Bestehen der GWDG vor Ort archiviert. Zusätzlich zu diesen bestehenden Verfahren wird jetzt ein gesonderter Archivbereich geschaffen, der gezielt den Anforderungen einer Langzeitspeicherung digitaler Daten dienen wird.

Im Rahmen des BMBF-Projektes **kopal** wurde Ende letzten Jahres ein digitales Langzeit-Archivsystem bei der GWDG installiert. Die geplante zusätzliche technische Infrastruktur soll im Bereich des Speicher-Backends für das Projekt kopal und für die Daten der Max-Planck- sowie Universitäts-Institute eine einheitliche Lösung bieten.

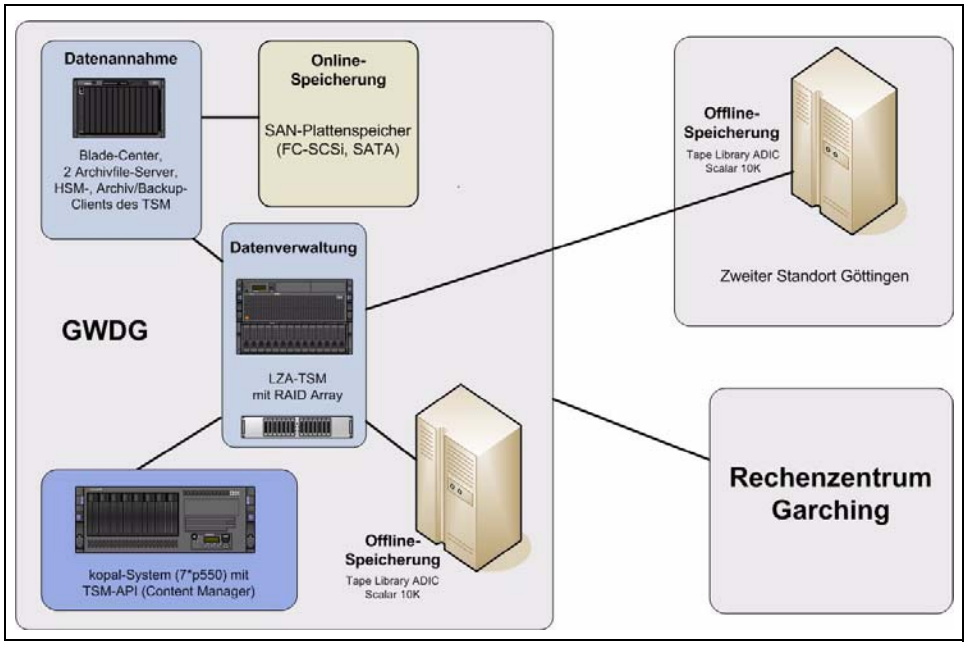
1.2 Ausgangssituation

Bereits bei der GWDG zur Langzeitarchivierung (LZA) vorhandene Daten werden derzeit projektspezifisch gehalten. Die Daten aus dem kopal-Projekt werden direkt an einen TSM-Server zur Speicherung auf Magnetbändern übergeben. Eine zusätzliche lokale Speicherung dieser Daten erfolgt derzeit nicht. Die Konfiguration sieht zur Zeit eine doppelte Offline-Sicherung vor. Im Gegensatz zu den kopal-Daten werden die Daten der Max-Planck-Institute derzeit noch dezentral über verschiedene Server vorwiegend unter Linux mit diversen Filesystemen verwaltet. Die Daten werden abhängig vom jeweiligen Datenvolumen, anwendbarem Transferverfahren und Zugriffsanforderungen im Storage Area Network (SAN) der GWDG, auf lokalen RAID-Systemen sowie auf Magnetbandkassetten gehalten. Insbesondere die derzeitige Haltung einiger Bestände auf schnellen und teuren FibreChannel-SCSI-Platten wird in dieser Form für die Langzeitarchivierung als nicht mehr sinnvoll angesehen. Sie macht dort Sinn, wo auch ein performanter Zugriff z. B. seitens eines Webservers erforderlich ist. Diese Speichervariante soll künftig nur im Bedarfsfall unabhängig von der Langzeitarchivierung über gesonderte Zugriffskopien erfolgen.

1.3 Konzept für eine LZA-eigene technische Infrastruktur

Die GWDG strebt ein Verfahren an, bei dem stets mindestens zwei Kopien der Daten auf den Magnetbandrobotern der GWDG gespeichert werden. Diese Roboter sind in Göttingen an zwei räumlich getrennten Standorten untergebracht. LZA-Bestände werden an beiden Standorten in Spiegelung gehalten. Künftig soll mindestens eine weitere Kopie beim Rechenzentrum Garching (RZG) gesichert werden. Bei besonders wertvollen Beständen kann die Zahl dieser Kopien erhöht werden, wobei zumindest für begrenzte Datenmengen auch eine zusätzliche dauerhafte Online-Haltung des Bestandes möglich sein soll.

Das künftige LZA-Konzept der GWDG zielt auf eine gut skalierbare und einheitliche Verwaltung der Daten über eigene Archivfile- und TSM-Server unter AIX. Es sollen zu Beginn zwei Archivfile-Server eingesetzt werden, die sowohl für den Datentransfer von den Instituten zur GWDG als auch für die Kommunikation mit dem ebenfalls geplanten LZA-eigenen TSM-Server (TSM = Tivoli Storage Manager) zuständig sind. Die Archivfile-Server werden an das GWDG-SAN angebunden und bieten so die Möglichkeit, Daten in einem zugehörigen Speicherbereich des GWDG-SANs entweder auf einem speziellen HSM-Filesystem oder in einem normalen Filesystem abzulegen. Von dort werden die Daten in definierten Zeitabständen über den HSM- oder den Archiv/Backup-Clienten des TSM an den neuen LZA-TSM-Server und anschließend an die Bandroboter für die Offline-Sicherung übergeben. Auf dem LZA-TSM-Server wird die Konfiguration speziell auf HSM und Archivierung ausgelegt. Der LZA-TSM-Server wird über das GWDG-SAN mit den vorhandenen Bandrobotern verbunden. Die folgende Skizze zeigt die derzeit geplante Speicherinfrastruktur:



1.3.1 Bestehende Infrastruktur

Derzeit hat die GWDG zwei TSM-Server im Einsatz. Auf diesen Servern läuft neben den primären Backup-Servern noch der TSM-Server des kopal-Projektes. Die Konfiguration dieser TSM-Server ist auf den Backup-Dienst der GWDG ausgerichtet. Hinter den beiden TSM-Servern befinden sich die im letzten Jahr neu erworbenen LTO3-Bandroboter (Scalar 10k) der Firma ADIC. Die Bandroboter wie auch die TSM-Server sind jeweils redundant an die beiden SAN-Fabrics der GWDG angebunden.

1.3.2 Geplante zusätzliche Komponenten

Als **Archivfile-Server** sollen IBM-Bladeserver mit PowerPC-Technologie zum Einsatz kommen. Die beiden Blades werden mit zwei Dualcore-PC970MP-Prozessoren ausgestattet sein. Das Blade-Center selbst besitzt aktuell für jedes Blade zwei Gigabit-Ethernet-Adapter sowie zwei 2-Gigabit-FibreChannel-Adapter.

Als **TSM-Server** soll eine entsprechend leistungsfähige und skalierbare Hardware zum Einsatz kommen. Da die bisherigen TSM-Server der GWDG unter AIX betrieben werden, wird dies auch bei dem neuem TSM-Server der Fall sein. Geplant ist eine pSeries 570 mit entsprechenden Anschlüssen. Diese Maschine bietet die Möglichkeit, mehrere virtuelle Maschinen bereit zu stellen, und verfügt über genügend interne Steckplätze, um mindestens acht FibreChannel-Anschlüsse a´ 4 GBit zur Verfügung zu stellen. Die Grundausstattung dieser Maschine besteht aus vier 1,9-GHz-Power5+-Prozessoren in 64-Bit-Technik mit 8 GByte Hauptspeicher.

Wie oben beschrieben, werden die Datenbestände zunächst im SAN der GWDG gespeichert. Für den erforderlichen SAN-Speicher, auf dem die Filesysteme aufgebaut werden, sollen kostengünstigere SATA-Systeme gewählt werden. Für die Offline-Speicherung der Daten werden die vorhandenen LTO3-Bänder der Bandroboter genutzt werden.

Für den LZA-TSM-Server wird ein eigener Cache- sowie ein Datenbankbereich für die interne TSM-Datenbank auf schnellen FibreChannel-SCSI-Festplatten berücksichtigt. Hierfür beabsichtigt die GWDG, ein schnelles und leistungsfähiges RAID-System der Firma IBM anzuschaffen. Geplant ist ein DS4800-Storage-System mit durchgängier 4-GBit-Technik.

1.3.3 Vorteile der geplanten Speicherinfrastruktur

Die räumliche Verteilung der Daten bietet Schutz vor Datenverlust durch äußeren Einfluss. Durch eine mögliche Online-Kopie und die zusätzliche Sicherung der Daten beim RZG (bzw. der RZG-Daten bei der GWDG) werden verschiedene Speichertechniken zum Einsatz kommen. Sie sichern vor zeitgleichen Migrationserfordernissen und somit vor möglichen systembedingten Fehlern oder Engpässen bei Kopiervorgängen. Die Verwaltung aller langfristig zu sichernden Datenbestände auf eigenen Speicherkomponenten erleichtert die Administrierbarkeit und die Kontrolle über Datenzugriffe. Auf Grund von Technologiesprüngen erforderliche Datenmigrationen können für alle betroffenen Bestände des Archivs gezielt angestoßen werden. Fehleranalysen und -statistiken werden Erkenntnisse über einzuplanende Kopierzeiten, Lebensdauer und Nutzbarkeit von Speicherhardware liefern. Der Einsatz von Archivfile-Servern mit Zugriff auf Speicher im SAN der GWDG bietet Vorteile hin-

sichtlich der Skalierbarkeit, der Flexibilität und der Sicherheit. Der verfügbare Online-Speicher kann abhängig vom Bedarf jederzeit erweitert werden. Die Speicherung im SAN erlaubt es außerdem, z. B. Zugriffskopien für andere Server zur Verfügung stellen zu können. Die doppelte Auslegung der Archivfile-Server dient sowohl der Ausfallsicherheit als auch der Schaffung von Testmöglichkeiten. Auf den Archivfile-Servern sind verschiedene Verfahren zur Sicherung der Datenintegrität, wie z. B. der Einsatz von Checksummen und ggf. von Antivirenkontrollen geplant. Hinsichtlich des Datentransfers können über die Archivfile-Server beliebige Verfahren eingesetzt werden, die keine festen Voraussetzungen seitens der Kunden benötigen. Je nach Bedarf kann ein rsync-, ein (s)ftp- oder ein scp-Verfahren genutzt werden. Unter Umständen ist auch das Versenden von USB-Platten (z. B. bei sehr schlechter Internetanbindung) möglich. Diese Flexibilität hat sich in den vergangenen Jahren als sehr wichtig erwiesen, da die Daten in völlig unterschiedlichen Kontexten entstehen, oft in Projekten, in deren Verlauf sich der Datenbestand noch verändert.

1.3.4 Zeitliche Planung zur Inbetriebnahme der geplanten Speicherinfrastruktur

Die aktuelle zeitliche Planung sieht eine Installation nach erfolgter Lieferung der neuen Hardware gegen Ende September 2006 vor. Nach erfolgreicher Installation sowie dem Abschluss von internen Tests ist die offizielle Inbetriebnahme für Ende 2006 geplant.

Scheller, Ullrich

---

2. Identity Management bei der GWDG

2.1 Einleitung

Ziel des Projekts „Meta-Directory“ der GWDG ist es, die bestehenden Verzeichnisse und Datenbanken für die Verwaltung von Benutzern (bzw. Identitäten) innerhalb der GWDG zu synchronisieren. Hierbei wird eine Vereinfachung der Administration bzw. Verwaltung der Identitäten (Homogenisierung und Erhöhung der Qualität der Benutzerdaten) sowie der Anwendbarkeit durch die Benutzer („Self-Service“ ihrer Identitäten bzw. Benutzeraccounts, „Single Password“, teilweise „Single Sign-On“) angestrebt.

Zusammen mit weiteren Teilprojekten wie z. B. der Realisierung und Etablierung einer Public-Key-Infrastruktur für die Max-Planck-Gesellschaft und die GWDG [1] bildet das „Meta-Directory“, das bis Ende 2005 als Keyproject vorangetrieben wurde, eine Basis für die „einheitliche Authentifizierung“ auch über die Grenzen konkreter Systeme der GWDG, insbesondere im Göttingen-weiten GÖ*-Kontext (vgl. [2]), hinweg.

2.2 Meta-Directory als Basis für Identity Management

In der GWDG bzw. am Standort Göttingen allgemein existieren viele separate Verzeichnisse und Datenbanken für Benutzerkonten. Die Vielzahl der Verzeichnisse und Datenbanken begründet sich beispielsweise durch unterschiedliche Anwendungen oder Plattformen, die jeweils einen separaten Verzeichnisdienst oder eine gesonderte Datenbank für die Benutzerverwaltung verwenden. Um den Benutzern (bzw. Identitäten) zu allen Anwendungen und Ressourcen Zugang zu ermöglichen, müssen diese daher in allen Benutzerverwaltungen separat angelegt und gepflegt werden. Administrativ entsteht somit ein hoher Aufwand im Rahmen der Verwaltung bzw. des Identity Managements.

Führen die Benutzer ihrerseits Veränderungen an Ihren Benutzerdaten durch, so müssen sie diese in allen Verzeichnissen und Datenbanken separat nachtragen, um einen einheitlichen Stand der Daten zu erhalten. Beispiel hierfür ist die Änderung eines Passwortes, die an allen Systemen durchgeführt werden muss, um ein konsistentes Ergebnis zu erzielen.

Häufig werden zentrale Verzeichnisse basierend auf LDAP (vgl. OpenLDAP [3] oder Active Directory [4]) eingesetzt, um die Identitäten an einer Stelle zu verwalten und sie auf diese Weise zusammenzuführen. Begrenzt wird diese Integration allerdings durch Inkompatibilitäten der Anwendungen, Authentifizierungsverfahren und -systeme, die zudem häufig nur auf bestimmten Plattformen betrieben werden können. Die GWDG verwaltet daher ein zentrales Verzeichnis für ihre UNIX-Systeme (siehe auch [5]) sowie ein Active Directory für Windows-Systeme.

Um den Aufwand sowohl für die Administration als auch die Verwendung durch die Benutzer über zentralisierte und nach wie vor dezentrale Verzeichnisse und Datenbanken zu verringern, bietet sich eine automatisierte Replikation bzw. Synchronisation der Identitäten und zugehörigen Informationen an. Eine solche Synchronisation, wie in Abb. 1 illu-

striert, kann z. B. durch ein Meta-Directory erfolgen, das als Drehscheibe für die Identitäten und Attribute fungiert. Als externe Organisation neben der GWDG nennt die Abb. 1 den Geschäftsbereich 3-7 des Bereichs Humanmedizin der Universität Göttingen (GB 3-7 IT).

Das Meta-Directory erkennt Veränderungen in den Verzeichnissen und überträgt sie anhand definierter Kriterien und Regeln in die weiteren angeschlossenen Systeme. Hierbei werden die Informationen zusätzlich an das im jeweiligen Zielverzeichnis benötigte Format angepasst.

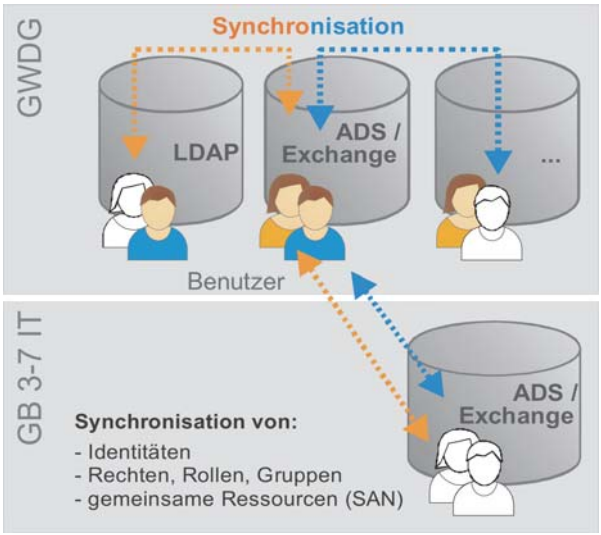


Abb. 1: Synchronisation von Identitäten über dezentrale Verzeichnisse

Die Synchronisation ermöglicht neben der einfacheren und effizienteren Administration und Verwendung auch den Abgleich von Passwörtern. Benutzer haben so die Möglichkeit ein einheitliches Passwort für die Verwendung der Anwendungen und Ressourcen zu verwenden („Single Password“). Dies steigert zusätzlich die IT-Sicherheit insbesondere bei der Vorgabe von Komplexitätskriterien für akzeptierte Passwörter (wie z. B. Länge, Sonderzeichen oder Passworthistorie), da die Benutzer mit zunehmender Anzahl von Passwörtern beginnen, diese aufzuschreiben (häufig in unmittelbarer Nähe ihres Rechners oder der verwendeten Ressource), direkt auf ihrem Rechner in der Anwendung abzuspeichern oder die Komplexitätskriterien (z. B. durch einen gezielten Überlauf der Passworthistorie) zu umgehen.

Zusätzlich können durch das Identity Management z. B. Rechte, Rollen und Gruppen für die der Authentifizierung folgende Autorisierung synchronisiert werden. Auch Daten für eine Nutzungsabrechnung (Accounting) nach erfolgreicher Authentifizierung und Autorisierung können abgeglichen werden. Insbesondere bei dezentralen und heterogenen IT-Strukturen ist jedoch die Bereitstellung der erforderlichen Infrastruktur für die Anwendung wesentlich. Nach erfolgreicher Authentifizierung und Autorisierung soll der Benutzer beispielsweise Zugriff auf sein Home-Verzeichnis erlangen, was geeignete Verfahren für die Verfügbarkeit der Daten auch an dezentralen Systemen erfordert (z. B. durch eine geeignete SAN-Infrastruktur). Erst dann kann eine übergreifende und dezentrale Anwendungsbereitstellung, wie z. B. Göttingen-weit im Rahmen des GÖ*-Projekts geplant, erfolgen.

2.2.1 Synchronisation von Attributen und Identitäten

Der Fokus bei der Synchronisation von Identitäten und ihren zugehörigen Attributen liegt im Keyproject „Meta-Directory“ der GWDG auf dem Abgleich zwischen dem OpenLDAP-Verzeichnisdienst für UNIX-Systeme und dem Active Directory für Windows-Systeme. Anders als in vielen anderen Meta-Directory-Projekten, die mit großen Anlaufschwierigkeiten in der IT gestartet wurden, wird im Keyproject „Meta-Directory“ der GWDG ein pragmatischer Ansatz verfolgt, der nicht sofort alle Informationen und möglichen Datenquellen resp. Verzeichnisse synchronisiert, sondern sukzessive skaliert. Im Gegensatz zu vielen gescheiterten Projekten, die im ersten Schritt alle technischen Details fokussierten, kann so eine schrittweise organisatorische Planung von Abläufen bzw. der Synchronisation allgemein erfolgen, die eine weitaus größere Herausforderung als die technische Umsetzung darstellt.

Derzeit werden primär Organisationsstrukturen (Hierarchien mit Organisationseinheiten, z. B. Abteilungen), Benutzer und Passwörter abgeglichen. Zukünftig ist auch der Abgleich von Rechten, Rollen und Gruppen geplant. Abb. 2 skizziert das Meta-Directory als Datendrehscheibe für die Attribute und Identitäten.

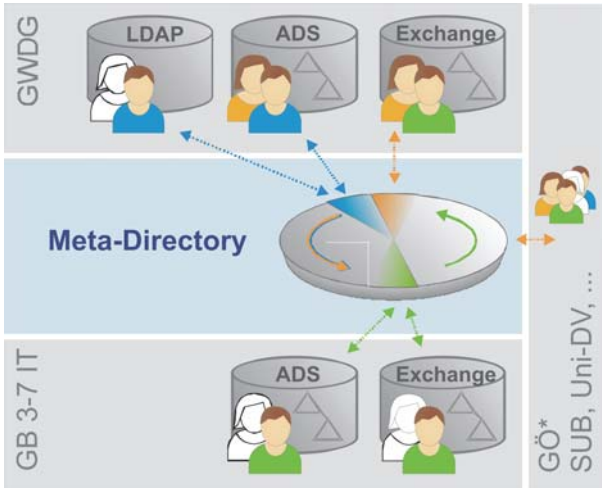


Abb. 2: Meta-Directory als Datendrehscheibe für Identitäten

Als initiale Quelle für die Fluss der Informationen resp. Attribute dient das OpenLDAP, das auch für die Anlegung neuer Benutzer bzw. deren Verwaltung durch das Keyproject „Benutzeraccount-Vergabe“ verwendet wird. Attribute wie beispielsweise Vor- und Nachname der Benutzer werden vom Meta-Directory nach festen Regeln in angeschlossene Zielsysteme übertragen und an die dortigen Anforderungen angepasst. Dadurch können zusätzlich Skripte, Individual-Lösungen und manuelle Synchronisation zugunsten einheitlicher sicherer Verfahren abgelöst werden.

Wie in Abb. 2 gezeigt, werden Identitäten beispielsweise direkt nach deren Erzeugung in relevante weitere Verzeichnisse und Datenbanken übertragen. So können beispielsweise neu angelegte Benutzer direkt auf ein Exchange-Postfach oder sowohl auf UNIX-Systeme, die OpenLDAP als Authentifizierungssystem verwenden, als auch auf Windows-Systeme am Active Directory zugreifen. Diese Synchronisation von Benutzern direkt nach deren Erzeugung wird auch als „Provisioning“ bezeichnet und umfasst zusätzlich das Starten von Workflows zur Einrichtung der benötigten Umgebung für die Benutzer, z. B. inkl. Rechte, Rollen und Gruppen.

Wird ein Benutzer als dem Quellsystem entfernt, so löscht das Meta-Directory bei Bedarf die synchronisierten Identitäten des Benutzers in allen anderen angeschlossenen Systemen, was in Bezug auf die zusätzlich ausgelösten Prozesse z. B. zum Entfernen der Umgebung des Benutzers im Zielsystem auch als „Deprovisioning“ bezeichnet wird.

2.2.2 Synchronisation von Passwörtern

Einen Sonderfall bei der Synchronisation stellt das Passwort der Benutzer dar, da es i. d. R. in den Systemen individuell und in irreversibler Form verschlüsselt (als Hash z. B. nach MD5, SHA1 oder crypt) gespeichert wird. Es kann somit nicht für die Verwendung in zusätzlichen Zielsystemen bei der Synchronisation durch das Meta-Directory konvertiert werden.

Beim Identity Management werden daher i. d. R. web-basierte Portale verwendet, um das Passwort in allen geschlossenen dezentralen Systemen zu setzen. Dabei werden vom Meta-Directory passende Hash-Werte für die angeschlossenen Zielsysteme erzeugt. Entsprechende Portale bieten ggf. zusätzlich die Möglichkeit für den Benutzer, seine Identität resp. mit dem Benutzeraccount verknüpfte Attribute selbst zu ändern (Identity Management „Self-Service“).

Für die initiale Anmeldung am Portal bieten die Portale die Möglichkeit, bestehende Hash-Werte zu verwenden. Ebenfalls kann das Passwort direkt über zusätzliche Schnittstellen (z. B. direkt per LDAP) im Meta-Directory gesetzt werden. Dadurch können auch klassische Passwort-Änderungen von UNIX-Systemen via PAM (Plugable Authentication Modules) integriert werden.

Eine weitere Lösung bieten spezielle Filter, die das Passwort im Quellsystem vor der Erzeugung des zugehörigen Hash-Werts im Klartext abgreifen und asymmetrisch verschlüsselt an das Meta-Directory übermitteln. Diese Lösung wird beispielsweise durch spezielle Komponenten im Active Directory geboten.

Häufig werden die Passwörter im Meta-Directory in verschlüsselter Form, aber nicht als irreversibler Hash-Wert gespeichert. Auf diese Weise können sie in später zusätzlich angebundene Systeme, die beispielsweise neue Hash-Verfahren bzw. eine alternative Form zur Speicherung der Passwörter verwenden, übertragen werden. Wird diese Funktionalität geboten, so erfolgt die Speicherung im Meta-Directory i. d. R. mit einem administrator-sicheren Zugriffsschutz, so dass unberechtigten Dritten und regulären Administratoren kein direkter Zugriff auf reversibel verschlüsselte Passwörter geboten wird. Beispielsweise werden Hardware-Tokens (bzw. Crypto-Karten) oder geteilte Passwörter für die Administration des Systems verwendet.

Zur Berücksichtigung des Datenschutzes haben die Benutzer nach wie vor die Möglichkeit, in den einzelnen Systemen getrennte Passwörter zu verwenden, indem die Kennwörter direkt im Zielsystem gesetzt werden. Portale und Passwortfilter gehen jedoch voreingestellt von einer Synchronisation in alle angeschlossenen Verzeichnisse aus.

Die Abb. 3 zeigt die zeitnahe Synchronisation von Passwörtern über das Meta-Directory als Drehscheibe. Diese erfolgt in aller Regel in wenigen Sekunden und erhält Priorität vor anderen synchronisierten Attributen. Grundlage für diese Synchronisationsform stellt die Reaktion auf Ereignisse (Events) dar, so dass in diesem Zusammenhang auch von „event-basiertem“ Identity Management gesprochen wird.

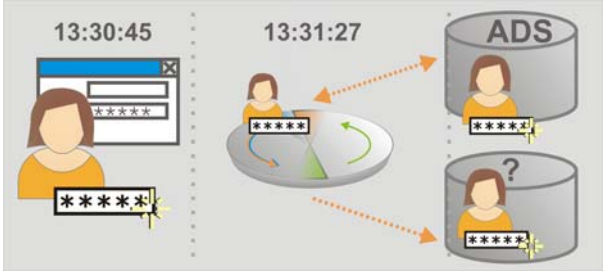


Abb. 3: Verteilung des Passworts in angeschlossene Systeme als „Event“

2.2.3 Einheitliche Identitäten

Neben dem Abgleich der Attribute und Passwörter einer Identität entsteht auch durch die Diversifikation der Benutzernamen ein Aufwand auf Seiten der Benutzer. Ideal wäre die Verwendung eines einheitlichen Benutzernamens in allen Anwendungen und Systemen. Dieser Anforderung stehen jedoch die zunehmend dezentrale Authentifizierung sowie technische Restriktionen der angebundenen Systeme gegenüber. So existieren beispielsweise in gängigen SAP-Systemen Längenbeschränkungen auf 12 Zeichen. Für die dezentrale Authentifizierung ist die Begrenzung der Gültigkeit bzw. Eindeutigkeit der Benutzernamen essentiell, um Namensdopplungen zu vermeiden.

Der Benutzername **`lmuelle`** (der fiktiven Benutzerin Lieschen Müller) dürfte ohne entsprechende Regelung nicht für den fiktiven Benutzer Lars Müller in einem anderen angeschlossenen System verwendet werden. Um für dieses Problem eine übergreifende, internationale Lösung z. B. für hohe Mobilität der Benutzer bzw. Roaming-Lösungen zu finden, haben sich im Identity Management Benutzernamen basierend auf der E-Mail-Adresse etabliert (z. B. **`lmuelle@institut-a.gwdg.de`**). Die der Adresse angehängte Domäne dient hierbei als Realm (wie auch für Authentifizierungsverfahren wie Kerberos verwendet) und sorgt für eine weltweit eindeutige Bezeichnung. Neben der Länge des Benutzernamens, die die Bequemlichkeit der Eingabe einschränkt, lässt sich diese Lösung auch aufgrund der o. g. technischen Restriktionen der angeschlossenen Systeme derzeit nicht vollständig realisieren.

Basis für die spätere Vereinheitlichung der Benutzernamen bildet die Definition einer eindeutigen Bezeichnung der Identität im Meta-Directory, der mehrere Ausprägungen bzw. Benutzernamen in den Zielsystemen untergeordnet werden können. Durch die Verknüpfung der Benutzernamen wird eine spätere Migration zu einem einheitlichen Namen durch die entsprechende Synchronisation der angebundenen Systeme ermöglicht. Dies bedingt jedoch zusätzlich ein einheitliches Schema für die Informationen der Benutzer sowie bei Bedarf einheitliche Gruppen, Rollen und Rechte-Modelle.

2.2.4 Starten von externen Prozessen

Um nach erfolgreicher Authentifizierung und Autorisierung dezentral zur Verfügung gestellte Anwendungen nutzen zu können, müssen diese auf gemeinsame Ressourcen zurückgreifen können. Beispielsweise benötigt ein Benutzer nach erfolgreicher Authentifizierung Zugriff auf sein Home-Verzeichnis. Wird der Benutzer neu im System angelegt, so müssen dieses Home-Verzeichnis sowie weitere für die Anwendung notwendige Ressourcen angelegt werden. Für ein reibungsloses Arbeiten auf Seiten der Benutzer werden die Änderungen zeitnah als Ereignis, wie im vorherigen Abschnitt für Passwörter beschrieben, verarbeitet. Abb. 4 illustriert die Erzeugung eines E-Mail-Kontos inkl. Speicherplatz und Home-Verzeichnis beim Anlegen des neuen Benutzers.

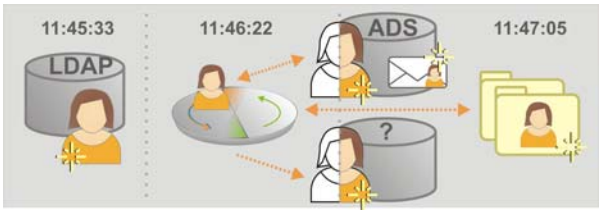


Abb. 4: Ausführung von externen Workflows / Skripten durch das Meta-Directory

Generell können Ereignisse wie z. B. Modifikationen, Löschungen oder das Anlegen neuer Benutzer externe Workflows z. B. über Skripte auf den Zielsystemen vom Meta-Directory gesteuert ausführen. Dabei werden den Aufrufen Parameter, z. B. die durchgeführten Änderungen oder relevanten Attribute, übergeben. Ausgaben der aufgerufenen Anwendungen können erneut ins Meta-Directory übernommen werden und neue Ereignisse auslösen (z. B. Abfrage des verfügbaren Speicherplatzes und bedingte Selektion eines alternativen geeigneten Speicherbereichs).

2.3 Integration von Public-Key-Infrastruktur, Single Sign-On und Federation

Identity Management umfasst mehr als die in den vorherigen Abschnitten beschriebenen Meta-Directory-Funktionen. Es umfasst die Verwaltung der Benutzeraccounts und zugehöriger Authentifizierungsinformationen von deren Erzeugung an. Daher kooperiert das Keyproject „Meta-Directory“ direkt mit dem Keyproject „Benutzeraccount-Vergabe“ der GWDG. Zusammen mit der Etablierung einer Public-Key-Infrastruktur (z. B. durch die Verwendung von Zertifikaten für unterschiedliche Anwendungen bzw. deren Integration auf Tokens) wie in [1] beschrieben, bildet es somit eine Basis für einheitliche Authentifizierung am Wissenschaftsstandort Göttingen.

Zukünftig wird die Integration in Föderationen (Identity Federation) mehr und mehr relevant. Diese ermöglichen eine dezentrale Nutzung und Single Sign-On für international verteilte Web-Anwendungen. Das Meta-Directory fungiert dabei als Identity Provider und stellt sog. Tokens aus, die als Sicherheitsmerkmal für die Authentifizierung an unterschiedlichen sog. Service Providern, die die

gewünschte Ressource vorhalten, akzeptiert werden. Als Standard für die Definition der Tokens dient die Security Assertion Markup Language (SAML [6]). Ein Beispiel für die Verwendung von SAML im Federation-Umfeld ist Shibboleth [7].

Für Single Sign-On außerhalb von Web-Anwendungen existiert derzeit nur der „de facto"-Standard Kerberos [8]. Somit sind auch unter der Voraussetzung, dass Benutzername und Passwort einheitlich sind, für Anwendungen, die Kerberos nicht unterstützen, nach wie vor mehrfache separate Authentifizierungsvorgänge erforderlich. Verschiedene Identity-Management-Anbieter lösen dies u. a. durch Software-Clients, die auf den Arbeitsplätzen installiert werden, und beim Starten der jeweiligen Anwendung Benutzername und Passwort für den Benutzer eintippen. Das dafür notwendige Passwort beziehen sie in einer verschlüsselten Sitzung z. B. aus dem Meta-Directory (wie im vorherigen Abschnitt beschrieben). Diese Lösungen bieten jedoch eine verminderte Sicherheit, sofern die Anwendungen und zugehörigen Passwort-Eingabe-Dialoge nicht eindeutig von der Software erkannt werden. Ein Beispiel für eine solche Lösung bietet die Fa. Novell mit dem Produkt Secure Login [9].

2.4 Implementierung bei der GWDG

Für den Einsatz im GÖ*-Umfeld wurden die Meta-Directory-Lösungen Microsoft Identity Integration Server [10], Novell Identity Manager [11] und Siemens DirX [12] evaluiert. Aufgrund des leichten funktionalen Vorsprungs wurde die Lösung der Fa. Novell für die Implementierung gewählt. Diese zeichnet sich durch eine flexible Passwort-Synchronisation anhand der o. g. Kriterien, eine dezentrale Administration des Systems, die einen kooperativen Betrieb ermöglicht, sowie eine gute Erweiterbarkeit z. B. um Single-Sign-On-Lösungen aus. Zusätzlich liefert die Lösung ein umfassendes Benutzer-Portal mit, das neben der zentralen Passwort-Verwaltung durch die Benutzer auch web-basierte Workflows und Identity Management Self-Services, wie eingangs beschrieben, bietet.

Die GWDG betreibt seit Oktober 2005 eine Testumgebung als „Proof-of-Concept" des Novell Identity Manager. Gemeinsam mit der Fa. Novell Consulting wurde in dieser Umgebung die reibungslose Synchronisation von Benutzerkonten und Passwörtern implementiert. Dies ermöglicht es, am Standort, innerhalb des GÖ*-Projekts sowie in der GWDG Benutzer-Accounts (Identitäten) in verschiedenen Verzeichnissen und Datenbanken synchron anzulegen und zu löschen. Um die Administration wie auch die Anwendbarkeit für die Benutzer nachhaltig zu vereinfachen, repliziert das System auch die Passwörter gesichert über die angeschlossenen Systeme und vereinheitlicht somit die Authentifizierung der Benutzer. Später kann sukzessive auch der Abgleich z. B. von Adressverzeichnissen, Gruppen, Rechten und Rollen-Modellen über den Identity Manager erfolgen, wie erfolgreiche Tests bestätigt haben. Ermöglicht wird auch die Ausführung von Prozessen während der Verteilung der Benutzer, z. B. um Datenspeicher oder E-Mail-Postfächer anzulegen.

Neben der Testumgebung als „Proof-of-Concept" wurde von der GWDG Ende 2005 ein Produktivsystem realisiert, das zunächst die ca. 33.000 Accounts (ca. 8.000 aktive Nutzer) der Internet-Hotline der Studierenden mit dem Active Directory der GWDG synchronisiert. Das Verfahren, das seit März 2006 produktiv eingesetzt wird, ermöglicht so den Nutzern der Internet-Hotline sowie der GWDG die einfache Verwendung von Arbeitsplätzen auf dem Campus (u. a. im Learning Resources Center (LRC) der SUB und der GWDG).

Erfahrungen bei der Integration der Identitäten aus der Internet-Hotline ermöglichen die für Quartal 3/2006 geplante Synchronisation von Identitäten aus dem GB 3-7 IT in das Active Directory der GWDG. Diese Accounts können dadurch die zentralen Exchange- und Active-Directory-Systeme der GWDG nutzen, und gleichzeitig eine eigenständige Active-Directory-Struktur mit individuellen Sicherheitsanforderungen unabhängig betreiben. Ab Quartal 3/2006 wird das Produktivsystem sukzessive um weitere angeschlossene Verzeichnisse erweitert.

Das Identity Management bzw. Meta-Directory der GWDG ist somit skalierbar ausgelegt und ermöglicht die langfristige Integration einer Vielzahl von Verzeichnissen am Wissenschaftsstandort Göttingen. Hierbei ist ein wesentlich kleinerer administrativer Aufwand für den Abgleich der Verzeichnisse notwendig, als über eigenständige und individuelle z. B. skript-basierte Lösungen. Nutzer und Administratoren können auf mehr Systeme einfach und zentral mit ihren bestehenden Benutzerdaten zugreifen. So wird nachhaltig auch die IT-Sicherheit gestärkt, da weniger Sonderlösungen existieren müssen und der Umgang mit Passwörtern vereinfacht wird.

Abb. 5 zeigt den derzeitigen Fluss der Identitäten im Eclipse-basierten Identity-Management-Werkzeug von Novell.

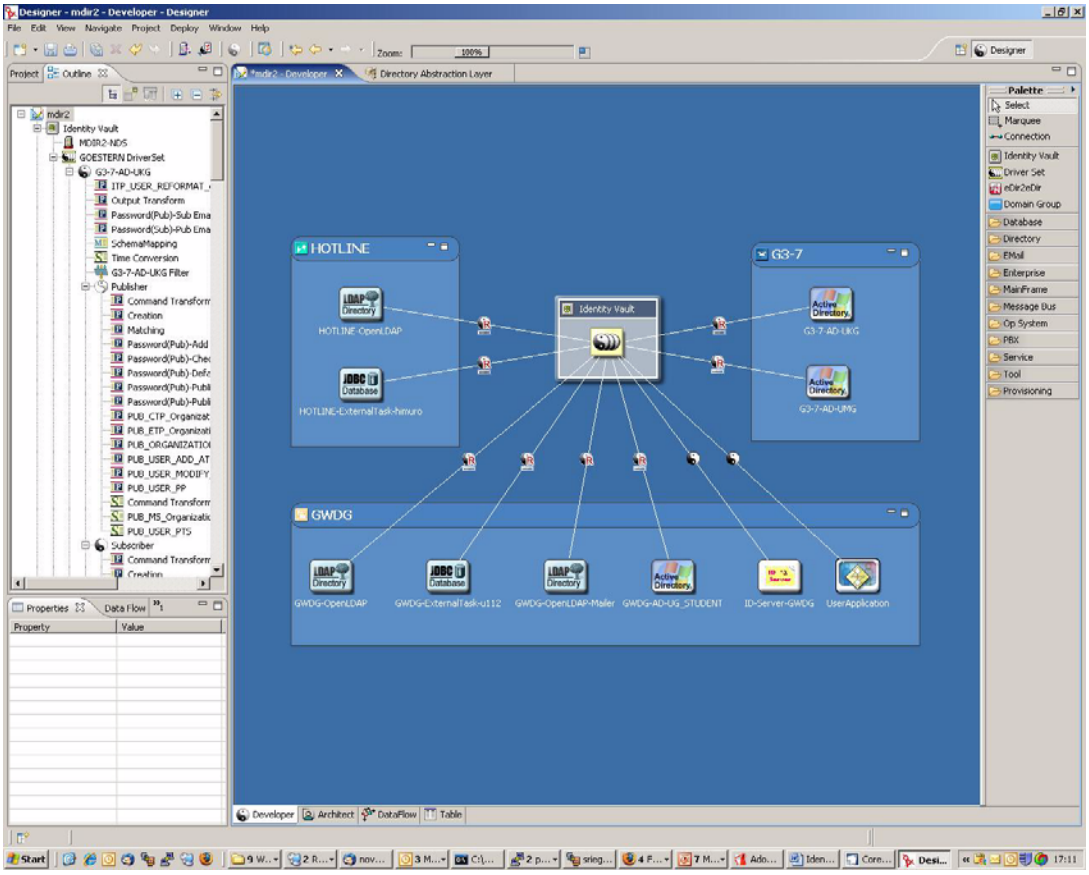


Abb. 5: Identity-Management-Benutzungsoberfläche

2.5 Status und zukünftige Planung

2.5.1 Abgeschlossene Meilensteine bzgl. der Implementierung der Test-Umgebung

- Die Produktauswahl wurde im November 2005 abgeschlossen:

  Novell, Siemens in Endausscheidung

  Novell Identity Manager wegen leichtem funktionalem Vorsprung als Meta-Directory-Lösung im GÖ*-Umfeld gewählt

  instanz-basierte Lizenz (pro gestartetem Meta-Directory), unabhängig von der Anzahl der Identitäten oder verwendeten Treiber

- Coaching von Novell Consulting für Umsetzung des „Proof-of-Concept“ zwischen GWDG und GB 3-7 IT

  Phase 1 (Okt 2005): Kick-Off und Integration OpenLDAP (UNIX)

  Phase 2 (Nov 2005): Integration Active Directory (Windows) / Exchange GWDG

  Phase 3 (Dez 2005): Integration Active Directory / Exchange GB 3-7 IT

- Benutzer- und Organisationsstrukturen werden synchronisiert
- Abgleich der Benutzer löst externe Prozesse (z. B. Anlegung von Verzeichnissen) aus
- Passwörter werden über Portal von Novell sowie aus den Systemen abgeglichen

2.5.2 Aktueller Status

- Die GWDG betreibt derzeit zwei Meta-Directory-Systeme (eine Testumgebung und ein Produktivsystem)
- Im Produktivsystem sind derzeit ca. 32.000 Identitätsobjekte von GB 3-7 IT des Bereichs Humanmedizin der Universität Göttingen, der GWDG und der Internet-Hotline für die Studierenden der Universität Göttingen vorhanden. Dies umfasst auch Identitätsobjekte (bzw. Benutzer) der Universität Göttingen sowie der Max-Planck-Gesellschaft allgemein.
- Innerhalb der GWDG wird der zentrale OpenLDAP-Server als führendes System z. B. mit Verzeichnissen des Mailers synchronisiert und es werden zentral Verwaltungsprozesse, Workflows und Skripte vom Meta-Directory gestartet.
- Die Synchronisation mit den Systemen des GB 3-7 IT ermöglicht hier den Abgleich der

Benutzerkonten zwischen PatLAN und Wiss-LAN im Universitäts-Klinikum.

- Die Integration des OpenLDAP-Servers der Internet-Hotline ermöglicht die Verwendung von Studierenden-Accounts z. B. für die Anmeldung am Active Directory der GWDG, wie sie im Learning Resources Center (LRC) in der Niedersächsischen Staats- und Universitätsbibliothek (SUB) angeboten wird.
- Für alle Benutzer steht ein zentrales Portal unter

  http://benutzer-portal.gwdg.de

  zur Verfügung, das neben dem zentralen Verwalten der Passwörter in den angeschlossenen Systemen auch delegierte Verwaltungsfunktionen sowie Self-Service für die Benutzer bietet. Hierzu folgt ein detaillierter Artikel in einer der nächsten Ausgaben der GWDG-Nachrichten.

2.5.3 Zukünftige Planung

- Im Quartal 3/2006 wird zusätzlich die Synchronisation der GB-3-7-IT-Benutzer zum Exchange-System der GWDG realisiert. Dies ermöglicht es den Benutzern, den Exchange-Service der GWDG zu verwenden, ohne eine weitere separate Benutzerverwaltung zu realisieren. Die Benutzerverwaltung verbleibt eigenständig im Active Directory des GB 3-7 IT und wird über das Meta-Directory synchronisiert.
- Der Abgleich mit dem Active Directory der GWDG wird Anfang Quartal 3/2006 abgeschlossen. Anschließend wird die Integration von externen Workflows im Active Directory z. B. für die Archivierung gelöschter Accounts realisiert.
- Erweiterungen um Verwaltungs-Workflows sowie Single-Sign-On-Lösungen insb. für Web-Anwendungen innerhalb der GWDG und in Kooperation mit der Medizinischen Informatik und der Niedersächsischen Staats- und Universitätsbibliothek sind geplant.
- Für die Quartale 3 u. 4/2006 ist geplant, die Anbindung weiterer Systeme (u. a. SAP und HIS der Universität Göttingen sowie ihres Bereichs Humanmedizin) zu realisieren.
- Um eine unterbrechungsfreie Synchronisation zu gewährleisten, wird im Quartal 3/2006 zusätzlich ein Redundanzystem als Meta-Directory im Rechenzentrum des GB 3-7 IT platziert.

2.6 Referenzen

[1] Rieger: PKI-Leistungen der GWDG. In: 21. DV-Treffen der Max-Planck-Institute; hrsg. v. Gartmann, Jähnke; GWDG-Bericht Nr. 67, 2005, S. 59 - 66

[2] Koke: Der Einfluss des GÖ*-Projektes auf die MPG. In: 19. und 20. DV-Treffen der Max-Planck-Institute; hrsg. v. Bussmann, Oberreuter; GWDG-Bericht Nr. 66, 2004, S. 65 - 79

[3] OpenLDAP:

http://www.openldap.org

[4] Active Directory:

http://www.microsoft.com/activedirectory

[5] Heuer, Ißleiber: LDAP in der GWDG - Einsatzspektrum. In: 21. DV-Treffen der Max-Planck-Institute; hrsg. v. Gartmann, Jähnke; GWDG-Bericht Nr. 67, 2005, S. 53 - 58

[6] Security Assertion Markup Language:

http://www.oasis-open.org/committees/security

[7] Shibboleth:

http://shibboleth.internet2.edu

[8] Kerberos:

http://web.mit.edu/kerberos

[9] Secure Login:

http://www.novell.com/securelogin

[10] Microsoft Identity Integration Server:

http://www.microsoft.com/miis

[11] Novell Identity Manager:

http://www.novell.com/idm

[12] Siemens DirX:

http://www.siemens.com/index.jsp?sdc_p=t4cz3s4u0o1180841pHPnfl0mi1077887

Rieger

3. Intrusion Detection und Prevention im GÖNET (Teil 1)

3.1 Einleitung

Im ersten Teil des zweiteiligen Artikels werden Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS) dargestellt sowie die Produktauswahl bei der Suche nach einer geeigneten Lösung zum Schutz des GÖNET vorgestellt. Der zweite Teil in der August-Ausgabe der GWDG-Nachrichten beschreibt dann das bei der GWDG eingesetzte IPS im Detail und verdeutlicht die Vorteile für die am GÖNET angeschlossenen Institute und Benutzer.

In den letzten Jahren haben sich IDS und IPS zu einem festen Bestandteil der Sicherheitsinfrastruktur entwickelt. IPS und IDS schließen eine wesentliche Lücke zwischen meist schon vorhandenen Firewalls und Virenscannern.

Für einen ausreichenden Schutz des GÖNET sind bereits an den zentralen Standorten leistungsfähige Firewallsysteme integriert (vgl. die GWDG-Nachrichten 2/2006). Überdies steht ein reichlich genutztes Angebot an Virenscannern zum Schutz der lokalen Systeme in den Instituten zur Verfügung. Dennoch existiert eine Bedrohungslage, die für den Benutzer nicht leicht zu erkennen ist. Attacken und Eindringlinge werden i. d. R. nicht durch Firewalls und Virenscanner erkannt und entsprechend bekämpft. Ausgenutzte Sicherheitslücken der Betriebssysteme führen häufig zu einer Kompromittierung des eigenen Rechners, oft auch über einen längeren Zeitraum und häufig vom Benutzer unbemerkt. In der Folge werden diese Rechner dann selbst zu einer Quelle diverser Attacken innerhalb des eigentlich sicheren Netzwerkes. Die von der GWDG erhobenen Statistiken hinsichtlich Attacken und Angriffen im GÖNET zeigen zwar einen positiven Einfluss als Folge der Integration der GÖNET-Firewalls, machen aber auch deutlich, dass die Anzahl subtiler und komplexer Attakken und Angriffe durch die bestehenden Komponenten allein nicht zu reduzieren ist.

Genau an dieser Stelle entsteht ein Bedarf an mehr Sicherheit, welcher durch den Einsatz eines IPS/IDS gedeckt werden kann.

3.2 Anforderungen und Motive für ein IPS/IDS

Die Anforderungen an einen so komplexen Sicherheitsmechanismus sind nicht gering. Für die Auswahl eines geeigneten Systems sind für die GWDG die folgenden Merkmale entscheidend:

- **Absicherung des lokalen Netzwerkes**

  Ein IDS/IPS soll in erster Linie das lokale Netzwerk vor Attacken schützen.

- **Automatische Abwehr**

  Um den Wartungsaufwand für ein solches System gering zu halten, sollte es nach Möglichkeit angemessen und vollständig autonom auf etwaige Bedrohungen reagieren, ohne das ein Administrator eingreifen muss.

- **Über Bedrohungen benachrichtigen**

  Entscheidend ist auch die Benachrichtigung über die erfolgte Abwehr von Attacken. Überdies sollten alle Ereignisse in einem geeigneten Verfahren mitprotokolliert werden können (Logging).

- **Hohe Bandbreite**

  Damit ein IPD/IDS den Datenverkehr nicht stört oder beeinträchtigt, muss es eine dem Netzwerk angepasste Bandbreite besitzen. Im GÖNET wird an den entscheidenden Knotenpunkten mit Bandbreiten von 1 GBit/s gearbeitet. Diese Bandbreite muss ein IPS beherrschen.

- **Schnelle Reaktion auf neue Bedrohungen sowie hohe Erkennungsrate**

  Die Qualität der Erkennung von Attacken ist das wesentliche Merkmal für ein IPS/IDS. Da nahezu täglich neue Varianten diverser Attakken auftreten, muss ein IPS diesem Umstand Rechnung tragen und sich entsprechend schnell an die immer wieder neue Bedrohungslage anpassen.

- **Einfaches Management**

  Das System sollte eine Managementumgebung mitbringen, mit der auch Nicht-Netzwerkexperten eine Einschätzung der Gefahrensituation erlaubt. Überdies sollte das IPS in eine standardisierte Managementumgebung integriert werden können und eine automatische Alarmierung bei Notsituationen erlauben.

Die Motive sind klar. Um sich vor weniger auffälligen und von den bisherigen Sicherheitseinrichtungen wie Firewall und Virenscannern nicht zu erkennenden Angriffen schützen zu können, muss eine neues System im Netzwerk integriert werden, welches speziell für diesen Zweck geschaffen wurde. Erfolgreiche Angriffe auf Rechner im GÖNET können erheblichen Schaden anrichten, wenn von dem befallenen System weitere Rechner attackiert werden.

3.3 Was ist ein IDS?

Die grundlegende Aufgabe eines IDS (Intrusion-**Detection**-System) ist die Erkennung von

- Attacken und
- abnormalen Verhalten im Netzwerk.

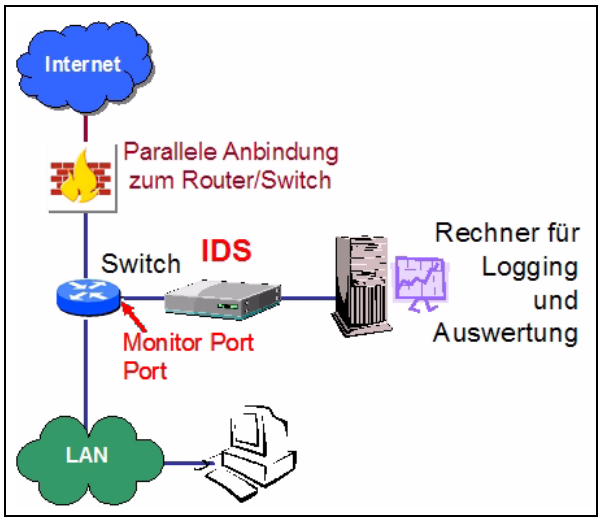
Anders als Firewalls versuchen IDS/IPS den Netzwerkverkehr auf den höheren Protokollschichten zu analysieren. Das wird in der Praxis bis zur Anwendungsschicht (Layer 7) realisiert. Über die Analyse des Datenverkehrs und das Vergleichen mit bekannten Angriffsmustern und Signaturen versuchen IDS Attacken zu erkennen. Ein IDS muss demnach so angeordnet sein, dass es den zu überwachenden Datenstrom „mitlesen“ kann. Hierbei werden die Systeme nicht unmittelbar in den Datenstrom integriert, sondern vielmehr parallel zum Datenstrom angebunden. Dieses kann häufig über Switches erreicht werden, bei denen ein bestimmter Port als „Monitoring“-Port eingestellt werden kann. Über diesen Monitoring-Port wird der Datenstrom parallel zum IDS geleitet, der wiederum die Netzwerkpakete auf Attacken und Unregelmäßigkeiten untersuchen kann. Eines der Probleme bei dieser Variante ist die Tatsache, dass bei einem Ethernet-Switch mit mehreren Ports nur ein Port für das Monitoring genutzt werden kann und dadurch nicht der gesamte über den Switch laufende Traffic über diesen Port sichtbar ist.

Nehmen wir einen 24-Port-FastEthernet-Switch mit 100 MBit/s pro Port. Wenn der Switch nur zur Hälfte auf allen anderen Ports ausgelastet ist (23 x 50 MBit/s = 1,18 GBit/s), kann der resultierende Gesamttraffic unmöglich auf dem einen 100-MBits/s-Monitoring Port ausgegeben werden. Deshalb sind meistens nur direkte Port-Paarungen möglich. Nur ein Port kann zu einem Monitoring-Port gespiegelt werden. Durch geschickte Auswahl des zu überwachenden Ports kann jedoch häufig eine Überwachung der entscheidenden Netzwerkdaten gelingen.

Für IDS ist es auch nicht unbedingt relevant, jedes Paket mitlesen zu können. Häufig genügt es, nur einen Teil des Netzwerkverkehrs zu überprüfen, basierend auf der Annahme, dass eine Attacke mehrfach vorkommt und die Wahrscheinlichkeit der Erkennung mit der Häufigkeit der Attacke wächst. Das trifft insbesondere bei (D)DOS-Attacken (DOS = Denial of Service) zu, die oft mit hohen Datenaufkommen einhergehen. Ein vollkommener Schutz vor Angriffen ist bekanntlich nicht möglich, so dass viele Systeme sich auf die Erkennung der wesentlichen Attacken beschränken.

Dennoch gibt es Angriffe, die nur aus einem einzigen Netzwerkpaket resultieren und dadurch oft nicht von einen IDS erfasst werden.

Das folgende Bild stellt eine typische Integration eine IPS im Netzwerk dar:



Der entscheidende Nachteil im Vergleich zu einem IPS ist die Tatsache, dass Angriffe zwar protokolliert werden, aber keine automatische Gegenabwehr eingeleitet wird. Ein IDS ist ein passives Überwachungssystem und daher vergleichbar mit einem „Wolf ohne Zähne“. Mit dem Einsatz eines IDS geht ein außerordentlich hoher Administrationsaufwand einher. Bei jeder Attacke bleibt es dem Administrator überlassen, welche Maßnahmen einzuleiten sind. Wenn man sich die Vielzahl der Attacken aus dem Internet in das GÖNET ansieht, wird schnell klar, dass der Einsatz eines IDS als alleiniges System zur Verhinderung von Angriffen nicht beherrschbar ist.

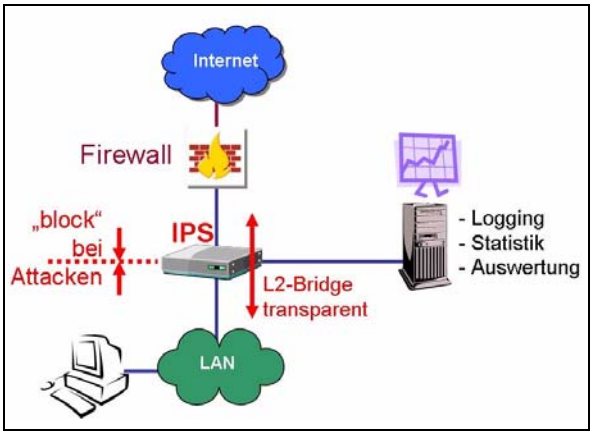
Uns erreichen im GÖNET täglich zwischen 1.000 und 100.000 Attacken von einigen Hundert bis einigen Tausend verschiedenen Quellen. Ein Administrator mit dem IDS als Werkzeug ist diesem Umstand hilflos ausgeliefert. Überdies ist auch die Gegenabwehr bei Attacken nicht trivial, wenn diese manuell erfolgen muss. Oft bleibt dem Administrator nur das „Unterbrechen“ der Kommunikationsbeziehung zwischen Angreifer und Opfer. Ist der Angriff eine (D)DOS-Attacke, wird das Szenario schnell zu einem Desaster, da die Angriffe aus vielen Quellen kommen.

3.4 Was ist ein IPS?

Die Fähigkeiten des IDS sind auch bei einem IPS (Intrusion-**Prevention**-System) zu finden. Es entdeckt Attacken sowie abnormales Verhalten. Der entscheidende Unterschied ist aber die von einem IPS ausgehende automatische Gegenabwehr bei Angriffen. Der Datenstrom wird beim IPS in gleicher

weise überwacht. Wird ein Angriff identifiziert, kann ein IPS die Kommunikationsbeziehung entweder vollständig unterbrechen oder nur die entscheidenden schadhaften Netzwerkpakete herausfiltern, indem die TCP- oder UDP-Verbindung für die benutzten (TCP/UDP)-Ports unterbrochen wird. Nützlicher bzw. gewünschter Datenverkehr kann so vom schadhaften Traffic isoliert werden.

Folgendes Bild verdeutlicht den Einsatz eines IPS im lokalen Netzwerk:



Durch ein IPS kann aufgrund der automatisierten Abwehr von Attacken der administrative Aufwand im Vergleich zum IDS ganz erheblich reduziert werden, im Idealfall bis hin zu einem vollkommen autonomen System nahezu ohne manuellen Eingriff. Die Zeit zwischen der Erkennung der Attacke und der Gegenabwehr ist beim IPS auf ein Minimum reduziert.

Ein IPS muss gute Filter haben!

Funktionsbedingt muss die Qualität der Erkennung bei einem IPS im Vergleich zum IDS erheblich höher sein. „False Positive“-Erkennung, also die Bewertung von legalem Traffic als Attacke, hat bei einem IPS viel weiterreichendere Konsequenzen als bei einem IDS, da die Verbindung automatisch blockiert werden würde. Sind Lücken oder Schwächen bei der Erkennung eines IPS bekannt, könnten diese quasi als DOS-Angriff zweckentfremdet werden. „False Positives“ sollten demnach bei einem IPS nicht auftreten, was zwar nicht immer der Realität entspricht, aber dennoch von vielen Systemen annähernd erreicht wird.

3.5 Vergleich IPS/IDS

Wenngleich die enge Verwandtschaft zwischen IPS und IDS deutlich ist, existieren aufgrund des entscheidenden Unterschieds gravierende Vor- und Nachteile beim direkten Vergleich der Systeme.

Die folgende Tabelle vergleicht IPS und IDS:

IDS	IPS
Vorteil: • Einsatz mehrerer Sensoren im Netz	Nachteile: • aktive Abwehr von Angriffen • geringerer administrativer Aufwand
Nachteile: • Überwachung des IDS durch Administrator erforderlich • manuelle Reaktion auf Attacken erforderlich • (zu) viele Logginginformationen	Nachteile: • im inline-mode: schnelle Erkennung und Reaktion erforderlich • teure Hardware, d. h. hoher Preis

3.6 Diverse „Typen“ von IDS und IPS

IDS sowie IPS können in verschiedenen Konfigurationen im Netzwerk integriert werden. Es lassen sich zwei grundlegend unterschiedliche Klassen unterscheiden:

1. Hostbasierte IDS/IPS (HIPS)

Kleinere Formen eines IDS/IPS sind bereits in einiger Antivirensoftware als Ergänzung zu finden. Hostbasierte Systeme sind immer auf einem Rechner als Software installiert und schützen damit auch ausschließlich das lokale System. Der entscheidende Vorteil ist die Erkennung von schadhaften Prozessen auf dem eigenen Rechner (RootKits etc.). Ein zentrales IPS kann nicht die Prozesse eines Betriebssystems erkennen und ggf. schützen.

2. Netzbasierte IDS/IPS (NIPS)

Netzbasierte IPS werden an zentraler Stelle im Netzwerk platziert. Sie schützen im Vergleich zum „HIPS“ ein gesamtes Netzwerksegment und sind weniger auf den Schutz des einzelnen lokalen Host fixiert.

Eine Kombination aus beiden Varianten ist durchaus denkbar, um die Vorteile beider Systeme nutzen zu können.

Die folgende Tabelle verdeutlicht die Vor- und Nachteile beider Verfahren:

Hostbasierte IPS (HIPS)	Netzbasierte IPS (NIPS)
Vorteile: • geringe Datenmenge, Bandbreite • Systemzustand auf Rechner erkennbar, „schädlicher Code“ • bei „false positive“ nur eigenes System betroffen	Vorteile: • kann ganzes Segment überwachen/schützen • besserer Schutz bei (D)DoS-Attacken • Überblick über gesamtes Netz (Gesamtbild ergibt erst eine Attacke) • sieht auch Attacken auf unbenutzten Adressen • zentrales Management
Nachteile: • ggf. auf OS-Ebene auszuhebeln, da Programm/Dienst-basierend • Verwaltung pro Host (Aufwand) • eingeschränkte Sicht (nur eigener Host)	Nachteil: • hohe Bandbreite (erforderlich) und damit verbundene Latenzen

3.7 Auswahl des geeigneten Systems

Die GWDG hatte für die Auswahl eines für das GÖNET geeigneten IDS/IPS verschiedene Produkte entweder im Test oder deren Fähigkeiten im Rahmen einer Produktstudie analysiert. Nahezu alle großen Netzwerkhersteller haben auch ein IPS im Produktportfolio. Gelegentlich sind es nur Erweiterungen bereits bestehender IDS, die durch Titelkosmetik und leichte Modifikationen zu einem IPS erweitert wurden. Abhängig davon, aus welchem Bereich der Hersteller kommt, besitzen die IPS entsprechende Stärken und Schwächen. Cisco, Enterasys, 3COM sowie Fortigate kommen aus dem Netzwerkbereich. McAffee stammt klassisch aus dem Bereich der Virenerkennung. Oft ist das Knowhow durch Zukauf einer Firma in die eigene Produktpalette des Herstellers gelangt (Bsp.: 3COM und McAffee) oder wurde durch Partnerschaften ergänzt (Bsp.: Cisco & McAffeee).

Auch die Fähigkeiten des OpenSource-nProduktes „Snort“ wurde als Alternative im Rahmen einer Testinstallation bei der GWDG untersucht.

Genauer betrachtet wurden:

Produkt	Grundlage der Bewertung
1. **Cisco IDS/IPS**	Bewertung durch Vorführung von Cisco sowie Besuche von Cisco-Partnern bei der GWDG
2. **McAffee** (Intrushield als Appliance)	Im Rahmen mehrerer Vorstellungen von McAffee bei der GWDG bewertet
3. **Fortigate** (Fortinet: Firewalls mit IDS/IPS-Zusatz basierend auf Snort in einer Appliance)	Vorstellung des Herstellers bei der GWDG sowie kurze 10-tägige Testphase im Rahmen der Firewallauswahl bei der GWDG
4. **Snort** (OpenSource)	Testphase im lokalen Netz sowie Schulung im Rahmen des DV-Treffens der Max-Planck-Institute 2005
5. **Dragon von Enterasys (IDS)**	Als Appliance; Betrieb bei der GWDG 2004
6. **Tippingpoint (3COM)**	Bewertung im Rahmen eines 14-tägigen Tests bei der GWDG.

3.8 Die Ergebnisse im Überblick

Ganz entscheidend für den Einsatz eines IPS im GÖNET ist die Bandbreite des Systems. Viele Produkte schieden allein aufgrund der geringen Performance aus. Immerhin verfügt die GWDG über eine Internetanbindung von 1 GBit/s. Ein System musste in der Lage sein, diese Bandbreite ohne nennenswerte Beeinträchtigungen für die Benutzer zu bedienen. Klar war überdies, dass ein reines IDS aufgrund der nicht vorhandenen Mechanismen zur Gegenabwehr und des hohen Administrationsaufwands nicht in Frage kommt.

1. Die **Cisco-**IPS-Lösung war Bestandteil eines großen Sicherheitskonzeptes mit dem Namen „Cisco Self-Defending Network“. Hier wurde ein IDS/IPS als Sensor im Netzwerk platziert und meldeten einer zentralen Einrichtung die Ergebnisse, die wiederum mit weiteren Ergebnissen aus Logfiles und Ereignisanalyse weiterer Systeme zu einem Gesamtbild korreliert werden. Der entscheidende Nachteil dieser Lösung in Hinblick auf die derzeitige Struktur im GÖNET war die Tatsache, dass das Gesamtsystem ausschließlich Cisco-Komponenten erwartet. Systeme anderer Hersteller wurden, wenn überhaupt, nur sehr unzureichend unterstützt. Darüber hinaus konnten andere Systeme in der Erkennungsleistung mehr überzeugen.

2. **McAffee**(s) Intrushield-Ansatz sah zunächst sehr vielversprechend aus. Hier werden nur Dinge überprüft, die auch wirklich eine Gefahr für die Rechner darstellen. Eine IIS(Internet Information Server)-Attacke auf einen Apache-Webserver bleibt in der Regel folgenlos und ist damit für das Erkennungssystem von geringem Interesse. Der Nachteil dieser Lösung lag in der geringeren Bandbreite. Für die Analyse von Datenströmen von 1 GBit/s an mehreren Stellen im GÖNET gleichzeitig war das System nicht ausgelegt.

3. Fortinets **Fortigate**-Lösung ist primär eine Firewall mit einem IPS als „AddOn“. Da die GWDG sich bei der Auswahl einer geeigneten Firewalllösung im GÖNET für Cisco entschiedenen hatten (vgl. die GWDG-Nachrichten 2/2006), ist ein wesentliches Argument hinsichtlich einer einheitlichen Gesamtlösung nicht mehr vorhanden. Überdies hatte Fortigate lediglich eine angepasste Snort-Lösung in den Firewalls integriert, welche die geforderte Bandbreite nicht erreichte.

4. **Snort** als einziges OpenSource-Produkt im Test ist primär ein IDS. Bereits 1998 waren erste Snort-Varianten verfügbar. Erst später kamen Mechanismen hinzu, unerwünschte Verbindungen aktiv zu beenden (TCP-Reset etc.). Gerade dieser Bereich ist aber im Vergleich zu einigen kommerziellen IPS-Lösungen noch nicht so weit entwickelt, so dass ein Einsatz im GÖNET als einziges IPS nicht sinnvoll erscheint. Dennoch hat Snort eine sehr große Verbreitung gefunden. In Verbindung mit kommerziellen Systemen wäre der Einsatz von Snort als „Sensor“ im GÖNET durchaus denkbar. Aufgrund der großen „Community“ findet bei Snort eine ständige, unter OpenSource stehende Weiterentwicklung statt, obwohl Snort auch einen kommerziellen Zweig besitzt. Die damaligen Snort-Entwickler hatten eine eigene Firma namens „Sourcefire“ gegründet.

   Ein weiteres im OpenSource-Bereich angesiedeltes IPS ist „**Hogwash**“ (`http://hogwash.sourceforge.net`). Im Vergleich zu Snort ist es als IPS konzipiert worden. Bei der Bewertung der Einsatzfähigkeit im GÖNET treffen aber die gleichen Kriterien zu wie bei Snort.

5. Enterasys **Dragon** schied von vornherein aus, da es sich lediglich um ein IDS handelt.

6. **Tippingpoint (3COM)** ist ein spezialisierter Hersteller von IDS/IPS gewesen, welcher von 3COM aufgekauft wurde und als eigene „Division“ bei 3COM unter dem alten Namen firmiert. Das System wurde der GWDG Ende 2005 von 3COM vorgestellt. Im Anschluss daran konnte wir das Tippingpoint-System für etwa drei Wochen im Einsatz bei der GWDG getestet werden. Aufgrund der Ergebnisse dieser Tests und der Vergleiche mit den anderen Lösungen hatte die GWDG sich für das Tippingpointsystem als zentrales IPS entschieden. Nicht zuletzt der sehr erfolgreiche Test bei der GWDG und die sehr hohe Bandbreite waren ausschlaggebend für diese Entscheidung. Das System lässt sich als vollkommen transparentes Gerät in den Datenstrom integrieren und ermöglicht damit einen sehr unkomplizierten Einsatz im GÖNET.

Im zweiten Teil dieses Artikels, der in der August-Ausgabe der GWDG-Nachrichten erscheint, wird das bei der GWDG eingesetzte IPS-System Tippingpoint näher beschrieben.

Ißleiber

4. Kurse des Rechenzentrums

4.1 Allgemeine Informationen zum Kursangebot der GWDG

4.1.1 Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

4.1.2 Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die

GWDG
Kursanmeldung
Postfach 2841
37018 Göttingen

oder per E-Mail an die Adresse auftrag@gwdg.de mit der Subject-Angabe „Kursanmeldung“ erfolgen. Für die schriftliche Anmeldung steht unter

http://www.gwdg.de/service/nutzung/antragsformulare/kursanmeldung.pdf

ein Formular zur Verfügung. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager - eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu authorisierte Person - oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils 7 Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit dem Dispatcher (Tel.: 0551 201-1523, E-Mail: auftrag@gwdg.de) möglich. Eine Anmeldebestätigung wird nur an auswärtige Institute oder auf besonderen Wunsch zugesendet. Falls eine Anmeldung wegen Überbelegung des Kurses nicht berücksichtigt werden kann, erfolgt eine Benachrichtigung.

4.1.3 Kosten bzw. Gebühren

Die Kurse sind - wie die meisten anderen Leistungen der GWDG - in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

4.1.4 Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu 8 Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

4.1.5 Kursorte

Die meisten Kurse finden in Räumen der GWDG oder des Max-Planck-Instituts für biophysikalische Chemie statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Fassberg, 37077 Göttingen, der Große Seminarraum im Allgemeinen Institutsgebäude dieses Instituts. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL

http://www.gwdg.de/gwdg/standort/lageplan

zu finden. Der gemeinsame Schulungsraum von GWDG und SUB befindet sich im Untergeschoss der Niedersächsischen Staats- und Universitätsbibliothek, Platz der Göttinger Sieben 1, 37073 Göttingen.

4.1.6 Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL

http://www.gwdg.de/service/kurse

zu finden. Anfragen zu den Kursen können an den Dispatcher per Telefon unter der Nummer 0551 201-1524 oder per E-Mail an die Adresse auftrag@gwdg.de gerichtet werden. Zweimal jährlich wird ein Katalog mit dem aktuellen GWDG-Kursprogramm versendet. Interessenten, die in den

Verteiler aufgenommen werden möchten, können dies per E-Mail an die Adresse gwdg@gwdg.de mitteilen.

4.2 Kurse von August bis Dezember 2006 in thematischer Übersicht

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	• 13.09.2006 • 15.11.2006	Dr. Heuer, Nolte, Wagenführ Dr. Heuer, Nolte, Wagenführ
Einführung in die Nutzung des Leistungsangebots der GWDG	• 06.09.2006 • 06.12.2006	Dr. Grieger Dr. Grieger
Einführung in Aufbau und Funktionsweise von PCs	• 31.10.2006	Eyßell
Einführung in die Bedienung von Windows-Oberflächen	• 01.11.2006 - 03.11.2006	Eyßell
Führung durch das Rechnermuseum	• 01.09.2006 • 29.09.2006 • 10.11.2006 • 15.12.2006	Eyßell Eyßell Eyßell Eyßell

Betriebssysteme

Kurse	Termine	Vortragende
Schnellkurs UNIX für Windows-Benutzer mit Übungen	• 27.11.2006 - 28.11.2006	Dr. Bohrer
Grundkurs UNIX/Linux mit Übungen	• 17.10.2006 - 19.10.2006	Hattenbach
UNIX für Fortgeschrittene	• 06.11.2006 - 08.11.2006	Dr. Sippel
UNIX/Linux-Arbeitsplatzrechner - Installation und Administration	• 11.12.2006 - 12.12.2006	Dr. Heuer, Dr. Sippel
UNIX/Linux-Server - Grundlagen der Administration	• 13.12.2006 - 14.12.2006	Dr. Heuer, Dr. Sippel
UNIX/Linux - Systemsicherheit für Administratoren	• 15.12.2006	Dr. Heuer, Dr. Sippel
Windows 2000/XP/2003 in kleinen Netzwerken	• 13.11.2006 - 14.11.2006	Quentin
Die Windows-Active-Directory-Domäne	• 15.11.2006 - 17.11.2006	Quentin
Cluster- und Raid-Konfigurationen unter Windows 2003	• 31.10.2006	Quentin

Netze / Internet

Kurse	Termine	Vortragende
Sicherheit im Internet für Anwender	• 01.12.2006	Reimann
Web Publishing II	• 31.08.2006 - 01.09.2006	Reimann

Grafische Datenverarbeitung

Kurse	Termine	Vortragende
Grundlagen der Bildbearbeitung mit Photoshop	• 06.09.2006 - 07.09.2006	Töpfer
Photoshop für Fortgeschrittene	• 09.10.2006 - 10.10.2006	Töpfer

Sonstige Anwendungssoftware

Kurse	Termine	Vortragende
Einführung in das Computeralgebra-System Mathematica	• 11.10.2006 - 12.10.2006	Dr. Schwardmann
MindMapping mit MindManager	• 05.10.2006	Reimann
Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG	• 20.10.2006	Reimann
Neuer Kurs !!! PDF-Formulare mit Acrobat Professional und Adobe Designer erstellen	• 05.09.2006	Dr. Baier
PowerPoint	• 09.11.2006 - 10.11.2006	Reimann
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, YACOP	• 25.09.2006 - 28.09.2006	Dr. Bohrer, Dr. Liesegang
DNA-Sequenzierung mit dem Staden Package	• 29.09.2006	Dr. Liesegang
Mit StarOffice zum Schwarzen Loch	• 14.11.2006	Dr. Grieger

Programmiersprachen

Kurse	Termine	Vortragende
Programmierung von Parallelrechnern	• 28.11.2006 - 30.11.2006	Prof. Haan, Dr. Boehme, Dr. Schwardmann
Neuer Kurs !!! Entwicklung von Anwendungen mit Visual Studio 2005 Express Editions - eine Einführung	• 12.09.2006	Hindermann

4.3 Kurse von August bis Dezember 2006 in chronologischer Übersicht

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Web Publishing II	Reimann	31.08.2006 - 01.09.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	24.08.2006	8
Führung durch das Rechner-museum	Eyßell	01.09.2006 10.00 - 12.30 Uhr	25.08.2006	0
Neuer Kurs !!! PDF-Formulare mit Acrobat Profes-sional und Adobe Designer erstellen	Dr. Baier	05.09.2006 09.15 - 12.00 Uhr und 13.00 - 16.00 Uhr	29.08.2006	4
Grundlagen der Bildbearbeitung mit Photoshop	Töpfer	06.09.2006 - 07.09.2006 09.30 - 16.00 Uhr	30.08.2006	8
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	06.09.2006 17.00 - 20.00 Uhr (SUB)	30.08.2006	0
Neuer Kurs !!! Entwicklung von Anwendungen mit Visual Studio 2005 Express Editions - eine Einführung	Hindermann	12.09.2006 09.00 - 12.30 Uhr und 13.30 - 17.30 Uhr	05.09.2006	4
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	13.09.2006 16.15 - 17.45 Uhr	06.09.2006	1
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, YACOP	Dr. Bohrer, Dr. Liesegang	25.09.2006 - 28.09.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	18.09.2006	16
DNA-Sequenzierung mit dem Staden Package	Dr. Liesegang	29.09.2006 09.30 - 12.30 Uhr und 13.30 - 16.00 Uhr	22.09.2006	4
Führung durch das Rechner-museum	Eyßell	29.09.2006 10.00 - 12.30 Uhr	22.09.2006	0
MindMapping mit MindManager	Reimann	05.10.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	28.09.2006	4
Photoshop für Fortgeschrittene	Töpfer	09.10.2006 - 10.10.2006 09.30 - 16.00 Uhr	02.10.2006	8
Einführung in das Computeralgebra-System Mathematica	Dr. Schwardmann	11.10.2006 - 12.10.2006 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	04.10.2006	8
Grundkurs UNIX/Linux mit Übungen	Hattenbach	17.10.2006 - 19.10.2006 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	10.10.2006	12
Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG	Reimann	20.10.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	13.10.2006	4

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Cluster- und Raid-Konfigurationen unter Windows 2003	Quentin	31.10.2006 09.15 - 12.30 Uhr und 13.30 - 16.15 Uhr	24.10.2006	4
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	31.10.2006 09.15 - 12.30 Uhr	24.10.2006	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	01.11.2006 - 03.11.2006 09.15 - 12.30 Uhr	25.10.2006	6
UNIX für Fortgeschrittene	Dr. Sippel	06.11.2006 - 08.11.2006 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr	30.10.2006	12
PowerPoint	Reimann	09.11.2006 - 10.11.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	02.11.2006	8
Führung durch das Rechner-museum	Eyßell	10.11.2006 10.00 - 12.30 Uhr	03.11.2006	0
Windows 2000/XP/2003 in kleinen Netzwerken	Quentin	13.11.2006 - 14.11.2006 09.30 - 15.30 Uhr	06.11.2006	8
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	14.11.2006 09.00 - 12.00 Uhr	07.11.2006	2
Die Windows-Active-Directory-Domäne	Quentin	15.11.2006 - 17.11.2006 09.30 - 15.30 Uhr (am 17.11. bis 13.30 Uhr)	08.11.2006	10
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	15.11.2006 16.15 - 17.45 Uhr	08.11.2006	1
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	27.11.2006 - 28.11.2006 13.00 - 16.00 Uhr	20.11.2006	4
Programmierung von Parallelrech-nern	Prof. Dr. Haan, Dr. Boehme, Dr. Schwardmann	28.11.2006 - 30.11.2006 09.15 - 12.15 Uhr und 13.30 - 16.30 Uhr	21.11.2006	12
Sicherheit im Internet für Anwender	Reimann	01.12.2006	24.11.2006	2
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	06.12.2006 17.00 - 20.00 Uhr	29.11.2006	0
UNIX/Linux-Arbeitsplatzrechner - Installation und Administration	Dr. Heuer, Dr. Sippel	11.12.2006 - 12.12.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	04.12.2006	8
UNIX/Linux-Server - Grundlagen der Administration	Dr. Heuer, Dr. Sippel	13.12.2006 - 14.12.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	06.12.2006	8
UNIX/Linux - Systemsicherheit für Administratoren	Dr. Heuer, Dr. Sippel	15.12.2006 09.30 - 12.30 Uhr und 13.30 - 15.00 Uhr	08.12.2006	4
Führung durch das Rechner-museum	Eyßell	15.12.2006 10.00 - 12.30 Uhr	08.12.2006	0

5. Betriebsstatistik Juni 2006

5.1 Nutzung der Rechenanlagen

Rechner	Zahl der Prozessoren	CPU-Stunden
DECalpha	8	268,21
IBM RS/6000 SP	152	4.701,53
IBM Regatta	124	64.815,51
Linux Parallel	252	133.723,02
Linux Opteron	96	59.994,79

5.2 Betriebsunterbrechungen

Rechner/PC-Netz	Störungen		System-pflege	
	Anzahl	Stunden	Anzahl	Stunden
UNIX-Cluster	0		0	
IBM SP/Regatta	1	10,00	0	
Linux Parallel	1	1,00	0	
Linux Opteron	1	1,00	0	
PC-Netz	0		0	
Nameserver	0		0	
Mailer	1	9,80	0	

6. Autoren dieser Ausgabe

Name	Artikel	E-Mail-Adresse / Telefon-Nr.
Andreas Ißleiber	• Intrusion Detection und Prevention im GÖNET (Teil 1)	aisslei@gwdg.de 0551 201-1815
Sebastian Rieger	• Identity Management bei der GWDG	srieger1@gwdg.de 0551 201-1878
Timo Scheller	• Digitale Langzeitarchivierung bei der GWDG – neue technische Infrastruktur	tschell@gwdg.de 0551 201-1559
Dagmar Ullrich	• Digitale Langzeitarchivierung bei der GWDG – neue technische Infrastruktur	dullric@gwdg.de 0551 201-1827