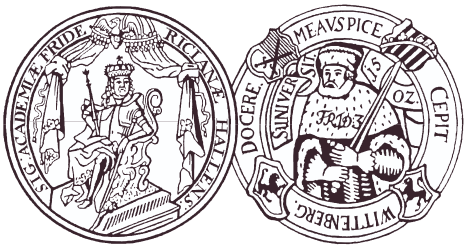
MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG



IT-Strategie der Martin-Luther-Universität Halle-Wittenberg

Verabschiedet vom Rektorat der MLU am 5. Juli 2011

Vorgelegt vom IT-Lenkungsausschuss der MLU am 21. Juli 2011 in Ergänzung der IT-Strategie der MLU vom 3. Juli 2011

Inhaltsverzeichnis

In diesem Dokument wird die IT-Strategie der Martin-Luther Universität Halle-Wittenberg dargestellt. Sie bezieht sich im Grundsatz auf alle Fakultäten und Einrichtungen der Universität. Für die Hochschulmedizin gilt, dass die IT-Infrastruktur der Medizinischen Fakultät in den Bereichen, die eng mit der Krankenversorgung des Universitätsklinikums verzahnt sind, über einen Geschäftsbesorgungsvertrag vom Klinikrechenzentrum betreut wird. Aus diesem Grund haben die Medizinische Fakultät und das Universitätsklinikum ein gemeinsames IT-Rahmenkonzept erarbeitet und verabschiedet. Dieses entspricht im Bereich Forschung und Lehre der IT-Strategie der Universität.

1. Einordnung

Die Martin-Luther-Universität Halle-Wittenberg ist mit einer 500-jährigen Geschichte eine traditionsreiche Universität im deutschen Sprachraum. Gegenwärtig studieren ca. 19.400 Studierende in 260 Studiengängen an der Universität. Rund 340 Professorinnen und Professoren, 3.000 Wissenschaftlerinnen, Wissenschaftler und sonstige Beschäftigte sind in 9 Fakultäten, einem Zentrum für Ingenieurwissenschaften und einer Reihe zentraler Einrichtungen tätig. Das Forschungs- und Lehrspektrum deckt weite Bereiche der Natur-, Geistes- und Sozialwissenschaften, der Theologie sowie der Medizin ab.

Forschungsschwerpunkte stellen die Biowissenschaften (Exzellenznetzwerk "Strukturen und Mechanismen der biologischen Informationsverarbeitung") und Materialwissenschaften (Exzellenznetzwerk "Nanostrukturierte Materialien"), Kultur- und Geisteswissenschaften (Exzellenznetzwerk "Gesellschaft und Kultur in Bewegung" und Exzellenznetzwerk "Aufklärung – Religion – Wissen. Transformationen des Religiösen und des Rationalen in der Moderne") dar.

2. Universitätsziele und IT

Die Martin-Luther-Universität Halle-Wittenberg verfolgt das übergeordnete Ziel, in Forschung und Lehre national wettbewerbsfähig, zum Teil führend zu sein und in ausgewählten Bereichen internationale Maßstäbe zu setzen. Die Universität ist sich der Verpflichtung bewusst, die Möglichkeiten der Informations- und Kommunikationstechnologien für eine wettbewerblich ausgerichtete Lehre und eine international ausgerichtete Forschung einzusetzen sowie aus einer integrierten Informationsverarbeitung die Chancen für eine effektive und serviceorientierte Verwaltung zu nutzen. Insofern ist der gesamte Informations- und Kommunikationsbereich an die strategischen Ziele der Universität so eng wie möglich anzubinden. Dazu gehören neben der Erhöhung der Organisationseffektivität, die Erhöhung der Mitarbeiterzufriedenheit sowie die Unterstützung der dezentralen Entscheidungsstruktur. Es wird eine Umorientierung von einer angebotsorientierten zu einer nutzerorientierten Steuerung der IT-Leistungen angestrebt, die sich in der Organisation der Dienste niederschlägt.

3. Ziele des Einsatzes von IT an der MLU

Entsprechend der Bedeutung der IT für die Erreichung der Hochschulziele richtet sich die IT-Strategie und die dazugehörigen, zum Teil noch zu entwickelnden IT-Konzepte der Martin-Luther-Universität Halle-Wittenberg an folgenden Erwartungen bzw. Ansprüchen aus:

1. Unterstützung von hochqualitativer Forschung und Lehre und deren Qualitätssicherung,
2. Unterstützung von Forschungsmanagement und Wissenstransfer sowie kooperativer und universitätsübergreifender Forschung,
3. Unterstützung der Mobilität der Studierenden sowie der Wissenschaftler und Wissenschaftlerinnen,
4. Wissenschaft unterstützen durch eine schlanke und effiziente Administration mit einer Harmonisierung zugeordneter Verantwortlichkeiten.

Um die Erwartungen erfüllen und den Ansprüchen genügen zu können, sind insbesondere

1. ein integriertes Campusmanagement zur Unterstützung des gesamten Studierendenlebenszyklus in Studium, Lehre und dazugehöriger Administration,
2. Werkzeuge und Plattformen für E-Learning bzw. Blended Learning sowie zur effizienten Verwaltung von Vorlesungen durch die Dozenten und Dozentinnen,
3. elektronische Möglichkeiten zum kooperativen Arbeiten der Studierenden sowie zur Kommunikation zwischen den Studierenden bzw. den Studierenden und Lehrenden,
4. alle für Lehre und Forschung notwendigen elektronischen Quellen und allgemeine Literaturverfügbarkeit einschließlich der technischen Möglichkeiten zum zeit- und ortsunabhängigen Zugriff auf die Lehrmaterialien durch die Studierenden,
5. projektspezifische Rechen- und Speicherkapazität,
6. ein zentral wie dezentral verfügbares Informationsmanagement zur Unterstützung akademischer und administrativer Prozesse

bereitzustellen.

Hierfür sind folgende Voraussetzungen zu schaffen:

a) Eine hohe, am aktuellen Stand der Technik orientierte Quantität und Qualität der IT-Infrastruktur, nicht nur in Bezug auf Verfügbarkeit, sondern auch hinsichtlich IT-Sicherheit und Einhaltung der Datenschutzrichtlinien und der Empfehlungen des IT-Grundschutzes.
b) Die Bereitstellung ausreichend vieler Rechnerarbeitsplätze für Studierende und Mitarbeiter bzw. Mitarbeiterinnen.
c) Ein hohes Maß an Vereinheitlichung der zentral angebotenen IT-Dienste und IT-Dienstleistungen.
d) Eine flächendeckende Versorgung mit den zentral angebotenen IT-Diensten.
e) Geeignete Schulungs- und Weiterbildungsmaßnahmen für alle Mitarbeiter und Mitarbeiterinnen unter Ausschöpfung aller Quellen.
f) Eine frühzeitige Einbindung der IT in strategische Überlegungen und wesentliche operative Entscheidungen (wie bspw. zu Investitionen und Bauvorhaben)

4. Aufgabenbereiche der IT

Um die oben genannten Ziele erreichen zu können, müssen folgende inhaltliche Aufgaben operativ durch die Universität erfüllt und strategisch entwickelt werden:

- IT-gestütztes Hochschulinformationssystem,
- Online-Bibliotheksrecherche und Online-Literaturversorgung,
- Hochschulweite Lehr- und Lernmanagement Plattform,
- Zugang zu IT-Diensten für Studierende durch Online-Zugang und öffentliche Rechnerarbeitsplätze,
- Versorgung mit Netz- und Kommunikationsdiensten,
- Versorgung mit qualitativ hochwertigen IT-Basisdiensten,
- Mobile und immobile Netzinfrastruktur,
- Zentrales Identitäts- und Zugangskontrollmanagement,
- Zentralisierung und Standardisierung der IT-Dienstleistungen (über SLA),
- Planung, Pflege und Erweiterung der zentralen technischen Infrastruktur,
- Einbindung der IT in wesentliche Prozesse.

5. Aktuelle Organisation in Bezug auf die IT-Verantwortlichkeiten

Die IT-Verantwortlichkeit lässt sich gegenwärtig in vier Bereiche gliedern:

- Zentrale Universitätsverwaltung (ZUV),
- Universitäts- und Landesbibliothek (ULB),
- Universitätsrechenzentrum (URZ),
- Fakultäten/Institute (FAK).

Die Zuordnung zu den Aufgabenbereichen gestaltet sich derzeit wie folgt:

Aufgabenbereich	**ZUV**	**ULB**	**URZ**	**FAK**
IT-gestütztes Hochschulinformationssystem	X		X	
Online-Bibliotheksrecherche und -Literaturversorgung		X		
Hochschulweite Lehr- und Lernmanagement Plattform			X	
Zugang zu IT-Diensten für Studierende	X		X	X
Versorgung mit Netz- und Kommunikationsdiensten	X		X	
Versorgung mit IT-Basis-Diensten	X		X	
Mobile und immobile Netzinfrastruktur			X	
Zentrales Identitäts- und Zugangskontrollmanagement	X	X	X	X
Zentralisierung und Standardisierung	X		X	X
Planung, Pflege, Erweiterung der technischen Infrastruktur	X	X	X	X

Die Koordination zentraler Prozesse, die über die Grenzen einzelner Einrichtungen (ZUV, URZ, ULB, Fakultäten) der Universität hinausgehen, obliegt dem IT-Lenkungsausschuss der Universität. Alle oben genannten Bereiche sowie das Rektorat sind in diesem IT-Lenkungsausschuss vertreten.

Die 2010 installierte Rektoratskommission Multimediales Lernen berät das Rektorat in Fragen des IT-Einsatzes im Bereich des Lernens und Lehrens.

6. Schlussbemerkung

Vorliegende IT-Strategie wird kurz- bzw. mittelfristig durch entsprechende Konzepte zur Realisierung der in der IT-Strategie formulierten Ziele untersetzt. Dazu zählen insbesondere die Konzepte

- IT-Sicherheitskonzept inklusive eines ID-Management-Konzeptes,
- Datenschutz-Konzept,
- Konzept des Ausbaus des universitären Netzes,
- Konzept universitätsoffener Studierendenpools,
- Service-Konzept (zentral angebotene IT-Dienste und IT-Services über SLA).

Anhang A: Studierenden-Pools (CIP) an der MLU

(1) universitätsoffene Pools

Institut/Fakultät	*Anzahl der Arbeitsplätze*	*Beschaffungsjahr*
Biochemie	25	2010
Landwirtschaft	20	2009
Universitätsrechenzentrum	52	2008
Univ.- und Landesbibliothek	70	2010
Mediathek	33	2006
Wirtschaftswissenschaften	100	2010
Jura	30	2010
Geowissenschaften	48	2010
Ingenieurwissenschaften	26	2008
Informatik/Mathematik/Physik	30	2010
Informatik/Mathematik/Physik	30	2006
Pädagogik	46	2008
Geschichte	30	2007
Medienkomm	31	2010

(2) institutseigene Pools

Institut/Fakultät	*Anzahl der Arbeitsplätze*	*Beschaffungsjahr*
Informatik	55	2006
Rehabilitationspädagogik	30	2007
Soziologie	15	2008
Psychologie	15	2008
Musikwissenschaften	10	2010
NatFak 2	40	2010
Medizin	40	2007
Chemie	8	2010
Medienkomm	50	2010
Sprache u. Literatur	18	2008

(3) in den nächsten 3 Jahren geplante Investitionen im Bereich der CIP-Pools

Institut/Fakultät	*Anzahl der Arbeitsplätze*	*Beschaffungsjahr*
NatFak 2	24	2011
Medizin	53	2011
Musik	10	2011
Chemie	12	2011
Wirtschaftswissenschaften	18	2011
Mediathek	47	2011
Informatik	85	2012

(4) Anzahl Studierende pro CIP-Rechner nach Standorten (ohne ULB)

Standort	**Anzahl CIP-Rechner**	**Anzahl Studierende**	**Studierende pro Rechner**
Innenstadt	302		
Campus Weinberg	111		
Franckesche Stiftungen	76		
Campus Heide	312		
Medizinische Fakultät	40		
Kröllwitz	30		
gesamt	**871**	**18 600**	**21,4**

Anhang B: An der MLU angebotene IT-Dienste

Innerhalb der unter Abschnitt 4 genannten Aufgabenbereiche werden den Mitarbeitern, Wissenschaftlern und Studierenden der Universität momentan folgende Dienste bereitgestellt.

IT-gestütztes Hochschulinformationssystem

- Online-Verfahren zu Bewerbung, Einschreibung, Rückmeldung, Prüfungsanmeldung und -abmeldung, Modulanmeldung und -abmeldung, Erzeugung sämtlicher Studiendokumente
- Online-Verfahren zur Prüfungsorganisation inkl. Leistungserfassung
- Online-Verfahren zur Modul- und Studiengangserfassung und -verwaltung inkl. der automatisierten Dokumentation und der automatisierten Schnittstelle zur Prüfungsverwaltung
- Multifunktionale Chipkarte
- Elektronische Zeiterfassung
- Online-Verfahren zur Haushaltsüberwachung
- IT-Lösungen innerhalb der ZUV und des Rektorates
  - Unified Communication incl. Sicherung, Archivierung und Unterstützung von mobilen Endgeräten (SmartFones)
  - Identitymanagement inkl. IDM-Synchronisierung eDir-Active Directory
  - Arriba – Bauausschreibungen
  - Adonis – Geschäftsprozessaufnahme und Visualisierung
  - Sharepoint-Server
  - EASY Contract – Vertragsmanagement
  - HIS SOS/POS/ZUL Studierenden, Prüfungs- und Zulassungsmanagement
  - HISSVA – Personalverwaltung
  - Prof.it – Berufungsdatenbank incl. WorkFlow
  - TransWare Personalkostenhochrechnung
  - HISFSV – Finanz-, Sachmittel- und Bauverwaltung
  - HISKBS - Kassensystem
  - Gebäudemanagementsysteme
  - Elektronische Zutrittssysteme, digitale Schließanlagen
- NetCallUp - Aufrufsystem im StudierendenServiceCenter
- NetVico - Hörsaalinformationssystem
- Kommunikationsverzeichnis
- Bereitstellung der Management-Cloud
- Sicheres Verwaltungsnetz. inkl. Netzdokumentation

Online-Bibliotheksrecherche und Online-Literaturversorgung

Die digitalen Dienstleistungen der Universitäts- und Landesbibliothek umfassen ein breites Spektrum onlinegestützter Verfahren.

Einen wesentlichen Bereich deckt das LBS (Lokales Bibliothekssystem) mit seinen Modulen Nutzerverwaltung, ACQ (Erwerbung), OUS (Ausleihe) und OPAC (Online-Katalog) ab.

Neben dem Zugriff auf E-Journals und Datenbanken erfolgt die Bedienung elektronischer Lieferdienste wie SUBITO (kostenpflichtiger Lieferdienst für Aufsatzkopien und Bücher), HARIEL (kostenloser Lieferdienst ausschließlich innerhalb der Martin-Luther-Universität). Die Online-Fernleihe (die Online-Fernleihe des GBV) bietet für Endbenutzer und Bibliotheksmitarbeiter die Möglichkeit, am Ort nicht vorhandene Dokumente im Original oder als Kopie über die Datenbanken des GBV direkt im Anschluss an die Recherche online zu bestellen.

Ein weiterer umfangreicher Teil der digitalen Dienstleistungen umfasst den Bereich der Retrodigitalisierung. Im Rahmen von durch Drittmittel geförderten Projekten wurden und werden umfangreiche digitale Medien hergestellt, erschlossen und über das Portal der ULB angeboten. Des Weiteren werden auf Benutzeranfrage gegen Entgelt Digitalisate von historischen Büchern und Karten im Rahmen der Inhouse-Digitalisierung erstellt.

Ein wesentlicher Teil der Dissertations- und Habilitationsschriften der Martin-Luther-Universität liegt in elektronischer Form vor. Elektronische Dokumente, die in Sachsen-Anhalt publiziert werden, sind im Rahmen des Sammelauftrages der ULB und der Pflichtablieferung der Verlage online verfügbar. Für die elektronische Veröffentlichung wissenschaftlicher Arbeiten stellt die ULB einen Server für die Hochschulen des Landes Sachsen-Anhalt zur Verfügung.

Hochschulweite Lehr- und Lernmanagement Plattform

An der gesamten Hochschule ist die Nutzung des LMS Stud.IP verpflichtend. Über die Plattform werden (z.T. ausschließlich) angeboten

- Vorlesungsverzeichnis
- Veranstaltungsanmeldung
- Individuelle Stundenpläne
- Vorlesungsskripte sowie weitergehende Lehr- und Lernmaterialien
- Diskussionsforen zu einzelnen Veranstaltungen
- Veranstaltungsspezifische E-Mail-Verteiler

Zugang zu IT-Diensten für Studierende

Die Universität stellt sicher, dass alle IT-gestützten Verfahren durch die Mitarbeiter und Studierenden genutzt werden können, für die sie konzipiert und angeboten werden. Dies bedeutet insbesondere, dass vor allem den Studierenden unabhängig von ihrer persönlichen Ausstattung mit eigenen Computern die Möglichkeit eingeräumt wird, alle elektronischen Lehr- und Lernangebote zu nutzen. Um sicher zu stellen, dass die notwendigen Hard- und Software Voraussetzungen hierfür gegeben sind, stellt die Universität Computerarbeitsplätze für Studierende in Computer-Pools bereit. Diese unterliegen entweder der Verantwortung der jeweiligen Institute oder der zentralen Verantwortung des URZ. Die Planung solcher Computer-Pools wird an der Universität abgestimmt und auf Übereinstimmung mit dieser Konzeption geprüft. Weitere Details sind im Anhang A zu finden.

Zentrale Versorgung mit Netz- und Kommunikationsdiensten

Das URZ stellt sicher, dass jeder Mitarbeiter- und Laborarbeitsplatz mit einer Anbindung an das Universitätsnetz ausgestattet werden kann. Dies schließt den Zugang zum Wissenschaftsnetz und das Internet ein. Neben der Anbindung stationärer Geräte über das kabelgebundene Netz wird ein flächendeckender Zugang zum WLAN-Netz der Universität angestrebt. Die Verantwortung hierfür liegt ausschließlich beim URZ. Dezentrale WLAN-Lösungen werden nicht unterstützt

Zentrale Versorgung mit IT-Basisdiensten

Das URZ bietet eine Reihe von zentralen IT-Basisdiensten an:

- das Universitätsnetz
- das universitätsweite WLAN- Netz
- zentrale Verwaltung der IT-Nutzer
- Verwaltung der IP-Domäne der Universität
- zentrale Dienste für
    - E-Mail,
    - Dateihaltung,
    - Web-CMS
    - Datenbanken

- Hochleistungsrechner
- Backup- und Archivserver
- zentrale Lehr- und Lernplattform
- PC-Pool-Managementsystem

Im Bereich des Hochleistungscomputings werden in begründeten Fällen auch dezentrale Systeme unterstützt. Erforderliche Infrastruktur hierfür ist jedoch zentral vom URZ zu nutzen (Klimatisierung, Stromversorgung, Brandschutz)

Mobile und immobile Netzinfrastruktur

Die Netzinfrastruktur der Universität orientiert sich am aktuellen Stand der Technik und wird durch das URZ gesteuert und gepflegt.

Die mobile Netzinfrastruktur wird universitätsweit betrieben und sieht verschiedene WLAN-Netze mit verschiedenen Nutzerrollen (z.B. Universitätsangehörige, Gäste, Angehörige von Einrichtungen im Verbund des DFN-Roaming, Veranstaltungsteilnehmer mit jeweils unterschiedlichen Zugangsrechten zu Intranet- und Internetdiensten) vor. Im Gegensatz zum kabelgebundenen Netz ist hier eine individuelle Authentifikation erforderlich.

Der Betrieb der Netzinfrastruktur schließt zentrale Schutz- und Sicherungsmaßnahmen wie Firewalls und Netzangriffsabwehr ein. Entsprechende Technik wird vom URZ betrieben. Für das Verwaltungsnetz als besonders abgesichertes Teilnetz des Universitätsnetzes gelten (entsprechend dem notwendigen Sicherheitsniveau) angepasste Regelungen.

Zentrales Identity- und Zugangskontrollmanagement

Die Nutzerautorisierung für die von der Universität zentral angebotenen IT-Dienste wird mit dem zentralen Datenbestand der ZUV abgeglichen und in das oder die Identitymanagement-Komponenten in Echtzeit synchronisiert. Dies gewährleistet die Aktualität der Daten und eine zeitnahe Reaktion auf Veränderungen (wie z.B. dem Ausscheiden eines Nutzers aus der Universität).

Das URZ stellt Teile der Daten entsprechend der Bestimmungen des Datenschutzes zweckgebunden, zum Beispiel in LDAP-Bäumen mit Zugriffsbeschränkung, dezentral angebotenen Diensten zur Verfügung.
In der Erprobungsphase befindet sich ein Authentifikationsmodell auf Basis von Smartcards (mit digitalen Zertifikaten auf einem Cryptochip) für den Einsatz im inner- und außeruniversitären Bereich.

Zentralisierung und Standardisierung

Die Universität strebt im Rahmen der Dienstkonsolidierung eine Zentralisierung von Basisdiensten und die Standardisierung von IT-Services (über SLA) an.

Planung, Pflege und Erweiterung der zentralen technischen IT-Infrastruktur

Die Planung, Inbetriebnahme, Wartung und Erweiterungen der zentralen IT-Infrastruktur werden durch das URZ geplant und durchgeführt. Beim weiteren Ausbau des Netzes wird u.a. eine Netzzugangskontrolle auch im kabelgebundenen Netz angestrebt.

Anhang C: IT-Sicherheit und Datenschutz (IST-Zustand)

IT-Sicherheit

Inhaltlich strategisches und operatives Vorgehen

Maßnahmen zur Absicherung der IT-Infrastruktur basieren auf der Umsetzung eines Konzeptes zum IT-Grundschutz. Darüber hinaus werden spezielle Absicherungsmaßnahmen für Bereiche mit erhöhtem Schutzbedarf getroffen, z.B. der Netzstruktur der Verwaltung und der Medizinischen Fakultät sowie interne Bereiche, in denen personenbezogene Daten verwaltet werden.

Wesentliche Anforderungen sind die Aufrechterhaltung der Betriebsfähigkeit der zur IT-Infrastruktur gehörenden Netze und Systeme (Verfügbarkeit) und eine möglichst umfassende Abdeckung der Daten- bzw. Informationssicherheit (Integrität und Vertraulichkeit).

Zu den Bausteinen des IT-Grundschutzes gehört die Absicherung der Daten, der Netzwerk-Infrastruktur, der einzelnen IT-Systeme (Server, Arbeitsplatzrechner, sonstige datenverarbeitende Systeme) und der Applikationen. Zusätzliche Maßnahmen betreffen die Absicherung der Nutzer bei Verwendung des universitären Internetzugangs.

Als Gefährdung sind neben technischen Ausfällen insbesondere folgende Quellen zu verzeichnen:

- mutwillige und vorsätzliche Störungen bzw. Angriffe aus dem Internet oder durch universitätszugehörige Personen über das interne Datennetz
- Fehlhandlungen von beteiligten Personen, verursacht durch unzureichende Kenntnisse oder bewusste Missachtung von Sicherheitsmaßnahmen
- organisatorische Mängel, z.B. hinsichtlich verpflichtender Schulungsmaßnahmen für Personen im Umgang mit IT-Systemen oder bei der Umsetzung von IT-Sicherheitsmaßnahmen (starke Authentifizierung, ID-Management)
- höhere Gewalt (Stromausfälle, externe Datennetzausfälle)

Unter Annahme dieser Gefährdungslage wurden folgende Maßnahmen zur Erfüllung der Anforderungen des Grundschutzes getroffen:

- **Netzversorgung:**

  Alle Zugänge zum Netz (Internet, WLAN) werden vom Gefährdungspotential gleichgesetzt und demzufolge auch gleich behandelt. Hauptmethoden zum Schutz vor illegaler oder unerwünschter Nutzung des Datennetzes der Universität stellen Firewalls, Protokollfilter und Systeme zur Einbruchserkennung (IDS, Intrusion Detection System) und -verhinderung

(IPS, Intrusion Prevention System) dar. Es gibt einheitliche Einstellungen im IPS und in den Firewalls.

Die Firewalleinstellungen für die Verbindung zwischen Internet und Universität wurden nach dem Prinzip gesetzt, dass alles was nicht explizit verboten ist, erlaubt ist. Diese Vorgabe erfolgt im Sinne der„Freiheit von Forschung und Lehre“. Werden Angriffe durch das IDS erkannt, werden die Regeln verschärft.

Bereiche der Universität wurden entsprechend der Organisationsstruktur in verschiedene Segmente gegliedert, welche sich in der logischen und physischen Struktur des Rechnernetzes widerspiegeln. Zwischen diesen Teilnetzen werden je nach Bedarf zusätzliche Absicherungsmaßnahmen (Layer 2/3-Firewall und Port-Filter, etc.) eingesetzt.

Die Netze der Zentralen Universitätsverwaltung (ZUV) sowie der Universitäts- und Landesbibliothek (ULB) wurden für Zugriffe aus dem Internet weitgehend abgeschottet (mit Ausnahme des öffentlichen Webauftritts, der zunehmend zentralisiert wird). Darüber hinaus gibt es inneruniversitäre Netzbereiche für eine organisatorische Verwendung (Systemadministration) sowie die Netze für die Verwaltung von Nutzerdaten, die nicht aus dem Internet erreichbar sind.

Werden keine weiteren Absicherungsmaßnahmen getroffen, so sind alle Endgeräte prinzipiell direkt im Internet "sichtbar", sofern dies nicht ausdrücklich anders vom Nutzer gewünscht ist.

Der Zugang über VPN (Virtual Private Network) gestattet zudem den Fernzugriff für authentifizierte Intranetnutzer. Aus diesem Grund existiert (noch) keine ausdrückliche Demilitarisierte Zone (DMZ), in der zentrale Dienste installiert werden, die aus dem Internet erreichbar sein müssen. Die Server dieser Dienste müssten dann auch im Universitätsrechenzentrum (URZ) stehen. Eine Zentralisierung z.B. von E-Mail-, Datenbank- und Webservern ist zwar recht weit vorangeschritten, leider allerdings noch nicht vollständig erfolgt. Bei vielen Diensten, wie z.B. bei fachspezifischen Datenbanken wird zudem eine vollständige Zentralisierung an einer Universität nicht möglich bzw. sinnvoll sein. In diesen Fällen sind gesonderte Maßnahmen in Abstimmung mit den verantwortlichen Bereichen zu treffen.

Mittelfristig ist die manuelle Rechneradressverwaltung durch ein zentrales Adressmanagement zu ersetzen, welches zusammen mit den Mitteln der Port-Security auf den Netzanschlussgeräten in den Einrichtungen den unkontrollierten Anschluss von privaten Rechnern erschwert oder unterbindet.

Angeschlossene mitversorgte Einrichtungen (Leopoldina usw.), die zurzeit noch im Universitätsnetz eingebunden sind, werden demnächst über Tunnel direkt zum Anschlussrouter verbunden. Damit müssen die Datenverbindungen aus diesen Einrichtungen in die Universität dieselben Sicherheitseinrichtungen durchlaufen wie jeder andere ankommende Datenverkehr auch.

Technische Umsetzung der Netzversorgung und des Netzzugangs:

- Internetanschluss:

  Die Absicherung erfolgt über ein redundantes IPS-System bestehend aus zwei Cisco-Modulen IDSM2 im Anschlussrouter. Diese Technik analysiert den Datenstrom hinsichtlich möglicher bekannter Bedrohungen und greift je nach Einstellung direkt ein, um diese zu minimieren. Sie wirkt in beide Richtungen, um auch von Rechnern der Universität ausgehende Gefährdungen anderer Netze möglichst zu unterbinden. Das System muss laufend aktualisiert werden (Update-Vertrag). Die Einstellungen sind sehr sensibel und können deshalb auch zu temporären Störungen bei normalen Datenverbindungen führen; daher sind zeitaufwändige Überwachungen und Anpassungen nötig.

- VPN- und WLAN-Anschluss:

  Hier handelt es sich um ein nicht-redundantes System - bestehend aus einer Cisco-ASA (Adaptive Security Appliance) und einem IPS-Modul. Dieses Gerät ermöglicht die VPN-Einwahl von außerhalb der Universität und damit die Nutzung interner Dienste sowie die Nutzung des WLANs, aktuelle Cisco-VPN und 802.1x. Das WLAN wird derzeit modernisiert, wodurch weitere Techniken zum Einsatz kommen werden.

- Neue WLAN-Generation:

  Die Zugangstechnik wird zentral gesteuert unter Verwendung von redundanten Cisco-Controllern. Es erfolgt aus Last- und Strukturgründen eine Zweiteilung östlich und westlich der Saale. Beide Seiten sind jeweils über ein IPS- und ein Firewall-Modul angeschlossen. Zusätzlich erfolgt eine Überwachung hinsichtlich der Erkennung von Fremdtechnik (Access-Points) im Netz. Die Hardware westlich der Saale ist bereits installiert.

- **Arbeitsplatzrechner und Server**

An der Universität wird eine Vielzahl heterogener Systeme mit unterschiedlichen Betriebssystemen auf verschiedenen Wartungsleveln eingesetzt. Nicht immer lassen sich alle Systeme – bedingt durch Verwendung spezieller Soft- und Hardware - zeitnah auf einem aktuellen Stand halten. In diesem Fall besteht eine gewisse Gefährdung des Eindringens und der Verbreitung von Schadsoftware (Viren, Würmer und Trojaner). Dieser Zustand wird durch die Möglichkeit des Einbindens privater Rechner verstärkt und kann sogar fahrlässig oder mutwillig erfolgen.

Die wesentliche Ausbreitung der Schädlinge erfolgt über E-Mail. Zur Eindämmung werden E-Mails zwangsweise über ein zentrales Gateway geleitet und an dieser Stelle auf schädliche Inhalte geprüft. Bei positivem Befund wird die Annahme verweigert. So erfährt auch

bei einem falsch positiven Befund der Absender, dass die E-Mail nicht zugestellt wurde. E-Mails werden durch das URZ nicht verworfen!

Damit verbunden sind zentrale Maßnahmen zur Bekämpfung unerwünschter E-Mails (Unsolicited Bulk oder Commercial E-Mail, auch als SPAM oder Junk bezeichnet). Durch eine Absenderverifizierung wird ein großer Teil von SPAM-Mails nicht zugestellt, da fiktiven Absendern die Annahme verweigert wird.

Die Universität nimmt am System der automatischen Benachrichtigung des DFN-Vereins teil. Im Rahmen dieses Verfahrens wird das URZ werktäglich über potentiell verseuchte Rechner informiert, so dass die betroffenen Systeme von den lokalen Administratoren in den Fakultäten und Einrichtungen geprüft und bereinigt werden können.

Darüber hinaus gehende Maßnahmen zur Informationssicherheit, insbesondere zur Wahrung der Vertraulichkeit, obliegen in der Regel dem Nutzer. Durch die Aufteilung und Abschottung von Teilnetzen ist der Zugriff auf Daten, falls vom Inhaber nicht explizit geändert, auf den Anwender bzw. die Arbeitsgruppe beschränkt. Die Daten werden sowohl dezentral (Arbeitsplatzrechner) als auch zentral (Workgroup-Server oder NAS des URZ) in der Regel unverschlüsselt gespeichert. Durch die derzeit stattfindende Einführung von Verschlüsselungssystemen auf Basis von X.509-Zertifkaten besteht für Nutzer bei Bedarf die Möglichkeit der kryptographisch gesicherten Speicherung von Informationen.

Die zentralen Systeme sind weitestgehend redundant ausgelegt, so dass die Integrität der gespeicherten Daten im Falle eines einzelnen Hardwareausfalls erhalten bleibt. Unterstützt wird dies durch ein tägliches Backup zu einem zentralen, von den Rechnern getrennten Backup-System, welches jeweils die letzten drei Versionen eines Dokuments aufbewahrt. Schutz vor mutwilliger Zerstörung bietet in begrenztem Maße die Einschränkung des Zugriffs auf berechtigte Personen, üblicherweise den Inhaber der Daten. Für Dokumente mit Gruppenzugriff bestehen derzeit keine integritätssichernden Maßnahmen, die vor Manipulation bzw. Zerstörung von Daten durch Gruppenmitglieder oder andere Personen mit Schreibberechtigung (Administratoren) schützen.

Für in dezentralen Systemen (Arbeitsplatzrechner) gespeicherte Daten sind die Anwender selbst verantwortlich. Das URZ bietet die Möglichkeit der Einbindung in das zentrale Backup-System oder die Auslagerung „wichtiger“ Daten auf zentrale Laufwerke mit Backup-Anbindung.

Als weitere Maßnahme können Nutzer die Abschottung ihrer Rechner gegenüber Zugriffen aus dem Internet oder den Netzen anderer Arbeitsgruppen verlangen, welche über Layer2/3-Portfilter und Firewalls ermöglicht wird.

Das URZ stellt zur Unterstützung einen zentralen Antivirensoftwareserver bereit. Gegenwärtig findet keine Kontrolle auf aktuellen Virenschutz der Endgeräte statt. Es ist vorgesehen, eine solche Kontrolle in naher Zukunft einzuführen und Geräten ohne Negativbescheinigung hinsichtlich Virenbefall den Zugang zum Netz zu verwehren.

Die Zugangs- und Rechteverwaltung an den Arbeitsplatzrechnern obliegt dem Nutzer bzw. den Bereichsadministratoren. Ausgenommen sind Poolrechner und weitere Systeme mit Zugang für einen wechselnden Personenkreis. Diese sind oder werden auf zentrale Nutzerverwaltung umgestellt und über Directory-Systeme versorgt.

Für die Zukunft ist die Anbindung an ein zentrales Management System mit einheitlicher Identitäts-Verwaltung (Identity-Management) geplant. Die Informationen in diesem System werden aus verbindlichen Quellen gespeist (Immatrikulationsamt, Personalabteilung, ULB) und ermöglichen die Zuordnung von Personen zu verschiedenen Rollen (Student/in, Mitarbeiter/in, sonstige/r Universitätsangehörige/r). Dadurch kann die Nutzung universitärer Ressourcen und die der verbundenen Einrichtung (z.B. Bibliotheken und Verlage) auf legitimierte Nutzer eingeschränkt werden.

Datenschutz

Alle Verfahren unter Verwendung von persönlichen Daten sind mit dem Datenschutzverantwortlichen abgestimmt bzw. abzustimmen. Dies bedingt die Trennung von universitätsinternen und nach außen offenen Diensten.

Anhang D: Personelle Ausstattung der zentralen Einrichtungen im Bereich IT

a) URZ 28,1 VbE

b) ULB 5 VbE

c) ZUV 17,5 VbE

Anhang E: Netzkonzept der MLU

1. Netzkonzept

1.1 Angestrebte Ziele

Das Universitätsnetz der Martin-Luther-Universität dient sowohl der wissenschaftlichen Kommunikation an den Arbeitsplätzen der Wissenschaftler als auch der Organisation von technischen und Verwaltungsabläufen. Es ist unverzichtbare Arbeits-, Organisations-, Informations- und Kommunikationsgrundlage sowohl für Studierende und Lehrende als auch für Wissenschaftlerinnen und Wissenschaftler der Universität sowie für die Universitätsverwaltung. Mit der Integration der Telekommunikation - mit der Entwicklung vom Datennetz zum Kommunikationsnetz schlechthin - ist das Netz eine wichtige infrastrukturelle Grundlage für Forschung, Lehre und Verwaltung. Von der Leistungsfähigkeit des Netzes hängt das erfolgreiche Wirken der Hochschule ab. Damit hat es als Infrastrukturkomponente den Stellenwert eines unverzichtbaren Basiswerkzeugs. Diesem Stellenwert entsprechend verdienen die Pflege und der Ausbau des Netzes höchste Aufmerksamkeit.

Die über das Netz verfügbaren Daten- und Kommunikationsdienste entwickeln sich mit dessen zunehmender Leistungsfähigkeit. Ziel des stetigen Netzausbaus und der stetigen Netzentwicklung ist die Bereitstellung eines flächendeckenden hochverfügbaren Netzes und der darüber verfügbaren, weitgehend ortsunabhängigen Dienste.

Planung, Entwicklung und Betreuung des Netzes liegen in der Hand des Universitätsrechenzentrums. Der IT-Lenkungsausschuss der Universität fällt Entscheidungen oder bereitet diese für das Rektorat und den Senat vor und kontrolliert die Umsetzung.

1.2 Wichtige Grunddaten der Universität

Die Universität Halle-Wittenberg ist eine Volluniversität mit derzeit über 19.400 Studierenden und ca. 3.000 Mitarbeitern in über 50 Instituten an neun Fakultäten und einem Zentrum für Ingenieurwissenschaften. Darüber hinaus existieren im Umfeld der Universität sieben interdisziplinäre wissenschaftliche Zentren sowie u.a. Sonderforschungsbereiche der DFG, Graduierten- und Innovationskollegs.

Grobstruktur des Aufbaues des Universitätsnetzes

Die historische Entwicklung der Universität Halle-Wittenberg hat zu einer Standortverteilung geführt, die gegenwärtig ca. 300 Gebäude im gesamten Stadtgebiet von Halle und auch außerhalb des Stadtgebietes umfasst. Erschwerend für die Netzwerkversorgung kommt hinzu, dass Stadt und Universität durch einen Fluss in zwei Standortbereiche geteilt wird. Dabei

konzentrieren sich die naturwissenschaftlichen Institute vor allem westlich der Saale im Bereich Weinbergweg und Campus Heide-Süd, während sich die geisteswissenschaftlichen Institute vorrangig im Stadtzentrum befinden.

Die Universität verfügt über ein eigenes Glasfasernetz mit ca. 60 km Glasfaserkabel, das bis auf wenige Ausnahmen alle Standorte erreicht und damit eine hohe Flexibilität der Netzversorgung gestattet. Die Tertiärverkabelung ist jeweils sternförmig mit zentralen Gebäudenetzknoten ausgeführt. Die externe Anbindung des Universitätsnetzes ist über einen 1 Gigabit/s X-WIN Anschluss - ausgelegt als ein mit der Hochschule Merseburg gemeinsamer Clusteranschluss - beim DFN realisiert.

Im Universitätsnetz wird transparent ein zentraler SMB-Fileserver angeboten. Darüber hinaus stehen den Nutzern zentrale Dienste wie Nameserver, Timeserver, Archiv- und Backup-Server (TSM), Computeserver (Hochleistungsrechner), Mailserver, Faxserver usw. und umfangreiche zentrale Dienste der ZUV und der Universitäts- und Landesbibliothek zur Verfügung.

Das Übertragungsvolumen liegt gegenwärtig bei einer Eingangsdatenrate aus WIN/Internet von ca. 25 TByte pro Monat mit steigender Tendenz. Der zentrale Backup- und Archivserver aktualisiert ca. 2 TByte täglich im LAN der Universität.

Jeder Nutzer zentraler Dienste wird in einer Datenbank erfasst. Gegenwärtig sind ca. 29.000 Nutzer registriert.

1.3 Geplante Netzentwicklung

Multimediale Inhalte sind zwischenzeitlich ein Muss in Lehre und Forschung und werden mit zunehmendem Einsatz zu weiter stark wachsenden Datenmengen führen. Bei der Netzentwicklung sind deshalb insbesondere Dienste zu berücksichtigen, die sowohl hinsichtlich Steuerung und Verwaltung als auch hinsichtlich Bandbreite immer anspruchsvoller werden. So erfordert die Nutzung von Videokonferenzen und Vorlesungsübertragungen oder die Nutzung von Lehr- und Lernangeboten aus dem Netz in Vorlesungen neben einer geeigneten zuverlässigen Struktur des Netzes auch eine Steuerung des Datenflusses. In diesem Rahmen sind die Leistungsfähigkeit der zu Grunde liegenden Technik und die eingesetzten Werkzeuge zu garantieren.

Ziel der Netzentwicklung ist die Verfügbarkeit eines multimediafähigen Netzzugangs an jedem Arbeitsplatz, in jedem Hörsaal und in jedem Seminarraum über Kabel sowie die leistungsfähige Abdeckung der Universitätsstandorte mit drahtlosen Netzzugängen. Die Netzstruktur sollte frei von Engpässen sein. Die Bandbreite sollte so bemessen sein, dass auch bei Parallelzugriffen keine Leistungseinbußen auf dem Weg vom Server zum Client innerhalb der eigenen Infrastruktur auftreten.

Neben der Bereitstellung der Daten, die unmittelbar von Applikationen genutzt werden, muss das Netz die Übertragungskapazität für die Sicherung und Verwaltung der Daten gewährleisten.

1.4 **Netzstrukturierung**

Grundlage der Netzstrukturierung ist das IP-Routing, mit dem die unterschiedlichen Struktureinheiten und Institute über eigene IP-Netze verfügen können. Dadurch wird zum einen der Netzverkehr stark lokalisiert. Zum anderen wird dadurch die Sicherheit für lokale Ressourcen erhöht, da neben der Zugriffsicherung auf der Anwendungsebene bereits tiefer angelegte Zugriffkontrollen (z. B. Datenexport nur an Rechner des gleichen Subnetzes) genutzt werden können. Durch die Nutzung der VLAN-Technologie können in geswitchten Netzen räumlich verteilte Arbeitsgruppen ohne Einschränkung in der gleichen Subnetzumgebung arbeiten. Gegenwärtig existieren an der Universität ca. 400 solcher Subnetze.

Die Universität ist mit Stand vom Juni 2011 zu 80 Prozent mit WLAN versorgt. Es wird angestrebt, die noch "weißen Flecken" ebenfalls mit WLAN zeitnah abzudecken. Es gibt sowohl personalisierte Zugänge über IEEE802.1x bzw. VPN für Studierende und Mitarbeiter der Universität als auch öffentliche Zugänge mit eingeschränkter Funktionalität für Tagungen und andere Veranstaltungen. Darüber hinaus nimmt die Universität am Roaming-Dienst des DFN-Vereins teil.

Als Sollzustand der Netzstruktur im Endnutzerbereich wird eine sternförmige Tertiärverkabelung mit zentralem Technikraum im Gebäude angestrebt. Die Konzentration der Netzknoten in solchen Technikräumen gestattet eine zentralisierte stetige Aktualisierung und eine Migration zu evtl. neuen Technologien unter Nutzung der einmal erfolgten Verkabelung für den gesamten Standort.

Das Universitäts-LAN besteht aus über 500 aktiven Netzknoten. Fünf Hochleistungs- Switchsysteme bilden den Kern des neuen 10-Gigabit-Backbones. Dahinter arbeiten Workgroup-Switchsysteme mit Fastethernet-Ports. Die zentralen Server (File-, Backup-, Archivserver, Parallelrechner) kommunizieren über Gigabitethernet- bzw. 10-Gigabitethernet-Ports im Universitäts-LAN.

In Hinblick auf eine leistungsfähige Internetanbindung über das X-WiN sollte die Bandbreite für jeden Server so bemessen sein, dass auch bei Parallelzugriffen möglichst jedem Client 100 Mbit/s zur Verfügung gestellt werden können.

Das bereits eingeführte 10-Gigabit-Backbone muss ein hohes Maß an Zuverlässigkeit bieten. Dies soll über eine Vermaschung, d. h. eine Verbindung der Hauptknoten über alternative Pfade erreicht werden. Die dazu u.a. notwendige zweite Flussüberquerung konnte bereits als Mietleitung realisiert werden.

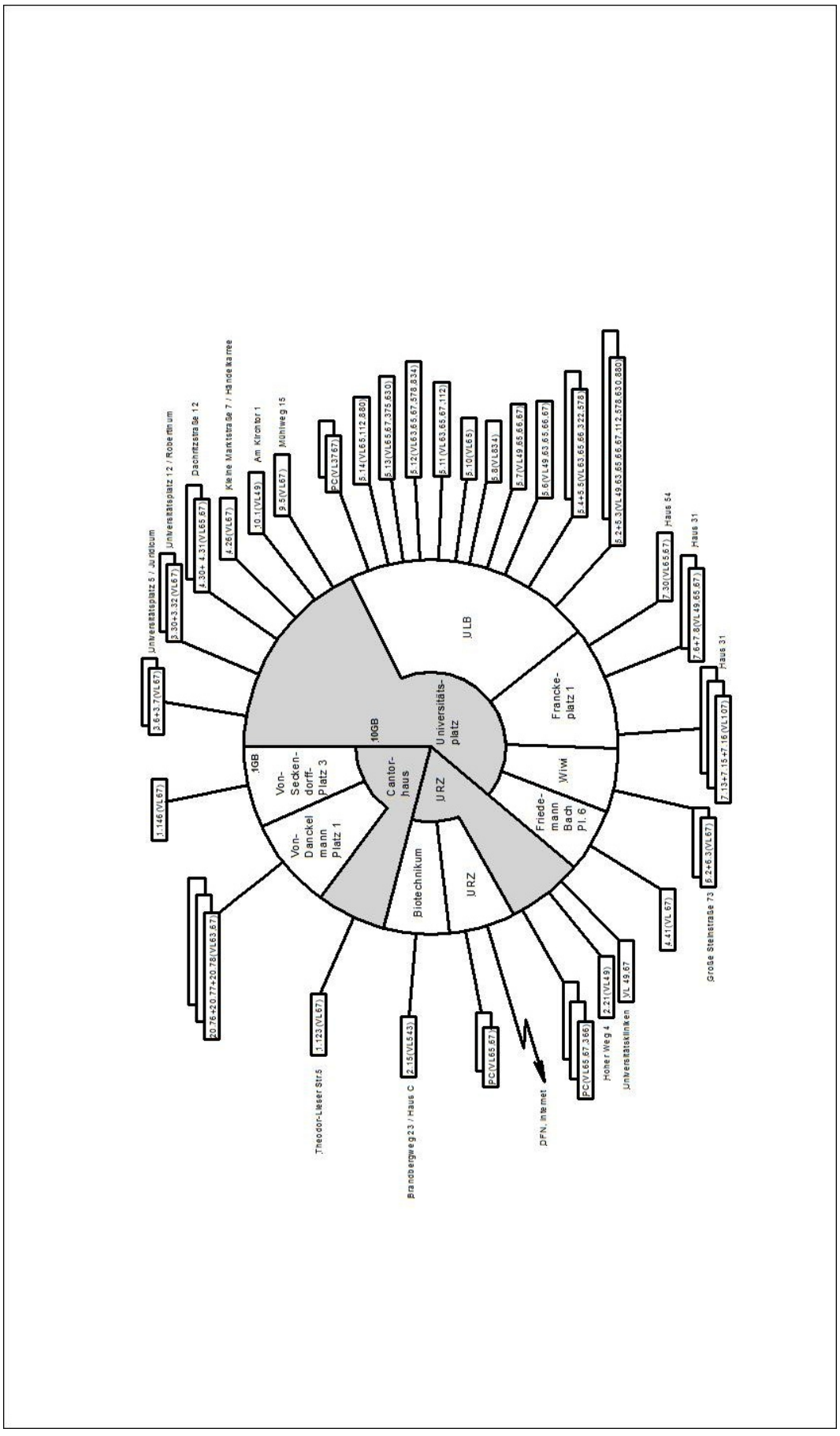


Abbildung: Schematische Netzstruktur im Backbone

1.5 Angaben zur Netzintegration

Die Netzinfrastruktur wird gleichzeitig für Wissenschaft und Verwaltung sowohl für eine reine Datenübermittlung als auch zur Telekommunikation genutzt. Letztere bezieht sich nicht nur auf das passive Medium, sondern auch auf die aktive Netzwerktechnik. So wird von der in einer Erprobungsphase exklusiven Benutzung von PoE-Switches für die Telefonie mittels VoIP dazu übergegangen, Switche gemischt für Telekommunikation und Datendienste zu nutzen. Damit wird dem Konvergenztrend – Telekommunikation nutzt z.B. Verzeichnisdienste, Computer dienen als Telefon, Fax-Übertragungen werden zu E-Mails und umgekehrt – Rechnung getragen. Die TK-Anlage wird modular erweitert und folgt der Struktur des Datennetzes. QoS sichert die störungsfreie Sprachübermittlung im Datennetz ab.

2. Netzentwicklungsplan

2.1 Realisierungsprioritäten

Das 10-Gigabit-Backbone muss redundant ausgelegt werden, damit eine höchstmögliche Ausfallsicherheit erzielt wird. Die wachsende Bedeutung des Netzes erfordert eine ständige Verfügbarkeit in höchster Qualität, da Ausfälle des Netzes immer gravierendere Beeinträchtigungen der Lehr- und Forschungstätigkeit an der Universität zur Folge haben können.

2.2 Meilensteine 2004-2013

Jahr	Maßnahmen
2004	Hochleistungsswitches zur Anbindung an Gigabit-Backbone und Umstellung auf Fastethernet-Switching
2005	Realisierung redundanter Ausbau des Gigabit-Backbones, IDS, WLAN
2006	Pilotprojekt zur Einführung von VoIP
2007	IDS > IPS
2008	Einführung 10-Gigabit-Backbone
2009	Controllerbasiertes WLAN
2010	Ausbau Layer 3 im Corebereich
2011	QoS netzweit einschl. WLAN
2012	Universitätsweiter Einsatz DHCP basierter Portsecurity (802.1x, MAC-basierend, Webauthentisierung)
2013	Universitätsweite IP-Adressverwaltung, Erneuerung zentraler Security-Hardware

2.3 Maßnahmen zur Fortschreibung des Netzkonzepts

An der Universität gibt es einen IT- Lenkungsausschuss, der sich aus Vertretern der zentralen Dienstleiter Universitätsrechenzentrum, Klinikrechenzentrum, Zentrale Universitätsverwaltung, Universitäts- und Landesbibliothek sowie dem Prorektor für Studium und Lehre, dem Kanzler und dem Leiter der Rektoratskommission für Rechentechnik-Großgeräte-Investitionen zusammensetzt. Hier werden Anforderungen an IT-Dienste und das Netz formuliert, die anhand der Erwartungen der Nutzer und aufgrund der technischen Entwicklung aktualisiert werden.

Die Anforderungen der Nutzer führen zu einer regelmäßigen Überprüfung der Leistungsfähigkeit der vorhandenen Netzwerktechnik und damit gegebenenfalls zur notwendigen Einführung neuer Technologien oder Dienste.

Einmal jährlich werden Soll- und Ist-Zustand anhand des Netzkonzepts geprüft und ggf. fortgeschrieben oder neu formuliert.

2.4 Migration von Diensten

Der endgültige Übergang zu VoIP geht mit der Ablösung der analogen Telefonhardware einher. Es werden keine Mittel mehr in die analoge Telefonie investiert.

3. Netzbetriebs- und Managementkonzept

3.1 Verteilung der Verantwortung zwischen zentralen und dezentralen Einrichtungen

Das Rechenzentrum bietet zentral Infrastruktur- und Basisdienste für die gesamte Universität an. Als wichtigste Softwarewerkzeuge zum Netzmanagement werden dabei Cisco Open View und HP Netview verwendet.

Fachspezifische Dienste werden zum Teil dezentral in den Fakultäten und Instituten bereitgehalten. Hierbei zeichnet sich eine weitere Zentralisierung im Sinne der Bereitstellung virtueller Server durch das URZ an Stelle physischer Server an dezentraler Stelle ab.

Verwaltungsdienste im weitesten Sinne (z.B. Campusmanagement usw.) werden durch das IT-Referat der Verwaltung bereit gestellt, Bibliotheksanwendungen werden durch die IT-Abteilung der Universitäts- und Landesbibliothek betrieben.

3.2 Festlegungen von Namens- und Adressräumen sowie Domänen

Die Vergabe von IP-Adressen erfolgt durch das URZ. (Sub-)Domänennamen werden, da sie i.d.R. für Webadressen verwendet werden, mit der Pressestelle abgestimmt und durch den Kanzler genehmigt.

Für Namensdienste werden im Rechenzentrum DNS-Server und LDAP-Server betrieben. In der Regel betreiben die anderen Struktureinheiten (bis auf wenige Ausnahmen) keine eigenen DNS- Server.

3.3 Zugangskontrollstrategien

Der Zugang zu allen Diensten unterliegt einer Nutzerkennzeichen- und Passwortpflicht. Durch das Rechenzentrum werden an jede/n interessierte/n Mitarbeiter/in und Studierenden eindeutige Nutzerkennzeichen vergeben. Diese können auf allen zentralen und dezentralen Servern benutzt werden. Die Aushändigung des Nutzerkennzeichens für Studierende erfolgt im Rahmen der Immatrikulation. Damit erhält der Studierende Zugang zu einem persönlichen Mailkonto, zum drahtlosen Netz sowie zu den universitätsoffenen Computerpools. In der Verwaltung gibt es aus Sicherheitsgründen hierzu gesonderte Regelungen. Dies trifft auch auf den Zugang und die Nutzung des Verwaltungsnetzes zu.

3.4 Sicherheit

Zu Sicherheitsfragen das Netz betreffend wird auf das Konzept zur IT-Sicherheit und zum Datenschutz der Universität verwiesen.

3.5 Accounting, Servicequalität, Netzüberwachung

Das Netz wird systematisch in regelmäßigen Abständen einer Qualitätskontrolle hinsichtlich der Dienstgüte (verfügbare und genutzte Bandbreite, Fehler usw.) unterzogen. Darüber hinaus wird die Auslastung an den Routerinterfaces und Trunkverbindungen erfasst (z. B. um den Auslastungsgrad der Internet-Anbindung zu messen). Nutzerbezogene Auswertungen finden nicht statt. Die Hauptkomponenten (Backbone) sind möglichst redundant ausgelegt, Standortverteiler zumindest vor Stromausfällen (durch USV) geschützt. Das URZ betreibt eine telefonische Servicehotline, die während der Kernarbeitszeit ständig besetzt ist. Als Troubleticket-System wird universitätsweit OTRS eingesetzt. Bei auftretenden Problemen wird eine Problemlösung am selben Arbeitstag angestrebt.

3.6 Regelungen der Netznutzung

Die Netznutzung wird durch entsprechende Ordnungen geregelt. Benutzerordnung, Betriebsordnung, Netzbetriebsordnung und Netzordnung sind unter

http://www.urz.uni-halle.de/ordnungen/

zu finden.

3.7 Unterstützung dezentraler Systeme und Dienste über das Netz

Die zu Beginn des neuen Jahrtausends noch in Vielzahl vorhandenen dezentralen Server wurden zu großen Teilen zunächst im Rechenzentrum untergebracht (housing), da sie häufig mindestens co-administriert wurden. Mittlerweile wurden bis auf wenige Ausnahmen fast alle dort gehaltenen Daten auf zentrale Systeme migriert . Da die hauptsächliche Aufgabe dieser Systeme in der arbeitsgruppenorientierten Dateihaltung bestand, konnte diese Funktion auf einen zentralen Nutzerdatenserver übertragen werden. Dadurch ist der dezentrale Administrationsaufwand auf ein Minimum reduziert. Mit der Einführung eines zentralen Virtualisierungsclusters besteht zudem die Möglichkeit, virtuelle Server für verschiedenste Anwendungen bereitzustellen, ohne dass z.B. Infrastrukturmaßnahmen zur Klimatisierung und erhöhten Stromzufuhr an dezentraler Stelle erforderlich sind. Das Datensicherungsvolumen beträgt gegenwärtig ca. 2 TB pro Tag; in 2014 werden bis zu 10 TB pro Tag erwartet. Bei dem gegenwärtigen Netzausbau, insbesondere im Backbone-Bereich sollte es keine Kapazitätsengpässe geben.

3.8 Klimatisierung und Energieversorgung

Gegenwärtig finden umfangreiche Umbauarbeiten am URZ statt. Ziel ist die Bereitstellung ausreichender Elektroenergie und Klimatisierungsleistung. Hierdurch soll zukünftig ein zentrales Housing ermöglicht werden. Der Umbau beinhaltet sowohl Netzersatztechnik als auch unterbrechungsfreie Stromversorgungstechnik. Es ist eine Endausbauleistung von bis zu 1 MW zur Stromversorgung geplant. Für eine effiziente Klimatisierung sorgen neue Klimaanlagen auch mit der Möglichkeit zur Wasserkühlung.