UNIVERSITÄT PADERBORN

Die Universität der Informationsgesellschaft

Netzbetriebs- und Managementkonzept der Universität Paderborn

Stand November 2012

IMT:

Zentrum für Informations- und Medientechnologien

Inhalt

1. Verantwortung- und Zuständigkeitsverteilung

Das IMT ist grundsätzlich für die Planung, den Betrieb und das Management des Hochschulnetzes bis zur Steckdose zuständig. Die Zuständigkeit wird in enger Zusammenarbeit mit den Fakultäten und der Verwaltung wahrgenommen. Dies geschieht durch intensiven Kontakt mit den Mitarbeitern, die für den Teilbereich Netzadministration Verantwortung übernommen haben. Sie können nach Schulung durch das IMT und in Absprache mit dem IMT Teilaufgaben der Netzadministration selbstständig wahrnehmen.

1.1. Planung

Beteiligt an der Netzausbauplanung sind die Fakultäten, die Betriebseinheiten, der Bau- und Liegenschaftsbetrieb NRW (BLB), das Dezernat 5 der Verwaltung und, federführend, das IMT. In Zusammenarbeit mit den Fakultäten und Instituten ermittelt das IMT den Bedarf und entwickelt eine Planung für die mittelfristige Entwicklung in quantitativer und qualitativer Hinsicht. Diese Planung ist Grundlage für die Umsetzung in konkrete Anträge, Bau- und Beschaffungsmaßnahmen, für die insbesondere auch die Verwaltung und der Bau- und Liegenschaftsbetrieb NRW im Rahmen ihrer Zuständigkeiten Verantwortung tragen. Durch geeignete Abstimmungsprozesse mit dem IMT wird sichergestellt, dass die Intentionen der Planung tatsächlich umgesetzt werden. Das IMT evaluiert in gemeinsamen Projekten mit anderen Bereichen der Universität regelmäßig innovative Netztechniken auf ihre Eignung für den hochschulweiten Einsatz.

1.2. Betrieb

Die grundsätzliche Zuständigkeit für den Betrieb des lokalen Netzes liegt beim IMT. Dabei gelten folgende Vereinbarungen:

1.2.1. Verkabelungsinfrastruktur

(Kabelwege, Verteilerräume, Primär-, Sekundär-, Tertiärverkabelung, Funkstrecken)

Der technische Betriebsdienst (TBD) des Dezernats 5 ist zuständig für die Bereitstellung und den Betrieb von Kabelwegen und Verteilerräumen. Alle Messungen, sofern diese nicht Bestandteil der Ersterstellung sind, die Beschaltung der Verteilerschränke samt zugehöriger Dokumentation und die Beseitigung von Störungen obliegen dem IMT. Der Betrieb der Verkabelungsinfrastruktur erfolgt in enger Abstimmung zwischen TBD und IMT.

1.2.2. Netzwerkkomponenten

(Switche, Router, Access Points)

Konfiguration, Überwachung und die Beseitigung von Störungen sind grundsätzlich Aufgabe des IMT. Die Netzwerkkomponenten sind in Verteilerräumen untergebracht. Sofern sie zum Betrieb dezentraler Infrastrukturen dienen, sind sie auch in den Räumen der Fakultäten aufgestellt und werden von diesen betreut. Die Netzwerkversorgung der Mitarbeiter- und Pool-Arbeitsplätze unterliegt bis auf wenige Ausnahmen dem IMT. In der Mathematik, dem Heinz Nixdorf Institut (HNI) sowie dem Paderborn Center for Parallel Computing (PC^2) werden einige spezielle Sub-Netzwerke selbständig betrieben, die jedoch vom IMT geroutet und an das Corenetz der Universität angeschlossen werden. Das Anbringen sowie der Betrieb eigener Access Points sind nur nach Absprache mit dem IMT gestattet. Die Funktionalität unautorisierter Access Points wird in Gebäuden der Universität aktiv unterbunden.

1.2.3. Netzdienste

Das IMT betreibt das Netz der Universität Paderborn und zentrale Netzdienste für die Hochschule. Einige der im Folgenden aufgelisteten Netzdienste (DNS, DHCP, RADIUS) werden grundsätzlich vom IMT und nur in einigen wenigen Fällen auch dezentral erbracht. Ähnlich wie bei anderen Diensten (E-Mail, WWW, Datensicherung) erfolgt weiterhin eine Rezentralisierung in Kooperation zwischen IMT und den dezentralen Betriebsgruppen.

1.2.4. Verfügbarkeit der angebotenen zentralen Netzdienste

Die Geschäftsprozesse der Universität hängen mittlerweile von der Verfügbarkeit zentraler Netzdienste ab. Um Ausfälle zu vermeiden, werden als grundlegende Policy zentrale Dienste, soweit technisch möglich, redundant ausgelegt und ausfallsicher hinter Loadbalancern zur Verfügung gestellt. Dadurch lassen sich Dienste auf unabhängigen Maschinen betreiben. Den Nutzern werden sie allerdings transparent unter einer IP-Adresse bzw. einem Namen zur Verfügung gestellt. Die Last verteilt sich gleichmäßig auf alle Systeme. Bei einem Ausfall, einem Software-Update o. ä. übernehmen die verbleibenden Maschinen die Anfragen ohne Rekonfigurationsaufwand bei den Nutzern.

1.2.5. Verwaltung von IP-Adressen, Betrieb des Domain-Name-Service (DNS)

Die Vergabe der IP-Adressen im Netz der Universität Paderborn wird vom IMT vorgenommen. Das IMT betreibt den primären und sekundären DNS-Server für die Domäne uni-paderborn.de. Für einige wenige Unterdomänen werden in den Fakultäten eigene DNS-Server betrieben.

1.2.6. DHCP

Das IMT betreibt einen zentralen DHCP-Dienst für die gesamte Universität. Dieser Service wird teilweise auch von den Fakultäten für die ihnen zugeteilten IP-Bereiche selbst erbracht.

1.2.7. Radius-Server

Um eine einheitliche Authentifizierung der Nutzer beim Zugang zum WLAN und per Wählmodem sicherzustellen, betreibt das IMT einen redundant ausgelegten, zentralen Radiusserver.

1.2.8. Sicherheitsdienste

Die implementierten netzseitigen Sicherheitsmechanismen werden in Kapitel 5 genauer erläutert.

1.2.9. Multicast

Multicastfähigkeit ist flächendeckend erreicht.

1.2.10. Internet-Anschluss

Der Betrieb des Internet-Anschlusses liegt in der vollen Verantwortung des IMT. Momentan besteht die Anbindung aus 2 aktiven Anschlüssen mit einer Bandbreite von je 600 Mbit/s. Die gleichzeitige Nutzung und gleichmäßige Auslastung der beiden Leitungen wird seitens DFN-NOC geregelt.

1.2.11. Weitere Dienste

(E-Mail, WWW, Daten- und Speicherverwaltung, Videodienste, digitale Bibliothek, eLearning)

Neben den bereits genannten Netzdiensten bietet das IMT eine Reihe von weiteren netzbasierten Diensten an. Diese sind genauer im Netzkonzept der Universität Paderborn erläutert und verfügen über jeweils eigene Betriebsregelungen.

2. Administration

2.1. Adress- und Namensraum

Die Universität Paderborn verfügt über ein eigenes Class-B-Netz (131.234.0.0) sowie über 17 Class-C-Netze. Die Struktur des Namensraums unterhalb von uni-paderborn.de/upb.de folgt den Strukturen auf der Ebene der Fakultäten, Institute, Lehrstühle und Arbeitsgruppen.

2.2. Identitätsmanagement und Benutzerverwaltung

Das IMT hat gemeinsam mit der Verwaltung ein hochschulweites Identitätsmanagement aufgebaut und betreibt darauf basierend eine zentrale Benutzerverwaltung. Hochschulweite Dienste nutzen die zentralen Authentifizierungsdienste via LDAP, Active Directory und Kerberos.

2.3. IP-Geräte

Alle am Datennetz der Hochschule stationär betriebenen Geräte müssen bei einem Netzverantwortlichen oder beim IMT angemeldet werden. Bei der Anmeldung muss eine verantwortliche Person benannt werden, die bei Missbrauch oder Problemen mit dem Gerät kontaktiert werden kann. Das IMT trägt von gemeldeten Geräten die Hostnamen und IP-Adressen in die zentrale Hosttabelle ein.

2.4. WLAN

Um das WLAN der Universität Paderborn benutzen zu können, muss man als Benutzer registriert sein. Die Authentifizierung erfolgt im eduroam-Verbund des DFN-Vereins für lokale Benutzer mittels 802.1X und X.509-Zertifikat. Für die anderen SSIDs erfolgt eine webbasierte Authentifizierung mittels Benutzername und Passwort.

3. Netzmanagement

3.1. Dienstqualität

Das IMT berät die Angehörigen der Universität Paderborn bei der Nutzung der angebotenen Netzdienste, unterstützt bei der Aufklärung von Störungen und hält regelmäßige Informations- und Schulungsveranstaltungen ab. Für die Netzverantwortlichen der Universität Paderborn ist ein geschlossener Webbereich eingerichtet, in dem interne Detailinformationen zur Verfügung gestellt werden. Zusätzlich werden Informationen über eine Mailingliste weitergeleitet.

3.2. Dienstgüte

3.2.1. Verfügbarkeit

Ziel des IMT ist es, mit dem vorhandenen Personal eine maximale Verfügbarkeit des Netzes zu gewährleisten. Dazu werden technisch alle Mechanismen (z. B. Redundanzen auf Komponenten- und Leitungsebene, HSRP, proaktives Management usw.) genutzt, die eine schnelle und möglichst automatische Umschaltung im Fehlerfall bewirken sollen. Zudem können Wartungskosten

niedriger gehalten werden, da keine sehr kurzen und damit sehr teuren Reaktionszeiten vereinbart werden müssen.

3.2.2. QoS

Die Mehrheit der von IMT installierten aktiven Netzwerkkomponenten erfüllt bereits die Anforderungen an IP QoS. Im bisher reinen Datennetzwerk war der Bedarf an flächendeckender QoS-Installation nicht vorhanden. Durch die Einführung von Sprachdiensten (VoIP) in einigen Neubauten (Gebäude O, Gebäude ZM1) wurde, begrenzt auf diese Gebäude, die Bereitstellung garantierter Netzleistung mittels QoS notwendig. Für die nächste Ausbaustufe des Netzes und die Migration auf VoIP ist die Evaluation und Umsetzung des flächendeckenden QoS geplant.

3.2.3. Bandbreitenbegrenzungen

Eine Bandbreitenbegrenzung ist an der Universität Paderborn nicht implementiert.

3.2.4. Service-Level-Reporting

Das IMT stellt in einem geschützten Webbereich den Netzverantwortlichen an der Universität die folgenden Informationen über den Zustand der Netzdienste zur Verfügung:

- Aktuelle Version der Konfiguration des zentralen IDS/IPD/Firewall-Systems
- IP-Filter für Subnetze
- Sicht auf den aktuellen Zustand des Netzes (Lese-Zugriff auf das Orion-Netzwerk-Management-System von SolarWinds) und Auslastungsstatistiken (Switche / Router)
- Die Host-Tabelle 131.234.0.0 der Universität Paderborn
- Liste der IP-Netze 131.234.0.0 und der zuständigen Betreuer
- Liste aller VLANs und Router zu den VLANs

3.3. Wartungskonzept für aktive Netzwerkkomponenten

Das IMT geht nicht davon aus, dass eine Komplettwartung des Hochschulnetzes durch einen externen Dienstbieter realisiert werden sollte. Einige wenige Dienste, die vom IMT nicht erbracht werden können, werden extern eingekauft.

Das Wartungskonzept des IMT beinhaltet:

- Redundante Auslegung der zentralen Netzleitungen und aktiven Netzwerkkomponenten (Kernnetz und Gebäude-Anbindung)
- Identifikation von Störungen, Störungsbehebung einschließlich Aus- und Einbau von Komponenten durch das IMT
- Einsatz möglichst einheitlicher Produktlinien, um eine homogene Netzinfrastruktur zu schaffen und dadurch Einarbeitungs- und Managementaufwand zu minimieren, eine einfache Austauschbarkeit der Geräte zu ermöglichen und eine hohe technische Kompetenz aufzubauen.
- Vorratshaltung einiger weniger Ersatzgeräte für meisteingesetzte Komponenten (Etagenswitche)

- Servicewartungsvertrag für alle Netzwerkkomponenten (außer Etage) mit einem Servicepartner mit folgenden Leistungen:
    - Austausch defekter Komponenten aus dem Kernbereich innerhalb von 4 Stunden
    - Austausch defekter Teile aus dem sekundären Bereich innerhalb von 24 Stunden
    - Lizenzrechte für Softwareupdates
    - Third-Level-Support bei inhaltlichen Problemen (Telefon-, E-Mail-Support)

3.4. Management der passiven Komponenten (Facility Management)

Das IMT betreibt ein so genanntes Facility-Management-System (System Command der Firma FNT), mit dessen Hilfe diverse Daten im Umfeld der passiven und aktiven Netzwerkkomponenten gepflegt und vorgehalten werden. Dazu zählt einerseits die Dokumentation sämtlicher Verbindungen in Form von verlegten Fixkabeln und geschalteten Patchkabeln. Andererseits werden Serien- und Inventarnummern sowie Standorte aller verbauten und eingelagerten Komponenten vorgehalten. In einer erweiterten (mit Einbeziehung der internen Kunden) Testphase befindet sich ein vom IMT entwickeltes nachgelagertes System, das den Administratoren in den Arbeitsgruppen ermöglicht, selber Switchports mit eigenen Netzen zu beschalten. Dieses System bezieht die benötigten Informationen zur Verkabelung aus dem Facility-Management-System und aggregiert diese mit Live-Daten aus den jeweiligen aktiven Komponenten.

Beide oben genannten Systeme verfügen über Mandantenfähigkeit und Benutzerverwaltung. So können auch Administratoren in den dezentralen Einheiten ihre lokal betriebenen Komponenten und Netzwerke dokumentieren und nach Bedarf mit ihren eigenen Subnetzen beschalten. Damit kann die Dokumentation immer auf dem aktuellen Stand gehalten werden. Gleichzeitig werden die Reaktionszeiten bei Rangierarbeiten weiterhin minimal gehalten. Um die Bedienbarkeit beider Systeme möglichst einfach zu halten, werden graphische Benutzerschnittstellen bereitgestellt.

Es wird zwischen lesenden und schreibenden Zugriffen auf die Managementdaten unterschieden. Ein schreibender Zugriff durch einen Netzverantwortlichen auf diese Daten hat das Absolvieren einer Schulung zur Bedienung beider Systeme zur Voraussetzung. Die Schulungen werden vom IMT vorbereitet und durchgeführt.

Die Administration der beiden Systeme obliegt dem IMT.

3.5. Netzüberwachung und Management der aktiven Komponenten

Gegenwärtig erfolgt ein permanentes Monitoring aller aktiven Netzkomponenten durch unterschiedliche Werkzeuge zum Monitoring – siehe 4.1.

Das Konfigurationsmanagement erfolgt im Wesentlichen manuell, unterstützt durch eigene Skripte. Die Wartung und der Betrieb dieser Vielzahl von Tools sind nicht effizient, die Funktionalität nicht ausreichend.

Angestrebt wird ein zentral installiertes, hardwareübergreifendes Netzwerk-Managementsystem, das auf standardisierte Protokolle und Schnittstellen zugreifen kann und folgende Funktionen realisiert:

- Konfigurationsverwaltung und Steuerung des Netzwerkes
- Unterstützung bei Planung, Erweiterung und Wartung des Netzwerkes

- Fehlermanagement, Aufdeckung von Engpässen im Netz und Lösungsvorschläge
- Performance-Management, Protokollierung, Steigerung der Netzeffizienz
- Report-, Event- und Benachrichtigungsfunktionen
- Verteilung von Netzwerk-Ressourcen QoS
- Energiemanagement

3.6. Störungsmanagement

Viele Geschäftsprozesse der Universität sowie die Arbeitsfähigkeit ihrer Angehörigen hängen wesentlich von der Funktionsfähigkeit des Netzes und der Netzdienste ab. Störungen werden durch Überwachungssysteme oder durch Meldungen der Nutzer erkannt. Fehlermeldungen können sowohl telefonisch an die Hotline des IMT (05251-605544) als auch per E-Mail an benutzerberatung@uni-paderborn.de gemeldet werden. Zur dokumentierten und nachhaltigen Verfolgung und Lösung von Problemen setzt das IMT das Open-Source-basierte Trouble-Ticket-System OTRS ein.

Je nach Störung werden vom IMT geeignete Maßnahmen ggf. in Zusammenarbeit mit dem DFN-Verein, Netzverantwortlichen oder Lieferanten eingeleitet. Ziel des IMT ist es, einen zuverlässigen Netzbetrieb auch außerhalb der Dienstzeiten sicherzustellen. Dies ist bislang durch das Engagement der Mitarbeiter und studentischen Hilfskräfte möglich gewesen; eine Garantie dafür existiert nicht.

4. Accounting

4.1. Nutzungsstatistiken zu Informations- und Planungszwecken

Zur frühzeitigen Erkennung von Engpässen in der Netzwerkinfrastruktur und zu allgemeinen Informationszwecken werden Kenndaten des über das Hochschulnetz transportierten Datenverkehrs sowie weitere Betriebsparameter an geeigneten Stellen gewonnen und für Auswertungszwecke zur Verfügung gestellt. Als Werkzeug dafür werden die Software Orion Network Performance Monitor von SolarWinds für das LAN und AirWave der Firma Aruba Networks für das WLAN eingesetzt.

4.2. Nutzungsstatistiken zu Abrechnungszwecken

Es werden keine Gebühren für die Nutzung des Netzes der Universität Paderborn berechnet.

4.3. Datenschutz

Im Zuständigkeitsbereich des IMT fallen Daten beim Betrieb des Netzes und der zentralen Server an. Es werden grundsätzlich nur die Daten gesammelt, die zur Erbringung der Netzwerkdienste erforderlich sind.

Dabei ist datenschutzrechtlich bei personenbezogenen Daten zwischen Bestands- und Verbindungsdaten zu unterscheiden:

- Bestandsdaten sind personenbezogene Daten wie Name, Adresse, Bankverbindung, die für ein Vertragsverhältnis notwendig sind bzw. in der Hochschule gespeichert werden, um eine Zuordnung zwischen Login-Namen und juristischen Personen sicherzustellen.

- Verbindungsdaten beschreiben den Zugang und die Aktivitäten eines Nutzers (Benutzerkennungen, dynamisch vergebene IP-Adressen, Verbindungen, genutzte Dienste etc.).

Häufig ist auch von Verbindungsdaten die Rede, wenn es spezieller darum geht, wer wann mit wem kommuniziert hat. Höchste datenschutzrechtliche Relevanz haben die Inhalte der Kommunikation.

Das IMT sammelt, speichert und wertet aktiv Verbindungsdaten aus, sofern sie für den ordnungsgemäßen Betrieb des Netzes oder der Server notwendig sind. Im IMT existiert eine Liste dieser Daten, in der der betriebliche Zweck und die daraus abgeleitete Dauer der Speicherung aufgelistet sind. Das IMT gibt Verbindungsdaten an auskunftsersuchende Behörden nur nach Rücksprache mit dem Justiziariat der Universität Paderborn weiter, wenn die entsprechenden juristischen Grundlagen dafür vorhanden sind.

Bezüglich der Netzdienste werden aufgezeichnet:

- **Logdaten**

  Bei den gesammelten Daten handelt es sich in der Regel um Logging-Einträge der Netzwerkgeräte und -dienste, die entweder auf den Geräten lokal oder auf einem gesonderten Server abgelegt werden. Genutzte Logdateien, gespeicherte Daten und die Dauer der Speicherung sind dokumentiert.

- **Personenbezogene Verbindungsdaten**

  Die Daten fallen an bei allen Netzwerkdiensten, die nur nach einer erfolgreichen Authentifizierung benutzbar sind, z. B. WLAN, Grüne Dosen, OpenVPN. Die Daten werden in den Logdateien der zuständigen Netzwerkgeräte (WLAN-Controller) oder der Server (Radius-, OpenVPN-Server) abgelegt. Es werden ein Zeitstempel und die Benutzerkennung eines Dienstteilnehmers gespeichert. Beim DHCP-Dienst wird kein direkter Bezug zu einer Benutzerkennung hergestellt. Es wird die Zuordnung IP zu MAC-Adresse des Rechners protokolliert. Diese Daten werden nach 7 Tagen gelöscht.

5. Sicherheit im Netz

Die Universität Paderborn ist sich bewusst, dass ihre Arbeitsfähigkeit zunehmend von der Sicherheit (Verfügbarkeit, Integrität und Authentizität) ihrer IT-Dienste abhängt, und sieht diesen Bereich als eine der großen Herausforderungen in den nächsten Jahren. Sie hat in Ergänzung zu dem ersten Sicherheitskonzept aus dem Jahr 1999 Anfang 2012 eine Leitlinie zur Informationssicherheit verabschiedet (siehe Anhang) und ist im Begriff, ein IT-Sicherheitsmanagement aufzubauen.

Grundlegende Maßnahmen der Netzsicherheit werden sich vermutlich im Zuge der Weiterentwicklung der IT-Sicherheit an der Universität Paderborn ebenfalls ändern. An dieser Stelle wird daher der IST-Zustand ohne weitere Bewertung beschrieben.

5.1. Verantwortlichkeit und Organisation

Die Verantwortung für das Netzwerk der Universität Paderborn liegt beim Zentrum für Informations- und Medientechnologien (IMT). Sie wird fachlich von der Netzgruppe im IMT wahrgenommen. Die Verantwortlichkeiten und die Stellvertretung sind geregelt. In besonderen Fällen werden Teilaufgaben des Netzbetriebs vom IMT an so genannte dezentrale Netzverantwortliche delegiert. Für den Netzbetrieb ist der Betrieb von Servern notwendig. Diese Aufgaben werden in Absprache mit der Servergruppe des IMT vorgenommen.

5.1.1. Aufgaben und Verantwortlichkeiten der dezentralen Netzverantwortlichen

Ein dezentraler Netzverantwortlicher fungiert als Vermittler zwischen dem Institut bzw. Fachbereich und dem IMT. Die Liste der dezentralen Netzverantwortlichen befindet sich unter http://www.uni-paderborn.de/imtnet/IP-Netz-Betreuer.htm. Dezentrale Netzverantwortliche können in besonderen Fällen einen Zugang zu den von IMT verwalteten Netzwerkkomponenten bekommen.

Aktionen, die ein Netzverantwortlicher durchführen darf, werden in definierten Workflows detailliert spezifiziert. Alle Aktionen, die im Rahmen eines Workflows geschehen, werden automatisch protokolliert und die Veränderungen an der Infrastruktur in einer Dokumentation erfasst.

Alle Eingriffe in die Netzwerkinfrastruktur außerhalb der Workflows dürfen nur nach vorheriger Rücksprache mit dem IMT erfolgen. Diese Eingriffe werden ebenfalls protokolliert und deren Ergebnisse in der Dokumentation erfasst.

Die dezentralen Netzverantwortlichen sind verpflichtet,

- die definierten Workflows einzuhalten,
- an Netzwerk- Schulungen, die vom IMT gehalten werden, teilzunehmen. Die Schulungen werden veranstaltet, um die jeweils aktuellen Entwicklungen im Netzwerkbereich zu kommunizieren.

5.1.2. Aufgaben und Verantwortlichkeiten der Servergruppe des IMT

Die Server für die Netzdienste werden von der Servergruppe installiert, die auch für das Einspielen von Sicherheitsupdates sowie für die Grundinstallation verantwortlich ist. Die Installation der Monitoring-/Managementsoftware geschieht in beidseitiger Absprache und wird von der Netzgruppe durchgeführt. Der Betrieb der Applikation-Software (Konfiguration, Updates und Wartung) wird von der Netzgruppe übernommen.

5.2. Physikalischer Zugriff auf Netzkomponenten

5.2.1. Zugriff auf Datenleitungen

Zugriff auf die passive Infrastruktur im Netz (Datenleitungen) haben die Mitarbeiter der Netzgruppe im IMT, die Mitarbeiter des TBD in Dez. 5 sowie auftragsorientiert externe Dienstleister nach vorheriger Absprache und Beauftragung durch Dez. 5 oder IMT.

5.2.2. Zugriff auf Hardware-Komponenten

Die Hardware-Komponenten (Router, Switche, Bridges, Controller, Server, AccessPoints, USV) im Netzbereich befinden sich in Netzwerkverteilerräumen, in Serverräumen und in der Freifläche.

- **Netzwerkverteilerräume**

  Der Zugang zu den Netzwerkverteilerräumen ist auf die Mitarbeiter der IMT-Netzgruppe sowie auf einige wenige dezentrale Netzverantwortliche beschränkt und wird durch einen Spezialschlüssel gesichert. Die Ausgabe des Spezialschlüssels wird autorisiert durch die Leitung der IMT-Netzgruppe und erfolgt durch Dez. 5. Alle Inhaber von Schlüsseln werden im IMT schriftlich festgehalten.

- **Serverräume**

  Eine Übersicht über alle Serverräume sowie die vom IMT verwalteten Netzkomponenten befindet sich im Anhang. Der Zugang zu den Serverräumen obliegt dem jeweiligen Verantwortungsbereich. Es ist von den Verantwortungsbereichen sicherzustellen, dass der Zugang beschränkt und gesichert ist. Für die IMT-Serverräume (N2.206, Gebäude O) gilt, dass sie über Zugangskontrollmaßnahmen sowie weitere Sicherungsmaßnahmen verfügen. Der Zugang zum Raum N2.206 ist auf Mitarbeiter der jeweiligen Kunden (Housingbereich) und auf Mitarbeiter des IMT (Bereich mit zentralen Servern) beschränkt. Der Zugang zum Rechenzentrum im Gebäude O ist auf vier Mitarbeiter (Netzwerk- und Serverbereich) des IMT beschränkt. Zu beiden Standorten haben außerdem Zugang ausgewählte technische Mitarbeiter des Technischen Betriebsdienstes sowie über Zugangsschaltungen im Notfall die Feuerwehr.

- **Freifläche**

  In der Freifläche sind AccessPoints angebracht. Grundsätzlich versucht das IMT, den direkten physikalischen Zugriff auf diese Komponenten durch Höhe zu unterbinden. Eine Funkbrücke mit Komponenten in den Gebäuden W und IBFM ist in den dortigen Netzverteilerräumen montiert.

5.3. Redundanz- und USV-Konzept

Zur Erhöhung der Verfügbarkeit werden wichtige Netzwerkkomponenten, soweit wirtschaftlich und technisch möglich, redundant ausgelegt. Dies betrifft das Kernnetz (die beiden Core-Router vertreten sich gegenseitig im Ausfall), die Gebäudeanbindung (alle Gebäude sind durch zwei Gebäuderouter, die jeweils an jedem der beiden Core-Switche angeschlossen sind, angebunden), die Außenanbindung (redundante Datenleitung zum Provider) als auch wichtige Netzdienste (Firewall, Loadbalancer, dhcp, dns, ntp und radius). Diese Komponenten sind zusätzlich auch durch USV-Anlagen abgesichert.

Switche auf den Etagen sind nicht redundant ausgelegt, jedoch jeweils redundant an beide Gebäuderouter angeschlossen und werden nur in einigen wenigen Fällen per USV abgesichert. Für die Etagenswitche hält das IMT Hardware zum kurzfristigen Ersatz auf Lager. Bei den WLAN-Controllern ist ein Controller mehr als notwendig im Einsatz. Durch die Überprovisionierung steigt zum einen die Performance, zum anderen die Verfügbarkeit, weil bei Ausfall eines Controllers die entsprechenden Access Points automatisiert von den übrigen bedient werden.

5.4. Administrativer Zugriff auf Netzkomponenten

5.4.1. Berechtigungskonzept

Der administrative Zugang zu den aktiven Netzkomponenten (Router, Switche, Controller) ist durch ein personenbezogenes sowie ein rechnerbezogenes Rollen- und Rechtekonzept realisiert.

Alle vom IMT gewarteten Netzwerkkomponenten liegen mit ihrem Management-Interface in einem besonders gesicherten VLAN. Der Zugang zum diesem VLAN wird mittels ACLs auf den zuständigen Routern eingeschränkt. Die Pflege der zugelassenen Rechner erfolgt durch die Leitung der IMT-Netzgruppe. Zusätzlich sind die zugelassenen Protokolle beschränkt. Es sind erlaubt:

- ssh und https für die Administration

- snmp, icmp für Monitoringzwecke

Der eigentliche Zugang erfolgt durch eine persönliche Benutzerkennung und ein Passwort. Für die administrativen Zugriffsrechte wird in der Netzgruppe ein Admin-Passwort bekannt gegeben. Das Passwort wird regelmäßig gewechselt und ist für Notfälle im Notfall-Ordner hinterlegt.

5.4.2. Konzept für Konfigurationen, Updates und Teststellungen

Konfigurationen und Updates werden von der Netzgruppe nach Tests, Freigabe durch die Leitung der Netzgruppe und vorheriger Ankündigung per Hand oder per Skript eingespielt. Eine Management-Software zur Unterstützung des Prozesses wird derzeit evaluiert (Stand August 2012). Teststellungen werden in physikalisch separierten Umgebungen durchgeführt.

5.4.3. Backup-Konzept

Die Konfiguration der Netzkomponenten wird per TFTP auf dem TFTP-Server isis.uni-paderborn.de regelmäßig gesichert und kann so im Notfall wiedereingespielt werden.

5.4.4. Monitoring-Konzept

Die Überwachung der Netzkomponenten wird mit Hilfe der Software Orion Network Performance Monitor der Firma SolarWinds für das LAN und AirWave der Firma Aruba Networks für das WLAN vorgenommen.

5.5. Maßnahmen zur Kontrolle von Datenströmen

Die folgenden netzseitigen Sicherheitsmaßnahmen sind an der Universität Paderborn implementiert.

5.5.1. Nutzung von Subnetzen und VLANs

Bis auf eine Ausnahme (direkte Verbindung zwischen zwei Datacenter-Standorten) sind Layer2-Netze auf einzelne Gebäude beschränkt, um unter anderem zu große Broadcast-Domänen zu vermeiden und eine schnelle Fehleranalyse und Begrenzung von Netzwerkfehlern auf nur ein kleines Segment des Netzes zu ermöglichen. In den Gebäuden werden nach Bedarf Subnetze (als VLANs) eingerichtet, die sich entweder aus dem Verantwortungsbereich oder aus der Sicherheitsklasse ergeben. Die zur Verfügung stehenden Sicherheitsklassen werden in der Regel durch Benutzeranforderungen im Dialog festgelegt. So gibt es unterschiedliche VLANs für Mitarbeiter-Arbeitsplätze, öffentliche studentische Arbeitsplätze (Pools), Labor-Arbeitsplätze, Server sowie besonders zu sichernde Arbeitsplätze (z. B. in Sekretariaten), und zwar auf Fakultäts-, Instituts- oder Arbeitsgruppen-Ebene.

5.5.2. Access Control Lists (stateless packet screen; Paketfilter)

Zwischen Subnetzen wird zur Sicherung der Sicherheitsklassen mit ACLs gearbeitet. Die ACLs werden zentral auf dem TFTP-Server isis.uni-paderborn.de verwaltet und per TFTP auf die entsprechenden Router umverteilt und aktiviert. Die aktuellen Versionen der ACLs sind nur für die Netzverantwortlichen zu sehen unter imt.uni-paderborn/imtnet/acls.

5.5.3. Firewall zwischen Uni-Netz und Internet

Zwischen dem Internet und der Universität sind zwei redundant ausgelegte Firewall/Intrusion-PreventionSysteme (Produkt Stonegate der Firma StoneSoft) implementiert. Die Geräte sind zwischen dem DFN-Internetrouter und den Core-Routern der Universität angebunden und wer-

den im so genannten Aktiv/Aktiv-Loadbalancing-Mode betrieben. Die Firewall-Regeln sind dokumentiert und für Netzverantwortliche einzusehen. Der Zugriff auf die Firewall-Systeme erfolgt in Analogie zu dem Zugriff auf alle anderen Netzkomponenten.

5.5.4. IDP / IPS

Das IMT setzt das o. a. Produkt Stonegate für das Monitoring des Zustands des Netzwerkes ein. Bei Auffälligkeiten wird manuell eingegriffen.

5.5.5. Quality of Service (QoS)

In einem Teilbereich des Netzes ist derzeit für die Sicherung von VoIP Quality of Service implementiert. Die implementierten Regeln sind unter https://wiki.uni-paderborn.de/QoS zu finden.

Vor dem weiteren Ausbau von VoIP soll der flächendeckende Einsatz von QoS evaluiert werden. Zusätzlich soll überprüft werden, ob sich QoS-Maßnahmen auch als ein technisches Hilfsmittel für die Abwehr von DoS-Attacken eignen.

5.6. Sicherer Verkehr über unsichere Netze

Mittels VPN ermöglicht das IMT allen registrierten Benutzern sichere Verbindungen über unsichere Netze (Internet, WLAN). Dazu betreibt das IMT eine Reihe von OpenVPN-Servern, mit denen sich Uni-Angehörige weltweit über einen beliebigen Netzzugang in das Uni-Netz einwählen können. Die Authentifizierung der Benutzer erfolgt wie im WLAN mit einem Netzwerkzertifikat. Je nach Zugehörigkeit zu einer LDAP-Gruppe, z. B. Mitarbeiter eines Instituts, Administratoren eines Netzes, Studenten einer Fakultät usw., werden die Benutzer in ein gruppenspezifisches IP-Netz angebunden.

Zur Sicherung der Vertraulichkeit der Daten wird an der Universität Paderborn unverschlüsselte Kommunikation wie TELNET oder FTP nicht unterstützt und vom IMT auch nicht angeboten. Es werden stattdessen Verfahren mit Verschlüsselung (ssh, scp, sftp) auch beim Zugriff auf den Mailserver via IMAP und POP oder beim Zugriff auf Webbereiche (https) eingesetzt.

5.7. Zugangskontrollregeln zum Netz

Der Netzzugang an der Universität Paderborn ist möglich über Festnetzdosen in Räumen, Festnetzdosen in Freiflächen (so genannte Grüne Dosen) und das WLAN. Grundsätzlich ist eine anonyme Nutzung des Netzes nicht möglich.

Nur die vom IMT zugewiesenen IP-Adressen und die dazugehörigen Hostnamen dürfen im Universitätsnetz verwendet werden. Zusätzlich kann an den Switchen sichergestellt werden, dass nur registrierte MAC-Adressen Zugang zum Netz erhalten. Bei der Verwendung von DHCP zur Vergabe von IP-Adressen empfiehlt das IMT, dass registrierten MAC-Adressen jeweils eine feste IP zugewiesen wird.

5.7.1. Regeln zu Konfiguration der Netzwerkdosen und Vergabe von IP-Adressen an Festnetzdosen

- **Dosen in Büros und in Räumen mit einem begrenzten physikalischen Zugang (Schlüssel, Zugangskarte), an den stationäre oder mobile Rechner angeschlossen sind (AG-Pools, Labore)**

  Die Dosen werden nur auf Antrag eines Netzverantwortlichen für ein gewünschtes VLAN freigeschaltet, die IP-Vergabe erfolgt durch eine Eintragung im DNS oder per

DHCP mit fester Zuordnung MAC-Adresse zu IP. An die Dosen dürfen beliebige Rechner angeschlossen werden oder nach Wunsch nur ein durch MAC-Adresse bekannter Rechner (PortSecurity). Zusätzlich können die Netzverantwortlichen VLANs, für die sie verantwortlich sind, nur in Räumen der eigenen Bereiche nach Bedarf mit Hilfe einer Benutzeroberfläche mandantengesteuert selbst schalten.

- **Dosen in frei zugänglichen Räumen, an die stationäre Rechner angeschlossen sind (Pools, Labore)**

  Eine Dose wird nur auf Antrag eines Netzverantwortlichen für ein gewünschtes VLAN freigeschaltet, die IP-Vergabe erfolgt durch eine Eintragung im DNS oder per DHCP mit fester Zuordnung MAC-Adresse zu IP. An der Dose darf nur ein durch die MAC-Adresse bekannter Rechner (PortSecurity) angeschlossen werden. Auch hier haben die Netzverantwortlichen die Möglichkeit, selbst Anschlüsse wie oben beschrieben zu schalten.

- **Dosen in frei zugänglichen Räumen/Flächen für mobile Rechner (Grüne Dosen)**

  Die Dosen werden vom IMT in ein bestimmtes, gesichertes VLAN geschaltet. Die IP-Vergabe erfolgt ohne feste Zuordnung per DHCP. Zugang zum Netz ist nur mit VPN (OpenVPN) möglich.

5.7.2. Netzzugang zum WLAN

Für den produktiven Einsatz existieren an der Universität Paderborn die SSIDs eduroam, webauth und upb_tmp. Für alle SSIDs erfolgt die Vergabe der IP-Adressen per DHCP ohne feste Zuordnung zum Nutzer oder der Mac-Adresse seines Rechners.

- **Webauth und upb_tmp**

  Webauth und upb_tmp benutzen eine Authentisierung via Webformular. Notwendig sind Uni-Kennung und zugehöriges Passwort. Die Authentisierungsabfrage erfolgt verschlüsselt per SSL, die restliche Kommunikation erfolgt unverschlüsselt. Die Benutzer werden auf die möglichen Konsequenzen hingewiesen. In der SSID upb_tmp werden nur zeitlich begrenzte Sammel-IDs für Tagungen oder andere Veranstaltungen mit vielen Teilnehmern vergeben.

- **Eduroam**

  Die SSID eduroam wird nach der Policy des DFN-Vereins betrieben (siehe www.dfn.de/dienstleistungen/dfnroaming). Für Benutzer der Universität Paderborn ist ein X.509-Zertifikat des Endgeräts notwendig, welche die Benutzer im SelfService über benutzerverwaltung.upb.de beantragen können. Benutzer anderer DFN-Einrichtungen authentifizieren sich nach dem Standard ihrer Einrichtung. Die Verbindung erfolgt in beiden Fällen verschlüsselt.

6. Betriebs- und Nutzungsregelungen

- Verwaltungsordnung (siehe http://imt.uni-paderborn.de/verwaltungsordnung/)

7. Anhang : Leitlinie zur Informationssicherheit der Universität Paderborn

PRÄAMBEL

Der Hochschulbetrieb erfordert zunehmend die Verwendung von Verfahren und Abläufen, die sich auf Möglichkeiten der Informations- und Kommunikationstechnik (IT) stützen. Sie sind somit eine zentrale Grundlage für die Leistungsfähigkeit der Universität Paderborn als Universität der Informationsgesellschaft. Unter diesen Bedingungen kommt der „Sicherheit in der Informationstechnik“ („IT-Sicherheit“) eine grundsätzliche und strategische Bedeutung zu. Auf Grund der komplexen Materie, der sich schnell weiter entwickelnden technischen Möglichkeiten, der Heterogenität der IT-Landschaft und verteilten Verantwortung, muss ein kontinuierlicher IT-Sicherheitsprozess realisiert werden, der den besonderen Bedingungen einer Hochschule gerecht wird.
Die Entwicklung und Fortschreibung des IT-Sicherheitsprozess soll sich einerseits an den gesetzlich festgelegten Aufgaben der Universitäten sowie an ihrem Mandat zur Wahrung der akademischen Freiheit orientieren, andererseits soll sie keinen Selbstzweck erfüllen, sondern auf Grund von gesetzlichen Auflagen, Anforderungen der Universität Paderborn sowie Belangen von Anwenderinnen und Anwendern eine risikogerechte Bewertung von Gefährdungen vornehmen sowie entsprechende Maßnahmen einleiten.
Die vorliegende Leitlinie zur Informationssicherheit und das ergänzende Regelwerk zur Informationssicherheit dienen dazu, diesen Anspruch umzusetzen. Das Präsidium hat die Leitlinie beschlossen und unterstützt die erforderlichen Maßnahmen zur Realisierung der Informationssicherheit.

ZIELE UND ADRESSATENKREIS

Diese Leitlinie regelt die Verantwortung und die Zuständigkeiten sowie die Zusammenarbeit im hochschulweiten IT-Sicherheitsprozess. Es ist ihr Ziel nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern auch die in der Hochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen vor Missbrauch zu schützen.
Sie ist an alle Organisationseinheiten, Mitglieder und Angehörige der Universität Paderborn sowie an Dritte gerichtet, die IT-Systeme und IT-Verfahren benutzen oder betreiben.

LEITSÄTZE

Die Universität erfüllt die gesetzlichen Regelungen und vertraglichen Auflagen im Bereich der Informationssicherheit und des Datenschutzes sowie die Grundsätze der guten wissenschaftlichen Praxis. Sie orientiert sich insbesondere an den Schutzzielen der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz beim Umgang mit personenbezogenen Daten.

Als zusätzliche Prinzipien der Informationssicherheit sind für die Universität Paderborn festgelegt

- **Wohlorganisiertheit:** Für alle IT-Systeme und IT-Verfahren gibt es klare Verantwortlichkeiten
- **Informiertheit:** Alle Anwenderinnen und Anwender von IT-Systemen und IT-Verfahren sollen sich der für sie wesentlichen Sicherheitsrisiken und deren Abwehrmaßnahmen bewusst sein.

- **Zurechenbarkeit:** Jede von vernetzten Rechnern der Universität Paderborn ausgehende Aktivität soll einer Person zugeordnet werden können.
- **Aktualität:** Die eingesetzten IT-Systeme und IT-Verfahren sollen den jeweils aktuellen Sicherheitsempfehlungen einschlägiger Institutionen entsprechen.
- **Angemessenheit:** Alle Maßnahmen sind mit Augenmaß und in Hinblick auf die Gefährdungen und Risiken sowie ihr Kosten-Nutzen-Verhältnis zu wählen.
- **Wahrung eines permanenten Regelkreislaufes:** Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen wird regelmäßig überprüft. Verletzungen der Informationssicherheit werden kommuniziert und dokumentiert.
- **Recht auf informationelle Selbstbestimmung:** Die Universität unterstützt aktiv das Recht auf informationelle Selbstbestimmung und ist bestrebt die Erhebung, Speicherung und Nutzung personenbezogener Daten auf das Notwendige zu beschränken (Minimalität).

VERANTWORTLICHKEITEN

Die Leitung der Universität trägt die Gesamtverantwortung für die Informationssicherheit an der Universität Paderborn. Diese wird fachlich durch den Lenkungskreis für Informationssicherheit (LIS) wahrgenommen.
Die Verantwortung für die IT-Sicherheit jeder Organisationseinheit oder Einrichtung liegt bei der jeweiligen Leitung. Sie kann fachlich durch einen IT-Verantwortlichen wahrgenommen werden.
Falls externe Dienstleister beauftragt werden sind diese bei Aufnahme einer Vertragsbeziehung über entsprechende Passagen im Regelwerk zur Informationssicherheit zu informieren und schriftlich auf dessen Einhaltung zu verpflichten.
Alle Anwenderinnen und Anwender tragen die Verantwortung, bestimmungsgemäß und sachgerecht mit den von ihnen genutzten IT-Systemen, IT-Verfahren und Informationen umzugehen.
Die Finanzierung von Maßnahmen zur Informationssicherheit wird von den jeweiligen Verantwortlichen sichergestellt. Bei der Einführung neuer Verfahren ist die Sicherheit bereits bei der Planung zu berücksichtigen.

ORGANISATIONSSTRUKTUR

Zur Gestaltung des Informationssicherheitsprozesses an der Universität Paderborn wird die im Folgenden beschriebene Organisationsstruktur festgelegt. Sie besteht aus dem Lenkungskreis für Informationssicherheit, dem IT-Sicherheitsbeauftragten sowie den IT-Verantwortlichen und dem Computer Notfallteam.

Lenkungskreis für Informationssicherheit (LIS)

Der Lenkungskreis für Informationssicherheit (LIS) steuert im Auftrag des Präsidiums den IT-Sicherheitsprozess an der Universität Paderborn.
Er erarbeitet und empfiehlt in Zusammenarbeit mit den Verantwortlichen im Bereich Informationssicherheit strategische Empfehlungen und Maßnahmen wie diese Leitlinie und das Regelwerk zur Informationssicherheit und überprüft ihre Umsetzung.
Er berät das Präsidium im Bereich Informationssicherheit und empfiehlt und verantwortet hochschulweite Projekte in diesem Bereich.

Er nimmt die jährlichen Berichte der IT-Verantwortlichen im Bereich Informationssicherheit entgegen und berichtet einmal jährlich dem Präsidium zum Stand der Umsetzung der Informationssicherheit an der Universität Paderborn.
Er wählt aus seiner Mitte einen Ansprechpartner für Informationssicherheit, den IT-Sicherheitsbeauftragten der Universität Paderborn.

Zum Lenkungskreis zählen

- der CIO oder ein anderer Beauftragte oder eine Beauftragte des Präsidiums
- die/der behördliche Datenschutzbeauftragte
- jeweils eine Vertreterin oder ein Vertreter der Personalräte
- jeweils eine Vertreterin oder ein Vertreter der zentralen Organisationseinheiten, die hochschulweite IT-Systeme und IT-Verfahren verantworten, derzeit die Universitätsverwaltung, die Universitätsbibliothek, das Zentrum für Informations- und Medientechnologien (IMT)
- eine vom Präsidium benannte fachkundige Wissenschaftlerin oder ein vom Präsidium benannter fachkundiger Wissenschaftler
- die IT-Verantwortlichen der Fakultäten
- eine fachkundige Vertreterin oder ein fachkundiger Vertreter aus der Studierendenschaft (nach der Einführungsphase)

Das Präsidium sowie der LIS können weitere Teilnehmende zur Beratung hinzuziehen.

IT-Sicherheitsbeauftragter der Universität

Die/Der IT-Sicherheitsbeauftragte ist die zentrale Ansprechperson zu Fragen der Informationssicherheit an der Universität Paderborn.
Sie/Er koordiniert die Umsetzung der vom LIS empfohlenen Maßnahmen und verantwortet die Weiterentwicklung und Veröffentlichung des Regelwerks für Informationssicherheit.
Sie/Er berät die Organisationseinheiten, die Datenschutzbeauftragte oder den Datenschutzbeauftragten und organisiert Schulungs- und Sensibilisierungsmaßnahmen.

IT-Verantwortliche

Jede Organisationseinheit (Fakultäten, zentrale wissenschaftliche Einrichtungen, ZV, zentrale Betriebseinheiten) bestellt eine Person, die auf Grund ihrer Stellung, ihrer beruflichen Erfahrung und ihres Wissens qualifiziert ist, die Aufgaben einer /eines IT-Verantwortlichen zu übernehmen. Die Tätigkeit kann auch bereichsübergreifend wahrgenommen werden. Die Benennung ist zu dokumentieren und dem LIS anzuzeigen. Falls kein IT-Verantwortlicher bestellt wird, nimmt die Leitung der Organisationseinheit diese Funktion wahr. Entsprechende personelle Ressourcen müssen von den Organisationseinheiten zur Verfügung gestellt werden.
Die IT-Verantwortlichen sind zugleich Ansprechpartner für Informationssicherheit und tragen Sorge für die Weiterentwicklung von Maßnahmen sowie die Umsetzung der im IT-Sicherheitsprozess erarbeiteten Vorgaben. Sie informieren und berichten dem IT-Sicherheitsbeauftragten über Sicherheitsvorfälle in ihrem Verantwortungsbereich. Vorfälle mit Bezug auf personenbezogene Daten sind unverzüglich und unmittelbar dem IT-Sicherheitsbeauftragten anzuzeigen.

Computer Notfallteam

Das Computer Notfallteam der Universität Paderborn berät und unterstützt Organisationseinheiten bei der technischen Eingrenzung und Behebung von Angriffen, Störungen und Problemen durch die die Informationssicherheit verletzt wird oder verletzt werden kann. Das Notfallteam ist dem Störungsmanagement des IMT angegliedert. Es wird bei hochschulweiten Sicherheitsvorfällen in Absprache mit dem IT-Sicherheitsbeauftragten und dem Störungsmanager des IMT tätig und berichtet dem LIS über Sicherheitsvorfälle und deren Behebung.

REGELWERK ZUR INFORMATIONSSICHERHEIT

Diese Leitlinie bestimmt die Grundzüge der Informationssicherheit an der Universität Paderborn. Sie wird ergänzt durch ein Regelwerk zur Informationssicherheit, in dem grundlegende allgemeine Regelungen und Hinweise wie beispielsweise physikalische Sicherheit, Zutritts- und Zugangskontrolle, Rollen- und Rechte, Update-und Patchverpflichtung festgeschrieben werden. Zusätzlich werden detaillierte Maßnahmen und Policies beispielsweise für Organisationseinheiten oder Klassen von IT-Verfahren oder IT-Systemen beschrieben.