Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Arbeiten in der WISO-Domäne aus Sicht der Benutzer/innen („Benutzerleitfaden“)

Stand: 09.03.2011

Inhaltsverzeichnis

1 Vorbemerkungen 4

2 Mit der neuen Domäne verfolgte Ziele 4

2.1 Sicherheit 4
2.2 Wirtschaftliche IT-Versorgung 4
2.3 Aufgabenadäquate IT-Versorgung 5
2.4 Mobiles Arbeiten 5
2.5 Service und Support 5
2.6 Verfügbarkeit 5

3 IT-Ausstattung von Arbeitsplätzen 6

3.1 Standardisierung 6
3.2 Standard-Arbeitsplatzsysteme 6
3.2.1 Arbeitsplatzrechner 6
3.2.2 Drucker am Arbeitsplatz 7
3.2.3 Multifunktionsgeräte 8
3.3 Software 8
3.3.1 Lizenzen 8
3.3.2 Software in der Basisinstallation 8
3.3.3 Erweitertes Softwareportfolio 9
3.3.4 Vor Ort installierte Software 10
3.4 Beschaffungswesen 11
3.4.1 Bedarfsanmeldung und Finanzierung 11
3.4.2 Beschaffungsvorgang 11

4 Basisdienste 12

4.1 E-Mail und Groupware 12
4.1.1 E-Mail-Adresse 12
4.1.2 Speicherplatz für E-Mails 12
4.1.3 Verteilerlisten 12
4.2 Content Management System 12
4.3 Kollaborationssysteme 13
4.3.1 SharePoint 13
4.3.2 WISO-CommSy 13

5 Dateiablage 13

5.1 Datenspeicherung auf Servern 13
5.1.1 Persönlicher Ordner (Laufwerk Z:) 14
5.1.2 Gemeinsame Ordner (Laufwerk N:) 14
5.2 Datenspeicherung auf lokalen Festplatten 14
5.3 Offline- Synchronisation servergespeicherter Daten 15

6 IT-Sicherheit 15
6.1 Active Directory und Benutzerverwaltung 15
6.2 Rechte der Anwender/innen auf Arbeitsplatzrechnern 17
6.2.1 Grundsatz minimaler Rechte für Anwender/innen 17
6.2.2 Spezielle Aspekte des Arbeitens ohne lokale Administrationsrechte 18
6.2.3 IT-Umgebung mit erweiterten Rechten („Sandbox“) 18
6.2.4 Vergabe lokaler Administrationsrechte 19
6.2.5 Zusätzliche Sicherheitsfeatures für vertrauliche Daten 20
6.3 Netzsicherheit 20
6.4 Rechte der WISO-IT-Mitarbeiter/innen in der Domäne 21
6.4.1 Systemadministration 21
6.4.2 Anwenderunterstützung 22
7 Support 22
7.1 First-Level-Support 23
7.2 Second-Level-Support/ Administration 23
7.3 Beschwerdemanagement 23
7.4 Service-Level-Agreements (SLA’s) 23
8 Nachwort 24
9 Anhang: Migration und Integration 25
9.1 Migration 25
9.2 Integration 25

1 Vorbemerkungen

Mit Rundschreiben vom 23.02.2010 hatten Dekanat, FIO und WISO-IT über die Umsetzung des WAP-Antrags und die Neustrukturierung der IT in der WISO-Fakultät informiert. Die neue IT-Infrastruktur wurde installiert und die Benutzerinnen und Benutzer sowie deren Rechner wurden aus der alten HWP-NET-Domäne in die neue WISO-NET-Domäne migriert. Im Anhang wird der Unterschied zwischen der bereits abgeschlossenen Migration und der auf dem Weg zu einer fakultätsweiten IT-Versorgung noch ausstehenden Integration erläutert.

In dieser Broschüre wollen wir das hauptamtliche Personal, vor allem die Wissenschaftlerinnen und Wissenschaftler, über wesentliche Neuerung des Arbeitens in der neuen WISO-Domäne informieren. Vorweg sei betont, dass diese Vorzüge z.T. erst bei den im Abschnitt 3 beschriebenen heutigen Standardarbeitsplatzsystemen voll zum Tragen kommen. Deshalb wird es sich bei vielen Arbeitsplatzrechnern empfehlen, nach der Migration auch die lokale Softwareausstattung zu aktualisieren.

Da technische Hintergründe und Details einen solchen Benutzerleitfaden überfrachten würden, haben wir hier darauf verzichtet. Wir konzentrieren uns auf Fragen, die viele von Ihnen in den letzten Monaten an uns gerichtet haben. Da immer neue Fragen von allgemeinem Interesse gestellt werden, wird der Benutzerleitfaden fortlaufend aktualisiert und auf der Homepage der Fakultät bereitgestellt[1].

2 Mit der neuen Domäne verfolgte Ziele

Kardinalziel der WISO-IT-Strategie ist es, dem Wissenschaftlichen und Verwaltungspersonal und den an der Fakultät Studierenden ein sicheres, qualitativ hochwertiges, aufgabenadäquates IT-Dienste-Angebot zur Verfügung zu stellen. Dafür sind folgende Teilziele von besonderer Bedeutung.

2.1 Sicherheit

Die Arbeitsplatzcomputer sollen hinsichtlich der Sicherheit stets auf dem aktuellsten Systemstand gehalten werden (vgl. Abschnitt 6). Dazu müssen die Rechner gegen Schadprogramme aller Art abgeschottet, gegenüber unerlaubten Zugriffen abgesichert und die Daten der Benutzer kontinuierlich und automatisch gesichert werden. Dies setzt u.a. eine Datenspeicherung auf zentralen Servern voraus, aber auch eine restriktivere Handhabung von Zugriffsrechten als auf privaten Computern[2].

2.2 Wirtschaftliche IT-Versorgung

Service und Support sind personalintensiv. Um die IT-Kosten im Griff zu behalten, müssen automatisierbare Prozesse auch möglichst automatisiert ablaufen. Ein zweites zentrales kostendämpfendes Element ist Standardisierung (vgl. Abschnitt 3.1). Unnötige Heterogenität bei Hardware, Betriebssystemen und Anwendungssoftware verteuert die Beschaffung und Wartung und beeinträchtigt die Qualität des Betriebs

---

[1] Ausführungen zu einzelnen Softwareprodukten sind ebenfalls nicht Gegenstand dieses Benutzerleitfadens. Detaillierte Regelungen bleiben einer Benutzerordnung vorbehalten.

[2] Eine sichere IT-Versorgung besaß schon in der von WiSo-IT betriebenen Vorgänger-Domäne einen hohen Stellenwert und steht auch im Mittelpunkt der IT-Konzepte anderer Universitäten, z.B. der Freien Universität Berlin (vgl. „IT-Sicherheitsrichtlinie für die Freie Universität Berlin“, 25.02.2008 und „Kommentierte IT-Grundschutzmaßnahmen für IT-Anwender. Auszug aus der IT-Sicherheitsrichtlinie für die Freie Universität Berlin“, August 2009).

und Supports, weil das Know-how dann zwangsläufig mehr in die Breite als in die Tiefe geht.

2.3 Aufgabenadäquate IT-Versorgung

Standardisierung darf nicht zu Lasten der Aufgabenerfüllung in Lehre und Forschung gehen. Aus der Aufgabenangemessenheit folgt nicht nur die bereits erwähnte Unterstützung des „mobile computing“, sondern auch, dass über die Standard-Softwareinstallation hinausgehende spezielle Software für einzelne Professuren zur Verfügung stehen muss – sei es auf Servern und / oder auf Arbeitsplatzrechnern. WISO-IT kann nicht für jede hochspezialisierte Software das erforderliche Know-how vorhalten und die Administration und den Support in alleiniger Regie gewährleisten. Hier sind flexible Einzelfall-Lösungen und Absprachen gefragt, welche die übrigen hier genannten Ziele gleichwohl nicht gefährden dürfen. Schließlich kann und muss nicht jede Applikation in der WISO-IT-Infrastruktur laufen. Im Rahmen des grundsätzlich kooperativ angelegten IT-Versorgungskonzepts können auch Ressourcen anderer IT-Dienstleiter, insb. die des Regionalen Rechenzentrums, nach Absprache genutzt werden.

2.4 Mobiles Arbeiten

Arbeitsplätze an Universitäten sind heute nicht nur durchgängig rechnerunterstützt, sondern auch zunehmend mobil. Deshalb soll der Zugang zu IT-Ressourcen auch von außen ähnlich gut und sicher funktionieren wie in den Räumen der Universität.

2.5 Service und Support

Da neue Rechner mit einer von WISO-IT vorgegebenen Installation betriebsfertig ausgeliefert werden, brauchen sich die Fakultätsangehörigen um die Standardinstallation (Windows, Office & Co.) nicht selbst zu kümmern. Software-Updates, neue Virensignaturen etc. werden automatisiert über das Netz verteilt. Ein Großteil der über die Standardinstallation hinausgehenden Softwareprogramme kann vom Benutzer „on demand“ über das Netz nachinstalliert werden, wobei zentrale Lizenzserver darüber wachen, dass die Lizenzbedingungen der Fakultät und Universität eingehalten werden. Die Installation vor Ort durch Mitarbeiter von WISO-IT ist nur ausnahmsweise erforderlich. Das spart Zeit, die für eine bessere Beratung und Betreuung zur Verfügung steht.

2.6 Verfügbarkeit

Ein Arbeitsplatzcomputer soll nach Möglichkeit nie ausfallen. Wenn ein Computer dennoch fehlerhaft arbeitet, sollen die Benutzer/innen möglichst zeitnah an einem anderen Rechner mit den üblichen Standardanwendungen und ihren persönlichen Dateien und Einstellungen weiterarbeiten können. Das geht nur, wenn diese sich nicht auf dem Arbeitsplatzrechner, sondern auf zentralen Servern befinden (vgl. Abschnitt 5.1). Soweit vorrätig wird ein Ersatzrechner mit der üblichen Basisinstallation (vgl. Abschnitt 3.3.2) zur Verfügung gestellt. Die Nachinstallation weiterer Software (vgl. Abschnitte 3.3.3 und 3.3.4) ist u.U. unvermeidlich.

3 IT-Ausstattung von Arbeitsplätzen

3.1 Standardisierung

Durch die Standardisierung der Arbeitsplatzsysteme soll für die Mitglieder der Fakultät eine einheitliche Grundausstattung mit Hardware und Software erreicht werden. Historisch bedingt gab es bisher bei den Arbeitsplatzrechnern eine kaum überschaubare Fülle von Herstellern und Modellen in unzähligen Ausstattungsvariationen. Die Betreuung dieser heterogenen Systeme ist wirtschaftlich nicht durchführbar. Dies liegt vor allem am komplexen Zusammenspiel von Hardware und Software. Eine Vielzahl von Treibern muss vorgehalten, unter Umständen erst gesucht und häufig umständlich von Hand installiert und aktualisiert werden.

Ähnlich verhält es sich bei der auf den Arbeitsplatzrechnern installierten Software. Schon bei dem in der Fakultät meist genutzten Betriebssystem Microsoft Windows sind mindestens drei verschiedene Versionen im Umlauf. Microsoft Office ist auf den Rechnern in fünf verschiedenen Versionen im Einsatz. Zum Schutz vor Angriffen aus dem Netz oder durch Schadsoftware sind unterschiedliche Virenscanner lokal installiert. Diese Geräte in einem akzeptablen Zeitraum zu warten und zu aktualisieren ist im Grunde nicht mehr möglich.

Hier ist also mehr Standardisierung notwendig, die ohnehin durch die Rahmenverträge nahegelegt wird, ohne dass dadurch IT-Erfordernisse beeinträchtigt würden. Um die Professuren zu entlasten und um die Beschaffungsordnung der Freien und Hansestadt Hamburg einzuhalten, werden sämtliche IT-Beschaffungen (vgl. Abschnitt 3.4) von WISO-IT koordiniert.

3.2 Standard-Arbeitsplatzsysteme

Aktuell werden die Arbeitsplatzrechner und Drucker aus dem Rahmenvertrag der Universität Hamburg mit Dell beschafft. Bei Arbeitsplatzsystemen im Büro und bei Laptops kommen z.Zt. folgende Modelle bzw. Serien zum Einsatz. Alle Geräte werden mit drei oder fünf Jahren Garantie und einem 24-Stunden-Vor-Ort-Service beschafft. Die hier vorgestellten Geräte stehen beispielhaft für eine moderne IT-Ausstattung. Eine individuelle Abstimmung auf Ihre Anforderungen ist möglich.

3.2.1 Arbeitsplatzrechner

Stationäre Arbeitsplatzrechner

Dell Optiplex MT 980	
Gerätetyp	Desktop-PC
Prozessor	Intel Core i3-540 (3.06GHz, 4M)
Arbeitsspeicher	4,0 GB DDR3
Festplatte	160 GB SATA II
Optisches Laufwerk	16X DVD+/-RW

Dell 2209WA Ultrasharp	
Gerätetyp	Monitor
Größe	22” Widescreen
Auflösung	1680 X 1050 Pixel

Mobile Arbeitsplatzrechner

Dell Latitude Serie	
Gerätetyp	Laptop
Prozessor	Intel Core Label i5
Arbeitsspeicher	4,0 GB DDR3
Festplatte	160 GB SATA II
Optisches Laufwerk	8X DVD+/-RW
Display	13.3“, 14.1“ und 15.6“
Auflösung	1366 X 768 Pixel

Dell Latitude Serie	
Gerätetyp	Tablet
Prozessor	Intel Core Duo SU9400
Arbeitsspeicher	2,0 GB DDR3
Festplatte	64 GB SSD
Optisches Laufwerk	optional extern
Display	12,1“ Multitouch
Auflösung	1280 x 800 Pixel

Bei besonderen und begründeten Anforderungen können leistungsfähigere Arbeitsplatzrechner beschafft werden. Diese Anforderungen sollten im Vorfeld von Beantragungen mit WISO-IT geklärt werden.

Arbeitsplätze werden üblicherweise mit Schwarz-Weiß-Laserdruckern ausgestattet, während z.B. in den Sekretariaten von Professuren zusätzlich Multifunktionsgeräte vorgehalten werden können, um Farbdrucken, Scannen, Faxen zu unterstützen.

3.2.2 Drucker am Arbeitsplatz

Dell 2330dn Laserdrucker	
Gerätetyp	Drucker
Typ	s/w
Auflösung	1200 x 1200 dpi

Um die Verwaltung der Drucker zu vereinfachen, werden alle Drucker an einem zentraler Druckserver betrieben, sind also eigentlich keine lokalen, sondern Netzwerkdrucker. Durch die Integration in den weiter unten beschriebenen Verzeichnisdienst Active Directory (vgl. Abschnitt 6.1) werden Drucker nur für einzelne Benutzer bzw. Arbeitsgruppen freigegeben. Dadurch können Professuren oder Projekte auf ein zentrales Gerät zugreifen, ohne dass diese Drucker von beliebigen anderen Anwendern genutzt werden können.

3.2.3 Multifunktionsgeräte

Dell 2145cn-Multifunktions-Farblaserdrucker	
Gerätetyp	Multifunktionsgerät
Typ	Farbe
Funktionen	Scanner, Drucker, Fax, Kopierer

Ähnlich wie die Drucker werden auch die Multifunktionsgeräte zentral verwaltet und für eine Professur oder ein Projekt im Netzwerk freigegeben. Diese Geräte können in Farbe drucken und ermöglichen das Kopieren, Scannen und Faxen von Dokumenten.

3.3 Software

3.3.1 Lizenzen

Die Verwendung kostenpflichtiger Software ist immer an den Erwerb einer Lizenz gebunden. Neben universitätsweiten Lizenzen stellt WISO-IT auch Lizenzen zur Verwendung innerhalb der Fakultät bereit. Je nach Vertrag stehen diese Lizenzen allen Mitgliedern der Fakultät zur Verfügung oder im Rahmen kontingentierter Lizenzen nur einem Teil der Fakultätsmitglieder (wie etwa MathType oder EViews).

Einige Hersteller schreiben den Betrieb von Lizenzservern vor, über den die Gültigkeit einer Lizenz und die Anzahl der zeitgleich laufenden Anwendungen kontrolliert werden kann. Die von WISO-IT betriebenen Lizenzserver sind nur innerhalb des Netzwerkes der WISO-Domäne erreichbar, also nicht von außerhalb über einen reinen Internet-Zugang, wohl aber über eine VPN-Verbindung.

Durch den Einkauf von Netzwerklizenzen reduzieren sich die Anschaffungskosten für Software oft erheblich. Deshalb sind Netzwerklizenzen unter den Aspekten der Administration und der Wirtschaftlichkeit wo immer möglich Einzelplatzlizenzen vorzuziehen.

Die Lizensierung von Microsoft-Produkten wird in Zukunft ebenfalls über einen Lizenzserver geschehen. Die Herausgabe von Lizenz-Keys und wird aus diesem Grunde nicht mehr nötig sein. Eine Kompromittierung und dadurch entstehende Folgekosten durch Erneuerung der betroffenen Keys sind damit ausgeschlossen.

3.3.2 Software in der Basisinstallation

Alle Arbeitsplatzrechner werden aktuell mit dem Betriebssystem Microsoft „Windows 7“[3] und vorinstalliertem Microsoft Office 2010 ausgeliefert. Rechner mit früheren Windows- und Office-Versionen können oder sollten bei Bedarf und in Absprache

[3] Der Einsatz anderer Arbeitsplatzrechner und Betriebssysteme (Apple, Linux etc.) sollte nur dann in Erwägung gezogen werden, wenn bestimmte Anwendungsprogramme nur auf diesen Plattformen und nicht unter Intel/Windows zur Verfügung stehen. Keinen Sinn macht es z.B., Windows-basierte Anwendungsprogramme auf einem Apple-Rechner unter Windows in einer virtuellen Maschine oder per Dual-Boot laufen zu lassen.

zwischen Benutzer/in und WISO-IT auf die aktuellen Versionen umgestellt werden. Zur Basisinstallation gehört z.Zt. ferner die nachfolgend aufgelistete Software[4].

Hersteller	Anwendung	Bereich
7-Zip	7-Zip	Datenkompression
Adobe	Flash	Web
Adobe	Adobe Reader 9	Büroanwendung
Gimp	Gimp	Grafik
Heinz	FreePDF	Büroanwendung
McAfee	VirusScan Enterprise	Sicherheit
Microsoft	Office 2010	Büroanwendung
Mozilla	Firefox	Web
OpenOffice.Org	OpenOffice	Büroanwendung
Swiss Academic	Citavi	Literaturverwaltung

3.3.3 Erweitertes Softwareportfolio

Neben der Software, die auf allen Arbeitsplatzrechnern eingesetzt wird, gibt es auch viele Programme, die nur auf einem Teil der Arbeitsplatzrechner benötigt und verwendet werden. Diese Software soll nach Fertigstellung eines ausreichenden Softwareportfolios im Softwareverteilungsdienst (Beginn SS 2011) nur noch in Ausnahmefällen von Mitarbeitern von WISO-IT vor Ort von Datenträgern installiert werden. Schon bisher konnte Software von WISO-IT-Administratoren über das Netz auf Arbeitsplatzrechner verteilt werden, die einen Bedarf an einem solchen Programm angemeldet hatten.

Ebenfalls zum Sommersemester 2011 kann Software eigenständig durch den Benutzer und ohne Intervention von WISO-IT auf Arbeitsplatzrechnern installiert werden. Hierfür wird ein zentrales Software-Portfolio vorgehalten, in dem sich ausschließlich vorkonfigurierte Installationspakete befinden, die auf automatisierte Installierbarkeit geprüft wurden.

Berechtigte Benutzer/innen können diese Software dann über die Windows-Systemsteuerung ohne administrative Rechte auf ihrem Arbeitsplatzrechner eigenständig nachinstallieren. Dazu wird ihnen eine Liste der verfügbaren Anwendungen angezeigt, die für sie freigeschaltet wurden[5]. Das erweiterte Software-Portfolio enthält momentan die folgende Auswahl häufig verwendeter Programme, darunter auch kostenfreie oder unter Open-Source-Lizenzen veröffentlichte Software.

Hersteller	Software	Lizenz

[4] WiSo-IT überprüft und erweitert die Liste der vorinstallierten Programme kontinuierlich, insbesondere hinsichtlich neuerer Versionen. Wir sammeln auch Anregungen und Wünsche der Benutzer/innen zu weiteren Programmen. Von der Anzahl der potentiellen Nutzer/innen dieser Programme und den Lizenzgegebenheiten hängt es dann u.a. ab, ob sie in die Basisinstallation oder in das Erweiterte Softwareportfolio aufgenommen werden.

[5] Eine Zugriffsbeschränkung auf bestimmte Benutzergruppen wird vor allem bei Programmen mit begrenztem Lizenzvolumen unvermeidlich sein, um dafür Sorge zu tragen, dass diese primär auf den Arbeitsplatzrechnern zu Verfügung stehen, wo sie dienstlich vorrangig benötigt werden.

Adobe	Adobe Acrobat 9	Universitätslizenz
	Creative Suite CS5	Universitätslizenz (Kontingent)
CA INC.	ERwin	Fakultätslizenz (Kontingent)
DATEV	Citrix Client	Fakultätslizenz
Design Science	MathType	Fakultätslizenz (Kontingent)
IDS Scheer	Aris	Fakultätslizenz
MathWorks	MathLab	Universitätslizenz
Microsoft	Project	Fakultätslizenz
	SQL Server	Fakultätslizenz
	Visual Studio	Fakultätslizenz
OpenOffice.Org	OpenOffice	Büroanwendung
Oracle	MySQL	Open-Source (GPL)
Sparx Systems	Enterprise Architect	Fakultätslizenz (Kontingent)
STATA Corp.	STATA	Fakultätslizenz
SPSS	AMOS	Fakultätslizenz
	Clementine	Fakultätslizenz
	SPSS	Fakultätslizenz
Thomson Reuters	Datastream	Fakultätslizenz
	Endnote	Universitätslizenz
Verbi	MaxQDA	Fakultätslizenz (Kontingent)
WinEdit	WinEdt	Fakultätslizenz (Kontingent)
Wolfram Research	Mathematica	Universitätslizenz
QMS	EViews	Fakultätslizenz

Die in der vorstehenden Tabelle aufgeführte Software steht nur für Arbeitsplatzrechner zur Verfügung, die in die WISO-Domäne integriert sind. Domänenfremde Arbeitsplatzrechner müssen anderweitig mit Einzelplatzlizenzen für Software versorgt werden, wofür die nutzende Kostenstelle u.U. belastet wird.

Zug um Zug werden alle Programme über das Software-Portfolio zur Verfügung gestellt, soweit dies von den Lizenzbestimmungen und von den Installationsmedien her ermöglicht wird. Durch die benutzerinitiierte Installation sollen die Arbeitsplatzrechner zeitgemäß und individuell mit Software bestückt werden.

3.3.4 Vor Ort installierte Software

Trotz aller Bemühungen, Software über das Netz zu installieren, wird es auch in Zukunft Anwendungen geben, die nur durch Mitarbeiter von WISO-IT vor Ort installiert werden können, da für einige Produkte nur eine begrenzte Anzahl an Einzelplatzlizenzen zur Verfügung steht.

3.4 Beschaffungswesen

3.4.1 Bedarfsanmeldung und Finanzierung

3.4.1.1 Jährliche IuK-Beschaffung

IT-Ersatzbedarfe und vorhersehbare neue IT-Bedarfe werden im Rahmen des jährlichen IuK-Verfahrens der Universität erhoben, sobald der RRZ-Direktor hierzu auffordert. Dies geschah bisher Anfang des Kalenderjahres und soll zukünftig auf das Ende des Vorjahres vorgezogen werden. Da dieses Verfahren nur einmal jährlich durchgeführt wird, ist es ratsam, im Rahmen der Ihnen aus den Vorjahren bekannten fakultären Bedarfserhebungen die im folgenden Jahr entstehenden Bedarfe vorausschauend mit aufzunehmen. WISO-IT fasst die Einzelanträge der Professuren und sonstigen Kostenstellen zu einem IuK-Antrag der Fakultät zusammen. Die Entscheidung über die Bewilligung liegt bei der IuK-Haushaltskommission der Universität.

3.4.1.2 Unterjährige IuK-Beschaffung (Berufungen, Drittmittelprojekte)

In die jährliche IuK-Planung nicht einbezogene IT-Bedarfe „on the fly“ zu befriedigen, ist nur dann möglich, wenn sie dringlich, aber nicht vorhersehbar sind. Hierzu zählen vor allem IT-Beschaffungen im Rahmen von Berufungsverhandlungen sowie für Drittmittelprojekte, für die die Universität sehr häufig die IT-Ausstattung vorhalten muss. Dekanat und FIO sind bemüht, der IuK-Haushaltskommission eine grobe Abschätzung der im Planungsjahr durch Berufungen und Drittmittelprojekte möglicherweise entstehenden IT-Kosten als „Hausnummer“ zukommen zu lassen. Angesichts der für beide Vorgänge typischen Unsicherheiten (Ausgang von Berufungsverfahren, Bewilligung von Drittmittelprojekten) kann es sich dabei nur um eine grobe Abschätzung handeln.

Da die Fakultät hierfür keine pauschale Zuweisung von IT-Mitteln erhält, sind Einzelanträge unerlässlich. Einzelheiten des Verfahrens werden vom Dekanat gesondert festgelegt und bekannt gemacht.

3.4.2 Beschaffungsvorgang

Alle IT-Beschaffungen, auch geringfügige, aus den Sachmitteln einer Kostenstelle getätigte Beschaffungen (z.B. von PDA’s), müssen über WISO-IT abgewickelt werden (it-beschaffung@wiso.uni-hamburg.de). Nur so kann eine Einpassung in die IT-Planung der Fakultät und die im Abschnitt 3.1 beschriebene Standardisierung gewährleistet werden. Beschaffungen, die nicht über WISO-IT veranlasst werden, sind nach einem Dekanatsbeschluss vom 01.12.2010 privat zu begleichen, wobei die eigene Kostenstelle nicht unter „privat“ fällt.

Die Beschaffung von Software wird grundsätzlich genauso gehandhabt wie die Beschaffung von Geräten. Vor der Beschaffung wird geprüft, welche Lizenzmodelle angeboten werden und ob bereits Lizenzabkommen für die Universität oder die Stadt Hamburg vorliegen. In der Regel dauert der Beschaffungsvorgang 2 bis 4 Wochen. Die Software wird anschließend innerhalb einer Woche bereitgestellt. Einige Hersteller bieten Testlizenzen an, so dass bereits während der Beschaffungsphase mit dem Bereitstellungsprozess begonnen werden kann.

4 Basisdienste

4.1 E-Mail und Groupware

WISO-IT betreibt einen E-Mail-Server für die Domäne „wiso.uni-hamburg.de“. Als Plattform kommt der Microsoft Exchange Server 2010 zum Einsatz, der neben den üblichen Funktionen zum Lesen und Versenden von E-Mails auch die Zusammenarbeit in Gruppen unterstützt. So können z.B. für eine Professur gemeinsame Kalender eingerichtet und verwaltet werden, Aufgaben zugewiesen und Verteilerlisten gepflegt werden.

4.1.1 E-Mail-Adresse

Alle Mitglieder der Fakultät erhalten automatisch mit der Einrichtung eines Benutzerkontos auch eine E-Mail-Adresse vorname.nachname@wiso.uni-hamburg.de. Standardisierte E-Mail-Adressen sind heute selbstverständliche Elemente einer corporate identity. Mit „@wiso.uni-hamburg.de“ wird die Zugehörigkeit zur Universität und zur WISO-Fakultät sichtbar gemacht. E-Mails können sowohl aus dem lokalen Netz der Fakultät als auch von außerhalb abgerufen werden. Auf den Standardarbeitsplatzsystemen ist als E-Mail-Programm Microsoft Outlook vorinstalliert, das sich innerhalb der Domäne selbstständig konfiguriert. Neben der Microsoft Exchange-Schnittstelle, die von Outlook und kompatiblen Anwendungen genutzt wird, steht auch eine IMAP-Schnittstelle zum Abruf von E-Mails bereit. Dadurch können Sie Ihre E-Mails auch mit anderen E-Mail-Programmen und mit einem Smartphone abrufen. Zudem erlaubt die Weboberfläche „Outlook Web Access“ (OWA) weltweit das Abrufen Ihrer E-Mails, Kontakte und Termine mit einem Internet Browser (Internet Explorer, Mozilla Firefox, Apple Safari u.a.), wenn auch nicht ganz so komfortabel wie mit Outlook selbst.

4.1.2 Speicherplatz für E-Mails

Da die Sicherung aller E-Mail-Konten sehr viel Speicherplatz beansprucht, wird der laufende Speicherplatz für ein E-Mail-Konto auf 1 Gigabyte begrenzt. Es empfiehlt sich, ältere E-Mails von Zeit zu Zeit zu löschen. Um E-Mails langfristig aufzubewahren, werden voraussichtlich ab Wintersemester 2011 spezielle Archivpostfächer zur Verfügung stehen, die WISO-IT bei Bedarf einrichtet. Diese Postfächer sind per Outlook und OWA von jedem Arbeitsplatz einer Benutzerin oder eines Benutzers bequem durchsuchbar, da sie serverseitig indiziert werden. Die Outlook-Datei archiv.pst wird damit überflüssig.

4.1.3 Verteilerlisten

Auf dem Exchange Server werden zentrale öffentliche Verteilerlisten geführt, unter anderem für die verschiedenen Statusgruppen, Gremienangehörige oder einzelne Arbeitsbereiche (Professuren, Abteilungen der Fakultätsverwaltung u.dgl.). Falls Sie eine für Sie passende und für mehrere Anwender nützliche Verteilerliste vermissen, können Sie bei WISO-IT deren Einrichtung beantragen. Ferner können Sie sich in Outlook nur für Ihren persönlichen Gebrauch bestimmte Verteilerlisten einrichten, die in Outlook 2010 als Kontaktgruppen bezeichnet werden.

4.2 Content Management System

Die Webseiten der Fakultät Wirtschafts- und Sozialwissenschaften werden mit dem Content Management System TYPO3 bereitgestellt. Die Pflege der Webseiten liegt im Verantwortungsbereich der Nutzerinnen und Nutzer. WISO-IT steht Ihnen beratend zur Seite, wenn Sie technische Probleme mit dem Aufbau oder der Pflege Ihrer

Webseiten haben. Um den Einstieg zu vereinfachen, werden regelmäßig Schulungen für Anfänger und für Fortgeschrittene angeboten.

4.3 Kollaborationssysteme

Während Exchange / Outlook die Zusammenarbeit vor allem via E-Mail-Kommunikation und bei der Terminplanung und Aufgabenverteilung unterstützt, bieten Kollaborationssysteme eine umfassendere Funktionalität. In der WISO-Fakultät sind zwei Systeme im Einsatz, die in diese Kategorie fallen.

4.3.1 SharePoint

Für die Koordination der Arbeit von Projekten und Arbeitsgruppen betreibt WISO-IT einen Microsoft Office SharePoint-Server, der das Einrichten von gemeinsamen Dokumentenbibliotheken, Wiki-Seiten oder Foren unterstützt. Zudem ist SharePoint eng mit in allen Office-Produkten verzahnt, so dass diese Funktionen nahtlos aus Word, Excel oder Outlook genutzt werden können. Gemeinsam genutzte Dokumente können direkt aus SharePoint bearbeitet werden und unterliegen einer Versionskontrolle. Dadurch können vorherige Versionen einer Datei geladen und mit dem aktuellen Versionsstand verglichen werden. WISO-IT berät sie bei geplanten SharePoint-Projekten und hilft bei der Einführung in Ihrem Arbeitsbereich.

4.3.2 WISO-CommSy

Vor allem zur Unterstützung von E-Learning-Prozessen betreibt das Regionale Rechenzentrum die Plattform CommSy, auf der der WISO-Ableger WISO-CommSy aufsetzt. Hierzu liegt die Beratung beim E-Learning-Büro unserer Fakultät.

5 Dateiablage

Unabhängig davon, wo Daten wie im Folgenden beschrieben gespeichert werden, wird betont, dass dabei gegen keine rechtlichen Vorschriften verstoßen werden darf.

5.1 Datenspeicherung auf Servern

Das WISO-NET bietet Benutzern/innen und Benutzergruppen die Möglichkeit, Dateien zentral auf einem Dateiserver im Netz abzulegen (sog. Homeverzeichnisse). Diese Netzlaufwerke werden durch redundante Datenspeicher bereitgestellt, die eine hohe Ausfallsicherheit aufweisen und die täglich auf Bandlaufwerken gesichert werden. Die Bänder werden außerhalb des Gebäudes aufbewahrt, um bei einem Feuer- oder Wasserschaden keinen Totalverlust zu erleiden.

Durch die Datenspeicherung auf Netzlaufwerken können einzelne Verzeichnisse für bestimmte Personengruppen freigegeben werden. So kann etwa eine Professur oder ein sonstiger Arbeitsbereich auf ein zentrales Laufwerk zugreifen und gemeinsame Daten dort für ihre Mitarbeiter/innen ablegen. Bestimmte Verzeichnisse auf einem Netzlaufwerk können zudem für andere Benutzer/innen und Benutzergruppen explizit gegen Zugriffe gesperrt werden.

Durch die netzbasierte Ablage von Dateien erhöht sich zusätzlich die Ausfallsicherheit. Sollte ein Arbeitsplatzrechner aufgrund eines Hardware- oder Softwaredefekts ausfallen, kann ein Ersatzgerät bereitgestellt werden. Da die Daten dann nicht auf dem defekten Arbeitsplatzrechner liegen, kann auf einem anderen Rechner des Arbeitsbereichs oder nach Bereitstellung eines Ersatzrechners zumindest mit der Software der Basisinstallation (vgl. Abschnitt 3.3.2) sofort weitergearbeitet werden.

5.1.1 Persönlicher Ordner (Laufwerk Z:)

Jeder Benutzer im WISO-NET hat auf dem Dateiserver ein persönliches Laufwerk, auf das nur der berechtigte Hauptbenutzer zugreifen darf[6]. Diese Laufwerke haben zunächst keine Größenbeschränkung.

Auf diese Daten können im Gegensatz zu den auf der lokalen Festplatte gespeicherten Daten die lokalen Administratoren des Rechners nicht zugreifen. Deshalb sind sensible Daten wie Klausuraufgaben und Gutachten im persönlichen Netzwerkordner besser aufgehoben als auf der lokalen Festplatte oder auf einem USB-Stick. Allerdings dürfen Ordner in Netzlaufwerken nicht verschlüsselt werden, da sie sonst nicht gesichert werden können. Auch muss das standardmäßige Zugriffsrecht für die Datensicherung[7] erhalten bleiben, da ohne dieses Recht eine regelmäßige, automatisierte Sicherung der Daten nicht möglich ist.

5.1.2 Gemeinsame Ordner (Laufwerk N:)

Um Dateien mit mehreren Benutzern bearbeiten zu können, werden im Laufwerk N: gemeinsame Ordner bereitgestellt. Dort befinden sich die Ordner, auf die Benutzer, je nach Gruppenzugehörigkeit, lesend und /oder schreibend gemeinsam zugreifen können. Im Ordner „Arbeitsbereiche“ sind zum Beispiel alle Ordner nur für die Mitglieder des entsprechenden Arbeitsbereichs sichtbar und zugänglich.

5.2 Datenspeicherung auf lokalen Festplatten

Selbstverständlich können Sie Ihre Daten teilweise oder gänzlich auch auf der lokalen Festplatte Ihres Arbeitsplatzrechners speichern. Die Vor- und Nachteile gegenüber einer Speicherung in Ihrem Homeverzeichnis auf dem Dateiserver sollten Sie genau abwägen. Die folgenden Aspekte sollte man dabei bedenken.

Auf dem Dateiserver gespeicherte Daten werden automatisch gesichert. Die Sicherung von Daten auf der lokalen Festplatte müssen Sie hingegen eigenständig betreiben und verantworten. Erfahrungsgemäß vertieft sich das Verständnis für eine zuverlässige Datensicherung nach dem ersten massiven Datenverlust. Auf der lokalen Festplatte eines Laptops gespeicherte Daten sind bei einem Plattendefekt, einem Diebstahl oder bei einem sonstigen Verlust mehrfach gefährdet. Wenn die Daten nicht gesichert wurden, können sie für den zugriffsberechtigten Benutzer unwiederbringlich verloren oder u.U. nur sehr aufwändig und zu hohen Kosten restaurierbar sein. Wenn die Daten nicht geeignet verschlüsselt wurden, können sie auch für nicht zugriffsberechtigte Benutzer zugänglich sein. Auch die Diskussion um die (personenunabhängige) Archivierungspflicht von Forschungsergebnissen spricht eher für eine serverbasierte Datenablage.

Dateien auf lokalen Festplatten können von Benutzer/innen mit lokalen Administrationsrechten[8] eingesehen, kopiert und gelöscht werden. Zu diesem Personenkreis

---

[6] Die Systemadministratoren von WiSo-IT können wie in anderen Organisationen auch auf alle IT-Ressourcen zugreifen. Dazu gehören die Studentischen Mitarbeiter von WiSo-IT nicht.

[7] Die Datensicherung ist ein systemseitiges Dienstkonto, das nur von WiSo-IT-Systemadministratoren bedient wird. Das „Leserecht“ der Systemadministratoren meint die Berechtigung zum lesenden Zugriff im Rahmen automatisierter Prozesse wie der Datensicherung. Nicht gemeint ist damit eine Berechtigung, z.B. die dort gespeicherte dienstliche Korrespondenz, Forschungsanträge, Gutachten o.dgl. „zu lesen“. Der Unterschied ergibt sich aus der Zweckbindung aller Tätigkeiten von Systemadministratoren.

[8] Lokale Administrationsrechte beschränken sich nur auf den jeweiligen Arbeitsplatzrechner und gewähren keine Administrationsrechte in der WiSo-Domäne.

gehören auch die Studentischen Mitarbeiter/innen von WISO-IT und Mitarbeiter externer, mit Wartungsaufgaben betrauter Firmen. Wenn Sie dennoch Daten auf der lokalen Festplatte speichern, sollten sie zumindest sensible Daten verschlüsseln.

Denken Sie daran, dass Sie Ihren Rechner bei Wartungsarbeiten aus der Hand geben. Das trifft auf Daten, die auf Ihrem persönlichen Serverlaufwerk (vgl. Abschnitt 5.1.1) gespeichert werden, nicht zu, auch nicht auf deren im Zuge der Offline-Synchronisation lokal abgelegte Kopien (vgl. Abschnitt 5.3).

Lokal gespeicherte Daten können Sie dann „unter Ihrer Kontrolle“ behalten, wenn Sie diese auf einer externen USB-Festplatte oder einem anderen externen Speichermedium (z.B. USB-Stick) speichern. Auch hier gilt, dass zumindest sensible Daten verschlüsselt werden sollten. Wegen des Risikos, solche Datenträger zu verlieren, und da solche Datenträger in keine automatisierte Datensicherung integriert sind, ist hiervon i.d.R. aber abzuraten.

5.3 Offline- Synchronisation servergespeicherter Daten

Auf den Netzlaufwerken gespeicherte Daten sind nicht nur am universitären Arbeitsplatz, sondern auch von außerhalb über eine VPN-Verbindung sicher zugreifbar. Auch bei fehlendem Zugang zum Internet oder bei einer Störung des VPN-Zugangs kann mit Dateien, die auf den Netzlaufwerken gespeichert sind, weiter gearbeitet werden, wenn Sie für den Ordner des Netzwerklaufwerks, in dem diese Dateien liegen, eine Offline-Synchronisation eingerichtet haben. Bei fehlendem Zugang zum Netzwerklaufwerk arbeiten Sie dann zwischenzeitlich mit einer Kopie dieser Dateien auf der lokalen Festplatte weiter. Bei der nächsten Verbindung mit dem Netzlaufwerk werden diese Dateien wieder synchronisiert. Die Offline-Synchronisation ist vor allem für das mobile Arbeiten mit Laptops und Smartphones außerhalb des WISO-NET sehr hilfreich.

Diese lokalen Kopien sind unter anderen Benutzerkonten nicht einsehbar, auch nicht unter den lokalen Administratorkonten.

6 IT-Sicherheit

In der WISO-Domäne werden Benutzer/innen und Arbeitsplatzsysteme zentral verwaltet, Aktualisierungen des Betriebssystems und der Anwendungssoftware werden auf den Arbeitsplatzrechnern automatisch über das Netz installiert[9].

6.1 Active Directory und Benutzerverwaltung

Die Benutzerverwaltung wird über das Microsoft Active Directory realisiert. Das Active Directory ist ein Verzeichnisdienst, das ähnlich wie ein Telefonbuch Einträge für Benutzer, Gruppen, Computer und andere Objekte hierarchisch geordnet verwaltet. An oberster Stelle dieser Hierarchie steht die WISO-Domäne. Unterhalb der Domäne wird mit Hilfe von Organisationseinheiten (Fachbereiche, Verwaltung) die Fakultätsstruktur abgebildet. Benutzer/innen und Computer werden in dieser Struktur der entsprechenden Organisationseinheit zugeordnet.

In den Benutzerkonten des Active Directory können weitere Informationen wie die Büroanschrift und die Telefonnummer gepflegt werden. Diese Informationen wer-

[9] Die Erfassung der IT-Geräte im Active Directory der WiSo-Domäne ermöglicht aktuelle Bestandsübersichten ohne lästige Nachfragen bei den Benutzern/innen, welche Rechner sie verwenden, und ohne aufwändige Inventarisierung durch Begehung der Dienstzimmer.

den für das Adressbuch und das Telefonbuch auf den Webseiten der Fakultät verwendet und müssen dort nicht händisch aktualisiert werden.

Auch die Authentifizierung beim Zugriff auf die IT-Ressourcen und -Dienste erfolgen über das Active Directory. Bei der Anmeldung an einem Computer müssen der Benutzername und das Kennwort eingegeben werden. Dadurch authentifiziert sich der Benutzer am System. Bei der Autorisierung wird geprüft, ob er/sie auf eine bestimmte IT-Ressource zugreifen darf. Die Authentifizierung und Autorisierung greift nicht nur beim Zugriff auf Netzwerk-Ressourcen und Dienste, sondern auch auf der Ebene des Arbeitsplatzsystems selbst.

Damit ein unbefugter Zugriff auf ein Benutzerkonto unterbunden werden kann, muss das Kennwort ein gewisses Maß an Komplexität aufweisen. Dazu sind vom Bundesamt für Sicherheit in der Informationstechnik[10] Kriterien vorgegeben. Ein Kennwort in der WISO-Domäne

- darf weder wesentliche Teile des Kontonamens des Benutzers noch den vollständigen Kontonamen enthalten,
- muss mindestens acht Zeichen lang sein,
- darf nicht identisch mit den letzten 24 Kennwörtern sein und
- muss Zeichen aus drei der vier folgenden Kategorien enthalten:
  - Großbuchstaben von A bis Z
  - Kleinbuchstaben von A bis Z
  - Ziffern der Basis 10 (0 bis 9)
  - Andere als alphabetische Zeichen (z. B. !, $, #, %)

Darüber hinaus darf Ihr persönliches Kennwort keinen Dritten zugänglich gemacht werden. Ein Benutzerkennwort ist maximal 90 Tage lang gültig[11]. Wird das Kennwort nicht innerhalb der 90 Tage neu gesetzt, erzwingt Windows die Änderung des Kennwortes während der Anmeldung. Die Anmeldung an Outlook Web Access ist mit einem abgelaufenen Kennwort nicht möglich! Erkennt der Verzeichnisdienst fünf ungültige Anmeldeversuche innerhalb von 15 Minuten, wird das Benutzerkonto automatisch für 15 Minuten gesperrt.

Kennwörter von Benutzerkonten werden bisher nur nach Vorlage eines offiziellen Ausweisdokuments durch Systemadministratoren/innen zurückgesetzt[12]. Eine technische Lösung zum selbsttätigen Zurücksetzen der Kennwörter durch die Benutzerinnen und Benutzer wird evaluiert.

Ein neues Benutzerkonto kann formlos durch den/die Kostellenverantwortliche/n bei WISO-IT beantragt werden. Bevor das Kennwort ausgegeben wird, muss die Mitarbeiterin oder der Mitarbeiter einmalig ein offizielles Ausweisdokument bei WISO-IT vorlegen.

Benutzerkonten werden auf die Dauer der Fakultätszugehörigkeit befristet angelegt. Danach läuft das Benutzerkonto ab. Grundsätzlich werden alle Daten der Benutzerinnen und Benutzer von der regelmäßig durchgeführten Datensicherung erfasst. Die dauerhafte Verwahrung von Daten nach Beendigung des Arbeitsverhältnisses

---

[10] Vgl. Bundesamt für Sicherheit der Informationstechnik: IT-Grundschutz-Kataloge, M 4.48 Passwortschutz unter NT-basierten Windows-Systemen.

[11] Vgl. Richtlinie zur Verwaltung von Passwörtern, IT-Handbuch für die Verwaltung der Freien und Hansestadt Hamburg, 01.10.2003 http://www.rrz.uni-hamburg.de/uploads/media/Passwortrichtlinie.pdf

[12] Aus Sicherheitsgründen können die WISO-IT-Support-Mitarbeiter/innen keine Kennwörter des Fakultätspersonals setzen.

wird sich nach der Archivierungsrichtlinie der Universität Hamburg richten, die aber gegenwärtig noch nicht vorliegt.

6.2 Rechte der Anwender/innen auf Arbeitsplatzrechnern

Da Systemsicherheit und Netzintegrität innerhalb der WISO-Domäne hohe Priorität genießen, müssen die Administrationsrechte auf den Arbeitsplatzsystemen restriktiv gehandhabt werden.

Die Vernetzung von Systemen erlaubt das kooperative Arbeiten, den gemeinsamen Zugriff auf Dateien oder die Verwendung von Druckern über das Netzwerk. Mit jedem von WISO-IT angebotenen Dienst steigt auch die Gefahr eines Angriffs oder Missbrauchs. Daher stehen aus administrativer Perspektive die Sicherheit und die Integrität aller Systeme und der Netzinfrastruktur im Vordergrund. Dies lässt sich jedoch nur realisieren, wenn Benutzer mit minimal notwendigen Rechten arbeiten und der nicht autorisierte Zugriff auf Dienste und Ressourcen unterbunden werden kann.

Ein ungeschütztes System gefährdet nicht nur dessen eigene Funktionsfähigkeit[13] sowie andere in der WISO-Domäne befindliche Geräte, sondern bietet Schadprogrammen wie Viren, Würmern und Trojanern potentielle Angriffsmöglichkeiten auf die gesamte Infrastruktur. Daher werden die Arbeitsplatzgeräte innerhalb der Domäne zentral verwaltet und Software-Aktualisierungen an die Arbeitsplatzrechner verteilt. In Kombination mit einem aktuellen Antiviren-Programm gewährt dies einen nach dem Stand der Technik weitgehenden Schutz der Daten, der Integrität der Rechner und der Sicherheit in der gesamten WISO-Domäne. Deshalb ist es wichtig, möglichst viele Programme in das zentrale Softwaremanagement von WISO-IT aufzunehmen.

6.2.1 Grundsatz minimaler Rechte für Anwender/innen

Wenn Benutzer/innen mit administrativen Berechtigungen arbeiten, können sie z.B. Dateien in den Systemverzeichnissen und die Grundkonfiguration des Rechners verändern. Dies führt zu einem erheblichen Mehraufwand bei der Behebung von Problemen mit dem Betriebssystem oder den darauf installierten Anwendungen. Es lässt sich beispielsweise nicht nachvollziehen, welche Änderungen am System durchgeführt wurden oder welches Programm Probleme hervorruft. Schadsoftware (Viren, Würmer oder Trojaner) kann so vollständigen Zugriff auf den Rechner erhalten. Solche Rechner sind nicht mehr wirtschaftlich und in angemessener Zeit wartbar und sollten in einer integrierten IT-Infrastruktur nicht betrieben werden. Deshalb dürfen auch Privat-Computer nicht in die WISO-Domäne integriert werden[14]. Mit einem nicht von WISO-IT ausgelieferten Rechner[15] kann man sich deshalb in der WISO-Domäne nicht anmelden, weder in der Universität noch von zu Hause über den VPN-Zugang. Auf diesem Weg kann nur über Internetzugänge auf WISO-IT-

---

[13] Dass Rechner mit Administrationsrechten des Anwenders gefährdeter sind als andere, hat sich gerade jüngst wieder durch eine Virenbefall gezeigt, dessen fehlgeschlagene Beseitigung durch den/die Anwender/in zu einem erheblichen Supportaufwand bei WiSo-IT geführt hat.

[14] Die Betriebsregelungen für die WiSo-Domäne sind in einigen Aspekten restriktiver als die derzeitigen Vorgaben des RRZ der UHH, z.B. hinsichtlich des Betriebs privater Notebooks im Hochschulnetz.

[15] Hierbei kann es sich um einen privaten oder einen sonstigen Rechner in der Regie Dritter handeln.

Dienste zugegriffen werden. Mit einem WISO-IT-Laptop stehen hingegen auch von außen per VPN alle Dienste der WISO-Domäne zur Verfügung.

Die Windows-Oberfläche des Arbeitsplatzrechners kann auch ohne lokale Administrationsrechte an die Benutzerwünsche angepasst werden. Das gilt auch für die Einstellungsoptionen der jeweiligen Anwendungsprogramme. Ohne administrative Rechte können Benutzer/innen allerdings keine Dateien in den Systemverzeichnissen verändern. Es können nur die Teile des Systems angepasst werden, für die der Benutzer keine erhöhten Rechte braucht. In der Regel führt dies zu keinen größeren Einschränkungen, verhindert aber zum Beispiel die Installation von neuen Anwendungen und Treibern.

6.2.2 Spezielle Aspekte des Arbeitens ohne lokale Administrationsrechte

In den folgenden Unterabschnitten werden einige spezielle Probleme beleuchtet, die das Arbeiten auf einem Arbeitsplatzrechner ohne lokale Administrationsrechte hervorrufen kann, für die WISO-IT aber automatisierte Lösungen entwickelt hat bzw. anstrebt. Sollte eines dieser Probleme oder ein anderes, hier nicht erwähntes bei Ihnen auftreten, so informieren Sie bitte unverzüglich den 1st-Level-Support (vgl. Abschnitt 7.1).

6.2.2.1 Einspielen von Patches und Updates

Updates und Patches müssen vor allem dann zwingend eingespielt werden, wenn Sicherheitslücken in installierten Programmen oder im Betriebssystem – vor allem durch Internetzugriffe – geschlossen werden müssen. Für die meisten auf den Rechnern installierten Programme erledigt WISO-IT das durch Prozesse, die ohne administrative Rechte der Benutzer/innen „im Hintergrund“ ablaufen.

Insbesondere bei sehr komplexen Anwendungsprogrammen kann die geeignete Softwareaktualisierungsstrategie nur in Kooperation mit speziell dafür zuständigen Mitarbeitern/innen der diese Software nutzenden Professuren erarbeitet werden.

6.2.2.2 Nachinstallation zusätzlicher Software

Die Installation zusätzlicher Programme aus dem erweiterten Software-Portfolio stoßen Sie wie im Abschnitt 3.3.3 beschrieben selbst an. Der Installationsprozess läuft im Hintergrund mit den dafür notwendigen Berechtigungen, ohne dass der Benutzer diese Rechte bräuchte.

6.2.2.3 Drucken auf anderen als WISO-NET-Netzwerkdruckern

Wie im Abschnitt 3.2.2 beschrieben sind die Drucker in der WISO-Domäne als Netzwerkdrucker und nicht als lokale Drucker konfiguriert, auch dann, wenn sie in Ihrem Büro stehen. Für diese Drucker sind die Druckertreiber mit vorinstalliert.

Sobald Sie außerhalb der WISO-Domäne, z.B. zu Hause, einen anderen Drucker an Ihren WISO-IT-Laptop anschließen wollen, für den im installierten Betriebssystem kein Druckertreiber vorgehalten wird, muss dieser von WISO-IT nachinstalliert werden. Wenden Sie sich dazu bitte an den First-Level-Support (vgl. Abschnitt 7.1).

6.2.3 IT-Umgebung mit erweiterten Rechten („Sandbox“)

Ein restriktives Betriebskonzept, wie es für Unternehmen und Behörden heute üblich ist oder sein sollte, kann nicht allen Anforderungen aus Forschung und Lehre, die sich aus der in Art. 5 (3) GG garantierten Wissenschaftsfreiheit begründet ablei-

ten lassen[16], umstandslos Rechnung tragen. Hierfür braucht es flexiblere Lösungen, die die IT-Sicherheit aber möglichst wenig beeinträchtigen.

Ein von WISO-IT verfolgter Ansatz ist die Bereitstellung einer „Sandbox“ als ein von der WISO-Domäne abgeschotteter Bereich. In einer solchen Sandbox könnten auch Dienste und Anwendungen betrieben werden, die ansonsten die Netzsicherheit gefährden könnten. Dazu gehören z.B. Trial-Versionen von bisher nicht vorgehaltener und geprüfter Software, die auf ihre Nützlichkeit für Lehre und Forschung getestet werden sollen[17]. Für eine solches erstes „Ausprobieren“ ist eine Einbindung in die WISO-Domäne zunächst nicht erforderlich.

Um die Sandbox bereit zu stellen, wird auf die Virtualisierungsumgebung zurückgegriffen, auf der bereits jetzt ein Teil der WISO-IT-Dienste laufen. Aufgrund der Vielzahl an technischen Möglichkeiten testet WISO-IT mehrere Varianten von Sandbox-Lösungen. Dabei wird derzeit eine Lösung favorisiert, die auf folgendem Prinzip beruht. Die Sandbox für die Arbeitsplatzrechner wird als mobiler Client auf dem jeweiligen Arbeitsplatzrechner ausgeführt. Der Host ist das Arbeitsplatzrechner-Betriebssystem, das gemäß dem Sicherheitskonzept der WISO-Domäne ausgeführt wird. Der Sandbox-PC ist eine virtuelle Umgebung, die Ressourcen des Hosts nutzt (CD/DVD-Laufwerk, Netzwerk für Internetzugang) aber in einer eigenen „offenen“ Sicherheitsumgebung läuft. Die einzigen Sicherheitsmechanismen, welche innerhalb dieser Sandbox laufen müssen, sind ein Antiviren-System und Routing-Einstellungen, die verhindern, dass das Sandboxsystem ungeschützt auf Ressourcen der WISO-Domäne zugreifen kann.

Die Benutzerin bzw. der Benutzer bekommt aus einer Server-gespeicherten Vorlage ein fertiges vorkonfiguriertes Windows-System gestellt, in dem er bzw. sie bis auf die Antiviren-Software und die Routing-Einstellungen vollständigen administrativen Zugriff hat. Die Installation von Anwendungen kann im Netzwerkbetrieb wie auch mobil erfolgen, da das Sandbox-System auf der Workstation des Benutzers zwischengespeichert wird. Der Zugriff auf Installationsmedien erfolgt über das CD/DVD-Laufwerk oder über einen gemeinsamen Ordner des Hostbetriebssystems in der Sandbox. Weitere Zugriffe auf Netzwerkressourcen hat die Sandbox nicht. Ausgenommen davon ist die Nutzung des Internets, das auf der Sandbox freigeschaltet wird, um Updates oder den Download von Software zum Testen zu ermöglichen.

Da die Sandbox die Sicherheit des Hosts (außer bei mutwilligem Missbrauch) kaum beeinträchtigt, kann sie grundsätzlich allen Benutzerinnen und Benutzern zur Verfügung gestellt und empfohlen werden.

6.2.4 Vergabe lokaler Administrationsrechte

Die Sandbox-Lösung ist einerseits relativ sicher und deshalb breit einsetzbar, andererseits ist sie mehr eine experimentelle Umgebung als ein Lösung für etablierte Applikationen im Softwareportfolie der WISO-Domäne, die gleichwohl für bestimmte Benutzerinnen und Benutzer erweiterte Rechte erforderlich machen, z.B. bei der

---

[16] Hier und da gibt es allerdings überzogene Vorstellungen von vermeintlichen IT-Ansprüchen nach Art. 5 (3) GG. So gibt es z.B. weder ein Grundrecht auf einen PC eines bestimmten Herstellers noch auf eine bestimmte Groupware-Lösung. Das hätte eine jeder Standardisierung zuwider laufende Heterogenität zur Folge. Letztlich ist es Sache des für die Bewirtschaftung zuständigen Dekanats, die Nutzung einer vorgegebenen IT nach dem Gebot der Sparsamkeit und Wirtschaftlichkeit zu bestimmen (Rechtsauskunft der Präsidialverwaltung vom 30.11.2010).

[17] Die jeweiligen Lizenzbedingungen sind auch hier zu beachten.

Administration von Datenbanksystemen oder Entwicklungsumgebungen, die ihrerseits Administrationsrechte auf dem Betriebssystem des Arbeitsplatzrechners oder eines Applikationsservers (lokale Administrationsrechte) erzwingt. In solchen begründeten Fällen, die die Ausnahme und nicht die Regel sind[18], werden lokale Administrationsrechte vergeben, wenn sich die vorstehenden Lösungen als nicht ausreichend praktikabel erweisen.

Dieser aus Sicherheits- und Supportgründen eher enger als weiter zu ziehende Kreis von Wissenschaftler/innen ist auf den sorgfältigen Umgang mit den lokalen Administrationsrechten zu verpflichten. Dazu gehören folgende Vorgaben:

- Die lokalen Administrationsrechte werden nur zur Erledigung dienstlicher Aufgaben in Forschung und Lehre benötigt und verwendet, also z.B. nicht für die Installation von Software für den Privatgebrauch.
- Das erste Testen von Software („Ausprobieren“), bei dem die Funktionalität der Software als solche im Vordergrund steht und die Einbindbarkeit in die WISO-Domäne noch keine Rolle spielt, erfolgt in einer Sandbox (vgl. Abschnitt 6.2.3). Erst wenn diese Tests soweit fortgeschritten sind, dass eine Beschaffungsentscheidung bevorsteht, wird eine solche Software in einer Test-Umgebung der WISO-Domäne oder testweise in der WISO-Domäne selbst installiert. Dies erfolgt durch oder in Abstimmung mit WISO-IT.
- Das lokale Administratorkonto wird nur für die unter dem normalen Domänenkonto des Benutzers bzw. der Benutzerin nicht durchführbaren administrativen Aufgaben verwendet, nicht für die sonstigen alltäglichen IT-Aufgaben.
- Deshalb dürfen die lokale Administrationsrechte auch nicht auf das Domänen-Konto des Benutzers übertragen werden.
- Für den Support selbstadministrierter Rechner sind primär deren Benutzerinnen und Benutzern selbst zuständig.
- Sobald und sofern WISO-IT andere technische Lösungen bereitstellen kann, die einen Verzicht auf lokale Administrationsrechte ermöglichen, wird im Interesse der Sicherheit und wirtschaftlichen Wartbarkeit des gesamten IT-Systems so verfahren. Benutzer und Benutzerinnen informieren WISO-IT über einen Wegfall der Vergabevoraussetzungen für lokale Administrationsrechte von sich aus.

6.2.5 Zusätzliche Sicherheitsfeatures für vertrauliche Daten

Werden vertrauliche Daten auf Festplatten von Arbeitsplatzrechnern, insbesondere von mobilen Computern, oder anderen lokalen Speichermedien gespeichert, sollten diese verschlüsselt werden. Windows 7 bietet auf modernen Computern mit TPM-Sicherheitsmodul[19] die Möglichkeit, die gesamte Festplatte mit Windows BitLocker zu verschlüsseln. Damit sind sämtliche Dateien, die sich auf dem Notebook befinden verschlüsselt. Im Normalbetrieb macht sich die Verschlüsselung kaum bemerkbar, lediglich bei ein- und ausgabeintensiven Programmen wird die Leistung um etwa 5% reduziert.

6.3 Netzsicherheit

Um die Sicherheit des Netzes und der Geräte in der WISO-Domäne sicherzustellen, wird die Netzkommunikation geschützt. Dadurch steht das Arbeitsplatzgerät nicht

---

[18] Eine generelle, technisch und dienstlich nicht notwendige Aufweichung einer sicherheitsorientierten Rechtevergabepolitik wäre nicht vertretbar. Es kann auch nicht im Interesse der Nutzerinnen und Nutzer liegen, den eigenen und womöglich andere Rechner zu gefährden.

[19] Trusted Platform Module

ungeschützt direkt im Internet, sondern hinter einer Schutzwand – der Firewall. Die Firewall filtert die ein- und ausgehende Kommunikation aller Systeme mit dem Internet und schützt so vor unerlaubten Zugriffen. Die Firewall erlaubt zudem das selektive Freigeben bestimmter Kommunikationskanäle, damit zum Beispiel auf Videokonferenzsysteme zugegriffen werden kann, unterbindet jedoch die Zugriffe von außen auf die Arbeitsplatzrechner.

Neben der Firewall wird auf allen Rechnern – Arbeitsplatzrechnern und Servern – eine zentral verwaltete Antiviren-Lösung eingesetzt. Der Virenscanner durchsucht Dateien auf den Servern und Arbeitsplatzrechnern und überprüft mit Hilfe von Signaturen, ob eine Datei mit einem Virus, Wurm oder Trojaner befallen ist. Die Virensignaturen werden mehrmals täglich aktualisiert, auch wenn sich das Gerät nicht im WISO-NET befindet.

Wenn jemand die Festplatte aus dem Computer entfernt und diese auszulesen versucht, benötigt er / sie hierfür den Wiederherstellungsschlüssel, der nur im Active Directory gespeichert wird und nur den Systemadministratoren zugänglich ist.

6.4 Rechte der WISO-IT-Mitarbeiter/innen in der Domäne

Die Vergabe von Zugriffsrechten innerhalb von WISO-IT erfolgt nach dem Need-to-Know-Prinzip[20], d.h. WISO-IT-Mitarbeiter erhalten nur Zugriffsrechte auf Systeme und Daten, die für die jeweilige Aufgabenerfüllung erforderlich sind. Im Folgenden werden die Zugriffrechte grob anhand von Rollen beschrieben, die bei WISO-IT zur Anwendung kommen.

Die Aufgabenverteilung innerhalb von WISO-IT lässt sich in zwei Bereiche trennen: die Unterstützung der Anwender bei der täglichen Arbeit (1st-Level-Support; vgl. Abschnitt 7.1) sowie die Systemadministration, also die Verwaltung, die Wartung und der Betrieb der IT-Infrastruktur (2nd-Level-Support, vgl. Abschnitt 7.2).

Um diese Aufgaben wahrzunehmen, sind unterschiedliche Berechtigungen nötig. Innerhalb einer Domäne wird zwischen domänenweiten und lokalen administrativen Rechten unterschieden. In Windows erhalten alle Benutzer lokale administrative Rechte, die sich in der Gruppe der lokalen Administratoren befinden. Über diese Gruppenmitgliedschaft wird der Zugriff auf alle Ressourcen, Dateien und Einstellungen des Geräts freigegeben. Ein Konto mit domänenweiten administrativen Rechten hat Zugriff auf alle Systemen, die innerhalb der Domäne betrieben werden. Dazu zählen neben allen Servern, die von WISO-IT betrieben werden, auch die Arbeitsplatzsysteme in der WISO-Domäne. Systemadministratoren sind deshalb zugleich Mitglieder der Gruppe der lokalen Administratoren.

Grundsätzlich sind hauptamtliche wie studentische Mitarbeiter der WISO-IT zum vertraulichen Umgang mit Daten und im Rahmen ihrer Arbeitsverträge zur Verschwiegenheit verpflichtet. Studentische Mitarbeiter erhalten im Gegensatz zu hauptamtlichen Mitarbeitern lokale Administrationsrechte nur auf den Arbeitsplatzsystemen, nicht jedoch auf die netzbasierte Datenablage und die Benutzerverwaltung.

Mitarbeiter der WISO-IT, die nicht mit administrativen Aufgaben oder der Anwenderunterstützung betraut sind, arbeiten mit normalen Benutzerrechten.

6.4.1 Systemadministration

Mitarbeiter mit der Rolle „Systemadministration“ verfügen zur Erfüllung ihrer Aufgaben über umfassende Rechte innerhalb der IT-Infrastruktur der Fakultät. Dazu

[20] Vgl. IT-Grundschutzkatalog, M 2.8 Vergabe von Zugriffsrechten, BSI

erhalten sie domänenweite administrative Rechte, hierzu zählen das Ausführen von Anwendungen auf jedem Arbeitsplatzsystem und das Lese-, Schreib- und Modifikationsrecht auf Daten, die auf Server- und Arbeitsplatzsystemen gespeichert sind. Dieses sind die üblichen Aufgaben und Rechte von Systemadministratoren, stellen also keine Besonderheiten der WISO-IT dar.

Aufgrund dieser notwendigen, umfassenden Rechte üben nur hauptamtliche Mitarbeiter diese Rolle aus.

6.4.2 Anwenderunterstützung

Mitarbeiter im 1st-Level-Support erhalten, im Gegensatz zu den Systemadministratoren, keine domänenweiten Administrationsrechte. Da sie jedoch die Wartung der Geräte, die Installation von Software und ähnliche Aufgaben auf den Arbeitsplatzsystemen übernehmen, können sie sich mit einem lokalen Administratorkonto direkt auf dem Gerät anmelden.

Da die Mitarbeiter im 1st-Level-Support keine domänenweiten administrativen Rechte besitzen, können sie nur auf die Ressourcen, Dateien und Einstellungen von Arbeitsplatzsystemen zugreifen und diese verändern. Der Zugriff erfolgt entweder vor Ort oder mit Hilfe von Fernwartungswerkzeugen. Der entfernte Zugriff mit diesen Werkzeugen muss von dem/der Benutzer/in freigegeben und kann von ihm/ihr am Bildschirm mitverfolgt werden. Der 1st-Level-Support wird zu einem erheblichen Teil von studentischen Mitarbeitern geleistet. Um mehr Kontinuität bei der Anwenderunterstützung zu erreichen, setzt WISO-IT verstärkt auch hauptamtliche Mitarbeiter ein, die zudem den Einsatz der studentischen Mitarbeiter koordinieren.

Aufgaben, die zwischen Anwenderunterstützung und Systemadministration liegen, werden nur von hauptamtlichen Mitarbeitern ausgeführt, die domänenweite Administrationsrechte besitzen.

7 Support

WISO-IT ist für Mitglieder der WISO-Domäne der uneingeschränkte Ansprechpartner für alle Belange rund um die IT-Versorgung. Dazu gehören nicht nur die Beschaffung von Geräten und Software, sondern auch Hilfestellungen bei der Arbeit. Um einen zeitgemäßen und an der Vorgabe der Wirtschaftlichkeit orientierten Service anzubieten, werden im direkten Anwendersupport vorrangig nur Geräte betreut, die sich auch in der WISO-Domäne befinden. Support für Geräte außerhalb der WISO-Domäne kann nur nachrangig geleistet werden.

Bei der täglichen Arbeit am Computer treten immer wieder Probleme auf oder es kommt zu Fehlern. Die Hilfestellung erfolgt telefonisch, per E-Mail oder durch Fernwartung, bei der Sie den Mitarbeitern von WISO-IT gezielt Zugriff auf Ihr System geben und dabei am Monitor beobachten können, welche Schritte zur Lösung Ihres Problems ergriffen werden. Zugleich können sie dadurch kontrollieren, dass mit Ihrem Rechner nichts Unstatthaftes geschieht. Von der technisch gegebenen Möglichkeit, Rechner auch bei Nichtbenutzung durch den Anwender hochzufahren und zu warten, vor allem durch nachts ausgeführte automatisierte Verfahren, wird z.Zt. kein Gebrauch gemacht[21].

[21] Eine Änderung dieser Verfahrensweise würde WiSo-IT dem Dekanat zur Entscheidung vorlegen.

7.1 First-Level-Support

Supportanfragen an WISO-IT sind grundsätzlich über das Ticket-System (http://www.wiso.uni-hamburg.de/einrichtungen/wiso-it/support/ticket-system/) und nicht direkt an WISO-IT-Mitarbeiter/innen zu richten, weder per E-Mail noch per Telefon oder persönliches Vorsprechen. Nur so kann gewährleistet und nachgehalten werden, wann Supportanfragen von wem zu welchem Problem gestellt und erledigt wurden. Zudem ist zu bedenken, dass die Support-Kräfte, wenn sie im Hause unterwegs sind, nicht jederzeit erreichbar sind. Ein „Support auf Zuruf“ ist in einer Fakultät unserer Größe nicht organisierbar.

Die hauptamtlichen und studentischen Mitarbeiter/innen des First-Level-Supports liefern Geräte aus, lösen Probleme mit der Hardware, dem Betriebssystem und der Anwendungssoftware und stehen generell bei IT-Fragen als erste Ansprechpartner zur Verfügung.

Um kurze Reaktionszeiten zu ermöglichen, befinden sich in allen größeren Gebäuden der Fakultät Support-Büros:
Allende-Platz 1: 238 (werktags von 8 – 18 Uhr)
Max-Brauer-Allee 60: 118 (montags von 10 – 15 Uhr)
Von-Melle-Park 5: Raum 1009 (werktags von 8 – 18 Uhr)
Von-Melle-Park 9: Raum A 516 (werktags von 8 - 21 Uhr, samstags 10 – 18 Uhr)
Welckerstraße 8: Raum 1.24 (dienstags und donnerstags von 10 – 18 Uhr)
Das Supportbüro im Von-Melle-Park 9, Raum A 516, ist zugleich das zentrale Supportbüro von WISO-IT.

7.2 Second-Level-Support / Administration

Lässt sich ein Problem auf der ersten Ebene nicht lösen, wird es vom First-Level-Support an den Second-Level-Support weitergereicht. Der Second-Level-Support ist für die Administration der IT-Infrastruktur, deren reibungsfreien Betrieb und für die Koordination der Aufgaben zwischen First-Level-Support und Benutzern zuständig. Für ihn sind nur Systemadministratoren von WISO-IT zuständig.

7.3 Beschwerdemanagement

Support-Anfragen sind grundsätzlich über das im Abschnitt 7.1 erwähnte Ticket-System zu stellen. Für die WISO-IT-interne Überwachung und Eskalation vom First-Level-Support an den Second-Level-Support sorgt seit Mitte November 2010 ein eigens hierfür zuständiger Mitarbeiter. Wenn nach angemessener Zeit keine Reaktion erfolgt oder keine Abhilfe geschaffen wurde, ist der WISO-IT-Leiter als erste Beschwerdeinstanz zu kontaktieren (claus.czygan@wiso.uni-hamburg.de). Die weiteren, nicht zeitgleich, sondern konsekutiv zu kontaktierenden Eskalationsstufen sind der FIO (manfred.sommer@wiso.uni-hamburg.de) und danach erst das Dekanat (kai-uwe.schnapp@wiso.uni-hamburg.de).

7.4 Service-Level-Agreements (SLA’s)

Was „angemessene Zeiten“ im Sinne des vorstehenden Abschnitts sind, lässt sich letztlich nur in Service-Level-Agreements festschreiben. Reaktionszeiten werden maßgeblich von (der Tendenz nach) „grenzenlosen“ Benutzerwünschen auf der einen Seite und von der Verfügbarkeit des (in der Realität stets) knappen Supportpersonals bestimmt. SLA’s sind nicht zuletzt der Versuch, einen alltagstauglichen Kompromiss zu definieren.

8 Nachwort

Die Informationstechnik ist nicht nur an Universitäten ständig im Fluss. Eine IT-Organisation wie WISO-IT muss deshalb eine „lernende Organisation“ sein. Schon deshalb sind wir auf das Feedback und eine konstruktive Kooperation des die IT nutzenden Fakultätspersonals angewiesen.

9 Anhang: Migration und Integration

Unter **Migration** wird in diesem Benutzerleitfaden die Überführung von Personen[22], Geräten, Postfächern und Dateien verstanden, die bereits in der alten, jetzt ab- und aufzulösenden HWP-NET-Domäne waren, also auch die bisher per VPN angebundenen User/innen aus anderen Fakultätsgebäuden als VMP 9, unter **Integration** die Einbeziehung von zur WISO-Fakultät gehörenden Benutzer/innen und ihrer IT-Ressourcen, die bisher nicht Bestandteil der HWP-NET-Domäne waren.

9.1 Migration

In den letzten Wochen wurden fast alle noch aktiven Benutzer/innen der alten HWP-NET-Domäne und deren Arbeitsplatzrechner, E-Mail-Postfächer und Dateien schrittweise in die neue, perspektivisch fakultätsweite IT-Infrastruktur migriert.

Ebenfalls migriert wurden die Studierenden aus dem HWP-NET und die CIP-Pools der Fakultät. Alle Studierenden an der Fakultät können in den WISO-CIP-Pools unter ihrer STiNE-Kennung arbeiten, auch solche, die wie z.B. Lehramtsstudierende, in Studiengängen studieren, die von anderen Fakultäten betreut werden. Da die CIP-Pools in allen Fakultätsgebäuden mit einem einheitlichen Image ausgestattet wurden, kann man bei Engpässen auf andere CIP-Pools ausweichen.

Die alte HWP-NET-Domäne wird in naher Zukunft abgeschaltet, da sie erheblichen zusätzlichen Wartungsaufwand verursacht, der den Betrieb und Support in der neuen Domäne belastet.

9.2 Integration

Professuren, die in den letzten Jahren nicht zur alten HWP-NET-Domäne gehörten und deshalb nicht migriert werden konnten, werden erst im Laufe des Jahres 2011 schrittweise, projektförmig und in enger Kooperation der Beteiligten in die neue Infrastruktur integriert. Näheres dazu entscheidet das Dekanat nach

- Konsolidierung des Betriebs und Supports in der neuen WISO-Domäne,
- Konsultation des CIO und der Datenschutzbeauftragten der Hamburger Hochschulen,
- Information von Fakultätsrat und Fakultätskammer und
- Abschluss der Integrationsplanung.

[22] Unter Personen, Benutzer/innen, User/innen wird hier, sofern nicht anders vermerkt oder aus dem Kontext ersichtlich, nur das Fakultätspersonal verstanden, nicht jedoch die Studierenden.