Sicherheitskonzept im Rahmen des Projekts Einführung von SAP R/3 an der Philipps-Universität Marburg

Anlagen:

A Backup-Konzept unter SAP R/3

B Recovery –Konzept unter SAP R/3

C Drucker-Konzept unter SAP R/3

D Datenschutz und Datensicherheit unter SAP R/3

E Checklisten für ein Sicherheitskonzept unter SAP R/3

1 Einführung

Mit der Einführung der SAP-Software R/3 an der Philipps-Universität Marburg und den daraus resultierenden Umstrukturierungen in den Verwaltungsabläufen sowie den von SAP geforderten Sicherheitsaspekten bei dem Betrieb ihrer Systeme muss eine neue Sicherheitskonzeption im Bereich der Verwaltungs-DV erstellt werden. Die Überlegungen beruhen auf einer Erweiterung des Verwaltungsnetzes *(um ein zusätzliches Sub-Netz)* und der vorgesehenen Dezentralisierung von Verwaltungsabläufen innerhalb der Universität. Dabei sind die Empfehlungen der SAP zum Betrieb ihrer Systeme und die Empfehlungen des hessischen Datenschutzbeauftragten zu diesem Thema eingearbeitet worden. Die Überlegungen und Konzepte hierzu sind sicher noch nicht vollständig und werden mit dem weiteren Fortgang des Projekts eine ständige Fortschreibung erfahren.

2 Ist-Zustand

Die Verwaltung der Philipps-Universität konzentriert sich im wesentlichen auf 2 Standorte, die Verwaltungsgebäude in der Biegenstraße 10 und 12 sowie das Technikgebäude in der Conradistraße auf den Lahnbergen. Die lokalen Netze der beiden Standorte sind über LWL miteinander verbunden und bilden das Verwaltungsnetz. Kleinere Bereiche, die nicht physisch am Verwaltungsnetz angebunden sind, werden über eine VLAN-Lösung, die vom HRZ betreut wird, mit dem Verwaltungs-LAN verbunden.
Die Verbindung bzw. Trennung zwischen dem abgesicherten Verwaltungsnetz und dem offenen Hochschulnetz erfolgt über eine Firewall. Dabei wird bei Zugriffen von Außen nach dem Prinzip der default deny alles definiert, was erlaubt sein soll und alles andere verboten. So sind die Datenbank- und Fileserver der Verwaltung von außen nicht erreichbar.

Als Netzwerkbetriebssystem ist derzeit WINDOWS NT 4.0 SP 6a im Einsatz, daneben existieren noch verschieden Unix-Datenbankserver für spezielle Anwendungen der Verwaltung (z.B. HESSOS, FlexNow!, ...). Alle Clients haben WINDOWS NT 4.0 oder WINDOWS 2000 als Betriebssystem.

3 Soll-Zustand

Durch die Entscheidung der hessischen Hochschulen, in Zukunft SAP R/3 als Instrument für die Finanzbuchhaltung, das Controlling, die Materialwirtschaft und das Personalwesen einzusetzen, ist keine Umstrukturierung des vorhandenen Verwaltungsnetzes erforderlich. Die SAP Systeme ermöglichen es, Verwaltungsabläufe stärker zu dezentralisieren und den Fachbereichen schnellere und bessere Informationen zu liefern.
Beim Ausbau des Verwaltungsnetzes wurden die Vorgaben der SAP zum Betrieb von SAP-Systemen (vgl. Checkliste im Anhang) ebenso einbezogen wie die dazu erfolgten Empfehlungen des hessischen Datenschutzbeauftragten.

Folgende Vorgaben der SAP zum Betrieb eines R/3 Systems wurden umgesetzt:

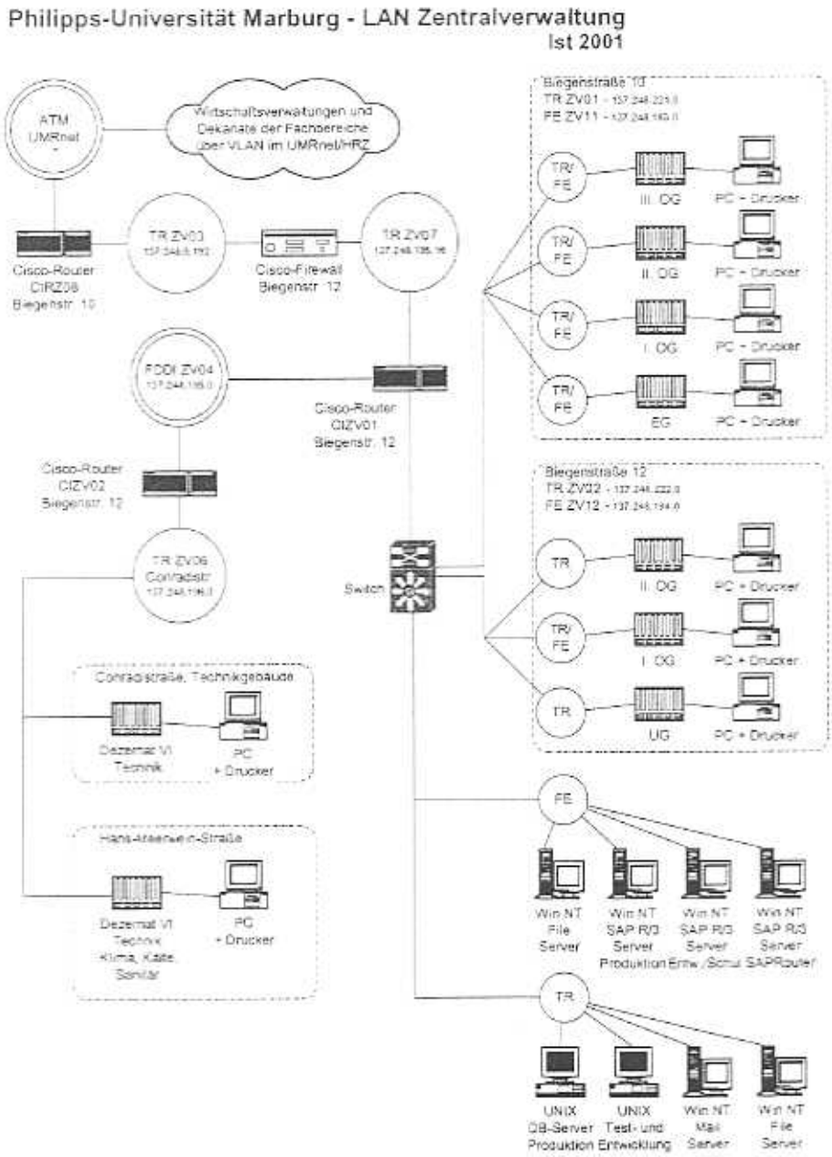
- Die SAP-Server stehen in einem separaten Subnetz.
- Das Subnetz besteht nur aus den Servern und einem SAProuter.
- Der Zugriff zu den SAP-Systemen erfolgt nur über den SAProuter.

Der Zugriff auf die SAP-Systeme kann über folgende Zugriffswege erfolgen:

- Die Benutzer in den Verwaltungsgebäuden Biegenstrasse 10 und 12, sowie der Wirtschaftsverwaltungen (über VLAN-Anbindung) erhalten Zugriff auf die R/3-Systeme aus dem Verwaltungsnetz heraus. Dieses Netz ist in sich als vertrauenswürdig anzusehen, da die sicherheitstechnischen Konfigurationen der Einzelsysteme identisch sind.
- Der Zugang der dezentralen Nutzer in den Fachbereichen und Einrichtungen an die SAP-Systeme wird auf Grund der heterogenen Netzwerkstruktur innerhalb des Wissenschaftsnetzes nicht mit der oben genannten Lösung abzudecken sein. Hier befinden sich die Nutzer in verschiedenen Netzen, die mit unterschiedlichem Sicherheitsgrad abgesichert sind (z.B. Eintrag in Firewall). Ferner gibt es die Möglichkeit einer Verbindung auf Basis einer Verschlüsselungssoftware, wie sie auch vom hessischen Datenschutzbeauftragten bei einem Zugang über das Internet gefordert wird.
- Eine dritte Gruppe von Nutzern des SAP-Systems, die in einer späteren Phase über das WWW und einen ITS-Server den Zugriff auf die SAP-Systeme erhalten, wird erst zu einem späteren Zeitpunkt betrachtet, da die dort geltenden Sicherheitsüberlegungen stark vom Stand der Technik zum jeweiligen Zeitpunkt abhängen werden. Zudem ist der Inhalt der Zugriffe bis jetzt noch nicht spezifiziert.

4 Das Verwaltungsnetz und seine Kommunikation zum Intranet der Philipps-Universität.

Das Verwaltungsnetz der Philipps-Universität (physikalisch eigenes Netz, bestehend aus mehreren Teilnetzen) wird als Netz folgendermaßen betrieben:



Die Teilnetze in den Gebäuden Biegenstraße 10 und 12 sowie Conradistraße bilden das sogenannte Verwaltungsnetz inklusive der NT- und Unix-Server.

Das gesamte Verwaltungsnetz wird durch eine Firewall gegen unberechtigte Zugriffe geschützt.

In einem separaten Subnetz der Verwaltung (Teilnetz ZV08) befinden sich die lokalen R/3–NT-Server, wie von SAP empfohlen. Der eigentliche Zugriff auf die SAP R/3 Systeme erfolgt zudem noch über den SAProuter (Port 3299), der im gleichen Subnetz wie die SAP-Systeme steht. Ein weiteres Teilnetz ist für das sogenannte öffentliche Netz vorgesehen (Web-Server, ITS-Server für SAP R/3).

Ziel ist, eine Sicherheitspolitik aufzubauen, die es auch den dezentralen Einheiten ermöglicht, auf das SAP R/3 System und zu einem späteren Zeitpunkt über den ITS-Server zugreifen zu können.

Ein Zugriff aus dem Intranet auf die R/3-Systeme muss nach Vorgabe des Hessischen Datenschutzbeauftragten verschlüsselt erfolgen. Die Verschlüsselung soll auf Applikationsebene erfolgen. Als Authentisierungs- und Verschlüsselungsprodukt für die SAP-R/3 Systeme wird von SAP das Produkt SECUDE empfohlen.

Die Philipps-Universität hat sich nach intensivem Informationsaustausch mit den anderen hessischen Hochschulen entschieden, als Verschlüsselungssoftware das Produkt SECUDE einzusetzen.

Die genaue Konfiguration und Administration der Verschlüsselungssoftware erfolgt nach den beratenden Gesprächen mit der Fa. Controlware und dem HRZ. Als Ziel des Einsatzes der Verschlüsselungssoftware wird der 1.7.2001 angestrebt.

5 Servergestütztes Netz der Verwaltung

Hier werden die notwendigen organisatorischen Maßnahmen beschrieben, die global auf die Administration aller beschriebenen IT-Systeme der Verwaltungs-DV an der Philipps-Universität zutreffen.

5.1 Infrastruktur des Serverraums

5.1.1 Raumbeschreibung

Der Serverraum befindet sich im Verwaltungsgebäude Biegenstraße 12 der Philipps-Universität im 1. Obergeschoss. Der Zugang wird durch eine Spezialfeuerschutztür gesichert. Die Raumfenster sind mit einer Spezialverglasung versehen.
Durch eine zum Dezernat V - DV gehörenden Schließanlage wird der Zugang nur für Angehörige dieses Dezernates gewährleistet.

5.1.2 Technische Infrastruktur

Durch Lastberechnungen der aufzustellenden Server und Geräte wurde sichergestellt, dass die dort neu vorgenommenen Elektroinstallationen den gegenwärtigen und zukünftigen Bedürfnissen entspricht.
Ein zentraler Stromausschalter, der sich im Verteilerschrank befindet, sorgt bei Gefährdung für ein schnelles Abschalten der Stromversorgung.
Jeder Server ist gegen Stromausfall durch eine eigene unterbrechungsfreie Stromversorgungen (USV) geschützt. Die Kapazitäten der USVs sind so dimensioniert, dass ein Stromausfall von mindestens 10 Minuten überbrückt werden kann und ausreichende Restkapazität für das ordnungsgemäße Herunterfahren des jeweiligen Servers zur Verfügung stehen.
Ein Klimatisierung des Serverraums sorgt für die bei IT-Geräten zulässige Betriebstemperatur.
Eine Brandmeldeanlage, die Rauch- und Qualmentwicklungen erfasst, und den Brandschutz alarmiert, ist derzeit nicht installiert aber im Laufe des Jahres 2001 geplant.
Für den IT-Einsatz geeignete entsprechende Handfeuerlöscher sind in ausreichender Zahl im und vor dem Serverraum vorhanden.

5.1.3 Zugangskontrolle

Das Dezernat V – Datenverarbeitung befindet sich in einem Schutzbereich, der nur über zwei ständig geschlossen gehaltene Türen zugänglich ist. Für diese beiden Türen als auch für alle Räume innerhalb des Dezernates V – DV ist eine gemeinsame, von der übrigen Verwaltung getrennte Schließanlage vorhanden. Der Serverraum ist in diese Schließanlage integriert, so dass nur zum Zutritt befugte Personen den Raum betreten können. Nicht befugte Personen dürfen nur in Begleitung einer autorisierten Person den Serverraum aufsuchen.

Die Ausgabe und der Einzug vorhandener Schlüssel wird über eine Liste im Dez. V – Datenverarbeitung, Herr Mehlinger, geführt. Eine Reserveschlüssel befindet sich im Dezernat IV, Sachgebiet Haus- und Liegenschaftsverwaltung, beim Sachgebietsleiter unter Verschluß. Für die Feuerwehr ist für Notfälle ein Schlüssel im Schlüsseltresor im Hörsaalgebäude, Biegenstr. 14, hinterlegt.

Das Administrationspersonal kontrolliert täglich den Zustand des Serverraums.

5.2 Organisation

5.2.1 Datenträgerverwaltung

Alle extern verwendeten Datenträger zur Datensicherung der einzelnen IT-Systeme werden in einem Safe des Dezernates V - Datenverarbeitung gelagert. Sie sind über äußerliche Kennzeichnung den jeweiligen Systemen zugeordnet und erlauben so eine schnelle Identifizierung. **Namenskonventionen ?**

Der Bestand verwendeter Sicherungsmedien wird regelmäßig durch die jeweiligen Systemadministratoren auf Vollständigkeit geprüft. Bei Austausch defekter oder nicht mehr zu verwendender Datenträger wird über geeignete Maßnahmen (physische Löschen oder physische Vernichtung) sichergestellt, dass die zu entsorgenden Datenträger keine Informationen mehr enthalten.

Als zweite Sicherungsmaßnahme existieren neben den genannten Sicherungskopien im Safe zusätzliche Sicherungskopien, die an einem sicheren Ort außerhalb des Dezernates V - DV verwahrt werden. Zugang zu diesen Verwahrorten haben nur die dafür vorgesehenen Administratoren.

5.2.2 Regelungen für Wartungs-und Reparaturarbeiten

Die für den Betrieb zuständigen Administratoren sind zuständig für vorbeugende regelmäßige Wartungstätigkeiten. Wartungs-und Reparaturarbeiten vor Ort, die durch externe Personen durchgeführt werden müssen, werden grundsätzlich unter Beaufsichtigung der betreffenden Personen getroffen.

Bei Durchführung der Wartung ausser Haus muss sichergestellt werden, dass keine sensitiven Daten auf den entsprechenden Systemen vorhanden sind. Ist dies nicht sicherzustellen, werden die mit der Reparatur beauftragten Unternehmen zur Einhaltung der erforderlichen IT-Sicherheitsmaßnahmen verpflichtet.

Die Durchführung aller Wartungsmaßnahmen wird protokolliert. *Wo? Formular ?*

5.2.3 Nutzungsverbot nicht freigegebener Software

Die auf den Systemen (Server, Clients) eingesetzte Software wird durch das Dezernat V - Datenverarbeitung freigegeben. Es ist untersagt, nicht registrierte Software in Betrieb zu nehmen, dies wird auch durch geeignete technische Maßnahmen unterbunden. **Org-Anweisung ?**

5.2.4 Hinterlegen der Passworte

Für alle zu betreuenden IT-System die mit einem Passwort versehen sind, ist durch die jeweiligen Systemadministratoren sicherzustellen, dass die entsprechenden aktuellen Passworte in einem verschlossenen Umschlag hinterlegt sind. Diese Umschläge werden im Safe des Dezernates V verwahrt und dienen in Notfällen der Absicherung und Notfallvorsorge bei Nichtanwesenheit der entsprechenden Administratoren zur Aufrechterhaltung des IT-Betriebs.

5.2.5 Dokumentation der Systemkonfiguration und Änderungen

Zum Zweck der Revisionsfähigkeit sowie für die Notfallplanung existiert eine aktuelle Dokumentation aller Systeme inklusive der Netzwerkstruktur. Nur so ist ein geordneter Wiederanlauf der Systeme im Notfall gesichert. Diese Dokumentation beinhaltet die physische und logische Netzkonfiguration, die Konfiguration der einzelnen System sowie die Zugriffsrechte der Benutzer und den Stand der Datensicherung. Jede vorgenommene Änderung ist durch die jeweiligen Systemadministratoren fortzuschreiben.

5.2.6 Benennung von Administratoren

Für jedes zu betreuende IT-System sind Administratoren und Stellvertreter (Stv) benannt:

- NT LAN-Server, EXCHANGE-Server: Herr Laran, Herr May (Stv)
- SAP R/3 : Herr Mehlinger, Herr Möller
- UNIX/AIX-Server: Herr Mehlinger, Herr Huth (Stv), Herr Größer (Stv)
- Firewall, Switches: Herr Laran, Herr Mehlinger (Stv), Herr Huth (Stv)

Es wird darauf geachtet, dass die Administratoren über Aus-und Fortbildungsmaßnahmen ihren Kenntnisstand den entsprechenden Weiterentwicklungen im IT-Bereich anpassen. Dies gilt insbesondere für den Bereich der Sicherheit der IT-Systeme.

6 Windows NT Netz

6.1 Organisation

6.1.1 Sicherheitsstrategie Windows NT Client-Server-Netz

Das Verwaltungsnetz der Philipps-Universität ist ein physikalisch eigenes Netz und wird mit NT-Servern und ca. 240 NT-Clients betrieben. Die Kommunikation aus und zu diesem Netz erfolgt ausschließlich über eine Firewall.

6.1.1.1 Definition der Client-Server-Netzstruktur

Im Verwaltungsnetz der Philipps-Universität wird das Single-Domänen-Konzept mit einem Primären Domainencontroller (PDC) unter NT 4.0 und mindestens einem Backup Domainencontroller (BDC) eingesetzt, alle Clients sind als NT 4.0 oder WINDOWS 2000 Workstation-Clients installiert.

6.1.1.2 Regelung der Verantwortlichkeiten

Die Netzwerkadministratoren des Dezernates V - DV sind zuständig für den sicheren Betrieb des Netzes und der NT-Server im Netzbereich der Zentralverwaltung. Sie alleine dürfen sicherheitsrelevante Parameter im Netz verändern. Zusätzlich sind sie verantwortlich für die Vergabe der entsprechenden Rechte und die Verwaltung der Benutzer und Benutzerkonten auf den Servern.

6.1.1.3 Festlegung der Namenskonventionen

Es werden eindeutige Namen für die Workstations, Benutzergruppen und Benutzer verwendet:

Workstation: PCZVyyy oder PSZVyyy, yyy=hostnummer im subnetz
Benutzergruppen: Dezernate, Referate, Abteilungen, Fachbereiche
Benutzer unter Windows NT: XXnn, XX = Kürzel in Abhängigkeit zur organisatorischen Zugehörigkeit, nn = laufende Nr. innerhalb XX mit führender 0

6.1.1.4 Festlegung der Regeln für Benutzerkonten

Das vom Systemadministrator initial gesetzte Passwort hat eine Minimallänge von 6 Zeichen und muss vom Benutzer bei der ersten Anmeldung geändert werden. Die Gültigkeitsdauer

des Passwortes ist auf 60 Tage beschränkt. Das Benutzerkonto wird nach 3 ungültigen Anmeldeversuchen gesperrt und automatisch nach einer Wartezeit von 30 Minuten entsperrt. Nur durch den Administrator kann es vorher entsperrt werden.

6.1.1.5 Einrichtung von Gruppen

Soweit möglich, werden Benutzer mit entsprechenden gleichen Anforderungen in Benutzergruppen zusammengefasst. Rechte werden Benutzergruppen zugeordnet und erleichtern so die Systemadministration. Die Benutzer werden der Gruppe Benutzer zugeordnet und erhalten keine Administratorrechte auf ihren Workstations.

6.1.1.6 Festlegung der Benutzerrechte

Ein Benutzer kann nach Anmeldung über ein Konto immer nur die Aktionen ausführen, die ihm direkt oder auf Grund seiner Gruppenmitgliedschaft erteilt werden. Das Ausführen aller nicht genehmigten Aktionen wird von Windows-NT verhindert.
Der lokalen Gruppe „Jeder" ist auf den NT-Servern das Recht: „Lokale Anmeldung" und „System herunterfahren" entzogen.

6.1.1.7 Festlegung der Vorgaben für Protokollierung

Protokollierungen können mit Hilfe des Benutzermanagers umgesetzt werden. Da unter NT sehr viele Protokollmöglichkeiten angeboten werden, muss eine Regelung gefunden werden, die zum einen die sicherheitsrelevanten Ereignisse protokolliert, zum anderen es aber noch ermöglicht, diese Protokolle noch auszuwerten und zudem die Systemleistung nicht durch Performanceeinbußen behindert. Im Allgemeinen sollte für einen mittleren Schutzbedarf folgende Regelung ausreichen:

- An- und Abmelden bei Erfolg und Fehler
- Datei- und Objektzugriff bei Fehler
- Verwendung von Benutzerrechten bei Fehler
- Benutzer- und Gruppenverwaltung bei Erfolg und Fehler
- Sicherheitsrichtlinienänderung bei Erfolg und Fehler
- Neustarten und Herunterfahren des Systems bei Erfolg und Fehler

6.1.1.8 *Regeln zur Datenspeicherung*

Es wird empfohlen, die Daten zentral auf dem NT-Server in den dem Benutzer zugeteilten Verzeichnissen abzulegen. Lokal steht das Laufwerk D als Datenablage zur Verfügung. Der Benutzer wird darauf hingewiesen, dass er für die Sicherung seiner lokalen Daten selbst verantwortlich ist.

6.1.1.9 *Vergabe der Zugriffsrechte*

Die Vergabe der Zugriffsregelungen werden auf den Servern von den Administratoren geregelt. Auf den Workstations können sie vom Besitzer des Objektes vergeben werden, hierbei sollte darauf geachtet werden, daß nie die Berechtigung „Vollzugriff" vergeben wird. Daher sollte der Besitzer regelmäßig prüfen, ob er noch Besitzer seiner Verzeichnisse und Dateien ist.

Ein Zugriff auf die Dateien und Verzeichnisse des Betriebssystems und den Programmverzeichnissen auf den Workstations (Laufwerk C) wird vom Administrator der Workstation unterbunden. Nur auf C:\temp und seine eigenen Profiles hat der Benutzer die für ihn notwendigen Rechte.

6.1.1.10 *Verantwortlichkeit für Administratoren und Benutzer im Client-Server-Netz*

Die Administratoren sind u.a. verantwortlich für den sicheren Betrieb des Netzes und somit für die regelmäßige Auswertung der Protokolldateien, die diesen Betrieb gewährleisten, für die Vergabe der Zugriffsrechte, die Durchführung der zentralen Datensicherung und das Anlegen der Benutzerkonten und die Vergabe der Passworte.

6.1.2 Sicherheitskontrollen im Windows NT-Client-Server-Netz

Folgende Punkte sind auf Server-Ebene regelmäßig von den Administratoren zu prüfen:

- Fehlgeschlagene Zugriffsversuche (wöchentlich);
- Benutzung von privilegierten Benutzerkonten (wöchentlich);
- System-Sicherheits-Einstellungen;
- Systemintegrität;
- Unbenutzte Benutzerkonten (halbjährlich).

Beim Auftreten von Unregelmäßigkeiten in diesen Punkten informieren die Administratoren die zuständige Dezernatsleitung und, soweit zuständig, den örtlichen Datenschutzbeauftragten.

6.1.3 Freigabe von Verzeichnissen unter Windows NT

Die Freigabe von Verzeichnissen erfolgt nur auf Servern und ist notwendig, damit die Benutzer Zugriff auf die entsprechenden Ressourcen erhalten. Die Freigabe auf Workstations erfolgt nur als begründete Ausnahme erfolgen und muss dementsprechend abgesichert sein.

6.2 Hardware/Software

6.2.1 Passwortschutz unter Windows NT

Der Benutzer erhält vom Administrator ein Initialkennwort, welches er bei der ersten Anmeldung ändern muss. Als Vorgabe ist ein mind. 6-stelliges Passwort verlangt. Die Gültigkeit des Passwortes wird auf 60 Tage eingeschränkt. Die Passwort-Historie läuft über 5 Passworte.

Es sollen folgende Regeln zum Passwortgebrauch beachtet werden:

Keine leicht zu erratenden Passworte nehmen, es soll mindestens 1 Sonderzeichen enthalten, Passwort muss geheim bleiben und bei bekannt werden an Dritte sofort gewechselt werden, Eingabe des Passworts soll unbeobachtet stattfinden, Passworte nicht auf programmierbare Funktionstasten speichern, bei schriftlicher Hinterlegung darf das Passwort nur in einem verschlossenen Umschlag an einem sicheren Ort deponiert werden.

Org.-Anweisung an Benutzer ?

6.2.2 Absicherung des Boot-Vorgangs

- Formatierung aller Partition mit NTFS.
- Keine parallele Installation eines anderen Betriebssystems.
- Bootreihenfolge ist C , A.
- Bios Passwort
- Gehäuseschloß

6.2.3 Strukturierte Systemverwaltung

Auf den Workstations werden lokale Gruppen definiert. Der Benutzer ist Mitglied der lokalen Gruppe Benutzer auf seiner Workstation. Da die Mitarbeiter im Verwaltungsnetz in der Regel ihre Arbeiten nur auf der ihnen zugeordneten Workstation erledigen, besitzt im Verwaltungsnetz ein Benutzer genau ein Konto auf einer ihm zugeordneten Workstation.

6.2.4 Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten

Das Gastkonto auf den Workstations ist deaktiviert.

6.2.5 Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse

Die Zugriffberechtigungen auf Dateien und Verzeichnisse stehen nur auf Datenträgern mit dem Dateisystem NTFS zur Verfügung und werden vom Besitzer oder Ersteller eines Objektes vergeben.
Auf den NT-Servern erfolgt diese Vergabe durch die Administratoren.
Die Attribute der Systemdateien werden so gesetzt, dass nur die Administratoren darauf vollen Zugriff haben. Die für die Benutzer benötigten Zugriffsformen müssen auf ein Minimum eingeschränkt werden (lesender und ausführender Zugriff). Gerade die EXE und DLL-Dateien sollte für die Benutzer mit lesenden Zugriff beschränkt bleiben.

6.2.6 Sichere Installation

- WINDOWS NT 4.0 oder WINDOWS 2000 Workstation, deutsch, neustes Service-Pack.
- NTFS Partitons.
- Administratorkonto wird nur von dem Administrator der jeweiligen Workstation verwaltet.
- Nur bestimmte zugelassene Programme werden installiert, z.B. Office-Produkte, Outlook, SAPgui, TCP/IP-Zugang zu Unix-Rechnern ***(keine X-Windows)***.
- Das Gastkonto ist gesperrt.
- Bildschirmschoner mit Kennwort. **(Herr May: bitte beachten !)**
- Zugriff auf die SAP R/3 Rechner erfolgt über die SAPgui mittels ein nur ihm bekannten Benutzernamen und Passwort. Die Verbindung basiert auf TCP/IP.

- Einsatz der Virenschutz-Software McAffee AntiVirus Version 4.0 bzw. 4.5. **Aktualisierungsabstände mit Herren May u. Mehlinger festlegen)**

6.2.7 Sicheres Löschen

Der Benutzer wird darauf hingewiesen, seinen Papierkorb regelmäßig zu löschen, bzw. sensitive Dateien explizit zu löschen und nicht im Papierkorb zu lassen. **(Org.-Anweisung)**

6.2.8 Deaktivieren der automatischen CD–ROM-Erkennung

Es wird empfohlen, die automatische CD-ROM Erkennung auszuschalten, bzw. den Benutzer zu informieren, wie die automatische CD-ROM-Erkennung temporär verhindert werden kann. **(Rücksprache Herren May u. Mehlinger; Org.-Anweisung)**

6.2.9 Schutz der Registrierung unter NT

Nur der Administrator hat Vollzugriff auf das Registrierungsverzeichnis von NT.

6.2.10 Sichere Systemversion

Der Administrator sorgt für das Einspielen der neusten service packs und hot fixes, soweit sie für den Betrieb notwendig sind.

6.2.11 Schutz der Administratorenkonten

Das Administratorkonto auf den Workstations wird mit einem sicheren Passwort versehen.

6.3 Kommunikation

6.3.1 Verschlüsselung

Auf eine Verschlüsselung der Kommunikation innerhalb des Verwaltungsnetzes wird verzichtet, da das Verwaltungsnetz als sicheres Netz gilt.

6.3.2 Sichere Konfiguration des Fernzugriffs unter NT

Der Fernzugriff von externen Clients auf die lokalen NT-Systeme über RAS wird nicht gestattet. **(Rücksprache Herren Mehlinger und May)**

6.3.3 Sichere Konfiguration der TCP/IP-Netzverwaltung

Um den Aufwand bei der Verwaltung der IP-Adreßinformation zu minimieren, werden über DHCP IP-Adressen und die zugehörigen Daten verwaltet. Die Installation und Pflege des DHCP-Servers wird vom Netzadministrator vorgenommen. Allen Clients im Netz werden feste IP-Adressen zugewiesen. Eine dynamische Vergabe findet nicht statt, da eine statische Zuordnung aufgrund genügend vorhandener IP-Adressen möglich ist.
Die Verwaltung betreibt ferner einen eigenen WINS-Server.

6.3.4 Sichere Konfiguration der TCP/IP-Netzdienste

Eine Absicherung der TCP/IP Netzdienste wird über die Firewall geregelt.
Im NT-Netz ist kein FTP zugelassen, da dort andere Möglichkeiten der Datenübertragung genutzt werden können. **(Rücksprache Herren Mehlinger und May)**

6.4 Notfallvorsorge

Über ein Notfallkonzept (**muß noch erstellt werden!**) wird geregelt, wie bei einem Ausfall des PDC der weitere Betrieb des Netzes gewährleistet ist. Dieses Konzept wird an sicherer Stelle verwahrt und soll auch ein weniger geübtes Mitglied (bei Ausfall der zuständigen Administratoren) des Dezernates im Notfall in die Lage versetzen, einen Ausfallserver (BDC) als zwischenzeitliches Produktivsystem zur Verfügung zu stellen.

Die Aufbewahrung der Datenträger der nachfolgend beschriebenen Sicherungsmaßnahmen erfolgt in einem Safe, der sich im Serverraum des Dezernates V - Datenverarbeitung, Biegenstraße 12, 2. Stock, befindet.

6.4.1 Regelmäßige Datensicherung

Die Datensicherung der NT-Server erfolgt mit dem Produkt ARCserve 2000 (SAP-Server) bzw. ARCserveIT 6.6.1 (alle anderen NT-Server).
Die regelmäßige Datensicherung der NT-Server liegt in der Verantwortung der Administratoren. Es gelten folgende Regeln:

- Tägliche Komplettsicherung Mo-Fr. Nachts auf DLT-Band.
- Die Tagessicherung wird im 1-wöchigen Turnus aufbewahrt.
- Die Freitagssicherungen werden als Wochensicherung einem Monat aufbewahrt.
- Am letzten Kalendertag im Monat erfolgt die Monatssicherung; die ggfls. an diesem Tag anstehende Tagessicherung entfällt. Die Monatssicherungen werden 12 Monate aufbewahrt.
- Der Benutzer ist für die Sicherung seiner lokalen Laufwerke selbst verantwortlich und wird über das ordnungsgemäße Sichern und Aufbewahren seiner Sicherungen informiert.

6.4.2 Erstellung von Rettungsdisketten für NT

Für jeden NT-Server werden Notfalldisketten erstellt, die jeweils nach Systemänderungen erneuert werden. **(beschreiben: ARCserve Disaster Recovery – Option auf Servern mit Library)**
Die NT-Workstations werden bei Bedarf neu konfiguriert, da sie mit einer Standardinstallation versehen sind.

6.4.3 Einsatz von Redundanzen in Windows-NT-Server

Die NT-Server sind mit einem Raid-System mit Hot-Spare-Drives, redundanten Netzteilen und Lüftern sowie doppelten LAN-Adaptern ausgestattet. Ein Wartungsvertrag mit dem Hardwarelieferanten stellt sicher, dass bei Hardwareausfall schnellstens Ersatz geleistet wird.

7 SAP R/3-Systeme

7.1 Datenschutz unter SAP R/3

Alle zu prüfenden und festgelegten Systemeinstellungen werden ausführlich in Anlage E: „Checklisten für das lokale SAP R/3 System für die Philipps-Universität" erläutert. Diese Checklisten werden ständig überarbeit und dem aktuellen Systemstand angepasst.

7.1.1 Server-Umgebung

Die lokalen SAP R/3 –Server befinden sich in einem eigenen Subnetz des Verwaltungsnetzes und sind, wie es den Empfehlungen von SAP entsprechen, nur über den SAPRouter und von ausserhalb der Zentralverwaltung nur über die Firewall zu erreichen. Alle Anmeldungen an das SAP-System werden durch den SAPRouter an die Systeme weitergeleitet.

Das SAP R/3-System ist als zentrale Instanz installiert, d.h. Datenbank-und Applikationsserver befinden sich auf einem Server. Eine Trennung in Datenbank-und Applikationsserver ist zu einem späteren Zeitpunkt bei steigenden Benutzerzahlen und abnehmender Performance möglich und ohne großen technischen Aufwand zu realisieren.
Es erfolgt eine physikalische Trennung in ein Test-und Qualitätssicherungssystem (DM1) und in das Produktivsystem (PM1) der Philipps-Universität.

Skizze einfügen (Möller)

7.1.2 Anmeldung am R/3 System aus dem Verwaltungsnetz.

Der Benutzer meldet sich am R/3 System über das Frontend-Programm SAPgui an.
Da die Verbindung zum SAP R/3 System über **den Saprouter ?** weitergegeben wird, muss die Firewall nur einen Port (3299) zur Verbindung mit dem SAProuter-Rechner öffnen, über den alle Zugriffe geleitet werden.
Die SAPgui baut über den Dispatcherprozess (Port 32) eine Verbindung zum Anwendungsserver auf.
Andere technische Möglichkeiten der Anmeldung, wie z.B. über das Internet mit Hilfe eines Browsers, werden hier erst einmal nicht betrachtet. Diese Technik erfordert zusätzliche Web-Server und ITS-Server und werden erst in einem zweiten Schritt an der Philipps-Universität

zum Einsatz kommen. Das Sicherheitskonzept dafür wird dementsprechend später konzipiert.

Die Anmeldung an das R/3-Sytem geschieht über eine eindeutige User-ID. Das Passwort und die Passwortbehandlung werden über feste Vorgaben geregelt (Transaktion RZ10, damit werden die Regeländerungen in der Datenbank protokolliert).

Die Tabelle USR40 legt Passworte fest, die von der Benutzung ausgeschlossen sind. Hier sollen für das Umfeld naheliegende Passwortverbindungen wie SAP, UMR, UNIMR und andere simple Passworte wie z.B. HUND, KATZE, MAUS, Monatsnamen, Namen der Wochentage, ... ausgeschlossen werden.

Auswertungen über die gesetzten Systemparameter erlauben die Transaktionen RZ10, RZ11 und der Report RSPARAM.

Fehlgeschlagene Anmeldungen bekannter Benutzer werden über den Report RSUSR006 ausgewertet. Eine Sperrung der Benutzerkennung erfolgt nach insgesamt 3 erfolglosen Anmeldeversuchen und verhindert somit weitere Versuche der erfolglosen, eventuell unberechtigten Anmeldungen. Der gesperrte Benutzer kann manuell durch die Basis-Administratoren nach Rücksprache mit dem jeweiligen Benutzer entsperrt werden. Automatisch erfolgt die Entsperrung um 0 Uhr.

7.1.3 Benutzer im SAP R/3

Neben den Benutzern, die im SAP R/3 System von den Systemadministratoren angelegt und verwaltet werden, werden bei der Installation des Systems folgende Standardbenutzer angelegt:

- SAP* - fest codierter Initialuser
- DDIC - Pflege des ABAP/4 Dictionaries
- SAPCPIC - wird benötigt innerhalb des Early-Watch-Services
- EARLYWATCH - Dialogbenutzer für den Early-Watch-Service

Die Passworte dieser Standardbenutzer sind in allen Mandanten geändert und im Safe des Dez. V – Datenverarbeitung hinterlegt.

7.1.4 Benutzerberechtigungskonzept im SAP R/3

Über das Berechtigungskonzept soll sichergestellt werden, dass im R/3 arbeitende Benutzer nur Zugriff auf die Funktionalitäten und Daten des Systems haben, die für die Ausübung ihrer Tätigkeit notwendig sind. Grundsätzlich soll das Prinzip der minimalen Berechtigung abgebildet werden. Die Berechtigungen und Profile, die bei der Auslieferung von SAP im System enthalten waren, werden nicht verwendet. Die Berechtigungen sind so gestaltet, dass sie der betrieblichen Organisation, Aufgabenstellung und Kompetenzverteilung gerecht werden.
Eine grobe Vorgabe der Berechtigungen für Benutzerklassen werden im Referenzmodell der hessischen Hochschulen abgebildet und über das Transportsystem auf die lokalen Systeme ausgerollt. Hier erfolgt dann eine Verfeinerung und Anpassung an die lokalen Gegebenheiten der Hochschule.

7.1.5 Benutzeradministration

Eine Benutzeradministration kann in 3 Aufgabenbereiche untergliedert werden:

- Administration der Berechtigung
- Aktivieren der Berechtigung
- Administration der Benutzer

Da dieses 3-gestufte Verfahren aufgrund mangelnder Personalkapazität nicht überall zu gewährleisten ist, soll mindestens eine funktionale Trennung der Pflege der Berechtigungen und der Pflege der Benutzer und Zuweisung zu den Berechtigungen eingehalten werden.
Dieses Verfahren wird auch bei den lokalen Systemen der Philipps-Universität eingesetzt. Die Verantwortung für die inhaltlich richtige Vergabe der Berechtigungen liegt bei den lokalen key-usern der SAP R/3 Systeme, die Basis-Administratoren sind zuständig für die Pflege der Benutzer und Zuweisung der Berechtigungen zu den Benutzern. **(Hinweis auf Antrag)**

Die Reports RSUSR005 und RSUSR002 prüfen ab, welche Benutzer umfassende Berechtigungen besitzen, bzw. welche Benutzer Berechtigungen ändern können.

7.1.6 Autorisierung und Berechtigungsprüfung

Die Berechtigungsprüfung findet zur Laufzeit der Programme statt. Über die Transaktion erfolgt der Abgleich ob der Benutzer die Berechtigung zur Ausführung des Programms hat. Bei Nichtberechtigung erfolgte eine Rückweisung des entsprechenden Benutzers.

Bei Eigenprogrammierung ist jeder Programmierer darauf verpflichtet, die entsprechenden Berechtigungsprüfungen im Programm zu hinterlegen.

7.1.7 Registrierung der Änderung der Software

Ziel ist es, die unerlaubte Manipulation und Nutzung von Programmen auszuschließen.
Grundsätzlich ist zur Konsolidierung der SAP R/3 Systeme und der Nachvollziehbarkeit bei Änderungen von Objekten empfohlen, 3 SAP-Systeme vorzusehen:

- ein Testsystem,
- ein Qualitätssicherungssystem und
- ein Produktivsystem.

Dies wird an der Philipps-Universität durch die Rechner DM1 (Qualitätssicherung und Test) und PM1 (Produktivsystem) gewährleistet.
Änderungen werden grundsätzlich im Testsystem DM1 vorgenommen und erst nach dem Transport in die Qualitätssicherung und dortiger Freigabe in das Produktivsystem PM1 übernommen. **(Verweis auf Transportlandschaft)**
Eine Berechtigung zur Anwendungsentwicklung und Modifikation wird auf dem Produktivsystem PM1 aus Gründen der Sicherheit der Datenbestände und zum Schutz vor unberechtigter Kenntnisnahme von personenbezogenen Daten nicht vergeben.
Änderungen an SAP-Standard-Objekten im DM1 können nur über die Beantragung eines Schlüssels bei SAP durchgeführt werden. Dazu muss der Anwendungsentwickler bei SAP registriert sein.

7.1.8 Tabellenprotokollierung und Auswertungen

Alle ablaufenden Aktivitäten können transaktions- und benutzerabhängig über das CCMS (Computing Management system) protokolliert werden.
Die Auswertungsmöglichkeiten von spezifisch personenbezogenen Daten werden in einer Dienstvereinbarung mit dem Personalrat der Philipps-Universität festgelegt. Die Basis-Administratoren müssen im Rahmen ihrer Aufgabe zur Gewährleistung eines sicheren Systembetriebs alle diesbezüglichen Auswertungen im regelmäßigen Turnus überwachen.

Eine spezielle Nutzung der Auswertungen ist über das SAP-Tool AIS (Audit Info System) möglich. Hier kann zwischen den System-Audit und dem kaufmännischen Audit unter-

schieden werden. AIS ist als Arbeitsmittel für Auditoren, Datenschutzbeauftragte und Revisoren gedacht.
Speziell für die Aufgabe des Datenschutzbeauftragten und des Revisionsbeauftragten können eigene Benutzermenüs mit den Prüffunktionen zur Verfügung gestellt werden, die genau auf die jeweilige Aufgabe zugeschnitten sind.

7.2 Notfallvorsorge

Über ein Notfallkonzept wird geregelt, wie bei einem Ausfall des PM1 der weitere Betrieb des Netzes gewährleistet ist. Dieses Konzept wird an sicherer Stelle verwahrt und soll auch ein weniger geübtes Mitglied (bei Ausfall der zuständigen Administratoren) des Dezernates im Notfall in die Lage versetzen, einen Ausfallserver (DM1) als zwischenzeitliches Produktivsystem zur Verfügung zu stellen.
Ein Wartungsvertrag mit dem Hardwarelieferanten stellt sicher, dass bei Hardwareausfall schnellstens Ersatz bereitgestellt wird.

7.2.1 Datensicherung

Die regelmäßige Datensicherung der SAP R/3-Server liegt in der Verantwortung der Administratoren. Die Datenträger der jeweiligen Sicherungsläufe werde im Safe des Dez. V – Datenverarbeitung, Biegenstr. 12, Serverraum, aufbewahrt. Es werden folgende Sicherungen durchgeführt:

R/3 Produktivsystem PM1:

- Tägliche (Mo. - Fr. Nachts) Sicherung der Datenbank mit Informix Onbar –b –L 0 auf DLT-Band.
- Die Tagessicherung wird im 2-wöchigen Turnus aufbewahrt.
- Die Logs einer ganzen Woche werden auf ein 4mm Band gesichert. Diese werden 2 Wochen aufbewahrt (3 Bänder).
- Die jeweilige Freitagssicherung wird als Vollsicherung des SAP-Servers mit ARCserve 2000 durchgeführt und einen Monat aufbewahrt, die letzte Freitagssicherung des Monates wird als Monatssicherung, jede 3. Monatssicherung wird als Quartalssicherung 12 Monate aufbewahrt.

- Nach entgültigem Abschluss des Geschäftsjahres (Mitteilung des Wirtschaftsprüfers) wird ausserhalb der o.g. Routinedatensicherung eine Sicherung erzeugt, die den gesetzlichen Anforderungen gem. GoBS entspricht.
- Bei Bedarf auch außerhalb dieser „Standardsicherungen", z.B. vor einem Release-Wechsel, Änderungen an der Systemeinstellung.

DM1

- Wöchentliche Sicherung (Montags) der Datenbank mit Informix Onbar –b –L 0 auf DLT-Band.
- Die Wochensicherung wird im 2-wöchigen Turnus aufbewahrt (3 Bänder).
- Die jeweilige Freitagssicherung wird als Vollsicherung des SAP-Servers mit ARCserve 2000 durchgeführt und einen Monat aufbewahrt, die letzte Freitags-sicherung des Monates wird als Monatssicherung 3 Monate aufbewahrt.
- Wochen aufbewahrt (3 Bänder).

SM1

- Eine Vollsicherung des SAP-Servers wird mit ARCserve 2000 nach Erzeugung der Mandantenkopie und sonstigem Bedarf durchgeführt und aufbewahrt (3 Bänder im Generationenprinzip).

7.2.2 Rettungsdisketten

Für jeden NT-Server werden Rettungsdisketten erstellt, die jeweils nach Systemänderungen erneuert werden.

7.2.3 Notfallkonzept

Der PM1 und DM1 sind identische Servertypen. Sie sind mit einem RAID-System und hot-spare-drives ausgestattet, haben doppelte Netzkarten sowie redundante Stromversorgungen und Lüfter. Das System wird mit dem RAID-Level 5 betrieben. Dies alles gewährleistet eine große hardwaretechnische Sicherheit der Systeme.

Bei Ausfall des PM1 wird der DM1 als Notfallserver für die Produktion zur Verfügung gestellt. Über das Einspielen der aktuellen Sicherungen kann der Zustand des PM1 auf dem DM1 abgebildet werden.

Quellen: BSI-IT-Grundschutzhandbuch, SAP R/3 Sicherheitskonzept.