Schulung IT-Grundschutz (in Anlehnung an BSI)

Version 1. 0

Beschreibung der Beispielschule Arminius-Gymnasium, Kalkriese

Stand: 22.04.06

Inhaltsverzeichnis:

1.Die Beispielschule Arminius-Gymnasium

Die Vorgehensweise bei der Anwendung des IT-Grundschutzhandbuchs soll ein Beispiel veranschaulichen und zwar ein Gymnasium mittlerer Größe, das selbstverständlich rein fiktiv ist. Es handelt sich dabei um das Arminius-Gymnasium in Kalkriese, das von ca. 1000 Schülern der Klassen 5 bis 13 besucht wird.

1.1.Organisatorische Gliederung

Die organisatorische Gliederung des Arminius-Gymnasiums gibt folgendes Organigramm wieder:

Schulleitung	
Verwaltung • Koordinatoren • Sekretariat • Haus- und Gebäudetechnik • Schulassistent	Lehre • Lehrer • Schüler

Es gibt keinen weiteren Standort als das Schulgebäude in Kalkriese.

Im Schulgebäude ist neben dem Arminius-Gymnasium auch ein RCC (Regionales Computer Centrum) für die Lehrerfortbildung untergebracht. Die vom RCC genutzten Räumlichkeiten sind von denen des Arminius-Gymnasiums getrennt. Mitarbeiter des RCC sind beauftragte Lehrer, der Leiter des RCC ist der Schulleiter des Arminius-Gymnasiums in Personalunion.

Darüber hinaus hat die Schule der Ehemaligenvereinigung gestattet, ihren Web-Server im Serverraum unterzustellen und über den DSL-Zugang der Schule den Online-Bereich zu publizieren.

1.2.Informationstechnik

Am Arminius-Gymnasium ist ein zentral administriertes **Schulnetz** mit insgesamt 83 angeschlossenen Arbeitsplätzen eingerichtet worden. Die Arbeitsplatzrechner sind mit den Betriebssystemen Windows 98 / 2000 / XP, üblichen Büro-Anwendungen (Standardsoftware für Textverarbeitung, Tabellenkalkulation und Präsentationen) sowie Internet-Browser und Lernsoftware ausgestattet. Zusätzlich gibt es je nach Aufgabengebiet auf verschiedenen Rechnern Spezialsoftware.

Im Schulnetz werden insgesamt 5 Server für folgende Zwecke eingesetzt:

- Ein Server stellt folgende Dienste bereit:
  1. Domänen-Controller,
  2. Dateiablage,
  3. Druckserver,
  4. Mailserver
  5. Proxyserver
  6. Internet-Filter

7. Web-Server
8. Sicherheitsgateway (Firewall)
9. Application-Server,

- ein weiterer Server dient ebenfalls als Application-Server,
- ein Server dient als Terminalserver (Linux),
- ein Server dient als Terminalserver (Windows 2003),
- der fünfte Server ist der Web-Server der Ehemaligenvereinigung.

Zum Schulnetz zählen auch die Schulungs-PCs im RCC sowie die PCs für die RCC-Mitarbeiter. Der Internet-Zugang im RCC erfolgt über einen eigenen DSL-Anschluss.

Das **Verwaltungsnetz** wird mit einem weiteren Server und 10 Arbeitsplatzrechnern vom Schulnetz getrennt betrieben. Der Server dient als Domänen-Controller sowie als Dateiserver für diesen IT-Verbund. Die Grundausstattung der Arbeitsplatzrechner im Verwaltungsnetz ist wesentlich einheitlicher:

- Betriebssystem: Windows XP
- Office-Paket
- Internet-Browser
- auf einigen PCs Spezialsoftware:
  - zur Verwaltung der Schüler-Stammdaten,
  - zur elektronischen Kontoführung,
  - zur Verwaltung der Lernmittel,
  - zur Verwaltung der gymnasialen Oberstufe,
  - zur Erstellung des Stundenplans,
  - zur Erstellung des Vertretungsplans.

Beide IT-Verbünde sind jeweils über eine eigene DSL-Leitung an das Internet angebunden. Der Internet-Zugang ist jeweils über eine Firewall und einen Router abgesichert. Alle Client-Rechner haben Zugang zum Internet.

Im Schulnetz wird dieser Zugang durch eine Filtersoftware beschränkt.

Die WWW-Seiten des Arminius-Gymnasiums werden auf dem landeseigenen Bildungsserver vorgehalten.

An zusätzlicher Informationstechnik sind zu berücksichtigen:

- Telekommunikationsanlagen im Verwaltungsnetz sowie im RCC
- 1 Faxgerät im Verwaltungsnetz (Standort: Sekretariat)

- 1 Laptop, der bei Bedarf via Netzwerkkabel oder WLAN in das Schulnetz eingebunden werden kann.

Für das reibungslose Funktionieren der Informationstechnik in beiden IT-Verbünden ist der dafür ernannte Fachobmann Informations- und Kommunikationstechnologien zuständig. Er wird im **Schulnetz** durch zwei Kollegen unterstützt, die als IT-Administratoren für die Benutzerverwaltung zuständig sind. Seitens der Schule wird nur der First-Level-Support wahrgenommen. Mit dem weiteren Support ist das Medienzentrum Osnabrück durch den Schulträger beauftragt. Grundlage dieser Beauftragung ist ein Leistungskatalog, welcher die Aufgabenverteilung detailliert festschreibt. Zum Umgang mit der Informationstechnik gibt es eine für alle Nutzer verbindliche Nutzerordnung, der zufolge die IT ausschließlich für unterrichtliche Zwecke genutzt werden darf.

Für den weitergehenden Support im **Verwaltungsnetz** ist der Schulträger zuständig. Beim Fachdienst Schule/Sport ist ein Mitarbeiter (derzeit: Herr Brune) der Ansprechpartner.

2.IT-Sicherheitsmanagement

Die Schulleitung beabsichtigt ein **IT-Sicherheitskonzept** für die Schule ausarbeiten zu lassen, das in allen Bereichen umgesetzt werden soll. Dazu müssen die Vorstellungen zur IT-Sicherheit und die vorhandenen Sicherheitsrichtlinien präzisiert werden. Zuerst wird für die Analysen, Konzepte und Folgearbeiten des IT-Sicherheitsprozesses ein **IT-Sicherheitsbeauftragter** ernannt. Da diese Aufgabe umfangreiche IT-Kenntnisse erfordert, wird hierfür der Fachobmann Informations- und Kommunikationstechnologien bestimmt. Danach wird ein **„IT-Sicherheitsmanagement“** eingerichtet, in dem neben dem IT-Sicherheitsbeauftragten der **Datenschutzbeauftragte** und **Zuständige für IT-Anwendungen und IT-Systeme** zu folgenden Ergebnissen zusammenarbeiten sollen:

- Vorschläge und Entscheidungsvorlage für eine IT-Sicherheitsleitlinie,
- Erstellung einer Übersicht vorhandener IT-Systeme,
- Ausarbeitung und Entscheidungsvorlage des IT-Sicherheitskonzepts und eines Realisierungsplans inklusive Maßnahmen zur Notfallvorsorge und Benutzerinformation,
- Vorschläge für Maßnahmen zur Aufrechterhaltung der IT-Sicherheit,
- Dokumentation aller Entscheidungsvorlagen, Entscheidungen und der umgesetzten Maßnahmen des IT-Sicherheitsprozesses.

Nach Vorarbeiten des IT-Sicherheitsbeauftragten und Beratungen des Projektteams „IT-Sicherheitskonzept“ werden folgende Vorschläge für die IT-Sicherheitsleitlinie mit der Schulleitung beraten:

2.1.Vorschläge für die IT-Sicherheitsleitlinie

2.1.1.Stellenwert der IT und Bedeutung der IT-Sicherheitsleitlinie

Erfolgreiches Arbeiten einer Schule setzt mittlerweile den Einsatz der Informationstechnik voraus. Die IT ist ein wichtiger, unterstützender Teil des Systems Schule.

Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind wesentliche Voraussetzungen für die Einhaltung der IT-Sicherheitsziele Verfügbarkeit, Integrität und Vertraulichkeit von Informationen.

Die Schulleitung hat aufgrund ihrer Verantwortung für die Informationssicherheit einen IT-Sicherheitsprozess in Gang gesetzt. Dazu gehören die Entwicklung und Umsetzung dieser Leitlinie und eines IT-Sicherheitskonzepts. Die Einhaltung der Leitlinie sowie Aktualität und Angemessenheit des Sicherheitskonzepts werden regelmäßig überprüft.

2.1.2.IT-Sicherheitsniveau und Ziele

Die Schulleitung schätzt die strategische und operative Bedeutung der Informationstechnik folgendermaßen ein:

Schwerpunkt der täglichen Arbeit im **Schulnetz** ist die Recherche, Bearbeitung und Präsentation von Informationen, die in digitaler Form vorliegen oder zur Verfügung gestellt werden. Es werden aber auch fachspezifische Anwendungsprogramme genutzt. Die Ergebnisse der Arbeit können individuell abgespeichert werden. Einige Anwendungsprogramme bieten die Möglichkeit einer fortlaufenden Speicherung der erbrachten Leistungen.

Im **Verwaltungsnetz** ist die Qualität der Arbeit abhängig von aktuellem und korrektem Datenmaterial, welches die Schule als Basis für die interne Kommunikation (Stundenplan, Raumplan, Vertretungsplan, Schulbuchausleihe, Listen etc.) und auch für die externe Kommunikation (Schulbehörde, Schulträger, Schülerbeförderung, Geldinstitute sowie weitere Institutionen) benötigt. Diese Daten werden zunehmend in elektronischer Form erstellt, bearbeitet und ausgetauscht.

In Abwägung der Gefährdungen, der Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für IT-Sicherheit, hat die Schulleitung bestimmt, dass

ein **niedriges (Schulnetz)** bzw. **niedriges bis mittleres (Verwaltungsnetz)**
IT-Sicherheitsniveau angestrebt werden soll.

Dieses Sicherheitsniveau bedingt folgende **Sicherheitsziele** und **Strategie**:

1. **Informationssicherheit** soll mit Sicherheitsbewusstsein der Beschäftigten bezüglich möglicher Gefährdungen und mit ihrem persönlich-verantwortlichen Verhalten praktiziert und mit organisatorischen und technischen Maßnahmen unterstützt werden. Dafür sollen regelmäßige Fortbildungsmaßnahmen zur IT-Sicherheit durchgeführt werden.
2. Die für die Schule wichtigen **Informationen** sollen gemäß ihrer Vertraulichkeit und bezüglich ihrer Integrität **geschützt** werden. Das bedeutet, dass auch im Umgang mit elektronischen Dokumenten und Daten Geheimhaltungsanweisungen strikt Folge zu leisten ist.
3. Die für die Schule relevanten **Gesetze** und **Vorschriften** sowie **vertragliche** und **aufsichtsrechtliche Verpflichtungen** müssen eingehalten werden.
4. Ziel ist, die **Sicherheit** der IT (gleichwertig neben Leistungsfähigkeit und Funktionalität) in der Schule aufrechtzuerhalten, so dass die benötigten Informationen **bei Bedarf verfügbar** sind. Ausfälle der IT haben Beeinträchtigungen des Schules zur Folge.
5. Durch Sicherheitsmängel im Umgang mit IT verursachte Ersatzansprüche, Schadensregulierungen und Image-Schäden müssen verhindert werden. [Kleinere Fehler können toleriert werden.]
6. In der Schule sollen für die **Zugangskontrolle** sowohl physikalische als auch logische Sicherheitsmaßnahmen angewandt werden.
7. Bereits betriebene und geplante **Informationstechnik** soll nach der Vorgehensweise des IT-Grundschutzhandbuchs des BSI in einem IT-Sicherheitskonzept erfasst, im Schutzbedarf eingeschätzt, modelliert und auf Sicherheitsmaßnahmen überprüft werden. Sicherheit der IT soll u. a. auch durch Anwenden von Normen und Standards und durch den Einsatz zertifizierter Systeme erreicht werden.

2.1.3.Verantwortungen

Das **IT-Sicherheitsmanagement** ist gemäß den Sicherheitsvorgaben verantwortlich für die Sicherheit im Umgang mit der IT und den Schutz aller Geschäftsinformationen. Ebenso ist es zuständig für die Weiterentwicklung des IT-Sicherheitsniveaus, des IT-Sicherheitskonzepts und für seine Umsetzung und Aufrechterhaltung von Sicherheit im Betrieb.

Jeder Nutzer soll im Rahmen seines Umgangs mit IT die erforderliche **Integrität** und **Vertraulichkeit** von Informationen und (wenn erforderlich) **Verbindlichkeit** und **Beweisbarkeit** von Geschäftskommunikation gewährleisten und die Richtlinien der Schule einhalten. Unterstützt durch sensibilisierende Schulung und Benutzerbetreuung soll jeder im Rahmen seiner Möglichkeiten, Sicherheitsvorfälle von innen und außen vermeiden. **Erkannte Fehler** sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

Ein „**Informationstreuhänder**“, der z. B. aufgrund eines Serviceauftrages für das Unternehmen Leistungen erbringt, hat diese IT-Sicherheitsleitlinie einzuhalten. Damit ist er verantwortlich für die Einhaltung der IT-Sicherheitsziele (Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Rechenschaftspflicht und Verbindlichkeit der Informationen). Bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen hat er das IT-Sicherheitsmanagement zu informieren.

2.1.4.Verstöße und Folgen

- Beabsichtigte oder grob fahrlässige Handlungen, die die Sicherheit von Daten, Informationen, Anwendungen, IT-Systemen oder des Netzes gefährden, werden als Verstöße verfolgt. Dazu gehören beispielsweise:
    - der Missbrauch von Daten, der finanziellen Verlust verursachen kann,
    - der unberechtigter Zugriff auf Informationen bzw. ihre Änderung und unbefugte Übermittlung,
    - die illegale Nutzung von Informationen aus der Schule,
    - die Gefährdung der IT-Sicherheit der Nutzer, Kooperationsspartner und der Schule sowie
    - die Schädigung des Rufes der Schule.

Bewusste Zuwiderhandlungen gegen die IT-Sicherheitsleitlinie werden bestraft – gegebenenfalls disziplinarisch, arbeitsrechtlich oder mit zivil- und strafrechtlichen Verfahren, in denen auch Haftungsansprüche und Regressforderungen erhoben werden können.

2.1.5.Geltungsbereich

Diese IT-Sicherheitsleitlinie gilt für die gesamte Schule. Jeder Mitarbeiter[1] ist daher verpflichtet, die IT-Sicherheitsleitlinie im Rahmen seiner Zuständigkeiten und Arbeiten einzuhalten und die Informationen und die Technik angemessen zu schützen.

Unter den Vorgaben dieser IT-Sicherheitsleitlinie und des Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnik, werden Ziele, Anforderungen, organisatorische und technische Sicherheitsmaßnahmen in dem IT-Sicherheitskonzept detailliert, geplant, dokumentiert und dann umgesetzt werden.

1 Mitarbeiter sind in diesem Sinne alle Nutzer der IT-Verbünde, insbesondere das Kollegium, nichtpädagogisches Personal, sowie Schülerinnen und Schüler.

2.2.Einführung der IT-Sicherheitsleitlinie in der Schule

Die Schulleitung lässt sich zu den Inhalten der IT-Sicherheitsleitlinie von dem IT-Sicherheitsbeauftragten und dem IT-Sicherheitsmanagement-Team ausgiebig beraten. Dann stellt sie die IT-Sicherheitsleitlinie in der Gesamtkonferenz vor. Nach Diskussion der Aussagen zur Bedeutung der IT und zum Sicherheitsniveau, der Sicherheitsziele, Strategieaussagen, organisatorischen Regelungen und Konsequenzen werden Vorschläge für Änderungen eingebracht. Nach einer Überarbeitung durch den IT-Sicherheitsbeauftragten lädt die Schulleitung alle Beschäftigten zu einer Versammlung ein (ggf. im Rahmen einer Gesamtkonferenz). Sie erläutert im Vortrag die Wichtigkeit der Leitlinie für das Schule und erklärt Ziele, Maßnahmen und Konsequenzen. Jeder Mitarbeiter bekommt eine schriftliche Ausfertigung der Leitlinie. Die Schulleitung kündigt eine Reihe von Fortbildungsveranstaltungen zur IT-Sicherheit an, damit die Mitarbeiter für mögliche Gefährdungen sensibilisiert und auf einzuhaltende IT-Sicherheitsmaßnahmen vorbereitet werden. Die Schulleitung gibt den Termin bekannt, ab dem die Leitlinie in Kraft gesetzt ist und verlangt ihre Einhaltung.

Weitere Informationen zum IT-Sicherheitsmanagement finden sich in Kapitel 3.0 des IT-Grundschutzhandbuchs.

3.IT-Strukturanalyse

Grundlage eines jeden IT-Sicherheitskonzepts ist eine genaue Kenntnis der im festgelegten IT-Verbund vorhandenen Informationstechnik, ihrer organisatorischen und personellen Rahmenbedingungen sowie ihrer Nutzung. Bei der IT-Strukturanalyse geht es darum, die dazu erforderlichen Informationen zusammenzustellen und so aufzubereiten, dass sie die weiteren Schritte bei der Anwendung des IT-Grundschutzhandbuchs unterstützen.

Dazu gehören die folgenden Arbeitsschritte:

1. Netzplanerhebung und Komplexitätsreduktion durch Gruppenbildung,
2. Erfassung der IT-Systeme sowie
3. Erfassung der IT-Anwendungen und der zugehörigen Informationen.

Weitere Informationen zur IT-Strukturanalyse finden sich in Kapitel 2.1 des IT-Grundschutzhandbuchs.

3.1.Netzplan

3.1.1.Erhebung

Ausgangspunkt für die IT-Strukturanalyse des Arminius-Gymnasiums ist der Netzplan in Abbildung 1 und 2 auf den folgenden Seiten. Um die Übersichtlichkeit zu bewahren, wurde darauf verzichtet, Geräte und Informationen in den Netzplan einzutragen, die bei den nachfolgenden Beschreibungen nicht weiter benötigt werden (zum Beispiel Netzdrucker, Sicherungslaufwerke, Netzadressen).

Da es sich bei der IT-Struktur des Arminius-Gymnasiums um zwei getrennte lokale Netzwerke handelt, werden hier zunächst einmal **zwei IT-Verbünde** (**Schulnetz, Verwaltungsnetz)** definiert, die auch in Teilen getrennt betrachtet werden. So findet sich zunächst in Abbildung 1 der Netzplan des IT-Verbunds **Schulnetz**. In Abbildung 2 ist der Netzplan des IT-Verbunds **Verwaltungsnetz** gezeigt.

3.1.2.Bereinigung

Nicht alle Informationen der IT-Erhebung sind für die nachfolgenden Schritte beim Vorgehen gemäß IT-Grundschutzhandbuch tatsächlich erforderlich. So können Komponenten zu einer Gruppe zusammengefasst werden, die

- vom gleichen Typ sind,
- gleich oder nahezu gleich konfiguriert sind,
- gleich oder nahezu gleich in das Netz eingebunden sind,
- den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen und
- die gleichen Anwendungen bedienen.

In den vorliegenden Netzplänen ist dieser Schritt vollzogen worden.

3.2.Erhebung IT-Systeme

Bei der Erhebung der IT-Systeme geht es darum, die vorhandenen und geplanten IT-Systeme und die sie jeweils charakterisierenden Angaben zusammenzustellen. Dazu zählen

- alle im Netz vorhandenen Computer (Clients und Server), Gruppen von Computern und aktiven Netzkomponenten, Netzdrucker, aber auch

- nicht vernetzte Computer wie Internet PCs und Laptops,
- Telekommunikationskomponenten wie TK-Anlagen, Faxgeräte, Mobiltelefone und Anrufbeantworter.

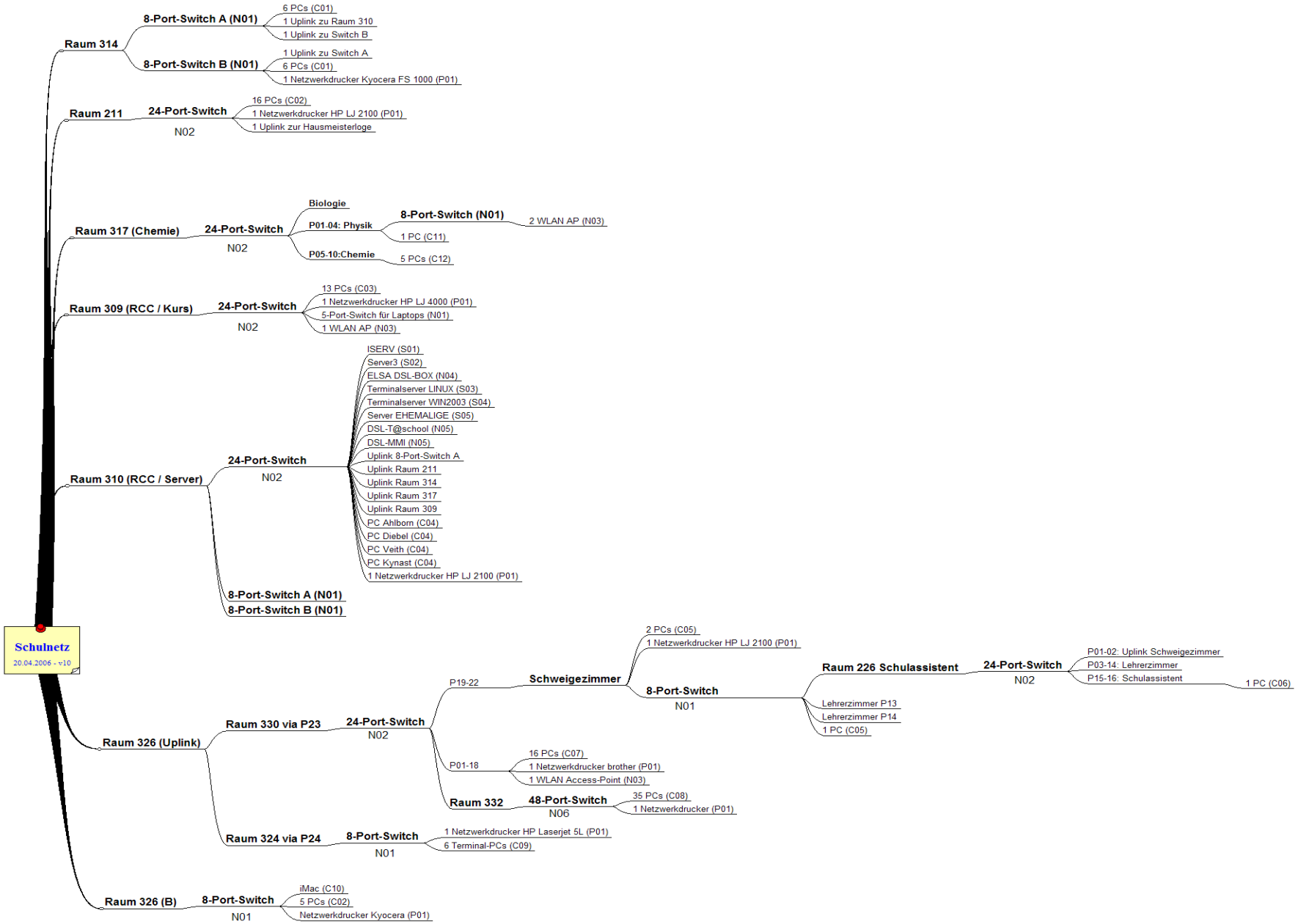
Aufgrund der damit verbundenen besseren Übersichtlichkeit empfiehlt sich eine tabellarische Darstellung, die folgende Angaben enthalten sollte:

- eindeutige Bezeichnung,
- Beschreibung (insbesondere der Einsatzzweck und der Typ, z. B. Server für Personalverwaltung, Router zum Internet),
- Plattform (Welcher Hardwaretyp, welches Betriebssystem?),
- Standort (Gebäude und Raumnummer),
- bei Gruppen: Anzahl der zusammengefassten IT-Systeme,
- Status (in Betrieb, im Test, in Planung) und
- Benutzer und Administrator[2].

Die Erhebung der IT-Systeme am Arminius-Gymnasium ergab die nachfolgend abgebildeten Übersichten.

Die IT-Systeme sind jeweils durchnummeriert. Ein vorangestellter Buchstabe kennzeichnet dessen Typ (S = Server, C = Client, N = Netzkomponente, T = Telekommunikationskomponente).

2 Die Zuständigkeiten sind für die IT-Verbünde einheitlich geregelt. Erster Ansprechpartner ist stets das IT-Sicherheitsmanagement. Es entscheidet über das weitere Vorgehen.


Schulnetz
20.04.2006 - v10
Raum 314
8-Port-Switch A (N01)
6 PCs (C01)
1 Uplink zu Raum 310
1 Uplink zu Switch B
8-Port-Switch B (N01)
1 Uplink zu Switch A
6 PCs (C01)
1 Netzwerkdrucker Kyocera FS 1000 (P01)
Raum 211
24-Port-Switch
N02
16 PCs (C02)
1 Netzwerkdrucker HP LJ 2100 (P01)
1 Uplink zur Hausmeisterloge
Raum 317 (Chemie)
24-Port-Switch
N02
Biologie
P01-04: Physik
8-Port-Switch (N01)
2 WLAN AP (N03)
1 PC (C11)
P05-10:Chemie
5 PCs (C12)
Raum 309 (RCC / Kurs)
24-Port-Switch
N02
13 PCs (C03)
1 Netzwerkdrucker HP LJ 4000 (P01)
5-Port-Switch für Laptops (N01)
1 WLAN AP (N03)
Raum 310 (RCC / Server)
24-Port-Switch
N02
ISERV (S01)
Server3 (S02)
ELSA DSL-BOX (N04)
Terminalserver LINUX (S03)
Terminalserver WIN2003 (S04)
Server EHEMALIGE (S05)
DSL-T@school (N05)
DSL-MMI (N05)
Uplink 8-Port-Switch A
Uplink Raum 211
Uplink Raum 314
Uplink Raum 317
Uplink Raum 309
PC Ahlborn (C04)
PC Diebel (C04)
PC Veith (C04)
PC Kynast (C04)
1 Netzwerkdrucker HP LJ 2100 (P01)
8-Port-Switch A (N01)
8-Port-Switch B (N01)
Raum 326 (Uplink)
Raum 330 via P23
24-Port-Switch
N02
P19-22
Schweigezimmer
2 PCs (C05)
1 Netzwerkdrucker HP LJ 2100 (P01)
8-Port-Switch
N01
Raum 226 Schulassistent
24-Port-Switch
N02
P01-02: Uplink Schweigezimmer
P03-14: Lehrerzimmer
P15-16: Schulassistent
1 PC (C06)
Lehrerzimmer P13
Lehrerzimmer P14
1 PC (C05)
P01-18
16 PCs (C07)
1 Netzwerkdrucker brother (P01)
1 WLAN Access-Point (N03)
Raum 332
48-Port-Switch
N06
35 PCs (C08)
1 Netzwerkdrucker (P01)
Raum 324 via P24
8-Port-Switch
N01
1 Netzwerkdrucker HP Laserjet 5L (P01)
6 Terminal-PCs (C09)
Raum 326 (B)
8-Port-Switch
N01
iMac (C10)
5 PCs (C02)
Netzwerkdrucker Kyocera (P01)

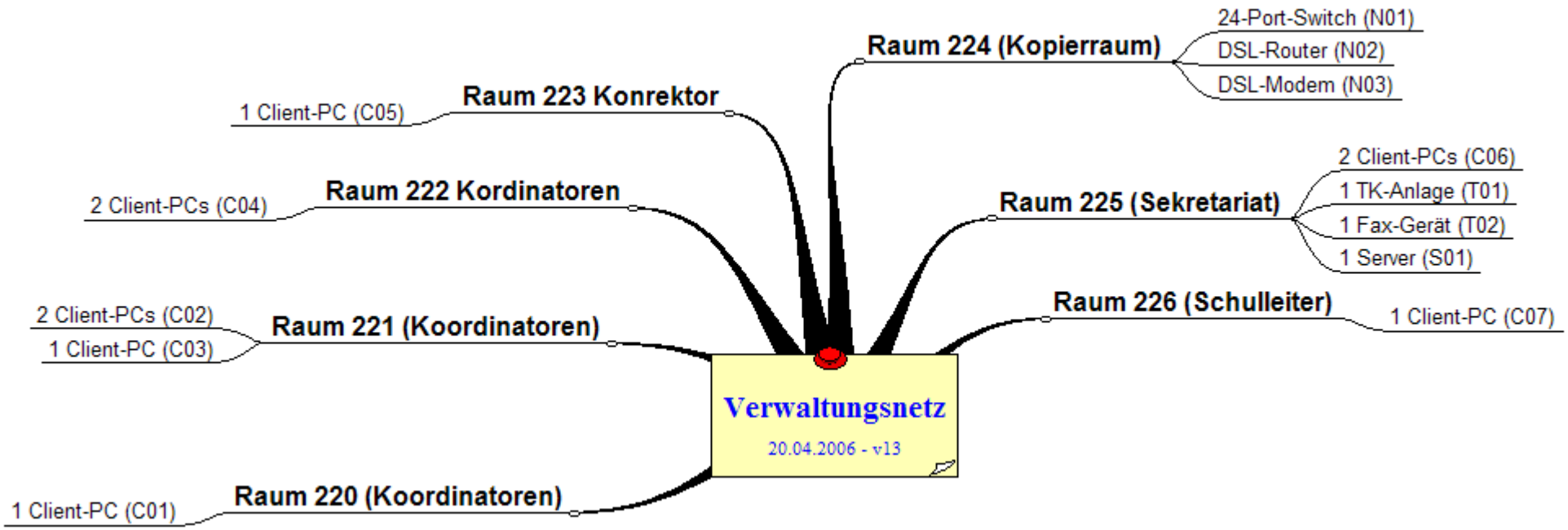
3.2.1.Übersicht Server, Clients, Netzkomponenten (Schulnetz)									
Nr.	**Beschreibung**	**Plattform**	**Anzahl**	**Raum**	**Status**	**Anwender**	**WLAN**	**BT**	**LAN (RJ45, 100 Mbit); 172.16.200.**
S01	Kommunikations- und Fileserver[3]	Linux	**1**	310	in Betrieb	alle	-----	-----	4
S02	Application-Server	WinNT 4	**1**	310	in Betrieb	alle	-----	-----	3
S03	Terminalserver	Linux	**1**	310	in Betrieb	alle	-----	-----	50
S04	Terminalserver	Win 2003	**1**	310	in Betrieb	alle	-----	-----	6
S05	Web-Server der EHEMALIGEN[4]	Linux	**1**	310	in Betrieb	Ehemalige	-----	-----	252
C01	Client-PC	Win 2000	**12**	314	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung
C02	Client-PC	Win XP	**21**	211 (16), 326 (5)	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung
C03	Client-PC	Win XP	**13**	309	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung
C04	Client-PC	Win 2000	**4**	310	in Betrieb	RCC	-----	-----	s. ISERV Rechnerverwaltung
C05	Client-PC	Win 2000	**3**	Schweigezimmer	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung
C06	Client-PC	Win XP	**1**	Schulassistent	in Betrieb	Schulass.	-----	-----	s. ISERV Rechnerverwaltung
C07	Client-PC	Win 98	**16**	330	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung
C08	*Client-PC*	*Win XP*	***35***	*332*	*geplant*	*alle*	***-----***	***-----***	***-----***
C09	Client-PC	Linux	**6**	324	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung
C10	Client-PC	Mac OS	**1**	326	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung

3 Es wird am Arminius-Gymnasium als zentraler Server das ISERV-System eingesetzt.

4 Der Server wird nur am Arminius-Gymnasium gehostet. Völlige Trennung von lokaler Benutzerverwaltung.

3.2.1.Übersicht Server, Clients, Netzkomponenten (Schulnetz)									
Nr.	**Beschreibung**	**Plattform**	**Anzahl**	**Raum**	**Status**	**Anwender**	**WLAN**	**BT**	**LAN (RJ45, 100 Mbit); 172.16.200.**
C11	Client-PC	Win 2000	**1**	Physik	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung
C12	Client-PC	Win 98	**5**	Chemie	in Betrieb	alle	-----	-----	s. ISERV Rechnerverwaltung
C13	Laptop	Win XP	**1**	Schulassistent	in Betrieb	alle	X	-----	s. ISERV Rechnerverwaltung
N01	8-Port-Switch		**9**	309, 314 (2), Physik, 310 (2), 324, 326, Schweigezimmer	in Betrieb	alle	-----	-----	-----
N02	24-Port-Switch		**6**	211, 317, 309, 310, 330, Schulassistent	in Betrieb	alle	-----	-----	-----
N03	WLAN AP		**4**	Physik (2), 309, 330	in Betrieb	alle	X	-----	s. ISERV Rechnerverwaltung
N04	DSL-Router		**1**	310	in Betrieb	RCC	-----	-----	254
N05	DSL-Modem		**2**	310	in Betrieb	alle	-----	-----	-----
N06	*48-Port-Switch*		***1***	*332*	*geplant*	*alle*	-----	-----	-----
T01	TK-Anlage		**1**	310	in Betrieb	RCC	-----	-----	-----

Art der Verkabelung: 100 Mbit / WLAN (IEEE 802.11) / **Netzprotokolle**: TCP/IP / **WAN-Anbindung**: T@school (Deutsche Telekom)


Verwaltungsnetz
20.04.2006 - v13
Raum 224 (Kopierraum)
24-Port-Switch (N01)
DSL-Router (N02)
DSL-Modem (N03)
Raum 223 Konrektor
1 Client-PC (C05)
Raum 222 Kordinatoren
2 Client-PCs (C04)
Raum 225 (Sekretariat)
2 Client-PCs (C06)
1 TK-Anlage (T01)
1 Fax-Gerät (T02)
1 Server (S01)
Raum 221 (Koordinatoren)
2 Client-PCs (C02)
1 Client-PC (C03)
Raum 226 (Schulleiter)
1 Client-PC (C07)
Raum 220 (Koordinatoren)
1 Client-PC (C01)

3.2.2.Übersicht Server, Clients, Netzkomponenten (Verwaltungsnetz)

Nr.	Beschreibung	Plattform	Anzahl	Raum	Status	Anwender	WLAN	BT	LAN (RJ45, 100 Mbit); 192.168.1.
S01	W2KServer	Windows 2000	**1**	325 (Sekretariat)	in Betrieb	alle	-----	-----	2
C01	Client-PC	Win XP	**1**	320	in Betrieb	NN	-----	-----	s. Rechnerliste
C02	Client-PC	Win XP	**2**	321	in Betrieb	NN, NN	-----	-----	s. Rechnerliste
C03	Client-PC	Win XP	**1**	321	in Betrieb	NN	-----	-----	s. Rechnerliste
C03	Client-PC	Win XP	**2**	322	in Betrieb	NN, NN	-----	-----	s. Rechnerliste
C04	Client-PC	Win XP	**1**	323	in Betrieb	Stellv. SL	-----	-----	s. Rechnerliste
C05	Client-PC	Win XP	**2**	325 (Sekretariat)	in Betrieb	NN, NN	-----	-----	s. Rechnerliste
C06	Client-PC	Win XP	**1**	326	in Betrieb	SL	-----	-----	s. Rechnerliste
N01	24-Port-Switch		**1**	324 (Kopierraum)	in Betrieb	alle	-----	-----	-----
N02	DSL-Router		**1**	324 (Kopierraum)	in Betrieb	alle	-----	-----	1
N03	DSL-Modem		**2**	324 (Kopierraum)	in Betrieb	alle	-----	-----	-----
T01	TK-Anlage		**1**	325 (Sekretariat)	in Betrieb	alle	-----	-----	-----
T02	Fax-Gerät		**1**	325 (Sekretariat)	in Betrieb	alle	-----	-----	-----

Art der Verkabelung: 100 Mbit / **Netzprotokolle**: TCP/IP / **WAN-Anbindung**: Osnatel

3.3.Erhebung IT-Anwendungen

3.3.1.Erhebung IT-Anwendungen (Schulnetz)

Bei der Erhebung der IT-Anwendungen werden die wichtigsten Anwendungen einer Organisation erfasst, also diejenigen

- deren Daten, Informationen und Programme den höchsten Bedarf an Geheimhaltung (Vertraulichkeit) haben,
- deren Daten, Informationen und Programme den höchsten Bedarf an Korrektheit und Unverfälschtheit (Integrität) haben oder
- die die kürzeste tolerierbare Ausfallzeit (höchster Bedarf an Verfügbarkeit) haben.

Unter Berücksichtigung der Auskünfte der Benutzer und fachlich Verantwortlichen wurden im IT-Verbund **Schulnetz** die folgenden Anwendungen in diesem Sinne als wesentlich identifiziert:

A01 Benutzerauthentisierung am LAN bzw. am Server der Ehemaligenvereinigung[5]

A02 Internet-Zugang

A03 Office-Anwendungen (Textverarbeitung, Tabellenkalkulation, Präsentation)

A04 Fachspezifische Software

A05 Zentrale Dateiablage

A06 E-Mail

A07 Sicherheitsgateway (Firewall)

A08 Druckservice

A09 Online-Datenbank der EHEMALIGEN

In den folgenden Tabellen sind die Anwendungen den Servern, Clients, Netz- und Telekommunikationskomponenten zugeordnet, die für deren Ausführung erforderlich sind. Zusätzlich ist für jede IT-Anwendung vermerkt, ob sie personenbezogene Daten verarbeitet oder nicht.

a) Zuordnung der Anwendungen zu den Servern (IT-Verbund **Schulnetz**)

Nr.	Beschreibung	Personenbezogene Daten	S01	S02	S03	S04	S05
A01	Benutzerauthentisierung	X	X				X
A02	Internet-Zugang		X				
A03	Office-Anwendungen						
A04	Fachspezifische Software	X[6]	X	X			
A05	Zentrale Dateiablage		X				

5 Der Server wird nur am Arminius-Gymnasium gehostet. Die Verwaltung und Betreuung ist von derjenigen des Schulnetzes völlig getrennt. Der Server ist ein reiner Web-Server, auch die Benutzerverwaltung wird über ein Web-Interface erledigt.

6 Personenbezogene Daten liegen hier nur vor, wenn die Software den erreichten Leistungsstand abspeichert. Das ist beispielsweise bei Cornelsens English Coach (zentral, auf S01 oder S02) möglich.

a) Zuordnung der Anwendungen zu den Servern (IT-Verbund **Schulnetz**)							
Nr.	Beschreibung	Personenbezogene Daten	S01	S02	S03	S04	S05
A06	E-Mail	X	X				
A07	Sicherheitsgateway (Firewall)		X				
A08	Druckservice		X				
A90	Online-DB der Ehemaligen	X					X

b) Zuordnung der Anwendungen zu den Clients (IT-Verbund **Schulnetz**)			
Nr.	Beschreibung	Personenbezogene Daten	C1 bis C 13[7]
A01	Benutzerauthentisierung	X	-----
A02	Internet-Zugang	-----	X
A03	Office-Anwendungen	-----	X
A04	Fachspezifische Software	X[8]	X
A05	Zentrale Dateiablage	-----	-----
A06	E-Mail	X	-----[9]
A07	Firewall	-----	-----
A08	Druckservice	-----	X
A09	Online-DB der Ehemaligen	X	X

c) Zuordnung der Anwendungen zu den Netz- und Telekommunikationskomponenten (IT-Verbund **Schulnetz**)								
Nr.	Beschreibung	Pers.-bez. Daten	N01	N02	N03	N04	N05	T01
A01	Benutzerauthentisierung	X	X	X	X	X	X	
A02	Internet-Zugang		X	X	X	X	X	
A03	Office-Anwendungen		X	X	X	X	X	

7 Da die Client-Gruppen sich nur hinsichtlich des Betriebssystems sowie der jeweiligen Fach-Software unterscheiden, können alle Clients hier als Einheit betrachtet werden.

8 Personenbezogene Daten liegen hier nur vor, wenn die Software den erreichten Leistungsstand abspeichert. Das ist beispielsweise bei Cornelsens English Coach (zentral auf S01 oder S02) möglich.

9 Es ist auf den Client-PCs keine E-Mail Software installiert. Zugriff auf E-Mails ist nur aus dem Browser über ein Web-Interface (verschlüsselt) möglich.

c) Zuordnung der Anwendungen zu den Netz- und Telekommunikationskomponenten (IT-Verbund **Schulnetz**)								
Nr.	Beschreibung	Pers.-bez. Daten	N01	N02	N03	N04	N05	T01
A04	Fachspezifische Software	X[10]	X	X	X	X	X	
A05	Zentrale Dateiablage		X	X	X	X	X	
A06	E-Mail	X	X	X	X	X	X	
A07	Firewall		X	X	X	X	X	
A08	Druckservice		X	X	X	X	X	
A09	Online-DB der Ehemaligen	X	X	X	X	X	X	

3.3.2.Erhebung IT-Anwendungen (Verwaltungsnetz)

Unter Berücksichtigung der Auskünfte der Benutzer und fachlich Verantwortlichen wurden im IT-Verbund **Verwaltungsnetz** die folgenden Anwendungen in diesem Sinne als wesentlich identifiziert:

A01 Benutzerauthentisierung

A02 Office-Anwendungen (Textverarbeitung, Tabellenkalkulation, Präsentation)

A03 Stammdaten-Verwaltung (Schüler)

A04 Elektronische Kontoführung

A05 Schulbuchausleihe

A06 Leistungsdaten-Verwaltung Oberstufe

A07 Kursplanung Oberstufe

A08 Allgemeiner Stunden- und Raumplan

A09 Vertretungsplan

A10 Zentrale Dateiablage

A11 Internet-Zugang

A12 E-Mail,

A13 Firewall

A14 Anti-Virus Software

A15 TK-Vermittlung

A16 Fax-Versand und -Empfang

In den folgenden Tabellen sind die Anwendungen den Servern, Clients, Netz- und Telekommunikationskomponenten zugeordnet, die für deren Ausführung erforderlich sind. Zusätzlich ist für jede IT-Anwendung vermerkt, ob sie personenbezogene Daten verarbeitet oder nicht.

10 Personenbezogene Daten liegen hier nur vor, wenn die Software den erreichten Leistungsstand abspeichert. Das ist beispielsweise bei Cornelsens English Coach (zentral auf S01 oder S02) möglich.

a) Zuordnung der Anwendungen zu den Servern (IT-Verbund **Verwaltungsnetz**)			
Nr.	Beschreibung	Personenbezogene Daten	S01
A01	Benutzerauthentisierung	X	X
A02	Office-Anwendungen		
A03	Stammdaten-Verwaltung	X	X
A04	Elektr. Kontoführung	X	
A05	Schulbuchausleihe	X	
A06	Leistungsdaten Oberstufe	X	
A07	Kursplanung Oberstufe	X	
A08	Stunden- und Raumplan		
A09	Vertretungsplan	X	
A10	Zentrale Dateiablage		X
A11	Internet-Zugang		
A12	E-Mail	X	
A13	Firewall		
A14	Anti-Virus Software		
A15	TK-Vermittlung		
A16	Fax-Versand und -Empfang		

b) Zuordnung der Anwendungen zu den Clients (IT-Verbund **Verwaltungsnetz**)									
Nr.	Beschreibung	Personenbezogene Daten	C01	C02	C03	C04	C05	C06	C07
A01	Benutzerauthentisierung	X							
A02	Office-Anwendungen		X	X	X	X	X	X	X
A03	Stammdaten-Verwaltung	X	X	X	X	X	X	X	X
A04	Elektr. Kontoführung	X						X	
A05	Schulbuchausleihe	X			X				
A06	Leistungsdaten Oberstufe	X		X	X		X		X

b) Zuordnung der Anwendungen zu den Clients (IT-Verbund **Verwaltungsnetz**)									
Nr.	Beschreibung	Personen-bezogene Daten	C01	C02	C03	C04	C05	C06	C07
A07	Kursplanung Oberstufe	X		X	X		X		X
A08	Stunden- und Raumplan	X				X			
A09	Vertretungsplan	X				X			
A10	Zentrale Dateiablage								
A11	Internet-Zugang		X	X	X	X	X	X	X
A12	E-Mail	X						X[11]	
A13	Firewall								
A14	Anti-Virus Software		X	X	X	X	X	X	X
A15	TK-Vermittlung								
A16	Fax-Versand und Empfang								

c) Zuordnung der Anwendungen zu den Netz- und Telekommunikationskomponenten (IT-Verbund **Verwaltungsnetz**)							
Nr.	Beschreibung	Pers.-bez. Da-ten	N01	N02	N03	T01	T02
A01 bis A14	Alle Anwendungen[12]	X	X	X	X		
A15	TK-Vermittlung					X	
A16	Fax-Versand und -Empfang						X

11 Nur auf dem Client-Typ C05 ist eine E-Mail-Software installiert. Nur dort werden E-Mails gespeichert. Alle anderen Plätze müssen E-Mail-Verkehr über ein Web-Interface verschlüsselt abwickeln. Lokale Speicherung von E-Mails ist den anderen Clients nicht gestattet.

12 Da es sich um ein großes Netzwerk handelt, das nicht in Teilnetze unterteilt ist, können an dieser Stelle aus Gründen der Vereinfachung alle Anwendungen in gleicher Weise betrachtet werden.

4.Schutzbedarfsfeststellung

4.1.Schutzbedarfsfeststellung (Schulnetz)

Wie viel Schutz benötigen die Informationstechnik und die durch diese unterstützten Anwendungen? Wie kommt man zu begründeten und nachvollziehbaren Einschätzungen des Schutzbedarfs? Welche Komponenten der Informationstechnik benötigen mehr Sicherheit, bei welchen genügen elementare Schutzmaßnahmen? Ziel der Schutzbedarfsfeststellung ist es, diese Fragen zu klären und damit die Auswahl **angemessener Sicherheitsmaßnahmen** für die verschiedenen Komponenten der Informationstechnik (Systeme, Anwendungen, Räume, Kommunikationsverbindungen) zu unterstützen. Zur Schutzbedarfsfeststellung gehören die folgenden Aktivitäten:

1. die auf Ihre Organisation zugeschnittene Definition von Schutzbedarfskategorien (z. B. „niedrig bis mittel“, „hoch“, „sehr hoch“),
2. die Schutzbedarfsfeststellung der in der IT-Strukturanalyse erfassten Anwendungen mit Hilfe der festgelegten Kategorien,
3. die Ableitung des Schutzbedarfs der IT-Systeme aus dem Schutzbedarf der Anwendungen,
4. daraus abgeleitet die Feststellung des Schutzbedarfs der Kommunikationsverbindungen und IT-genutzten Räume und
5. die Dokumentation und Auswertung der vorgenommenen Einschätzungen.

Weitere Informationen zum Vorgehen bei der Schutzbedarfsfeststellung finden sich in Kapitel 2.2 des IT-Grundschutzhandbuchs.

4.1.1.Anpassung der Schutzbedarfskategorien

Für den IT-Verbund **Schulnetz** wurden die Schutzbedarfskategorien vom zuständigen IT-Sicherheitsmanagement folgendermaßen definiert und mit der Schulleitung abgestimmt:

- **Schutzbedarfskategorie niedrig bis mittel (I):**

  Ein möglicher Schaden hätte nur begrenzte und überschaubare Auswirkungen auf das Arminius-Gymnasium :

  - Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen allenfalls geringfügige juristische Konsequenzen oder Konventionalstrafen.
  - Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten nur geringfügige Auswirkungen auf die davon Betroffenen und würden von diesen toleriert.
  - Die persönliche Unversehrtheit wird nicht beeinträchtigt.
  - Die Abläufe am Arminius-Gymnasium werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.
  - Das Ansehen der Schule bei den Eltern und in der Öffentlichkeit wird nicht beeinträchtigt.

- **Schutzbedarfskategorie hoch (II):**

  Ein möglicher Schaden hätte beträchtliche Auswirkungen auf das Arminius-Gymnasium :

  - Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen schwerwiegende juristische Konsequenzen oder hohe Konventionalstrafen.

- Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten beträchtliche Auswirkungen auf die davon Betroffenen und würden von diesen nicht toleriert.

- Die persönliche Unversehrtheit wird nicht beeinträchtigt.

- Die Abläufe am Arminius-Gymnasium werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.

- Das Ansehen der Schule bei den Eltern und in der Öffentlichkeit wird erheblich beeinträchtigt.

- **Schutzbedarfskategorie sehr hoch (III):**

Ein möglicher Schaden hätte katastrophale Auswirkungen:

- Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen juristische Konsequenzen oder Konventionalstrafen, welche die Existenz der Schule gefährden.

- Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten ruinöse Auswirkungen auf die gesellschaftliche oder wirtschaftliche Stellung der davon Betroffenen.

- Die persönliche Unversehrtheit wird nicht beeinträchtigt.

- Die Abläufe am Arminius-Gymnasium werden so stark beeinträchtigt, dass Ausfallzeiten, die über 2 Stunden hinausgehen, nicht toleriert werden können.

- Das Ansehen der Schule bei den Eltern und in der Öffentlichkeit wird grundlegend und nachhaltig beschädigt.

4.1.2.Schutzbedarfsfeststellung der IT-Anwendungen

Bei der Schutzbedarfsfeststellung der IT-Anwendungen ist für alle in der IT-Strukturanalyse erfassten Anwendungen und differenziert nach den drei Grundwerten Vertraulichkeit (A), Integrität (B) und Verfügbarkeit (C) eine Zuordnung zu den zuvor festgelegten Schutzbedarfskategorien vorzunehmen.

Die folgende Tabelle zeigt die Zuordnungen, die für den IT-Verbund **Schulnetz** vorgenommen wurden:

IT-Anwendung (IT-Verbund Schulnetz)			Schutzbedarfsfeststellung		
Nr.	Bezeichnung	PD[13]	GW[14]	SB[15]	Begründung
A01	Benutzer-authentisierung	X	A	I	Die Passwörter sind verschlüsselt gespeichert und damit praktisch nicht zugänglich.
			B	II	Der hohe Schutzbedarf ergibt sich daraus, dass sich alle Mitarbeiter hierüber identifizieren.
			C	II	Bei Ausfall dieser Anwendung sind keine Identifizierung und damit keine Ausführung von IT-Verfahren möglich. Ein Ausfall ist allenfalls bis zu 24 Stunden tolerabel.
A02	Internet-Zugang		A	I	Es werden keine vertraulichen Daten verarbeitet.
			B	I	Fehlerhafte Daten können in der Regel leicht erkannt werden.
			C	II	Ein Ausfall ist höchstens 24 Stunden hinnehmbar.
A03	Office-Anwendungen		A	I	Es werden keine vertraulichen Daten verarbeitet.
			B	I	Fehlerhafte Daten können leicht erkannt und korrigiert werden. Es sind keine finanziellen Schäden zu erwarten.
			C	I	Der Ausfall auf einem Client ist bis zu einer Woche hinnehmbar. Ersatzweise kann auf einem Laptop weitergearbeitet werden.

13 PD = Personenbezogene Daten

14 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

15 SB = Schutzbedarf

IT-Anwendung (IT-Verbund Schulnetz)			Schutzbedarfsfeststellung		
Nr.	Bezeichnung	PD	GW	SB	Begründung
A04	Fachspezifische Software[16]	X	A	I	Die gespeicherten Leistungsdaten sind per individuellem Passwort geschützt. Die Passwörter sind nicht im Klartext gespeichert.
			B	I	Die gespeicherten Leistungsdaten können anteilig in die Gesamtnote einfließen.
			C	I	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
A05	Zentrale Dateiablage		A	I	Die hier gespeicherten Dateien sind nicht vertraulich. Sie werden zum Teil sogar öffentlich gemacht.
			B	I	Fehler werden in der Regel schnell erkannt und können nachträglich bereinigt werden.
			C	I	Bei Ausfall des Dienstes können die Dokumente auf den Client-PCs zwischengespeichert und bei Verfügbarkeit übertragen werden.
A06	E-Mail	X	A	I	Zugang zu E-Mails nur über verschlüsselte Verbindung via Web-Interface. Keine E-Mail-Software lokal installiert.
			B	II	Die Integrität dieser Informationen ist zu schützen. Einziger Aufbewahrungsort ist der E-Mail-Server (S01).
			C	II	Ausfallzeit nur unter 24 Stunden.
A07	Firewall		A	I	Über diesen Dienst werden keine vertraulichen Daten geleitet.
			B	II	Einbrüche in das Schulnetz müssen verhindert werden. Es könnten vertrauliche Daten kompromittiert werden.
			C	II	Ein Ausfall ist höchstens für 24 Stunden hinnehmbar.

16 Personenbezogene Daten liegen hier nur vor, wenn die Software den erreichten Leistungsstand (zentral) abspeichert. Das ist beispielsweise bei Cornelsens English Coach möglich.

IT-Anwendung (IT-Verbund Schulnetz)			Schutzbedarfsfeststellung		
Nr.	Bezeichnung	PD	GW	SB	Begründung
A08	Druckservice		A	I	Es werden keine vertraulichen Daten verarbeitet.
			B	I	Fehlerhafte Ausdrucke sind schnell zu identifizieren.
			C	I	Es besteht in dringenden Fällen die Möglichkeit zum Ausdruck an lokalen Druckern im RCC.
A09	Online-DB der Ehemaligen		A	I	Die Passwörter sind verschlüsselt gespeichert und damit praktisch nicht zugänglich.
			B	II	Alle Mitglieder müssen sich an diesem Server anmelden.
			C	I	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.

4.1.3. Schutzbedarfsfeststellung der IT-Systeme

Der Schutzbedarf eines IT-Systems hängt im Wesentlichen von dem Schutzbedarf derjenigen Anwendungen ab, für deren Ausführung es benötigt wird. Der Schutzbedarf der Anwendung vererbt sich auf den Schutzbedarf des IT-Systems. Bei der Vererbung lassen sich folgende Fälle unterscheiden:

- In **vielen** Fällen lässt sich der höchste Schutzbedarf aller Anwendungen, die das IT-System benötigen, übernehmen (**Maximumprinzip**).
- Der Schutzbedarf des IT-Systems kann höher sein als der Schutzbedarf der einzelnen **Anwendungen** (**Kumulationseffekt**). Dies ist z. B. dann der Fall, wenn auf einem Server mehrere Anwendungen mit mittlerem Schutzbedarf in Betrieb sind. Der Ausfall einer dieser Anwendungen könnte überbrückt werden. Wenn aber alle Anwendungen gleichzeitig ausfallen würden, dann kann ein hoher Schaden entstehen.
- Der Schutzbedarf kann niedriger sein als der Schutzbedarf der zugeordneten Anwendungen, wenn eine Anwendung mit hohem Schutzbedarf auf mehrere Systeme verteilt ist, und auf dem betreffenden IT-System nur weniger wichtige Teile dieser Anwendung ausgeführt werden (**Verteilungseffekt**). Bei Anwendungen, die personenbezogene Daten verarbeiten, sind z. B. Komponenten, in denen die Daten nur in pseudonymisierter oder aggregierter Form verwendet werden, weniger kritisch.

Auch der Schutzbedarf für die IT-Systeme sollte für jeden der drei Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit) festgelegt und anschließend z. B. tabellarisch dokumentiert werden.

Die folgenden Tabellen enthalten die Schutzbedarfsfeststellung für die Server, Clients, Netz- und Telekommunikationskomponenten im IT-Verbund **Schulnetz**.

a) Schutzbedarf Server (IT-Verbund **Schulnetz**)[17]

IT-System IT-Verbund Schulnetz		Schutzbedarfsfeststellung		
Nr.	Beschreibung	GW[18]	SB[19]	Begründung
S01	Kommunikations- und Fileserver ISERV	A	I	Gemäß Maximumprinzip
		B	II	Gemäß Maximumprinzip (A01, A06, A07)
		C	II	Gemäß Maximumprinzip (A01, A02, A06, A07)
S02	Application-Server	A	I	Gemäß Maximumprinzip
		B	I	Gemäß Maximumprinzip
		C	I	Gemäß Maximumprinzip
S05	Web-Server EHEMALIGE	A	I	Gemäß Maximumprinzip (A01)
		B	II	Gemäß Maximumprinzip (A01)
		C	II	Gemäß Maximumprinzip (A01)

b) Schutzbedarf Clients (IT-Verbund **Schulnetz**)

IT-System IT-Verbund Schulnetz		Schutzbedarfsfeststellung		
Nr.	Beschreibung	GW[20]	SB[21]	Begründung
C*nn*	alle Client-PCs	A	I	Gemäß Maximumprinzip ist der Schutzbedarf der Client-PCs mit „niedrig bis mittel“ einzustufen.
		B	I	Gemäß Maximumprinzip ist der Schutzbedarf der Client-PCs mit „niedrig bis mittel“ einzustufen.
		C	I	Gemäß A02 ist der Schutzbedarf als hoch einzustufen. Da aber in den PC-Räumen jeweils mehrere Client-PCs zur Verfügung stehen, kann der Ausfall eines Rechners bis zu einer Woche toleriert werden. Der Schutzbedarf ist daher gemäß Verteilungseffekt geringer einzustufen.

17 Die Server S03 und S04 sind aufgrund ihrer Funktionalität als Terminalserver nur in die Gruppe der Client-PCs einzuordnen.

18 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

19 SB = Schutzbedarf

20 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

21 SB = Schutzbedarf

c) Schutzbedarf Netzkomponenten (IT-Verbund **Schulnetz**)

IT-System IT-Verbund Schulnetz		Schutzbedarfsfeststellung		
Nr.	Beschreibung	GW[22]	SB[23]	Begründung
N*nn*	alle Netzkomponenten	A	I	Alle aktiven Netzkomponenten sind nicht konfigurierbar. Daher können auch keine Manipulationen vorgenommen werden, die eine Manipulation der übertragenen Daten zur Folge hätten. Die Benutzerauthentisierung erfolgt verschlüsselt, ebenso soll das Aufrufen der E-Mails im Browser über eine sichere Verbindung (SSL / https) erfolgen.
		B	I	Fehler in den übertragenen Daten werden leicht erkannt und korrigiert.
		C	II	Ein Ausfall erscheint höchstens bis zu 24 Stunden tolerabel.

d) Schutzbedarf Telekommunikationskomponenten (IT-Verbund **Schulnetz**)

IT-System IT-Verbund Schulnetz		Schutzbedarfsfeststellung		
Nr.	Beschreibung	GW[24]	SB[25]	Begründung
T01	TK-Anlage RCC	A	I	Die Anlage wird von 2 Apparaten aus exclusiv für ausgehende Telefonate genutzt. Anrufe werden stets von der Telekom auf eine Mobilfunk-Nummer geleitet.
		B	I	Störungen sind sofort erkennbar.
		C	I	Telefonanrufe können im Notfall auch via Handy oder über das Sekretariat des Arminius-Gymnasiums erledigt werden.

4.1.4.Schutzbedarf der Kommunikationsverbindungen

Im nächsten Arbeitsschritt geht es darum, den Schutzbedarf für die Kommunikationsverbindungen festzustellen. Es gibt Verbindungen, die gefährdeter sind als andere und durch doppelte Auslegung oder durch besondere Maßnahmen gegen Angriffe von außen oder innen geschützt werden müssen.

Als kritische **Verbindungen** gelten:

22 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

23 SB = Schutzbedarf

24 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

25 SB = Schutzbedarf

- **Verbindungen**, die aus der Schule **in ein öffentliches Netz** (z. B. Telefonnetz, Internet) oder **über ein öffentliches Gelände** reichen. Über solche Verbindungen können Computer-Viren und trojanische Pferde in das Schulnetz eingeschleust werden, Schulserver angegriffen werden oder Mitarbeiter vertrauliche Daten an Nichtbefugte weiterleiten.

- Verbindungen, über die besonders **schützenswerte Informationen** übertragen werden. Mögliche Gefährdungen sind Abhören, vorsätzliche Manipulation und betrügerischer Missbrauch. Vom Ausfall solcher Verbindungen sind Anwendungen, für die eine hohe Verfügbarkeit erforderlich ist, besonders betroffen.

- **Verbindungen**, über die vertrauliche Informationen **überhaupt nicht übertragen werden dürfen**. Personaldaten dürfen zum Beispiel nur von der Schulleitung eingesehen und bearbeitet werden. Daher muss verhindert werden, dass diese Daten bei ihrer Übertragung von unbefugten Mitarbeitern eingesehen werden können.

Im IT-Verbund **Schulnetz** werden über die Kommunikationsverbindungen keine besonders schützenswerten Daten unverschlüsselt übertragen. Daher existieren auch keine Verbindungen, über die vertrauliche Daten überhaupt nicht übertragen werden dürfen.

- **Die direkten Verbindungen vom Server S01 und dem DSL-Router N04 ins Internet können als kritische Verbindungen bezeichnet werden.**

- **Auch die Verbindungen der WLAN-Access Points N03 ins LAN müssen potentiell als kritisch bezeichnet werden, da eine Nutzung vom Außenbereich der Schule aus nicht sicher ausgeschlossen werden kann.**

4.1.5.Schutzbedarfsfeststellung der IT-genutzten Räume

Bei der Schutzbedarfsfeststellung für Räume werden sowohl Räume berücksichtigt,

- die zum Betrieb von IT-Systemen dienen (z. B. Serverräume, Räume für eine TK-Anlage und andere Räume mit technischer Infrastruktur), als auch

- in denen IT-Systeme genutzt werden (z. B. Büroräume).

Der Schutzbedarf eines Raumes bemisst sich nach dem Schutzbedarf der IT-Systeme, die sich in diesem Raum befinden. Auch hier können Sie (wie schon bei der Schutzbedarfsfeststellung der IT-Systeme) wieder im Allgemeinen das Maximumprinzip anwenden. Befinden sich jedoch in einem Raum mehrere Systeme, dann kann sich für den Raum ein höherer Schutzbedarf als für jedes einzelne IT-System ergeben (Kumulationseffekt). Dies gilt z. B. für Serverräume.

Die folgende Tabelle zeigt das Ergebnis der Schutzbedarfsfeststellung für die IT-genutzten Räume im IT-Verbund **Schulnetz**. Der Schutzbedarf der Räume wird hier festgelegt nach dem jeweils höchsten Schutzbedarf der darin installierten Systeme (Maximumprinzip).

IT-Verbund Schulnetz Raum		IT	Schutzbedarf		
Nr.	Art	Installierte IT	Vertraulichkeit	Integrität	Verfügbarkeit
211, 309, 314, 324, 326, 330, 332	Schulungsraum	Nnn, Cnn	niedrig bis mittel	niedrig bis mittel	hoch
PHY, CHE	Büroraum (Sammlung)	Nnn, Cnn	s. o.	s. o.	s. o.

IT-Verbund Schulnetz Raum		IT	Schutzbedarf		
Nr.	Art	Installierte IT	Vertraulich-keit	Integrität	Verfügbarkeit
Schulas, Schwei	Büroraum	Nnn, Cnn	s. o.	s. o.	s. o.
310	Serverraum	S01-S05, Nnn, Cnn	hoch	hoch	hoch

Auf den folgenden Seiten wird die Erhebung der IT-Anwendungen sowie die Schutzbedarfsfeststellung in vergleichbarer Weise noch einmal für den IT-Verbund **Verwaltungsnetz** durchgeführt.

4.2.Schutzbedarfsfeststellung (Verwaltungsnetz)

4.2.1.Anpassung der Schutzbedarfskategorien

Für den IT-Verbund **Verwaltungsnetz** wurden die Schutzbedarfskategorien vom zuständigen IT-Sicherheitsmanagement folgendermaßen definiert und mit der Schulleitung abgestimmt:

- **Schutzbedarfskategorie niedrig bis mittel (I):**

Ein möglicher Schaden hätte nur begrenzte und überschaubare Auswirkungen auf das Arminius-Gymnasium :

- Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen allenfalls geringfügige juristische Konsequenzen oder Konventionalstrafen.
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten nur geringfügige Auswirkungen auf die davon Betroffenen und würden von diesen toleriert.
- Die persönliche Unversehrtheit wird nicht beeinträchtigt.
- Die Abläufe am Arminius-Gymnasium werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.
- Das Ansehen der Schule bei den Eltern und in der Öffentlichkeit wird nicht beeinträchtigt.

- **Schutzbedarfskategorie hoch (II):**

Ein möglicher Schaden hätte beträchtliche Auswirkungen auf das Arminius-Gymnasium :

- Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen schwerwiegende juristische Konsequenzen oder hohe Konventionalstrafen.
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten beträchtliche Auswirkungen auf die davon Betroffenen und würden von diesen nicht toleriert.
- Die persönliche Unversehrtheit wird nicht beeinträchtigt.
- Die Abläufe am Arminius-Gymnasium werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.
- Das Ansehen der Schule bei den Eltern und in der Öffentlichkeit wird erheblich beeinträchtigt.

- **Schutzbedarfskategorie sehr hoch (III):**

Ein möglicher Schaden hätte katastrophale Auswirkungen:

- Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen juristische Konsequenzen oder Konventionalstrafen, welche die Existenz der Schule gefährden.
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten ruinöse Auswirkungen auf die gesellschaftliche oder wirtschaftliche Stellung der davon Betroffenen.

- Die persönliche Unversehrtheit wird nicht beeinträchtigt.
- Die Abläufe am Arminius-Gymnasium werden so stark beeinträchtigt, dass Ausfallzeiten, die über 2 Stunden hinausgehen, nicht toleriert werden können.
- Das Ansehen der Schule bei den Eltern und in der Öffentlichkeit wird grundlegend und nachhaltig beschädigt.

4.2.2. Schutzbedarfsfeststellung der IT-Anwendungen

Bei der Schutzbedarfsfeststellung der IT-Anwendungen ist für alle in der IT-Strukturanalyse erfassten Anwendungen und differenziert nach den drei Grundwerten Vertraulichkeit (A), Integrität (B) und Verfügbarkeit (C) eine Zuordnung zu den zuvor festgelegten Schutzbedarfskategorien vorzunehmen.

Die folgende Tabelle zeigt die Zuordnungen, die für den IT-Verbund **Verwaltungsnetz** vorgenommen wurden:

IT-Anwendung IT-Verbund Verwaltungsnetz			Schutzbedarfsfeststellung		
Nr.	Bezeichnung	PD[26]	GW[27]	SB[28]	Begründung
A01	Benutzer-authentisierung	X	A	I	Die Passwörter sind verschlüsselt gespeichert und damit praktisch nicht zugänglich.
			B	II	Der hohe Schutzbedarf ergibt sich daraus, dass sich alle Mitarbeiter hierüber identifizieren.
			C	II	Bei Ausfall dieser Anwendung sind keine Identifizierung und damit keine Ausführung von IT-Verfahren möglich. Ein Ausfall ist allenfalls bis zu 24 Stunden tolerabel.
A02	Office-Anwendungen		A	I	Es werden keine vertraulichen Daten verarbeitet.
			B	I	Fehlerhafte Daten können leicht erkannt und korrigiert werden. Es sind keine finanziellen Schäden zu erwarten.
			C	I	Der Ausfall auf einem Client ist bis zu einer Woche hinnehmbar. Ersatzweise kann auf einem Laptop weitergearbeitet werden.

26 PD = Personenbezogene Daten

27 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

28 SB = Schutzbedarf

IT-Anwendung IT-Verbund Verwaltungsnetz			Schutzbedarfsfeststellung		
Nr.	Bezeichnung	PD	GW	SB	Begründung
A03	Stammdaten-Verwaltung (Schüler)	X	A	II	Die gespeicherten Daten sind schützenswerte personenbezogene Daten.
			B	I	Fehler werden rasch erkannt und können entweder aus der Datensicherung eingespielt oder durch Eingabe korrigiert werden.
			C	I	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
A04	Elektronische Kontoführung	X	A	II	Es werden vertrauliche Finanzdaten der Schule verarbeitet.
			B	II	Bei nicht korrekten Daten können finanzielle Schäden entstehen
			C	I	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
A05	Schulbuchausleihe	X	A	II	Es werden vertrauliche Finanzdaten der Schule verarbeitet.
			B	II	Bei nicht korrekten Daten können finanzielle Schäden entstehen
			C	I	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
A06	Leistungsdaten Oberstufe	X	A	I	Missbrauch hätte nur geringfügige Auswirkungen auf die Betroffenen und würde von ihnen toleriert.
			B	I	Fehler werden rasch erkannt und können leicht korrigiert werden.
			C	I	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
A07	Kursplanung Oberstufe	X	A	I	Missbrauch hätte nur geringfügige Auswirkungen auf die Betroffenen und würde von ihnen toleriert.
			B	I	Fehler werden rasch erkannt und können leicht korrigiert werden.
			C	I	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.

IT-Anwendung IT-Verbund Verwaltungsnetz			Schutzbedarfsfeststellung		
Nr.	Bezeichnung	PD	GW	SB	Begründung
A08	Stunden- und Raumplan	X	A	I	Missbrauch hätte nur geringfügige Auswirkungen auf die Betroffenen und würde von ihnen toleriert.
			B	I	Fehler werden rasch erkannt und können leicht korrigiert werden.
			C	II	Ausfallzeit nur unter 24 Stunden.
A09	Vertretungsplan	X	A	I	Missbrauch hätte nur geringfügige Auswirkungen auf die Betroffenen und würde von ihnen toleriert.
			B	I	Fehler werden rasch erkannt und können leicht korrigiert werden.
			C	II	Ausfallzeit nur unter 24 Stunden.
A10	Zentrale Dateiablage		A	I	Die hier gespeicherten Dateien sind nicht vertraulich. Sie werden zum Teil sogar öffentlich gemacht.
			B	I	Fehler werden in der Regel schnell erkannt und können nachträglich bereinigt werden.
			C	I	Bei Ausfall des Dienstes können die Dokumente auf den Client-PCs zwischengespeichert und bei Verfügbarkeit übertragen werden.
A11	Internet-Zugang		A	I	Es werden keine vertraulichen Daten verarbeitet.
			B	I	Fehlerhafte Daten können in der Regel leicht erkannt werden.
			C	I	Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
A12	E-Mail[29]	X	A	II	Es werden auch wichtige Daten der Schulbehörde per E-Mail übermittelt.
			B	II	Die Integrität dieser Informationen ist zu schützen.
			C	II	Ausfallzeit nur unter 24 Stunden.

29 Diese Einschätzung gilt nur für den Client-Typ C06.

IT-Anwendung IT-Verbund Verwaltungsnetz			Schutzbedarfsfeststellung		
Nr.	Bezeichnung	PD	GW	SB	Begründung
A13	Firewall		A	I	Über diesen Dienst werden keine vertraulichen Daten geleitet.
			B	II	Einbrüche in das Schulnetz müssen verhindert werden. Es könnten vertrauliche Daten kompromittiert werden.
			C	II	Ein Ausfall ist höchstens für 24 Stunden hinnehmbar.
A14	Anti-Virus Software		A	I	Es werden keine vertraulichen Daten verarbeitet.
			B	II	Fehlerhafte Daten können ein System kompromittierbar machen
			C	II	Ein Ausfall ist höchstens für 24 Stunden hinnehmbar.
A15	TK-Vermittlung		A	I	Die Betroffenen werden nur unerheblich beeinträchtigt, wenn die Daten bekannt werden.
			B	I	Fehler können leicht erkannt und korrigiert werden. Finanzielle Schäden sind nur gering.
			C	II	Ein Ausfall ist höchstens für 24 Stunden hinnehmbar.
A16	Fax-Versand und -Empfang		A	II	Es können auch personenbezogene Daten (Krankmeldungen etc.) übertragen werden.
			B	I	Fehler können leicht erkannt und korrigiert werden.
			C	I	Bei Ausfall kann auch per Telefon kommuniziert werden.

4.2.3.Schutzbedarfsfeststellung der IT-Systeme

Die folgenden Tabellen enthalten die Schutzbedarfsfeststellung für die Server, Clients, Netz- und Telekommunikationskomponenten im IT-Verbund **Verwaltungsnetz**.

a) Schutzbedarf Server (IT-Verbund **Verwaltungsnetz**)				
IT-System		Schutzbedarfsfeststellung		
Nr.	Beschreibung	GW[30]	SB[31]	Begründung
S01	Fileserver	A	II	Maximumprinzip gemäß A03
		B	II	Maximumprinzip gemäß A01
		C	II	Maximumprinzip gemäß A01

b) Schutzbedarf Clients (IT-Verbund **Verwaltungsnetz**)				
IT-System		Schutzbedarfsfeststellung		
Nr.	Beschreibung	GW[32]	SB[33]	Begründung
C01, C02, C04,	Koordinatoren	A	I	Gemäß Maximumprinzip
		B	II	Gemäß Maximumprinzip (A14)
		C	II	Gemäß Maximumprinzip (A14)
C03	Koordinator Schul-buchausleihe	A	II	Gemäß Maximumprinzip (A04, A05)
		B	II	Gemäß Maximumprinzip (A14)
		C	II	Gemäß Maximumprinzip (A14)
C05, C07	Stellv. SL SL	A	II	Gemäß Maximumprinzip (A03)
		B	II	Gemäß Maximumprinzip (A14)
		C	II	Gemäß Maximumprinzip (A14)
C06	Sekretariat	A	II	Gemäß Maximumprinzip (A03, A04)
		B	II	Gemäß Maximumprinzip (A14)
		C	II	Gemäß Maximumprinzip (A14)

30 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

31 SB = Schutzbedarf

32 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

33 SB = Schutzbedarf

c) Schutzbedarf Netzkomponenten (IT-Verbund **Verwaltungsnetz**)				
IT-System		Schutzbedarfsfeststellung		
Nr.	Beschreibung	GW[34]	SB[35]	Begründung
N01	24-Port-Switch	A	I	Die Benutzerauthentisierung erfolgt verschlüsselt, ebenso kann das Aufrufen der E-Mails im Browser über eine sichere Verbindung (SSL / https) erfolgen. Daher keine erhöhte Vertraulichkeit.
		B	I	Fehler werden leicht erkannt und korrigiert.
		C	II	Ein Ausfall erscheint höchstens bis zu 24 Stunden tolerabel.
N02, N03	DSL-Router, DSL-Modem	A	I	Der Router kann nur per Software konfiguriert werden. Die Konfiguration ist durch Passwort geschützt.
		B	I	Fehler in den Daten werden schnell erkannt und können schnell korrigiert werden.
		C	II	Ein Ausfall erscheint höchstens bis zu 24 Stunden tolerabel.

d) Schutzbedarf Telekommunikationskomponenten (IT-Verbund **Schulnetz**)				
IT-System		Schutzbedarfsfeststellung		
Nr.	Beschreibung	GW[36]	SB[37]	Begründung
T01	TK-Anlage	A	I	Gemäß Maximumprinzip (A15)
		B	I	Gemäß Maximumprinzip (A15)
		C	II	Gemäß Maximumprinzip (A15)
T02	Fax-Gerät	A	II	Gemäß Maximumprinzip (A16)
		B	I	Gemäß Maximumprinzip (A16)
		C	I	Gemäß Maximumprinzip (A16)

34 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

35 SB = Schutzbedarf

36 GW = Grundwert (A = Vertraulichkeit, B = Integrität, C = Verfügbarkeit)

37 SB = Schutzbedarf

4.2.4.Schutzbedarf der Kommunikationsverbindungen

Im nächsten Arbeitsschritt geht es darum, den Schutzbedarf für die Kommunikationsverbindungen festzustellen. Es gibt Verbindungen, die gefährdeter sind als andere und durch doppelte Auslegung oder durch besondere Maßnahmen gegen Angriffe von außen oder innen geschützt werden müssen.

Als kritische **Verbindungen** gelten:

- Verbindungen, die aus der Schule **in ein öffentliches Netz** (z. B. Telefonnetz, Internet) oder **über ein öffentliches Gelände** reichen. Über solche Verbindungen können Computer-Viren und trojanische Pferde in das Schulnetz eingeschleust werden, Schulserver angegriffen werden oder Mitarbeiter vertrauliche Daten an Nichtbefugte weiterleiten.
- Verbindungen, über die besonders **schützenswerte Informationen** übertragen werden. Mögliche Gefährdungen sind Abhören, vorsätzliche Manipulation und betrügerischer Missbrauch. Vom Ausfall solcher Verbindungen sind Anwendungen, für die eine hohe Verfügbarkeit erforderlich ist, besonders betroffen.
- Verbindungen, über die vertrauliche Informationen **überhaupt nicht übertragen werden dürfen**. Personaldaten dürfen zum Beispiel nur von der Schulleitung eingesehen und bearbeitet werden. Daher muss verhindert werden, dass diese Daten bei ihrer Übertragung von unbefugten Mitarbeitern eingesehen werden können.

Im IT-Verbund **Verwaltungsnetz** werden über die Kommunikationsverbindungen keine besonders schützenswerten Daten unverschlüsselt übertragen. Daher existieren auch keine Verbindungen, über die vertrauliche Daten überhaupt nicht übertragen werden dürfen.

Allein die direkte Verbindung vom DSL-Router N02 ins Internet kann als kritische Verbindung bezeichnet werden.

4.2.5.Schutzbedarfsfeststellung der IT-genutzten Räume

Bei der Schutzbedarfsfeststellung für Räume werden sowohl Räume berücksichtigt,

- die zum Betrieb von IT-Systemen dienen (z. B. Serverräume, Räume für eine TK-Anlage und andere Räume mit technischer Infrastruktur), als auch
- in denen IT-Systeme genutzt werden (z. B. Büroräume).

Der Schutzbedarf eines Raumes bemisst sich nach dem Schutzbedarf der IT-Systeme, die sich in diesem Raum befinden. Auch hier können Sie (wie schon bei der Schutzbedarfsfeststellung der IT-Systeme) wieder im Allgemeinen das Maximumprinzip anwenden. Befinden sich jedoch in einem Raum mehrere Systeme, dann kann sich für den Raum ein höherer Schutzbedarf als für jedes einzelne IT-System ergeben (Kumulationseffekt). Dies gilt z. B. für Serverräume.

Die folgende Tabelle zeigt das Ergebnis der Schutzbedarfsfeststellung für die IT-genutzten Räume im IT-Verbund **Verwaltungsnetz**. Der Schutzbedarf der Räume wird hier festgelegt nach dem jeweils höchsten Schutzbedarf der darin installierten Systeme (Maximumprinzip).

Raum		IT	Schutzbedarf		
Nr.	Art	Installierte IT	Vertraulichkeit	Integrität	Verfügbarkeit
220, 222	Büroraum	C01, C04	niedrig bis mittel	hoch	hoch
221, 223, 225, 226	Büroraum	S01, C02, C03, C05, C06, C07	hoch	hoch	hoch

Raum		IT	Schutzbedarf		
Nr.	Art	Installierte IT	Vertraulichkeit	Integrität	Verfügbarkeit
224	Serverraum	N01, N02, N03	niedrig bis mittel	niedrig bis mittel	hoch

5.Modellierung gemäß IT-Grundschutz

Ziel der Modellierung gemäß IT-Grundschutz ist es festzulegen, welche Bausteine (= Kapitel) des IT-Grundschutzhandbuchs auf welche Zielobjekte der Informationstechnik einer Organisation anzuwenden sind.

Das Ergebnis ist ein **IT-Grundschutzmodell**, das für geplante IT als Entwicklungskonzept und für bestehende IT als Prüfplan verwendet werden kann.

Am Arminius-Gymnasium dient dieses Modell als Prüfplan für den Basis-Sicherheitscheck. Die nachfolgenden Tabellen zeigen die Dokumentation der am Arminius-Gymnasium vorgenommenen Modellierung.

Weitere Informationen zur Modellierung gemäß IT-Grundschutz finden sich in Kapitel 2.3 des IT-Grundschutzhandbuchs.

5.1.Schicht 1: Übergreifende Aspekte

Baustein	Zielobjekt	Hinweise
1.0 IT-Sicherheitsmanagement	Gesamte Organisation	Gilt einheitlich für beide IT-Verbünde.
1.1 Organisation	Gesamte Organisation	Gilt einheitlich für beide IT-Verbünde.
1.2 Personal	Gesamte Organisation	Gilt einheitlich für beide IT-Verbünde.
1.3 Notfallvorsorge-Konzept	Gesamte Organisation	Gilt einheitlich für beide IT-Verbünde.
1.4 Datensicherungskonzept	IT-Verbund Schulnetz	Alle Client-PCs sind per HWS abgesichert, Daten werden lokal nicht gespeichert, es müssen nur Daten auf Servern gesichert werden.
	IT-Verbund Verwaltungsnetz	Die Client-PCs sind nicht abgesichert, Daten werden auch lokal gespeichert.
1.6 Computer-Virenschutzkonzept	IT-Verbund Schulnetz	Alle Client-PCs sind per HWS abgesichert, nur die Server müssen geschützt werden.
	IT-Verbund Verwaltungsnetz	Die Client-PCs sind nicht abgesichert.
1.7 Kryptokonzept	Gesamte Organisation	Gilt einheitlich für beide IT-Verbünde.

5.1.Schicht 1: Übergreifende Aspekte

Baustein	Zielobjekt	Hinweise
1.8 Behandlung von Sicherheitsvorfällen	Gesamte Organisation	Gilt einheitlich für beide IT-Verbünde.
1.9 Hard- und Softwaremanagement	Gesamte Organisation	Wird zentral von der IT festgelegt.
1.10 Standard-Software	Gesamte Organisation	Gilt einheitlich für beide IT-Verbünde.
1.11 Outsourcing	Gesamte Organisation	Gilt nur für IT-Verbund Schulnetz.
1.13 IT-Sicherheitssensibilisierung und -schulung	Gesamte Organisation	Gilt einheitlich für beide IT-Verbünde.

5.2.Schicht 2: Infrastruktur

Baustein	Zielobjekt	Hinweise
2.1 Gebäude	Schulgebäude	Beide IT-Verbünde befinden sich in einem Gebäude.
2.2 Verkabelung	IT-Verbund Schulnetz	Die Verkabelung muss für beide Gebäude gesondert betrachtet werden.
	IT-Verbund Verwaltungsnetz	
2.3. Büroraum	Büroräume (IT-Verbund Verwaltungsnetz)	Da alle Räume denselben Standard haben, soll als Stichprobe ein Raum für zwei Mitarbeiter untersucht werden.
2.3. Büroraum	Sekretariat (IT-Verbund Verwaltungsnetz)	Publikumsverkehr!
2.3. Büroraum	IT-Verbund Schulnetz: Schulassistent	Nur mit Schlüssel zugänglich
2.3. Büroraum	IT-Verbund Schulnetz: Schweigezimmer	Mit Lehrer-Schlüssel zugänglich
2.4 Serverraum	R 310	IT-Verbund Schulnetz
2.4 Serverraum	R 224 (Kopierraum)	IT-Verbund Verwaltungsnetz

5.2.Schicht 2: Infrastruktur

Baustein	Zielobjekt	Hinweise
2.10 Mobiler Arbeitsplatz	Laptop	
2.11 Besprechungs-, Veranstaltungs- und Schulungsräume	Alle PC-Räume im IT-Verbund Schulnetz	Da die Räume denselben Standard haben, soll als Stichprobe einer der PC-Räume untersucht werden.

5.3.Schicht 3: IT-Systeme

Baustein	Zielobjekt	Hinweise
3.101 Allgemeiner Server	IT-Verbund Schulnetz: S01, S02, S03, S04, S05	Dieser Baustein behandelt die nicht betriebssystem-spezifischen Sicherheitsaspekte von Servern. Die Server S01 bis S05 sind unterschiedlich konfiguriert. Der Baustein wird daher auf jedes System getrennt angewendet.
	IT-Verbund Verwaltungsnetz: S01	
3.102 Server unter UNIX	IT-Verbund Schulnetz: S01	Das ISERV-System basiert auf dem UNIX-Derivat LINUX.
	IT-Verbund Schulnetz: S03	Dieser Terminalserver wird ebenfalls unter LINUX betrieben.
	IT-Verbund Schulnetz: S05	Der Web-Server der Ehemaligenvereinigung wird ebenfalls unter LINUX betrieben.
3.103 Server unter Windows-NT	IT-Verbund Schulnetz: S02	
3.106 Windows 2000 Server	IT-Verbund Schulnetz: S04	Dieser Terminalserver wird unter dem Nachfolge-Betriebssystem Windows 2003 betrieben.
	IT-Verbund Verwaltungsnetz: S01	
3.201 Allgemeiner Client	IT-Verbund Schulnetz	
	IT-Verbund Verwaltungsnetz	

5.3.Schicht 3: IT-Systeme

Baustein	Zielobjekt	Hinweise
3.203 Laptop	Laptop	
3.206 Client unter Windows 95	IT-Verbund Schulnetz: C01 bis C13	Unabhängig vom Betriebssystem sind alle Client-PCs per HWS geschützt. Sie sind einheitlich so konfiguriert, dass sie sich wie ein PC mit Windows 95 verhalten. Es bestehen im Betrieb keine Restriktionen seitens des Betriebssystems.
3.209 Client unter Windows XP	IT-Verbund Verwaltungsnetz: C01 bis C07	
3.301 Sicherheitsgateway (Firewall)	IT-Verbund Schulnetz	Das ISERV-System (S01) fungiert als Sicherheitsgateway.
	IT-Verbund Verwaltungsnetz	Der Router (N02) fungiert als Sicherheitsgateway.
3.302 DSL-Router	IT-Verbund Verwaltungsnetz	
3.401 TK-Anlage	IT-Verbund Schulnetz	ISDN-Anlage im RCC
	IT-Verbund Verwaltungsnetz	Telefonanlage im Sekretariat
3.402 Fax-Gerät	IT-Verbund Verwaltungsnetz	Standort: Sekretariat
WLAN Access Point	IT-Verbund Schulnetz	kein spezieller Baustein vorhanden

5.4.Schicht 4: Netze

Baustein	Zielobjekt	Hinweise
4.1 Heterogene Netze	IT-Verbund Schulnetz	
	IT-Verbund Verwaltungsnetz	
4.2 Netz- und Systemmanagement	Gesamte Organisation	
4.3 Modem	IT-Verbund Schulnetz: C13	Das Laptop hat ein eingebautes Modem.

5.4.Schicht 4: Netze		
Baustein	Zielobjekt	Hinweise
4.4 Remote Access	IT-Verbund Schulnetz: S01	Das ISERV-System ist via Web-Interface erreichbar. Auch Fernwartung via SSH ist eingerichtet.

5.5.Schicht 5: Anwendungen		
Baustein	Zielobjekt/Gruppe	Hinweise
5.3 E-Mail	Gesamte Organisation	Erarbeitung einer Sicherheitspolitik für E-Mail und Überprüfung des Mail-Servers S01 sowie als Stichprobe der E-Mail Client im Sekretariat.
5.4 WWW-Server	IT-Verbund Schulnetz: S01	Das ISERV-System fungiert als WWW-Server.
5.8 Telearbeit	IT-Verbund Schulnetz	Die Arbeit mit dem ISERV-System ist am ehesten mit diesem Punkt vergleichbar.
5.11 Apache Webserver	IT-Verbund Schulnetz: S01	Das ISERV-System arbeitet mit dem Apache Webserver.

6.Basis-Sicherheitscheck

Mit einem Basis-Sicherheitscheck ermitteln Sie, ob und inwieweit die Maßnahmen-Empfehlungen des IT-Grundschutzhandbuchs für die einzelnen Zielobjekte des betrachteten IT-Verbunds umgesetzt sind. Bei einem systematischen Vorgehen greifen Sie dazu auf die Ergebnisse der vorangegangenen Schritte zurück:

- Bei der IT-Strukturanalyse haben Sie die vorhandenen IT-Systeme und die von diesen unterstützten Anwendungen erfasst.
- Anschließend haben Sie den Schutzbedarf der IT-Systeme, Anwendungen, Räume und Kommunikationsverbindungen bestimmt und
- bei der Modellierung durch Auswahl der anzuwendenden Bausteine einen Prüfplan („Grundschutz-Modell“) für die verschiedenen Zielobjekte (gesamter IT-Verbund, Räume, Rechner, Kommunikationsverbindungen, Anwendungen) zusammengestellt.

Den Prüfplan wenden Sie beim Basis-Sicherheitscheck an, indem Sie für jedes Zielobjekt und für jede Maßnahme, die in den anzuwendenden Bausteinen empfohlenen wird, prüfen,

- ob sie überhaupt auf das Zielobjekt anzuwenden ist, und falls ja,
- ob sie vollständig, teilweise oder überhaupt nicht umgesetzt ist.

Die nachfolgenden Tabellen zeigen in Auszügen einen Basis-Sicherheitscheck für die Beispielschule Arminius-Gymnasium, und zwar die Anwendung der Bausteine

- 1.0 IT-Sicherheitsmanagement auf die gesamte Organisation,
- 2.4 Serverraum auf den **Serverraum im IT-Verbund Schulnetz**,
- 4.1 Heterogene Netze auf den **IT-Verbund Schulnetz.**

Wenn Sie einen Basis-Sicherheitscheck durchführen, dürfen Sie selbstverständlich kein Zielobjekt und keinen Baustein auslassen, wenn Sie einen umfassenden IT-Grundschutz für Ihre Schule anstreben.

Für den Basis-Sicherheitscheck greifen wir auf die Maßnahmenkataloge zurück, wie sie im IT-Grundschutzhandbuch des BSI vorgeschlagen werden. Layout-Grundlage unserer Formblätter sind Formblätter des BSI (im DOC-Format), die sich in ihrer konkreten Ausgestaltung jedoch als nicht genau passend erwiesen. Wir haben die Reihenfolge der aufgelisteten Maßnahmen derjenigen im aktuellen IT-Grundschutzhandbuch (2005) angepasst.

6.1.Schicht 1: Übergreifende Aspekte

Baustein 1.0 IT-Sicherheitsmanagement

Maßnahme (Priorität)	Name	entbehrlich	ja	teilw.	nein	Bemerkung / Begründung bei Nicht-Umsetzung
M 2.192 (1)	Erstellung einer IT Sicherheitsleitlinie		X			s. IT-Sicherheitskonzept
M 2.335 (1)	Festlegung der IT-Sicherheitsziele und -strategie		X			s. IT-Sicherheitskonzept
M 2.336 (1)	Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene		X			s. IT-Sicherheitskonzept
M 2.193 (1)	Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit			X		im Aufbau
M 2. 195 (1)	Erstellung eines IT-Sicherheitskonzepts			X		im Entstehen
M 2.197 (2)	Integration der Mitarbeiter in den Sicherheitsprozess			X		Die Mitarbeiter werden im Prozess der Einführung des IT-Sicherheitskonzepts angemessen beteiligt.
M 2.337 (1)	Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse			X		Im Prozess der Einführung des IT-Sicherheitskonzepts wird die Integration der IT-Sicherheit erfolgen.
M 2.338 (1)	Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien	X				Organisationsstruktur ist so überschaubar, dass von zielgruppengerechten IT-Sicherheitsrichtlinien abgesehen werden kann.
M 2.339 (1)	Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit	X				Organisationsstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 2.199 (1)	Aufrechterhaltung der IT-Sicherheit		X			Mit Einführung des IT-Sicherheitskonzepts sind jährliche Fortschreibungen des Konzepts verbunden.
M 2.200 (1)	Managementreporte und -bewertungen der IT-Sicherheit	X				Organisationsstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 2.201 (2)	Dokumentation des IT-Sicherheitsprozesses			X		im Entstehen
M 2. 340 (2)	Beachtung rechtlicher Rahmenbedingungen		X			Die Schulleitung sorgt für die Bekanntgabe neuer oder geänderter rechtlicher Vorschriften, welche den Bereich der IT-Sicherheit betreffen.

6.2.Schicht 2: Infrastruktur

Baustein 2.4 Serverraum (IT-Verbund Schulnetz)

Maßnahme (Priorität)	Name	entbehrlich	ja	teilw.	nein	Bemerkung / Begründung bei Nicht-Umsetzung
M 1.3 (1)	Angepasste Aufteilung der Stromkreise		X			
M 1.7 (2)	Handfeuerlöscher		X			
M 1.10 (2)	Verwendung von Sicherheitstüren und -fenstern		X			
M 1.18 (2)	Gefahrenmeldeanlage		X			
M 1.24 (2)	Vermeidung von wasserführenden Leitungen				X	Zuständig ist der Schulträger.
M 1.25 (2)	Überspannungsschutz				X	Zuständig ist der Schulträger.
M 1.26 (2)	Not-Aus-Schalter				X	Zuständig ist der Schulträger.
M 1.27 (2)	Klimatisierung	X				Die Fernüberwachung der Server berücksichtigt auch die Temperatur. Bisher gab es keine Hitzeprobleme.
M 1.28 (1)	Lokale unterbrechungsfreie Stromversorgung	X				Es gibt keine wichtigen Cache-Daten. Alle wichtigen Daten sind auf den Festplatten gespeichert.
M 1.31 (3)	Fernanzeige von Störungen	X				Der Serverraum wird täglich mindestens einmal vom IT-Sicherheitsmanagement aufgesucht.
M 1.52 (3)	Redundanzen in der techn. Infrastruktur	X				Keine Notwendig gegeben (s. Schutzbedarfsfeststellung)
M 1.58 (1)	Technische und organisatorische Vorgaben für Serverräume		X			
M 1.62 (1)	Brandschutz von Patchfeldern		X			
M 2.17 (2)	Zutrittsregelung und -kontrolle		X			
M 2.21 (2)	Rauchverbot		X			
M 1.15 (1)	Geschlossene Fenster und Türen		X			
M 1.23 (1)	Abgeschlossene Türen		X			

6.3.Schicht 4: Netze

Baustein 4.1 Heterogene Netze (IT-Verbund Schulnetz)

Maßnahme (Priorität)	Name	entbehrlich	ja	teilw.	nein	Bemerkung / Begründung bei Nicht-Umsetzung
M 2.139 (1)	Ist-Aufnahme der aktuellen Netzsituation		X			Die IT-Strukturanalyse bietet hinreichende Informationen.
M 2.140 (1)	Analyse der aktuellen Netzsituation	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 2.141 (1)	Entwicklung eines Netzkonzeptes	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 2.142 (1)	Entwicklung eines Netz-Realisierungsplans	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 4.79 (1)	Sichere Zugriffsmechanismen bei lokaler Administration		X			
M 4.80 (1)	Sichere Zugriffsmechanismen bei Fernadministration		X			Zugang per SSH-Verbindung
M 5.2 (1)	Auswahl einer geeigneten Netz-Topographie	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 5.13 (1)	Geeigneter Einsatz von Elementen zur Netzkopplung	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 5.60 (1)	Auswahl einer geeigneten Backbone-Technologie	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 5.61 (1)	Geeignete physikalische Segmentierung	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 5.62 (1)	Geeignete logische Segmentierung	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 5.77 (1)	Bildung von Teilnetzen	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 4.7 (1)	Änderung voreingestellter Passwörter		X			
M 4.82 (1)	Sichere Konfiguration der aktiven Netzkomponenten	X				Komponenten sind nicht konfigurierbar.
M 5.7 (1)	Netzverwaltung	X				Netzstruktur macht diesbezügliche Maßnahmen entbehrlich.
M 4.81 (2)	Audit und Protokollierung der Aktivitäten im Netz		X			SysMon-Dienst (ISERV)

6.3.Schicht 4: Netze

Baustein 4.1 Heterogene Netze (IT-Verbund Schulnetz)

Maßnahme (Priorität)	Name	entbehrlich	ja	teilw.	nein	Bemerkung / Begründung bei Nicht-Umsetzung
M 4.83 (3)	Update/Upgrade von Soft- und Hardware im Netzbereich		X			
M 6.52 (1)	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten	X				Keine Konfigurationsdateien vorhanden.
M 6.53 (1)	Redundante Auslegung der Netzkomponenten	X				Für aktive Komponenten und Server existiert eine Reaktionszeit von 4 Stunden.
M 6.54 (3)	Verhaltensregeln nach Verlust der Netzintegrität			X		Entsprechende Formulierungen sind Teil des zu formulierenden IT-Sicherheitskonzepts.

7.Realisierungsplanung

Insbesondere dann, wenn viele Sicherheitsmaßnahmen umzusetzen sind, ist es hilfreich, wenn Sie sich bei der Realisierungsplanung an die folgende Reihenfolge halten:

Ergebnisse sichten

Sichten Sie zunächst die Ergebnisse des Basis-Sicherheitschecks und ggf. einer ergänzenden Sicherheitsanalyse und stellen Sie die noch nicht oder nur teilweise realisierten Sicherheitsmaßnahmen tabellarisch zusammen.

Maßnahmen konsolidieren

Prüfen und konkretisieren Sie die Maßnahmen im Zusammenhang. Dies reduziert gegebenenfalls die umzusetzenden Maßnahmen. Das Ergebnis ist ein konsolidierter Realisierungsplan.

Aufwand schätzen

Schätzen Sie den finanziellen und personellen Aufwand, der mit der Umsetzung der einzelnen Maßnahmen verbunden ist. Unterscheiden Sie dabei zwischen dem einmaligen Aufwand bei der Einführung einer Maßnahme und dem wiederkehrenden Aufwand im laufenden Betrieb.

Umsetzungsreihenfolge festlegen

Legen Sie eine sinnvolle Umsetzungsreihenfolge fest. Berücksichtigen Sie dabei sowohl die sachlogischen Zusammenhänge der einzelnen Maßnahmen, als auch deren Wirkung auf das Sicherheitsniveau des IT-Verbunds.

Verantwortliche bestimmen

Entscheiden Sie, bis zu welchem Termin eine Maßnahme umzusetzen ist und wer für die Realisierung und deren Überwachung zuständig sein soll.

Begleitende Maßnahmen festlegen

Die praktische Wirksamkeit der Sicherheitsmaßnahmen hängt von der Akzeptanz und dem Verhalten der betroffenen Mitarbeiter ab. Planen Sie daher Schritte zu ihrer Sensibilisierung und Schulung ein.

Die Schritte 1, 3 und 4 können entfallen, falls nur wenige Maßnahmen zu realisieren sind oder die Maßnahmen insgesamt nur geringe personelle und finanzielle Ressourcen benötigen.

7.1.Konsolidierter Realisierungsplan

Einige der fehlenden Maßnahmen können kurzfristig korrigiert werden und bedürfen daher keiner umfangreichen Realisierungsplanung. So sollten Mängel in einer Dokumentation in der Regel umgehend und leicht behebbar sein. Wer derartige Maßnahmen bis wann umzusetzen hat und wer überprüft, ob dies tatsächlich geschehen ist, kann unkompliziert bereits beim Basis-Sicherheitscheck dokumentiert werden. Diese und vergleichbare Maßnahmen werden daher in der Darstellung nicht weiter berücksichtigt.

Die folgenden Tabellen enthalten alle übrigen Maßnahmen, die im Basis-Sicherheitscheck als nicht oder nur teilweise umgesetzt identifiziert wurden. Sie beschränken sich ferner auf die exemplarisch ausgewählten Zielobjekte und Bausteine und geben den Stand der Realisierungsplanung nach dem Schritt 2 (Konsolidierung der Maßnahmen) an.

Zielobjekt: Gesamte Organisation Arminius-Gymnasium		
Baustein: 1.0 IT-Sicherheitsmanagement		
Maßnahme (Priorität)	Aufwand[38]	Bemerkungen
M 2.193 (1) Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit	a) 1 AT b) ----- c) ----- d) -----	
M 2.195 (1) Erstellung eines IT-Sicherheitskonzepts	a) 20 AT b) 1 AT/Jahr c) ----- d) -----	Derzeit muss das IT-Sicherheitskonzept noch fertig gestellt werden. Regelmäßiger Aufwand für die Fortschreibung des Konzepts ist berücksichtigt.
M 2.197 (2) Integration der Mitarbeiter in den Sicherheitsprozess	a) 2 AT b) 1 AT/Jahr c) ----- d) -----	Wird bei der Erarbeitung des IT-Sicherheitskonzepts berücksichtigt. Das Schulungskonzept soll jährlich aktualisiert werden.
M 2.337 (1) Integration der IT-Sicherheit in organisationsweite Abläufe	a) 0,5 AT b) 0,5 AT c) ----- d) -----	Wird bei der Erarbeitung des IT-Sicherheitskonzepts berücksichtigt. Das Konzept soll im Rahmen der jährlichen Revision überprüft werden.
M 2.201 (1) Dokumentation des IT-Sicherheitsprozesses	a) 5 AT b) 2 AT/Jahr c) ----- d) -----	In elektronischen Dokumenten, die von den Mitarbeitern jederzeit abgerufen werden können.

Zielobjekt: IT-Verbund Schulnetz: Serverraum		
Baustein: 2.4. Serverraum		
Maßnahme (Priorität)	Aufwand[39]	Bemerkungen
M 1.24 (2) Vermeidung von wasserführenden Leitungen (optional)	a) ????? b) 0 AT/Jahr c) ????? d) -----	Die Maßnahme muss vom Schulträger realisiert werden.
M 1.25 (2) Überspannungsschutz	a) ???? b) 0 AT/Jahr c) ????? d) -----	Die Maßnahme muss vom Schulträger realisiert werden.

38 Legende: a) = Einmaliger Personalaufwand, b) = Wiederkehrender Personalaufwand, c) Einmalige Kosten, d) Wiederkehrende Kosten

39 Legende: a) = Einmaliger Personalaufwand, b) = Wiederkehrender Personalaufwand, c) Einmalige Kosten, d) Wiederkehrende Kosten

Zielobjekt: IT-Verbund Schulnetz: Serverraum		
Baustein: 2.4. Serverraum		
M 1.26 (2) Not-Aus-Schalter	a) ???? b) 0 AT/Jahr c) ????? d) -----	Die Maßnahme muss vom Schulträger realisiert werden.

Zielobjekt: IT-Verbund Schulnetz		
Baustein: 4.1 Heterogene Netze		
Maßnahme (Priorität)	Aufwand[40]	Bemerkungen
M 6.54 (3) Verhaltensregeln nach Verlust der Netzintegrität	b) 0 AT d) 0 AT/Jahr c) ----- d) -----	Die Formulierung entsprechender Verhaltensregeln ist Bestandteil des zu entwickelnden Sicherheitskonzepts. Es entsteht hier kein zusätzlicher Aufwand.

7.2.Abgestimmter Realisierungsplan

Die folgenden Tabellen enthalten den mit der Schulleitung abgestimmten Realisierungsplan mit eingetragenen Verantwortlichen und Umsetzungsterminen.

Zielobjekt: Gesamte Organisation Arminius-Gymnasium				
Baustein: 1.0 IT-Sicherheitsmanagement				
Maßnahme (Priorität)	Termin	Verantwortlich	Budget[41]	Bemerkungen
M 2.193 (1) Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit	1.8.2006	OStR Varus	a) 1 AT b) ----- c) ----- d) -----	
M 2.195 (1) Erstellung eines IT-Sicherheitskonzepts	1.8.2006	OStR Varus	a) 20 AT b) 1 AT/Jahr c) ----- d) -----	Derzeit muss das IT-Sicherheitskonzept noch fertig gestellt werden. Regelmäßiger Aufwand für die Fortschreibung des Konzepts ist berücksichtigt.
M 2.197 (2) Integration der Mitarbeiter in den Sicherheitsprozess	1.8.2006	IT-Sicherheitsmanagement: OStR Varus	a) 2 AT b) 1 AT/Jahr c) ----- d) -----	Wird bei der Erarbeitung des IT-Sicherheitskonzepts berücksichtigt. Das Schulungskonzept soll jährlich aktualisiert werden.

40 Legende: a) = Einmaliger Personalaufwand, b) = Wiederkehrender Personalaufwand, c) Einmalige Kosten, d) Wiederkehrende Kosten

41 Legende: a) = Einmaliger Personalaufwand, b) = Wiederkehrender Personalaufwand, c) Einmalige Kosten, d) Wiederkehrende Kosten

Zielobjekt: Gesamte Organisation Arminius-Gymnasium				
Baustein: 1.0 IT-Sicherheitsmanagement				
M 2.337 (1) Integration der IT-Sicherheit in organisationsweite Abläufe	1.8.2006	IT-Sicherheitsmanagement: OStR Varus	a) 0,5 AT b) 0,5 AT c) ----- d) -----	Wird bei der Erarbeitung des IT-Sicherheitskonzepts berücksichtigt. Das Konzept soll im Rahmen der jährlichen Revision überprüft werden.
M 2.201 (1) Dokumentation des IT-Sicherheitsprozesses	1.8.2006	IT-Sicherheitsmanagement: OStR Varus	a) 5 AT b) 2 AT/Jahr c) ----- d) -----	In elektronischen Dokumenten, die von den Mitarbeitern jederzeit abgerufen werden können.

Zielobjekt: IT-Verbund Schulnetz: Serverraum				
Baustein: 2.4. Serverraum				
Maßnahme (Priorität)	Termin	Verantwortlich	Budget[42]	Bemerkungen
M 1.24 (2) Vermeidung von wasserführenden Leitungen (optional)	?????	Schulleitung	a) ????? b) 0 AT/Jahr c) ????? d) -----	Die Maßnahme muss vom Schulträger realisiert werden.
M 1.25 (2) Überspannungsschutz	?????	Schulleitung	a) ???? b) 0 AT/Jahr c) ????? d) -----	Die Maßnahme muss vom Schulträger realisiert werden.
M 1.26 (2) Not-Aus-Schalter	?????	Schulleitung	a) ???? b) 0 AT/Jahr c) ????? d) -----	Die Maßnahme muss vom Schulträger realisiert werden.
Zielobjekt: IT-Verbund Schulnetz				
Baustein: 4.1 Heterogene Netze				
Maßnahme (Priorität)	Termin	Verantwortlich	Budget[43]	Bemerkungen
M 6.54 (3) Verhaltensregeln nach Verlust der Netzintegrität	1.8.2006	IT-Sicherheitsmanagement: OStR Varus	a) 0 AT b) 0 AT/Jahr c) ----- d) -----	Die Formulierung entsprechender Verhaltensregeln ist Bestandteil des zu entwickelnden Sicherheitskonzepts. Es entsteht hier kein zusätzlicher Aufwand.

42 Legende: a) = Einmaliger Personalaufwand, b) = Wiederkehrender Personalaufwand, c) Einmalige Kosten, d) Wiederkehrende Kosten

43 Legende: a) = Einmaliger Personalaufwand, b) = Wiederkehrender Personalaufwand, c) Einmalige Kosten, d) Wiederkehrende Kosten

8.Anhang

8.1.Leistungskatalog der Netzwerkbetreuung für Schulen

Leistungen der Netzwerkbetreuung für Schulen	Gemeinsame Aufgaben	Leistungen der Schulen
Einbau und Installation neuer Hardwarekomponenten; Erledigung aller Reparaturen (excl. Kosten für Ersatzteile); Einspielen von Updates (Betriebssystem), Installation von Hotfixes; Regelmäßige Überprüfung und Wartung der Server[44]; Notdienst bei Systemausfall (Server, Router) innerhalb 4 h, PCs maximal 24 Stunden; Begutachtung angebotener Hardware-Geschenke; Einrichtung von Usern und Usergruppen; Verteilung der Zugriffsrechte auf Ressourcen (Verzeichnisse, Drucker, Internet-Zugriff,...); Planung und Organisation von Strategien, um Hackerangriffe von innen und ggf. von außen abzuwehren (Firewalls); Beratung und Schulung der Raumverantwortlichen; Schulinterne Fortbildung für Kolleginnen und Kollegen im Umgang mit dem lokalen Netz; Hilfen bei der Erstellung von Unterrichtsmaterialien (Päd. Mitarb.);	Planung der Beschaffung von Hard- und Software; Installation neuer Programme und Programmversionen (Anwendungssoftware / Mehrplatzlizenz im Netzwerk) Netzwerkplanung (incl. Backupstrategien) Formulierung von Ausschreibungstexten; Inventarisierung von Hard- und Software[45];	Feststellung des Bedarfs an Unterrichtsmitteln; Installation neuer Programme und Programmversionen (Anwendungssoftware / Einzelplatzlizenz); Beschaffung von Verbrauchsmaterial (Disketten, Toner, ...); Backup-Maßnahmen nach gemeinsamer Planungsvorgabe; kurzfristige Behebung von Problemen, die durch unsachgemäße Handhabung von Hard- und Software entstanden sind, sofern dies möglich ist; ansonsten Erfassung und Weiterleitung von Fehlern und Mängeln bei Hard- und Software an die Netzwerkbetreuung[46]; Softwareverwaltung (sichere Aufbewahrung der Datenträger, Lizenzierung); Platzierung der schulischen HTML-Seiten auf dem entsprechenden Webserver, ggf. Sicherstellen eines einheitlichen Designs der schulischen Webseiten, Überprüfen der angegebenen Links, Aktualisierung der Seiten;

44 Die Fernwartung der betreuten Server ist Ziel der Netzwerkbetreuung. Die Zustimmung zum Remote-Zugriff auf die betreuten Server wird vorausgesetzt.

45 Die Inventarisierung von Hard- und Software ist ein wichtiger Bestandteil des Betreuungskonzeptes. Parallel zum Aufbau der Netzwerkbetreuung soll die Einrichtung einer zentralen Datenbank mit den wichtigsten Informationen erfolgen. Hierzu wird eine detaillierte Erhebung des Ist-Zustandes vor Ort durchgeführt.

46 Die Raumverantwortlichen leisten weiterhin einen First-Level-Support, der zumindest in der Diagnose einer Systemstörung besteht. Die konstruktive Zusammenarbeit mit den Raumverantwortlichen ist ein zentraler Baustein des Betreuungskonzeptes. Die Beratung und Schulung der Raumverantwortlichen wird durch die Netzwerkbetreuung sicher gestellt (s.o.).

8.2.Benutzerordnung für das IServ-System am Arminius-Gymnasium

Anmeldung zur Benutzung der Schulrechner und des IServ-Systems am Arminius-Gymnasium, Kalkriese

Vorname: _____ Name: _____ Klasse:_____

Schuleintrittsjahr: _____

1. Wesentliche Nutzungssoftware auf den Rechnern des Arminius-Gymnasiums ist die ***Kommunikationsplattform IServ***.

2. Mit der ***Einrichtung des Accounts*** erhält der Benutzer ein vorläufiges Passwort, das umgehend durch ein mindestens sechs Zeichen langes, eigenes Passwort zu ersetzen ist. Der Benutzer muss dafür sorgen, dass dieses Passwort nur ihm bekannt bleibt. Alle Login-Vorgänge werden protokolliert und kontrolliert. Das Ausprobieren fremder Benutzerkennungen („Hacking“) mit geratenen oder erspähten Passwörtern muss wie Diebstahl angesehen werden und führt zu entsprechenden Konsequenzen.

3. In der Zugangsberechtigung zu den Schulrechnern ist ein persönliches ***E-Mail-Konto*** enthalten. Die E-Mail-Adresse lautet: **vorname.nachname@schulname.de**. Die Nutzung dieser E-Mail-Adresse ist nur für den schulischen Gebrauch gestattet. Um den reibungslosen Betrieb des E-Mail-Systems zu gewährleisten, gelten folgende Regeln: Nicht erlaubt sind

   3.1. das Versenden von Massenmails, Joke-Mails und Fake-Mails,

   3.2. der Eintrag in Mailinglisten oder Fan-Clubs und die Nutzung von Mail-Weiterleitungsdiensten (GMX, Hotmail, etc.) auf das IServ-Konto.

4. Jeder Benutzer erhält außerdem eine eigene ***Homepage***, die er nach eigenen Vorstellungen gestalten kann. Dieser Bereich dient ausschließlich der Präsentation nicht-kommerzieller Inhalte. Diese Seite ist aus dem Internet unter **http://www.vorname.nachname.schulname.de** zu erreichen.
   Die Veröffentlichung rechtswidriger Inhalte sowie Inhalte, die gegen die guten Sitten verstoßen, führen zum sofortigen Verlust des Accounts. Über die Anwendung von Ordnungs- oder Erziehungsmaßnahmen entscheidet die vom Nds. Schulgesetz vorgesehene Konferenz.
   Es muss ein vorschriftsmäßiges Impressum vorhanden sein. Außerdem ist darauf zu achten, dass Urheberrechte nicht verletzt werden.
   Auf die Möglichkeit der straf- sowie der zivilrechtlichen Verfolgung bei festgestellten Verstößen wird ausdrücklich hingewiesen.

5. Jeder Benutzer erhält einen ***Festplattenbereich*** von 10MB (Homeverzeichnis), der zum Speichern von Mails, der eigenen Homepage und unterrichtsbezogenen Dateien genutzt werden kann. Anderweitige Nutzung ist nicht gestattet. Ein Rechtsanspruch der Nutzer auf den Schutz persönlicher Daten im Netzwerk vor unbefugten Zugriffen besteht gegenüber dem Arminius-Gymnasium nicht.
   Es besteht ebenfalls kein Rechtsanspruch gegenüber dem Arminius-Gymnasium auf die verlustfreie Sicherung der im Netzwerk gespeicherten Daten. Sicherheitskopien wichtiger Dateien auf externen Speichermedien werden dringend empfohlen.
   Eine Geheimhaltung von Daten, die über das Internet übertragen werden, kann in keiner Weise gewährleistet werden. Die Bereitstellung jedweder Information im Internet auf jedwede Art und Weise kommt damit einer Öffentlichmachung gleich. Es besteht daher kein Rechtsanspruch gegenüber dem Arminius-Gymnasium auf Schutz solcher Daten vor unbefugten Zugriffen.

6. Das ***Ablegen von Dateien auf lokalen Festplatten*** ist nicht gestattet. Etwaige dennoch angelegte Dateien werden ohne Rückfrage von Administratoren gelöscht. Das Aufspielen von Software muss vom Systemadministrator genehmigt werden. Das Verändern von Rechnereinstellungen ist verboten.

7. Die ***Nutzung von Internetdiensten*** zu unterrichtlichen Zwecken (Freiarbeit usw.) ist erwünscht. Dazu vergeben die zuständigen Tutoren auf Anfrage Online-Zeitmarken, sog. NACs (Network Access Code) oder schalten die Rechner für den notwendigen Zeitraum frei. Die private Nutzung des Internets ist grundsätzlich nicht gestattet. Der Zugriff auf das Internet wird durchgehend protokolliert, so dass auch im Nachhinein eine eindeutige Kontrolle der Nutzung möglich ist. Die Schule behält sich ausdrücklich das Recht zur Überprüfung der Internetzugriffe vor.

8. Jeder IServ-Nutzer ist verpflichtet, im ***Adressbuch*** seine aktuelle Klasse bzw. den Jahrgang einzutragen. Der Eintrag weiterer Daten darf nur mit dem Einverständnis eines Erziehungsberechtigten erfolgen. Dieses Einverständnis ist unten gegenzuzeichnen. Die Daten bleiben schulintern, sie dienen der besseren Kommunikation untereinander. Bewusst falsche Einträge führen zur Deaktivierung des Accounts.
9. Im ***Schulchat*** wird nicht mit Phantasienamen sondern unter dem eigenen Vornamen gechattet. Als Spitzname ist der Vorname einzustellen.
10. Teilnahme und Nutzung von Chats (auch ICQ) und ***Foren im Internet*** sind nicht erlaubt. Die Abwicklung von geschäftlichen Transaktionen über das Internet (z. B. über ebay) ist ebenfalls nicht zugelassen.
11. Das ***Drucken*** wird über Druck-Marken, sog. PACs (Printer Access Code) ermöglicht. Die Schule stellt den Nutzern diese Möglichkeit zur Verfügung. Druck-Marken werden von den zuständigen Druck-Operatoren vergeben. Die Preisgestaltung orientiert sich an den entstehenden Kosten.
12. Mit meiner Unterschrift erkenne ich diese Benutzerordnung an. Verstöße führen zur sofortigen befristeten, in gravierenden Fällen zur dauernden Sperrung meiner Nutzungsrechte.

_____ _____

Datum Unterschrift der Schülerin / des Schülers

Ich weiß, dass die Schule technisch bedingt das Sperren von Web-Seiten mit strafrechtlich relevanten Inhalten nicht garantieren kann. Ich habe meiner Tochter / meinem Sohn den Zugriff auf solche Seiten ausdrücklich verboten. Ich stimme zu / nicht zu (Unzutreffendes streichen), dass meine Tochter / mein Sohn in seinem Adressbuch weitere Daten (z. B. Anschrift, Telefon-Nr., Geburtsdatum) einträgt.

_____ _____

Datum Unterschrift eines Erziehungsberechtigten

Account eingerichtet durch: am:

8.3. Nutzungsordnung für die Computerräume am Arminius-Gymnasium

Geltungsbereich

Diese Nutzungsordnung ist Bestandteil der jeweils gültigen Schulordnung des Arminius-Gymnasiums.

Die Nutzungsordnung wird in den betroffenen Räumen durch Aushang sichtbar gemacht.

Nutzungsberechtigung

Nutzungsberechtigt sind Schülerinnen und Schüler der Einrichtung im Rahmen des Unterrichts. Außerhalb des Unterrichts kann ein Nutzungsrecht gewährt werden. Die Entscheidung darüber trifft/treffen der/die verantwortlichen Systemadministrator(en).

Weisungsrecht

Weisungsberechtigt sind die unterrichtenden Fachlehrer, der Systemadministrator sowie weitere vom Schulleiter festgelegte Personen.

Verhalten in den Computerräumen

- Innerhalb der Räume ist den Anweisungen der aufsichtführenden Personen Folge zu leisten.
- Das Essen, Trinken und Rauchen in den Computerräumen ist generell untersagt.
- Das Kopieren von Daten, Veränderungen der Installation und Konfiguration der Arbeitsstationen und des Netzwerkes sowie Manipulationen an der Hardwareausstattung sind grundsätzlich untersagt.
- Daten, die während der Nutzung einer Arbeitsstation entstehen, können auf dem zugewiesenen Arbeitsbereich im Netzwerk abgelegt werden.
- Die lokale Festplatte der Arbeitsstation dient nur als Speichermedium für das Betriebssystem und die Anwendungssoftware.
- Daten, die auf der lokalen Festplatte des Computers gespeichert wurden, werden automatisch ohne Rückfrage gelöscht.
- Das Starten von eigenen Programmen, die nicht durch die Schule installiert wurden, bedarf der Genehmigung durch die aufsichtführende Person.

Eingriffe in die Hard- und Softwareinstallation

An den einzelnen Geräten der Computerräume arbeiten täglich die unterschiedlichsten Personen. Jeder Nutzungsberechtigte erwartet, mit der gewohnten Technik in gewohnter Art und Weise arbeiten zu können. Jeder noch so gut gemeinte Eingriff stellt in erster Linie eine Veränderung dar, die das Ausüben erlernter Tätigkeiten behindert und somit störend wirkt. Insofern sind Eingriffe in die Hard- und Softwareinstallation nur mit Erlaubnis der Netzwerkadministratoren zulässig.

Nutzung von Informationen aus dem INTERNET und INTRANET

Die bereitgestellten Informationen können bedingt durch die Art und Weise der Verbreitung keiner hausinternen Selektion unterworfen werden. Sie entstammen weltweit verteilten Quellen und werden durch technisch, nicht inhaltlich bedingte Vorgänge verbreitet. Sollte sich irgendjemand durch solche Informationen verletzt, entwürdigt oder in anderer Art und Weise angegriffen fühlen, muss er diesen Sachverhalt mit dem Urheber der Information klären.

Das Arminius-Gymnasium ist in keiner Weise für den Inhalt der über seinen Internet-Zugang bereitgestellten Informationen verantwortlich.

Die Nutzung des Internets über den Zugang des Arminius-Gymnasiums dient allein unterrichtlich oder schulisch bedingten Zwecken. Die Nutzung von Internetangeboten, die nicht dem Bildungs- und Erziehungsauftrag der Schule entsprechen oder diesem sogar entgegenstehen (beispielsweise rassistische, gewaltverherrlichende, pornographische Seiten) ist ausdrücklich untersagt.
Kein Benutzer hat das Recht, Vertragsverhältnisse im Namen des Arminius-Gymnasiums einzugehen (z. B. Bestellung von Artikeln über das Internet) oder kostenpflichtige Dienste im Internet zu nutzen.

Versenden von Informationen ins INTERNET und INTRANET

Werden Informationen in das Internet versandt, geschieht das unter der Domain (Namen) des Arminius-Gymnasiums. Jede versandte Information kann deshalb durch die Allgemeinheit der Internetnutzer und -betreiber unmittelbar oder mittelbar mit dem Arminius-Gymnasium in Zusammenhang gebracht werden.

Es ist deshalb grundsätzlich untersagt, den Zugang des Arminius-Gymnasiums zur Verbreitung von Informationen zu verwenden, die dazu geeignet sind, dem Ansehen der Einrichtung in irgendeiner Weise Schaden zuzufügen. Dies gilt insbesondere für rassistische, ehrverletzende, beleidigende oder aus anderen Gründen gegen geltendes Recht verstoßende Nachrichten.

Datenschutz und Datensicherheit

Die auf den Arbeitsstationen und im Netzwerk zur Verfügung stehende Software ist für das Arminius-Gymnasium lizenziert. Das Arminius-Gymnasium ist berechtigt, diese Software für Ausbildungszwecke zu nutzen. Eine Vervielfältigung oder Veräußerung ist nicht gestattet.

Alle auf den Arbeitsstationen und im Netzwerk befindlichen Daten (einschließlich persönlicher Daten und E-Mails) unterliegen dem Zugriff des Systemadministrators. Bei Verdacht auf ordnungswidriges Verhalten entscheidet die Schulleitung darüber, die persönlichen Daten und E-Mails verdächtiger Nutzer zu überprüfen. Die Systemadministratoren werden nicht von sich aus tätig.

Ein Rechtsanspruch der Nutzer auf den Schutz persönlicher Daten im Netzwerk vor unbefugten Zugriffen besteht gegenüber dem Arminius-Gymnasium nicht.

Es besteht ebenfalls kein Rechtsanspruch gegenüber dem Arminius-Gymnasium auf die verlustfreie Sicherung der im Netzwerk gespeicherten Daten. Sicherheitskopien wichtiger Dateien auf externen Datenträgern werden dringend empfohlen.

Eine Geheimhaltung von Daten, die über das Internet übertragen werden, kann in keiner Weise gewährleistet werden. Die Bereitstellung jedweder Information im Internet auf jedwede Art und Weise kommt damit einer Öffentlichmachung gleich. Es besteht daher kein Rechtsanspruch gegenüber dem Arminius-Gymnasium auf Schutz solcher Daten vor unbefugten Zugriffen.

Eine Virenfreiheit des Systems wird angestrebt, kann aber nicht garantiert werden. Werden ausnahmsweise in den Räumen des Arminius-Gymnasiums benutzte Disketten auf anderen externen Rechnern verwendet, so sind diese vorher unbedingt auf Virenbefall zu prüfen. Schadenersatzansprüche können in diesem Zusammenhang gegenüber dem Arminius-Gymnasium nicht geltend gemacht werden.

Zuwiderhandlungen

Nutzer, die unbefugt Dateien von den Arbeitsstationen oder aus dem Netzwerk kopieren, machen sich strafbar und können sowohl zivil- als auch strafrechtlich verfolgt werden.

Zuwiderhandlungen gegen diese Ordnung können neben dem Entzug der Nutzungsberechtigung für das Netzwerk und die Arbeitsstationen disziplinarische Maßnahmen nach sich ziehen. Insbesondere ein Missbrauch des Internet-Zugangs kann schwere disziplinarische Maßnahmen nach sich ziehen.

Kalkriese, den 13.02. 2001

(Der Schulleiter)