

Medienentwicklungsplan der Stadt Münster

Fortschreibung

: Amt für Schule
und Weiterbildung:

Impressum

Herausgeberin:

Stadt Münster

Amt für Schule und Weiterbildung

48127 Münster

Tel.: 0251 / 492-4001

Fax: 0251 / 492-7723

Mail: schulamt@stadt-muenster.de

citeq

48127 Münster

Tel.: 0251 / 492-1801

Fax: 0251 / 492-7710

Mail: info@citeq.de

Autoren:

Eugen Rickling

Markus Rother

Helmuth Gauczinski

Norbert Spichala

Amt für Schule und Weiterbildung

citeq

citeq

citeq

September 2007

I.	Neue Medien in Schulen - Fortschreibung	1
1.	Allgemeine Anforderungen und Vorgaben	1
1.1.	Notwendigkeit der Fortschreibung.....	1
1.2.	Rahmenbedingungen und Grundsatzentscheidungen	1
1.3.	Änderungen	3
1.4.	Ausgangssituation 2007	4
1.4.1.	Schulen und Schüler im Schuljahr 2006/2007	4
1.4.2.	Ausstattung der Schulen mit IT	4
2.	IT-Konzeption	6
2.1.	Zielsetzung	6
2.2.	Reinvestition der Hardware - Planung und Umsetzung	7
2.2.1.	Grundsätzliches	7
2.2.2.	Start der schulspezifischen Projekte	8
2.2.3.	Auftrag der Schule	8
2.2.4.	Umsetzung des Reinvestitionsprojekts.....	9
2.2.5.	Verwendung der Althardware	9
2.3.	Diebstähle	9
2.4.	Software.....	11
2.4.1.	Softwareausstattung der Schulverwaltungen	11
2.4.2.	Software für den unterrichtlichen Bereich	11
3.	Kundenbetreuung	13
3.1.	Allgemeines	13
3.2.	MEP-net.....	14
3.3.	Anwendertreffen	15
4.	Medienpädagogische Begleitung	15
5.	IT-Nutzungsvereinbarungen für Schulverwaltungen.....	16
II.	Ausstattungs- und Betriebskonzept	17
1.	Technische Grundsatzentscheidungen	17
1.1.	Allgemeines	17
1.2.	Servertechnologie.....	17
1.3.	Clients.....	18
1.4.	Drucker	18
1.5.	Monitore.....	19
1.6.	Einbindung eigener Systeme.....	19
2.	Beschaffung	20

3. Katalog der Standardkomponenten	21
4. Datenschutz und Datensicherheit	21
5. Protokollierung von Nutzerdaten	23
6. Internetauftritt der Schulen	24
7. IT-Bestandsmodul der citeq.....	24
8. Technisches Ausstattungskonzept.....	25
8.1. Netzwerk.....	25
8.2. Inhouse-Verkabelung / Netzkomponenten - LAN (Local Area Network).....	26
8.3. WLAN (Wireless Local Area Network)	30
8.4. Anbindung der Schulen an die citeq - WAN (WideAreaNetwork)	31
8.5. Streaming	31
8.6. Netzwerkmanagement.....	32
9. Server	33
9.1. Hardwareausstattung	33
9.2. Virtualisierung von Servern	36
9.3. Betriebssystem und Version.....	37
9.4. Serverdienste.....	38
9.4.1. Fileservices.....	38
9.4.2. Printservices	39
9.4.3. Dynamic Host Control Protocol (DHCP).....	39
9.4.4. Domain Name Service (DNS).....	39
9.4.5. Mailing	40
9.4.6. Spam	40
9.4.7. Intranet in der Schule	41
9.4.8. Virenschutz	42
9.4.9. CD -Manager	42
9.4.10. Internetzugang mittels Proxy-Services.....	42
9.5. Internetfilter SquidGuard	43
9.6. Arbeiten bei Ausfall der Netzanbindung.....	44
9.7. Benutzer-/Gruppenverwaltung / eDirectory	44
9.8. Rechte der IT-Koordinatoren	46
9.9. Datenhaltung	47
9.10. Softwarerepository.....	48
9.11. Datensicherung Server.....	49
9.12. Remote Administration	51
10. Clients	51
10.1. Hardwareausstattung	51
10.2. Wächterschutz	51

10.3. Betriebssystem	52
10.4. Clientsoftware	53
10.4.1. Standardsoftware.....	53
10.4.2. Stand-alone-Betrieb.....	55
10.4.3. Servergespeicherte Profile (Roaming-Profiles)	55
10.4.4. Verbindliche Profile (Mandatory-Profiles)	55
10.4.5. Virenschutz und Updates	56
10.5. Vorbereitung der Clients und Softwareverteilung.....	56
11. Technisches Betriebskonzept	59
11.1. Begriffsdefinition	59
11.2. Service-Desk / Störungsmeldung und –verfolgung.....	59
11.3. Problemmanagement	62
11.4. Konfigurations- und Änderungsmanagement.....	62
11.5. Testcenter	63
11.6. Qualitätsmanagement	63
11.7. Operations Management	64
11.7.1. Überwachung der IT-Infrastruktur.....	64
11.7.2. Störungsbehebung	65
11.7.3. Aufgaben der IT-Koordination	65
11.7.4. Störungen der Leitungsanbindung (WAN)	66
11.7.5. Störungen des Inhouse-Netzes (LAN).....	66
11.7.6. Störungen dezentraler und zentraler Server	66
11.7.7. Störungen zentraler Dienste	67
11.7.8. Störungen von Client-Rechnern	67
11.7.9. Wartung der Beamer	67
Glossar	69

I. Neue Medien in Schulen - Fortschreibung

1. Allgemeine Anforderungen und Vorgaben

1.1. Notwendigkeit der Fortschreibung

Die Stadt Münster hat mit der Verabschiedung des Medienentwicklungsplanes im Jahre 2002 die notwendigen Strukturen für ein neues Lernen und Lehren an den städt. Schulen geschaffen. Der MEP wurde den Wünschen der Schulen gerecht, in dem er die Ausstattungsmängel in den Schulen beseitigte, für die notwendige Entlastung der bis dahin für die Wartung und Betreuung der Hardware zuständigen Lehrerinnen und Lehrer sorgte, eine gesicherte IT-Infrastruktur bereitstellte und die Schulverwaltungen an das städtische Netz anband.

Eine Fortschreibung des Medienentwicklungsplanes war bereits bei seiner Erstellung im Jahre 2002 vorgesehen, um den organisatorischen, technischen und pädagogischen Anforderungen und Änderungen, die sich während der Umsetzungsphase des MEP ergeben würden und auch ergeben haben, Rechnung zu tragen.

Im Rahmen dieser Fortschreibung werden die aktuellen und mit dem MEP gesetzten Standards daraufhin überprüft, ob sie sich bewährt haben. Die Wünsche der Schulen, die sich insbesondere in der im Januar 2007 durchgeführten Kundenumfrage der citeq geäußert haben, werden, sofern wirtschaftlich und technisch sinnvoll und möglich, ebenfalls berücksichtigt.

Natürlich werden auch die aktuellen Technikrends aufmerksam verfolgt und bewertet und nach Möglichkeit im Rahmen des MEP berücksichtigt.

1.2. Rahmenbedingungen und Grundsatzentscheidungen

Wesentlicher Bestandteil eines ganzheitlichen und zukunftsicheren Konzeptes für die Wartung der IT-Infrastruktur in den Schulen der Stadt Münster ist die Festlegung und Einhaltung der Rahmenbedingungen. Die Erfahrungen aus der erstmaligen Umsetzung des MEP bestätigen den bereits bei der Erstellung des MEP aufgestellten Kernpunkt:

Standardisierung

Für eine verlässliche Kalkulation der Wartungs- und Betreuungsaufwände stellt eine standardisierte IT-Infrastruktur für alle Schulen die Grundvoraussetzung dar. Nur so ist

es möglich, den MEP mit den vom Rat der Stadt Münster zur Verfügung gestellten Mitteln wirtschaftlich zu betreiben.

Für die Umsetzung der Standardfestlegungen mussten daher einige Grundsatzentscheidungen getroffen werden. Neben technischen Entscheidungen wurden auch folgende allgemeine Bedingungen festgelegt:

- Alle Schulen bleiben breitbandig an die citeq und an das Internet angebunden.
- Die Reinvestition der in den Schulen eingesetzten Rechner (einschließlich Notebooks) und Monitore erfolgt regelmäßig nach den festgelegten Standzeiten (zurzeit 4,5 Jahre).
- Die Röhrenmonitore werden bei der Reinvestition durch TFT-Monitore ersetzt.
- Die sonstige Hardware wird erst dann ausgetauscht, wenn sie aus technischen oder wirtschaftlichen Gründen nicht mehr eingesetzt werden kann.
- Es werden keine lokalen Drucker mehr installiert.
- Die Endgeräte- und Softwareausstattung der Schulen erfolgt aus einem Warenkatalog, der der ständigen Fortschreibung unterliegt.
- Installationen im pädagogischen Netz erfolgen durch die citeq.
- Schuleigene Drucker und Kopierer, die aktuell auch bei der Stadtverwaltung eingesetzt werden, können in das Schulnetz integriert werden.
- Schuleigene PDA (Personal Digital Assistants), die aktuell auch bei der Stadtverwaltung eingesetzt werden, können in das Schulnetz (Verwaltung) integriert werden.
- Sonstige schuleigene Hardware wird nicht in das Schulnetz integriert.
- Die bestehenden IT-Dienstanweisungen für die Stadt Münster werden als IT-Nutzungsvereinbarungen auf den Verwaltungsbereich der Schulen angepasst, damit sie auch für die dort tätigen Lehrkräfte Gültigkeit haben.
- Die Schulen erhalten Zugriff auf das IT-Bestandsmodul der citeq und pflegen darüber selbst durchgeführte Bestandsveränderungen.

Wichtige Maßnahmen und Entscheidungen im Rahmen des MEP werden in der Lenkungsgruppe beraten. Die Lenkungsgruppe besteht aus jeweils einem Vertreter der Schulformen und dem Medienberater des Kompetenzteams Münster.

1.3. Änderungen

Die wesentlichen Änderungen der Fortschreibung sind hier im Überblick aufgeführt. Eine detaillierte Erläuterung und Begründung wird im Ausstattungs- und Betriebskonzept vorgenommen.

- Verzicht auf lokale Drucker und CRT-Monitore,
- Festlegung eines einheitlichen Monitorstandards,
- Kennzeichnung der Hardware gegen Diebstahl,
- Zentrale Datensicherung an Stelle von lokalen Bandsicherungen,
- Erhöhte Verfügbarkeit von Servern (u. a. durch Einsatz von USV),
- Mehr (ungesicherter) Speicherplatz in der Pädagogik,
- Ausschluss bestimmter Dateitypen von der regelmäßigen Sicherung,
- Einsatz eines Internetfilters (SquidGuard),
- Umstellung des Serverbetriebssystems auf Novell Linux OES,
- Erweiterung der Rechte für IT-Koordinatoren,
- Einrichtung von Quoting in der Pädagogik,
- Einsatz der Wächterschutzsoftware „Drive“ (statt Hardwarelösung PC-Wächterkarte) im unterrichtlichen Bereich,
- Stand-alone-Betrieb, lokale Benutzerkonten zur Nutzung der Rechner ohne Netzwerkverbindung,
- Wahlweise Einrichtung von servergespeicherten (Roaming-Profiles) und verbindlichen Profilen (Mandatory-Profiles),
- Einführung eines Verfahrens zur Wartung der Beamer,
- Kundenbetreuung mit festen Ansprechpartnern je Schule,
- Informationsportal MEP-net.
- Optional:
 - Einbindung schuleigener standardisierter Drucker,
 - Einbindung schuleigener standardisierter PDA (Personal Digital Assistants),
 - Unterstützung im Bereich Internetauftritt der Schulen
 - Streaming
 - WLAN (Wireless Local Area Network) in der Pädagogik
 - Virtualisierung von Servern in Schulzentren

1.4. Ausgangssituation 2007

1.4.1. Schulen und Schüler im Schuljahr 2006/2007

In Münster gibt es zur Zeit 89 städtische Schulen mit rund 44.000 Schülerinnen und Schülern. Die Zahl der Schulen hat damit seit der Erstellung des MEP im Jahre 2002 um zwei abgenommen (zwei Grundschulen: Josefschule, Gertrudenschule). Die Zahl der Schüler und Schüler hat zugenommen. Die Verteilung auf die verschiedenen Schulformen stellt sich wie folgt dar:

Schulform	Anzahl der Schulen	Zahl der Schüler/innen	Veränderung Zahl der Schüler/innen gegenüber 2002
Grundschulen	46	9.800	+44
Hauptschulen	8	2.744	-434
Realschulen	10	4.896	-77
Gymnasien	12	9.771	+1081
Förderschulen	7	1.296	-16
Berufskollegs	6	15.455	+341
Summe	89	43.962	+939

Tabelle 1: Verteilung der Zahl der Schulen sowie Schüler/innen auf die verschiedenen Schulformen (einschl. Abendrealschule und Abendgymnasium), Stand: Oktoberstatistik 2006

Hinweis: Berufskollegs sind nicht in den MEP einbezogen.

1.4.2. Ausstattung der Schulen mit IT

Bei der Ausstattung der Schulen ist zu unterscheiden zwischen dem unterrichtlichen Bereich und dem Schulverwaltungsbereich. Die Schulverwaltung besteht aus der Schulleitung, dem Sekretariat sowie aus dem Lehrpersonal mit besonderen Funktionen (Oberstufenkoordination, Stundenplanung etc.). Beide Bereiche verfügen aus datenschutzrechtlichen Gründen über jeweils eigenständige Netzwerke.

Ende 2006 war der Medienentwicklungsplan an 80 Schulen umgesetzt. Lediglich die Augustin-Wibbelt-Schule, die Helen-Keller-Schule und das Abendgymnasium waren noch nicht einbezogen.

Sowohl im unterrichtlichen Bereich als auch im Schulverwaltungsbereich sind die Schulgebäude mit einer vollständigen Inhouse-Verkabelung ausgestattet.

Insgesamt sind etwa 2.760 PC und Notebooks mit den dazugehörigen Peripheriegeräten in den Schulen installiert. Die schulformbezogene Verteilung stellt sich wie folgt dar:

Schulform	PC	Notebooks	Drucker	Scanner	Beamer
Grundschulen:	596	46	156	37	22
Hauptschulen:	262	145	68	23	25
Realschulen:	318	128	72	33	32
Gymnasien:	820	190	155	37	92
Förderschulen:	139	14	86	15	5
SZ Kinderhaus (Realsch./Gymn. - gemeinsame Nutzung):	104	21	22	5	27
Summe:	2.239	544	559	150	203

Tab. 2: MEP- Hardwareausstattung 2003-2006 getrennt nach Schulform und Hardwarekomponenten (ohne Augustin-Wibbelt-Schule, Helen-Keller-Schule und Abendgymnasium)

Die Verteilung der PC bzw. Notebooks auf die Verwaltungs- bzw. Pädagogikbereiche stellt sich aktuell wie folgt dar:

Schulform	Zahl der MEP-Schulen	PC / Notebook	davon Verwaltung		davon Pädagogik
		insgesamt	insgesamt		insgesamt
GS	46	642	132		510
HS	8	407	47		360
RS	10	492	38		408
GY	11	1089	138		872
FÖ	5	153	19		134
Summen	80	2783	374		2284

Tab. 3: Verteilung der PC/Notebooks auf die Verwaltungs- und Pädagogikbereiche der jeweiligen Schulform (ohne Augustin-Wibbelt-Schule, Helen-Keller-Schule und Abendgymnasium) - Stand: Ende 2006

Darüber hinaus sind 147 Server und rund 450 aktive Netzwerkkomponenten (Switches) für den Betrieb der Netzwerke in den Schulen installiert.

2. IT-Konzeption

2.1. Zielsetzung

*W*er aufhört, besser werden zu wollen, hört auf, gut zu sein

Marie von Ebner-Eschenbach
österr. Schriftstellerin 1830-1916

Das Lernen mit neuen Medien erfordert eine Infrastruktur, die leistungsfähig, dauerhaft verfügbar und zukunftsorientiert ist. Mit der ersten Umsetzung des MEP in den Jahren 2003 bis 2006 ist die Stadt Münster diesen Anforderungen bereits nachgekommen. Gleichwohl haben sich die damaligen Zielsetzungen nicht grundlegend verändert und müssen auch zukünftig beachtet und verfolgt werden.

Allgemeine Ziele

- Die IT-Ausstattung soll kostenextensiv insbesondere bzgl. der laufenden Kosten und damit dauerhaft finanzierbar sein.
- Vorhandene IT-Komponenten können integriert werden, wenn wirtschaftlich und technisch sinnvoll.
- Die Infrastruktur soll zukunftssicher sein.
- Eine angemessene Verfügbarkeit der Systeme ist sicherzustellen.

Unterrichtlicher Bereich

- Die pädagogischen Anforderungen der Schulen sollen möglichst optimal abdeckt werden
- Zur Sicherung einer hohen Verfügbarkeit der Systeme sollen die Administration und die qualifizierte Wartung der Systeme grundsätzlich durch professionelles Personal des Schulträgers erfolgen.
- Um Anwendungssängste abzubauen, sollen die Systeme durch die Lehrkräfte und Schülerinnen und Schüler einfach zu bedienen und gegen Manipulationsversuche weitgehend geschützt sein.
- Einzelne schulspezifische Administrationen und kleinere Fehlerbehebungen sollen durch IT-Koordinatoren in den Schulen (Fachlehrer mit entsprechender Einweisung) ermöglicht werden.

- Problemlose Zusammenarbeit mit zentralen Diensten wie Mailserver, Internet (Zugriffsverweigerung für unerwünschte Webseiten), Firewall für alle Schulen → Verhinderung des Missbrauchs des Internets.

Verwaltung

- Die Sicherung der personenbezogenen Schüler- und Lehrerdaten soll datenschutzrechtliche Anforderungen erfüllen.
- Das Verwaltungsnetz muss vom pädagogischen Netz getrennt und auch gegen Gefahren aus dem Internet geschützt sein.
- Die Kommunikation und Information der Schulverwaltung mit dem Amt für Schule und Weiterbildung und übergeordneten Stellen (Intranet) soll vereinfacht werden.
- Die Funktionalitäten, Zuverlässigkeit und Verfügbarkeit sollen den Standards der Stadtverwaltung entsprechen.

2.2. Reinvestition der Hardware - Planung und Umsetzung

2.2.1. Grundsätzliches

Bei der Umsetzung des IT-Konzeptes nach den zentralen Vorgaben und den schulspezifischen Wünschen wird jede Schule im Rahmen der Reinvestition als eigenständiges Projekt geführt (Reinvestitionsprojekt). Jedes Reinvestitionsprojekt wird von einem/einer zentralen Ansprechpartner/in beim Amt für Schule und Weiterbildung und bei der citeq geleitet (siehe auch unter „Kundenbetreuung“). Die Planung und Terminierung der Reinvestitionsprojekte erfolgt grundsätzlich in Abstimmung zwischen dem Amt für Schule und Weiterbildung und der citeq für ein Kalenderjahr im Voraus.

Alle PC, Notebooks und Monitore die älter als 4,5 Jahre sind, werden ausgetauscht. Die übrige Hardware (insbesondere Drucker, Beamer und Scanner) wird erst dann reinvestiert, wenn sie aus technischen oder wirtschaftlichen Gründen nicht mehr eingesetzt werden kann. Dieses wird dann im Rahmen der laufenden Betreuung der Schulen geschehen. Ausgenommen hiervon sind die lokalen Drucker, die im Rahmen des jeweils ersten Reinvestitionsprojekts in das der Schule zur Verfügung stehende Budget eingerechnet werden mit dem Ziel, dass stattdessen andere Hardware (insbesondere Netzwerkdrucker) installiert wird.

Durch verschiedene Einflüsse seit der Erstausrüstung der einzelnen Schulen (z. B. Defekte, Diebstähle, Nachinstallationen) sind einzelne PC, Notebooks und Monitore zum Zeitpunkt des Reinvestitionsprojekts noch nicht älter als 4,5 Jahre. Diese Hardware wird erst dann ausgetauscht, wenn sie das entsprechende Alter erreicht hat.

2.2.2. Start der schulspezifischen Projekte

Rechtzeitig vor Projektstart (i. d. R. 12 Wochen vorher) werden in einem gemeinsamen Gespräch (Amt für Schule und Weiterbildung, citeq und Schule) der Projektablauf erläutert und die Termine abgestimmt. Das Beratungsgespräch wird dokumentiert und den Gesprächsteilnehmern zur Verfügung gestellt.

Die Schule erhält von der citeq eine Übersicht der Hardware, die im Rahmen des Reinvestitionsprojekts ausgetauscht werden soll. Die Schule überprüft die Standorte und meldet die Veränderungen an die citeq zurück.

2.2.3. Auftrag der Schule

Das Amt für Schule und Weiterbildung stellt der Schule eine Liste mit dem Ausstattungsrahmen zur Verfügung, die die Basis für die Installation der neuen Hardware bildet. Anhand dieses Rahmens entscheidet sich die Schule für die Neuausrüstung mit Hardware. Dafür sendet sie die ausgefüllte Budgetliste bis spätestens acht Wochen vor Projektbeginn an das Amt für Schule und Weiterbildung und an die citeq mit den folgenden Angaben zurück:

- Standort der neuen Hardware
- Benennung der ggfs. neu zu patchenden Netzwerkdosen
- zu installierende Software

Die Unterlagen der Schule stellen für die citeq den Auftrag für die Durchführung des Reinvestitionsprojekts dar.

Auf der Grundlage des Auftrags bestätigt die citeq der Schule den Leistungsumfang und die Terminkette für das Reinvestitionsprojekt (Auftragsbestätigung).

2.2.4. Umsetzung des Reinvestitionsprojekts

Nach der Auftragsbestätigung werden durch die citeq unverzüglich die erforderlichen Schritte für die Beschaffung der für das Projekt erforderlichen Hardware in die Wege geleitet. Informationen über evtl. Lieferverzögerungen, die die planmäßige Durchführung des Projektes gefährden könnten, sind unverzüglich mit dem Amt für Schule und Weiterbildung und der Schule zu kommunizieren.

Im Reinvestitionsprojekt wird die vereinbarte Hardware funktionsfähig an die Schule übergeben.

Zum Abschluss des Projektes wird ein Abnahmetermin mit der Schule vereinbart. Das in diesem Rahmen mit der Schule zu führende Abnahmegespräch dient der Qualitätssicherung des durchgeführten Reinvestitionsprojekts. Anschließend erklärt die Schule schriftlich die Abnahme des Projekts.

2.2.5. Verwendung der Althardware

Nach der Standzeit von zurzeit 4,5 Jahren ist die Althardware technisch überholt und auch vermehrt reparaturanfällig. Der weitere Betrieb im MEP-Netz ist daher aus technischen und wirtschaftlichen Gründen nicht sinnvoll.

Auch die netzunabhängige Nutzung ist nicht möglich, da alle Softwareinstallationen aus lizenzrechtlichen Gründen durch die citeq deinstalliert werden müssen.

Die Althardware wird daher vollständig abtransportiert.

2.3. Diebstähle

Die Erfahrungen im Verlauf der Erstausrüstung machen deutlich, dass Schutzmaßnahmen gegen Einbruch und Diebstahl ergriffen werden müssen. Die von der citeq installierten Geräte sind zwar gegen Einbruchdiebstahl versichert. Das Schadensaufkommen ist jedoch so hoch, dass mit deutlichen Prämien erhöhungen bzw. mit der Kündigung des Versicherungsschutzes gerechnet werden muss.

Die in Betracht kommenden Maßnahmen zur Verbesserung des Einbruchschutzes wurden mit Vertretern des Polizeipräsidiums Münster, der Westfälischen Provinzial Versi-

cherung AG, des Amtes für Schule und Weiterbildung, des Amtes für Gebäudemanagement und der citeq erörtert.

Als Ergebnis des Prüfverfahrens wurde seitens der citeq ein in Abstimmung mit dem Hersteller der Hardware ausgewähltes Verfahren zur Kennzeichnung der Geräte eingeführt. Die Kennzeichnung ist allerdings auf Notebooks beschränkt, da diese bisher den größten Anteil an der Schadenshöhe hatten. Die Kennzeichnung erfolgte mit einem Aufkleber, der mit einem Spezialkleber befestigt wurde und einer Zugfestigkeit von bis zu 400 kg widersteht. Durch die Verwendung des Spezialklebers wird ein weiterer, auf den ersten Blick nicht sichtbarer Aufkleber derart mit dem Notebookdeckel verschweißt, dass die Entfernung ohne Beschädigungen am Notebookdeckel nicht mehr möglich ist. Der untere Aufkleber kennzeichnet das Notebook als Eigentum der citeq, das gestohlen worden ist.

Die Erfahrungen des Anbieters und der Polizei lassen erwarten, dass sich die Diebstahlquote durch die Kennzeichnung deutlich verringern wird. Die Kennzeichnung erfolgt an Neugeräten und an bereits ausgelieferten Geräten bis zu einem Gerätealter von 3 Jahren und wird über eine Pressemitteilung entsprechend kommuniziert.

Darüber hinaus hat das Amt für Schule und Weiterbildung in Abstimmung mit der citeq die Schulen über die Folgen von Einbrüchen und Diebstahl informiert. Dabei wurden auch die von den Schulen selbst durchführbaren Maßnahmen (z. B. Ausgabeverfahren, grundsätzlicher Umgang mit Hardware, erhöhte Aufmerksamkeit) angesprochen.

In Einzelfällen wird ein gemeinsamer Beratungstermin mit der Polizei und Versicherung stattfinden. Das Amt für Schule und Weiterbildung und die citeq bleiben mit diesen Einrichtungen in Kontakt. Dabei werden weitere in Betracht kommende Diebstahlschutzmaßnahmen hinsichtlich ihrer Wirtschaftlichkeit und Zweckmäßigkeit geprüft.

2.4. Software

2.4.1. Softwareausstattung der Schulverwaltungen

Die Softwareausstattung in der Schulverwaltung orientiert sich an den Ausstattungsrichtlinien der Stadtverwaltung Münster. Um Synergieeffekte zu nutzen und damit Kosten zu reduzieren, gelten in den Schulverwaltungen die gleichen Ausstattungsgrundsätze bei der Standardsoftware wie bei der Stadt Münster, Erfahrungen, die die citeq bei der Betreuung des relativ großen Netzwerks der Stadtverwaltung Münster macht, kommen so auch unmittelbar den Schulverwaltungen zugute. Dadurch können weitere Verbesserungen in der Betreuungs- und Beratungsleistung erzielt werden.

Darüber hinaus werden auf allen Verwaltungsrechnern die folgenden vom Land NRW kostenlos bereitgestellten Softwareprodukte zur Schulverwaltung installiert:

- SchILdNRW
- ASDPC
- WinPlan
- Kurs42

Die Festlegung weiterer Produkte als Standardsoftware für Schulverwaltungen erfolgt in Abstimmung mit den Schulen.

2.4.2. Software für den unterrichtlichen Bereich

Im unterrichtlichen Bereich wird Software, die über die Standard-Applikationen hinausgeht, grundsätzlich nur im Rahmen des vereinbarten Kataloges installiert. Ausnahmen von dieser Vorgehensweise werden nur in begründeten Einzelfällen vereinbart. Bei der Vielzahl der unterschiedlichsten Anwendungen in den Schulen ist eine individuelle Softwareinstallation und –betreuung ohne einen vorgegebenen Rahmen mit den beschränkten personellen und finanziellen Ressourcen nicht zu leisten. Die Beibehaltung der heterogenen Softwarelandschaft würde zu einer wesentlichen Verschlechterung der Serviceleistungen führen oder einen deutlich erhöhten Personalbedarf für die Betreuung erfordern. Aus diesem Grund wird von einer durch die Schulen vorgegebenen, beschränkten Produktmenge (dem Software-Katalog) ausgegangen, um durch zentrale Lizenz- und Softwarebeschaffung für die Schulen eine kostengünstige und übersichtliche Möglichkeit

zu schaffen, die geeignete Lernsoftware für die jeweiligen pädagogischen Anforderungen auszuwählen. Dadurch lassen sich die Kosten für Wartung und Administration reduzieren.

Der Software-Katalog wird in regelmäßigen Zyklen in Verbindung mit den Schulvertretern an die veränderten Gegebenheiten angepasst. Neue Lehrpläne, neue Produkte, veränderte Lizenzbedingungen oder technische Anpassungen sind die Faktoren, die u.a. eine regelmäßige Überarbeitung des Warenkataloges notwendig machen. Die von den jeweiligen Schulformen geäußerten und priorisierten Softwarewünsche werden über den Schulformvertreter an die Lenkungsgruppe, die citeq und das Amt für Schule und Weiterbildung geleitet. In der Lenkungsgruppe werden die Wünsche aggregiert und als Arbeitsplanung für die Softwaretests der citeq in eine priorisierte Gesamtliste übertragen. Die Lenkungsgruppe ist damit das letztlich entscheidende Gremium. Die citeq prüft und bewertet die Produkte, die in den Katalog aufgenommen wurden auf ihre technische Einsetzbarkeit. Der Status der Tests wird im MEP-net veröffentlicht.

Die citeq wird gemeinsam mit der Lenkungsgruppe eine technische Lösung erarbeiten, die die browserbasierte Erfassung und Weiterleitung von Softwareprodukten an die citeq ermöglicht.

Hinsichtlich der Eignung von Softwareprodukten ist folgendes zu beachten:

- Software ist nur auf den Rechnern ablauffähig, die die vom Hersteller genannten Mindestanforderungen an Betriebssystem, Prozessor, Hauptspeicher usw. erfüllen.
- Software darf nur installiert werden, wenn die rechtlichen Voraussetzungen für ihren Einsatz gegeben sind (Software-Lizenz, Freeware).

Die vollständige Verfügbarkeit und Funktionalität der installierten Software kann – aufgrund der Einschränkungen, die die Wächtersoftware mit sich bringt sowie der Tatsache, dass zum ordnungsgemäßen Betrieb unter Umständen auf Ressourcen im Netz zugegriffen werden, nur in einer vernetzten Umgebung garantiert werden.

Um die volle Funktionalität der Lernsoftware zu sichern, wird die Software auf unterschiedlichsten Wegen zur Verfügung gestellt. Die Speicherung von Lernständen, Zugangskennungen oder Zugriffe auf externe Medien machen für einige Programme einen Netzwerkzugriff zur Laufzeit erforderlich oder es kommen bewusst reine Netzwerkversi-

onen zum Einsatz. Das hat zur Folge, dass im netzunabhängigen Stand-alone-Betrieb Programme nur in Ausnahmefällen uneingeschränkt nutzbar sind; Arbeitsergebnisse oder Lernstände können nicht oder nur eingeschränkt gespeichert werden. Die Einstellungen für das Programm werden nicht wirksam. Für den Fall, dass die Leitungsanbindung zur citeq zur Verfügung steht, ist der Netzwerkzugriff innerhalb der Schule uneingeschränkt möglich. Die für den Stand-alone-Betrieb genannten Einschränkungen gelten dann nicht.

3. Kundenbetreuung

3.1. Allgemeines

Bei der Aufstellung des MEP wurde der Bereich Kundenbetreuung nicht in dem erforderlichen Maß berücksichtigt. Es wurde davon ausgegangen, dass sich die Betreuung der Schulen durch die citeq im Wesentlichen auf die Beseitigung von Störungen und Installation neuer Softwareprodukte für den unterrichtlichen Bereich beschränken wird.

Die Erfahrungen des MEP haben allerdings gezeigt, dass eine dauerhafte Betreuung der Schulen durch feste Ansprechpartner für eine erfolgreiche Umsetzung des MEP eine wichtige Voraussetzung darstellt. Das ist auch ein Ergebnis aus der Anfang 2007 durchgeführten Kundenbefragung der citeq. Die Schulen wünschen sich dabei auch die regelmäßige Präsenz der Kundenbetreuer in den Schulen zu Beratungsterminen, um dem laufenden Informations- und Abstimmungsbedarf nachkommen zu können. Dabei geht es z. B. um Themen wie die

- Nutzung des Netzwerks,
- Nutzung der Hardware,
- räumliche Verteilung der Hardware,
- Installation von weiteren Softwareprodukten,
- Verwaltung der Benutzerkennungen,
- Entwicklung neuer Lösungen mit der nun zur Verfügung stehenden Technik.

Der Beratungsbedarf wird insbesondere aufgrund der steigenden Technisierung im Schulumfeld und den damit einhergehenden (neuen) Anforderungen fortbestehen, evtl. sogar noch steigen. Ebenso ist die citeq auf Informationen und Beratung durch die Schulen angewiesen. Aus diesem Grund hat die ständige Kommunikation zwischen den Schulen und der citeq eine große Bedeutung. Besondere oder innovative Nutzungsmög-

lichkeiten der installierten Technik können häufig erst nach einer längeren Erfahrungsphase erkannt werden. Nur in enger Abstimmung mit den Schulen lassen sich die besonderen Anforderungen aus der Pädagogik und der Schulverwaltung in der Praxis umsetzen, sodass die Potentiale hier entsprechend ausgeschöpft werden können. Hierbei setzen allerdings die zur Verfügung stehenden Personalkapazitäten Grenzen.

Für die laufende Betreuung der Schulen sind beim Amt für Schule und Weiterbildung und bei der citeq feste Ansprechpartner vorgesehen, die den Schulen in allen IT-Fragen beratend zur Seite stehen.

Bei der Reinvestition wird aufgrund der von den Schulen im Rahmen des MEP gemachten Erfahrungen und unter Berücksichtigung der neuen Rahmenbedingungen des technischen Betriebskonzeptes (siehe unter II. 1. "Technische Grundsatzentscheidungen") die Hardware nicht in identischer Weise ersetzt. Daher muss zur Vorbereitung der Reinvestitionsprojekte (siehe unter II. 2.2. "Reinvestition der Hardware - Planung und Umsetzung") ein mit der Erstausrüstung vergleichbares Beratungsverfahren durchgeführt werden.

3.2. MEP-net

Zur Bereitstellung von Informationen für die Schulen wurde im ersten Halbjahr 2007 eine Internetplattform eingerichtet. Diese wird MEP-net genannt und ist sowohl über das Verwaltungsnetz als auch über das pädagogische Netz der Schulen allen Lehrkräften, Sekretärinnen und Hausmeistern (sofern eine Kennung eingerichtet wurde) zugänglich. Die Lehrkräfte haben zudem über das Internet auch außerhalb der Schule Zugang zum MEP-net. Die Authentifizierung erfolgt über die für die Lehrkräfte eingerichteten Novell-Benutzerkennungen.

Im MEP-net werden wesentliche Informationen für die Lehrkräfte veröffentlicht. Darüber hinaus werden hierüber aktuelle Mitteilungen der citeq für die Lehrkräfte kommuniziert. Im MEP-net werden z. B.

- die aktuellen Hardwarestandards,
- die aktuellen Softwarestandards,
- Hinweise der Anwenderbetreuung zur Nutzung der IT allgemein,
- Hinweise zur Nutzung von Tools für IT-Koordinationen,
- Hinweise zur Benutzerverwaltung,
- Hinweise zu geplanten Wartungsarbeiten,

- Verlinkungen zum Service-Desk,

veröffentlicht.

Weiterhin bietet das Intranet der Stadt Münster Informationen für die Schulverwaltungen. Auch hier erfolgt die Authentifizierung über die für die Mitglieder der Schulverwaltung eingerichteten Novell-Benutzerkennungen.

3.3. Anwendertreffen

Die citeq führt schulformbezogene Anwendertreffen durch. Für diese Treffen werden vorab über die Lenkungsgruppe Themen abgefragt, damit die Vorbereitung und Teilnahme von Vertretern der citeq auf den Anwendertreffen entsprechend abgestimmt werden kann. Die Treffen finden für jede Schulform ein Mal im Jahr statt.

4. Medienpädagogische Begleitung

Mit der Bereitstellung von Hard- und Software sowie der Anbindung an das Internet haben die Schulen die ideale Plattform zur Integration neuer Medien in den Unterricht und zur Stärkung der Medienkompetenz erhalten.

Es werden hier jedoch zwei eigenständige Säulen beschrieben, die eng miteinander verknüpft sind und sich gegenseitig bedingen.

Einerseits die Ausstattung der Schulen, die Bereitstellung eines technischen Supports und die breitbandige Anbindung an das Internet und andererseits das Einbeziehen der neuen Medien in den Unterrichtsalltag.

Beide Säulen müssen inhaltlich und organisatorisch miteinander verkettet werden, um sicherzustellen, dass die mit der Umsetzung des MEP geleisteten Investitionen intensiv pädagogisch genutzt werden.

Viele Schulen haben daher in den vergangenen Jahren ihre eigenen Kompetenzen entwickelt und die angebotenen Fortbildungsveranstaltungen der verschiedenen Institutionen genutzt.

Nach den bisherigen Erfahrungen lässt sich jedoch festhalten, dass insgesamt noch ein gewisser Nachholbedarf zu verzeichnen ist. Die bisher angebotene Betreuung ist nicht in jedem Fall ausreichend. Es erscheint daher sinnvoll, zusätzlich weitere medienpädagogische Fortbildungs- und Betreuungsangebote vorzuhalten, um zielgerichtete Arbeit mit

den neuen Medien in den Schulen zu gewährleisten. Hier ist sicherlich auch das Land NRW in seiner Verantwortung für die inneren Schulangelegenheiten gefordert.

5. IT-Nutzungsvereinbarungen für Schulverwaltungen

In IT-Nutzungsvereinbarungen werden Rahmenbedingungen für den Umgang der Nutzer mit der von der citeq installierten IT-Infrastruktur festgelegt (z.B. Nutzung des Internets, Behandlung der Geräte). Die bestehenden IT-Dienstanweisungen für die Stadt Münster gelten nur für das bei der Stadt Münster beschäftigte Personal (z. B. Schulsekretärinnen). In den Schulverwaltungen arbeiten aber auch Personen, die nicht bei der Stadt Münster beschäftigt sind (Landesbedienstete). Daher ist es u. a. aus Sicherheitsgründen für das Schulverwaltungsnetz erforderlich, die bestehenden Dienstanweisungen so anzupassen, dass sie auch für die dort tätigen Lehrkräfte Gültigkeit haben. Dieser Prozess wird von der citeq gemeinsam mit dem Amt für Schule und Weiterbildung im ersten Quartal 2008 umgesetzt.

II. Ausstattungs- und Betriebskonzept

1. Technische Grundsatzentscheidungen

1.1. Allgemeines

Wie bereits in der Einleitung (siehe unter I. 1.1. "Notwendigkeit der Fortschreibung") beschrieben, verfolgt die citeq aufmerksam die aktuellen Techniktrends und bewertet sie im Hinblick auf die Möglichkeit der Berücksichtigung im Rahmen des MEP.

Sicherlich sind nicht alle Technologien bzw. Trends geeignet, um in der Fortschreibung des MEP berücksichtigt zu werden. Sofern dieses aber sinnvoll erscheint, werden sie im technischen Ausstattungs- und Betriebskonzept genannt werden. Die Umsetzung neuer Technologien im MEP ist ein ständiger Vorgang, der nicht an diese Fortschreibung gebunden ist.

1.2. Servertechnologie

Im Rahmen des MEP werden "klassische" Serverkonfigurationen eingesetzt. Die Gründe, die bei der ersten Aufstellung des MEP gegen den Einsatz von Terminalservern gesprochen haben, liegen weiterhin vor. Aufgrund der stark parallelen Nutzung hochmultimedialer Anwendungen kann die Terminalserver-Technologie in den Schulen wegen der mit dieser Technik verbundenen Funktionseinschränkungen nicht wirtschaftlich eingesetzt werden.

Pro Schule bzw. Schulzentrum werden mindestens zwei Server installiert (je ein Server pro unterrichtlichem Netz und Schulverwaltungsnetz). Diese Server stellen die allgemeinen Dienste (Dateien, Druck, Datensicherung), Netzwerkdienste (DHCP, DNS, Proxy) und Applikationsdienste (WWW, E-Mailing) zur Verfügung. In Schulzentren sind die Server entsprechend größer dimensioniert, sodass sich mehrere Schulen diese teilen können.

Auf allen Servern wird das Betriebssystem Novell Linux Open Enterprise Server eingesetzt. Die Begründung für diese Entscheidung ist dem folgenden technischen Ausstattungskonzept (siehe unter 9.3 "Betriebssystem und Version Server") zu entnehmen.

1.3. Clients

Zum Einsatz kommen in der Schulverwaltung und im pädagogischen Bereich nur neue, standardisierte PC und Notebooks, die über den jeweils aktuell gültigen Rahmenvertrag der citeq beschafft werden. Die eingesetzten Hardwarekomponenten der PC und Notebooks werden regelmäßig durch die Regelungen des Rahmenvertrages an die marktüblichen technischen Ausstattungen für Business-PC/-Notebooks angepasst.

Auf allen Rechnern wird zurzeit das Betriebssystem Windows XP Professional eingesetzt. Die Begründung für diese Entscheidung ist dem folgenden technischen Ausstattungskonzept (siehe unter 10.3. "Betriebssystem Clients") zu entnehmen.

1.4. Drucker

Insbesondere in Grundschulen wurden bei der Erstaussstattung lokale (Tintenstrahl-) Drucker installiert. Begründet war dies durch die Medienkonzeption „Medienecken“, die Insellösungen (zwei PC – ein Drucker) in den jeweiligen Klassenräumen der Grundschulen vorsieht. Dadurch ergab sich ein relativ hoher Druckerbedarf in der einzelnen Schule, der zumindest zu Beginn des Projektes nur durch den Einsatz lokaler Drucker bedient werden konnte. Aus wirtschaftlicher Sicht war dies nachteilig. In größeren Netzwerken ist der Einsatz und Betrieb einer geringeren Zahl von netzwerkfähigen Druckern wirtschaftlicher als viele lokal installierte Drucker. Diese Aussage hat sich nach den Erfahrungen der vergangenen Jahre mehr als bestätigt. Neben den relativ hohen Verbrauchskosten, die lokale (Tintenstrahl-) Drucker in der Regel verursachen, stehen diese immer nur jeweils dem PC zur Verfügung, an dem sie angeschlossen wurden. Der Anschluss an andere PC ist aufgrund des Wächterschutzes nicht durch die Schule und nur durch eine entsprechend aufwändige Installation zu bewerkstelligen.

Weiterhin können lokale Drucker nicht über das Netzwerk gewartet werden, was als größter Nachteil anzusehen ist. Jeder Ausfall kann nur durch einen Supporteinsatz vor Ort analysiert werden. Schlimmstenfalls muss die Schule bis zur Fehlerbehebung auf die Dienste des Druckers verzichten, was die Schulabläufe entsprechend behindert. Diese in der Vergangenheit häufig aufgetretenen Aufwände im Störfall verteuern das Produkt „lokaler Drucker“. Der Einsatz lokal installierter Drucker ist aus wirtschaftlichen Gründen nicht mehr zu vertreten ist.

Lokale Drucker werden daher zukünftig nicht mehr eingesetzt. Unter Berücksichtigung der Ausstattungsbudgets der jeweiligen Schule und der Räumlichkeiten werden die bereits installierten lokalen Drucker im Rahmen der Reinvestition und im Falle eines Defektes gegen Netzwerkdrucker ausgetauscht.

1.5. Monitore

In den Schulen werden zurzeit unterschiedliche Monitortypen in unterschiedlichen Größen (17“-CRT, 17“-TFT, 19“-TFT und 20“-TFT) eingesetzt. Im Hardwarelager der citeq müssen diese unterschiedlichen Monitortypen im Bereich der Ersatzgeräte vorgehalten werden.

Die Hersteller haben inzwischen den Produktionsstopp sowohl der CRT- als auch der 17“-TFT-Monitore angekündigt. Aufgrund des Herstellungsprozesses können technisch aufwändigere 19“-Monitore zu mit 17“-Monitoren vergleichbaren Konditionen hergestellt werden.

Das Amt für Gebäudemanagement hat die Energieeinsparung durch den Einsatz von TFT-Monitoren an Stelle von CRT-Monitoren hochgerechnet. Danach können im angesetzten Einsatzzeitraum von zurzeit 4,5 Jahren Energiekosten in Höhe von ca. 65,00 € je Monitor eingespart werden.

Der Einsatz von TFT-Monitoren ist im Vergleich zum bisherigen Einsatz der CRT-Monitore wirtschaftlicher. Aufgrund der Preisentwicklung, der aufwändigen Lagerhaltung und des Stromverbrauchs wird im Rahmen des MEP zukünftig nur noch ein 19“-TFT-Monitortyp eingesetzt, der über den aktuellen Rahmenvertrag der citeq beschafft wird.

1.6. Einbindung eigener Systeme

Schuleigene Hardware wird grundsätzlich nicht in das Schulnetz integriert. Hiervon werden aber die folgenden Ausnahmen zugelassen:

- Standardisierte Drucker und Kopierer, die aktuell auch bei der Stadtverwaltung eingesetzt und von der citeq unterstützt werden, können grundsätzlich in das Schulnetz integriert werden, sofern sie netzwerkfähig sind. Für die Integration und den Betrieb hat die citeq laufende monatliche Kosten ermittelt. Diese sind aus dem MEP-Budget der Schulen zu finanzieren.

- Standardisierte PDA (Personal Digital Assitants), die aktuell auch bei der Stadtverwaltung eingesetzt und von der citeq unterstützt werden, können in das Schulnetz (Verwaltung) integriert werden. Dabei ist allerdings aus Sicherheitsgründen die "Geschäftsanweisung für den Umgang mit mobilen Endgeräten der Informationstechnik" zu beachten, die auch für die Schulverwaltungen Gültigkeit hat. Diese besagt u. a., dass PDA, die von der citeq in das Schulnetz integriert werden, nicht mit dem Internet oder mit IT-Systemen anderer Anwender verbunden werden dürfen. Die laufenden monatlichen Kosten für die Integration und den Betrieb sind ebenfalls aus dem MEP-Budget der Schulen zu finanzieren.
- Schuleigene Peripheriegeräte im pädagogischen Netz (z. B. Messgeräte) werden von der citeq nur aufgrund besonderer Vereinbarungen in Betrieb genommen, da ohne eine Standardisierung der Hardwarekomponenten eine hohe Verfügbarkeit der Anwendersysteme nur durch eine personal- und damit kostenintensive Betreuung zu erreichen ist. Die Dienstleistung beschränkt sich auf die Installation von Gerätetreibern, die durch die Schule zur Verfügung gestellt werden müssen. Ein Support wird für diese Geräte nicht übernommen.

Sofern diese schuleigene Hardware durch die citeq in das Schulnetz integriert wird, wird diese Hardware in das Bestandsverzeichnis der citeq aufgenommen (Gerätebezeichnung, Gerätetyp, Standort, Seriennummer), eine Identnummer vergeben und als Eigentum der Schule geführt. Das ist erforderlich, damit die citeq für die Funktionsfähigkeit der Hardware im Netzwerk optimalen Support leisten kann.

2. Beschaffung

Ein weiterer wesentlicher Bestandteil der Konzeption ist die zentrale Beschaffung der Hard- und Softwarekomponenten. Die zentrale Beschaffung der Hardware durch die citeq stellt die Homogenität der Systeme sicher. Hierdurch ist es möglich den Grundsatz der Standardisierung (siehe oben) umzusetzen.

Aufgrund der höheren Stückzahlen, die sich durch eine zentrale Beschaffung ergeben, können wesentlich bessere Preiskonditionen ausgehandelt werden. Besonders vorteilhaft haben sich hier auch Kooperationen mit weiteren citeq-Kunden (z. B. Stadt Hamm) sowie der KDN, dem Dachverband Kommunaler IT-Dienstleister, ausgewirkt. Zukünftig

wird angestrebt, durch Ausweitung der Kooperationen noch bessere Preiskonditionen auszuhandeln. Für einige Komponenten hat der Abschluss von Rahmenverträgen zu deutlichen Erleichterungen und Zeiteinsparungen bei der Bestell- und Lieferabwicklung geführt.

Für die Inventarisierung der Hard- und Softwarekomponenten wird eine zentrale Datenbankanwendung eingesetzt, die auch für die IT-Komponenten der Stadtverwaltung genutzt wird.

3. Katalog der Standardkomponenten

Die citeq entwickelt und veröffentlicht einen Warenkatalog von Standard-Komponenten (Hardware und Lernsoftware entsprechend dem Software-Katalog je Schulform (siehe unter I. 2.4.2. "Software für den unterrichtlichen Bereich")). Die darin aufgelisteten Systeme sind mit dem Betriebskonzept kompatibel und können für die Ergänzung und Änderung der Ausstattungsstandards genutzt werden. Dadurch, dass i. d. R. ausschließlich Komponenten aus diesem Warenkatalog eingesetzt werden, können die positiven Auswirkungen der Standardisierung verstärkt werden.

Aus diesem Warenkatalog können die Schulen auch Einzelbeschaffungen nach Umsetzung des Ausstattungskonzeptes außerhalb des MEP aus eigenen Mitteln tätigen.

4. Datenschutz und Datensicherheit

Die citeq ist eine kommunale Einrichtung und betreut in ihrer Funktion als kommunales Rechenzentrum u. a. die Verwaltung der Stadt Münster. Daher muss sie die Vorschriften des Datenschutzgesetzes NRW und die sich daraus ergebenden technischen und organisatorischen Vorgaben bei der Verarbeitung von personenbezogenen Daten beachten.

Die citeq wurde vom Rat der Stadt Münster mit der Umsetzung des MEP und damit auch mit der Ausstattung und Vernetzung der Verwaltungsbereiche der Schulen beauftragt. Bei der Konzeption der technischen Umsetzung des MEP wurden für die Verwaltungsbereiche der Schulen die gleichen Standards hinsichtlich Datensicherheit und Datenschutz berücksichtigt, wie sie für die Daten der Stadtverwaltung Münster (z.B. Personendaten des Sozial- und Gesundheitsamtes, Einwohner- und Personaldaten etc.)

gelten. Dies gilt auch für die pädagogischen Netzwerke in den Schulen mit der Einschränkung, dass das Lehrpersonal grundsätzlich Leserechte an sämtlichen von den Schülerinnen und Schülern gespeicherten Daten besitzt.

Folgende Vorgaben wurden beachtet:

- Die Sicherung und Verarbeitung der personenbezogenen Schüler- und Lehrerdaten muss datenschutzrechtliche Anforderungen erfüllen.
- Das Verwaltungsnetz muss vom pädagogischen Netz getrennt und auch gegen Gefahren aus dem Internet geschützt sein.
- Die Kommunikations- und Informationswege der Schulverwaltung mit dem Amt für Schule und Weiterbildung und sonstigen Stellen soll vereinfacht werden.
- Die Funktionalitäten, Zuverlässigkeit und Verfügbarkeit sollen den Standards der Stadtverwaltung Münster entsprechen.

Die technische Umsetzung dieser Vorgaben stellt sich wie folgt dar:

- Es wurde in jeder Schule ein eigenes vom pädagogischen Bereich strikt getrenntes Netzwerk mit einem eigenen Verwaltungsserver eingerichtet.
- Das Verwaltungsnetzwerk ist in das Mailsystem der Stadtverwaltung Münster integriert. Die Arbeitsplätze haben Zugang zum Intranet der Stadtverwaltung Münster.
- Der Internet-, Intranet-, E-Mail- und sonstige Datenverkehr von und zu den PC in den jeweiligen Netzwerken verläuft über ein mehrstufiges System, um einen möglichst weitgehenden Schutz vor Viren oder unbefugten Zugriffen aus dem Internet zu erreichen. Der Datenverkehr verläuft über die mit eigener Virenschutzsoftware ausgestatteten Server in den Schulen über eine Standleitung zu der zentralen Netzwerkinfrastruktur der citeq und den dort eingerichteten Schutzmechanismen mit Viren- und Firewall-schutz.

Die Daten auf den Servern in den Schulen werden einmal täglich im Wege einer so genannten Differenzsicherung auf einen zentralen Server bei der citeq gesichert. Einmal täglich werden diese Daten auf dem zentralen Server wiederum im Wege einer Diffe-

renzsicherung auf Datenbänder gesichert. Alle zwei Wochen werden die Daten nochmals im Wege einer so genannten Vollsicherung im vollen Umfang auf Datenbänder gesichert. Die Datensicherung reicht 6 Wochen zurück. Die Datensicherung im pädagogischen Netzwerk ist Einschränkungen unterworfen (siehe unter 9.11. "Datensicherung Server").

Die Räumlichkeiten, in denen die zentralen und dezentralen (in den Schulen) Server installiert werden, müssen besondere Anforderungen erfüllen (u. a. geschlossene und nicht für jedermann zugänglich, ausreichende Lüftung, abschließbare Serverschränke; siehe unter 8.2 "Inhouse-Verkabelung / Netzkomponenten - LAN (Local Area Network)").

Die zuvor beschriebenen technischen Maßnahmen und Einrichtungen müssen durch die citeq betreut und gewartet werden. Dazu ist es zwingend notwendig, dass Mitarbeiter der citeq im Rahmen ihrer administrativen Tätigkeit Zugriffsmöglichkeiten auf die zu verarbeitenden Datenstrukturen besitzen. Der Schutz der auf den Schulservern vorhandenen personenbezogenen Daten im Sinne des Datenschutzgesetzes NRW (DSG-NRW) ist auch bei der Behandlung der Daten durch die Mitarbeiter der citeq voll gewährleistet.

Jede Mitarbeiterin und jeder Mitarbeiter der citeq wird regelmäßig auf die Wahrung des Datengeheimnisses (§ 6 DSG-NRW) verpflichtet und bestätigt dies durch Unterschrift. Sollten also insbesondere im Rahmen der Systembetreuung/Fehlerbereinigung im Ausnahmefall personenbezogene Daten zur Kenntnis gelangen, ist dies zur rechtmäßigen Aufgabenerfüllung unbedingt erforderlich und entspricht damit den datenschutzrechtlichen Vorgaben.

5. Protokollierung von Nutzerdaten

Durch die Authentifikation der einzelnen Benutzer im eDirectory (in Novell NetWare enthaltener Verzeichnisdienst) wird automatisch mitprotokolliert, welche Kennung sich wann an welchem Rechner angemeldet hat und, falls die Kennung das Internet genutzt hat, auf welchen Seiten sie gesurft hat. Die citeq speichert diese Daten, die im übrigen dem Fernmeldegeheimnis unterliegen, für die geschäftsmäßige Erbringung der Telekommunikationsdienste (Bereitstellung des Internetzugangs) für die Schulen einschließlich des Schutzes ihrer technischen Systeme. Nach dem Telekommunikationsgesetz ist es der citeq untersagt, sich über das erforderliche Maß hinaus Kenntnis vom Inhalt oder

den näheren Umständen der Telekommunikation zu verschaffen. Die citeq darf Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den vorstehenden (s. o.) Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit das Telekommunikationsgesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Eine Herausgabe von entsprechenden Daten ist daher grds. nur an Ermittlungsbehörden (Polizei, Staatsanwaltschaft) auf Anforderung zulässig. Das gilt nicht für die unter 9.7. ("Benutzer-/Gruppenverwaltung / eDirectory") aufgeführten Daten, die nicht von den Vorschriften des Telekommunikationsgesetzes betroffen sind.

6. Internetauftritt der Schulen

Mit der flächendeckenden IT-Ausstattung in den Schulen nehmen auch die Bedarfe im Bereich der Internetauftritte zu. Die citeq stellt den Schulen über den Softwarekatalog Webeditoren und eine FTP-Software zur Verfügung, sodass die bestehenden Auftritte durch die Schulen selbst weitergepflegt werden können. Allerdings sind viele Schulen dazu nicht in der Lage, da das entsprechende Know-How fehlt.

Im Rahmen der im Januar 2007 durchgeführten Kundenumfrage der citeq äußerten daher auch mehr als die Hälfte der befragten Schulleitungen und IT-Koordinatoren Bedarf an den Unterstützungsleistungen im Bereich „Internetauftritt der Schulen“:

- an der Bereitstellung von Webspace (Hosting) durch die citeq
- an einer Beratung bei der Entwicklung oder laufenden Betreuung der Homepage
- an der Bereitstellung eines Redaktionssystems

Die citeq kann den Schulen in allen drei Bereichen mit ihrer Erfahrung, vorhandenen Produkten und ihrem Personal Unterstützung anbieten. Die damit verbundenen Kosten müssen von den Schulen aus ihren eigenen Etats finanziert werden.

7. IT-Bestandsmodul der citeq

Für einen reibungslosen Support der in den Schulen installierten Hardware durch die citeq ist eine wichtige Voraussetzung, dass der citeq die Standorte der Hardware bekannt

sind. Das gilt insbesondere für den Fall, dass eine Garantieabwicklung einer Hardwarestörung direkt durch den Rahmenvertragspartner der citeq vorgenommen wird. Auch für die Durchführung der Reinvestitionsprojekte (siehe unter I. 2.2. "Reinvestition der Hardware - Planung und Umsetzung") müssen die tatsächlichen Standorte der Hardware entsprechend im Bestandsverzeichnis dokumentiert sein.

Die Pflege des Bestandsverzeichnisses hat die citeq bislang exklusiv vorgenommen. Sofern Hardware durch die citeq umgesetzt wurde, sind die Standorte im Bestandsverzeichnis auch entsprechend nachgepflegt worden. Hat die Schule die Hardware allerdings selber umgesetzt, um kurzfristigen Bedarfsänderungen in der Nutzung der Hardware nachzukommen, wurde dieses der citeq nicht in jedem Fall gemeldet. In diesen Fällen stimmen die tatsächlichen Standorte der Hardware nicht mehr mit den im Bestandsverzeichnis dokumentierten Standorten überein. Um diese Differenzen auszumergen, haben die IT-Koordinationen über die Kennung in der Schulverwaltung die Möglichkeit erhalten, Standortveränderungen selber über das Browser basierte IT-Bestandsmodul in das Bestandsverzeichnis der citeq einzupflegen. Sofern die Schule die Standortveränderung selber vorgenommen hat, ist es auch die Aufgabe der IT-Koordination diese in das Bestandsverzeichnis einzupflegen (siehe unter 11.7.3. "Aufgaben der IT-Koordination").

Das IT-Bestandsmodul bietet den Schulen zudem eine Übersicht der in der Schule eingesetzten und von der citeq betreuten Hardware. Das Führen eigener Listen ist dadurch nicht mehr erforderlich.

8. Technisches Ausstattungskonzept

8.1. Netzwerk

Im Rahmen der Umsetzung des Konzeptes wird ein Schulnetz betrieben, welches aus jeweils einem LAN (Local Area Network) je Schulstandort und der Vernetzung der einzelnen Schulstandorte untereinander mit gleichzeitiger Anbindung an die citeq als zentralem IT-Dienstleister besteht.

Bei der Implementierung ist besonders berücksichtigt, dass aus Datenschutzgründen jeweils zwei Bereiche in den Schulen - unterrichtliches Netz und Schulverwaltungsnetz -

durch entsprechende Kabelführungen und jeweils eigene aktive Netzkomponenten im LAN getrennt voneinander aufgebaut sind.

8.2. Inhouse-Verkabelung / Netzkomponenten - LAN (Local Area Network)

Alle Schulen sind mit einer strukturierten Gebäudeverkabelung gemäß Ethernet-Standard ausgestattet. Bei der baulichen Umsetzung wurden die gemeinsam mit dem Amt für Gebäudemanagement für alle städtischen Gebäude definierten Rahmenbedingungen zu Grunde gelegt.

Abgestimmt auf die jeweilige Örtlichkeit gibt es grundlegende Festlegungen, wie die

- **Auswahl des zentralen Systemraumes:**

Die sternförmige Zusammenführung der Inhouse-Verkabelung auf einen Konzentrationpunkt sowie die Aufstellung der weiteren zentralen IT-Komponenten (Server, zentrale Netzwerkkomponenten, Übergabepunkt der WAN-Gebäudeanbindung) werden in einem ausschließlich für diesen Zweck gebundenen Raum vorgenommen. Der Raum ist von der Schule zu benennen, wobei in Absprache mit dem Amt für Gebäudemanagement folgende Kriterien Berücksichtigung fanden:

- o zentrale Lage zur Minimierung der Kabellängen,
- o ausreichende Raumgröße (min. 10 qm),
- o zugangsgesichert durch separate Schließanlage (Zugang nur für citeq, IT-Koordination der Schule sowie den Hausdienst),
- o Minimierung des Einbruchsriskos (vorzugsweise Kellerraum, ansonsten durch geeignete Fenstersicherungsmaßnahmen),
- o ausreichende Belüftung (ggf. unterstützt durch geeignete Lüftung),
- o eigener Stromkreis zur Erhöhung der Ausfallsicherheit,
- o keine Wasser führenden Leitungen,
- o erhöhte Anforderungen an den Brandschutz, auch unter Berücksichtigung der angrenzenden Räume, Rohr- und Kabeleinführungen,
- o keine Parallelnutzung (z.B. als Lagerraum o. ä.).

Nicht alle ausgewählten Systemräume erfüllen die vorgenannten Kriterien. Die Gründe hierfür sind vielfältig (z. B. mangelnde räumliche Alternativen bei beengter Raumsituation).

Die Systemräume werden regelmäßig von der citeq geprüft. Hierbei wird eine standardisierte Prüfliste abgearbeitet. Ein Protokoll mit einem Maßnahmenkonzept wird erstellt und nach entsprechender Entscheidung kontrolliert abgearbeitet. Dabei wird insbesondere auch überprüft, ob die Planungsgrundlagen für den Systemraum sich mittlerweile in relevanter Weise verändert haben (z.B. in Bezug auf die Leistungswerte).

Sofern sich aus der vorgenannten Prüfung oder im Störfall (z. B. bei zu großer Hitzeentwicklung) dringende Maßnahmen ergeben, werden diese von der citeq an das Amt für Gebäudemanagement weitergeleitet. Dieses erstellt daraufhin die Fachplanung, die von der citeq abgenommen wird. Anschließend erfolgt die Umsetzung der Maßnahmen entsprechend der aufgestellten Fachplanung.

- Auswahl der Lokationen für Etagen-Unterverteilungen

An die in größeren Gebäudekomplexen erforderlichen Etagen-Unterverteilungen sind ebenfalls besondere Anforderungen gestellt. Ihre Lage ergibt sich aus der jeweiligen räumlichen Situation und ist daher spezifisch an die Gegebenheiten des Gebäudes angepasst. Die Etagen-Unterverteilungen sind regelmäßig in Schranksystemen mit der Standardbreite von 19 Zoll. Diese Schränke lassen sich auch in Hängetechnik an der Wand verschrauben, sodass beispielsweise Lager-, Karten- oder ähnliche Funktionsräume zur Aufstellung durchaus geeignet sind. Den Anforderungen des Datenschutzes und der Datensicherheit ist dadurch Rechnung getragen, dass es sich bei den Verteilerschränken um abschließbare Schränke in Metallausführung handelt und die genannten Funktionsräume nicht jedermann zugänglich sind.

- Kabelwege

Die Festlegung der notwendigen Kabelwege sowie des daraus resultierenden Installationsaufwandes ist vom Amt für Gebäudemanagement vorgenommen worden. Das Amt für Gebäudemanagement betreut auch die bautechnischen Arbeiten hinsichtlich der Gebäudestruktur, z. B. Prüfung der Gebäudestatik bei Wand- und Bodendurchbrüchen oder Kernbohrungen. Das Amt für Gebäudemanagement beauftragt die ausführenden Firmen und beschafft die erforderlichen Materialien entsprechend der mit der citeq vereinbarten Spezifikation, wie z. B.

- o Kabel (Kupfer- bzw. LWL),
- o Kabelkanäle und –bühnen,
- o Dämmstoffe,

- o Verteilerschränke,
- o Rangierfelder,
- o Netzwerk-Steckdosen.

Berücksichtigt sind hierbei auch eventuell vorhandene Netzinfrastrukturen, die aus Kostengründen - soweit sie den Anforderungen entsprechen - integriert wurden.

Die Anzahl und Verteilung der Netzwerkdosen erfolgte in Abstimmung zwischen der Schule, dem Amt für Schule und Weiterbildung und dem Amt für Gebäudemanagement.

Aus Gründen der Kostenoptimierung ist gleichzeitig mit der Verkabelung der Unterrichtsbereiche auch die Verkabelung der Schulverwaltungsräume vorgenommen worden.

Im Rahmen des Projektes ist über das Amt für Gebäudemanagement eine Überprüfung des vorhandenen Stromnetzes vorgenommen worden. Sofern Anpassungsbedarf erkannt wurde, sind die notwendigen Anpassungs- bzw. Erweiterungsarbeiten durchgeführt worden.

Die Verkabelung ist sternförmig in Kupfer auf die gewählten Systemräume und Etagen- oder Unterverteilungen geführt. Die Kupferkabel sind entsprechend der Ethernet-Spezifikation als STP (Shielded Twisted Pair) der Kategorie 5 oder höher ausgeführt mit Abschluss auf Rangierfeldern bzw. Netzwerkdosen mit der in der Netzwerktechnik gängigen RJ45-Stecktechnik.

Kupferkabel können nur in Bereichen mit Kabellängen von bis zu maximal 80 Metern eingesetzt werden. Sind Etagen- oder Unterverteilungen weiter vom zentralen Systemraum entfernt, wurden Lichtwellenleiterverbindungen (Multi-mode) mit Abschluss auf SC-Stecktechnik (IEC 874-19) verwendet.

Räume mit großer Anzahl an Endgeräten (Informatikräume bzw. sonstige Fachräume) sind mit einer eigenen Unterverteilung im Raum verkabelt und durch Verwendung eines Switch mit ausreichender Portdichte an das Netz angeschlossen. Bei der Raumverkabelung ist den Belangen der Sicherheit durch geeignete Maßnahmen Rechnung getragen (z.B. Verwendung von Brüstungskanälen oder dergleichen) zur Vermeidung von Stolperfallen.

Alle Verkabelungen im zentralen Systemraum oder in geschaffenen Unterverteilungen sind in 19-Zoll-Industrieschränken auf Rangierfeldern abgeschlossen. Diese Schränke stehen in verschiedenen Bauhöhen und damit unterschiedlichen Aufnahmekapazitäten zur Verfügung und dienen auch zur Aufnahme der weiteren IT-Infrastruktur wie Server, Router und Switche.

Als aktive Netzkomponenten sind für den Anschluss der Endgeräte (PC, Netzwerkdrucker, ...) Fast-Ethernet-Switches verwendet. Switches bieten hohe Performance von 10/100Mbit dediziert pro Port (Anschlussmöglichkeit für ein Endgerät) bei gleichzeitig günstigem Preis-/Leistungsverhältnis. Für jedes Endgerät sowie für kaskadierte Switches in Unterverteilungen wird ein entsprechender Anschluss bereitgestellt. Die Geräte bieten skalierbare Portdichten von 24 bis 144 Ports. Zur Einhaltung eines wirtschaftlichen Kostenrahmens erfolgt die Dimensionierung der aktiven Netztechnik nach den konkreten, schulspezifischen Anforderungen zzgl. einer Sicherheitsreserve (ca. 10 Prozent Netzwerkports über den aktuellen Bedarf hinaus als Anschlussmöglichkeit für zusätzliche Endgeräte).

Im Systemraum ist ein zentraler Switch eingesetzt von dem aus die Unterverteilungen kaskadiert werden. Für den Anschluss der Server und Switchkaskaden im Verwaltungs- und Pädagogikbereich stehen auf den zentralen Switchen 1Gbit Ports in Kupfer und Lichtwelle zur Verfügung.

Die verwendeten Switches bieten eine entsprechende Konfigurationsschnittstelle zur Fernadministration durch die citeq. Alle erforderlichen Einstellungen können daher durch die citeq von zentraler Stelle wahrgenommen werden. Die Switches sind per Passwortschutz gegen unbefugte Zugriffe geschützt.

Die Anschlüsse für den Schulverwaltungsbereich sind auf einem eigenen Switch im Systemraum abgeschlossen. Dadurch wird der Forderung nach einer echten "galvanischen Trennung" des Schulverwaltungs- und des unterrichtlichen Netzes Rechnung getragen. Erst an der Übergabestelle zum aufgebautem Schulnetz (WAN) werden die Daten auf gemeinsamen Medien übertragen.

8.3. WLAN (Wireless Local Area Network)

Als Ergänzung zu einer klassischen Kupferverkabelung sind Funknetze (WLAN) untersucht, und für den Ausbau von "fliegenden" Klassenzimmern ausschließlich im pädagogischen Netz als geeignet bewertet worden.

Funknetze (Wireless LAN / WLAN) stellen für die flexible Abbildung von größeren Arbeitsgruppen mit Notebook in Klassenräumen einen technisch machbaren Lösungsansatz dar. WLAN sind lokale Netze, die ohne Kabelverbindungen arbeiten. Sie sind standardisiert unter dem IEEE-Standard 802.11. Die Übertragung erfolgt entweder mit Funkfrequenzen im Mikrowellenbereich.

In den letzten Jahren hat sich der Standard im Bereich von WLAN zu deutlich höheren Bandbreiten bei gleichzeitig höherer Sicherheit durch komplexere Verschlüsselungsmethoden weiter entwickelt. Die Hersteller von Hard- und Software haben insbesondere dem Thema Sicherheit deutlich mehr Beachtung geschenkt. Es stehen mittlerweile aktuelle und sichere Verschlüsselungsmethoden im WLAN zur Verfügung. Wichtig bei der Implementierung von WLAN ist, dass die angebotenen Sicherheitsfeatures konsequent angewandt und umgesetzt werden. Da WLAN kabellos die Umgebung zur Übertragung von Daten nutzt, sind die Mitlesemöglichkeiten über entsprechende Funkscanner im Gegensatz zum kabelgebundenen Netz durchaus gegeben. Ohne entsprechende Verschlüsselung im WLAN wäre hiermit dem Diebstahl von Daten natürlich Tür und Tor geöffnet. Neben der konsequenten Anwendung aller angebotenen Sicherheitsfeatures ist bei der Planung eines WLAN zu beachten, dass sich alle Teilnehmer im gleichen Frequenzbereich die Bandbreite als Shared LAN teilen müssen.

Ob WLAN ein erhöhtes Risiko durch Emissionen (Stichwort: „Elektro-Smog“) darstellen, ist in der öffentlichen Diskussion. Die citeq als IT-Dienstleister möchte diese Diskussionen nicht bewerten und beschränkt sich auf die Prüfung der technischen Umsetzbarkeit.

Für den Einsatz von WLAN in Schulen wären im Rahmen eines Projektes Hard- und Software auszusuchen, sowie die erhöhten Aufwände für Einrichtung und laufender Administration zu kalkulieren. Neben den zusätzlichen personellen Aufwänden würde dies zum Aufbau einer zusätzlichen IT-Infrastruktur führen.

Sofern Schulen den Einsatz von WLAN wünschen, sind die damit verbundenen schulindividuellen Kosten aus dem MEP-Budget der jeweiligen Schule zu finanzieren.

8.4. Anbindung der Schulen an die citeq - WAN (WideAreaNetwork)

Für den Aufbau eines Schulnetzes für die Stadt Münster sind ca. 80 Standorte vernetzt. Dieses Schulnetz ist als eigenes, in sich geschlossenes Netz aufgebaut. Für den Aufbau der komplexen WAN-Infrastrukturen ist ein Vertrag mit einem Telekommunikationsprovider abgeschlossen worden (zurzeit Fa. Versatel).

Am zentralen Übergabepunkt des Schulnetzes an die citeq sind entsprechende Server installiert:

- Firewall zur Kontrolle des gesamten Datenstromes (Wer darf Was Wo tun?)
- Virenschutz, neben lokalen Virenscannern als zusätzliche Barriere für Viren (siehe unter 9.4.8. "Virenschutz")
- Proxy-Server als Cache zum Internet (siehe unter 9.4.10. "Internetzugang mittels Proxy-Services")

Der Zugang zum Internet wird mit der erforderlichen Bandbreite von 34 Mbit/s direkt vom zentralen Übergabepunkt über die installierte Firewall realisiert. Die Firewall regelt auch nötige Datenbeziehungen zwischen dem Schulnetz und dem kommunalen Verwaltungsnetz der citeq.

Der Aufbau eines eigenständigen Schulnetzes und die Nutzung zentraler Dienste (Internetzugang, Firewall, Virenschutz) stellt auf Dauer den reibungslosen Betrieb der gesamten Infrastruktur sicher. Eine Öffnung des Netzes zum Beispiel durch eigene Internetzugänge in den Schulen würde gerade den hoch zu bewertenden Sicherheitsaspekt eines geschlossenen Netzes gefährden und wird aus diesem Grund ausgeschlossen.

8.5. Streaming

Die zentral von der citeq bereit gestellten Technologien zur Sicherheit im Internetzulauf, Firewall, Virenschutz und Proxyserver sind ein besonderes Qualitätsmerkmal für die Absicherung privater Netze gegenüber dem Internet. Es ist jedoch zu beobachten, dass die Ansprüche der Schulen im pädagogischen Netz den hohen Sicherheitseinstellungen der citeq in Teilen entgegenstehen. Hier ist insbesondere der Anspruch auf Darstellung von multimedialen Inhalten über Streaming im Unterricht zu sehen.

Bereits heute kann in den Schulen ein Großteil der im Internet angebotenen Inhalte gestreamt werden. Das liegt daran, dass es "ein Streaming" nicht gibt, sondern verschiedene Protokolle. Zu unterscheiden ist hier zwischen HTTP (Hypertext Transfer Protocol) und RTSP (RealTime Streaming Protocol). Das HTTP-Streaming ist über die citeq-Infrastruktur aktuell abbildbar, das RTSP-Streaming nicht.

Ein Lösungsansatz könnte in der Kombination von gewünschten Sicherheitsfunktionen wie Virenschutz und Proxy mit eigener Internetfirewall sein. Auf einer eigenen MEP-Firewall mit eigenem Internetzugang wäre eine gegenüber der Verwaltungsfirewall abgeänderte Sicherheitspolicy denkbar. Sofern dies von den Schulen gewünscht würde, müssten im Rahmen eines Projektes die Kosten und Aufwände für einen eigenen MEP-Internetknoten erarbeitet werden. Die Finanzierung ist durch den MEP nicht abgedeckt.

Die Leitung von der Schule zur citeq stellt die Grenze des Möglichen im Bereich Streaming dar. Wenn z. B. von mehreren Rechnern (je nach Übertragungsrate können zwei schon ausreichen) gleichzeitig Streams angestoßen würden, wäre damit der restliche Internet- und damit auch der Mailverkehr in der Schule blockiert. Es empfiehlt sich daher, die gewünschten Dateien im Rahmen der Unterrichtsvorbereitung vorab herunterzuladen, um sie im Unterricht abspielen zu können.

8.6. Netzwerkmanagement

Die Einrichtung, Überwachung und Verfügbarkeit des Schulnetzes im WAN obliegt dem Telekommunikationsprovider. Die mit dem Telekommunikationsprovider verhandelten Servicelevel (Verfügbarkeits-, Reaktions- und Störungsbehebungszeiten) orientieren sich an den Servicevereinbarungen zwischen Schulträger und citeq.

Die Administration und Einrichtung der installierten Switches erfolgt zentral über die citeq. Im Rahmen vorhandener Prozeduren wird die Erreichbarkeit der aktiven Netzkomponenten im LAN geprüft und auf Kontrollmonitoren sichtbar gemacht. Zusätzlich werden die Störungen als Fehlermeldungen in das Service-Desk (siehe auch unter „Technisches Betriebskonzept“) eingebracht und entsprechend den Servicevereinbarungen beseitigt.

9. Server

9.1. Hardwareausstattung

Zum Einsatz kommen nur neue Server aus dem jeweils gültigen Server-Rahmenvertrag der citeq.

Die Server erfüllen mindestens den folgenden Standard:

- Gehäuse zum Einbau in 19-Zoll-Industrieschränke ("rack mountable")
- Aktuelle Server-CPU
- RAID-Controller (0,1,5)
- mindestens 3 Festplatten
- DVD-ROM Laufwerk
- 1GBit/s Netzwerkkarten
- redundante Netzteile
- Absicherung der Server durch eine USV
- Lights Out Management (LOM)

Eine hohe Verfügbarkeit wird zum einen durch die Spiegelung der Platten durch den RAID-Controller und die redundanten Netzteile sichergestellt. Zum anderen werden alle Server durch das „Simple Network Management Protocol“ (SNMP) überwacht, welches sowohl Software- wie auch Hardwarefehler an einen zentralen SNMP-Server meldet.

Die einheitliche Hardware einer Serverreihe ermöglicht einen flexiblen Austausch von Hardware zwischen den Servern zur Anpassung an veränderte Bedarfe und eine schnelle Reaktion durch Austausch von Hardware bei Serverdefekten. Hierfür hält die citeq je ein System für Schulverwaltung und Pädagogik für den Austausch bei Defekten vor.

Um die schnelle und einfache Installation gleichartiger Server zu ermöglichen, werden die Server soweit wie möglich automatisiert installiert. Dieses wird je nach eingesetztem Betriebssystem (Netware / Linux, s. u.) entweder durch Installation mittels Antwortdateien bzw. durch Übertragung einer Musterkonfiguration auf ein anderes System (Cloning) realisiert. Diese Vorgehensweise reduziert die Aufwände für die Inbetriebnahme eines Servers von einigen Tagen auf wenige Stunden. Allerdings ist auch hierfür die Einheitlichkeit der Server Voraussetzung.

Die oben genannten Leistungsdaten sind zum heutigen Zeitpunkt ein Minimum für ein performantes System. Die Skalierbarkeit der eingesetzten Server ermöglicht dabei die problemlose Erweiterung um zusätzliche Prozessoren, des Hauptspeichers und der Festplatten und trägt somit zu einem optimalen Einsatz der Server auch bei wachsenden Anforderungen bei. Zur Vermeidung einer frühzeitigen Hochrüstungsnotwendigkeit werden bei der Erstausrüstung des Servers Leistungsreserven in wirtschaftlich vertretbarem Umfang eingeplant.

Alle bei der citeq eingesetzten Server sind für eine möglichst hohe Ausfallsicherheit ausgelegt. Dies wird gewährleistet durch die eingesetzten Komponenten und die sorgfältige Qualitätsprüfung durch den Hersteller der Server. Zusätzlich trägt die Überwachung der Server mittels SNMP zur hohen Verfügbarkeit bei. Sie ermöglicht im Zusammenspiel mit entsprechenden Treibern die Meldung von Problemen der fehlertoleranten Hardware an einen zentralen Server der citeq. Dieser wiederum leitet jeden gemeldeten Fehler per Mail und auch per SMS an den zuständigen Administrator weiter. Durch diese ständige Überwachung ist auch eine Reaktion auf Warnmeldungen im Voraus, also vor dem Auftreten einer Störung, möglich.

Die hohe Verfügbarkeit wird auch durch die von der citeq gewählte Konfiguration der Server gewährleistet. Dazu tragen vor allem der RAID-Controller und die Plattenspiegelung bei. Bei diesem Verfahren werden die Daten nicht nur auf eine Platte geschrieben, sondern abhängig vom gewählten Verfahren (Raid 1 bzw. Raid 5) auf eine oder mehrere weitere Platten geschrieben. Hierdurch bleibt der Betrieb des Servers auch bei Ausfall einer Platte weiterhin gewährleistet.

Im Fehlerfall ist trotzdem ein unverzüglicher Austausch der defekten Platte notwendig, da ein weiterer Plattenausfall einen Gesamtausfall des Systems verursachen und damit folgende Aktivitäten erforderlich machen würde:

- Austausch der defekten Platten,
- Neuinstallation des Servers,
- Rückspielen der Datenbestände aus der Datensicherung.

Diese Neuinstallation des Servers wäre wesentlich aufwändiger, zudem könnte die Schule während des gesamten Ausfalls des Servers nicht mit ihrer IT arbeiten. Weiterhin würden in der Schule Datenverluste auftreten. Die Daten, die sich seit der letzten Sicherung geändert haben, sind nicht mehr wiederherzustellen. Bei einem Ausfall eines Ser-

vers in der Pädagogik sind zusätzlich die Dateien, die aus der Sicherung ausgeschlossen sind (siehe unter 9.11 "Datensicherung Server"), unwiederbringlich verloren.

Der zeitnahe Austausch der Festplatten wird durch einen der oben beschriebenen Mechanismen (Benachrichtigung durch den SNMP-Server oder den Service-Desk) umgehend veranlasst.

Trotzdem kann eine Spiegelung eine Datensicherung nicht ersetzen, da die Spiegelung nur vor Hardwareproblemen schützt und nicht vor Fehlern wie unbeabsichtigtem Löschen von Daten.

Zur hohen Verfügbarkeit tragen auch andere, redundant ausgelegte Komponenten bei. Erfahrungsgemäß ist ein hoher Anteil der Hardwarestörungen durch defekte Netzteile (hohe Belastung im Dauerbetrieb) verursacht. Die Auswirkungen sind oft gravierend. Neben Datenverlust ist oft auch der Aufwand zur Wiederherstellung der Betriebsfähigkeit hoch. Diese Probleme werden durch das zweite Netzteil, welches den Betrieb auch bei Ausfall eines Netzteils weiterhin sicherstellt, vermieden. Der umgehende Austausch eines defekten Netzteils wird auf die gleiche Weise veranlasst, wie der Austausch einer defekten Platte (siehe oben).

Für eine möglichst hohe Geschwindigkeit der Daten zwischen dem Server und den Clients werden zurzeit Netzwerkkarten mit einer Geschwindigkeit von 1GBit/s verwendet.

Seit der Aufstellung des MEP hat sich gezeigt, dass in einigen Schulstandorten Schwankungen im Stromnetz bzw. kurzzeitige Stromausfälle zu vorübergehenden Serverausfällen führten. So mussten die Server nach der Stromschwankung bzw. dem Stromausfall von der citeq per Fernwartung zunächst wieder neu gestartet werden, bevor im Normalbetrieb weitergearbeitet werden konnte. In wenigen Fällen führte die Stromschwankung sogar zum Defekt der Serverhardware. Um dieses zu vermeiden wurden in allen Schulstandorten unterbrechungsfreie Stromversorgungen (USV) installiert. Diese dienen dazu, Stromschwankungen herauszufiltern und kurzfristige Stromausfälle mit einer Dauer von wenigen Minuten zu überbrücken, sodass die Server in diesen Situationen nicht mehr ausfallen können.

9.2. Virtualisierung von Servern

Zu den aktuell zehn wichtigsten Technologien bzw. Trends der IT-Branche zählt die Virtualisierung. Die Virtualisierung wird während der nächsten Jahre eine wichtige Technologie bleiben. Sie kann helfen, die Kosten zu reduzieren, mehr Flexibilität zu schaffen und darüber hinaus auch Energie in Rechenzentren einzusparen. Die citeq beobachtet diesen Trend genau und prüft zurzeit, ob es sinnvoll ist, mehrere Server auf einer physikalischen Hardware zu „virtualisieren“ (sog. Division). Unter Division versteht man in diesem Zusammenhang, mehrere Server auf einer physikalischen Hardware abzubilden. Im MEP sind dabei jedoch folgende Punkte zu beachten:

- Aufgrund der in § 2 Abs. 1 Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Erziehungsberechtigten (VO-DV I) verlangten galvanischen Trennung von Verwaltung und Pädagogik („... ist in der Schule grundsätzlich eine ausschließlich für die Verwaltung der Schule vorgesehene ADV-Anlage zu verwenden...“), entfällt die Möglichkeit zur Virtualisierung von Verwaltung und Pädagogik auf einem Server. Aus diesem Grunde wird hiervon abgesehen.
- In Schulzentren teilen sich zurzeit alle Schulen jeweils einen entsprechend dimensionierten Server für die Pädagogik und einen Server für die Verwaltung. Diese Konstellation wurde so gewählt, weil sie entsprechende wirtschaftliche Vorteile mit sich bringt, obwohl sie für die automatisierte Softwareverteilung nicht optimal ist. Hier wäre es von Vorteil, wenn jeder Schule ein eigener Server virtualisiert zur Verfügung gestellt würde, der explizit die in der jeweiligen Schule benötigte Software vorhalten würde.
- In beiden Fällen ist zu berücksichtigen, dass pro virtuelle Maschine, die auf dem Server eingerichtet würde, entsprechend mehr Hardwareressourcen zur Verfügung stehen müssten, und die hierbei eingesetzte Serverhardware somit deutlich teurer würde. Zudem würde der personelle Aufwand für die Einrichtung und Betreuung der virtuellen Server steigen. Vor einer Virtualisierung von Servern in Schulzentren wäre daher die Wirtschaftlichkeit dieser Maßnahme zu prüfen. Nur wenn die mit den zu erwartenden Vorteilen verbundenen Einsparungen die zu erwartenden höheren Aufwände deutlich übersteigen würden, wäre die Umsetzung sinnvoll. Für die Prüfung der technischen Umsetzbarkeit und der Wirtschaftlichkeit läuft ein Projekt innerhalb der citeq.

9.3. Betriebssystem und Version

Als Betriebssystem kommt zurzeit der Novell Open Enterprise Server Version 1 mit NetWare-Kernel (vormals Novell Netware 6.5) mit den jeweils aktuellen Updates und Patches zum Einsatz. Die Entscheidung für Novell NetWare wurde bei der Aufstellung des MEP aufgrund einer Nutzwertanalyse zwischen den Betriebssystemen Microsoft Windows Server, Novell NetWare und Linux (SuSE Linux Enterprise Server) in den damals jeweils aktuellen Versionen getroffen.

Im Rahmen der Nutzwertanalyse wurden verschiedene Aspekte für und wider der Entscheidung für eines der genannten Betriebssysteme abgewogen. Dabei erreichte Novell NetWare die höchste Punktzahl. Unter Berücksichtigung heutiger Gegebenheiten kommt die Nutzwertanalyse zum gleichen Ergebnis. Die citeq überprüft die Nutzwertanalyse und deren Ergebnis erneut, sobald sich wesentliche Faktoren im technischen oder wirtschaftlichen Umfeld ändern.

Zukünftig wird die Firma Novell den bisherigen NetWare-Server durch den Open Enterprise Server ablösen. Dabei handelt es sich um einen Linux-Server, der die bislang unter NetWare vorhandenen Dienste zur Verfügung stellt. Damit vereint die Firma Novell das Beste aus den beiden Betriebssystemen NetWare und Linux in dem Open Enterprise Server. Da die citeq in Zukunft den Open Enterprise Server einsetzen wird, stehen den Schulen dann die Funktionen beider Betriebssystemwelten zur Verfügung.

Um die Funktionalität der Server zu gewährleisten, installiert die citeq regelmäßig die von Novell bereitgestellten Patches und Servicepacks. Die citeq testet vor der Installation die entsprechenden Patches und Servicepacks. Nur diese ständige Pflege der Systeme gewährleistet einen sehr fehlerfreien Betrieb und damit eine hohe Verfügbarkeit. Durch diese Aktualisierungen der Server wird zudem die Sicherheit der Server gegen Angriffe von außen und auch von innen erhöht. Dabei liegt die Priorität auf der Funktionalität der Server, d.h. eine Korrektur wird von der citeq nur dann installiert, wenn die Funktionalität des Servers nicht beeinträchtigt wird.

9.4. Serverdienste

Die Server stellen in jeder Schule vor Ort die folgenden Funktionen bereit:

- Fileservices,
- Printservices,
- Dynamic Host Control Protocol (DHCP),
- Domain Name Service (DNS),
- Mailing,
- Intranetserver,
- Antivirus,
- Softwarerepository der Clients,
- zentrale Vorhaltung von CD-Rom,
- Internetzugang mittels Proxy.

Diese Dienste werden zur Verfügung gestellt durch die Produkte Novell NetWare bzw. Novell Linux Open Enterprise Server, Novell GroupWise in den Schulverwaltungen bzw. mittels Web-Mail-Zugang in der Pädagogik, Novell Border Manager unter NetWare bzw. Squid unter Linux, Novell ZENworks und McAfee Virus Scan.

Die Server werden für die Bereitstellung der zentralen Dienste vor Ort in den Schulen benötigt. Eine Bereitstellung der oben genannten Dienste zentral bei der citeq auf wenigen Servern ist aufgrund der WAN-Struktur des Netzes und der vielen Standorte nicht möglich.

9.4.1. Fileservices

Als Fileservice bezeichnet man die zentrale Datenhaltung an einer Stelle auf einem Server. Für die zentrale Datenhaltung an einer Stelle spricht ein einfacher Austausch von Daten mit Hilfe dieser zentralen Stelle zwischen mehreren Anwendern. Alle Anwender (oder eine Gruppe von Anwendern) erhalten lesenden und / oder schreibenden Zugriff auf bestimmte Speicherorte auf dem Server. Diese Möglichkeiten werden durch eine entsprechende Verzeichnisstruktur und ein Berechtigungssystem gewährleistet.

Eine zentrale Datenhaltung ermöglicht erst eine zuverlässige Sicherung der Daten der Benutzer.

9.4.2. Printservices

Die Novell Server ermöglichen die Bereitstellung von Druckdiensten im Netzwerk mittels iPrint. Der Vorteil liegt darin, dass von allen Arbeitsplätzen auf alle Drucker zugegriffen werden kann. Dies ermöglicht die Reduzierung der Anzahl der Drucker. Das Konzept weniger Netzdrucker ist preiswerter als ein Konzept mit vielen kleinen Druckern, die lokal an jeden einzelnen PC angeschlossen werden. Darüber hinaus ist es möglich, von jedem Arbeitsplatz auf spezielle Drucker (DIN-A3 / Laser / Farbe) zuzugreifen, während sonst für jeden PC nur der jeweils angeschlossene Drucker zur Verfügung steht.

9.4.3. Dynamic Host Control Protocol (DHCP)

Zur Identifizierung und Adressierung erhält jeder Rechner eine Netzwerkadresse, die so genannte IP-Adresse (Internet Protocoll Address). Um andere Komponenten im Netzwerk erreichen zu können, benötigt der Rechner weitere Informationen über die Struktur des Netzwerk-Segmentes:

- die Netzmaske,
- das Standard-Gateway in andere Netzsegmente,
- den Namen des Rechners, auf dem der DNS-Dienst (s. u.) vorgehalten wird.

Diese Informationen werden sinnvoller Weise nicht auf jedem PC einzeln eingetragen, sondern vom PC beim Starten von einem besonderen Serverdienst, dem DHCP, abgefragt. Die Vergabe der Adressen mittels DHCP ermöglicht gegenüber dem Eintragen der Informationen auf jedem einzelnen Client-PC auch eine einfache Änderung der Daten an zentraler Stelle, eben dem DHCP-Dienst auf dem Server. Deswegen sprechen höhere Flexibilität, raschere Änderungsmöglichkeit und vor allem aber die erhebliche Reduzierung des Betreuungsaufwandes (Kosten) für die Nutzung dieses Dienstes.

9.4.4. Domain Name Service (DNS)

Die Rechner in einem Netzwerk kommunizieren intern mit den oben genannten IP-Adressen. Da diese Ziffernfolgen schlecht zu merken sind, erhalten Server und PC in einem Netzwerk zusätzlich "sprechende" Rechnernamen. Zur Umwandlung der Rechnernamen zu den IP-Adressen und umgekehrt wird der Dienst DNS verwendet. Ohne den lokalen DNS-Dienst wäre auch ein Zugriff auf die Server des Internet unmöglich, da die Adressierung im Internet ausschließlich über das DNS erfolgt.

9.4.5. Mailing

Für die Bereitstellung der Funktion Mailing kommt in den Schulverwaltungen das Produkt "GroupWise" der Fa. Novell zum Einsatz. Dabei handelt es sich um einen Mailserver, der sowohl in das Betriebssystem Novell NetWare wie auch in den Novell Linux Open Enterprise Server optimal integriert ist. So benötigt man nur eine Benutzerverwaltung für die Dienste des Servers. Dieser Dienst ermöglicht den Austausch von Mail, also Briefen zwischen verschiedenen Nutzern. Die großen Vorteile gegenüber der Briefpost liegen in den geringeren Kosten, der höheren Transportgeschwindigkeit und der Vermeidung eines Medienbruchs. Die elektronisch vorliegenden Daten müssen nicht gedruckt, verschickt und wieder erfasst werden.

GroupWise hat sich bei der Stadt Münster auch bei großen Benutzerzahlen (mehr als 3000) über die Jahre bewährt. Für die Schulverwaltungen ist so eine optimale Integration in die Bürokommunikation der Stadt Münster gegeben. Dabei kann abhängig von den Anforderungen sowohl der Client für GroupWise als solcher, als auch Web-Access zum Einsatz kommen.

Bei GroupWise Web-Access handelt es sich um eine Zugriffsmöglichkeit auf GroupWise mittels Web-Mail unter Verwendung des Standard-Internetbrowsers.

In der Pädagogik erfolgt das Mailing ausschließlich durch einen Dienst, auf den über einen Web-Mail-Zugang zugegriffen werden kann, so dass neben einem Standard-Internetbrowser keine zusätzliche Software auf dem Client benötigt wird. Mit diesem Dienst können die Schüler und Lehrer Mails untereinander, mit anderen MEP-Schulen sowie auch mit externen E-Mail-Empfängern weltweit austauschen. Damit kann der Bereich "Mailing" als fester Bestandteil in der Medienerziehung von den Schulen eingeplant werden. Es steht den Schulen jedoch frei zu entscheiden, das Mailing in der Pädagogik grundsätzlich bzw. für einzelne Benutzer nicht zuzulassen.

9.4.6. Spam

Die citeq begegnet dem Problem der unerwünschten Mails (SPAM) bereits seit Jahren. Im Laufe der Zeit wurden die Maßnahmen zur Abwehr bzw. Kennzeichnung im Verwaltungsnetz stetig erweitert. Bisher kommen zwei Maßnahmen zum Einsatz:

- Zum einen die Blockung von Mail von Einwahlrechnern und

- zum anderen die Kennzeichnung von SPAM mittels "****SPAM****" im Betreff.

Für die Blockung von Mail von Einwahlrechnern kamen ursprünglich statische, von der citeq gepflegte Listen zum Einsatz. Seit Mitte 2006 wird zusätzlich zu den statischen Listen auch Greylisting zur Abwehr von SPAM von Einwahlrechnern eingesetzt.

Die Kennzeichnung der Mails als SPAM erfolgt durch die Software SpamAssassin. Leider werden kaum mehr SPAM Mails durch SpamAssassin gekennzeichnet, da die Versender von SPAM die Mails an SpamAssassin trainieren. Die SPAM Mails werden solange verändert, bis sie durch SpamAssassin nicht mehr gekennzeichnet werden.

Erfolgreich wehrt die citeq SPAM mit den statischen Listen und durch das Greylistings ab. Hier werden an einem Werktag etwa 50%, an einem Wochenende etwa 80% der eingehenden Mail im Sinne einer SPAM Abwehr durch die citeq blockiert. Eine höhere Quote kann mit den genannten Listen zurzeit nicht erreicht werden, da sich die Versender von SPAM Mails entsprechend auf diese Abwehrmethoden eingestellt haben und SPAM Mails solange anpassen, bis sie nicht mehr herausgefiltert werden.

Um die SPAM Abwehr weiter zu verbessern hat die citeq Anfang 2007 mehrere Produkte zur SPAM Kennzeichnung getestet. Als Ergebnis hat die citeq einen zentralen SPAM Filter beschafft. Durch den Einsatz des vorgenannten SPAM Filters erwartet die citeq nach den bisherigen Tests eine weitere Reduzierung der bislang nicht blockierten SPAM Mails um ca. 80 %. Der Einsatz erfolgt voraussichtlich ab September 2007 auch im Verwaltungsbereich des MEP.

9.4.7. Intranet in der Schule

Um auch im internen Netz den Umgang mit der Technik des Internet zu ermöglichen und zentral allgemeine Daten bereitstellen zu können, wurde auf dem Novell Server ein WWW-Dienst installiert. Bei dem Produkt handelt es sich um einen „Apache“-Webserver. Dieser Dienst findet eine starke Verbreitung im Internet auf weit mehr als 50% aller WWW-Server.

Praktisch wird dieser Dienst bereits bei der Nutzung der sog. Info-Displays in den Schulverwaltungen genutzt. Über die Info-Displays werden an einem oder mehreren Orten in der Schule Informationen zur Verfügung gestellt, die vorab in ein bestimmtes Verzeichnis des Dienstes abgelegt wurden (in der Regel Vertretungspläne).

9.4.8. Virenschutz

Für einen umfassenden Schutz vor Viren wird ein Viren-Scanner auf dem Server eingesetzt. Dieser Scanner untersucht alle Dateien, die auf dem Server abgelegt werden, auf Viren. Werden Viren in einer Datei gefunden, wird dies dem Benutzer und dem Administrator des Servers gemeldet und der Virus wird gelöscht. Darüber hinaus können vom Administrator bei Bedarf weitere Maßnahmen veranlasst werden.

Der Schutz vor Virenbefall ist auch bei restriktiver Handhabung von Datenaustausch über Disketten- und CD-ROM-Laufwerke, sowie bei Absicherung der PC-Clients mit PC-Wächtersoftware erforderlich. Viren könnten ansonsten auch bei jeder autorisierten Softwareinstallation unerkannt ins Netz gelangen und sich über Netzlaufwerke, Softwareinstallation oder Mailing verbreiten.

Die Aufwände und damit auch die Kosten zur Beseitigung eines eingetretenen Virenbefalls sind erheblich. Weiterhin wären bei einem Viren- oder Trojanerbefall der Datenschutz und die Datensicherheit gefährdet. Aus diesen Gründen und um Imageschäden zu vermeiden sieht die citeq auch auf dem Server den Einsatz eines Virenschanners vor.

9.4.9. CD -Manager

Die Nutzung vieler Lernsoftwareprodukte setzt voraus, dass nach dem Programmstart auf die Original-CD zugegriffen werden kann. Die Bereitstellung dieser Medien erfolgt über die Dateidienste des Novell-Servers im Zusammenspiel mit einem virtuellen CD-Rom-Laufwerk auf den Client-PC. In der Vergangenheit hat sich die zentrale Bereitstellung der CD bewährt. Durch die Ablage der CD auf dem Server können Probleme vermieden werden, die bei der Nutzung der lokalen CD-ROM-Laufwerke auftreten würden (Anzahl der benötigten Medien, Funktionsstörungen durch Verschmutzung oder Kratzer auf dem Medium). Allerdings ist nicht jede CD-basierte Software für diese Betriebsart geeignet. Aus diesem Grund ist für jedes Produkt ein eigener Test erforderlich.

9.4.10. Internetzugang mittels Proxy-Services

Für den Zugriff auf das Internet ist der Einsatz eines Proxy-Dienstes auf den Novell Servern sinnvoll.

"Proxy" heißt Bevollmächtigter oder Stellvertreter. Ein Proxy-Server ermöglicht Systemen, die keinen direkten Zugang zum Internet haben, den indirekten Zugang zum Netz. Das sind insbesondere solche Systeme, die durch eine Firewall aus Sicherheitsgründen vom unmittelbaren Zugang ausgeschlossen sind. Ein Proxy kann einzelne Datenpakete aus dem Datenstrom zwischen dem Internet und einem lokalen Netz herausfiltern und so zur Erhöhung der Sicherheit beitragen. Proxies werden auch dazu benutzt, Zugriffe auf bestimmte Server zu begrenzen. Beim Zugang über Proxy-Server können auch gezielt Internet-Dienste wie zum Beispiel "Telnet" ausgeschaltet werden, um die Nutzung nicht gewollter Dienste zu verhindern.

Der Einsatz eines Proxy-Servers ermöglicht zum einen einfachere Regeln beim Zugriff der Clients auf das Internet durch die Firewall der citeq, da die Client-PC sich alle an den Server wenden und nur der Proxy-Server entsprechend freigeschaltet werden muss. Dies stellt eine erhebliche Vereinfachung der Administration der Firewall dar. Zum anderen speichert der Proxy bereits abgefragte Webseiten in einem Speicher des Proxy temporär zwischen und stellt sie bei erneutem Abruf der Webseite dem Benutzer direkt zur Verfügung. Dies spart zum einen Kosten bei der Internetanbindung der citeq, zum anderen beschleunigt es den Internetzugriff auf häufig genutzte Seiten erheblich.

Darüber hinaus ist eine Untersuchung der aus dem Internet geladenen Dateien auf Viren durch den zentralen Virens Scanner der citeq in der Firewall nur bei Zugriff auf das Internet über einen Proxy möglich. Dabei wird der Proxy der Schule auf dem Novell Server so konfiguriert, dass er die Daten nicht direkt aus dem Internet liest, sondern sie über den auch als Proxy dienenden Virens Scanner-Server in der Firewall der citeq holt.

9.5. Internetfilter SquidGuard

Mit der gleichen Technik - der Umleitung auf den Proxy der citeq - wird mit Hilfe des Produkts SquidGuard die Filterung der Daten auf unerwünschte Inhalte durchgeführt (Pornografie, Gewalt usw.).

Bei der Aufstellung des MEP wurde vorgesehen, den Zugriff auf die von der Bundesprüfstelle für jugendgefährdende Schriften veröffentlichten Links zu sperren. Die Praxis hat allerdings sehr schnell gezeigt, dass die Schulen damit nicht ausreichend gegen unerwünschte Inhalte im Internet geschützt waren. Deshalb wurde das Produkt SquidGuard implementiert, da es kurzfristig und mit relativ geringem Aufwand in die IT-

Landschaft der citeq integriert werden konnte. Mit SquidGuard werden zurzeit ca. 60.000 Seiten mit unerwünschten Inhalten gesperrt.

Da in den SquidGuard-Listen auch immer wieder Websites zu finden sind, die nicht gesperrt werden sollen, hat die citeq eine sog. Whitelist implementiert. Über die Whitelist können Seiten, für die der SquidGuard ursprünglich den Zugriff verweigern würde, freigeschaltet werden (z. B. www.love-line.de, Informationsseite der Bundeszentrale für gesundheitliche Aufklärung). Für den Fall, dass Seiten, für die der SquidGuard ursprünglich den Zugriff erlauben würde, gesperrt werden sollen, hat die citeq eine sog. Blacklist implementiert. Beide Listen werden vom Amt für Schule und Weiterbildung in Abstimmung mit den Schulen gepflegt.

Der SquidGuard wird in regelmäßigen Abständen von der citeq aktualisiert.

9.6. Arbeiten bei Ausfall der Netzanbindung

Grundsätzlich ist die gesamte Serverinfrastruktur auf eine dauerhaft bestehende WAN-Leitung ausgelegt. Dieses ist für die uneingeschränkte Funktionalität des eDirectory (siehe unten) zwingende Voraussetzung, da alle im eDirectory vorhandenen Server in regelmäßigen Abständen miteinander kommunizieren.

Die bisherigen Erfahrungen im MEP haben gezeigt, dass es bei den durch einen Telekommunikationsprovider zur Verfügung gestellten WAN-Verbindungen zu den Schulen gelegentlich zu Ausfällen kommt. Um den Schulen auch während eines Ausfalls der WAN-Verbindung die Nutzung der IT-Technik zu ermöglichen, sind Umstellungen im Sinne eines autarken Betriebes der IT-Technik in den Schulen notwendig. In den Schulverwaltungen sind diese Umstellungen durch die citeq bereits vorgenommen worden. Somit stehen hier alle Standarddienste - mit Ausnahme des Mailings und dem Zugriff auf das Internet - auch bei Ausfall der Netzanbindung zur citeq zur Verfügung. In den pädagogischen Netzen ist die Umstellung aufgrund der geschützten Rechner mit einem wesentlich höheren Aufwand verbunden. Die Umstellung dieser Rechner durch die citeq erfolgt bis Ende 2007.

9.7. Benutzer-/Gruppenverwaltung / eDirectory

Für die Verwaltung von Benutzern und Gruppen und den dazugehörigen Rechten wird der in Novell NetWare enthaltene Verzeichnisdienst eDirectory (vormals NDS) verwen-

det. Benutzer-Accounts können für Lehrkräfte, Schüler, Klassen und Kurse mit entsprechenden Rechten eingerichtet werden. Ändert sich z. B. der Status eines Schülers durch Versetzung, dann sind Anpassungen der Rechte erforderlich.

Für die Nutzung insbesondere der Dienste File-, Printservices und Mailing sind diese Benutzerkennungen (Accounts) zur Festlegung von Rechten an den einzelnen Dateien und Mailkonten notwendig. Ohne diese Abstufungen hätte jeder Benutzer Zugriff auf alle Daten, also auch die Schüler auf die Daten der Lehrer.

Für die Verwaltung der Rechte der Benutzer werden Benutzergruppen eingerichtet und den Gruppen werden Rechte zugeordnet. Die Rechte eines Benutzers sind dann abhängig von den Gruppen, deren Mitglied er ist.

Der Verzeichnisdienst eDirectory wird bei der citeq seit einigen Jahren sehr erfolgreich zur Verwaltung der ca. 3.500 Benutzer-Accounts der Stadt Münster und der ca. 21.000 Benutzer-Accounts des pädagogischen Netzes des MEP verwendet. Er ermöglicht eine einheitliche Administration der Benutzerinformationen über Servergrenzen hinweg. Die bei der Aufstellung des MEP angedachte Übernahme der Änderungen von Benutzerdaten aus der Schülerverwaltung wäre sinnvoll, da sie die Pflege der Daten sowohl für die Schulen als auch für die citeq erleichtern würde, weil keine parallele Pflege der Daten im eDirectory und in der Schülerverwaltung mehr erforderlich wäre. Die Realisierung würde allerdings voraussetzen, dass alle Schulen das gleiche Schülerverwaltungsprogramm nutzen würden,.

Auf Wunsch der Schulen wird auf allen Servern mitprotokolliert, welche Kennung sich wann an welchem Client angemeldet hat. Auf diese Information haben sämtliche Lehrer Zugriff. Sie dienen der Schule zur Kontrolle der IT-Nutzung durch die Schüler für den Fall, dass dadurch Schäden an der Hardware oder den genutzten Räumen auftreten sollten.

Es muss allerdings berücksichtigt werden, dass durch das Protokollieren der Nutzung der Clients lediglich festgestellt werden kann, welche Kennung sich angemeldet hatte. Dieses bedeutet aber nicht zwangsläufig, dass auch die Person, der diese Kennung zugeordnet war, an dem entsprechenden Rechner gearbeitet hat. Zum einen kann es sein, dass jemand den Rechner verlassen hat ohne sich abzumelden oder ihn zu sperren, zum anderen ist es möglich, dass das Kennwort auch anderen Personen bekannt war, welche sich dann mit der entsprechenden Kennung authentifiziert haben. Aus diesem

Grund sollte man sich immer vom Rechner abmelden bzw. ihn sperren, wenn man ihn nur kurz verlässt, und niemals sein Kennwort an andere Personen weitergeben.

Weiterhin sollte der Rechner nicht im laufenden Betrieb übernommen werden, da der Vornutzer temporäre Installationen vorgenommen haben könnte, mit denen er einen Remotezugriff versuchen könnte. Vor Arbeitsbeginn mit der eigenen Kennung sollte der Rechner in jedem Fall neu gestartet werden, damit der Wächterschutz verbliebene temporäre Installationen löschen kann.

Auf Wunsch der Schulen wird im pädagogischen Netz ein sog. Druckerauditing eingerichtet. Dieses bietet die Möglichkeit, sämtliche Daten aller Druckereignisse im pädagogischen Bereich in einer Datei zu protokollieren. Gespeichert werden

- • Name des Anwenders
- • Name des Druckers
- • Datum/Uhrzeit des Abschickens und des Fertigstellens
- • Seitenanzahl des Auftrages
- • Größe des Druckauftrages
- • Ist ein Auftrag erfolgreich beendet oder evtl. abgebrochen worden
- • Name des Dokuments

Auf die so erzeugte Datei haben alle Lehrer Zugriff, um z. B. die Verbrauchskosten der Drucker den Kennungen zuzuweisen.

9.8. Rechte der IT-Koordinationen

Ziel des MEP war u. a., die mit IT-Aufgaben betrauten Lehrer an den Schulen entsprechend zu entlasten. Einzig der unabdingbare First-Level-Support sollte noch von den IT-Koordinationen geleistet werden. In der Praxis hat sich allerdings gezeigt, dass insbesondere die IT-Koordinationen der weiterführenden Schulen nach Möglichkeiten gefragt haben, um kleinere administrative Aufgaben kurzfristig selber erledigen können. Die cit-teq ist bemüht, den IT-Koordinationen diese Möglichkeiten zur Verfügung zu stellen. Hierzu zählen zurzeit:

- das Zurücksetzen der Benutzerkennwörter im eDirectory
- das Sperren von Kennungen
- die Änderung der Gruppenzugehörigkeiten

- die Vergabe der Rechte am ungesicherten Laufwerk (s. u.)
- das Löschen von Druckaufträgen
- das Ändern der Druckerzuordnungen auf den Client-PC
- das Aufräumen der Server von nicht mehr benötigten bzw. nicht unterrichtsrelevanten Dateien
- das Ändern von Quotings, sofern eingerichtet

Hierzu stehen den IT-Koordinatoren folgende Tools zur Verfügung: Console One, Windows-Dateiexplorer, Druckerverwaltung, TreeSize. Dieses Angebot wird bei Bedarf erweitert. Die Dokumentationen für diese Tools sind zukünftig im MEP-net zu finden. Die Schulen können die vorgenannten administrativen Tätigkeiten selbstverständlich auch von der citeq durchführen lassen. Das empfiehlt sich insbesondere für kleinere Schulen und/oder IT-Koordinatoren, die mit dem Umgang der zur Verfügung gestellten Tools nicht vertraut sind.

9.9. Datenhaltung

Die Daten werden in einer auf allen Servern einheitlichen Verzeichnisstruktur abgelegt. Hierzu gehören für jeden Benutzer ein persönliches Laufwerk, für jede Klasse ein Klassenordner, für jede Gruppe ein Gruppenordner und für die schulweite Kommunikation ein weiterer Ordner. Darüber hinaus richtet die citeq für die Bereitstellung von Software und sonstiger Dienste weitere Ordner / Laufwerke auf dem Server ein.

Eine einheitliche, standardisierte Verzeichnisstruktur und eine ebenso einheitliche Zuordnung dieser Verzeichnisse zu Laufwerksbuchstaben auf allen Servern an allen Schulen ist erforderlich, um bei der hohen Anzahl an Servern und Client-PC Abläufe, z. B. bei der Installation, automatisieren zu können.

Persönliche Laufwerke ermöglichen die Ablage von Daten, ohne dass Andere auf diese Daten zugreifen können. Allerdings können Lehrkräfte grundsätzlich alle Schülerdaten einsehen, um Ihrem Lehrauftrag grundsätzlich und im Vertretungsfall nachkommen zu können. Andere Dateien werden von mehreren Benutzern benötigt und ggf. verändert. Dafür stehen, abhängig von der gemeinsamen Zugehörigkeit zu einem Jahrgang, einer Klasse oder Gruppe spezielle Verzeichnisse zur Verfügung, auf die nur die jeweiligen Gruppenmitglieder zugreifen können. Darüber hinaus steht allen Lehrern und Schülern ein schulweiter Ordner (Schulforum) für die Bereitstellung von Informationen durch die Lehrer zur Verfügung. Für den Austausch von Daten untereinander wird den weiterfüh-

renden Schulen ein Tauschordner eingerichtet, auf den auch die Schüler schreibenden Zugriff haben. Der Tauschordner wird automatisch jeden Abend geleert.

Schulformübergreifend stehen allen Schulen in der Verwaltung zurzeit 10 GB an Speicherplatz zur Verfügung. In der Pädagogik stehen den Grundschulen zurzeit 10 GB und den weiterführenden Schulen zurzeit 30 GB Speicherplatz zur Verfügung. Die Beschränkung des Speicherplatzes je Schule wurde vorgenommen, da nur unter diesen Bedingungen die regelmäßige Datensicherung (siehe unter 9.11 "Datensicherung Server") durchgeführt werden kann.

Die Erfahrungen des MEP haben gezeigt, dass die weiterführenden Schulen in der Pädagogik mehr Speicherplatz benötigen als die ursprünglich vorgesehenen 30 GB. Aus diesem Grund wurde jeder weiterführenden Schule noch ein zusätzliches Laufwerk von zurzeit ebenfalls 30 GB zur Verfügung gestellt. Die Verwaltung dieses Laufwerks (z. B. Rechtevergabe) liegt in der alleinigen Verantwortung der Schule. Dieses Laufwerk wird jedoch nicht gesichert. Bei einem totalen Serverausfall lassen sich die Daten dieses Laufwerks nicht zurücksichern. Es ist daher erforderlich, dass die Schule die Sicherung dieser Daten (z. B. auf DVD) selber im erforderlichen Rahmen organisiert.

Um die Verwendung des beschränkten Plattenplatzes auf den Servern nicht ausufern zu lassen, gibt es die Möglichkeit, den einzelnen Benutzern am Dateisystem des Servers Grenzen zu setzen. Diese Begrenzung von Plattenplatz durch Einrichtung von Schwellwerten wird "Quoting" genannt. Das Quoting wurde auf Anforderung der Schulen eingeführt, weil einzelne User wiederholt und in großem Umfang Speicherplatz auf dem Server belegt hatten. Durch das Quoting kann dieses verhindert werden. Je nachdem, wie die Schwellwerte gewählt werden, ist das Abspeichern größerer Dateien ohne Unterrichtsbezug (z. B. Kopien von Spielen) nicht mehr möglich. Die Einrichtung des Quotings ist den Schulen freigestellt. Die bisherigen Erfahrungen mit dem Quoting sind durchweg positiv.

9.10. Softwarerepository

Für die Installation der Client-PC müssen die Updates der Clients und die Informationen über die Updates auf dem Server abgelegt werden. Dies erfolgt in einem so genannten Repository auf dem Server.

Für die Installation der Client-PC wird die Softwareverteilung "Zero Efforded Network" (ZEN) eingesetzt. Dabei wird die zu installierende Software zu Paketen zusammengestellt und auf die PCs kopiert. Da die Pakete sehr große Datenmengen umfassen können und die Leitungsbandbreite auf dem Übertragungsweg zwischen citeq und der Schule beschränkt ist, muss in jeder Schule ein Zwischenspeicher vor Ort vorhanden sein. Dieser Zwischenspeicher ist der Novell Server mit entsprechender Plattenkapazität für diese Pakete der Softwareverteilung. Zur Ablage der Pakete werden besondere Verzeichnisstrukturen geschaffen.

9.11. Datensicherung Server

Die Sicherung der Daten erfolgt in zwei Stufen.

In der ersten Stufe werden nur die geänderten Daten aller DAT:-Volumes der Server in den Schulen mittels des Tools rsync jede Nacht auf einen zentralen Server der citeq übertragen. Dies führt dazu, dass der gesicherte Datenbestand sowohl auf dem Server in der Schule vor Ort als auch auf einem zentralen Server vorhanden ist.

In der zweiten Stufe werden nun die Daten des zentralen Servers der citeq mittels eines Datensicherungsroboters auf Bänder für mindestens sechs Wochen gesichert. Es ist somit sichergestellt, dass Daten, die vor sechs Wochen gelöscht wurden, noch wiederhergestellt werden können. Alle zwei Wochen erfolgt am Wochenende eine Vollsicherung aller Daten des zentralen Servers. An allen anderen Werktagen erfolgt eine inkrementelle Bandsicherung, das heißt, es werden nur die geänderten Daten auf Band geschrieben. Durch diese Methode der Sicherung werden große Bandressourcen gespart. Ansonsten wäre es bei der heutigen Datenmenge nicht mehr möglich, alle Daten für mindestens sechs Wochen vorzuhalten. Bei der inkrementellen Sicherung wird bewusst in Kauf genommen, dass bei einem Totalausfall eines Servers die Datenrücksicherung einige Zeit in Anspruch nimmt.

Die zentrale Datensicherung hat den Vorteil, dass vor Ort keine Bänder gewechselt werden müssen. Auch kann auf Reinigung und Wartungsarbeiten an den Laufwerken verzichtet werden.

In der Praxis hat sich herausgestellt, dass die täglichen Änderungen des Datenbestandes im pädagogischen Netz teilweise so groß waren, dass auf die Sicherung einiger Dateitypen wie z.B. Filme, CD- bzw. DVD-Images, Fotos oder Musikdateien verzichtet werden musste. Es ist war nicht mehr möglich, alle an einem Tag geänderten Dateien in-

nerhalb einer Nacht zum zentralen Server zu synchronisieren. Falls die Schule eine Sicherung dieser Dateien benötigt, ist sie hierfür selbst zuständig. Z.B. kann die Datensicherung durch Brennen auf DVD durchgeführt werden.

Die folgenden Dateitypen werden aus den oben genannten Gründen in der Pädagogik nicht durch die citeq gesichert (Stand 03/2007):

- *.wma Windows Media Audio Datei
- *.asf Audio- bzw. Active-Streaming Datei
- *.wmv Windows Media Video Datei
- *.swf Macromedia Flash Datei
- *.ogg OGG-Audio Datei
- *.nrg Nero Image Datei
- *.vob DVD-Video-Datei
- *.c2d WinOnCD Image-Datei
- *.iso ISO-Image Datei
- *.gif GIF Grafik
- *.bmp Bitmap Grafik
- *.jp[e]g Jpeg Grafik
- *.exe ausführbare Datei
- *.rm Real Media Datei
- *.mov Quicktime Datei
- *.avi Avi Video Datei
- *.mp[g34] Mpeg Video Datei
- *.mpeg Mpeg Video Datei
- *.rar Rar gepackte Datei
- *.r[0-9][0-9] Rar gepackte Datei
- *.tmp temporäre Datei
- dbCache.dat Datendatei von Google Earth

Die jeweils aktuelle Liste kann im MEP-net eingesehen werden.

In der Verwaltung sind die Änderungen in der Regel deutlich geringer, so dass dort nach wie vor alle Dateien über Nacht synchronisiert werden können.

9.12. Remote Administration

Für die Verwaltung der Novell-Server stehen verschiedene Möglichkeiten zur Verfügung. Zum einen kann mittels der Fernkonsolen „RconJ“ bzw. „Putty“, die Serverkonsole vom Büroarbeitsplatz aus bedient werden. Weiterhin kann die Administration der Server und deren Dienste über Web-Interfaces wie dem „iManager“, dem „iMonitor“ oder dem „Remote Manager“ durchgeführt werden. Als dritte Möglichkeit zur Fernwartung verfügen die Server über ein so genanntes LOM (Lights Out Management). Dieses ist zu verstehen als ein kleiner Administrationscomputer im Server, mit dessen Hilfe sich z.B. virtuelle Laufwerke ansprechen lassen. Die Server können zudem aus der Ferne aus- und eingeschaltet oder auch wie über eine Fernkonsole vom Arbeitsplatz aus bedient werden.

Die Kombination dieser Möglichkeiten ermöglicht die Fernwartung und Administration der Server über die WAN-Leitungen von der citeq aus. Es ist daher nur in seltenen Fällen notwendig, dass ein Mitarbeiter der citeq im Rahmen der Serveradministration zu einer Schule fährt. Dies spart Wegezeiten, Kosten und reduziert vor allem die Dauer von Betriebsstörungen.

10. Clients

10.1. Hardwareausstattung

Entsprechend der Festlegung in den Rahmenbedingungen des technischen Ausstattungs- und Betriebskonzeptes kommen in der Schulverwaltung und im pädagogischen Bereich nur neue, standardisierte PC zum Einsatz.

Weitere Hardwarekomponenten (Brenner, Scanner, Drucker, Druck-Kopier-Systeme, Bildschirme, etc.) werden, soweit durch die citeq beschafft, in Betrieb genommen. Die dazu notwendige Software wird auf der angeschlossenen Workstation installiert.

10.2. Wächterschutz

Neben einer aktuellen Hardwareausstattung ist für den späteren Betrieb im Unterricht selbstverständlich ein hoch verfügbares Betriebssystem notwendig. Nur dadurch lässt sich eine Akzeptanz bei den Anwendern und ein möglichst störungsfreier Unterricht erreichen. Dazu zählt auch ein Mechanismus zum Schutz vor mutwilligen Manipulationen

an den Programmen und dem Betriebssystem. In der ursprünglichen Fassung des MEP war der Einsatz einer hardwaregebundenen Lösung, den so genannten PC-Wächterkarten, vorgesehen. Schon zu Beginn des praktischen Einsatzes traten beim Betrieb der Wächterkarte technische Schwierigkeiten auf. Ursache war ein nicht vorhersehbarer Konflikt mit der Konfiguration der Software ZENworks, die u. a. für die Softwareverteilung zum Einsatz kommt (siehe unter 10.5. "Vorbereitung der Clients und Softwareverteilung"). Als Ergebnis intensiver Tests wurde der Einsatz der Wächterkarten verworfen und die ebenfalls von der Fa. Dr. Kaiser angebotene softwarebasierende Wächterlösung "PC-Drive" als Schutz für alle Rechner im unterrichtlichen Bereich eingeführt.

Die Wächtersoftware sorgt dafür, dass bei aktivem Wächterschutz alle Veränderungen des Betriebssystems und der Software (z.B. die testweise Installation von Software, aber auch unabsichtliches oder mutwilliges Löschen von Software oder Dateien) nach einem Neustart des Rechners wieder in den definierten Betriebszustand zurückgestellt werden. Dadurch lässt sich der Rechner als "normale Workstation" benutzen. Alle Einstellungen können eingesehen und auch verändert werden. Erst bei einem Neustart der Workstation wird der Ursprungszustand wieder hergestellt.

Die Wächtersoftware kann darüber hinaus über das Netzwerk administriert werden. Sie verringert den Wartungsaufwand für den Betrieb der Clients, da diese vom Benutzer nicht verkonfiguriert werden können und stellt somit eine hoch verfügbare Nutzung der Rechner sicher. Die Funktionalität der PC-Wächtersoftware hat sich als absolut sicher erwiesen.

Lediglich der citeq ist es durch einen administrativen Zugang möglich, dauerhafte Veränderungen am Betriebssystem oder an der Software vorzunehmen.

Im Schulverwaltungsnetz ist der Einsatz einer Wächtersoftware nicht notwendig, da hier mit einer mutwilligen Manipulation des Betriebssystems bzw. der Programme nicht zu rechnen ist. Aus diesem Grund wird in den Schulverwaltungen keine Wächterlösung installiert.

10.3. Betriebssystem

Für das Schulnetz ist ein Betriebssystem auszuwählen, das aktuelle Technologien (z.B. USB, Multimediaanwendungen) unterstützt, aber auch in Fragen der Stabilität und Ad-

ministration alle Ansprüche erfüllt. Eine Unterstützung gängiger Netzwerktechnologien (Roaming-Profile, etc.) ist dabei ebenfalls von entscheidender Bedeutung.

Bei der Aufstellung des MEP wurde daher entschieden, Windows XP Professional in der Schulverwaltung und dem unterrichtlichen Bereich einzusetzen. Die Professional-Edition von Windows XP ist von Microsoft besonders für den Einsatz in Netzwerken konzipiert worden und erfüllt alle Anforderungen an ein modernes Betriebssystem.

Laut der Microsoft wird für Windows XP noch bis zum 08.04.2014 ein so genannter „Extended Support“ gewährt (<http://support.microsoft.com/lifecycle/?p1=3223#>). Die Unterstützung mit aktuellen Sicherheitspatches ist damit dauerhaft gewährleistet, obwohl bereits mit Windows Vista ein Nachfolge-Betriebssystem zur Verfügung steht.

Alternative Betriebssysteme wie Microsoft Vista oder Linux können erst nach intensiver Prüfung durch die citeq zum Einsatz kommen. Vor einer Entscheidung ist immer eine Kosten-Nutzen-Abwägung vorzunehmen und die technischen Umsetzungsmöglichkeiten in der bestehenden IT-Infrastruktur zu prüfen. Aktuell hält die citeq über 230 Programme und Installationsroutinen vor, die unter Windows XP getestet wurden. Für sämtliche Produkte müssten für ein anderes Betriebssystem neue oder angepasste Installationsroutinen geschaffen werden, wobei es fraglich ist, ob auch alle bisherigen Produkte die alternativen Betriebssysteme unterstützten. Wahrscheinlich würden weitere Kosten durch die Beschaffung zusätzlicher Lizenzen und aktueller Softwareversionen, sowie durch einen erhöhten administrativen Aufwand, den ein paralleler Einsatz unterschiedlicher Betriebssysteme verursachen würde, entstehen. Aus wirtschaftlichen Gründen wird zum jetzigen Zeitpunkt kein Wechsel in Erwägung gezogen.

Auch technische Notwendigkeiten für den Umstieg auf Windows Vista oder Linux sind im Moment nicht ersichtlich. Für Vista Ultimate endet z. B. der Support durch Microsoft bereits am 10.04.2012 (<http://support.microsoft.com/lifecycle/?p1=11734>); 2 Jahre vor dem Supportende für Windows XP Prof.

10.4. Clientsoftware

10.4.1. Standardsoftware

Im pädagogischen Bereich wird auf allen Workstations standardmäßig folgende Software installiert:

- Office- und Textverarbeitungsprogramme:
 - o Office-Komponenten Winword, Excel, Powerpoint und Access (z. Zt. in der Version von Microsoft Office XP)
 - o Adobe Acrobat Reader
 - o Freeware zur Erstellung von PDF-Dateien (z. Zt. Ghostscript)
- Internet
 - o Web-Browser: Microsoft Internet Explorer
 - o Freeware-FTP-Client: FileZilla
- Multimediaprogramme:
 - o Windows MediaPlayer
 - o WinDVD
 - o Quicktime Viewer
 - o MM-Dateibetrachter IrfanView
- Hilfsprogramme
 - o Freeware-Packer bzw. -Archivierer (z. Z. PowerArchiver)
- Laufzeitumgebungen:
 - o Sun Java Runtime Environment
 - o Microsoft .Net-Framework V1.1 und V2.0
 - o Microsoft .Net-Visual J V1.1
- Sonstiges:
 - o McAfee Virenschutzprogramm
 - o notwendige Updates und Patches
 - o notwendige Druckertreiber

Zusätzliche oder ergänzende Softwarekomponenten werden nur nach den Regelungen, die für Zusatzsoftware gilt, installiert.

Die Installation von neuen Programmversionen und Updates der Standardsoftwareprodukte kommt nur dann in Betracht, wenn es aus technischen oder pädagogischen Gründen erforderlich ist. Die Planung und Durchführung der Installationen richtet sich nach dem damit verbundenen Aufwand und den zur Verfügung stehenden Ressourcen.

10.4.2. Stand-alone-Betrieb

Zur Nutzung der Rechner ohne Netzwerkverbindung stehen zwei allgemeine lokale Benutzerkonten zur Verfügung:

- Auf Notebooks wird ein Benutzer für den mobilen Einsatz mit der Möglichkeit, Daten permanent zu speichern, eingerichtet.
- Auf Desktop-Rechnern existiert eine Benutzerkennung, ohne die Möglichkeit Daten permanent zu speichern (zum Beispiel zum Schreiben von Klausuren). Eine Datensicherung ist dabei nur unter Zuhilfenahme von externen Datenspeichern (USB-Stick, mobile Festplatte) möglich.

10.4.3. Servergespeicherte Profile (Roaming-Profiles)

Für Nutzer, die an wechselnden Arbeitsplatzrechnern arbeiten (Roaming-Users), besteht die Möglichkeit eine persönliche Arbeitsumgebung an zentraler Stelle zu speichern. Windows XP Prof. bietet dafür so genannte "servergespeicherte Profile" an. Dabei werden anwenderbezogene Einstellungen, z.B. Desktop-Icons, im Netzwerk gesichert und bei der nächsten Anmeldung wieder geladen. Der Anwender findet also an jedem Rechner, immer wieder seine speziell eingerichtete Arbeitsumgebung vor. Die Profile werden auf dem Server der Schule vorgehalten, und von der citeq und den IT-Koordinatoren verwaltet. Eine lokale Speicherung des Profils ist, aufgrund der eingesetzten Schutzsoftware nicht möglich.

10.4.4. Verbindliche Profile (Mandatory-Profiles)

Die Möglichkeit der individuellen Gestaltung der Arbeitsumgebung hat jedoch im Schulumfeld, besonders bei Klassenkonten, den Nachteil, dass Schüler nicht gewollte Einstellungen vornehmen können. Um dieses zu vermeiden werden auf Wunsch der Schule verbindliche Profile (Mandatory-Profiles) eingerichtet. Hierbei handelt es sich um ein Masterprofil, das von der Schule vorgegeben wird, und von den Schülern nicht verändert werden kann. Dieses Masterprofil wird dann bei der Anmeldung der Schüler benutzt.

Lehrerkennungen erhalten in der Regel keine verbindlichen Profile.

10.4.5. Virenschutz und Updates

Obwohl die Rechner im unterrichtlichen Bereich weitgehend durch die Wächtersoftware gegen Virenangriffe geschützt sind, werden diese PC zusätzlich durch einen aktuellen Virens Scanner überwacht. Durch diese Maßnahme soll eine optimale Sicherheit von persönlichen Daten, insbesondere beim Datenaustausch via E-mail oder durch Wechselmedien, wie z. B. CD-ROM und USB-Sticks, gewährleistet werden. Ein zusätzlicher, lokaler Virens Scanner ist notwendig, da während des Rechnerbetriebes am lokalen PC keinerlei Virenschutzmechanismen greifen. Erst nach einem Neustart des Rechners würde die Wächtersoftware den geschützten Urzustand wieder herstellen, bis dahin könnten jedoch sämtliche Daten und Programme auf dem Server oder auf anderen Medien durch einen möglichen Virus beschädigt oder infiziert werden.

Die citeq installiert alle Aktualisierungen, die für einen ordnungsgemäßen Betrieb der Workstation notwendig sind. So ist beispielsweise eine regelmäßige Aktualisierung der lokalen Viren-Definitions-Files selbstverständlich.

Weiterhin werden auf allen Workstations die notwendigen Updates und Patches eingespielt, um den aktuellen Sicherheitsanforderungen zu genügen, und um mögliche Softwareprobleme zu beseitigen. Alle Maßnahmen in diesem Bereich werden von der citeq im Vorfeld auf ihre Notwendigkeit hin überprüft, um die Arbeit der Anwender so wenig wie möglich zu beeinträchtigen.

10.5. Vorbereitung der Clients und Softwareverteilung

Als administrative Aufgaben sind die Wartung und Pflege der eingesetzten System- und Anwendungssoftware durch die citeq wahrzunehmen. Hierzu gehören neben der Verteilung von Programmen des jeweiligen Software-Herstellers zur Fehlerbeseitigung ("Patches"), das Update von Software, die Verteilung von Software aus dem Warenkorb und die Betriebssysteminstallation neuer Systeme, bzw. das Zurücksetzen von vorhandenen Systemen in einen Grundzustand, z.B. nach einem Festplattenaustausch.

Bei allen Verfahren wird an die Softwareverteilung die Anforderung gestellt, dass die Installation möglichst rasch, zuverlässig und weitestgehend ohne Eingriff des Anwenders ablaufen soll und der administrative Aufwand dazu so gering wie möglich gehalten wird.

Für die Betriebssysteminstallation wendet die citeq daher eine Kombination aus Scripting- und Imageing-Verfahren an. Durch diese Kombination sollen die Vorteile beider Verfahren, bei gleichzeitiger Minimierung der Nachteile, ausgenutzt werden.

Dazu und für die Softwareverteilung wird auf den Workstations das Produkt ZENworks for Desktops der Firma Novell eingesetzt. Die citeq verwendet dieses Produkt bereits seit mehreren Jahren und hat damit gute Erfahrungen gemacht und entsprechendes Know-how aufgebaut.

Als nahezu einziges Produkt dieser Klasse bietet ZENworks das Desktop-Management und Remote Control an. Weiterhin wird ZENworks zu einem sehr günstigen Preis im Vergleich zu einer Kombination von Einzellösungen anderer Hersteller angeboten.

Durch die standardisierte Hardwareausstattung in den Schulen lässt sich ZENworks for Desktops in idealer Weise einsetzen. Die Rechner werden bei einer Erstinstallation oder bei Reparaturinstallationen innerhalb kürzester Zeit in der gewünschten Form eingerichtet. Dieses Verfahren ist personalexintensiv und daher sehr ressourcen- und kostensparend.

Es garantiert ein Minimum an Störungen für den Anwender und lässt sich in Einzelfällen sogar im normalen Unterrichtsbetrieb durchführen. Voraussetzung dazu ist, dass die PC-Wächtersoftware vorher abgeschaltet wird. Dies wird jedoch durch die citeq mittels Netzadministration der Wächterkarten sichergestellt. Um die Softwareverteilung außerhalb des Unterrichtsbetriebes zu gewährleisten, ist es unabdingbar, dass die Rechner ständig am Stromnetz angeschlossen und über das Netzwerk erreichbar sind. Notebooks sollten ebenfalls regelmäßig an das Netzwerk angeschlossen werden.

Als weiteres Feature bietet ZENworks "Remote-Control" und "Desktop Management" an. Remote-Control bietet die Möglichkeit für Administratoren Workstations von einem anderen Arbeitsplatz aus fern zu bedienen. Dabei kann die Funktion der Maus und Tastatur übernommen werden. Vor einem Remote-Zugriff wird der Anwender jedoch aufgefordert, der Sitzung zuzustimmen, so dass eine unbemerkte Überwachung des Rechners ausgeschlossen werden kann. Remote-Control bietet sich als Hilfsmittel zur kurzfristigen und schnellen Fehleranalyse an.

Über das Desktop Management von ZENworks lassen sich Richtlinien festlegen, um die Rechte von Benutzern zu beschränken. Damit werden mutwillige oder versehentliche

Manipulationen der Workstation weitgehend verhindert. Allerdings kann man die Rechner angesichts der häufig sehr experimentierfreudigen Schülerinnen und Schülern nur mit hohem personellem Aufwand wirklich zuverlässig schützen. Aus diesem Grund wird auf den Einsatz dieses Features von ZENworks weitestgehend verzichtet und der Einsatz von PC-Wächtersoftware befürwortet.

Im Bereich der Schulverwaltungen werden, wie bereits ausgeführt, keine Wächterkarten eingesetzt. Hier kommen Richtlinien zum tragen, die sich an den bereits bewährten Standards der Stadt Münster orientieren. Die Einschränkungen werden dabei so gering wie möglich gehalten. Der Virenschutz ist in beiden Umgebungen sichergestellt.

11. Technisches Betriebskonzept

11.1. Begriffsdefinition

Das Betriebskonzept umfasst die Summe aller Maßnahmen, die die Verfügbarkeit der in den Schulen bereitgestellten IT-Infrastruktur (Netzwerk, Server, Clients und Anwendungen) in einem vereinbarten Rahmen gewährleisten. Bedingt durch den hohen Ausstattungsgrad der Schulen kann eine den Belangen der Schulen entsprechende ausreichende Verfügbarkeit der IT-Infrastruktur nur durch eine geregelte Betriebsführung sichergestellt werden, wobei allerdings der Umfang der Maßnahmen zur Betriebsführung limitiert wird von den zu diesem Zweck bereitgestellten Mitteln.

Das Betriebskonzept orientiert sich verfahrenstechnisch an ITIL, einer herstellerunabhängigen Sammlung sog. „Best Practices“, mit denen es IT-Dienstleistern möglich ist, die IT-Prozesse effizient bereitzustellen und somit den Kunden einen optimierten und gleich bleibenden IT-Service zu gewährleisten. ITIL steht für „Information Technology Infrastructure Library“ und hat sich seit den 90er Jahren zu einem internationalen De-facto-Standard entwickelt.

Das technische Betriebskonzept umfasst vor allem Beschreibungen zu folgenden Themen:

- Organisation (Benennung der Mitarbeiter und deren Aufgaben)
- Prozesse (Arbeitsanweisungen),
- Schnittstellen (organisatorisch und technisch),
- Qualitätsmanagement.

Im Folgenden werden die verschiedenen erforderlichen Service Managements beschrieben, mit denen die geregelte Betriebsführung sichergestellt werden kann.

11.2. Service-Desk / Störungsmeldung und –verfolgung

Das Service-Desk bildet den zentralen Eingang der citeq für alle Störungsmeldungen der Schulen („Single Point of Contact“, SPOC) und ist zuständig für alle Anrufe, Fragen, Beschwerden, Ereignisse („Incidents“) und Anmerkungen die sich auf den Betrieb der IT-Infrastruktur beziehen.

Ziel des Service-Desk ist die schnellstmögliche Lösung aller von den Schulen gemeldeten Störfälle. Ziel des Service-Desk ist es auch, bereits im Rahmen der Störungsannahme möglichst viele Störungen direkt zu beheben. Ansonsten dient das Service-Desk selbst nicht der Behebung der Störungen, sondern der Weiterleitung an die nachgelagerten Funktionsgruppen (Operational Management, Problemmanagement) und somit der Steuerung des Entstörungsvorganges.

Die erste Klärung von einfachen Störungen obliegt dem First-Level-Support (IT-Koordination in der Schule). Alle weiteren Störungen meldet die IT-Koordination an das Service-Desk der citeq.

Störungen sollen grundsätzlich nur auf einem von zwei Wegen zum Service-Desk kommen:

- telefonisch über die citeq-Hotline,
- elektronisch über das web-basierte Meldungssystem Service-Desk.

Weitere Medien wie e-Mail bzw. Fax zur Störungsmeldung bzw. -annahme kommen nur im Einzelfall nach vorheriger Absprache zum Einsatz.

Die citeq bietet zu den im Intranet der Stadt Münster und MEP-net (siehe unter I. 3.2. "MEP-net") ausgewiesenen Servicezeiten den Schulen die Möglichkeit, jede Störung per Telefon an die zentrale citeq-Hotline zu melden.

Diese ergreift zur Beseitigung des Fehlerzustandes folgende Maßnahmen:

- direkte Hinweise zur Fehlerbeseitigung noch während der telefonischen Störungsannahme,
- Entstörungsversuch durch Fernbedienen (Remote Control) der gestörten Geräte in Absprache mit dem Meldenden,
- Aufzeigen einer möglichen temporären Fehlerumgehung („WorkAround“) bis zur Entstörung,
- Aufnahme eines Service-Desk-Auftrages im Service-Desk-System und umgehende Weiterleitung an die zuständigen Netz- bzw. Systembetreuer bzw. die Technische Servicestelle der citeq.

Das Melden von Störungen über das Service-Desk-System ist zu jeder Zeit möglich. Das Service-Desk ist sowohl aus dem MEP-Netz wie auch aus dem Internet heraus erreichbar.

Das Service-Desk-System ist ein Programmsystem zur Störungsaufnahme und -verfolgung, welches auch im Verwaltungsumfeld der Stadt eingesetzt wird. Als Bedienoberfläche verwendet Service-Desk-System den auf allen Rechnern vorhandenen Standard-Webbrowser. Störungen können von den berechtigten Benutzern (in der Regel sind dies die IT-Koordinatoren) in das System eingegeben werden. Innerhalb der vereinbarten Servicezeiten werden die Störungsmeldungen von der citeq-Hotline an die zuständigen nachgelagerten Fachleute innerhalb der citeq weitergeleitet (sog. „Dispatcher-Funktion“). Der Meldende kann sich über die Web-Oberfläche jederzeit selbst über den aktuellen Bearbeitungsstand der Störungsmeldung informieren.

Innerhalb des Service-Desk kann der Meldende eine Priorisierung der Dringlichkeit vornehmen.

Es wird unterschieden nach:

- sehr kritischer Fehler: Gesamtausfall eines Systems mit Auswirkungen für die gesamte Schule
- kritischer Fehler: Teilausfall eines Systems mit Auswirkungen auf einen größeren Teil der Schul-IT (z.B. Informatikraum)
- einfacher Fehler: Ausfall eines Einzelsystems mit Auswirkungen einzelne Arbeitsplätze
- unkritischer Fehler: Ausfall einer Funktion oder eines Systems ohne gravierende Auswirkungen

Eine Priorisierung ist auch im Service-Desk-System möglich, wo zu den jeweiligen Störungsprioritäten unterschiedliche Eskalationszeiten zur automatischen Eskalation von Störungen (auch an die citeq-Leitungsebene) hinterlegt sind.

Die Rahmenbedingungen des Service-Desk (Annahme-, Reaktions-, Verweil- und Eskalationszeiten) entsprechen den Bedingungen, wie sie für die Stadtverwaltung Münster festgelegt werden.

11.3. Problemmanagement

Ziel des Problemmanagements ist eine schnelle und effiziente Diagnose und Lösung aller auftretenden Probleme innerhalb der IT-Infrastruktur. Es ist vor allem für diejenigen Probleme innerhalb der IT-Infrastruktur zuständig, die nicht bereits durch das Service-Desk behoben werden können.

Das Problemmanagement ist zuständig für:

- neue Problemereignisse („Incidents“), wobei die Ursache des Fehlerzustandes nicht bekannt ist,
- bekannte Fehler („Known Errors“), bei denen die Ursache des Fehlerzustandes offensichtlich bzw. aufgrund erfolgreicher Ursachenforschung bereits identifiziert ist.

Das Problemmanagement dient:

- der Erhöhung der Produktivität,
- der reaktiven Verfolgung von Fehlerursachen ,
- der Minimierung der Fehlerwahrscheinlichkeit durch präventive Maßnahmen.

Die Wahrnehmung des Problemmanagements obliegt als Eskalationsstufe dem Second-Level-Support in der citeq.

11.4. Konfigurations- und Änderungsmanagement

Aufgaben des Konfigurationsmanagements sind vor allem:

- Beschreibung und eindeutige Identifizierung aller IT-Komponenten,
- Kontrolle und Freigabe der Komponenten für den laufenden Betrieb,
- Informationssammlung zu allen technischen und wirtschaftlichen Aspekten der Komponenten,
- ständige Überprüfung und Abgleichung der Konfigurationsdaten mit den aktuellen Gegebenheiten.

-

Das Konfigurationsmanagement verwaltet alle im Rahmen dieses Konzeptes in den Schulen und bei der citeq eingesetzten Hard- und Softwarekomponenten. Hierzu wird

eine Inventarisierung durch Verwendung eines geeigneten Verwaltungswerkzeuges (Inventar-Datenbank, CMDB) durchgeführt. Die Inventarisierung obliegt der citeq als zentraler Schnittstelle bei Beschaffung und Betrieb der Komponenten.

Änderungen ergeben sich im Laufe des Betriebes von Geräten zwangsläufig. Das Änderungsmanagement der citeq plant und steuert die vorgeschlagenen und genehmigten Änderungen. Es stellt sicher, dass diese Änderungen gut vorbereitet, in kurzer Zeit und kontrolliert ablaufen.

Vorschlag und Genehmigung von Änderungen beim Hard- und Softwareeinsatz erfolgen durch die jeweils zuständigen Gremien.

11.5. Testcenter

Die citeq betreibt ein Testcenter zur Überprüfung der vorgeschlagenen Änderungen der IT-Infrastruktur auf ihre technische Umsetzbarkeit. Innerhalb dieses Testcenters wird außerdem die Bearbeitung komplexer Störfälle unter Laborbedingungen durchgeführt.

Nur durch die Einrichtung eines Testcenters kann sichergestellt werden, dass geplante Änderungen mit möglichst geringen Reibungsverlusten in den laufenden Betrieb integriert werden können. Störungen durch nicht freigegebene und daher möglicherweise inkompatible Hard- und Software werden dadurch weitestgehend vermieden.

Das Testcenter ist temporär besetzt durch Mitarbeiter aus allen Fachbereichen der citeq.

11.6. Qualitätsmanagement

Neben den Maßnahmen zur Beseitigung einzelner Störungen ist ein regelmäßiger Informationsaustausch zur Sicherung bzw. Verbesserung des erreichten Qualitätsstandards erforderlich.

Die Lenkungsgruppe kommt vierteljährlich zusammen, um grundlegende Änderungen in der Bereitstellung von IT-Infrastruktur und die Abläufe der Zusammenarbeit zu besprechen.

Die in diesen Treffen vereinbarten Maßnahmen stellen sicher, dass sich die IT-Infrastruktur auch über einen längeren Zeitraum optimal an den Bedarfen der Schulen ausrichten lässt. Hierzu werden bei Bedarf Evaluationen durchgeführt.

11.7. Operations Management

Die Wahrnehmung dieser Aufgabe umfasst vor allem die Bereiche der täglichen, regelmäßigen Administration und Betreuung der Client-/Server-Infrastruktur und der Netzwerkinfrastruktur und stellt sicher, dass die Verfügbarkeit und der reibungslose Betrieb dieser Infrastruktur gewährleistet ist.

Dies wird u. a. erreicht durch programmgesteuerte Überwachung aller beteiligten Komponenten, sowie durch geeignete Maßnahmen zur Datensicherung und -rücksicherung.

11.7.1. Überwachung der IT-Infrastruktur

Die citeq stellt sicher, dass während der vereinbarten Servicezeiten bei Eintreten von definierten Fehlerzuständen eine automatische Alarmierung des Second-Level-Supports erfolgt.

Solche Fehlerzustände sind beispielsweise folgende Ausfälle:

- Leitungsanbindungen an die citeq (WAN),
- aktive Netzkomponenten im Gebäudenetz der Schule (LAN),
- zentrale und dezentrale Server,
- zentrale Dienste.

Das Eintreten ist grundsätzlich als kritischer Zustand einzuschätzen und wird daher mit höchster Priorität in das Service-Desk eingestellt, so dass mit der Entstörung umgehend begonnen werden kann.

Liegt die Störungsbeseitigung nicht bei der citeq (z.B. bei Ausfall einer von einem Provider angemieteten Leitungsverbindung), wird die Eskalation an den externen Dienstleister gemäß dem mit ihm abgeschlossenen Service Level Agreements (SLAs) vorgenommen. Die citeq verfolgt den Entstörungsvorgang kontinuierlich und informiert die Schulen zeitnah.

11.7.2. Störungsbehebung

Die Störungsbehebung wird gesteuert durch das Service-Desk.

Für alle Störfälle gilt:

- Bei Hardware-Störungen wird die citeq entsprechend der Gewährleistungs- und Garantieansprüche die Fehlerbehebung durch den jeweiligen Lieferanten veranlassen. Soweit wirtschaftlich vertretbar, wird die Vorhaltung von Ersatzhardware angestrebt, um eine zeitnahe Entstörung vornehmen zu können.
- Nach Ablauf der Gewährleistungs- und Garantiezeiten ist die Behebung von Hardwarestörungen unter technischen und wirtschaftlichen Gesichtspunkten abzuwägen und durchzuführen.
- Bei Software-Problemen wird die Störungsbeseitigung zunächst mit den jeweils geeigneten Programmen zur Ferndiagnose vorgenommen.
- Störungen zentraler Funktionen werden ihrer Bedeutung entsprechend in der Regel mit der höchstmöglichen Priorität ins Service-Desk eingestellt.
- Reaktions-, Verweil- und Entstörungszeiten von anderen Dienstleistern und Lieferanten sind nicht in jedem Fall vorhersehbar. Soweit wirtschaftlich vertretbar werden daher mit ihnen Wartungsverträge abgeschlossen.

11.7.3. Aufgaben der IT-Koordination

Die Sicherstellung eines geordneten IT-Einsatzes und die zeitnahe Behebung von Störungen kann nur im Zusammenspiel zwischen der citeq und einer vor Ort in den Schulen zu installierenden IT-Koordination gewährleistet werden. Auch unter Ausnutzung aller Möglichkeiten einer Fernwartung können bestimmte Tätigkeiten nur vor Ort durch entsprechend qualifiziertes Personal der Schule durchgeführt werden.

Aufgaben der IT-Koordination sind vor allem:

- Beseitigung kleinerer Störungen, ggf. nach Einweisung durch Fachpersonal der citeq (z.B. Beseitigung von Papierstaus bei Druckern),
- Qualifizierte Schnittstelle zum Service-Desk der citeq,
- Aufnahme von Störungsmeldungen
- Fehleranalyse, -beschreibung, -meldung
- Verfolgung des Service-Desk-Auftrages

- Durchführung einfacher Wartungsarbeiten (z.B. Patronenwechsel bei Druckern),
- Pflege des IT-Bestandsmoduls im Falle von selbst durchgeführten Veränderungen des IT-Standortes,
- Teilnahme an Qualifizierungsmaßnahmen,
- Teilnahme an regelmäßigen Arbeitskreisen zum Erfahrungsaustausch.

Für die Störungsbehebung durch die IT-Koordination gilt die so genannte „5-Minuten-Regel“:

Die IT-Koordination sollte sich nicht länger als fünf Minuten an der Lösung eines Problems versuchen. Danach ist der Second-Level-Service einzuschalten.

Bezüglich weiterer Möglichkeiten zur Durchführung administrativer Tätigkeiten durch die IT-Koordinationen siehe unter 9.8. "Rechte der IT-Koordinationen".

11.7.4. Störungen der Leitungsanbindung (WAN)

Störungen der Leitungsanbindung (WAN) können nur in Verbindung mit dem gewählten Telekommunikationsprovider behoben werden. Die notwendigen Vereinbarungen über Reaktionszeiten bzw. zugesicherte Entstörungszeiten werden mit dem Provider getroffen.

11.7.5. Störungen des Inhouse-Netzes (LAN)

Die im Inhouse-Netz verwendeten aktiven Netzkomponenten (Switches) sind fernadministrierbar und können daher in der Regel ohne Zeitverzug von der citeq überprüft und ggf. entstört werden. Zur Minimierung der Ausfallzeiten durch schwerwiegende Hardware-Fehler werden Ersatzgeräte durch die citeq vorgehalten.

11.7.6. Störungen dezentraler und zentraler Server

Bei Hardware-Störungen wird die citeq entsprechend der Garantie- und Gewährleistungsansprüche die Fehlerbehebung durch den jeweiligen Lieferanten veranlassen.

Die Vorhaltung kompletter Ersatz-Serverhardware für jeden einzelnen Schulstandort ist aus wirtschaftlichen Gründen nicht zu vertreten. Für Verwaltung- und Pädagogiknetze hält die citeq jeweils einen Ersatzserver lagerseitig vor.

11.7.7. Störungen zentraler Dienste

Die Behebung von Fehlerzuständen bei zentralen Diensten wie z.B. DNS, DHCP, Proxy wird grundsätzlich mit höchster Priorität ins Service-Desk eingestellt und bearbeitet.

11.7.8. Störungen von Client-Rechnern

Software-Probleme auf Client-Rechnern sind durch die Qualitätskontrolle im Vorfeld der Installation (Stichwort: Testcenter) weitestgehend ausgeschlossen und durch Verwendung der PC-Wächtersoftware sowie die zentrale Softwareverteilung wird die Wahrscheinlichkeit von Fehlern nochmals verringert.

Auftretende Störungen werden über das Service-Desk bearbeitet.

11.7.9. Wartung der Beamer

Mit der Erstausstattung der Schulen wurden rd. 200 Beamer in die Schulen ausgeliefert. Die Beamer sind für den mobilen Einsatz vorgesehen oder wurden an vorinstallierten Deckenbefestigungen angebracht.

Die Beamerlampen sind als Verbrauchsmaterial anzusehen. Die Beschaffung und Finanzierung liegt in der Verantwortung der Schulen. Die Beschaffung kann über den Rahmenvertrag der citeq abgewickelt werden.

Für die Wartung der Beamer wurde bislang keine verbindliche Regelung festgelegt. Die Einführung eines entsprechenden Verfahrens ist jedoch notwendig, um eindeutige Zuständigkeiten festzulegen und Störungen bzw. Beschädigungen am Gerät, die durch mangelnde Wartung verursacht wurden (z.B. Staubfilterreinigung), zu vermeiden. Eine Verlagerung der Aufgabe auf die Schulen kommt nicht in Betracht. Hier stehen keine ausreichenden Personalkapazitäten zur Verfügung. Auch darf das technische Grundverständnis nicht an jeder Schule vorausgesetzt werden. Die citeq prüft zurzeit die Möglichkeiten zur Durchführung einer regelmäßigen Wartung durch eigenes Personal oder der

Vergabe an einen externen Dienstleister. Die Kosten, die für hierfür entstehen werden, werden auf die Preise der Beamer angerechnet und werden auf diesem Wege über die MEP-Budgets der Schulen refinanziert.

Glossar

In diesem Glossar sollen einige der technischen Begriffe für den Leser dieser Fortschreibung erläutert werden.

Authentifizierung

Authentifizierung (v. griech. authentikos für „Urheber“, „Anführer“) ist der Vorgang der Überprüfung (Verifikation) der behaupteten Identität eines Gegenübers, beispielsweise einer Person oder eines Computersystems in einem Dialog. Authentisierung hingegen ist der Vorgang des Nachweises der eigenen Identität. Im Englischen wird zwischen den beiden Begriffen nicht unterschieden: Das Wort authentication steht für beide Vorgänge. Dementsprechend werden die beiden Ausdrücke im Deutschen oft (ungenau) synonym verwendet.

CRT-Monitor

Ein Kathodenstrahlröhren-Bildschirm ist ein Bildschirm, der auf der Kathodenstrahlröhre von Ferdinand Braun basiert. Häufig wird er auch als Kathodenstrahl-, Röhren- oder CRT- (Abk. für engl. Cathode Ray Tube) Bildschirm bezeichnet. Er wird in so unterschiedlichen Geräten wie Oszilloskopen, Fernsehern und PC-Bildschirmen eingesetzt, neuerdings aber immer mehr durch Flachbildschirme (Plasmabildschirm, Flüssigkristallbildschirm) verdrängt.

Domain Name Service (DNS)

Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Seine Hauptaufgabe ist die Umsetzung von „Internetadressen“ in die zugehörige IP-Adresse.

Dynamic Host Control Protocol (DHCP)

Das Dynamic Host Configuration Protocol (DHCP) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter an Computern in einem Netzwerk (z. B. Internet oder LAN).

eDirectory

eDirectory ist ein Verzeichnisdienst der Firma Novell und die Weiterentwicklung der Novell Directory Services. Mittlerweile ist dieses Programm LDAP v3 kompatibel und unterstützt XML sowie das Webservice-Protokoll SOAP. Dieser Dienst ist plattformübergreifend und kann nativ unter Netware, Windows, Linux, Solaris u. v. m. laufen.

Fernwartung

Die Fernwartung (Remote Control) von Computern gewinnt beim Support von Hard- und Software zunehmend an Bedeutung. Durch die immer stärkere Vernetzung der Computer über das Internet, den Aufbau von firmeninternen Intranets und herkömmliche Telekommunikationswege (ISDN, Telefon) erweitern sich die Möglichkeiten der direkten Unterstützung im Support. Nicht zuletzt wegen der Einsparmöglichkeiten bei Reisekosten und die bessere Ressourcennutzung (Personal und Technik) werden Produkte der Fernwartung zur Kostensenkung in Unternehmen genutzt.

galvanische Trennung

Ein galvanisch getrennter Informationsaustausch ist durch nicht-elektrische Übertragungswege mit entsprechenden Wandlern möglich. In unserem Fall sprechen wir von 2 getrennten Netzen.

Intranet

Ein Intranet ist ein Rechnernetzwerk, das auf den gleichen Techniken wie das Internet (TCP/IP, HTTP) basiert, jedoch nur von einer festgelegten Gruppe von Mitgliedern einer Organisation genutzt werden soll.

IP-Adresse (Internet Protocol Address)

Das Internet Protocol (IP) ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll. Es ist eine (bzw. die) Implementierung der Internet-Schicht des TCP/IP-Modells bzw. der Vermittlungsschicht (Network Layer) des OSI-Modells.

kaskadiert

Bei einer Kaskadenschaltung wird eine elektrische Baugruppe mehrfach hintereinander angeordnet (kaskadiert), um eine höhere Wirkung zu erzielen, beispielsweise mehrere Switches zum Erreichen einer höheren Portanzahl.

LAN (Local Area Network)

Ein Lokales Netz (engl. local area network, daher auch im Deutschen oft abgekürzt LAN) ist ein Rechnernetz, dessen Größe jene von PANS übertrifft, das aber kleiner ist als MANs, WANs und GANs.

Netzmaske

Die Netzmaske oder Netzwerkmaske, teils noch als Subnetzmaske bezeichnet, ist eine Bitmaske, die eine IP-Adresse in einen Netzwerk- und einen Geräte- bzw. Hostteil trennt. Sie wird in IP-Netzwerken verwendet, um Routingentscheidungen zu treffen.

PDA (Personal Digital Assitants)

Ein Personal Digital Assistant (PDA) (englisch für persönlicher digitaler Assistent) ist ein kleiner tragbarer Computer mit eigener Stromversorgung, der neben vielen anderen Programmen hauptsächlich für die persönliche Kalender-, Adress- und Aufgabenverwaltung benutzt wird.

Peripheriegeräte

Das Peripheriegerät ist eine Komponente oder ein Gerät, das sich außerhalb der Zentraleinheit eines Computers befindet. (kurz: Zubehör) Vereinfacht kann von im Computer verbauten (internen) und mit diesem durch ein Kabel (oder auch durch Infrarot- oder Funktechnik) verbunden (externen) Peripheriegeräten unterschieden werden. Peripheriegeräte dienen der Ein- und Ausgabe von Daten oder Befehlen in die Zentraleinheit. Sie erbringen eine sog. "Dienstleistung" für den Benutzer, diese kann entweder "sichtbar" (z.B. Papier-Ausdruck) oder unsichtbar (z.B. Postskript-Umwandlung im Drucker) sein.

Quotings

Der aus dem Englischen stammende Begriff Quoting wird im Computerbereich häufig verwendet, bezeichnet aber je nach Kontext unterschiedliche Dinge:

- Bei E-Mails bezeichnet Quoting das optisch eingerückte Zitat einer beantworteten E-Mail.
- Auf der Kommandozeile von z. B. einer Unix-Shell, aber auch bei z. B. regulären Ausdrücke bezeichnet Quoting das Entfernen einer Sonderbedeutung eines Zeichens durch Umklammern mit Anführungszeichen oder Davorsetzen eines Sonderzeichens (z. B. Backslash). Letzteres wird auch Escaping genannt.

RAID

Ein RAID-System (ursprünglich redundant array of inexpensive disks, heute redundant array of independent disks) dient zur Organisation mehrerer physischer Festplatten eines Computers zu einem logischen Laufwerk, das eine größere Speicherkapazität, eine höhere Datensicherheit bei Ausfall einzelner Festplatten und/oder einen größeren Datendurchsatz erlaubt als eine physische Platte. Während die meisten in Computern verwendeten Techniken und Anwendungen darauf abzielen, Redundanzen (das Vorkommen doppelter Daten) zu vermeiden, werden bei RAID-Systemen redundante Informationen gezielt erzeugt, damit beim Ausfall einzelner Komponenten das RAID als Ganzes seine Funktionalität behält.

Redaktionssysteme

Redaktionssystem ist ein häufig benutzter Begriff für Content-Management-Systeme. Wesentliches Merkmal aller Redaktionssysteme ist die Trennung von Inhalten (Content) und Design (Layout).

Remote Administration

Remote Services sind Systeme zur Fehlerbehebung, die ohne Eingriff eines Benutzers am betroffenen Rechner auskommen, zum Beispiel über automatische Software-Updates. Grundlage ist die Auswertung von Laufdaten des betroffenen Rechners in Echtzeit.

Router

Ein Router ist eine Netzwerkkomponente, die mehrere Rechnernetze koppelt; das bedeutet, bei ihm eintreffende Netzwerk-Pakete eines Protokolls werden auf Basis von Layer-3-Informationen analysiert und zum vorgesehenen Zielnetz (auch Ziel-Subnetze) weitergeleitet oder geroutet. Im Deutschen wird ein Router hin und wieder auch als „Wegewähler“ bezeichnet. Der Begriff konnte sich allerdings nicht durchsetzen.

Simple Network Management Protocol (SNMP)

Das Simple Network Management Protocol (englisch für „einfaches Netzwerkverwaltungsprotokoll“, kurz SNMP), ist ein Netzwerkprotokoll, das von der IETF entwickelt wurde, um Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern zu können. Das Protokoll regelt hierbei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. Hierzu beschreibt SNMP den Aufbau der Datenpakete, die gesendet werden können, und den Kommunikationsablauf. SNMP wurde dabei so ausgelegt, dass jedes netzwerkfähige Gerät mit in die Überwachung aufgenommen werden kann. Zu den Aufgaben des Netzwerkmanagement, die mit SNMP möglich sind, zählen:

- Überwachung von Netzwerkkomponenten.
- Fernsteuerung und Fernkonfiguration von Netzwerkkomponenten.
- Fehlererkennung und Fehlerbenachrichtigung.

Durch seine Einfachheit, Modularität und Vielseitigkeit hat sich SNMP zum Standard entwickelt, der von den meisten Managementprogrammen als auch Endgeräten unterstützt wird. So ist SNMP z. B. nicht auf das Netzwerkprotokoll IP als Transport angewiesen. Es gibt Implementierungen, die über IPX (Novell, NetWare) oder AppleTalk (Apple, MacOS) angesprochen werden können.

SPAM

Als Spam oder Junk (englisch für: „Abfall“ oder „Plunder“) werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, welche dem Empfänger unverlangt zugestellt werden und massenhaft versandt wurden oder werbenden

Inhalt haben. Dieser Vorgang wird Spamming oder Spammen genannt, der Verursacher Spammer.

Standard-Gateway

Ein Gateway (englisch gateway, deutsch auch Protokollumsetzer) erlaubt es Netzwerken, die auf völlig unterschiedlichen Protokollen basieren, miteinander zu kommunizieren.

Standleitung

Eine Standleitung ist eine permanente (stehende) Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetzwerk. Im Gegensatz zu einer Wählleitung steht der gesamte Übertragungsweg immer zur Verfügung.

Streaming

Unter Streaming (engl. streaming „Strömen, Fließen“) versteht man die kontinuierliche Übertragung von Daten, das heißt die Übertragung von Datenströmen.

Switch

Ein Switch (engl. Schalter, auch Weiche), ist eine Netzwerk-Komponente zur Verbindung mehrerer Computer bzw. Netz-Segmente in einem lokalen Netz (LAN). Da Switches den Netzwerkverkehr analysieren und logische Entscheidungen treffen, werden sie auch als intelligente Hubs bezeichnet. Die Funktionsweise eines Switches ist der einer Bridge sehr ähnlich, daher wurde anfangs auch der Begriff Multi-Port-Bridge benutzt.

Telekommunikationsprovider

Ein Provider wird ein Anbieter von Telekommunikationsdiensten bezeichnet. Dabei kann es sich sowohl um einfache als auch um höherwertige Dienste handeln. Besitzt der Provider ein eigenes Kommunikationsnetz, wird er als Telekommunikationsnetzbetreiber bezeichnet.

Terminalserver

Ein Terminalserver ist ein Computer, der mehrere Terminals (PCs, Bildschirme bzw. Desktops oder Kommandozeilen) emuliert bzw. die Software, die besagte Emulation ermöglicht. Auf jedem emulierten Terminal können, wie auf einem normalen PC, mehrere verschiedene Programme laufen. Diese emulierten Terminals werden auf den Bildschirmen von meist entfernten (remote) PCs oder Thin Clients dargestellt. Für Terminalserver, die sich nur auf die Emulation von Kommandozeilen spezialisieren, ist inzwischen der Begriff Server-Console gebräuchlich.

USV

Eine unterbrechungsfreie Stromversorgung (USV), englisch Uninterruptible Power Supply (UPS), wird von Kunden der Energieversorgungsunternehmen eingesetzt, um bei Störungen in deren Stromnetz die Stromversorgung sicherzustellen. Entgegen der Bezeichnung kann die Stromversorgung bei einfachen Ausführungen für wenige Millisekunden unterbrochen sein.

WAN

Ein Weitverkehrsnetz (engl. wide area network, daher auch im Deutschen oft abgekürzt WAN), auch Weitbereichsnetz, ist ein Rechnernetz, das sich im Gegensatz zu einem LAN oder MAN über einen sehr großen geografischen Bereich erstreckt.

Webspace (Hosting)

Webspace, auch Webhosting oder auch Nethosting genannt, beschreibt einen Speicherplatz für Dateien auf einem Server, auf den über das Internet dauerhaft zugegriffen werden kann. Webspace wird von Internetdiensteanbietern angeboten, um Kunden zu ermöglichen, Internetpräsenzen oder Teile solcher zu speichern und zu veröffentlichen.

Workstation

Mit Workstation bzw. Arbeitsplatzsystem bezeichnet man einen – im Vergleich zum normalen IBM-kompatiblen PC – besonders leistungsfähigen Arbeitsplatzrechner zur Benutzung durch eine oder mehrere Personen. Typischerweise werden Workstations für anspruchsvolle technisch-wissenschaftliche Anwendungen eingesetzt, im Gegensatz zu dem Bereich der Büroanwendungen, den sich der IBM kompatible PC eroberte. Übli-

cherweise erbringen Workstations im Bereich Grafikdarstellung, Rechenleistung, Speicherplatz und/oder Multitasking überdurchschnittliche Ergebnisse, oft können zusätzliche Terminals verwendet werden.