

Medienentwicklungsplan der Stadt Münster

Stand: Januar 2012

: 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

Amt für Schule und Weiterbildung
citeq

Januar 2012

I.	Neue Medien in Schulen - aktueller Stand	1
1.	Allgemeine Anforderungen und Vorgaben	1
1.1.	Rahmenbedingungen und Grundsatzentscheidungen	1
1.2.	Änderungen	2
1.3.	Aktueller Stand 2011	4
1.3.1.	Schulen und Schüler im Schuljahr 2010/2011	4
1.3.2.	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.	Funktionskontrolle.....	9
2.2.6.	Abnahme	9
2.2.7.	Verwendung der Althardware	10
2.3.	Diebstähle	10
2.4.	Software.....	11
2.4.1.	Softwareausstattung der Schulverwaltungen	11
2.4.2.	Software für den unterrichtlichen Bereich	11
3.	Kundenberatung	13
3.1.	Allgemeines	13
3.2.	MEP-net.....	14
3.3.	Fortbildungen/Workshops für IT-Kontaktlehrer	15
II.	Ausstattungs- und Betriebskonzept	16
1.	Technische Grundsatzentscheidungen	16
1.1.	Allgemeines	16
1.2.	Servertechnologie.....	16
1.3.	Clients.....	17
1.4.	Drucker	17
1.5.	Monitore.....	17
1.6.	Einbindung eigener Systeme.....	17
2.	Beschaffung	18
3.	Katalog der Standardkomponenten	18
4.	Datenschutz und Datensicherheit	19

5. Protokollierung von Nutzerdaten	21
6. Inventarisierung der Hardware	22
7. Technisches Ausstattungskonzept.....	23
7.1. Netzwerk.....	23
7.2. Inhouse-Verkabelung / Netzkomponenten - LAN (Local Area Network).....	23
7.3. WLAN (Wireless Local Area Network)	27
7.4. Anbindung der Schulen an die citeq - WAN (WideAreaNetwork)	28
7.5. Nutzung der Telekom@school-Anschlüsse für das Internet	29
7.6. Streaming	30
7.7. Netzwerkmanagement.....	30
7.8. Anschluss privater Rechner an das Internet	31
8. Server	33
8.1. Hardwareausstattung	33
8.2. Virtualisierung von Servern	35
8.3. Betriebssystem und Version	36
8.4. Serverdienste.....	37
8.4.1. Fileservices.....	38
8.4.2. Printservices	38
8.4.3. Dynamic Host Control Protocol (DHCP).....	38
8.4.4. Domain Name Service (DNS).....	39
8.4.5. Mailing	39
8.4.6. Spam	40
8.4.7. Intranet in der Schule	41
8.4.8. Virenschutz	41
8.4.9. CD -Manager	41
8.4.10. Internetzugang mittels Proxy-Services	42
8.5. Internetfilter SquidGuard	43
8.5.1. Zentral administrierter SquidGuard	43
8.5.2. Von der Schule zu administrierender SquidGuard	43
8.6. Arbeiten bei Ausfall der Netzanbindung	44
8.7. Benutzer-/Gruppenverwaltung / eDirectory	44
8.8. Rechte der IT-Kontaktlehrer	46
8.9. Datenhaltung	46
8.10. Zugriff auf Daten/Mails von Außen	48
8.11. Kommunikationsplattform	49
8.12. Softwarerepository.....	49
8.13. Datensicherung Server.....	50
8.14. Remote Administration	51
8.15. Zentrale Serverbereitstellung	51
9. Clients	52
9.1. Hardwareausstattung	52

9.2.	Wächterschutz	52
9.3.	Betriebssystem	53
9.4.	Clientsoftware	54
9.4.1.	Standardsoftware.....	54
9.4.2.	Stand-alone-Betrieb.....	55
9.4.3.	Servergespeicherte Profile (Roaming-Profiles)	56
9.4.4.	Verbindliche Profile (Mandatory-Profiles)	56
9.4.5.	Virenschutz und Updates	56
9.5.	Vorbereitung der Clients und Softwareverteilung.....	57
9.6.	Plattform für die Aktualisierung von Standard-Software (PASS)	58
9.7.	Info-Displays	59
10.	Technisches Betriebskonzept	60
10.1.	Begriffsdefinition	60
10.2.	Service-Desk / Störungsmeldung und –verfolgung	60
10.3.	Problemmanagement	63
10.4.	Konfigurations- und Änderungsmanagement.....	63
10.5.	Testcenter	64
10.6.	Qualitätsmanagement	64
10.7.	Operationsmanagement.....	65
10.7.1.	Überwachung der IT-Infrastruktur.....	65
10.7.2.	Störungsbehebung	66
10.7.3.	Aufgaben der IT-Kontaktlehrer	66
10.7.4.	Störungen der Leitungsanbindung (WAN)	67
10.7.5.	Störungen des Inhouse-Netzes (LAN).....	67
10.7.6.	Störungen dezentraler und zentraler Server	68
10.7.7.	Störungen zentraler Dienste.....	68
10.7.8.	Störungen von Client-Rechnern	68
Glossar		69

I. Neue Medien in Schulen - aktueller Stand

1. Allgemeine Anforderungen und Vorgaben

1.1. Rahmenbedingungen und Grundsatzentscheidungen

Mit der Verabschiedung des Medienentwicklungsplanes wurden die notwendigen Strukturen für ein neues Lernen und Lehren an den städtischen 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.

Wesentlicher Bestandteil eines ganzheitlichen und zukunftssicheren Konzeptes für die Wartung der IT-Infrastruktur in den Schulen der Stadt Münster ist die Festlegung und Einhaltung der Rahmenbedingungen. Die Erfahrungen der vergangenen Jahre bestätigen den Kernpunkt:

S t a n d a r d i s i e r u n g

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 zur Verfügung stehenden 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 sind breitbandig (über MPLS oder Lichtwelle) an die citeq und an das Internet angebunden.
- Soweit technisch und wirtschaftlich möglich, erfolgt die Anbindung an die citeq über eigene Lichtwellenleitungen (LWL). Ansonsten wird die Anbindung über MPLS realisiert.
- Die Reinvestition der in den Schulen eingesetzten Rechner (einschließlich Notebooks) und Monitore erfolgt regelmäßig nach den festgelegten Standzeiten (zurzeit 4,5 Jahre).
- Die Reinvestition der in den Schulen eingesetzten Netzwerkdrucker und Beamer erfolgt regelmäßig nach den festgelegten Standzeiten (zurzeit 8 bis 10 Jahre).

- Es werden ausschließlich TFT-Monitore eingesetzt.
- Andere Hardware wird erst dann ausgetauscht, wenn sie aus technischen oder wirtschaftlichen Gründen nicht mehr eingesetzt werden kann.
- Es werden nur noch Netzwerkdrucker unterstützt. Der Austausch noch vorhandener lokaler Drucker erfolgt im Rahmen der Reinvestition bzw. bei Defekt.
- Die Endgeräte- und Softwareausstattung der Schulen erfolgt aus einem Warenkatalog, der der ständigen Fortschreibung unterliegt.
- Installationen im pädagogischen Netz erfolgen grundsätzlich durch die citeq (Ausnahmen siehe unter 9.6 "Plattform für die Aktualisierung von Standard-Software (PASS)").
- Schuleigene Drucker und Kopierer, die aktuell auch bei der Stadtverwaltung eingesetzt werden, können in das Schulnetz integriert werden.
- Sonstige schuleigene Hardware wird nicht in das Schulnetz integriert.
- Die Schulen erhalten Zugriff auf das IT-Bestandsmodul der citeq und pflegen darüber selbst durchgeführte Bestandsveränderungen.

Im Rahmen der Fortschreibung werden die aktuellen Standards daraufhin überprüft, ob sie sich bewährt haben. Die Wünsche der Schulen werden, sofern wirtschaftlich und technisch sinnvoll und möglich, ebenfalls berücksichtigt. Natürlich werden auch die aktuellen Techniktrends aufmerksam verfolgt und bewertet und nach Möglichkeit im Rahmen des MEP berücksichtigt.

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.

1.2. Änderungen

Die wesentlichen Änderungen zur letzten Fortschreibung aus 2007 sind hier im Überblick aufgeführt. Eine detaillierte Erläuterung und Begründung wird im Ausstattungs- und Betriebskonzept vorgenommen.

- Anbindung von 27 Schulen über Lichtwellenleitungen
- Erhöhung der Bandbreite in weiterführenden Schulen und Schulzentren, die nicht über Lichtwellenleitungen angebunden sind
- Verbesserung der Leitungsqualität in allen Schulen

- Festlegung eines einheitlichen Monitorstandards
- Regelmäßige Reinvestition von Beamern und Druckern
- Mehr Speicherplatz in der Verwaltung
- Mehr (ungesicherter) Speicherplatz in der Pädagogik
- Erweiterung der Rechte für IT-Koordinatoren
- WLAN (Wireless Local Area Network) in der Pädagogik
- Virtualisierung von Servern
- Konsolidierung von Servern
- Schulindividuelle Sperrung von Internetseiten
- Plattform für die Aktualisierung von Standard-Software (PASS)
- Info-Displays für die Darstellung von z. B. Vertretungsplänen
- Folgende Punkte werden im Rahmen von Projekten untersucht:
 - Internetnutzung mit privaten PC über schuleigene Leitungen
 - Nutzung der Telekom@school-Anschlüsse für das Internet (Pädagogik)
 - Datenzugriff auf das pädagogische Netz von Außerhalb
 - Zugriff auf pädagogische Mails von Außerhalb
 - Zentrale Serverbereitstellung in der Pädagogik
- Bereitstellung einer Kommunikationsplattform

1.3. Aktueller Stand 2011

1.3.1. Schulen und Schüler im Schuljahr 2011/2012

In Münster gab es im abgelaufenen Schuljahr 2010/2011 82 städtische Schulen (ohne Berufskollegs) mit rund 27.000 Schülerinnen und Schülern. Durch die Auflösung der Wartburg-Hauptschule zum 31.07.2011 hat sich die Zahl der Schulen um eins verringert. Die Zahl der Schülerinnen und Schüler hat um rund 500 abgenommen. Die Zahl der Klassen reduzierte sich um 43. 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 2007	Zahl der Klassen	Veränderung Zahl der Klassen seit 2007
Grundschulen	46	9.223	-577	398	- 34
Hauptschulen	7	1.982	-762	91	- 45
Realschulen	10	4.754	-142	156	- 6
Gymnasien	12	10.880	+1.109	381	+ 51
Förderschulen	6	928	-134	82	- 9
Summe	81	26.937	-506	1.408	- 43

Tabelle 1: Verteilung der Zahl der Schulen sowie Schüler/innen auf die verschiedenen Schulformen (einschl. Abendrealschule und Abendgymnasium, ohne Helen-Keller-Schule), Stand: Oktoberstatistik 2011

Hinweis: Die sechs Berufskollegs sind nicht in den MEP einbezogen.

1.3.2. Ausstattung der Schulen mit IT

Bei der Ausstattung der Schulen wird unterschieden 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.

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

Insgesamt sind rund 3.000 PC und Notebooks mit den dazugehörigen Peripheriegeräten in den Schulen installiert. Die schulformbezogene Verteilung stellt sich wie folgt dar:

Verteilung Hardware nach Schulformen (Stand: Mai 2011)								
Schul- form	PC/Notebook		Drucker		Scanner		Beamer	
	Päd.	Verw.	Päd.	Verw.	Päd.	Verw.	Päd.	Verw.
GS	522	139	77	53	30	14	18	5
HS	379	46	36	29	19	6	27	2
RS	399	46	47	29	23	6	35	
GY	1.032	157	87	72	34	8	139	
FÖ	180	26	51	14	7	4	2	1
2. BW	63	15	14	5	5	2	5	
Summe	2.575	429	312	196	118	40	226	8

Tab. 3: Verteilung der PC/Notebooks auf die Verwaltungs- und Pädagogikbereiche der jeweiligen Schulform (ohne Helen-Keller-Schule) - Stand: Mai 2011

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

Das Lernen mit neuen Medien erfordert eine Infrastruktur, die leistungsfähig, dauerhaft verfügbar und zukunftsorientiert ist. Mit der Umsetzung des MEP in den Jahren 2003 bis 2007 und der ersten Reinvestition in den Jahren 2008 bis 2011 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 Anwendungsängste 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

Alle PC, Notebooks und Monitore die älter als 4,5 Jahre sind, werden ausgetauscht. Im Jahr 2011 wurde der erste Reinvestitionszyklus abgeschlossen. Die o.g. Hardware wurde in allen Schulen zum ersten Mal ersetzt. Der zweite Reinvestitionszyklus hat im Jahr 2012 bereits begonnen. Jede Schule wird dann wieder als eigenständiges Reinvestitionsprojekt geplant, das von einem/einer zentralen Ansprechpartner/in beim Amt für Schule und Weiterbildung und bei der citeq geleitet wird (siehe auch unter 3. "Kundenberatung"). 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.

Durch verschiedene Einflüsse im Verlauf der Ausstattung 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 aus wirtschaftlichen Gründen erst dann ausgetauscht, wenn sie das entsprechende Alter erreicht hat.

Im Rahmen der MEP-Ausstattung stellt die citeq verschiedene Druckertypen und -modelle zur Verfügung. Dabei wird darauf geachtet, stets leistungsfähige und haltbare Geräte anzuschaffen. Wesentlich längere Standzeiten als 8 bis 10 Jahre werden jedoch vermieden. Die Anzahl der eingesetzten Druckermodelle und der Umfang der verschiedenen Verbrauchsmaterialien, die vorgehalten werden müssten, nähmen sonst einen

Umfang an, der nicht mehr wirtschaftlich wäre. Darüber hinaus wird auch die technische Entwicklung bei der Ausstattung berücksichtigt.

Für Beamer ist eine entsprechende Regelung vorgesehen. Die technische Entwicklung hinsichtlich der Funktionalitäten und der Leistungsfähigkeit der Beamer macht es erforderlich, auch Beamer nach einer Laufzeit von 8 bis 10 Jahren auszutauschen. In jedem Fall sind diese Geräte im Falle eines Lampendefektes gegen aktuelle Systeme auszutauschen.

Scanner werden reinvestiert, wenn der Einsatz aus technischen oder wirtschaftlichen Gründen nicht mehr sinnvoll ist.

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 Neuausstattung 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, werden unverzüglich mit dem Amt für Schule und Weiterbildung und der Schule kommuniziert.

2.2.5. Funktionskontrolle

Im Reinvestitionsprojekt wird die vereinbarte Hardware funktionsfähig an die Schule übergeben. Die mit der Schule vereinbarten Softwareinstallationen werden an einem Musterrechner in der Schule auf ihre Funktionsfähigkeit überprüft. Der Musterrechner ist der PC, der die meisten Softwareinstallationen beinhaltet. Die Überprüfung wird mittels Fernzugriff zu Beginn der Installationsarbeiten in der Schule durchgeführt. Der IT-Kontaktlehrer der jeweiligen Schule wird gebeten, möglichst noch im Rahmen des vereinbarten Projektzeitraumes die Installationen ebenfalls (möglichst auch inhaltlich) zu prüfen.

2.2.6. Abnahme

Zusätzlich zur Funktionskontrolle vereinbart die Kundenberatung nach einer ersten Betriebsphase der neuen Ausstattung einen Abnahmetermin mit der Schule. 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.

2.2.7. Verwendung der Althardware

Nach der Standzeit von zurzeit 4,5 Jahren ist die Althardware (PC, Notebooks und Monitore) technisch überholt und auch vermehrt reparaturanfällig. Von einem weiteren Betrieb im MEP-Netz ist daher abzusehen.

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 und vorhandene Daten werden sicher gelöscht.

2.3. Diebstähle

Die Erfahrungen in der Anfangsphase des MEP haben sehr deutlich gemacht, dass Schutzmaßnahmen gegen Einbruch und Diebstahl ergriffen werden müssen. Dies gilt auch weiterhin.

Das Schadensaufkommen hat jedoch deutlich nachgelassen. Dies lässt sich auf verschiedene Ursachen zurückführen:

- Die Schulen wurden durch entsprechende Informationen sensibilisiert, im Umgang mit den zur Verfügung gestellten Systemen Gesichtspunkte der Diebstahlvorsorge zu beachten (z. B. Ausgabeverfahren, grundsätzlicher Umgang mit Hardware, erhöhte Aufmerksamkeit, sichere Aufbewahrung).
- Die Notebooks werden mit einem speziellen Diebstahlschutz-Aufkleber gekennzeichnet.
- In Einzelfällen wurden Sicherungsmaßnahmen in den Räumlichkeiten durchgeführt.

Es ist auch weiterhin möglich, in Einzelfällen einen gemeinsamen Beratungstermin mit der Polizei durchzuführen, um in Betracht kommende Diebstahlschutzmaßnahmen zu erörtern.

2.4. Software

2.4.1. Softwareausstattung der Schulverwaltungen

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

Software-Katalog

Im unterrichtlichen Bereich wird Software, die über die Standard-Applikationen hinausgeht, grundsätzlich nur im Rahmen des vereinbarten Kataloges installiert. Ausnahmen von dieser Vorgehensweise werden in begründeten Einzelfällen (z. B. für die Installation eines Smartboards) 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. Nur mit einer homogenen Softwarelandschaft können die gewohnten Service-Leistungen mit dem vorhandenen Personalschlüssel für die Betreuung erbracht werden. 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.

Der Software-Katalog ist im MEP-net (siehe unter 3.2. "MEP-net") veröffentlicht. Lehrkräfte können sich die Softwareprodukte über die Softwareübersicht ansehen und nach verschiedenen Kriterien filtern. Soll ein Softwareprodukt des Kataloges in der Schule installiert werden, kann browserbasiert ein Installationsauftrag für das ausgewählte Softwareprodukt erstellt werden. Damit wird sichergestellt, dass der Auftrag alle für die Installation erforderlichen Informationen beinhaltet. Der Installationsauftrag kann anschließend ausgedruckt und unterschrieben an die Kundenberatung der citeq geschickt werden. Dieses Verfahren ist mit der Lenkungsgruppe abgestimmt. Durch den Papierausdruck soll sichergestellt werden, dass die Schulleitung in jedem Fall beteiligt wird. Das ist insbesondere dann wichtig, wenn mit der avisierten Installation Lizenzkosten verbunden sind.

Software-Anmeldeverfahren

Neue Lehrpläne, neue Produkte, veränderte Lizenzbedingungen oder technische Anpassungen sind die Faktoren, die u. a. eine regelmäßige Überarbeitung des Warenkataloges notwendig machen.

Für die Erweiterung des Software-Kataloges hat die citeq gemeinsam mit der Lenkungsgruppe eine technische Lösung erarbeitet, die eine browserbasierte Erfassung und Weiterleitung von Anmeldungen für den Einsatz neuer Softwareprodukte an die citeq ermöglichen.

Jede Schule kann Softwareanmeldungen browserbasiert erfassen und an den Schulformvertreter der Lenkungsgruppe weiterleiten. Das Lenkungsgruppenmitglied entscheidet über die Weiterleitung der Softwareanmeldung an die citeq und priorisiert den Softwaretest gegebenenfalls. Die citeq prüft und bewertet die Produkte, die in den Katalog aufgenommen werden sollen, auf ihre technische Einsetzbarkeit. Anschließend erfolgt der Praxistest der Software in der Schule, die die Software angemeldet hat.

Der aktuelle Status der Softwaretests wird im MEP-net veröffentlicht und kann dort jederzeit von allen Lehrern eingesehen werden.

Eignung und Installation

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 Netzwerkversionen 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.

Softwareprodukte können und sollen von Lehrern beurteilt werden. Diese Beurteilung soll allen Schulen helfen, geeignete Produkte zur Unterstützung des Unterrichts zielgerichtet auswählen zu können. Diese Beurteilung ist ebenfalls browserbasiert für die Produkte des Software-Kataloges möglich.

3. Kundenberatung

3.1. Allgemeines

Die Erfahrungen haben gezeigt, dass eine dauerhafte Beratung der Schulen durch feste Ansprechpartner für eine erfolgreiche Umsetzung des MEP eine wichtige Voraussetzung darstellt. Die Schulen wünschen sich auch die regelmäßige Präsenz der Kundenberater 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 bedarfsgerechter Lösungen.

Der Beratungsbedarf wird insbesondere aufgrund der steigenden Technisierung im Schulumfeld und den damit einhergehenden (neuen) Anforderungen fortbestehen, evtl. sogar noch steigen. Ebenso sind das Amt für Schule und Weiterbildung und die citeq auf Informationen und Beratung durch die Schulen angewiesen. Aus diesem Grund hat die ständige Kommunikation zwischen den Schulen und Amt für Schule und Weiterbildung bzw. citeq eine große Bedeutung. Besondere oder innovative Nutzungsmöglichkeiten 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, so dass die Potentiale hier entsprechend ausgeschöpft werden können. Hierbei setzen allerdings die zur Verfügung stehenden Personalkapazitäten Grenzen.

Für die laufende Beratung 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. Dafür wird mit jeder Schule mindestens jährlich ein Gesprächstermin vor Ort vereinbart.

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 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 Benutzerkennungen.

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

- die aktuellen Hardware- und Softwarestandards,
- Hinweise zur Nutzung der IT allgemein,

- Benutzerhandbücher für die Nutzung von Tools für IT-Kontaktlehrer,
 - Hinweise zur Benutzerverwaltung,
 - Informationen über geplante Wartungsarbeiten und Installationen,
 - Verlinkungen zum Service-Desk, zum Softwareanmeldeverfahren, oder zum IT-Bestandsmodul,
 - aktuelle Bestellvorlagen für Tonerkartuschen
- veröffentlicht.

Unter dem Menüpunkt „Ich bin neu hier“ erhalten insbesondere Lehrer, die noch keine oder nur wenige Kenntnisse über die IT in den Münsteraner Schulen haben, Antworten auf häufig gestellte Fragen.

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. Fortbildungen/Workshops für IT-Kontaktlehrer

Bislang waren im Rahmen des MEP Fortbildungsveranstaltungen für IT-Kontaktlehrer nicht vorgesehen. Im Rahmen der Umsetzung des MEP wurden für diesen Personenkreis technische Möglichkeiten geschaffen, die eine eigenständige Administration vor Ort ermöglichen (siehe unter 8.8. "Rechte der IT-Kontaktlehrer" oder 9.6 "Plattform für die Aktualisierung von Standard-Software (PASS)"). Je nach Bedarf in den Schulen werden diese Möglichkeiten entsprechend von der citeq ausgeweitet. Für den professionellen Umgang mit den dafür zur Verfügung gestellten Werkzeugen sind Fortbildungsveranstaltungen sinnvoll. Das gilt insbesondere für den Fall, dass IT-Kontaktlehrer im Umgang damit unsicher und/oder nicht geübt sind (z. B. nach einem Wechsel dieser Aufgabe in der Schule).

Die citeq plant die Erarbeitung eines Schulungskonzeptes für regelmäßige Fortbildungsveranstaltungen der IT-Kontaktlehrer aller Schulformen. Hierzu wurden im Rahmen der Jahresgespräche 2011 bei allen Schulen Informationen zu Schulungsbedarfen und -Inhalten erhoben. Die citeq hat in Abstimmung mit dem Amt für Schule und Weiterbildung im vierten Quartal 2011 bereits bedarfsgerechte Fortbildungsveranstaltungen für die IT-Kontaktlehrer der Grundschulen durchgeführt.

II. Ausstattungs- und Betriebskonzept

1. Technische Grundsatzentscheidungen

1.1. Allgemeines

Die citeq verfolgt permanent 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 Aufstellung des MEP und auch im Rahmen der Fortschreibung in 2007 gegen den Einsatz von Terminalservern gesprochen haben, liegen weiterhin vor. Aufgrund der stark parallelen Nutzung hochmultimedialer Anwendungen kann die Terminalserver-Technologie in den Schulen nicht wirtschaftlich eingesetzt werden.

Pro Schule bzw. Schulzentrum werden zwei Server installiert (je ein Server für Verwaltung und Pädagogik). Für die Schulen, die per Lichtwellenleiter (LWL) an die citeq angebunden sind, wird geprüft, die Server vor Ort zu konsolidieren und für mehrere Schulen auf Servern in zentralen Serverräumen der citeq zusammen zu führen. 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 8.3 "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 9.3. "Betriebssystem Clients") zu entnehmen.

1.4. Drucker

Im Rahmen des MEP werden weiterhin nur netzwerkfähige Drucker eingesetzt. In größeren Netzwerken ist der Einsatz und Betrieb einer geringeren Zahl von netzwerkfähigen Druckern wirtschaftlicher als viele lokal installierte Drucker. Die Gründe, die gegen den wirtschaftlichen Einsatz lokaler Drucker sprechen sind:

- nur lokaler Zugriff von einem PC
- relativ hohe Verbrauchskosten
- keine Wartungsmöglichkeiten über das Netzwerk

1.5. Monitore

Bereits im Rahmen der letzten Fortschreibung wurde festgelegt, dass im Rahmen des MEP zukünftig nur noch ein 19"-TFT-Monitortyp eingesetzt wird. Dieser wird über den aktuellen Rahmenvertrag der citeq beschafft. Der Einsatz von TFT-Monitoren ist im Vergleich zum früheren Einsatz der CRT-Monitore wirtschaftlicher. Sofern noch Restbestände anderer Monitortypen und -Größen im Einsatz sind, werden diese im Rahmen der Reinvestition bereinigt.

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 ein-

gesetzt 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.

- 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 optimale Unterstützung leisten kann.

2. Beschaffung

Die zentrale Beschaffung der Hardwarekomponenten und der Standard-Software (Betriebssysteme, Serverlizenzen) durch die citeq ist ein wesentlicher Bestandteil der Konzeption. Dadurch wird die weitgehende Homogenität der Systeme sichergestellt. Hierdurch ist es möglich den Grundsatz der Standardisierung umzusetzen.

Aufgrund der höheren Stückzahlen, die sich durch eine zentrale Beschaffung ergeben, können wesentlich bessere Preiskonditionen ausgehandelt werden. Besonders vorteilhaft hat sich die Kooperationen mit dem KDN Dachverband kommunaler IT-Dienstleister, ausgewirkt. Für die wesentlichen Hardware-Komponenten (PC, Notebooks, Monitore, Drucker, Beamer) hat der Abschluss von Rahmenverträgen zu deutlichen Erleichterungen und Zeiteinsparungen bei der Bestell- und Lieferabwicklung geführt.

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 Sys-

teme 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 sollen 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 Firewallschutz.

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 Differenzsicherung 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 8.13. "Datensicherung Server").

Die Räumlichkeiten, in denen die zentralen und dezentralen (in den Schulen) Server installiert werden, müssen besondere Anforderungen erfüllen (u. a. geschlossen und nicht für jedermann zugänglich, ausreichende Lüftung, abschließbare Serverschränke; siehe unter 7.2 "Inhouse-Verkabelung / Netzkomponenten - LAN (Local Area Network)").

Die zuvor beschriebenen technischen Maßnahmen und Einrichtungen werden durch die citeq betreut und gewartet. 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 des Landes Nordrhein-Westfalen (DSG NRW) ist auch bei der Behandlung der Daten durch die Mitarbeiter der citeq voll gewährleistet.

Jede Mitarbeiterin und jeder Mitarbeiter der citeq wird jährlich 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.

Die Verwaltungsbereiche des MEP sind in die Sicherheitskonzeption der citeq eingebunden, das auf der Basis der IT-Grundschutzvorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umgesetzt wird.

Im Dezember 2008 wurde eine IT-Sicherheitsleitlinie als verbindliche Vorgabe für das Handeln aller Mitarbeiterinnen und Mitarbeiter der citeq verabschiedet. Oberster Grundsatz dieser Sicherheitsleitlinie ist die sichere Verarbeitung von Informationen.

Die für die BSI-Standards erforderliche Sicherheitsorganisation wurde im Jahre 2009 mit dem „citeq Security Board (cSB)“ aufgebaut. Ab 2010 wurde mit der Erstellung der Sicherheitskonzeption nach BSI begonnen mit der Folge, dass auch die IT-Komponenten der MEP-Verwaltungsbereiche (Systemräume, Server, Clients) nach den Vorgaben der IT-Grundschutzkataloge überprüft und etwaige erforderliche Maßnahmen zur Herstellung der notwendigen Schutzstufen initiiert werden.

5. Protokollierung von Nutzerdaten

Durch die Authentifizierung der einzelnen Benutzer im eDirectory (der von Novell zur Verfügung gestellte 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 Telekommunikati-

onsgesetz 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 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 8.7. "Benutzer-/Gruppenverwaltung / eDirectory" aufgeführten Daten, die nicht von den Vorschriften des Telekommunikationsgesetzes betroffen sind.

Alle von der citeq in diesem Zusammenhang erhobenen Daten werden nach Ablauf von drei Monaten automatisch gelöscht.

6. Inventarisierung der Hardware

Für die Inventarisierung der Hard- und Softwarekomponenten wird eine zentrale Datenbankanwendung eingesetzt, die auch für die IT-Komponenten der Stadtverwaltung genutzt wird. Jedes Gerät besitzt eine eindeutige ID-Nummer, die mit Hilfe eines Aufklebers sichtbar auf den Geräten angebracht ist.

Für die IT-Kontaktlehrer wurde eine webbasierte Anwendung, das IT-Bestandsmodul entwickelt. Dieses Modul ermöglicht eine Auswertung der zentralen Hardware-Datenbank und listet die für die entsprechende Schule inventarisierte Hardware auf. Es ist aus dem Internet, d.h. auch von zu Hause aus, zu erreichen. Zugriff auf das IT-Bestandsmodul haben alle Personen, die im pädagogischen Netzwerk der Schule als IT-Kontaktlehrer eingerichtet sind. Die Anmeldung erfolgt mit der Kennung für das pädagogische Netz. Die Hardware kann nach den beiden Netzwerken Pädagogik oder Verwaltung und den unterschiedlichen Hardwaretypen gefiltert werden.

7. Technisches Ausstattungskonzept

7.1. 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 - pädagogisches Netz und Schulverwaltungsnetz - durch entsprechende Kabelführungen und jeweils eigene aktive Netzkomponenten im LAN getrennt voneinander aufgebaut sind.

7.2. 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 Einbruchsisikos (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.

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 werden für den Anschluss der Endgeräte (PC, Netzwerkdrucker) Fast-Ethernet-Switche und Gigabit-Ethernet-Switche verwendet. Switche bieten hohe Performance von 10/100/1000 MBit/s dediziert pro Port (Anschlussmöglichkeit für ein Endgerät) bei gleichzeitig günstigem Preis-/Leistungsverhältnis. Die Gigabit-Technik wird in Zukunft die Fast-Ethernet-Technik ersetzen. Der Ausbau des lokalen Netzwerkes erfolgt mit Gigabit-Ethernet-Komponenten, technische Gründe könnten einen Tausch älterer Fast Ethernet Switches beschleunigen.

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 aufgebauten Schulnetz (WAN) werden die Daten auf gemeinsamen Medien übertragen.

7.3. WLAN (Wireless Local Area Network)

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

Funknetze (Wireless LAN / WLAN) stellen für die flexible Abbildung von größeren Arbeitsgruppen mit Notebooks 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 mittels elektromagnetischer Funkwellen.

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. Die citeq folgt hier einer Empfehlung des BSI (Bundesamt für Sicherheit in der Informationstechnik) und setzt die WPA2 Verschlüsselung mit einem 63 Zeichen langen Passwort ein. 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.

Im pädagogischen Netzwerk kann ein drahtloses Funknetzwerk nach dem Standard IEEE 802.11 installiert werden. Das Netzwerk wird als "fliegendes Klassenzimmer" in den Schulen eingesetzt. Damit können bis zu 20 Benutzer drahtlos verbunden und diesen WLAN Clients zentrale Dienste der citeq zu Verfügung gestellt werden. Der Access Point wird nicht fest installiert und wird bei Bedarf im jeweiligen Klassenzimmer in Betrieb genommen. Dieser stellt eine Verbindung vom LAN zu den Wireless-Clients her.

Für den Anschluss im Klassenzimmer muss ein funktionierender Netzwerkanschluss sowie eine 220 Volt Stromsteckdose vorhanden sein.

Die Einrichtung raumübergreifender WLAN in den Schulen ist nicht vorgesehen. Eine Gebäudeeinmessung und Installationsplanung ist daher nicht erforderlich.

Die WLAN-Notebooks werden so konfiguriert, dass sie sich sowohl kabelgebunden, als auch über WLAN im Netzwerk anmelden können. Durch die Vergabe nur einer IP-Adresse je Gerät für Kabel und WLAN wird vermieden, dass in weiterführenden Schulen der IP-Adressbereich evtl. nicht mehr ausreichen könnte. Alle von der citeq über den Warenkatalog zur Verfügung gestellten Notebooks können in ein WLAN eingebunden werden.

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

7.4. 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. Die Schulstandorte werden mit SDSL Technik (symmetrische Bandbreiten) an das Providernetzwerk angeschlossen. Für den Aufbau der komplexen WAN-Infrastrukturen ist nach euweiter Ausschreibung ein Vertrag mit einem Telekommunikationsprovider abgeschlossen worden (zurzeit Fa. Versatel). Sieben Schulen sind bereits per LWL mit einer Geschwindigkeit von 1000 Mbit/s direkt an das Netz der citeq angebunden (Stand: Anfang Dezember 2011). Der weitere Ausbau von LWL-Verbindungen ist geplant. Bis zum Ende des 3. Quartals 2012 werden voraussichtlich 27 Schulen per LWL angebunden sein. Aufgrund der hohen Einrichtungskosten für LWL-Verbindungen muss für jeden Standort eine wirtschaftliche Überprüfung stattfinden.

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 8.4.8. "Virenschutz")

- Proxy-Server als Cache zum Internet (siehe unter 8.4.10. "Internetzugang mittels Proxy-Services")

Der Zugang zum Internet für alle Schulen, die nicht per LWL an die citeq angebunden sind, wird mit einer Bandbreite von 100 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) stellen 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 ist aus diesem Grund bislang ausgeschlossen (siehe aber hierzu auch 7.5 "Nutzung der Telekom@school-Anschlüsse für das Internet").

Nur über hochverfügbare und symmetrische Leitungsanbindungen kann die citeq notwendige Wartungsarbeiten, Softwareaktualisierungen und die Überwachung sämtlicher Systeme jederzeit sicherstellen. Das wäre über die im privaten Bereich weit verbreiteten Leitungsanbindungen auf Basis von ADSL nicht möglich.

7.5. Nutzung der Telekom@school-Anschlüsse für das Internet

Für die fortschreitende Nutzung insbesondere multimedialer Inhalte über das Internet stellen die den Schulen zur Verfügung gestellten Bandbreiten dort, wo dauerhaft eine Anbindung über LWL nicht realisiert werden kann, unter Berücksichtigung einer Vielzahl von Rechnern im pädagogischen Netz eine deutliche Grenze dar. Das liegt daran, dass über das MPLS z. Z. nur Bandbreiten von bis zu 8 Mbit/s je Standort wirtschaftlich realisiert werden können.

Gleichwohl verfügt jede Schule, die Erstausbildung betreibt, über das Projekt Telekom@school über einen weiteren Zugang zum Internet mit einer Geschwindigkeit von bis zu 16 Mbit/s. Die Geschwindigkeit ist abhängig von der technischen Verfügbarkeit am Standort des Anschlusses. Die Leistung ist für die Schulen auf Dauer entgeltfrei, nur das notwendige DSL-Modem muss käuflich erworben oder angemietet werden. Schulen in VDSL(Very High Speed DSL)-Ausbaubereichen können gegen einen kleinen Aufpreis auch einen VDSL-Anschluss mit einer Geschwindigkeit von bis zu 50 Mbit/s erhalten.

Diese Schulen wurden von der Telekom vor den Sommerferien 2011 angeschrieben und über diese Option informiert.

Einige Schulen versorgen über diese Anschlüsse bereits schuleigene Rechner mit einem Internetzugang. Auf Grund der vorgenannten möglichen Bandbreiten wird die citeq prüfen, ob Telekom@school-Anschlüsse für die Nutzung des Internets im pädagogischen Netz des MEP genutzt werden können. Im Rahmen eines Projektes wird daher intensiv untersucht ob und unter welchen Voraussetzungen das möglich sein könnte.

7.6. 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.

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.

7.7. 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 unter 10.2. „Service-Desk / Störungsmeldung und –verfolgung“) eingebracht und entsprechend den Servicevereinbarungen beseitigt.

7.8. Anschluss privater Rechner an das Internet

Um vorhandene Ressourcen nutzen und flexibler arbeiten zu können, wollen Lehrer und Schüler auch ihre privaten Rechner auch in der Schule nutzen. Avisiert ist dabei in erster Linie die Nutzung des Internets.

Dabei ist die Nutzung der von der citeq zur Verfügung gestellte Schulanbindung aus verschiedenen allgemeinen und sicherheitstechnischen Gründen nicht möglich:

- Die Bandbreite der Schulanbindung ist für den zusätzlichen Datenverkehr, den eine noch unbestimmte Anzahl privater Rechner bei der Nutzung des Internets erzeugen würde, nicht ausgelegt. Der Betrieb der von der citeq im Rahmen des MEP bereitgestellten Hardware könnte dadurch erheblich eingeschränkt werden (siehe hierzu auch 7.5 "Nutzung der Telekom@school-Anschlüsse für das Internet").
- Sicherheitstechnische Aspekte schließen eine Nutzung des MEP-Schulnetzes ebenfalls aus. Einerseits wäre ein zentral gesteuerter Virenschutz für die privaten Rechner nicht gegeben, was zu einer Infizierung des Netzwerks mit Viren und anderer Schadsoftware führen könnte. Andererseits könnte auf den privaten Rechnern verschiedenste Software installiert sein, mit deren Hilfe sich Angriffe auf Netzwerkkomponenten und die Server in der Schule durchführen ließen. Ein Schutz vor solchen Angriffen könnte nicht sichergestellt werden, sodass die gewohnte Sicherheit und Stabilität des MEP-Schulnetzes von der citeq nicht mehr gewährleistet werden könnte.

Alternativ dazu kann die citeq den privaten Rechnern über den in allen Schulen vorhandenen kostenlosen Telekom@school-Anschluss oder über noch breitbandigere kostenpflichtige Internetanschlüsse anderer Provider der Zugang zum Internet über ein WLAN ermöglichen.. Die dazu erforderliche Hard- und Software wird von der citeq installiert und gewartet. Die Administration des WLAN (Einrichten von Zugängen) erfolgt durch die Schule.

Die Kosten werden aus dem MEP-Budget der jeweiligen Schule finanziert. Die Funktionsfähigkeit der schuleigenen Internetverbindung ist durch die jeweilige Schule sicherzustellen. Eine Störungsüberwachung bzw. -Verfolgung durch die citeq erfolgt nicht.

8. Server

8.1. 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 mittels Antwortdatei 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, sondern auf mehrere Platten geschrieben (RAID 5). 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 Servers in der Pädagogik sind zusätzlich die Dateien, die aus der Sicherung ausgeschlossen sind (siehe unter 8.13. "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.

Zur Vermeidung der durch Stromschwankungen möglichen Risiken (Neustarts per Fernwartung, Defekt der Serverhardware) werden in allen Schulstandorten unterbrechungsfreie Stromversorgungen (USV) eingesetzt. Diese filtern Stromschwankungen heraus und überbrücken kurzfristige Stromausfälle mit einer Dauer von wenigen Minuten, sodass die Server in diesen Situationen nicht mehr ausfallen können.

8.2. Virtualisierung von Servern

Zu den wichtigsten Technologien bzw. Trends der IT-Branche zählt die Virtualisierung. Virtualisierung ermöglicht den parallelen Betrieb mehrerer virtueller Server auf einer physikalischen Hardware. Die Virtualisierung hilft dabei mehr Flexibilität zu schaffen und Kosten zu reduzieren, da sowohl Serverhardware wie auch Stromverbrauch eingespart werden. In den zentralen Serverräumen wird zudem die Wärmelast entsprechend reduziert. Im MEP sind dabei jedoch folgende Punkte zu beachten:

- Aufgrund der Isolierung der verschiedenen virtuellen Maschinen ist die in § 2 Abs. 1 Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schü-

lern und Erziehungsberechtigten (VO-DV I) verlangte galvanischen Trennung von Verwaltung und Pädagogik („... ist in der Schule grundsätzlich eine ausschließlich für die Verwaltung der Schule vorgesehene ADV-Anlage zu verwenden...“) als gegeben anzusehen. Somit wird - zunächst in den Grundschulen - die Möglichkeit zur Virtualisierung von Verwaltung und Pädagogik auf einem Server umgesetzt.

- In Schulzentren teilen sich zurzeit die 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 virtueller Maschine auf einem Server entsprechend mehr Hardwareressourcen zur Verfügung stehen müssen. Auch erhöht sich der personelle Aufwand für die Einrichtung und Betreuung der virtuellen Server. Vor einer Virtualisierung von Servern in Schulzentren muss daher die Wirtschaftlichkeit dieser Maßnahme geprüft werden. Nur wenn die mit den zu erwartenden Vorteilen verbundenen Einsparungen die zu erwartenden höheren Aufwände deutlich übersteigen, wäre eine Umsetzung sinnvoll.

8.3. Betriebssystem und Version

Als Betriebssystem kommt zurzeit der Novell Open Enterprise Server basierend auf dem SuSE Linux Enterprise Server mit den jeweils aktuellen Updates und Patches zum Einsatz. Die Entscheidung für Novell wurde bei der Aufstellung des MEP aufgrund einer Nutzwertanalyse zwischen den Betriebssystemen Microsoft Server, Novell Server und 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 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.

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 fehlerfreien Betrieb und damit eine hohe Verfügbarkeit. Durch diese Aktualisierungen 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.

8.4. 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,
- Authentifizierung und Authorisierung.

Diese Dienste werden zur Verfügung gestellt durch die Produkte Novell Linux Open Enterprise Server, Novell GroupWise in den Schulverwaltungen bzw. mittels Web-Mail-Zugang in der Pädagogik, Squid, 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 Bandbreite des Netzes an vielen Standorten nicht möglich. Bei der Anbindung von Schulen per LWL an die citeq wird eine zentrale Bereitstellung bei der citeq geprüft werden (siehe unter 8.15. "Zentrale Serverbereitstellung").

8.4.1. 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.

8.4.2. 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.

8.4.3. Dynamic Host Control Protocol (DHCP)

Zur Identifizierung und Adressierung erhält jeder Rechner eine Netzwerkadresse (Internet Protocol Address / IP-Adresse). 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 sinnvollerweise 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.

8.4.4. 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.

8.4.5. 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 in das Betriebssystem 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 zurzeit durch GroupWise Web-Access, so dass neben einem Standard-Internetbrowser keine zusätzliche Software auf dem Client benötigt wird. Mit diesem Dienst können die Schüler und Lehrer Mails mit E-Mail-Empfängern weltweit austauschen. Damit kann der Bereich "Mailing" als fester Bestandteil in der Me-

dienerziehung 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.

Der Funktionsumfang von Web-Access ist gegenüber dem Voll-Client eingeschränkt, weil auf das Mailsystem ausschließlich per Browser zugegriffen werden kann. So ist es nur sehr eingeschränkt möglich, Regeln zu definieren. Für eine komfortablere Nutzungsmöglichkeit wäre hier auch die Installation des GroupWise Voll-Clients erforderlich. Dafür muss zunächst geprüft werden, ob und in welchem Umfang hierfür Lizenzkosten anfallen würden. Danach wird angestrebt, den GroupWise Voll-Client als weiteres Softwareprodukt für die Pädagogik zur Verfügung zu stellen.

8.4.6. 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:

- Blockung von Mail von Einwahlrechnern und
- 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 das Produkt WatchGuard XCS. Diese Anwendung kennzeichnet Mails als SPAM nach verschiedenen Kriterien. Unter anderem gehen die Absender-IP und der Inhalt mit in die Bewertung ein.

Die citeq wehrt SPAM erfolgreich mit den statischen Listen und durch das Greylisting ab. An einem Werktag werden etwa 60%, an einem Wochenende etwa 95% der eingehenden Mail im Sinne einer SPAM Abwehr durch die citeq blockiert. Eine höhere Quote kann 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.

Die Kennzeichnung durch WatchGuard XCS vereinfacht durch die Kennzeichnung den Umgang mit unerwünschten Mails.

8.4.7. 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 Info-Displays werden an einem oder mehreren Orten in der Schule Informationen (in der Regel Vertretungspläne) zur Verfügung gestellt, die vorab in einem bestimmten Verzeichnis abgelegt wurden (siehe unter 9.7. "Info-Displays").

8.4.8. 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 CD-ROM-Laufwerke und USB-Schnittstellen, 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 sieht die citeq auch auf dem Server den Einsatz eines Virenschanners vor.

8.4.9. 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 Bereitstel-

lung 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.

8.4.10. 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 Internetzugang 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.

8.5. 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.).

8.5.1. Zentral administrierter SquidGuard

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 dem zentralen 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. 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 zentrale SquidGuard wird in regelmäßigen Abständen von der citeq aktualisiert.

8.5.2. Von der Schule zu administrierender SquidGuard

Häufig besteht die Notwendigkeit, Internetseiten nicht im gesamten pädagogischen Bereich des MEP, sondern nur in einer Schule zu sperren. Die Sperre kann durch den IT-Kontaktlehrer der Schule kurzfristig eingerichtet und auch wieder aufgehoben werden. Somit können auf einfachem Wege Internetseiten temporär gesperrt werden. Die Verwaltung der gesperrten Internetseiten erfolgt über das Lehrerportal, welches auf jedem pädagogischem Schulserver installiert ist.

Ferner besteht für die IT-Kontaktlehrer die Möglichkeit, auf die gleiche Weise das Internet für die gesamte Pädagogik temporär zu sperren und auch wieder frei zuschalten.

8.6. Arbeiten bei Ausfall der Netzanbindung

Grundsätzlich ist die gesamte Serverinfrastruktur auf eine dauerhaft bestehende Netzanbindung ausgelegt. Dieses ist für die uneingeschränkte Funktionalität des eDirectory zwingende Voraussetzung, da alle im eDirectory vorhandenen Server sowohl eventorientiert als auch 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 sehr selten zu Ausfällen kommen kann. Um den Schulen auch während eines Ausfalls der WAN-Verbindung die Nutzung der IT-Technik zu ermöglichen, sind an den Servern und Clients entsprechende Anpassungen 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.

Anders sieht es in den Schulen aus, die auf Grund der Leitungsanbindung mittels LWL auf zentralisierten Servern arbeiten. Sollte es hier einmal zum Ausfall der Verbindung kommen, ist ein Arbeiten auf den betroffenen Arbeitsstationen für die Dauer des Ausfalls nicht möglich. Da es sich hierbei um städtische Standleitungsverbindungen handelt, ist die Störungsanfälligkeit geringer als bei den v.g. WAN-Verbindungen. Störungen traten in der Vergangenheit nur durch physikalische Beschädigungen einer Leitung während Tiefbauarbeiten auf und wurden innerhalb weniger Stunden wieder behoben.

8.7. Benutzer-/Gruppenverwaltung / eDirectory

Für die Verwaltung von Benutzern und Gruppen und den dazugehörigen Rechten wird der im Novell Open Enterprise Server enthaltene Verzeichnisdienst eDirectory (vormals NDS) verwendet. 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.

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.

8.8. Rechte der IT-Kontaktlehrer

Ziel des MEP ist 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, kleinere administrative Aufgaben kurzfristig selber erledigen zu können. Die citeq ist bestrebt, 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-Koordinationen folgende Tools zur Verfügung: Console One, Windows-Dateiexplorer, Druckerverwaltung, TreeSize. Dieses Angebot wird bei Bedarf erweitert. Die Dokumentationen für diese Tools sind im MEP-net veröffentlicht. Die Schulen können die vorgenannten administrativen Tätigkeiten selbstverständlich auch von der citeq durchführen lassen. Das empfiehlt sich insbesondere für kleinere Schulen und/oder IT-Koordinationen, die mit dem Umgang der zur Verfügung gestellten Tools nicht vertraut sind.

8.9. 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 zugreifen können. Allerdings können Lehrkräfte grundsätzlich alle Schülerdaten einsehen, um Ihrem Lehrauftrag grundsätzlich sowie im Vertretungsfall nachkommen zu können. Sofern Dateien von mehreren Benutzern benötigt und ggf. verändert werden, stehen dafür, 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 weiterführenden Schulen ein Tauschordner eingerichtet, auf den auch die Schüler schreibenden Zugriff haben. Der Tauschordner wird automatisch jeden Abend geleert.

Zurzeit stehen allen Grundschulen je 15 GB und allen weiterführenden Schulen je 30 GB gesicherter Speicherplatz sowohl in der Verwaltung als auch in der Pädagogik zur Verfügung. Die Beschränkung des Speicherplatzes je Schule wurde vorgenommen, da nur unter diesen Bedingungen die regelmäßige Datensicherung (siehe unter 8.13. "Datensicherung Server") durchgeführt werden kann.

Die Erfahrungen des MEP haben gezeigt, dass die Schulen in der Pädagogik mehr Speicherplatz benötigen als ursprünglich vorgesehen war. Aus diesem Grund wurde jeder weiterführenden Schule noch ein zusätzliches Laufwerk von zurzeit 500 GB, jeder Grundschule 15 GB zur Verfügung gestellt. Auf diesem Laufwerk (N:) befindet sich ein Ordner „Schule“, dessen Verwaltung (z. B. Rechtevergabe) in der alleinigen Verantwortung der Schule liegt. Dieses Laufwerk wird 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, ext. HDD) selber im erforderlichen Rahmen organisiert.

Einige Schulen äußerten den Wunsch mehr Speicherplatz in einer durch die citeq verwalteten Ordnerstruktur zur Verfügung gestellt zu bekommen. Aus diesem Grunde wird den Schulen freigestellt, die persönlichen- und die Gruppenordner nicht mehr auf dem 30 GB großen gesicherten Laufwerk, sondern auf dem 500 GB großen ungesicherten

Laufwerk zu speichern und den Standardspeicherpfad (J:) entsprechend anpassen zu lassen. Jeder User hat zudem weiterhin die Möglichkeit, wichtige Daten auf dem gesicherten Laufwerk (H:) zu speichern.

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 PC-Spielen) nicht mehr möglich. Die Einrichtung des Quotings ist den Schulen freigestellt. Die bisherigen Erfahrungen mit dem Quoting sind durchweg positiv.

8.10. Zugriff auf Daten/Mails von Außen

Das mehrstufige Sicherheitskonzept der citeq verhindert wirkungsvoll Angriffe aus dem Internet auf die Systeme (Server und PC) in den Schulnetzwerken (siehe unter 4. "Datenschutz und Datensicherheit"). Ein Aufweichen dieser Schutzstufen würde einen erheblichen Eingriff in das Betriebs- und Sicherheitskonzept des MEP darstellen.

Auf Grund des besonders hohen Schutzbedarfs für die Daten der Schulverwaltung sind Zugriffe von Außen ausschließlich über VPN (kostenpflichtiger Einzelzugang mit Sicherheitstoken) möglich. Diese Zugangsmöglichkeit wurde von der citeq als sicher bewertet. Die laufenden Kosten für einen VPN-Zugang wären von der Schule zu tragen.

Aus den weiterführenden Schulen wird vermehrt der Bedarf geäußert, auf das in der Schule erarbeitete pädagogische Material einerseits und die pädagogischen Mailkonten andererseits auch von zu Hause aus zugreifen zu können. Da die Schutzstufe der Daten im pädagogischen Netz geringer ist als die der Schulverwaltung, lohnt sich hier eine weitere Untersuchung im Hinblick auf mögliche Realisierungsmöglichkeiten.

Die citeq wird im Rahmen eines Projektes prüfen ob und unter welchen Voraussetzungen Zugriffe von Außerhalb auf die im pädagogischen Netz erzeugten Daten direkt oder indirekt möglich sind. Sofern hierfür weitere Hard- und Software erforderlich sein sollte, wird die citeq diese aussuchen, sowie die Aufwände für Einrichtung und laufender Admi-

nistration kalkulieren. Da die Anforderung nur aus den weiterführenden und nicht von allen Schulen kommt, werden die zusätzlichen Kosten schulindividuell kalkuliert und sind aus dem Budget der Schule zu finanzieren. Sofern das Projekt zu dem Ergebnis kommen sollte, dass direkte Zugriffe von Außerhalb auf die im pädagogischen Netz erzeugten Daten nicht möglich sein sollten, könnte die unter 8.11. skizzierte "Kommunikationsplattform" eine Lösung darstellen.

8.11. Kommunikationsplattform

Kommunikations- und Lernplattformen gewinnen zunehmend an Bedeutung. Kommunikationsplattformen sind webbasierte Programme, in denen Inhalte dargestellt und verwaltet werden können, um die Kommunikation untereinander zu unterstützen. Diese Plattformen ermöglichen Schülerinnen und Schülern sowie Lehrkräften einen über das Internet orts- und zeitunabhängigen Zugriff auf gemeinsame Daten. Die Nutzer erhalten die Möglichkeit, über verschiedene Wege auch klassen- oder schulübergreifend miteinander zu kommunizieren und sich über Themen auszutauschen.

Die citeq setzt bereits seit mehreren Jahren eine Plattform zur Unterstützung von städteübergreifenden Projekten ein. Dieses System basiert auf der Open-Source Lernplattform-Software Moodle, welche lizenzkostenfrei eingesetzt werden kann. Moodle ist eine flexible und äußerst vielfältig nutzbare Lern- und Kommunikationsplattform. Sie wird permanent weiterentwickelt und ist auch im Schulumfeld in NRW bereits weit verbreitet.

Für zunächst ausgewählte Pilotschulen wird basierend auf dem Moodle-System eine Kommunikationsplattform namens „Schulen Intern“ eingerichtet. Nach erfolgreichem Abschluss dieser Pilotphase soll das System allen Münsteraner Schulen angeboten werden.

8.12. 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 kön-

nen 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.

8.13. 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.

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 war nicht mehr möglich, alle an einem Tag geänderten Dateien innerhalb einer Nacht zum zentralen Server zu synchronisieren. Falls die Schule eine Sicherung dieser Dateien benötigt, ist sie hierfür selbst zuständig.

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

8.14. Remote Administration

Für die Verwaltung der Novell-Server stehen verschiedene Möglichkeiten zur Verfügung. Zum einen kann mittels der Fernkonsole „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.

8.15. Zentrale Serverbereitstellung

Wie bereits an anderer Stelle ausgeführt lassen sich durch Virtualisierung von Servern einerseits Kosten sparen und andererseits kann die Wärmelast in den zentralen Serverräumen der Schulen gesenkt werden. Die Virtualisierung kommt in erster Linie in Grundschulen und in Schulzentren zum Tragen, die nicht per LWL angebunden werden können.

Bei Schulen, die per LWL angebunden sind, müssen die Server für die Verwaltung nicht mehr vor Ort stehen. Sie können ohne Einschränkungen für den Datenzugriff zentral bei der citeq platziert werden. Durch die zentrale Serverbereitstellung können weitere Kosten, die im Rahmen der Virtualisierung anfallen würden, eingespart werden. Dieses Verfahren ist bei der Stadt Münster seit vielen Jahren mit gutem Erfolg im Einsatz.

In der Pädagogik stellt sich die Situation etwas anders dar. Auf Grund der Vielzahl an unterschiedlichen Lernsoftwareprodukten kann nicht mit Sicherheit ausgesagt werden, dass deren Nutzung bei zentraler Serverbereitstellung uneingeschränkt möglich sein wird. Die citeq wird daher im Rahmen eines Projektes die Möglichkeiten der zentralen Serverbereitstellung auch im pädagogischen Netz prüfen.

9. Clients

9.1. Hardwareausstattung

Entsprechend der Festlegung in den Rahmenbedingungen des technischen Ausstattungs- und Betriebskonzeptes kommen in der Schulverwaltung und im pädagogischen Bereich nur neue, standardisierte PC oder Thin Clients (im Bereich der sog. Info-Monitore) zum Einsatz.

Im Gegensatz zu PCs handelt es sich bei Thin Clients um Rechner mit reduzierter Hardwareausstattung und -leistung, deren Hauptaufgabe darin besteht, von einem Server bereitgestellte Daten darzustellen. Entsprechende Thin Client Anwendungen sind u. a. Web-Browser und Software für den Zugriff auf Terminalserver. Als Betriebssystem wird z. Z. Windows Embedded Standard 2009 eingesetzt, welches auf Windows XP basiert und für die besonderen Anforderungen von Thin Clients optimiert wurde.

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.

9.2. 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. Daher wird die von der Fa. Dr. Kaiser angebotene softwarebasierende Wächterlösung "PC-Drive" als Schutz für alle Rechner im unterrichtlichen Bereich eingesetzt.

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.

Konzeptionelle Änderungen beim Einsatz der Wächtersoftware im Rahmen des Projektes zur Einführung von Windows 7 werden nicht ausgeschlossen, können aber zum jetzigen Zeitpunkt noch nicht beurteilt werden. Eine eventuelle Anpassung erfolgt in Abstimmung mit der Lenkungsgruppe und dem Amt für Schule und Weiterbildung.

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. Eine Ausnahme stellt die Plattform für die Aktualisierung von Standard-Software (PASS) dar (siehe unter 9.6.).

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.

9.3. Betriebssystem

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

Die Fa. Microsoft wird für Windows XP noch bis zum 08.04.2014 einen „Extended Support“ gewähren. Die Unterstützung mit aktuellen Sicherheitspatches ist damit dauerhaft gewährleistet, obwohl bereits mit Windows 7 ein Nachfolge-Betriebssystem zur Verfügung steht.

Alternative Betriebssysteme 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 300 Programme und Installationsroutinen vor, die unter Windows XP getestet wurden. Für sämtliche Produkte müssen für ein anderes Betriebssystem neue oder angepasste Installationsroutinen geschaffen werden

Zurzeit wird Windows 7 (64-bit) für den Einsatz im MEP getestet. Da dieses Betriebssystem nicht von ZENworks für Desktops (ZfD) unterstützt wird, wird zeitgleich zur Umstellung des Betriebssystems der Einsatz von ZENworks Configuration Management (ZCM) notwendig sein.

Aufgrund einer grundsätzlich abweichenden Struktur in weiten Bereichen des ZCM sowie des Einsatzes der 64-Bit-Version von Windows 7 sind alle Installationen pädagogischer Software zu überprüfen und umzustellen. Zudem muss eingesetzte Hardware auf ihre Kompatibilität in der 64-Bit-Umgebung getestet werden.

9.4. Clientsoftware

9.4.1. 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 und Mozilla Firefox
 - o Freeware-FTP-Client: FileZilla

- Multimediaprogramme:
 - o Windows MediaPlayer
 - o PowerDVD
 - o Quicktime Viewer
 - o MM-Dateibetrachter IrfanView
- Hilfsprogramme
 - o Freeware-Packer bzw. -Archivierer (z. Z. 7-Zip)
- Laufzeitumgebungen:
 - o Sun Java Runtime Environment
 - o Microsoft .Net-Framework
 - o Microsoft .Net-Visual J
- 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.

9.4.2. 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 eingerichtet mit der Möglichkeit,
- 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.

9.4.3. Servergespeicherte Profile (Roaming-Profiles)

Für Nutzer, die an wechselnden Arbeitsplatzrechnern arbeiten (Roaming-Users), besteht die Möglichkeit ihre Arbeitsumgebung an zentraler Stelle zu speichern. Windows XP Prof. bietet dafür "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 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.

9.4.4. 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.

9.4.5. 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.

9.5. 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.

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 Wächtersoftware 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. Während des Installati-

onsvorganges ist es notwendig, dass ein Ansprechpartner / eine Ansprechpartnerin vor Ort erreichbar ist, um ggfs. manuell einzugreifen zu können (z. B. Rechnerneustart).

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.

9.6. Plattform für die Aktualisierung von Standard-Software (PASS)

Zurzeit finden die finalen Tests der Plattform für die Aktualisierung von Standard-Software (PASS) statt. Bei PASS handelt es sich um ein webbasiertes System, mit dem IT-Kontaktlehrern die Möglichkeit gegeben wird, von der citeq vorbereitete Systemsoftware und –updates (z. B. Microsoft Internet Explorer, Adobe Flashplayer, Java Runtime Environment) eigenverantwortlich und in selbst festgelegten Zeitfenstern auf einzelne Rechner oder Rechnergruppen (z. B. Computerräume) zu verteilen.

Nachdem über das Web-Interface die zu installierende Software und die Rechner ausgewählt wurden, auf denen diese Software installiert werden soll, werden die Rechner manuell oder per Wake-on-Lan eingeschaltet. Im Rahmen des automatischen Prozesses

wird u.a. der Wächterschutz ausgeschaltet, die gewählte Software installiert, der Wächterschutz wieder eingeschaltet und der/die Rechner zum Abschluss heruntergefahren.

Während der Installationsphase, in der der Wächterschutz deaktiviert ist, werden Tastatur und Maus mittels eines Tools (z. Z. Computer Lock Up) gesperrt.

9.7. Info-Displays

Beim Info-Display handelt es sich um ein elektronisches "Schwarzes Brett", über das Informationen zu tagesaktuellen Ereignissen wie z. B. Vertretungen oder Unterrichtsausfälle, aber auch Veranstaltungshinweise oder Klausurtermine publiziert werden können.

Hardwareseitig können sowohl PC als auch Thin Clients zum Einsatz kommen. Auf Grund ihrer platz- und energiesparenden Bauweise wird der Einsatz von Thin Clients präferiert. Diese sind für diesen speziellen Einsatzzweck besonders geeignet (siehe unter 9.1. "Hardwareausstattung"). Mit ihnen können die Info-Displays wirtschaftlicher gesteuert werden als mit PC.

Die Darstellung (i. d. R. Web-Inhalte, die aus entsprechenden Stundenplan-Anwendungen (z. B. gp-Untis) generiert werden) erfolgt über TFT-Monitore oder LCD-Fernseher im Ein- oder Mehr-Monitor-Betrieb. Beim Mehr-Monitor-Betrieb wird der Windows-Desktop eines Rechners auf mehreren Monitoren dargestellt.

Bei baulichen Situationen, in denen der Abstand zwischen Rechner und Monitor mehr als 3 Meter beträgt, wird das Videosignal mittels VGA-to-LAN-Adaptern über das bestehende Netzwerk übertragen, um Qualitätsverluste in der Darstellung zu vermeiden.

10. Technisches Betriebskonzept

10.1. 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.

10.2. 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:

- über die telefonische Hotline der citeq,
- über das webbasierte Meldungssystem Service-Desk-System.

Aufgrund der in allen Schulen ähnlichen Zeitfenster (=Unterrichtspausen) ist die telefonische Störungsannahme über die Telefonhotline oftmals durch die Anzahl freier Telefonleitungen bzw. die im Service-Desk verfügbare Personalkapazität limitiert. Daher sollte von den IT-Koordinationen der Schulen regelmäßig die Störungsmeldung über das webbasierte Meldungssystem einer telefonischen Meldung vorgezogen werden.

Zur weiteren Verbesserung der Kommunikation im Störfall stellt die citeq im „MEP-net“ ein Webformular bereit, welches die Eingabe einer Störungsmeldung auch ohne vorherige Anmeldung an das Service-Desk-System erlaubt. Damit ist eine Störungsmeldung nicht nur durch die IT-Kontaktlehrer, sondern durch jeden Lehrer oder das Sekretariat möglich. IT-Kontaktlehrer werden über das Service-Desk-System von solcherart eingegangenen Störungsmeldungen informiert und bei Rückfragen im Rahmen des Entstörungsvorganges durch die Hotline direkt angesprochen.

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 Störungsnahme,
- Entstörungsversuch durch Fernbedienen (Remote Control) der gestörten Geräte in Absprache mit dem Meldenden,
- Aufzeigen einer möglichen temporären Fehlerumgehung („WorkAround“) bis zur Ent-störung,
- Aufnahme eines Auftrags 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. Über das MEP-net besteht zudem die Möglichkeit, in dringenden Fällen Störungen über ein vereinfachtes Meldeformular aufzugeben.

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.

10.3. 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.

10.4. 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 Kom-

ponenten,

- 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.

10.5. 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.

10.6. 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.

10.7. Operationsmanagement

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 sind.

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

10.7.1. 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-System 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.

10.7.2. 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-System 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.

10.7.3. Aufgaben der IT-Kontaktlehrer

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 (IT-Kontaktlehrer) 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-Kontaktlehrer 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 der Service-Desk-Aufträge,
- Anschluss und Einschaltung nicht permanent genutzter Endgeräte (z.B. Laptops) zu Installationszwecken,
- 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 Fortbildungen/Workshops zum Erfahrungsaustausch.

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

Der IT- Kontaktlehrer 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- Kontaktlehrer siehe unter 8.8. "Rechte der IT-Kontaktlehrer".

10.7.4. 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.

10.7.5. 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.

10.7.6. 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 Verwaltungs- und Pädagogiknetze hält die citeq jeweils einen Ersatzserver lagerseitig vor.

10.7.7. Störungen zentraler Dienste

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

10.7.8. Störungen von Client-Rechnern

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

Auftretende Störungen werden über das Service-Desk-System bearbeitet.

Glossar

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

Authentifizierung

Authentifizierung ist der Vorgang der Überprüfung der behaupteten Identität eines Gegenübers, beispielsweise einer Person oder eines Computersystems in einem Dialog. Authentisierung hingegen ist der Vorgang des Nachweises der eigenen Identität.

Browser-basiert

Browser-basierte Programme benötigen keine zusätzliche Installation, sondern kommen ohne Zusätze aus. Sie greifen ausschließlich auf die Fähigkeiten des Browsers z.B. XML zurück.

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-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.

Ethernet

Ethernet ist eine Technologie, die Software und Hardware für kabelgebundene Datennetze spezifiziert, welche ursprünglich für lokale Datennetze (LANs) gedacht war und daher auch als LAN-Technik bezeichnet wird. Sie ermöglicht den Datenaustausch in Form von Datenpaketen zwischen den in einem lokalen Netz (LAN) angeschlossenen Geräten. Derzeit sind Übertragungsraten von 10 Megabit/s, 100 Megabit/s (Fast Ethernet), 1000 Megabit/s (Gigabit-Ethernet) bis 10 Gigabit/s spezifiziert.

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.

Freeware

Freeware bezeichnet im allgemeinen Sprachgebrauch Software, die vom Urheber zur kostenlosen Nutzung zur Verfügung gestellt wird.

galvanische Trennung

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

Inhouseverkabekung

Die In-House-Verkabelung ist ein Teil des Basisanschlusses die als Bus angelegt ist und die Endgeräte mit dem NTBA verbindet. Sie wird S₀-Bus genannt und besteht aus zwei Doppeladern. Sie gehört dem Anschlussinhaber, der für ihre Funktion selbst verantwortlich ist.

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 Protocoll 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 Switche 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.

LWL

Lichtwellenleiter sind aus Lichtleitern bestehende oder zusammengesetzte, mit Steckverbindungen versehene Kabel und Leitungen zur Übertragung von Licht in der Nachrichtentechnik.

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.

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 Informati-

onen gezielt erzeugt, damit beim Ausfall einzelner Komponenten das RAID als Ganzes seine Funktionalität behält.

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 ist ein Netzwerkprotokoll 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.

Smartboard

Ein digitales Whiteboard ist eine elektronische Tafel, die an einen Computer angeschlossen wird. Das Bild wird im Regelfall von einem Beamer projiziert. Das interaktive Whiteboard stellt nun über Sensoren ein Koordinatensystem dar, das es ermöglicht, einen Computer mit all seinen Funktionen und für alle sichtbar einzusetzen; also im Prinzip einen Bildschirm darstellt.

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.

Stand-Alone

Mit dem englischen Begriff Stand-Alone (deutsch: *alleine stehend*) bezeichnet man Geräte, Hardware oder Software, die eigenständig, ohne weitere Zusatzgeräte, ihre Funktion erfüllen können.

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.

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.

Wake-On-Lan

Wake on LAN (kurz WOL) ist ein 1995 von AMD in Zusammenarbeit mit Hewlett-Packard veröffentlichter Standard, um einen ausgeschalteten Computer über die eingebaute Netzwerkkarte zu starten.

