Empfehlungen für Einrichtung von öffentlichen Computer- oder Netzarbeitsplätzen

Arbeitsgruppe öCNAP im DINI eV

Oktober 2004

Präambel

Hochschulen und Bibliotheken stellen eine Vielzahl von Diensten auf der Basis von IuK-Technik zur öffentlichen Nutzung bereit. Um allen Benutzern ein breites Servicespektrum anbieten zu können und Synergieeffekte im Management zu erzielen, sollten alle elektronischen Dienste innerhalb einer Organisation koordiniert, übergreifend verwaltet und einheitlich angeboten werden. Dazu dienen die folgenden Empfehlungen, die sich an Serviceeinrichtungen innerhalb einer Hochschule – insbesondere Rechenzentren, Bibliotheken und Medienzentren – oder sonstige öffentliche Einrichtungen richten. Sie umfassen rechtliche, organisatorische und technische Hinweise und verfolgen die Ziele,

- eine Orientierungshilfe beim Betrieb von öffentlichen Computer- und Netzarbeitsplätzen zu bieten,
- eine Entscheidungshilfe für Planungen zur Einrichtung von öffentlichen Computer- und Netzarbeitsplätzen zu geben,
- gemeinsame organisatorische Rahmenbedingungen und Standards zu formulieren.

Öffentliche Computer- oder Netzarbeitsplätze (öCNAPs) im Sinne dieser Empfehlungen sind elektronische Arbeitsplätze in Serviceeinrichtungen, die einen sicheren, zuverlässigen, schnellen und im Rahmen der finanziellen Möglichkeiten technisch aktuellen Zugang zu öffentlichen elektronischen Diensten bieten. Sie werden von unterschiedlichen Personen mit unterschiedlichen Berechtigungen genutzt. Einschränkungen in der Nutzung sind so weit wie möglich zu vermeiden, können sich aber aus technologischen, finanziellen, sicherheitstechnischen oder rechtlichen Gesichtspunkten ergeben.

Gliederung

1. Dienste

Öffentliche Computer- und Netzarbeitsplätze dienen den Benutzern einer Einrichtung

- zur Recherche nach Informationen,
- zum Abruf und Speichern von Informationen,
- zur Bearbeitung und Bewertung von Informationen,
- zur Erstellung und Veröffentlichung von Informationen.

Hierzu werden öCNAPs frei und uneingeschränkt zur Verfügung gestellt, sofern nicht Einschränkungen zwingend erforderlich sind. Gründe für eventuell notwendige Beschränkungen sind in Abschnitt 3 aufgeführt. Konkurrenzsituationen zu kommerziellen Anbietern mit ähnlichen Dienstangeboten sollten vermieden werden (Internet-Cafe, Copyshop). Die verschiedenen Dienste können zur anonymen oder authentifizierten Nutzung bereitgestellt werden. Sie lassen sich in folgende Kategorien einteilen:

- uneingeschränkter Zugang zum Internet
- eingeschränkter Zugang zum Internet durch Ausschluss bestimmter Informationsdienste („Negativlisten“)
- Zugang zu ausgewählten Informationsdiensten im Internet („Positivlisten“)
- Zugang zum Intranet und damit zu den elektronischen Diensten, die nur innerhalb der Einrichtung und nicht von außen genutzt werden können
- Zugang zu kostenpflichtigen Diensten im Internet (z.B. kostenpflichtige Datenbank-Recherchen)
- Nutzung von lizenzierter Software
- Nutzung von freier Software
- Zugang zu spezieller Peripherie
- Zugang zu zentralen IT-Services (Fileservice, Computeservice usw.)
- Erstellung elektronischer Publikationen
- Zugang zu Diensten mit speziellen Anforderungen an die Sicherheit und/oder an den Datenschutz
- Verwaltungsprozesse (Anmeldung, Ausleihe usw.)

Die Dienste können realisiert werden mit öCNAPs der folgenden Form:

- Arbeitsplätze für alle IT-Standarddienste
- Arbeitsplätze für eingeschränkte IT-Dienste
- Hochwertige Multimediaarbeitsplätze mit Peripheriegeräten
- Arbeitsplätze zum Anschluss eines eigenen Gerätes (Notebook) an ein Fest- oder Funknetz
- Arbeitsplätze in Clusterräumen zu Schulungs- und Ausbildungszwecken

2. Authentifizierung

Die Authentifizierung von Benutzern für die Benutzung von Diensten an öCNAPs kann auf Grund rechtlicher, kapazitiver oder sicherheitsrelevanter Gegebenheiten notwendig sein. Sie erfolgt in Abhängigkeit der Rolle, die die Benutzer einnehmen bzw. der Benutzergruppen, zu denen sie gehören (z.B. angemeldeter Benutzer, Gast, Student, usw.).

Grundsätzlich wird empfohlen, die Benutzergruppen im Rahmen eines einheitlichen Identitätsmanagements der Serviceeinrichtung festzulegen. Dabei sind zur Minimierung des Personalaufwands elektronische Verfahren den manuellen vorzuziehen. Insbesondere muss die Möglichkeit zeitnaher Identitätsänderungen (Anmeldung, Abmeldung) berücksichtigt werden.

Für eine Empfehlung hinsichtlich des Zeitpunktes und der Qualität der Authentifizierung in Abhängigkeit der angebotenen Dienste sind bei öffentlichen Einrichtungen der gesetzliche Auftrag und die sich daraus ergebenden Benutzerordnungen maßgebend.
Aus diesem Grund werden öffentliche Dienstleister hier in 3 Gruppen eingeteilt:

a) Einrichtungen mit allgemeinem öffentlichen Auftrag (typisch sind hier öffentliche und Landesbibliotheken)
b) Einrichtungen mit spezifischem öffentlichen Auftrag (typisch zentrale universitäre Dienstleister Universitätsbibliothek UB, Universitätsrechenzentrum URZ, usw.)
c) Einrichtungen mit speziellem öffentlichem Auftrag (typisch Computerpools in Instituten)

Die Qualität der Authentifizierung wird wie folgt unterschieden:
(-) keine Authentifizierung (anonymer Zugang, freier Zugang)
(X) einfache Authentifizierung (Kennung und Passwort, Benutzerausweis)
(Z) Zertifikats-basierte Authentifizierung

Die Einrichtung muss entscheiden, ob sie einen anonymen Zugang zum Internet zulässt. Dabei ist das Recht auf freie Informationsgewinnung und auch auf eine anonyme Informationsbeschaffung abzuwägen gegenüber einem authentifizierten Zugang, der es bei vorliegendem Missbrauch ermöglicht, den Verursacher festzustellen.
Eine Zertifikats-basierte Authentifizierung kann in mehreren Abstufungen erfolgen (z.B. auf der Basis einer einfachen, fortgeschrittenen oder qualifizierten Signatur, Art der Einbindung der PKI usw.). Sie wird hier nicht weiter spezifiziert, da sie nur bei wenigen Anwendungen eine Rolle spielen wird.

Angebotener Dienst	Einrichtungsgruppe		
	a	b	c
Uneingeschränkter Zugang zum Internet	- / X[1]	- / X[1]	X
Eingeschränkter Zugang zum Internet (Negativliste)	- / X[1]	- / X[1]	X
Ausgewählte Informationsdienste im Internet (Positivliste)	-	-	X
Zugang zum Intranet	-	-	X
Zugang zu kostenpflichtigen Diensten im Internet	X	X	X
Nutzung lizenzierter Software	- / X	- / X	X
Nutzung freier Software	-	-	X
Zugang zu spezieller Peripherie	X	X	X
Zugang zu zentralen IT-Services (Fileservice, Computeservice usw.)	X	X	X
Erstellung elektronischer Publikationen	X / Z	X / Z	X / Z
Zugang zu Diensten mit speziellen Anforderungen an die Sicherheit und / oder an den Datenschutz	Z	Z	Z
Verwaltungsprozesse (Anmeldung, Ausleihe usw.)	X / Z	X / Z	X / Z
Arbeitsplätze für alle IT-Standarddienste	- / X	- / X	X
Arbeitsplätze für eingeschränkte IT-Standarddienste	-	-	X
Hochwertige Multimedia Arbeitsplätze	X	X	X
Anschluss eines eigenen Notebooks	- / X[1]	- / X[1]	X
Arbeitsplätze in Clusterräumen zu Schulungs- und Ausbildungszwecken	- / X	- / X	X

Tabelle: Empfehlung zur Authentifizierung bei angebotenen Diensten

[1] je nach Entscheidung der Einrichtung für oder gegen einen anonymen Zugang zum Internet.

3. Betriebsorganisation

ÖCNAPs können innerhalb einer Institution von verschiedenen Einrichtungen betrieben werden (z.B. Bibliothek, Rechenzentrum). Dabei ist auf einheitliche betriebliche Rahmenbedingungen zu achten. Die Systemadministration kann dabei zentral auch für dezentrale öCNAPS oder öCNAP-Cluster erfolgen.

Zur Betriebsorganisation gehören Öffnungszeiten und deren betriebliche Absicherung, Maßnahmen zur Nutzungskontrolle und zur Nutzungsbeschränkung sowie Beratungs- und Supportstrukturen.

Öffnungszeiten

Im Idealfall sind die öCNAPs 24 h am Tag 7 Tage die Woche zugänglich und benutzbar. Auch bei einem grundsätzlichen Betrieb in Selbstbedienung ergeben sich Reduktionen insbesondere aus Gründen nicht ausreichend zur Verfügung stehender personeller Betreuung:

- unzureichende Sicherheit der Geräte und Installationen (Zerstörung/Vandalismus, Diebstahl, Benutzung ohne „optische Kontrolle aus der Ferne“ usw.)
- Notwendigkeit des Eingreifens bei Fehlern/Havarien
- Einhalten der Benutzungsordnung
- notwendige qualifizierte Beratungskapazität
- Verknüpfung mit anderen Diensten, die Personal erfordern (z.B. Bibliotheksdienste)

Bedarf und Aufwand sind zu kalkulieren und einander gegenüber zu stellen.
In den Räumen sind sicherheitsrelevante Hinweise (zum Brandschutz, zum Verhalten in Notfällen, usw.) auszuhängen.

Nutzungskontrolle und -beschränkung

Gründe für die Notwendigkeit einer Nutzungskontrolle und –beschränkung bezogen auf:

- Dienste
  - lizenzrechtliche Gründe
  - Sicherheit (inkl. Sicherheit der Installation)
  - Kapazität des Angebots
  - Verfügbarkeit
  - Aufwand in der (personellen) Betreuung
  - Absicherung kostenpflichtiger Dienste
  - Sperrung von Diensten aus rechtlichen Gründen (Benutzungsordnung)
  - Qualifizierung in der Benutzung
  - Steuerung des Bedarfs durch den Betreiber
- Räume
  - Sicherheit
  - Reservierungen für Veranstaltungen
  - Öffnungszeiten des Gebäudes
  - aktive/passive Störungen anderer/durch andere Bereiche (z.B. Lautstärke)
- Geräte
  - Sicherheit
  - Kapazität in Anzahl und Ausstattung
  - Verfügbarkeit
  - Qualifizierung in der Benutzung

Realisierung einer Nutzungskontrolle und –beschränkung:

- Grundsätzlich können Nutzungsbeschränkungen durch positive (es werden explizit die erlaubten Dienste zugelassen - Positivliste) oder negative Maßnahmen (es werden explizit die nicht erlaubten Dienste gesperrt, alles was nicht gesperrt ist, ist erlaubt - Negativliste) umgesetzt werden. Beispiel: über Ports spezifizierbare Internet-Dienste können über eine Firewall oder über Filter des Netzrouters explizit zugelassen oder ausgeschlossen werden.
- durch Authentifizierung
- durch dedizierte Arbeitsplätze, die nur eine spezielle Nutzung zulassen oder bestimmte Nutzungen ausschließen
- durch beaufsichtigendes Personal
- Öffnungszeiten

Beratung und Support

Das Angebot von Beratung und Support ist aus rechtlichen Gründen (Einhaltung der Benutzungsordnung durch die Benutzer), zum Schutz der eigenen Installationen und als zusätzliche Dienstleistung vorzuhalten. Dazu gehören

- elektronische Informationssysteme
- Informationsblätter, Aushänge usw.
- Ansprechpartner
- Schulungen und Kurse
- Podium für Hinweise der Benutzer
- Trouble Ticket System

4. Installation/Pflege

Im Folgenden werden technisch orientierte Hinweise für öCNAPs gegeben. Teilweise sind nur Kategorien aufgeführt, weil eine weitere Detaillierung den Rahmen dieser Empfehlungen sprengen würde.

- **Hard- und Software der elektronischen Arbeitsplätze - unterschieden nach DV-Technik:**
  - Hardware (Rechnerplattform, Ausstattung, PC/Terminal, Medienanschluss, lokale Peripherie usw.)
  - Betriebsystem (Windows, Linux, sonst. Unix, MacOS usw.)
  - Anwendungssoftware
  - Netzwerk (LAN, Terminalserver)
  - Netzanschluss (Protokoll, Kabel/WLAN)
  - Persönliche Computertechnik (Strom-/Netzanschluss für Notebooks, Kabel, WLAN usw.)
- **Möglichkeiten der automatisierten Installation von öCNAPs:**
  - Terminalserver-Betrieb
    Der Terminalserver stellt eine Server-basierte Verarbeitungslösung auf Windows-Basis dar. Bei dieser Lösung werden die Anwendungen vollständig auf dem Server implementiert, verwaltet, unterstützt und ausgeführt. Die Client-Geräte dienen nur zur Interaktion. Veränderungen in den Installationen haben sofort Auswirkungen auf alle angeschlossenen Clients.
    Für einen „überschaubaren“ Bereich von öCNAPS ist der Einsatz von Windows Terminal Server 2003 (keine frühere Version) ausreichend, bei größeren Installationen oder bei sich stark unterscheidenden Client-Plattformen wird zusätzlich der

Einsatz von Citrix MetaFrame empfohlen.
Folgende Nachteile bzw. Probleme sind zu festzustellen:
- starke Abhängigkeit des gesamten Betriebes von der Verfügbarkeit und Bandbreite des Netzes
- zusätzliche Kosten für Citrix MetaFrame
- Lizenzierung der Anwendungen (nicht alles technisch Machbare ist lizenzrechtlich gestattet)
- dedizierte Arbeitsplätze mit sich unterscheidenden Diensten

- Spiegelung von Festplatten
  Bei dieser Technologie wird von einer Installation (Partition) ein Image erzeugt, das auf weitere PC-Arbeitsplätze übertragen wird (z.B. Drive Image von PowerQuest, Norton Ghost)
  Folgende Nachteile bzw. Probleme sind festzustellen:
  - Die Hardware-Plattform der Arbeitsplätze muss relativ identisch sein
  - Nach dem Klonen sind Nacharbeiten notwendig (SetID, IP-Adresse, Computername usw.), diese sind über Skripte automatisierbar
  - Die Images sind relativ groß (die Hälfte bis zwei Drittel des belegten Bereiches der Partition)
  - keine Unterstützung des Handlings von Lizenz-Spezifika
- Automatisierte Installation
  Installation des Betriebssystems und von Anwendungen (z.B. Remote Installation Service von MS, On Command CCM, WinMason)
  Folgende Nachteile bzw. Probleme sind zu festzustellen:
  - zeitaufwändig in der Skript-Erstellung
  - zeitaufwändig in der Installation
- Netzwerkinstallation
  die „SETUP /N“-Methode
  Folgende Nachteile bzw. Probleme sind zu festzustellen:
  - nur wenige Anwendungen sind so installierbar
  - individuelle Anpassungen schwierig bis unmöglich
- Manuelle Installation
  funktioniert immer und überall, keine große Einarbeitung oder Vorbereitung notwendig
  Folgende Nachteile bzw. Probleme sind zu festzustellen:
  - zeitaufwändig
  - skaliert extrem schlecht

5. Sicherheit/Schutz

Die Geräte der Serviceeinrichtung sowie die mitgebrachten Geräte der Benutzer sind vor Diebstahl, Veränderungen und Ausspähungen zu schützen. Regelungen und Maßnahmen zum Datenschutz und zur Datensicherheit, die sich aus dem Datenschutz- und Telekommunikationsgesetz ergeben, sind vorzunehmen.

Folgende Spezifika beim Betrieb von öCNAP sind besonders zu berücksichtigen:

- **Schutz der Geräte der Serviceeinrichtung vor Diebstahl**
  Kann keine Aufsicht gewährleistet werden, müssen elektronische (über Alarmsysteme) und / oder mechanische Maßnahmen vorgenommen werden.
- **Schutz der Geräte der Serviceeinrichtung gegen Veränderungen durch Benutzer**
  Eine Stabilität der Konfiguration gegenüber Änderungen der Benutzer kann

auf zwei Arten erreicht werden. Zum einen kann versucht werden, durch entsprechende Systemeinstellungen Änderungen zu verhindern. Zum anderen können Änderungen durch Rückführung in einen definierten Ausgangszustand neutralisiert werden. Zur ersten Kategorie gehören Terminalserverlösungen (s. Abschnitt 4) oder Wächterkarten. Zur zweiten Kategorie gehören Boot-Images, die von geschützten Servern aus bei jedem neuen Benutzer geladen werden.

- **Schutz der öCNAPs vor Schadenssoftware (Malware)**
  Hier sind technische Sicherungen analog zu anderen Computernetzen vorzusehen, wie Serversicherheit, Reproduzierbarkeit der Installationen, Virenscanner, Firewalls, Verfahren für Patch-Einspielungen, Installationsbeschränkungen usw.
- **Schutz anderer Geräte im Netz der Serviceeinrichtung vor Hackern und Malware durch mitgebrachte mobile Geräte**
  Hierzu kann man in der Serviceeinrichtung unbekannte Geräte vor deren Netzzugang gegen einen speziellen Server auf eine aktuelle und sichere Konfiguration, also u.a. auf Vollständigkeit der Updates und auf Virenfreiheit prüfen. Mobile Geräte sollten bei Anschluss an das Netz auf einen Subnetzbereich beschränkt bleiben (z.B. mittels eigenem VPN).
- **Schutz mitgebrachter mobiler Geräte der Benutzer**
  Hier muss sichergestellt werden, dass mitgebrachte mobile Geräte nicht aus dem Netz der Serviceeinrichtung verseucht werden. Hier sind entsprechende Empfehlungen für den Einsatz eines Virenscanners und einer lokalen Firewall zu geben, für deren Einsatz der Benutzer allerdings selber verantwortlich ist. Entsprechende Haftungsausschlüsse sind in den Nutzungsregeln zu formulieren.
- **Schutz der Authentifizierungsinformationen (in der Regel Benutzerkennungen und Passwörter)**
  Hier sind Empfehlungen für einen Mindest-Sicherheitsstandard der Passwörter durch einen komplexen Aufbau zu geben. Durch entsprechende Tools können sowohl der Zeitpunkt (z.B. Passwortwechsel spätestens nach 6 Monaten, sonst Sperrung des Accounts) als auch ein gefordertes Sicherheitslevel (z.B. minimale Länge, Buchstaben und Sonderzeichen und Ziffern gefordert, Dudenwörter ausgeschlossen) automatisch erzwungen werden.
  Passwörter sind grundsätzlich nur verschlüsselt zu übertragen. Wünschenswert ist die Übertragung über gesicherte Verbindungen.
- **Informationspflicht gegenüber dem Benutzer**
  Der Benutzer muss zum einen über die von der Serviceeinrichtung durchgeführten, zum anderen über die von ihm geforderten Sicherungsmaßnahmen aktuell informiert werden.

6. Kostenpflicht/Bezahlungen

Der Zugang zu Informationen über einen öCNAP sollte grundsätzlich kostenlos sein. Gründe für eine Kostenpflicht von Diensten können allenfalls Beiträge zur Kostendeckung sein, wobei ein direkter Bezug zwischen Kosten und Leistungen erkennbar sein muss. Auch kostenpflichtige Dienste müssen kurzfristig nutzbar sein. Zudem ist der Aufwand für das Inkasso zu beachten. Von daher kommt nur ein direktes Inkasso (Barzahlung an einer Theke, Geldeinwurf in Druckautomaten oder die Nutzung einer Geldkarte) in Frage. Die Kosten können pauschal (z.B. für Support), zeitabhängig (z.B. für den reinen Internetzugang) oder verbrauchsabhängig (z.B. zum Drucken) verrechnet werden.

Kostenpflichtige Dienste können ausgelagert werden (von einer Firma betriebene Druckstationen oder Drucken in einem Copyshop mit vorherigem Filetransfer).

7. Rechtliche Hinweise/Ordnungen

Die Benutzung von öCNAPs ist durch entsprechende Ordnungen/Regelungen bzw. durch gesetzliche Vorgaben sowohl für den Betreiber als auch für die Benutzer rechtlich abzusichern. Dabei sind folgende Aspekte zu berücksichtigen:

Benutzungsordnung

Die lokale Benutzungsordnung setzt gesetzliche Vorgaben nicht außer Kraft. Sie dient der Ergänzung insbesondere in Bezug auf lokale Besonderheiten. Folgendes ist zu regeln:

- Gegenstand und Geltungsbereich
- Art des Nutzungsverhältnisses (z.B. öffentlich/rechtlich)
- Benutzungsberechtigung und Zulassung zur Benutzung/Benutzungserlaubnis
- Rechte und Pflichten der Benutzer und der Betreiber
- Spezielle Regelungen für die Benutzung von Datennetzen
- Spezielle Regelungen für die Benutzung von Hard- und Software
- Verhalten in den Räumen
- Haftung und Haftungsausschluss
- Ausschluss von der Benutzung

Gebühren- bzw. Entgeltordnung

Gebühren legen eine Ordnung nahe. Entgelte sind in der Regel eine Erstattung der Kosten für die Inanspruchnahme von Leistungen. Festzulegen sind:

- Gegenstand und Geltungsbereich
- Benutzergruppen
- Gebührenbemessung
- Fälligkeit, Stundung, Erlass
- Berechnungsgrundlagen bzw. Gebührentabelle

gesetzliche Randbedingungen

- Zivilrechtliche Haftung
- Strafrechtliche Verantwortlichkeit (z.B. Ausspähen von Daten (§ 202 a StGB); Verletzung des Datenschutzes (§ 32 BlnDSG, § 43 - 44 BDSG); Datenveränderung (§ 303 a StGB) und Computersabotage (§ 303 b StGB); Computerbetrug (§ 263a StGB); Verbreitung pornographischer Darstellungen (§ 184 StGB), insbesondere Abruf oder Besitz kinderpornographischer Darstellungen (§ 184 Abs. 5 StGB); Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB) Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB); Strafbare Urheberrechtsverletzungen, z. B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG))
- Haftung für Inhalte
- allg. Datenschutz

Checklisten und Muster

- Recht im DFN (-Verein):
  http://www.dfn.de/content/beratung-weiterbildung/rechtimdfn/
- Checkliste für Rechenzentren (DFN-Verein):
  http://www.dfn.de/content/beratung-weiterbildung/rechtimdfn/checkliste/

- Entwurf einer Muster-Benutzungsordnung für Universitätsrechenzentren und sonstige wissenschaftliche Forschungseinrichtungen im Deutschen Forschungsnetz: http://www.dfn.de/index.jsp?mode=print&id=17669

8. Links und Verweise

Alle Einrichtungen, die öCNAPs betreiben, sind aufgerufen, Informationen zu den Bereichen

- angebotene Dienste
- Authentifizierung
- Betriebsorganisation
- Installation und Pflege
- Sicherheit
- Kostenregelungen
- Benutzungsordnungen

in einschlägigen Web-Seiten und Mailing-Listen bereitzustellen und ständig aktuell zu halten. Hierbei sind besonders auch Details und technische Realisierung von breitem Interesse. Um eine größtmögliche Verbreitung zu gewährleisten, sollen dazu folgende bereits etablierte Plattformen benutzt werden:

Bereich Bibliotheken:

Plattform:	Forum Benutzung des deutschen Bibliotheksverbands
Inhalt:	Dokumente, Projekte, Links zur Bibliotheksbenutzung
URL:	http://www.forum-benutzung.de
Arbeitsbereich:	9.2 Computerarbeitsplätze
Realisierung:	Dokumentenverwaltungssystem BCSW Gastzugang zum Lesen von Dokumenten Registrierter Zugang zum Einstellen von Dokumenten Abgabeformular zum Einstellen von Dokumenten ohne Registrierung

Mailing-Liste:	Inetbib
URL:	http://www.inetbib.de
Inhalt:	Internetnutzung in Bibliotheken
Realisierung:	Anmeldung per Mail an majordomo@ub.uni-dortmund.de Text: subscribe inetbib end

Checkliste „Internet in den Universitätsbibliotheken“ NRW Mai 2000
http://www.hrz.uni-dortmund.de/DINI-WS/NRW-Checkliste.html

Bereich Rechenzentren:

Zki-Atlas
http://zki-atlas.uni-duisburg.de

Hier wird eine entsprechende Kategorie eingerichtet.