Deutsche Initiative für Netzwerkinformation e.V. (DINI)

Arbeitskreis "Umgang mit öffentlichen Computer- und Netzarbeitsplätzen (öCNAP)"

Umfrage zu Betriebskonzepten für öffentliche Computer- und Netzarbeitsplätze

Januar 2007

Die DINI-Arbeitsgruppe „Umgang mit öffentlichen Computer- und Netzarbeitsplätzen (öCNAP)“ führte vom 13.6. bis 27.9.2006 eine Umfrage durch. Sie richtete sich an Bibliotheken, Rechenzentren und vergleichbare Hochschuleinrichtungen. Ziel der Umfrage war eine Bestandsaufnahme der für den Betrieb öffentlicher Computer- und Netzarbeitsplätze eingesetzten Konzepte. Grundlage dafür waren die von der Arbeitsgruppe erarbeiteten Empfehlungen für die Einrichtung von öffentlichen Computer- oder Netzarbeitsplätzen (http://www.dini.de/documents/oecnap_102004_final.pdf) von Oktober 2004.

Gliederung

1. Umgang mit der Umfrage

Die große Beteiligung an der Umfrage mit fast 150 Teilnehmern hat den Arbeitskreis dahingehend bestätigt, dass die angesprochene Problematik von vielen Einrichtungen gesehen wird und auf großes Interesse stößt.

Da bei der Umfrage auch Ansprechpartner in den Einrichtungen erfragt wurden, stellt die aufgebaute Datenbasis eine umfangreiche Informationsquelle dar, die den Mitgliedseinrichtungen verfügbar gemacht werden kann. Über die Arbeitsgruppe kann dabei eine Zuordnung von Betreiber und Lösung erfolgen.

Haben Sie Fragen zu der Umfrage und ihrer Auswertung oder möchten Sie Informationen / Ansprechpartner zu speziellen Themenbereichen, so wenden Sie sich bitte an die Arbeitsgruppe

ocap@dini.de

Die mit der Umfrage gesammelten 50 URLs zu den Verwaltungs- und Benutzungsordnungen der Einrichtungen werden über die DINI-Webseite verfügbar gemacht.

Weiterhin ist unter

http://wiki.uni-due.de/ocap

ein Wiki für die Arbeitsgruppe eingerichtet worden.

2. Überblick / Teilnehmerkreis

Der Fragebogen wurde auf Grundlage der Software Globalpark erstellt und webbasiert verfügbar gemacht. Er umfasst 31 Fragen. Das Ausfüllen erforderte ca. 15 Minuten. Die Erstellung und Durchführung erfolgte mit Unterstützung von Herrn Dipl.-Soz.-Wiss. Karl-Heinz Stammen vom Zentrum für Hochschul- und Qualitätsentwicklung der Universität Duisburg-Essen.

Das System Globalpark war schnell erlernbar und die Erstellung des Fragebogens auch für Nicht-Fachleute einfach. Teilnehmer wurden frei geschaltet und per Mail aufgefordert den Fragebogen auszufüllen.

Nachteilig war, dass der Teilnehmer den Fragebogen vorher nicht anschauen konnte. Beendete man die Internet-Sitzung nach ein paar Fragen und gab den Link auf den Fragebogen z.B. an einen Mitarbeiter weiter, so konnte dieser nur ab der noch nicht betrachteten Frage weitermachen. Dies wurde von vielen Teilnehmern kritisiert. Allerdings konnte der Fragebogen durch den Administrator erneut frei geschaltet und anschließend neu bearbeitet werden.

Der Teilnehmerkreis wurde aus den Mitgliederlisten der Organisationen „Deutsche Initiative für Netzwerkinformationen e.V. (DINI)“, „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung (ZKI)“ und „Deutscher Bibliotheksverband e.V. (dbv)“ gebildet. Der Einfachheit halber fand keine Selektion statt, so dass teilweise doppelte Anfragen erfolgten aber auch, z.B. bei Firmen, Adressanten angeschrieben wurden, die nicht zur gewünschten Zielgruppe gehörten. Insgesamt wurden 473 Mails am 13.6.2006 versandt. Am 6.9.2006 wurde an 231 Adressaten, die noch nicht mit der Bearbeitung begonnen hatten, eine Erinnerung verschickt. Zu dieser 2. Runde wurde auch eine PDF-Version des Fragbogens auf der DINI-Webseite veröffentlicht (http://www.dini.de/documents/Umfrage.pdf).
Die Umfrage wurde nach der DINI-Mitgliederversammlung am 27.9.2006 geschlossen. Insgesamt liegen 149 auswertbare Fragebogen vor.

Die Auswertung erfolgte mittels Excel. Sie ist im Detail im Anhang veröffentlicht. Bei skalaren Größen ist dabei Minimum, Maximum und der Durchschnittswert aufgeführt.

3. Zusammenfassende Wertung

Im Folgenden wird ein Auszug der Ergebnisse gegeben, die im Abschnitt 6 ausführlich dargestellt sind.

Die Umfrage richtete sich an Einrichtungen unterschiedlichster Größe von 200 bis 150.000 Nutzern.

Die Anzahl der eingesetzten öffentlichen Computer- und Netzarbeitsplätze (öCNAPs) schwankt zwischen 2 und 1.000.
Bei fast allen Einrichtungen (131) verfügen sie über eine Internet-taugliche Netzanbindung.

Die 31 Fragen (s. Seite 6) gliedern sich nach den von der Arbeitsgruppe erarbeiteten Empfehlungen.

So zielt ein Fragenkomplex (Frage 4 und 5) auf die für öCNAPS verwendeten Betriebssysteme, Browser und andere Software. Vielleicht etwas überraschend sind der hohe Linux-Anteil mit 63 und der niedrige MacOS-Anteil mit 11 Einrichtungen. Modzilla/Firefox (108) überflügelte sogar den Microsoft Internet Explorer (101).

Breiten Raum nahmen die Fragen zu Installations- und Managementtechniken ein (Frage 6, 7 und 8): einen Bootserver setzen 46 Einrichtungen ein, Terminalserver werden von 34 Einrichtungen betrieben. 39 spiegeln ihre Festplatten, 34 führen die Installation automatisch durch, 56 über das Netzwerk und immerhin noch 31 Einrichtungen arbeiten manuell. Zahlreiche Detailangaben mit speziellen Produkten folgen.

118 Einrichtungen stellen WLAN-Anschlüsse zur Verfügung (Frage 16 und 17). Der WLAN-Deckungsgrad wurde abgefragt. Er ist bei 66 Einrichtungen größer als 50 %, bei 21 Einrichtungen sogar 100%. Der WLAN-Zugang wird durch verschiedene Techniken realisiert: persönliche Anmeldung über eine Webseite (21), Anmeldung an einem VPN-Server (86), MAC-Adressen (23).

96 Einrichtungen stellen zudem direkte LAN-Anschlüsse für Laptops bereit.

67 Einrichtungen haben keine! Probleme mit nicht-zweckgemäßer Nutzung des Internets. 45 Einrichtungen haben Probleme mit dem Herunterladen großer Datenmengen, 41 mit ausuferndem Chatten und Mailen, 29 mit Aufrufen pornographischer Inhalte, 30 mit Manipulationen der Festplatte. Für weitere Details s. Frage 18 im Anhang.

Bei dem Bereich Sicherheit wurden nicht nur Techniken sondern auch der organisatorische Rahmen abgefragt:
Bei der Steuerung des Zugangs nehmen immerhin 43 Einrichtungen keine Differenzierung zwischen verschiedenen Nutzergruppen (z.B. Studierende, Mitarbeiter, Externe) vor.
7 Einrichtungen bieten den freien Internetzugang ohne Authentifizierung. Bei 118 Einrichtungen erfolgt die Authentifizierung standardmäßig über Login / Passwort (Frage 12), bei 8 Einrichtungen über eine Chipkarte und bei 7 Einrichtungen über Zertifikate.
Die Frage (13) der Internetnutzung durch Externe wurde von 68 Einrichtungen verneint.

An Ausgabemöglichkeiten von Internet-Recherchen bieten 106 Einrichtungen Datenträger wie Disketten / ZIP, 122 Druckausgaben, 115 den Mailversand und 62 das Brennen von CDs / DVDs an.

86 Einrichtungen schränken den Internetzugriff nicht ein. Bei 22 Einrichtungen erfolgt dies durch Positivlisten, bei 20 durch Negativlisten.
Bei der Erstellung der Listen arbeiten 11 Einrichtungen mit anderen Institutionen zusammen, z.B. Belwue, NRW Bibliotheken
14 Einrichtungen verwenden verschiedene Filtersoftware.

63 Einrichtungen haben keine kostenpflichtigen Dienste (Frage 21).

Bei 82 Einrichtungen ist das Drucken, bei 16 die Ausgabe auf Datenträger, bei 7 der Internetzugang und auch bei 7 die Nutzung von Spezialperipherie wie Plotter und Scanner kostenpflichtig.

Beim Geräteschutz wurden verschiedenste Maßnahmen beschrieben.
Interessant ist, dass sich 12 Einrichtungen vor Diebstahl durch Videoüberwachung schützen, eine setzt sogar Video Dummies ein.
Gegen Konfigurationsänderungen schützen sich 31 Einrichtungen durch Rechteeinschränkungen. Dies setzt ein abgestuftes Rechtekonzept voraus wie es u.a. Microsoft Windows bietet. Über Domänen abgesicherte Windowsinstallationen machen Manipulationen nahezu unmöglich. 13 Einrichtungen setzen auf technische Restriktionen, die von Wächterkarten überwacht werden.
Vor Schadenssoftware (Malware) schützen sich tatsächlich nur 68 Einrichtungen mittels Antivirensoftware. Die Spitzenreiter bei den eingesetzten Produkten sind MacAfee und Sophos. 14 Einrichtungen schützen sich mit einer Firewall.
Vor Hacks und Malware durch mitgebrachte mobile Geräte schützen sich 13 Einrichtungen durch einen separaten Netzbereich.
Authentisierungsinformationen (in der Regel sind dies Benutzerkennung / Passwort) werden durch Verschlüsselungsverfahren wie ssl, https, ssh, slogin geschützt.
2 Einrichtungen verwenden Kerberos, eine IPsec.

Informationen über die durchgeführten Sicherheitsmaßnahmen werden am häufigsten über das Web gegeben (45). Sie stehen aber auch in der Benutzungsordnung (21).

Eine Unterstützung bei der Nutzung der öCNAPs erfolgt bei 88 Einrichtungen im Rahmen einer Vorort-Präsenz, bei 57 durch besondere Ansprechpartner, bei 33 durch eine Hotline.

114 Einrichtungen haben ihre betreuten Nutzungszeiten spezifiziert, 81 haben auch unbetreute Zeiten. 12 Einrichtungen haben bei der unbetreuten Nutzung kein Sicherheitskonzept.
An Sicherheitskonzepten bei der unbetreuten Nutzung kommen die Videoüberwachung (12), die Elektronische Zugangskontrolle (7) und ein Wachdienst (3) zum Einsatz.

106 Einrichtungen reglementieren die Internet-Nutzung über ihre Verwaltungs- und Benutzungsordnung, 34 verfügen über ergänzende Regelungen zu ihrer Verwaltungs- und Benutzungsordnung (Frage 27).
Allein 50 Einrichtungen haben die URL zu ihrer Verwaltungs- und Benutzungsordnung angegeben.

Bei Frage 28 konnten Wünsche für zukünftige Empfehlungen / Richtlinien geäußert werden. 40 Einrichtungen wünschen sich weitergehende Hinweise für die technische Realisierung von öCNAPs, 39 Empfehlungen für die Gebührenerhebung, 68 für die Behandlung von Nutzern, die nicht Angehörige der Institution sind, 41 zu der inhaltlichen Reglementierung des Internet-Zugriffs.

In Frage 29 wurde der Bekanntheitsgrad der Empfehlungen der Arbeitsgruppe erfragt.

Nur 29 Einrichtungen kannten die Empfehlungen, immerhin weitere 44 durch den Fragenbogen. Hier muss also noch einiges an Öffentlichkeitsarbeit geleistet werden Diejenigen, die die Empfehlungen kannten, halten sie für ein nützliches Grundkonzept (23).

Zum Schluss des Fragebogens unter den Punkten 30 und 31 wurden noch Name und Anschrift der Institution (Bibliothek oder Rechenzentrum) und der Ansprechpartner ggf. auch für Teilgebiete mit E-Mail-Adresse und Telefonnummer erfragt.

4. Ausblick

Die Arbeitgruppe hat sich zu einer Videokonferenz am 5./7.12.2006 getroffen, um das weitere Vorgehen zu besprechen.
Da bei der Umfrage auch Ansprechpartner in den Einrichtungen erfragt wurden, stellt die aufgebaute Datenbasis eine umfangreiche Informationsquelle dar, die den Mitgliedseinrichtungen verfügbar gemacht werden sollte. Über die Arbeitsgruppe kann dabei eine Zuordnung von Betreiber und Lösung erfolgen (z.B. für den Betrieb eines MacOS-Pools). Die AG beabsichtigt, dafür ein moderiertes Forum einzurichten.
Die 50 URLs zu den Verwaltungs- und Benutzungsordnungen werden in der nächsten Zeit über die DINI-Webseite verfügbar gemacht.
Darüber hinaus sollten die Mitgliedseinrichtungen die Nutzung des Tools Globalpark auch für andere Umfragen prüfen, da hier eine schnell erstellbare und einfach auswertbare elektronische Form zur Verfügung steht, die die aufwendige Papierform oder auch selbst-programmierte Verfahren überflüssig machen.

5. Fragen

1. Wie viele Nutzer/Leser hat ihre Institution (Anzahl)?

2. Über wie viele öffentlich zugängliche Computer/Netzarbeitsplätze verfügt ihre Institution* (Anzahl)?

3. Über welchen Funktionsumfang verfügen die öffentlichen Computerarbeitsplätze?

4. Mit welchen Betriebssystemen betreiben Sie die öffentlichen Computerarbeitsplätze?

5. Welche Browser und welche Software sind auf den öffentlichen Computerarbeitsplätzen installiert?

6. Wenn die öffentlichen Computerarbeitsplätze über einen Boot Server verfügen, beschreiben Sie die eingesetzte Technik.

7. Wie werden die öffentlichen Computerarbeitsplätze installiert?

8. Wie viele der öffentlichen Computerarbeitsplätze werden nicht von einem zentralen Server bedient?

9. Wird beim Zugang zu den Geräten/Diensten zwischen verschiedenen Nutzergruppen (z.B. Studierende, Mitarbeiter, Externe) differenziert?

10. Steuern Sie den Zugang zu den Geräten/Diensten / zum Internet in Ihrer Institution durch eine persönliche Anmeldung/Identifizierung Ihrer Nutzer/Leser

11. Benutzen und verwalten Sie Daten Ihrer Nutzer, um den Zugang zum Internet oder allgemein zu den öffentlichen Computerarbeitsplätzen zu steuern (Accounts)?

12. Nutzen Sie für die Authentisierung der Nutzer beim Zugang zu den Geräten/Diensten die folgenden Techniken?

13. Können in Ihrer Institution Externe (Nutzer, die nicht Angehörige oder eingetragene Leser Ihrer Einrichtung sind) das Internet nutzen?

14. Welche der folgenden Ausgabemöglichkeiten gibt es in Ihrer Institution im Rahmen internet-basierter Recherchen?

15. Betreiben oder planen Sie LAN-Anschlussmöglichkeiten für mobile DV-Geräte von Nutzern/Lesern, z.B. für Laptops?

16. WLAN

17. Wie steuern Sie den Zugang zum WLAN?

18. Hatten Sie in ihrer Institution bereits nennenswerte Probleme mit der nicht zweckgemäßen Nutzung Ihrer Internet-Rechner?

19. Schränken Sie den Internetzugriff in Ihrer Einrichtung von vornherein ein?

20. Arbeiten Sie bei der Erstellung von Access-Listen oder ähnlichen Adresslisten für Filter-Software mit anderen Institutionen zusammen?

21. Planen oder praktizieren Sie die kostenpflichtige Nutzung der Dienste über eine Auslagenerstattung, Gebührenerhebung etc. für bestimmte Benutzergruppen

22. Wie werden die Geräte Ihrer Einrichtung bzw. die mitgebrachten Geräte der Nutzer geschützt?

23. Wie werden die Nutzer über die Sicherheitsmassnahmen und die Sicherheitsanforderungen informiert?
24. Wie wird die Benutzung der öffentlichen Computerarbeitsplätze unterstützt?

25. In welchem Zeitraster stehen die öffentlichen Computerarbeitsplätze zur Verfügung?

26. Welche Sicherungskonzepte setzen Sie bei der unbetreuten Nutzung ein?

27. In welcher rechtlichen Form reglementieren Sie die Internet-Nutzung in Ihrer Institution?

28. In welchen Bereichen oder bei welchen Fragen im Zusammenhang mit der Internet-Nutzung in Ihrer Institution halten Sie Empfehlungen oder Richtlinien eines übergeordneten Verbandes für wünschenswert bzw. notwendig?

29. Kennen Sie die "Empfehlungen für die Einrichtung von öffentlichen Computer- und Netzarbeitsplätzen" der Arbeitsgruppe öCNAP im DINI eV vom Oktober 2004 http://www.dini.de/documents/oecnap_102004_final.pdf und welche Meinung haben Sie dazu?

30. Name und Anschrift Ihrer Institution (z.B. Bibliothek oder Rechenzentrum)

31. Ansprechpartner (auch für Teilgebiete) / E-Mail / Telefon

6. Auswertung

Öffentliche Computer/Netzarbeitsplätze und Internet
Eine Umfrage von Deutsche Initiative für Netzwerkinformation e.V. (DINI)
Arbeitskreis "Umgang mit öffentlichen Computer-Arbeitsplätzen, Nutzerverwaltung und Accountvergabe (ÖCAP)"

149 auswertbare Antworten

1. Wie viele Nutzer/Leser hat ihre Institution (Anzahl)?

Antworten gesamt	durchschnittl. Anzahl pro Einrichtung	max. Anzahl pro Einrichtung	min. Anzahl pro Einrichtung
149	10.300	150.000	200

2. Über wie viele öffentlich zugängliche Computer/Netzarbeitsplätze verfügt ihre Institution* (Anzahl)?

Antworten gesamt	durchschnittl. Anzahl pro Einrichtung	max. Anzahl pro Einrichtung	min. Anzahl pro Einrichtung
149	283	1.000	2

3. Über welchen Funktionsumfang verfügen die öffentlichen Computerarbeitsplätze?

- **mit Netzanbindung, dabei Internet tauglich (Anzahl)**

Antworten gesamt	durchschnittl. Anzahl pro Einrichtung	max. Anzahl pro Einrichtung	min. Anzahl pro Einrichtung
131 von 149	134	650	1

- **mit Netzanbindung, aber nur Terminalfunktion für einzelne Dienste (z.B. OPAC/Katalog) (Anzahl)**

Antworten gesamt	durchschnittl. Anzahl pro Einrichtung	max. Anzahl pro Einrichtung	min. Anzahl pro Einrichtung
50 von 149	31	200	1

- **Einzelplatz ohne Netzanbindung (Anzahl)**

Antworten gesamt	durchschnittl. Anzahl pro Einrichtung	max. Anzahl pro Einrichtung	min. Anzahl pro Einrichtung
30 von 149	5	20	1

- **weiterer, und zwar (Funktionen verbal aufzählen) (Anzahl)**

25 von 149 Einrichtungen gaben weitere Funktionen an
9 Einrichtungen gaben dabei Arbeitsplätze zur Bild/Videobearbeitung an.

Weitere Antworten bezogen sich auf verschiedene Softwareprodukte und Ausgabegeräte, die an anderer Stelle des Fragebogens berücksichtigt werden (Frage 5, Frage 14) und hier nicht eingehen.

4. Mit welchen Betriebssystemen betreiben Sie die öffentlichen Computerarbeitsplätze?

Betriebssystem	Anzahl Einrichtungen (von 149)	durchschnittl. Anzahl pro Einrichtung	max. Anzahl pro Einrichtung	min. Anzahl pro Einrichtung
MS Windows	122	110	600	1
Linux	63	83	340	6
MacOS	11	18	50	1

6 Einrichtungen von 149 gaben Solaris als weiteres Betriebssystem an.

5. Welche Browser und welche Software sind auf den öffentlichen Computerarbeitsplätzen installiert?

Browser/ Software	Anzahl Einrichtungen (von 149)	durchschnittl. Anzahl pro Einrichtung	max. Anzahl pro Einrichtung	min. Anzahl pro Einrichtung
Netscape	26	99	500	2
Mozilla/Firefox	108	117	650	2
Microsoft IE	101	116	600	1
Office	85	127	650	2

66 von 149 Einrichtungen machten zusätzliche Angaben.

	Nennungen
Bildbearbeitung (Corel, Photoshop, etc.)	17
Acrobat	15
Statistiksoftware (SPSS, SAS, etc.)	12

Mathematik (Maple, etc.)	12
Programmiersprachen	11
Open Office	8
Brennsoftware (Nero, etc.)	5
Makromedia	4
Citrix ICA	3
Tex	3
ZIP	3
Sonstige Software	82

6. Wenn die öffentlichen Computerarbeitsplätze über einen Boot Server verfügen, beschreiben Sie die eingesetzte Technik.

46 von 149 Einrichtungen setzen einen Bootserver ein.

Technik beim Bootserver	Nennungen
Terminalserver	7
Rembo	6
PXE-Boot	6
Etherboot	4
Linux-Bootserver	2
Bootp	2
IBA-Lösung der NRW-Bibliotheken	2
IGEL Server für Thin Clients	2
NFSRoot	1
RIS	1
Scout	1
SunRay	1

7. Wie werden die öffentlichen Computerarbeitsplätze installiert?

	Nennungen
Terminalserver-Betrieb	34
Spiegelung von Festplatten	39
automatisierte Installation	34
Netzwerkinstallation	56
manuelle Installation	31
Sonstige	23

An sonstigen Installationstechniken wurde genannt:

Sonstige Installationstechniken	Nennungen
Images	6
Novell ZenWorks	3
Microsoft MSI über Active Directory	3

Diskless Festplattenimage mit manuellen Anpassungen	2
Clonic mit Symantec	2
Cloning mit Acronis	1
Microsoft SMS	1
Scout	1
Wyse Rapport	1
NFS-Boot	1
Norton	1
SunRay	1

8. Wie viele der öffentlichen Computerarbeitsplätze werden nicht von einem zentralen Server bedient?

Antworten gesamt	durchschnittl. Anzahl pro Einrichtung	max. Anzahl pro Einrichtung	Min. Anzahl pro Einrichtung
53 von 149	35	250	1

9. Wird beim Zugang zu den Geräten/Diensten zwischen verschiedenen Nutzergruppen (z.B. Studierende, Mitarbeiter, Externe) differenziert?

130 von 149 Einrichtungen haben geantwortet (nur freie Antworten).

- 43 Einrichtungen nehmen keine Differenzierung vor.
- 29 Einrichtungen haben explizit angegeben zwischen Hochschulangehörigen, Bibliotheksnutzern und sonstigen Nutzern zu differenzieren
- 74 haben angegeben, den Zugang über Accounts zu steuern, davon
  - 9 mit speziellen Accounts der Bibliothek, bei
  - 7 wird die Differenzierung über LDAP vorgenommen, bei
  - 3 über Active Directory und
  - 2 haben zusätzlich explizite Gast-Accounts,
  - 4 lassen explizit keine Externen zu.
- 7 Einrichtungen bieten den freien Zugang ins Internet

10. Steuern Sie den Zugang zu den Geräten/Diensten / zum Internet in Ihrer Institution durch eine persönliche Anmeldung/Identifizierung Ihrer Nutzer/Leser

ja	71	
nein	25	
sowohl als auch	45 Bei welchen Geräten/Diensten ist dabei keine persönliche Anmeldung/Identifizierung erforderlich?	
	Opac	22
	Spezialstationen ohne Internetanbindung (Multimedia, Scannen, Brennen, Office)	6
	Allgemeiner Internetzugang	4
	Lokal (Internetangebot der Hochschule, Intranet, Zugang zu Internetangeboten über Positivlisten)	10
	Geräte unter Aufsicht	4

11. Benutzen und verwalten Sie Daten Ihrer Nutzer, um den Zugang zum Internet oder allgemein zu den öffentlichen Computerarbeitsplätzen zu steuern (Accounts)?

	Nennungen	
eigene Nutzerverwaltung (z.B. Proxy Server Squid)	60	
Nutzerverwaltung einer Partnereinrichtung (z.B. Rechenzentrum)	43	
nicht automatisiertes Anmeldeverfahren	14	
andere Lösung und zwar	9	
	Anonymer Zugang	4
	Gastaccount	1
	LDAP/NIS	3
	selbstgeschriebenes Programm	1

Beschreiben Sie die eingesetzte Technik:

	Nennungen
LDAP	14
proprietär (selbst entwickelte Zugangsüberprüfung)	6
Active Directory	3
Novell	3
Sisis	3
Aleph	1

SNLP (davon einmal mittels LDAP)	2
Kiosk	1
Proxy	1
KEN	1

12. Nutzen Sie für die Authentisierung der Nutzer beim Zugang zu den Geräten/Diensten die folgenden Techniken?

	Nennungen	
Chipkarten	8	
Zertifikate, digitale Signaturen, Schlüssel	7	
Login/Passwort	118	
Sonstiges und zwar	6	
	Fingerscanner	1
	Gastaccount	1
	Anonym	2
	Händisch	2

13. Können in Ihrer Institution Externe (Nutzer, die nicht Angehörige oder eingetragene Leser Ihrer Einrichtung sind) das Internet nutzen?

	Nennungen		
Ja, keine Zugangsbeschränkung	25		
Nein	68		
nur Angehörige benachbarter Hochschulen oder Hochschulen des gleichen Bundeslandes	10		
Angehörige anderer Hochschulen	21		
Sonstige und zwar	42		
	Bibliotheksnutzer	7	
	Angemeldete Nutzer (Gäste)	20	
	Im Rahmen von Roaming (z.B. über DFN)	2	
	mit Ressourcen-beschränkung	9	
		zeitlich	2
		Nur Bibliotheks-angebote	4
		Kein Drucken	1
		im Rahmen von bestimmten Veranstaltungen	2

14. Welche der folgenden Ausgabemöglichkeiten gibt es in Ihrer Institution im Rahmen internet-basierter Recherchen?

	Nennungen	
Abspeichern (Disketten-, Zip-Laufwerke etc.)	106	
Drucken	122	
Brennen von CDs/DVDs	62	
Versand von Mails an sich selber	115	
Sonstiges und zwar	17	
	USB	13
	Homedirectory	3
	Scannen	1

15. Betreiben oder planen Sie LAN-Anschlussmöglichkeiten für mobile DV-Geräte von Nutzern/Lesern, z.B. für Laptops?

	Nennungen
nein	30
ja, wird betrieben	96
ja, ist geplant	15

16. WLAN

ein WLAN-Zugang wird nicht bereitgestellt	22
ein WLAN-Zugang wird bereitgestellt	118

Der Deckungsgrad beträgt (geschätzt in Prozent):

	< 10%	>19% <50%	>50% <80%	>80%	100%
Nennungen	19	22	25	20	21

17. Wie steuern Sie den Zugang zum WLAN?

	Nennungen
durch eine persönliche Anmeldung über eine Webseite	21
durch eine persönliche Anmeldung an einem VPN-Server	86
durch Zulassung von MAC-Adressen	21

Sonstiges und zwar	23	
	RZ-Account	12
	Zertifikat	2
	Radius	1
	DFN-Roaming	1
	Port Authenti-fizierung	1
	Web-Key	1

18. Hatten Sie in ihrer Institution bereits nennenswerte Probleme mit der nicht zweckgemäßen Nutzung Ihrer Internet-Rechner?

	Nennungen	
nein	67	
ja, durch ausuferndes Chatten und Mailen	41	
ja, durch Handel / private Online-Marktplätze (z.B. eBay)	17	
ja, durch Herunterladen großer Datenmengen zum Privatgebrauch	45	
ja, durch Aufrufe extremer politischer Inhalte	5	
ja, durch Aufrufe pornografischer Inhalte	29	
ja, durch Manipulation der Installation	30	
ja, andere Probleme und zwar	19	
	Computerspiele	1
	Missbräuchliche Geschäfte über das Internet (Pizza bestellen, Kreditkartenbetrug)	3
	Softwareverteilung (Peer to peer – Netze)	2
	IP-Telefonie, Skype	1
	Übermäßiges Ausdrucken	1
	Virenverseuchte Notebooks am WLAN	1
	Keine Probleme, weil die Rechner öffentlich aber gut einsehbar aufgestellt sind und eine persönliche Anmeldung notwendig ist.	1
	Missbrauch auf Grund nicht erfolgter Abmeldung.	1

19. Schränken Sie den Internetzugriff in Ihrer Einrichtung von vornherein ein?

	Nennungen	
nein	86	
ja, durch Access-Listen im Sinne von Negativlisten, z.B. über Proxy-Server	20	
ja, durch Access-Listen im Sinne von Positivlisten, z.B. über Proxy-Server	22	
ja, durch den Einsatz von Filter-Software auf einzelnen Geräten	14	
	Beschreiben Sie ggf. die eingesetzte Filter-Software	
	Squid Guard	3
	Filter des Belwue-Proxy-Servers	1
	IDS (intrusion detection system) mit selbst erstellten Filterregeln	1
	Filterung durch Server des bayrischen Kultusministeriums	1
	Parents Friend	1
	Proventia Web – Filter	1
	Safer Serv der Firma Nutzwert	1
	SiteKiosk	1
	Tauschbörsenfilter	1
	WebWasher	1
	Dansguardian	1
ja, durch zeitliche oder mengenmäßige Begrenzungen.	Welche?	
	Zeitliche Beschränkung (z.B. 1 Stunde, 6 Stunde pro Woche, 1 Stunde täglich. 30 Minuten dann 30 Minuten Sperre, in Lehrveranstaltungen, wenn vom Professor gewünscht)	10
	Loadvolumina (Up / Down)	2
ja, Sonstiges	20 davon	
	Portfilter	5
	Chat	1
	Internetgebühr	1
	Einschränkungen nur von außen nach innen	1
	URL-Blocker	1

aus Proxy-Positivliste ohne Anmeldung, ansonsten Anmeldung (dies aber nur für Personen > 18 Jahre)	1

20. Arbeiten Sie bei der Erstellung von Access-Listen oder ähnlichen Adresslisten für Filter-Software mit anderen Institutionen zusammen?

	Nennungen	
nein, da keine Access- oder Adresslisten eingesetzt werden	78	
nein, Access- oder Adresslisten werden ausschließlich selbst erstellt	39	
ja und zwar	11	
	Belwue	3
	Blacklists aus dem Internet mit eigenen Erweiterungen	1
	Mit anderen NRW Bibliotheken	1
	Rechenzentren	2
	Sophos	1
	Squidguard.org	1
	Uni Bibliothek	2

21. Planen oder praktizieren Sie die kostenpflichtige Nutzung der Dienste über eine Auslagenerstattung, Gebührenerhebung etc. für bestimmte Benutzergruppen

	Nennungen	
nein	63	
ja, für den Zugang zum Internet	7	
ja, für die Nutzung der Computerarbeitsplätze	1	
ja, für Speicherplatz	1	
ja, für das Drucken	82	
ja, für Datenträger	16	
ja, für Spezialperipherie	7	
Welche?	Scannen	3
	Plotten/Laminieren	4
	Readerprinter	1
ja, für Spezialsoftware	0	

für Sonstiges		
Welche?	Internetzugang im Wohnheim	1
	Internetzugang für Externe geplant	1

22. Wie werden die Geräte Ihrer Einrichtung bzw. die mitgebrachten Geräte der Nutzer geschützt?

- Schutz der Geräte der Serviceeinrichtung vor Diebstahl.
  109 Einrichtungen haben geantwortet und Verfahren angegeben:

	Nennungen
Mechanisch (z.B. durch eine Blechhalterung)	10
Mechanisch durch Festschrauben	2
Mechanisch durch Kette/Seil (ggf. auch mit Schloss)	52
Mechanisch durch Schloss (Kensington) (ggf. auch mit Kette)	37
Elektronische Alarmanlage (Bewegungsmelder oder bei Kontaktunterbrechung)	7
Aufsicht	19
Videoüberwachung	6
Video Dummy	1
Plakette/Gravuren	5
Elektronische Zugangskontrolle (Chipkarte)	2
Nur Maus/Tastatur (Rechner zu alt)	3
Ping durch zentrale Server	1
Scheiben-Einbruchfolie	1

- Schutz der Geräte der Serviceeinrichtung gegen Veränderungen durch Benutzer.
  110 Einrichtungen haben geantwortet und Verfahren angegeben:

	Nennungen
Rechteeinschränkung (über Domänen abgesicherte Windowsinstallationen machen Manipulationen nahezu unmöglich)	31
Images	2
Spiegeln	1
Wächterkarten (Watchdog, PC-Sheriff, HDD-Sheriff, Einschränken von Laufwerkszugriffen, virtuelle Laufwerke, etc.)	13
Radix Protector Karte	1
IBA	1

Rembo	3
Einschränkungen der Zugriffsmöglichkeiten mittels Policy Editor	1
Reborn Card (Daten-Air-Bag)	1
Unterbinden des Bootens von mitgebrachten Datenträgern	1
Thin Clients	4
Terminalserver	2
Standardprofil bei Neustart (Windows/Linux)	3
Originalzustand bei Neustart (automatisch / händisch)	9
DKS-Software von Dr. Kaiser	1
Kiosk-Software (Sitekiosk, XP-Kiosk-Modus)	4
Abgesichertes Linux	3
Win Control	1
Microsoft Shared Computer Toolkit	1
Reduzierter Funktionsumfang von Betriebssystem und Browser	2
Nur WWW	1
Read Only System	2
Monitoring	1
Registry Passend	1
Software Deep-Freeze	1

- Schutz der Geräte vor Schadenssoftware (Malware).
  102 Einrichtungen haben geantwortet.
  Teilweise wurden Funktionalitäten genannt, die auch schon unter der letzten Teilfrage (Schutz der Geräte der Serviceeinrichtung gegen Veränderungen durch Benutzer) genannt wurden. Sie werden hier nicht mehr aufgeführt.

	Nennungen
Antivirensoftware (häufige Nennung von MacAffee und Sophos)	68
Firewall	14

Betriebssystemupdates wurden auch vereinzelt genannt. Ein sorgfältige Betriebssysteminstallation und – pflege muss allerdings grundsätzlich vorausgesetzt werden.

- Schutz anderer Geräte der Serviceeinrichtung vor Hackern und Malware durch mitgebrachte mobile Geräte.
  66 Einrichtungen haben geantwortet. Teilweise wurden Funktionalitäten genannt, die auch schon unter den letzten Teilfragen der Frage 22 genannt wurden. Sie werden hier nicht mehr aufgeführt.

	Nennungen
Access-Listen	3
Separater Netzbereich (Subnetz teilweise mit VPN und Firewall)	13
Logisch über VPN-Server (verschlüsselt)	5
Empfehlungen	1
MAC-Adresse	2
IDS	3
Verschlüsselte Kommunikation (bei drahtlosen Peripheriegeräten z.B. Tastaturen)	1
Sperrung des WLAN-Accounts bei Viren/Wurm-Befall	1

- Schutz mitgebrachter mobiler Geräte der Benutzer.
  23 Einrichtungen haben geantwortet. Teilweise wurden Funktionalitäten genannt, die auch schon unter den letzten Teilfragen der Frage 22 genannt wurden. Sie werden hier nicht mehr aufgeführt.

	Nennungen
Sache des Benutzers	3
Empfehlungen	1

- Schutz der Authentisierungsinformationen (in der Regel Benutzerkennungen und Passwörter).
  61 Einrichtungen haben geantwortet.
  Angaben wie „Benutzerkennung/Passwort“ wurden ignoriert.

	Nennungen
Verschlüsselung (ssl, https, ssh, slogin)	32
IPSEC	1
VPN	5
Kerberos	2
Ntlmv4	1
Chipkarte	1
Zertifikate	1
Keine Speicherung der Daten im Browser	1

- Sonstige Schutzmaßnahmen
  6 Einrichtungen haben geantwortet. Teilweise wurden Funktionalitäten genannt, die auch schon unter den letzten Teilfragen der Frage 22 genannt wurden. Sie werden hier nicht mehr aufgeführt. Neu genannt wurden
  - CISCO MARS
  - Sicherung mobiler Geräte über eine Buchsicherungsanlage

23. Wie werden die Nutzer über die Sicherheitsmassnahmen und die Sicherheitsanforderungen informiert?

110 von 149 Einrichtungen haben geantwortet.

	Nennungen
Service/Point/Theke	3
Aushang / Infoblätter	21
Web	45
Belehrungen bei Immatrikulation / Beginn des Studienjahres (auch elektronisch)	3
Bei Beantragung Kennung / Passwort	5
Benutzungsordnung	21
Einführungsveranstaltung	6
Benutzerzeitschrift / Newsletter / Flyer	11
Aktuele Infos beim Einloggen	8

24. Wie wird die Benutzung der öffentlichen Computerarbeitsplätze unterstützt?

	Nennungen	
keine besondere Betreuung	22	
im Rahmen einer Vorort-Präsenz	88	
Hotline	33	
Benutzerforum	5	
besondere Ansprechpartner	57	
Sonstiges	21	
und zwar	Servicecenter / Auskunftstheke (auch für andere Zwecke)	8
	Anleitung	5
	Beratung	2
	FAQ	1
	Schulung	3
	Helpdesk	2

25. In welchem Zeitraster stehen die öffentlichen Computerarbeitsplätze zur Verfügung?

114 von 149 Einrichtungen haben die **betreuten** Zeiten spezifiziert.
81 von 149 Einrichtungen haben auch die **unbetreuten** Zeiten spezifiziert.
An dieser Stelle wird keine Detailanalyse vorgenommen.

26. Welche Sicherungskonzepte setzen Sie bei der unbetreuten Nutzung ein?

75 von 149 Einrichtungen haben geantwortet.
Die folgenden Angaben müssen ggf. in den Antworten zu Frage 22 eingearbeitet werden.
35 Antworten bezogen sich direkt auf Frage 22

	Nennungen
Keine besondere Sicherung	12
Chipkarte	5
Automatische Abfrage von einem zentralen Server	1
Elektronische Zeitschlösser	1
Elektronische Zugangskontrolle	7
Wachdienst	3
Stichprobenartige Kontrolle	1
Videoüberwachung	12
Soziale Kontrolle	1
Erfassung von Anmeldedaten	1

27. In welcher rechtlichen Form reglementieren Sie die Internet-Nutzung in Ihrer Institution?

	Nennungen
im Rahmen einer Verwaltungs- oder Benutzungsordnung	106
im Rahmen einer ergänzenden oder vorläufigen Regelung als Ergänzung zur Verwaltungs- oder Benutzungsordnung	34
derzeit keine eigene Regelung, es wird jedoch auf Regelungen anderer Einrichtungen verwiesen	4
eine Regelung ist geplant	6
keine Regelung	10

Es liegen 50 Hinweise zu den zu Grunde liegenden Dokumenten in Form von URLs vor.

28. In welchen Bereichen oder bei welchen Fragen im Zusammenhang mit der Internet-Nutzung in Ihrer Institution halten Sie Empfehlungen oder Richtlinien eines übergeordneten Verbandes für wünschenswert bzw. notwendig?

	Nennungen
technische Realisierung der Internet-Plätze	40
Gebührenerhebung oder Auslagenerstattung	39

Behandlung und Zulassung von Nutzern, die nicht Angehörige Ihrer Institution sind	68	
inhaltliche Reglementierung des Internet-Zugriffs, z.B. über Access-Listen	41	
Sonstiges	9	
und zwar	Rechtsfragen (Zugangsreglementierung, Accounting, etc.)	3
	Druckkostenabrechnung	1
	Lizenz- und Urheberrecht	1
	Persönliche Homepages	1

Es wurden die folgenden Anmerkungen gemacht:

	Nennungen
Bitte nur Empfehlungen	2
Empfehlungen / Richtlinien speziell für Externe	1
BSI Handbuch reicht	1
Erfahrungsaustausch erwünscht	1
Erstellung von Musterordnungen	1
Richtlinien / Empfehlungen nicht notwendig	1

29. Kennen Sie die "Empfehlungen für die Einrichtung von öffentlichen Computer- und Netzarbeitsplätzen" der Arbeitsgruppe öCNAP im DINI eV vom Oktober 2004 http://www.dini.de/documents/oecnap_102004_final.pdf und welche Meinung haben Sie dazu?

	Nennungen
Nein	70
Ja	29
Ja, durch diesen Fragebogen	44

Dazu wurde noch das folgende Meinungsbild geäußert:

	Nennungen
Nützliches Grundkonzept	23
Könnte spezieller sein	3
Bestätigung der eigenen Technologie / Handlungsweise	3
Nichts Neues	2
Wäre vor 10 Jahren nützlich gewesen	1
In Teilen überarbeitungswert	1
Mit vielen Mitarbeitern und viel Geld kann man viel machen	1
Viel zu restriktiv und gegen alles absichernd	1

Zum Schluss des Fragebogens unter den Punkten 30 und 31 wurden noch Name und Anschrift der Institution (Bibliothek oder Rechenzentrum) und der Ansprechpartner ggf. auch für Teilgebiete mit E-Mail-Adresse und Telefonnummer erfragt.