Freie Universität Berlin

{tip4u://056} Version 5

Zentraleinrichtung für Datenverarbeitung (ZEDAT)
www.zedat.fu-berlin.de

# Campusnetz Policy

Die vielfältigen Möglichkeiten, Rechner in das Campusnetz der Freien Universität Berlin und damit in das Internet einzubinden, bringen neben dem Nutzen in den Bereichen Kommunikation und Information auch Gefahren und Sicherheitsrisiken mit sich. Mit den Festlegungen der Capusnetz Policy werden daher einige Regeln aufgestellt, deren Beachtung für einen sicheren und stabilen Betrieb unabdingbar ist.

zedat

Zentraleinrichtung für Datenverarbeitung
Fabeckstraße 32 / 14195 Berlin
Hotline (030) 838 77777 / hilfe@zedat.fu-berlin.de

# Campusnetz Policy

## 1 Ansprechpartner für Subnetze und (Sub-) Domains

Für die Betreuung und Verwaltung von Subnetzen und Domains im Campusnetz benötigt die ZEDAT kompetente Ansprechpartner in den jeweiligen Bereichen. Die Daten der Ansprechpartner werden mit Hilfe eines Formulars bei der ZEDAT gemeldet oder geändert. Die Einreichung der Formulare erfolgt über die IT-Verantwortlichen des jeweiligen Bereiches. Es handelt sich um ein PDF-Formular, welches unter

http://www.zedat.fu-berlin.de/aspform.pdf

abgerufen, elektronisch ausgefüllt und dann ausgedruckt werden kann.

## 2 Nameserver für Zonen unterhalb von fu-berlin.de

Die ZEDAT hat die Aufgabe, Rechnernamen und IP-Adressen der FU im Domain Name System (DNS) zu verwalten. Hierzu betreibt sie zur Ausfallsicherheit derzeit drei Nameserver (ns{1,2,3}.fu-berlin.de). Einige FU-Bereiche betreiben für ihre Zonen auch eigene Nameserver. Sämtliche Zonen innerhalb des Namensraumes fu-berlin.de - auch die dezentral administrierten - müssen die zentralen Nameserver ns{1,2,3}.fu-berlin.de als primary oder secondary Nameserver eingetragen haben, um die für DNS erforderliche Stabilität und Kontinuität zu gewährleisten.

## 3 Anmeldung von Rechnern im Domain Name System (DNS)

Die Eintragung von Rechnernamen in das DNS ist nicht nur Voraussetzung für die Nutzung vieler Internetdienste, sie dient auch der Identifikation und Zuordnung von Systemen zu den Bereichen der jeweiligen Betreiber. Es ist geplant, Systemen, die nicht korrekt im DNS eingetragen sind, den Zugang zum Internet zu verwehren oder nur eingeschränkt zu ermöglichen. Nicht korrekt im DNS eingetragene Systeme gelten als Testsysteme, auf die bei Störungen oder Unterbrechungen keine Rücksicht genommen wird.

Rechner, die nicht nur testweise im Campusnetz betrieben werden, müssen daher in das DNS eingetragen werden. Fachbereiche und Einrichtungen, die keine eigenen Nameserver betreiben, melden einzutragende Rechner an die folgende E-Mail-Adresse:

hostmaster@ZEDAT.FU-Berlin.DE

Weitere Hinweise hierzu sind unserem Merkblatt Tip4U #55[1] *Rechneranmeldung für DNS* zu entnehmen.

## 4 DHCP

Die Verwendung des Dynamic Host Configuration Protocol (DHCP) erleichtert die Administration von Rechnern und erlaubt u.a. die Zuweisung von IP-Nummern an teilnehmende Systeme. Für die häufig erforderliche Verfolgung und Aufklärung von Missbrauchsfällen sowie die Bekämpfung von Viren ist es wichtig, die betroffenen Rechner auch im Nachhinein identifizieren zu können. Die Administratoren mit DHCP verwalteter Systeme müssen

[1] http://zedat.fu-berlin.de/tip4u_55.pdf

jederzeit über den Standort eines Rechners mit einer bestimmten IP-Nummer zu einem gegebenen Zeitpunkt sowie die Identität des Verantwortlichen bzw. Nutzers Auskunft geben können. Dies ist erfahrungsgemäß schwierig, wenn die Möglichkeit von DHCP genutzt wird, den Client-Rechnern IP-Adressen dynamisch zuzuweisen. Es ist daher dafür zu sorgen, dass den über DHCP administrierten Systemen immer dieselbe IP-Nummer zugewiesen wird (Bindung an die MAC-Adresse). Unbekannten Rechnern bzw. MAC-Adressen dürfen keine IP-Nummern zugewiesen werden.

## 5 Access Points – Wireless LAN

Um den FU-Angehörigen einen drahtlosen Zugang zum Campusnetz zu ermöglichen, betreibt die ZEDAT eine große Zahl von Access Points nach einem Betriebskonzept, das sowohl eine Identitätsprüfung des Nutzers als auch eine verschlüsselte Datenübertragung und damit einen weitgehenden Schutz vor Missbrauch bietet. Fachbereiche und Einrichtungen, die die Aufstellung von Access Points wünschen, können sich mit ihrem Wunsch an die ZEDAT wenden. Allerdings werden im Rahmen eines groß angelegten Projekts ohnehin nahezu sämtliche Gebäude der FU flächendeckend mit Access Points ausgestattet.

Keinesfalls ist es gestattet, Access Points „in eigener Regie“ aufzustellen und zu betreiben. Damit würde nicht nur das Sicherheitskonzept untergraben, sondern auch die ZEDAT-Planung der recht knappen Frequenzen gestört, die für Access Points verwendet werden können. Die „Funkhoheit“ auf dem Campus liegt in der Hand der ZEDAT.

## 6 Ethernet-Dosen im Campusnetz

Ethernetdosen im Campusnetz stellen ein Sicherheitsrisiko dar, wenn sie ohne Zugangskontrolle benutzt werden können. Dosen in nicht öffentlichen Räumen wie Büros, Laboren etc. sind in der Regel durch die baulichen Gegebenheiten hinreichend vor unbefugter Nutzung geschützt. Dosen in öffentlichen Räumen, die auch für Unbefugte leicht zugänglich sind, müssen vor Missbrauch besonders geschützt werden. Sie dürfen entweder nicht beschaltet sein oder müssen von der ZEDAT nach dem VPN-Konzept betrieben werden. Solche Anschlüsse bieten einen Zugang zum zentralen VPN-Server, über den das Campusnetz und das Internet erreicht werden können. Zur Anmeldung beim VPN-Server sind ein Account bei der ZEDAT sowie die VPN-Client-Software erforderlich. Auf Wunsch der Bereiche können „öffentliche“ Ethernet-Dosen entsprechend diesem Konzept eingerichtet werden.

## 7 Betrieb „öffentlicher“ PCs

In einigen Fachbereichen und anderen Einrichtungen der FU werden Pools mit quasi öffentlich zugänglichen PCs zur Nutzung z.B. durch Studierende betrieben. Werden solche PCs ohne jede Zugangskontrolle angeboten, stellen auch sie eine Möglichkeit zum Missbrauch von FU-Ressourcen dar.

Öffentliche PCs müssen daher mit einer Zugangskontrolle versehen sein, die eine unauthorisierte, anonyme Nutzung verhindert. Unter anderem gibt es folgende Möglichkeiten der Realisierung eines kontrollierten Zugangs:

- Einbindung in das Betriebskonzept der ZEDAT für Windows-PCs
  (Voraussetzung für die Nutzung ist ein ZEDAT-Account)

- Betrieb der PCs an „öffentlichen“ Ethernetdosen gemäß Punkt 6
  (Voraussetzungen für die Nutzung sind die Installation eines VPN-Clients und ein ZEDAT-Account, die erst zusammen den Netzzugang gestatten)
- Eine eigene Nutzerverwaltung
  mit den Mitteln des Betriebssystems unter der Regie des betreibenden Bereiches