Zugriffsvoraussetzungen für die Nutzung von CIFS/SMB/Samba

Der Zugriff auf den zentralen Speicherplatz an der Bauhaus-Universität Weimar soll prinzipiell von jedem Rechner und jedem Betriebssystem aus möglich sein. Aus Sicherheitsgründen kann aber nicht jedem Clientsystem uneingeschränkt Zugriff auf das Speichersystem eingeräumt werden, weil nicht allen Clientsystemen in den Netzen der Bauhaus-Universität Weimar gleichermaßen vertraut werden kann.
Im Folgenden wird versucht eine Klassifizierung der vorhanden Arbeitsstationen innerhalb der Bauhaus-Universität vorzunehmen. Ziel dieser Einteilung ist es, die Arbeitsstationen nach ihrer Vertrauenswürdigkeit zu kategorisieren und dann eine Übersicht aufzustellen, in der man die Zugriffsmöglichkeiten einer jeden Arbeitsstationsklasse ablesen kann.
Bei der Erteilung von Zugriffsrechten wird davon ausgegangen, dass Rechnersysteme mit zentraler Betreuung im allgemeinen einen vertrauenswürdigeren Sicherheitszustand aufweisen, als Rechnersysteme bei denen keine konkreten Aussagen über den Betreuungszustand gemacht werden kann. Auf der Basis dieser Voraussetzung werden folgende Arbeitsstationsklassen definiert:

- Zentral administrierte Arbeitsstationen (ZaA) innerhalb des Active Directory Domäne oder einem vertrauenden Kerberos-Domäne
- Zentral administrierte Arbeitsstationen außerhalb des Active Directory
- Arbeitsplatzrechner mit unbestimmten Administrationskonzeptes innerhalb der Bauhaus-Universität Weimar
- Alle anderen Arbeitsstationen einschließlich Studentenwohnheime und VPN-Rechner

Gegenüberstellung Speicherdienste und Arbeitsstationsklassen

In der nachfolgenden Tabelle werden die Arbeitsstationsklassen und die zur Verfügung stehenden Netzwerkdienste gegenübergestellt. In dieser Gegenüberstellung können die Möglichkeiten der Arbeitsstationsklassen abgelesen werden:

	DC	CS	WP	WS
ZaA mit Domänenintegration	x	x	x	x
ZaA ohne Domänenintegration		x	x	x
Unbestimmte Administration UNI-WE			x	x

Erläuterung für die Abkürzungen der Netzwerkdienste

- DC ➔ Domänencontroller (Authentisierungs- und Authroisierungsserver)
- CS ➔ CIFS-Server (DFS/Round-Robin)
- WP ➔ WebDAV Standard
- WS ➔ WebDAV TLS/SSL

Nachfolgend werden die einzelnen Arbeitsstationsklassen genauer beschrieben, um anhand dieser Erläuterungen eine Zuordnung vorhandener Clientsysteme abzuleiten.

Zentral administrierte Arbeitsstationen (ZaA)

Unter zentral administrierten Arbeitsstation sollen all diejenigen Rechnersysteme verstanden werden, deren Wartung und Pflege von zentral autorisierten IT-Institutionen innerhalb der Bauhaus-Universität übernommen werden. Den Nutzern dieser Arbeitsstationen werden keine administrativen Rechte auf ihren Arbeitsplatzrechnern eingeräumt. Der Betrieb (WWW, E-Mail usw.) dieser Systeme erfolgt immer unter unprivilegierten Nutzerkennungen, was die

Gefährdung für diese Systeme wesentlich reduziert und wodurch diese Systeme als die Vertrauenswürdigsten eingestuft werden. Diese Arbeitsstationsklassen können noch in zwei weitere Klassen unterteilt werden

ZaA mit Domänenintegration

Arbeitsstationen die zentral administriert werden und sich innerhalb eines Domänen/Kerberos-Verbundes befinden, sind in der Lage bei der Authentifizierung auf Kerberos zurückzugreifen und können somit ein sicheres Authentifizierungsverfahren nutzen. Für die Nutzung von Kerberos benötigen diese Rechner Zugriff auf die Domänencontroller innerhalb des Active Directories.

ZaA ohne Domänenintegration

Arbeitsstationen in dieser Klasse besitzen die selbe Vertrauenswürdigkeit wie die zentral administrierten Arbeitsstationen, die in einem Domänenverbund integriert sind. Da sie aber außerhalb dieses Verbundes stehen, können sie innerhalb der Bauhaus-Universität kein Kerberos für die Authentifizierung nutzen und benötigen daher auch kein Zugriff auf die Domänencontroller.

Arbeitsstationen mit unbestimmten Administrationskonzept

Alle Arbeitsstationen innerhalb der Bauhaus-Universität Weimar, die einen fest zugeordneten Internetanschluss innerhalb des BUW-Netzes haben und sich nicht innerhalb der beiden vorangestellten Arbeitsstationsklassen befinden, erfüllen die Kriterien dieser Klasse. Explizit ausgeschlossen aus dieser Klasse werden Rechnersystemen aus den Studentenwohnheimen, sowie VPN- und Gastanschlüsse.

Übersicht über den Zugriff auf den zentralen Speicherplatz der Bauhaus-Universität Weimar

	MS-Freigabe	WebDAV
ZaA mit Domänenintegration	x	x
ZaA ohne Domänenintegration	x	x
Unbestimmte Administration UNI-WE		x