

Bei Verstößen gegen diese Richtlinie behält sich das Rechenzentrum (RZ) eine Außerbetriebnahme vor.

§1 Infrastruktur und Betrieb

§1.1 Aktive Netzwerkgeräte (Ausnahmen: Notebooks, PCs) dürfen nicht ohne mit dem Rechenzentrum abgesprochene Betriebsvereinbarungen am Campusnetzwerk angeschlossen und betrieben werden.

§1.2 Office-Switche (ungemanagte Switche) müssen vor Inbetriebnahme unter Nennung des Installationsortes und des Modells schriftlich an technik@rz.uni-kiel.de gemeldet werden.

§1.3 Gemanagte Switche dürfen ausschließlich durch RZ-Personal installiert, konfiguriert und betrieben werden.

§1.4 Netzwerkschränke dürfen ausschließlich von RZ-Personal oder in Absprache mit diesem geöffnet und gewartet werden.

§1.5 In Netzwerkschränken ist ausschließlich der Betrieb zentral verwalteter Netzwerkhardware zulässig.

§1.6 Funknetze dürfen ausschließlich vom Rechenzentrum betrieben werden.

§2 Netzwerke

§2.1 In Mitarbeiternetzen dürfen ausschließlich Arbeitsgeräte betrieben werden (Desktop-PCs, Notebooks, Drucker, Peripherie-Geräte). Server und ähnliche Geräte dürfen ausschließlich in Dienstnetzwerken betrieben werden. Für Geräte außerhalb dieser Kategorien behält sich das Rechenzentrum eine Abnahme und Anforderung einer Betriebsvereinbarung vor.

§2.2 Dienstnetzwerke dürfen ausschließlich in Räumlichkeiten des Rechenzentrums betrieben werden. Ausnahmen bedürfen einer Betriebsvereinbarung.

§2.3 Statische IP-Adressierung ist nur in Dienstnetzwerken erlaubt. In Mitarbeiternetzen ist DHCP zu verwenden.

§2.4 Netzwerkbasis- und Netzwerkkonfigurationsdienste dürfen ausschließlich vom Rechenzentrum betrieben werden (DHCP, DNS, RADIUS, VPN etc.).

§2.5 Der regelmäßige Zugang zu Netzen von außerhalb des Universitätsnetzes ist nur über das vom RZ betriebene VPN gestattet. Der Zugang zu dedizierten Mitarbeiternetzen bedarf eines Antrags.

§2.6 Der Einsatz von Fernwartungsdiensten (Teamviewer, AnyDesk etc.) ist nur temporär zur Nutzerunterstützung gestattet und nicht als dauerhafte Zugangsmöglichkeit.

§2.7 Der Einsatz von sog. Netzwerk-Scannern ist nur durch autorisierte Personen und ausschließlich innerhalb von Sub-Netzen der eigenen Einrichtung temporär für Administrationszwecke erlaubt. Jegliche, darüber hinaus gehende Analyse, Überwachung (Monitoring) oder Filterung von Netzwerk-Aktivitäten ist untersagt.

§2.8 Sowohl Client- als auch Dienstnetze sind nur für Geräte vorgesehen, für die regelmäßig von den Systemverantwortlichen (egal ob RZ oder dezentral) aktuelle Updates eingespielt werden können. Systeme, für die vom Hersteller keine Softwareupdates mehr bereitgestellt werden, müssen vom Netzwerk getrennt oder in speziell dafür vorgesehenen Netzen betrieben werden. Die Geräte sind entsprechend zu melden und bedürfen einer Betriebsvereinbarung.

Erläuterungen

1 Office-Switche

Office-Switche sind Layer-2-Switche ohne Konfigurationsmöglichkeit und unterstützen insb. keine Layer2 Virtualisierung-, Layer3 Routing- oder Spanning-Tree-Protokolle. Sie sind allerdings grundlegend von Hubs zu unterscheiden (Layer-1-Betrieb).

2 Mitarbeiternetze

Mitarbeiternetze sind die in Einrichtungsräumlichkeiten betriebenen Netze für die üblichen Arbeitsmittel der Einrichtung. Routen von außerhalb in Mitarbeiternetze werden nur über VPN gewährt. Routen aus dem Netz heraus beschränken sich auf Dienstnetze und das Internet.

3 Dienstnetze

Dienstnetze sind für Netzwerkhosts vorgesehen, die Ressourcen für mehrere Nutzer bereitstellen sollen. Darunter fallen dementsprechend virtuelle und physische Server, Appliances und verwandte Gerätekategorien.

4 Statische IP-Adressen vs. DHCP

Eine statische IP-Adresse ist eine IP-Adresse, die einem Endgerät oder Dienst bspw. durch manuellen Eintrag dauerhaft vergeben wird. In Mitarbeiternetzen mit ständig wechselnden Endgeräten verwenden wir hingegen dynamische IP-Adressen, die bei jedem erneuten Einbuchen des Endgerätes temporär von einem dafür vorgesehenen Dienst per DHCP (Dynamic Host Configuration Protocol) automatisch zugewiesen werden.

5 Netzwerkschränke

Netzwerkschränke in Einrichtungsräumlichkeiten sind Betriebsorte für Rechenzentrumshardware und dementsprechend nicht für die Unterbringung von Ressourcen vorgesehen, die Rechenzentrumsdienste wie Computing und Storage provisorisch zu ersetzen versuchen. Manipulationen an der Bestückung und/oder Verkabelung sind dementsprechend untersagt.

6 Funknetze

Bei den Funknetzen handelt es sich im Allgemeinen um das eduroam-WLAN. Parallelbetrieb von WLAN-Infrastrukturen wirkt sich störend auf die Primärinfrastruktur aus und stellt ein Sicherheitsrisiko dar, weshalb der Betrieb untersagt ist. Ferner ist bei Geräten, die zu Verwaltungs- oder Nutzungszwecken eigene WLANs ausstrahlen (z.B. Drucker, Smartscreens etc.), dieses zu deaktivieren.

7 Eine Betriebsvereinbarung im Sinne dieser Netzwerkrichtlinie ist ein Dokument, das für die betrachteten Objekte die Betriebsparameter definiert und den Betrieb regelt. Des Weiteren legt sie Rechte und Pflichten des Betreibers und des Rechenzentrums fest.