# Vernetzung der Rechner, Schulhausvernetzung

Für die Schulhausvernetzung sind gewisse Mindestanforderungen zu erfüllen:

* Die zentralen Komponenten eines Netzwerks (z. B. Router, konfigurierbare Switches, Server) müssen besonders geschützt werden. Ein physikalischer Schutz ist gegeben, wenn diese Komponenten in einem separaten **verschlossenen Serverraum** oder in abschließbaren Verteilerschränken untergebracht sind.
* Die ausreichende Kühlung bzw. Klimatisierung von Serverräumen und Verteiler- schränken erhöht die Verfügbarkeit und Lebensdauer der Geräte und ist deshalb anzuraten.
* Eine **unterbrechungsfreie Stromversorgung (USV)** kann sicherstellen, dass Server im Falle eines Stromausfalls ordnungsgemäß heruntergefahren werden, um eventuellen Schaden und damit verbundenen Datenverlust zu vermeiden.
* Ebenso müssen die zentralen Komponenten eines Netzwerks gegen Manipulationen und vor nicht berechtigten Zugriffen geschützt sein. Eine Absicherung erreicht man dadurch, dass der Konfigurationszugang zu den Geräten mit sicheren Passwörtern versehen ist und aus dem Unterrichtsnetz grundsätzlich nicht möglich ist.
* Schulnetze müssen zu bestimmten Zeiten (Unterrichtsbeginn und -ende) besondere Lastspitzen verarbeiten können. Gleichzeitige An- und Abmeldevorgänge oder der Zugriff auf einen Fileserver verursachen ein hohes Datenaufkommen und erfordern hochperformante Netzwerkhardware. Dies gilt sowohl für die kabelgebundene Infrastruktur als auch für Funknetze. Beim Zugriff auf cloudbasierte Dienste ist dies auch bei der Dimensionierung der Internetzugangsbandbreite zu berücksichtigen.
* **Datenschutz und Datensicherheit sind gerade im Verwaltungsbereich von heraus- gehobener Bedeutung**. Bei der Schulhausvernetzung gilt es dahingehend voraus- schauend zu planen und die dafür nötigen technischen Rahmenbedingungen zu schaffen.
* Die Integration aller Arbeitsplätze sowie aller Schüler- und Lehrergeräte in ein leistungsfähiges Rechnernetz ist heute Standard. Es wird empfohlen, mit der Planung, der Installation, der Wartung sowie der Reparatur einen darauf spezialisierten Dienstleister oder Anbieter zu beauftragen. Die Einweisung der mit der Systembetreuung betrauten Lehrkraft in die Administrationsmöglichkeiten des Rechnernetzes muss gewährleistet sein.

## Ethernet-Verkabelung (LAN)

Eine strukturierte, dienstneutrale Gebäudeverkabelung stellt eine Basisinfrastruktur dar. Die Netzwerkinfrastruktur wird dabei nicht mehr nur für die Informationstechnik, sondern auch für die Kommunikationstechnik sowie gegebenenfalls für Bereiche der Gebäude- und Gebäudeleittechnik genutzt und sollte daher großzügig geplant werden. Die Planungsrichtlinien für Kommunikationsnetze sind zu beachten (siehe Kapitel [11](#_bookmark0), [Weiterführende Literaturhinweise](#_bookmark0)). Bei Neu- und Umbauten sollten in allen Räumen ausreichend Netzwerkressourcen vorgesehen werden.

In großen vernetzten Umgebungen unterscheidet man zwischen

* **Primärverkabelung** (gebäudeübergreifendes Campusnetzwerk; typisch: Lichtwellen- leiter)
* **Sekundärverkabelung** (Backbone-Verkabelung innerhalb eines Gebäudes; Licht- wellenleiter, derzeit typische Übertragungsrate 10 GBit/s)
* **Tertiärverkabelung** (Arbeitsplatzverkabelung; Twisted-Pair-Kupfer-Verkabelung, derzeit typische Übertragungsrate 1 GBit/s)

Die Anbindung fester Arbeitsplätze und weiterer netzwerkfähiger nicht mobiler Clients (z. B. Drucker, interaktive Tafeln, zunehmend auch Beamer oder Dokumentenkameras) wird üblicherweise über eine Kupferverkabelung (Twisted-Pair-Verkabelung) mit Gigabit- Ethernet (1 GBit/s) durchgeführt. Im Backbone-Bereich wird 10 Gigabit-Ethernet (10 GBit/s) auf LWL-Basis empfohlen. Für jeden Arbeitsplatz sollte für gegebenenfalls zukünftige Erweiterungen mindestens eine LAN-Doppeldose (2 x RJ45) vorgesehen werden. Für die Anbringung von Access-Points sowie gegebenenfalls für das Anschließen von Beamern sind auch im Deckenbereich Stromsteckdosen und Netzwerkdosen sinnvoll.

Zunehmend ist es auch üblich, über die vorhandene Ethernet-Verkabelung Audio- oder Video-Signale (z. B. mit Ethernet-HDMI-Extender) zu übertragen oder diese zur Stromversorgung (PoE) zu nutzen.

Nachfolgend ist eine strukturierte Gebäudeverkabelung mit Primärverkabelung, Sekundärverkabelung und Tertiärverkabelung symbolhaft dargestellt.

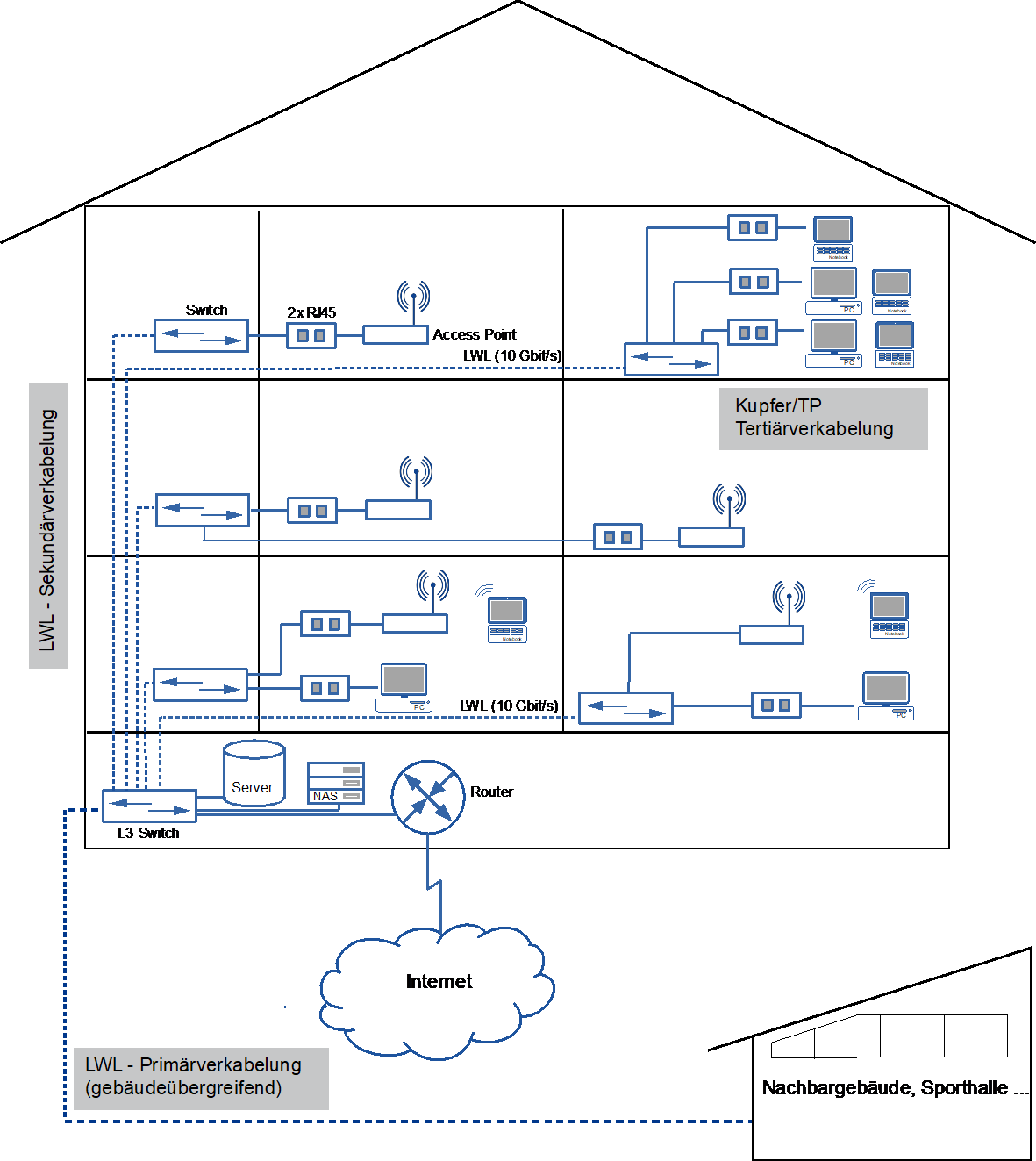
Die zentralen Komponenten des Netzwerks (z. B. Router mit Internetanbindung, Layer 3-Switch, Server, NAS) sollten in einem Serverraum (Gebäudehauptverteiler) unter- gebracht sein.

Die Switches (Layer-2-Switches), die die Verbindung zwischen Sekundär- und Tertiär- verkabelung herstellen, sollten in abschließbaren Verteilerschränken (Bereichsverteiler) untergebracht sein.

### Powerline

Eine Ergänzung zur strukturierten Verkabelung stellt die Powerline-Technologie dar. Sie eignet sich, wenn die Verbindung zu einem Gebäudeteil über eine strukturierte Verkabelung nicht möglich ist, aber vorhandene Stromnetze, Antennennetze oder Telefonleitungen verwendet werden können. Die Datenübertragungsrate bei Powerline ist mit WLAN vergleichbar. Die Betriebsstabilität und tatsächlich nutzbare Bandbreite muss individuell im Einsatzumfeld ermittelt werden.

Ähnlich wie bei WLAN ist auch bei Powerline eine räumliche Begrenzung des Zugangs praktisch nicht möglich. Von der Nutzung im Verwaltungsbereich wird deshalb abgeraten.



Strukturierte Gebäudeverkabelung mit Primär- Sekundär- und Tertiärverkabelung.

## Funknetz (WLAN)

Der Einsatz von mobilen Endgeräten, insbesondere Tablets oder Smartphones, ist ohne eine Funkanbindung nicht sinnvoll möglich. Ein Funknetz ergänzt eine strukturierte Gebäudeverkabelung, kann diese jedoch nicht ersetzen. Für stationäre IT-Geräte ist eine kabelgebundene Anbindung an das lokale Netz zu bevorzugen.

Die Anbindung von WLAN-fähigen Clients wird über Access-Points realisiert. Letztere sind per Kabel in das lokale Netz eingebunden. Für eine flächendeckende WLAN- Versorgung muss das Gebäude über eine entsprechende kabelbasierte Erschließung verfügen, um Access-Points geeignet positionieren zu können.

Möglich sind derzeit Übertragungsraten bis in den Gigabit-Bereich (Standards nach IEEE 802.11ac / WiFi 5 und IEEE 802.11ax / WiFi 6). Zu beachten ist, dass die Übertra- gungsqualität und die Übertragungsreichweite oftmals schwer einschätzbaren Umgebungseinflüssen (z. B. Stahlbetonwände) unterliegen. Dabei wird bei schlechter Übertragungsqualität die Übertragungsrate drastisch reduziert. In der Praxis wird selten mehr als ein Drittel der Brutto-Übertragungsrate erreicht, die sich alle an einem Access- Point angebundenen Clients teilen.

Bei Neuinstallationen sollte der Standard IEEE 802.11ac / WiFi 5 bzw. bereits der Nachfolger IEEE 802-11ax / WiFi 6 berücksichtigt werden. Geeignete Access-Points unterstützen die Clients im 2,4 GHz- und im 5 GHz-Bereich und bieten ausreichend hohe Übertragungsraten. Die Anbindung der Access-Points an das lokale Netz erfolgt dabei über Gigabit-Ethernet mit Übertragungsraten von 1 bzw. 2,5 GBit/s.

Bei der Planung einer WLAN-Infrastruktur ist auch darauf zu achten, dass die Schule über eine ausreichend große interne LAN- sowie Internetbandbreite (Download und Upload) verfügt. Nur so können ein stabiler Netzzugriff und die performante Nutzung externer Ressourcen gewährleistet werden.

Wenn WLAN die zentrale Netzzugangstechnik im Klassenzimmer ist und intensiv im Unterricht genutzt wird, kann vereinfacht von der Installation eines Access-Points pro Klassenzimmer ausgegangen werden. Bei komplizierten baulichen Situationen ist ggf. eine professionelle Ausleuchtung zur Planung der WLAN-Infrastruktur sinnvoll.

### WLAN-Controller

Eine WLAN-Infrastruktur mit mehreren Access-Points sollte über einen zentralen WLAN- Controller administriert werden. Dies ermöglicht eine schnelle Anpassung oder Erweiterung sowie ein zentrales Monitoring des WLAN-Netzes. Controller gibt es „On Premises” als Software auf einem Computer oder als separate Hardware und als cloudbasierte Variante. Cloudbasierte Controller sind, je nach Hersteller, auch mandantenfähig; d. h., mehrere Schulen lassen sich zentral über eine Plattform administrieren.

Grundsätzlich müssen die Access-Points zum Controller kompatibel sein. Dies bedingt die Festlegung auf einen Systemanbieter bzw. Hersteller. Bei Planung und Beschaffung empfiehlt es sich, auf eine Technologie zu setzen, die erweiterbar ist und auch in Hochlastumgebungen stabil funktioniert.

### Alternative Strukturen

WLAN-Mesh-Systeme können in einem Gebäude eine großflächige WLAN-Abdeckung ermöglichen, ohne dass alle Access-Points jeweils an ein kabelgebundenes Netzwerk angeschlossen sind. Mesh-Systeme bestehen aus sog. Satelliten und einer Basisstation. Sie bilden die Knoten des Mesh-Netzwerks. Alle Knoten kommunizieren untereinander über das Funknetz. Die zur Steuerung genutzten Signale und Datenübertragungen verringern die Bandbreite des Gesamtsystems. Mesh-Systeme sind nicht hersteller- übergreifend kompatibel. Als schulweite funktionsstabile WLAN-Infrastruktur ist dieser Ansatz nicht zu empfehlen, kann aber im Home-Bereich oder für spezielle Anwendungs- situationen sinnvoll sein.

WLAN-Repeater sind nicht geeignet, ein Funknetz mit den schultypischen Lastszenarien aufzubauen. Repeater verstärken Funksignale und vergrößern die Reichweite einer Funkzelle, sie erhöhen aber nicht die Bandbreite innerhalb des Empfangsbereichs. Der Einsatz von WLAN-Repeatern ist im Schulumfeld, mit Ausnahme sehr spezieller Einsatzszenarien, nicht zu empfehlen.

### Zugriffsschutz

Der Zugriff auf vertrauliche Ressourcen der Schule (z. B. Dateifreigaben) über das Funknetz der Schule muss abgesichert und darf nur autorisierten Personen möglich sein. Erreicht werden kann dies z. B. durch

* eine verschlüsselte Verbindung (z. B. mit WPA2 bzw. WPA3), deren Schlüssel nur autorisierten Personen bekannt ist (PSK, Pre-Shared-Key) oder
* eine zentrale individuelle Authentifizierung (z. B. Hotspot-Lösung mit Captive Portal- Authentifizierung, MAC-Adressen-Filterung oder IEEE 802.1x und Radius-Server).

Von der Nutzung von WLAN in Verwaltungsnetzen wird abgeraten, da eine räumliche Begrenzung dieser Netze ausschließlich auf den Verwaltungsbereich nicht möglich ist.

Ein separates, vom eigentlichen Schulnetz logisch getrenntes WLAN-Netz mit Internetzugang ist eine weitere Zugangsmöglichkeit, die z. B. für schülereigene Geräte sinnvoll sein kann. Dies ist z. B. bei BayernWLAN, einer Initiative des Bayerischen Staatsministeriums der Finanzen und für Heimat so realisiert. Informationen dazu sind unter <https://www.ldbv.bayern.de/breitband/bayernwlan.html>zu finden.

### Gesundheitliche Aspekte bei der Verwendung von WLAN

WLAN nutzt zur Datenübertragung Frequenzen im 2,4 GHz- und 5 GHz-Bereich. Alle in Deutschland zugelassenen technischen Geräte für den Aufbau von Funknetzwerken halten die empfohlenen strahlungsrelevanten Höchstwerte ein. Bei einem flächen- deckenden WLAN-Einsatz, z. B. bei Installation eines Access-Point je Klassenzimmer, kann die erforderliche Sendeleistung pro Access-Point reduziert und damit die punktuelle Strahlenbelastung minimiert werden.

WLAN-Systeme emittieren zur drahtlosen Informationsübertragung hochfrequente elektromagnetische Felder. Gesundheitliche Risiken dieser Felder wurden national und international, u. a. auch im Rahmen des Deutschen Mobilfunkforschungsprogramms, untersucht. Unterhalb der empfohlenen Höchstwerte sind vom Bundesamt für Strahlenschutz keine negativen gesundheitlichen Auswirkungen nachgewiesen. Messungen zeigen, dass bei der Anwendung von WLAN und anderen drahtlosen Übertragungstechniken die empfohlenen Höchstwerte bei Weitem nicht erreicht werden (siehe auch [https://www.bfs.de/SharedDocs/Downloads/BfS/DE/broschueren/emf/info-](https://www.bfs.de/SharedDocs/Downloads/BfS/DE/broschueren/emf/info-bluethooth-und-wlan.pdf?__blob=publicationFile&v=7) [bluethooth-und-wlan.pdf? blob=publicationFile&v=7](https://www.bfs.de/SharedDocs/Downloads/BfS/DE/broschueren/emf/info-bluethooth-und-wlan.pdf?__blob=publicationFile&v=7) sowie gleichlautende LT-Druck- sache 16/2362).

Ergänzende Hinweise zu Auswirkungen elektromagnetischer Felder bietet das Bayerische Staatsministerium für Gesundheit und Pflege unter [https://www.stmgp.bayern.de/vorsorge/umwelteinwirkungen/elektromagnetische-](https://www.stmgp.bayern.de/vorsorge/umwelteinwirkungen/elektromagnetische-strahlung) [strahlung](https://www.stmgp.bayern.de/vorsorge/umwelteinwirkungen/elektromagnetische-strahlung) und das Bayerische Staatsministerium für Umwelt und Verbraucherschutz unter <https://www.stmuv.bayern.de/themen/strahlenschutz/index.htm>.

Der Netzzugang mit Notebooks, Tablets oder Smartphones per WLAN ist, aufgrund einer geringeren Strahlung, einer Mobilfunkverbindung vorzuziehen (siehe z. B. BfS: „Smart- phones und Tablets – Tipps zur Reduzierung der Strahlenbelastung“, [https://www.bfs.de/DE/themen/emf/kompetenzzentrum/mobilfunk/schutz/smartphone-](https://www.bfs.de/DE/themen/emf/kompetenzzentrum/mobilfunk/schutz/smartphone-tablet.html) [tablet.html](https://www.bfs.de/DE/themen/emf/kompetenzzentrum/mobilfunk/schutz/smartphone-tablet.html)).

## Logische Trennung des lokalen Netzes in Teilnetze

Lokale Netze können in mehrere voneinander geschützte Teilnetze unterteilt werden. Jedes dieser Teilnetze ist ein eigenes logisches Netz, in dem eigene Sicherheits- standards definiert werden können. Die Teilnetze können über VLANs (bei Nutzung der gleichen physikalischen Verkabelung) oder über eine getrennte Verkabelung gebildet werden.

Zur Verbindung von Teilnetzen bzw. zur Kommunikation zwischen den Teilnetzen ist ein Router oder ein Layer-3-Switch nötig. Damit lassen sich kontrollierbare Übergänge einrichten. Durch Firewall-Regeln wird festgelegt, zwischen welchen Teilnetzen kommuniziert und wie jeweils auf das Internet zugegriffen werden kann.

In der Grafik sind verschiedene Teilnetze dargestellt, die durch einen zentralen Router verbunden sind. Über die im Router integrierte Firewall können Zugriffe zwischen den einzelnen Netzen bzw. dem Internet geregelt werden.



Internet

Notebook

Gäste-WLAN/BYOD

Firewall

+Router

Switch

Access Point

Digitale Geräte

für den Unterricht

Notebook

Notebook

Notebook

PC

Unterricht Lehrer Verwaltung

PC

PC

PC

Beispielhafte Darstellung verschiedener Teilnetze in der Schule

Zur Gewährleistung des jeweiligen Schutzbedarfes ist es sinnvoll, Verwaltungsbereich, Lehrerbereich und Schüler-/Unterrichtsbereich in verschiedene Teilnetze zu trennen. Ein Zugriff vom Schüler-/Unterrichtsbereich aus auf Rechner in den beiden anderen Bereichen darf nicht möglich sein. Ein Zugriff vom Lehrerbereich auf Rechner des

Verwaltungsbereichs ist auf diejenigen Dienste der Schulverwaltung einzuschränken, die zur Verwendung durch die Lehrkräfte vorgesehen sind.

Über WLAN-Multi-SSID lassen sich auch unterschiedliche WLAN-Netze und Einsatz- varianten definieren (z. B. Lehrer-WLAN, Schüler-WLAN, Gäste-WLAN etc.). So kann für schuleigene oder schulfremde Geräte bestimmt werden, auf welche Ressourcen, wie Internet oder interne Serverangebote diese zugreifen dürfen. Auch Störungen oder Überlastungen sind so üblicherweise auf die jeweiligen Teilnetze beschränkt.

Eine weitere Trennung in mehrere Teilnetze innerhalb des Unterrichtsbereiches kann aus denselben Gründen sinnvoll sein (z. B. in einzelne Computerräume, Klassen- bereiche, Fachräume).

# Verbindung mit dem Internet

## Internetzugang

Ein ausreichend leistungsstarker Internetzugang ist für Schulen unverzichtbar. Um in Zeiten einer zunehmenden Verlagerung von Ressourcen und Diensten ins Internet Online-Angebote in der Schule sinnvoll nutzen zu können, ist eine möglichst hohe Bandbreite notwendig. Erklärtes Ziel der Bayerischen Staatsregierung ist die Anbindung der Schulen über einen breitbandigen Glasfaseranschluss.

Grundsätzlich werden aktuell drei unterschiedliche Techniken beim kabelgebundenen Internetzugang angeboten: DSL, Kabelnetz und Glasfaser. Die Techniken unterscheiden sich hinsichtlich Bandbreite und Stabilität deutlich. DSL verwendet die vorhandenen Kupferkabel des Telefonnetzes und hat aufgrund technischer und physikalischer Beschränkungen nur eine gewisse maximale Bandbreite, die nahezu ausgereizt ist. Hier sind zukünftig keine großen Zuwächse in der Bandbreite zu erwarten. Im Kabelnetz wird der Breitbandzugang über die Kabelfernsehnetze realisiert. Es handelt sich dabei um ein

„Shared Medium”, das heißt, die vorhandene Bandbreite wird auf die Anschlussinhaber aufgeteilt. Es kann somit unabhängig von der gebuchten maximalen Bandbreite zu deutlichen Leistungsschwankungen in Stoßzeiten kommen.

Lichtwellenleiter (Glasfaser) haben die genannten Probleme der Bandbreitenbeschrän- kung bzw. Leistungsschwankungen nicht. Hier ist eine erheblich höhere maximale Bandbreite möglich. Im Kontext des Breitbandzugangs einer Schule ist aufgrund der deutlich besseren Skalierbarkeit und Zukunftssicherheit unbedingt ein Glasfaser- anschluss anzustreben.

Im Bereich der DSL-Anschlüsse sind aktuell bis zu 250 Mbit/s im Downstream und 40 Mbit/s im Upstream möglich. Im Kabelnetz sind Datenraten von bis zu 1000 Mbit/s und 50 Mbit/s im Upstream möglich. Glasfaser-Tarife sind sowohl mit symmetrischer als auch asymmetrischer Bandbreitenaufteilung verfügbar. Hier werden Datenraten von z. B.

1.000 Mbit/s im Down- und Upstream angeboten.

Neben der Bandbreite sind die Verfügbarkeit und der Support wichtige Leistungs- merkmale. Geschäfts- bzw. Business-Anschlüsse bieten oft den notwendigen Service und eine kurzfristigere Entstörung.

Der Bandbreitenbedarf einer Schule ist von verschiedenen Faktoren abhängig. Schulart und Schüleranzahl sind grundlegende Kalkulationsgrößen. Die Anwendungsart und

-intensität ergeben sich aus den unterrichtlichen Nutzungsszenarien. In besonderem Maße ist bei der Nutzung externer Lernplattformen, Videokonferenztools oder von Cloud-Diensten der deutlich zunehmende Bedarf an Upstream-Geschwindigkeit zu berücksichtigen. Das Aufrufen und Abspeichern von Daten bei Cloud-Diensten führt vor allem am Unterrichtsanfang und -ende zu hohen Netzbelastungen.

Für typische Anwendungsszenarien, wie zum Beispiel die aktive Medienarbeit und das Speichern von Daten auf internetbasierten Cloudspeichern, kann zur Berechnung vereinfacht von einem symmetrischen Bandbreitenbedarf von etwa 1 MBit/s pro aktivem Nutzer ausgegangen werden. Insgesamt sollte die verfügbare Internetbandbreite einer Schule – abhängig von der Schulgröße – bei einer DSL-Anbindung idealerweise nicht weniger als 100 MBit/s (40 MBit/s im Upstream) betragen.

Mit zunehmender Schülerzahl sollte überlegt werden, ob ein weiterer Internetzugang für die Schule zur Lastverteilung und Ausfallsicherheit sinnvoll ist. Schulen, die noch keinen Breitbandzugang zum Internet haben, wird empfohlen, über ihre Kommune eine Auf- nahme in den Ausbaubereich im Rahmen der verschiedenen Breitbandförderprogramme des Freistaats Bayern und des Bundes zu erwirken.

Der Internetzugang über das Mobilfunknetz per LTE/5G kann den kabelgebundenen Zugang flexibel ergänzen oder als Backupverbindung herangezogen werden. Bei der Wahl des Mobilfunktarifs ist darauf zu achten, dass dieser keine Volumenbegrenzung hat. Verschiedene Anbieter haben oftmals spezielle Bildungstarife in ihrem Portfolio.

## Internetzugangsrouter mit Firewall

Dem Internetzugangsrouter der Schule kommt als zentraler Übergangsknotenpunkt, an dem sehr effektiv der Datenfluss zwischen dem lokalen Netz und dem Internet gesteuert werden kann, eine besondere Bedeutung zu. Der Router sollte den Einsatz unter hohen Lastbedingungen gewährleisten, unterschiedliche Netze anbinden können, differen- zierte Firewall-Einstellungen bieten und gegebenenfalls einen redundanten Internet- anschluss ermöglichen. Internetzugangsrouter aus dem Heimbereich bieten diese Eigenschaften nicht.

Bereits mit einer Standardkonfiguration bieten Internetzugangsrouter einen guten Schutz gegen Angriffe oder ungewollte Zugriffe aus dem Internet.

### Dedizierte Firewall-Systeme und UTM

Umgebungen mit hohen Sicherheitsanforderungen setzen komplexe und aufwändig zu konfigurierende Firewalls bzw. UTM-Systeme (Unified-Threat-Management) ein. Diese Systeme integrieren neben klassischen Filtern auf IP- und Protokollebene zusätzliche Sicherheits- und Filterfunktionen, wie z. B. Authentifizierung, VPN, Intrusion-Detection, Intrusion-Prevention oder Content-Filter.

UTM-Systeme gehen oft über den Sicherheitsbedarf einer Schule hinaus. Die komplexe Konfiguration und Administration sind neben den meist anfallenden regelmäßigen Lizenzgebühren zu bedenkende Kriterien.

## Webfilter

Der Schutz der Kinder und Jugendlichen vor unerwünschten Inhalten aus dem Internet ist Anliegen und Auftrag der Schule. Dazu wurden als technisches Hilfsmittel Webfilter entwickelt, die den Zugang zu Internet-Ressourcen kontrollieren sollen, um Kinder und Jugendliche vor schwierigen Situationen im Umgang mit digitalen Medien, vor allem der Konfrontation mit unangemessenen Inhalten, zu bewahren.

Der Einsatz eines Webfilters entbindet die Schule jedoch nicht von ihrer zentralen Aufgabe, die Medienkompetenz der Schülerinnen und Schüler zu fördern. Diese werden durch die Lehrkräfte zum verantwortungsbewussten Arbeiten mit Medien angeleitet und dabei begleitet.

Die zunehmende Digitalisierung erfordert den kompetenten, selbstverantwortlichen Umgang auch insofern, als das Internet außerhalb der schulischen Infrastruktur für Kinder und Jugendliche immer häufiger als selbstverständliche Ressource überall und zumeist ohne Beschränkungen verfügbar ist.

Wenn sich eine Schule für einen Webfilter entscheidet, um die kontinuierliche und präventive Aufsicht der Schule zu unterstützen, kann die Berücksichtigung folgender Kriterien bei der Auswahl hilfreich sein:

### Betriebsstabilität, Performanz und technische Zuverlässigkeit

Ein Webfilter beeinflusst an einem zentralen Punkt die Anbindung des Unterrichtsnetzes an das Internet. Ein dauerhaft stabiler und zuverlässiger Betrieb ist deshalb unabdingbar. Der Webfilter darf die Internetverbindung oder das Aufrufen von Webseiten nicht merklich verlangsamen und muss mit allen Desktop-Computern, Notebooks, Tablets und weiteren mobilen Endgeräten funktionieren. Die Filterung von http- und https-Seiten muss gleichermaßen möglich sein.

### Integration in das Unterrichtsnetz

Ein Webfilter muss in das Unterrichtsnetz der Schule integrierbar sein und muss sich in das Nutzungskonzept der Schule einfügen. An den schüler- bzw. lehrereigenen Geräten sollte der Webfilter funktionieren, ohne dass dort Änderungen an der Konfiguration vorgenommen werden müssen.

### Inhaltliche Zuverlässigkeit

Bei der bestimmungsgemäßen Arbeit im Unterricht sollte man den Webfilter nicht bemerken. Üblicherweise werden Webfilter danach bewertet, wie zuverlässig diese unerwünschte Webseiten sperren. Ebenso wichtig ist, dass Webfilter erwünschte Web- seiten und Dienste zulassen und den Unterricht nicht behindern.

### Globale Einstellung durch die Schule

Die Schule sollte eine einfache Möglichkeit haben, die Filterung zu beeinflussen (z. B. Auswahl der zu filternden Kategorien, eigene Blacklist, eigene Whitelist). Sinnvoll ist es, wenn die Filterregeln entsprechend dem Alter, der Medienkompetenz, der Selbstverant- wortung und Einsichtsfähigkeit der Schülerinnen und Schüler voreingestellt werden können.

### Nutzung durch die Lehrkraft

Flexible Differenzierungen der Filtereinstellungen in einzelnen Unterrichtsstunden und für einzelne Klassen sind oft unpraktikabel. Der Unterricht am Computer sollte möglich sein, ohne dass die Lehrkraft im Vorfeld den Filter zwingend anpassen muss.

### Protokollierung der Web-Zugriffe

Werden von einem Webfilter personenbezogene Daten in Logdateien gespeichert, sind die Anforderungen des Datenschutzes zu beachten.

### Technische Umsetzung

Webfilter über einen Proxyserver erlauben sehr differenzierte Einstellungen anhand von Benutzerkennungen, Computerkennungen oder auch differenzierte zeitliche Ein- stellungen (z. B. Ausschalten der Filterregeln für einzelne Unterrichtsstunden). Bei der Filterung von https-Seiten und bei der Arbeit mit mobilen Geräten bereiten Proxyserver häufig Probleme. Zahlreiche Apps bei Smartphones und Tablets funktionieren unter Verwendung eines (auch transparenten) Proxyservers nicht wie gewünscht.

Eine andere Möglichkeit ist eine Filterung über den DNS-Dienst, der von allen Geräten, die einen Internetzugang benötigen, verwendet wird. Eine externe DNS-Filterung bindet keine Ressourcen in der Schule, erlaubt jedoch keine differenzierten Filtereinstellungen innerhalb der Schule.

Es besteht keine grundsätzliche Verpflichtung für Schulen, eine technische Lösung einzusetzen, um unerwünschte Internetseiten zu filtern bzw. Internetaktivitäten zu protokollieren.