Bayerisches Staatsministerium für
Unterricht und Kultus

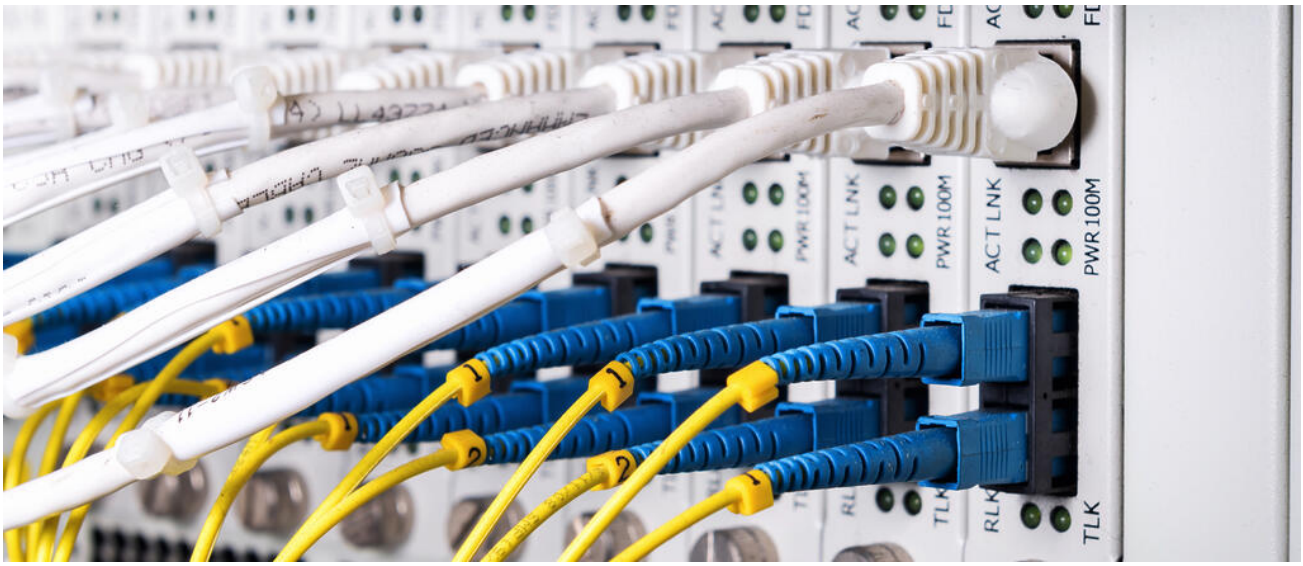
Schulnetz

Stand: 22.12.2024

→ www.km.bayern.de / gestalten / digitalisierung / datensicherheit / schulnetz

Inhaltsverzeichnis

Schulnetz



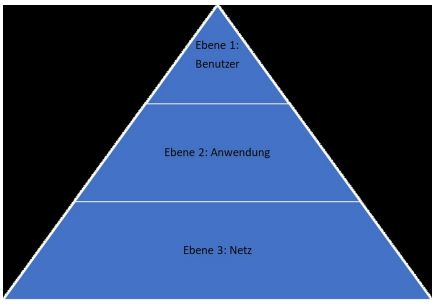
Standards garantieren einen sicheren Aufbau des Schulnetzes ©jackykids - stock.adobe.com

Sicherheit im Schulnetz

Datenschutz, Datensicherheit und Funktionsstabilität sind zentrale Anforderungen an ein funktionierendes Schulnetz.

Sicherheit im Schulnetz

- bezieht sich auf benutzerbasierte individuelle Aspekte (Ebene 1)
- und hat einen Bezug zu Anwendungen und den möglichen Zugriff auf Ressourcen (Ebene 2).
- Bereits auf der Netzwerkebene kann der Wirkbereich eines Nutzers eingeschränkt und damit die Sicherheit erhöht werden (Ebene 3).



©Bayerisches Staatsministerium für Unterricht und Kultus

Während die Ebenen 1 und 2 an anderen Stellen dieses Internetauftritts behandelt werden, gibt diese Seite einen Überblick über die wichtigsten Komponenten und Maßnahmen der Netzebene (Ebene 3), damit ein reibungsloser und sicherer Betrieb des Schulnetzes gewährleistet ist.

Zielgruppe: Systembetreuer, Schulleitung, Schulaufwandsträger

Schulnetzdesign

Schulnetze stehen teilweise unter enormen Belastungen, da Lernende und Lehrkräfte gleichzeitig auf das WLAN und das Internet zugreifen. Ohne eine gut geplante und strukturierte Netzwerkinfrastruktur drohen Leistungseinbußen und Sicherheitsrisiken. Besonders wichtig ist die **Trennung von pädagogischem Netzwerk und Verwaltungsnetz**, um sensible Daten zu schützen. Eine durchdachte Segmentierung mit Virtual LANs (VLANs) und Firewalls sorgt dafür, dass verschiedene Netzbereiche eine sichere und effiziente Kommunikation ermöglichen. Nur so lassen sich die Anforderungen an Datensicherheit und Datenschutz erfüllen, während das Netz auch Lastspitzen problemlos bewältigt.

Mehr zu Netzdesign

Funktionsstabilität und Datensicherheit

Schulnetze sind hohen Lastsituationen ausgesetzt. In kurzen Zeitabschnitten melden sich Lernende und Lehrkräfte an, greifen auf das WLAN und das Internet zu. Ein gut strukturiertes und dimensioniertes Schulnetz bietet die notwendige Funktionsstabilität und diese Lastspitzen verarbeiten zu können.
Voraussetzung dafür sind ausreichende Bandbreiten auf den Übertragungsstrecken, leistungsfähige Netzwerkgeräte und eine, von der Schulnetzgröße abhängige, Segmentierung. Durchgängig performante Kommunikationspfade sind das Ergebnis einer korrekten Planung und Umsetzung.

Weitere Anforderungen

Neben dem pädagogischen Netzwerk ist das Verwaltungsnetz ein weiterer Bereich der Schulnetzinfrastruktur. Im Verwaltungsnetz gelten hohe Anforderungen bezüglich der Datensicherheit und des Datenschutzes.

Die Kommunikation zwischen den Teilnetzen Unterrichtsnetz und Verwaltungsnetz sollte, aufgrund der hohen Vertraulichkeit im Verwaltungsnetz, unmöglich oder aber auf sehr wenige spezifische Ausnahmefälle beschränkt sein.

Netzwerktechnik

Mit geeigneten Netzwerkgeräten lassen sich Teilnetze innerhalb der Infrastruktur bilden. Die Technik **Virtual LAN (VLAN)** bietet die Möglichkeit, das Schulnetz zu segmentieren. Schulinterne Firewalls steuern die Kommunikation zwischen diesen Netzbereichen. Die Firewall-Funktionen sind Bestandteil der zentralen Router bzw. L3-Switches.

Beispiele für Netzsegmente bzw. Teilnetze in der Schule sind: Unterricht-, Schüler-WLAN,

Verwaltungsnetz.

Weiterführende Informationen zum Netzdesign und eine Konfigurationsübersicht mit Checkliste zum Switch befinden sich in den nachfolgenden Dokumenten.

Handreichung Netzdesign
/download/4-24-11/241107_Handreichung_Netzdesign.jpg

Beispielkonfiguration Netzdesign
/download/4-24-11/241107_Beispielkonfiguration_Netzdesign.jpg

Muster Netzdesign
/download/4-24-11/241107_Muster_KonfigNetzdesign.jpg

Berechtigungsmatrix

Eine Schule muss festlegen, auf welche Netze, Server oder Clouddienste der Schule die einzelnen Benutzer Zugang haben. Dabei sind stets das **need-to-know**-Prinzip und die gesetzlichen Vorgaben zu beachten. Aus der Berechtigungsmatrix muss ersichtlich sein, welche Dienste aus dem Verwaltungsnetz bzw. aus Unterrichtsnetz erreichbar sind.

Mehr zu Berechtigungsmatrix

Die Berechtigungsmatrix ist zu Dokumentationspflichten zu verakten und vor unberechtigtem Zugang zu schützen.

Ein Beispiel- und ein Musterdokument ist nachfolgend abrufbar.

Beispiel einer Berechtigungsmatrix
/download/4-24-02/241114_Beispiel_Berechtigungsmatrix.jpg

Muster Berechtigungsmatrix
/download/4-24-02/Mustertabelle-Berechtigungsmatrix.jpg

Fernzugriff (VPN)

Der Fernzugriff auf das Schulnetzwerk über VPN bietet eine sichere Möglichkeit, sensible Daten zu übertragen, birgt jedoch auch potenzielle Risiken. Um unbefugten Zugriff zu verhindern, ist eine starke Authentifizierung unerlässlich. Neben der Verschlüsselung der Daten ist die Implementierung von Zwei-Faktor-Authentifizierung (2FA) eine wichtige Sicherheitsmaßnahme. Ein VPN-Gateway auf der Schulseite und ein kompatibler Client auf der Nutzerseite sind Voraussetzung für den sicheren Betrieb. Besonders bei der Anbindung externer Standorte (Site-to-Site-VPN) müssen erhöhte Sicherheitsanforderungen beachtet werden.

Mehr zu Fernzugriff (VPN)

Mit VPN-Technik auf das Netz der Schule zugreifen.

Der Zugriff auf Daten oder Systeme im Netzwerk der Schule kann aus verschiedenen Gründen notwendig sein. Da dies nur ausgewählten Personen möglich sein soll, muss die **Authentizität** nachgewiesen werden.

Zur Wahrung der **Vertraulichkeit** ist es erforderlich, die Daten zu verschlüsseln.

VPN-Technologien (Virtual Private Network) bieten die Merkmale einer sicheren Datenübertragung und ermöglichen damit die vertrauliche Kommunikation über unsichere Netze (Internet).

Der Zugriff auf das Schulnetz bzw. das Netzwerk der Verwaltung einer Schule darf nur ausgewählten Personen möglich sein. Dazu zählen Schulleitungen oder Mitarbeitende der IT-Administration (Client-to-Site-VPN). Erhöhte Sicherheitsanforderungen können die Integration einer 2-Faktor-Authentifizierung (2FA) erforderlich machen.

Um eine VPN-Verbindung nutzen zu können, muss auf der Seite der Schule die Funktion des VPN-Gateways eingerichtet sein. Auf der Anwenderseite ist ein kompatibler Client erforderlich.

Die Anbindung einer Außenstellung ist ein weiteres Szenario für den Einsatz von VPN (Site-to-Site-VPN).

Eine mögliche VPN-Technik ist das Protokoll IPSec.

Weiterführende Informationen zu VPN und eine Konfigurationsübersicht mit Checkliste befinden sich in den nachfolgenden Dokumenten

Handreichung VPN
/download/4-24-11/241111_Handreichung_VPN.jpg

Beispielkonfiguration VPN
/download/4-24-11/241111_Beispielkonfiguration_VPN.jpg

Muster VPN
/download/4-24-11/241111_Muster_VPN.jpg

Firewall

Für eine sichere und kontrollierte Kommunikation in Schulnetzen sind Firewalls unverzichtbar. Sie filtern Datenpakete nach vordefinierten Regeln und verhindern unbefugte Zugriffe, insbesondere aus dem Internet. Der Zugriff ins Schulnetz von außen ist nur über sichere VPN-Verbindungen möglich. Gleichzeitig wird der ausgehende Datenverkehr auf notwendige Protokolle beschränkt. Firewalls trennen zudem interne Netzbereiche, um unerlaubte Zugriffe, etwa vom Unterrichts- ins Verwaltungsnetz, zu verhindern. Moderne Lösungen wie Next-Generation-Firewalls bieten zusätzlichen Schutz vor komplexen Bedrohungen.

Mehr zu Firewall

Firewall-Systeme blockieren unerwünschte Kommunikation

Die sichere Kommunikation über Netzgrenzen hinweg, erfordert die kontrollierte Weiterleitung oder auch das Blockieren von Daten. Dies gilt sowohl für schulinterne Kommunikationsprozesse als auch für den Datenaustausch mit dem Internet.

Firewalls untersuchen die übertragenden Datenpakete und filtern auf Basis vordefinierter Regeln.

Der Verbindungsaufbau aus dem Internet in das lokale Schulnetz muss verhindert werden. Eine Ausnahme bilden kontrollierte Zugänge per VPN. Viele Hackerangriffe lassen sich durch Firewalls wirkungsvoll blockieren.

Der Netzwerkverkehr aus dem Schulnetz in das Internet sollte gefiltert und damit auf die notwendigen Protokolle begrenzt werden. Dies verhindert unerwünschte Verbindungs-aufbauten auf Netzwerkebene.

Firewall-Systeme werden darüber hinaus auch für die Steuerung der schulinternen Datenkommunikation eingesetzt. Auf diese Art lassen sich Netzbereiche voneinander abtrennen. Ein unerlaubter Zugriff, zum Beispiel aus dem Unterrichts- auf das Verwaltungsnetz, ist damit unterbunden.

Die Firewall-Funktion ist in aller Regel Bestandteil der eingesetzten Router. In besonderen Fällen ist können dedizierte Firewalls (IPS/IDS, Next-Generation-Firewall) spezielle erhöhte Sicherheitsanforderungen erfüllen.

Detaillierte Informationen, sowie eine Checkliste und eine Beispielkonfiguration zu Firewalls und Routern finden sich in den nachfolgenden Dokumenten.

Handreichung Router mit Firewall
/download/4-24-11/241108_Handreichung_RouterFirewall.jpg

Beispielkonfiguration Firewall-Router
/download/4-24-11/241108_Beispielkonfiguration_RouterFirewall.jpg

Muster Firewall-Router
/download/4-24-11/241108_Muster_KonfigRouterFirewall.jpg

Webfilter

Webfilter bieten einen wichtigen Schutz vor ungeeigneten Inhalten und Bedrohungen im Internet. Sie sperren nicht nur gefährliche Websites, sondern auch den Internetzugriff von Apps und Links aus Spam-Mails. Besonders die DNS-Filtertechnologie überzeugt durch Skalierbarkeit und Geschwindigkeit, ohne spezielle Hardware zu benötigen. Schulen sind zwar nicht verpflichtet, Webfilter einzusetzen, doch sie bieten eine effektive Möglichkeit die Schülerinnen und Schüler zu schützen. Bei der Auswahl eines Filters sollten Kriterien wie Jugendschutz, Zuverlässigkeit und einfache Konfiguration im Fokus stehen.

Mehr zu Webfiltern

Webfilter in der Schule

Nicht alle Internetseiten und Inhalte sind lernförderlich, im Schuleinsatz erwünscht oder sogar jugendgefährdend. Mit Webfiltern können Zugriffe auf solche unerwünschten Webseiten und Inhalte eingeschränkt werden.

Rahmenbedingungen und Herausforderungen

Schulnetzwerke zeichnen sich durch heterogene Systeme bzw. Endgeräte aus. Webfilter müssen daher an einer zentralen Kommunikationsschnittstelle platziert werden. Der Internetzugangsrouter oder ein zentraler DNS-Server der Schule sind solche Schnittstellen. Bei entsprechender Konfiguration müssen alle Endgeräte diese Dienste nutzen.

An diesen Stellen können Filterfunktionen integriert werden. Relativ einfach und effektiv lassen sich Filter auf Basis der Namensauflösung DNS (Domain Name Service) realisieren.

Technik

Ein DNS-Filterdienst kategorisiert Webseiten und meldet, wenn eine Webseite zu einer Sperrkategorie gehört. Dieser Filterserver ist auf dem Router der Schule eingetragen, alternative DNS-Server sind durch die Firewall nicht erreichbar.

Neben der DNS-basierten Filtertechnologie gibt es weitere, meist komplexere Web- und Content-Filter. Die Heterogenität der (mobilen) Clients, die Anforderung an eine performante Netzwerkkommunikation sowie die einfache Integration in das Schulnetzwerk geben in der Regel dem DNS-basierten Webfilter den Vorzug.

Filterfunktionen und Grenzen

Der Aufruf von Webseiten erfolgt über die Angabe des Namens der Seite bzw. des Webservers. Ist bekannt, dass dieser Server jugendgefährdende Inhalte (z.B. Gewalt, Pornografie, Waffen etc.) anbietet, wird er entsprechend kategorisiert und die Web-Kommunikation mit diesem Server unterbunden. DNS-Filter sind nicht dafür ausgelegt, spezifische Inhalte zu erkennen und zu filtern. Auch für die Erkennung von Spam oder Malware müssen andere Systeme hinzugezogen werden.

Hinweise

Der Einsatz von Webfiltern obliegt der pädagogischen Verantwortung der Schule. Es besteht keine grundsätzliche Verpflichtung für den Einsatz von Filtertechnik.

Weiterführende Informationen finden sich in den „Empfehlungen zur IT-Ausstattung von Schulen“ unter dem folgenden Link.

Votum 23/24 S. 48ff
https://mebis.bycs.de/beitrag/votum

WLAN

Sicheres WLAN ist in Schulen unerlässlich, um sowohl den Zugang zum Internet als auch zu lokalen Ressourcen zu ermöglichen. Doch drahtlose Netzwerke bergen Risiken: Da Daten über Funk übertragen werden, sind sie potenziell abhörbar. Um dies zu verhindern, sollten moderne Verschlüsselungsstandards wie WPA2/3 eingesetzt werden. Besonders wichtig ist die Trennung von Netzen, um sensible Daten von allgemeinen Internetzugängen zu schützen. Multi-SSID-Lösungen und VLANs ermöglichen eine flexible Netzwerknutzung mit unterschiedlichen Sicherheitsstufen für Schüler, Lehrkräfte und Gäste. Die richtige Konfiguration der Access Points, eine starke Authentifizierung und regelmäßige Firmware-Updates sind entscheidend, um Sicherheitslücken zu vermeiden und den Unterrichtsbetrieb nicht zu gefährden.

Mehr zu WLAN

Kabellos im Unterricht

Wireless-LAN (WLAN) bietet mobilen Endgeräten den unkomplizierten Zugang zum Schulnetz mit Internetzugang.

Sicherheit

Da die Datenübertragung per WLAN nicht an eine geschützte Verkabelung gebunden ist, müssen zusätzliche Maßnahmen zur Absicherung getroffen werden. Aktuelle Sicherheitsmechanismen bieten die Authentifizierung mittels gemeinsamen Passwortes und die Verschlüsselung der Daten (WPA2/3-PSK). Die Forderungen an einen einfachen, technisch niederschwelligen, aber auch sicheren Netzzugang, können mit diesem Verfahren erfüllt werden.

Besondere Anforderungen im Verwaltungsnetz

Für das Verwaltungsnetz der Schule bestehen erhöhte Sicherheitsanforderungen. In diesem Bereich sollte auf den Einsatz von WLAN verzichtet werden.

Segmentierung

Um die Funktionsstabilität und Sicherheit zu steigern, kann das WLAN als ein separates Teilnetz (WLAN als VLAN) betrieben werden. Dabei ist zu prüfen, auf welche internen Systeme der Schule (Drucker, Bildschirmübertragung etc.) WLAN-Clients zugreifen müssen. Der Zugang zum Internet und Cloud-Diensten wird Schwerpunkt der Nutzung sein.
WLAN in der Schule bedeutet die Berücksichtigung von Lastsituationen (Hochlastbetrieb, High Density). Die Anforderungen an eine solche Umgebung gilt es bereits bei der Planung zu

beachten.

Die Administration und Wartung der WLAN-Access-Points erfolgen in aller Regel über einen WLAN-Controller.

Detailliertere Informationen und Beispiele zur Dokumentation beim Einsatz von WLAN in Schulen befinden sich in der nachfolgenden Handreichung.

Handreichung WLAN
/download/4-24-11/241111_Handreichung_WLAN.jpg

Beispielkonfiguration WLAN
/download/4-24-11/241111_Beispielkonfiguration_WLAN.jpg

Muster WLAN
/download/4-24-11/241111_Muster_WLAN.jpg

Nutzungsordnung

Votum