

## Handreichung

# Netzwerkarchitektur für die Schul-IT

## Zweck

Die vorliegende Handreichung richtet sich primär an die umsetzenden Personen im Bereich der Netzwerkarchitektur für Schulen und Schulträger. Dieser Personenkreis inkludiert Fachpersonal im IT-Bereich der Schulträger und Schulen. Konkret können das Personen aus Rechenzentren oder der IT-Abteilung eines Schulträgers sowie Lehrkräfte in Schulen sein, die für die Umsetzung der IT in den Schulen verantwortlich sind.

Darüber hinaus sollen auch Verantwortliche für die Informationssicherheit angesprochen werden, da die Netzwerkarchitektur grundlegend für die Informationssicherheit und IT-Sicherheit ist.

Da die Zielgruppe dieses Papiers Experten und Expertinnen sowie Fachpersonal in der Netzwerkarchitektur sind, ist dieses sehr auf die Technik bezogen, ohne weitere Erklärungen für Laien, aufgebaut.

## Anwendungsempfehlungen

Ziel ist es, die Umsetzungsverantwortlichen der Netzwerkarchitektur über die notwendigen Maßnahmen zur IT-Sicherheit zu informieren und sie zur Umsetzung zu befähigen.

Des Weiteren sollen sich IT-Verantwortliche einen Eindruck darüber verschaffen können, welche Ressourcen im Bereich des Netzwerks notwendig sind, um eine sichere IT in den Schulen und beim Schulträger aufzubauen.



### **Schon gewusst?**

Mehr Fachwissen zum Thema Schul-IT finden Sie auf unserer Webseite:

 [www.schul-it-navigator.de](http://www.schul-it-navigator.de)

### **Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen noch etwas?**

Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden. Wir freuen uns auf Ihre Rückmeldung.

 [feedback@schul-it-navigator.de](mailto:feedback@schul-it-navigator.de)

## Inhaltsverzeichnis

<b>Zweck</b> .....	<b>1</b>
<b>Anwendungsempfehlungen</b> .....	<b>1</b>
<b>Einleitung</b> .....	<b>3</b>
<b>Netzpläne – Grundlagen und wichtige Konzepte</b> .....	<b>3</b>
Zonierung und Mikrosegmentierung .....	3
P-A-P-Struktur (Paketfilter – Application Level Gateway – Paketfilter) .....	4
Erster Paketfilter – äußerer Paketfilter zum Internet .....	5
A – Application Level Gateway (ALG) / Proxy-Firewall .....	6
Zweiter Paketfilter – innerer Paketfilter zu den internen Netzzonen .....	6
Was verhindert die P-A-P-Struktur? .....	7
Was ist eine DMZ und wie hängt sie mit der P-A-P-Struktur zusammen? .....	7
Warum ist die P-A-P-Struktur besonders für Schulen wichtig? .....	8
<b>Ausfallsicherheit und Redundanz</b> .....	<b>8</b>
Anbindung einer Schule an einen externen IT-Dienstleister .....	8
Netz und Out-of-Band-Management (OOB) .....	9
RADIUS-Server und Authentifizierung im Schulnetz .....	10
<b>Backup und die 3-2-1-Regel – Schutz vor Datenverlust und Ransomware</b> .....	<b>11</b>
Backups im Kontext von Ransomware .....	11
Die 3-2-1-Regel – der zentrale Leitfaden .....	12
Warum externe und „Air-Gap“-Backups unverzichtbar sind .....	12
Backups müssen geplant, dokumentiert und getestet werden .....	13
Was passiert ohne funktionierendes Backup? .....	13
Warum BYOD-Geräte besonders risikobehaftet sind .....	14
<b>Herausforderungen von Bring Your Own Device (BYOD) im schulischen Netzwerk</b> .....	<b>14</b>
Warum die Netztrennung mit BYOD unverzichtbar ist .....	15
Rolle von RADIUS und 802.1X im Kontext von BYOD .....	15
Technische Maßnahmen zur Absicherung von BYOD .....	16
Organisatorische Herausforderungen .....	16
BYOD hat Vorteile – aber nur in klaren Sicherheitsstrukturen .....	16
<b>Darstellung der zwei Beispiele als Pläne mit Erklärung</b> .....	<b>18</b>
Beispiel 1: Alleinstehende Schule mit direkter Internetanbindung .....	18
Beispiel 2: Schule mit Anbindung an ein kommunales Rechenzentrum .....	20
<b>Fazit – Ohne Netzarchitekturplan keine sichere Struktur</b> .....	<b>23</b>
<b>Glossar</b> .....	<b>24</b>
<b>Autorinnen und Autoren</b> .....	<b>27</b>

## Einleitung

In einer zunehmend digitalisierten Schule – mit Lernplattformen, Videokonferenzen, WLAN für Schülerinnen und Schüler, Lehrkräften sowie digitalen Verwaltungsprozessen – ist eine klare Netzarchitektur essenziell. Ohne sie ist nicht nachvollziehbar, wie Geräte miteinander verbunden sind, wo sensible Verwaltungsdaten verarbeitet werden oder wie externe Zugriffe abgesichert sind. Ein Netzplan schafft Transparenz, ermöglicht sichere Planung und erlaubt es Pädagogen wie auch IT-Dienstleistern, zielgerichtet über Datenschutz und Sicherheit zu entscheiden. Netzpläne sind strukturierte Darstellungen aller wichtigen Komponenten eines IT-Netzwerks: Server, Geräte, Verbindungen, Sicherheitsmechanismen und Verantwortlichkeiten. Sie bilden die Grundlage jeder sicheren IT-Architektur, da sie zeigen, **wie Daten fließen, wo Risiken bestehen, und wie Schutzmaßnahmen sinnvoll platziert werden können.**

## Netzpläne – Grundlagen und wichtige Konzepte

In den letzten Jahren sind die Netzwerke der Schul-IT durch die erhöhten Herausforderungen an die Technik, Sicherheit und die Anzahl der Endgeräte stetig gewachsen. Dabei wurde oft vorhandene Netzarchitektur erweitert, ohne eine neue Gesamtplanung zu erstellen. Im folgenden Kapitel werden notwendige Grundlagen der Planung und Umsetzung einer sicheren Netzwerkarchitektur dargestellt.

## Zonierung und Mikrosegmentierung

**Zonierung** bedeutet, ein Netzwerk in klar voneinander getrennte Bereiche (Zonen oder Segmente) zu unterteilen – etwa das pädagogische Netz, das Verwaltungsnetz, ein Gäste-WLAN oder ein Technik-/Managementnetz. Die Unterteilung erfolgt nach Funktion, Sicherheitsstufe, Organisation etc.). Die Kommunikation zwischen diesen Netzzonen kann einfacher kontrolliert und reglementiert werden, da sie in einer Zone vergleichbare Kommunikationsanforderungen haben und diese an der Zonengrenze geprüft werden können.

**Mikrosegmentierung** geht noch weiter und trennt selbst innerhalb einer Zone einzelne Dienste oder Gerätegruppen, um Angriffsflächen zu minimieren. Beispielsweise können Tablets der Schüler getrennt von Verwaltungs-PCs und Servern gehalten werden, obwohl sie im selben Gebäudekomplex betrieben werden.



### Hinweis

**Siehe hierzu:** BSI IT-Grundschutz [NET.1.1 Netzarchitektur und -design: Netztrennung in Zonen](#).

## P-A-P-Struktur (Paketfilter – Application Level Gateway – Paketfilter)

Die P-A-P-Struktur ist ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenes Sicherheitskonzept für Netzarchitekturen. Sie beschreibt eine dreistufige Firewall-Architektur, die das interne Netz wirkungsvoll vor Angriffen schützt. Die Bezeichnung steht für:

**P – Paketfilter (äußerer Paketfilter)**

**A – Application Level Gateway (ALG) / Proxy-Firewall**

**P – Paketfilter (innerer Paketfilter)**

Diese Struktur wird typischerweise eingesetzt, um eine DMZ (Demilitarisierte Zone siehe unten) abzusichern und gleichzeitig das interne Netz vor direkten externen Verbindungen (Internet) zu schützen. Sie kann und wird aber auch intern für die Trennung von Netzwerkzonen verwendet, insbesondere wenn Zonen mit hohem Schutzbedarf eine Verbindung zu anderen Zonen benötigen.



### Hinweise

#### Siehe hierzu:

BSI IT-Grundschutz [NET.1.1 Netzarchitektur und -design](#): Absicherung eingehender und ausgehender Kommunikation zum Internet

BSI IT-Grundschutz [NET.1.1 Netzarchitektur und -design](#): P-A-P Struktur für die Internet Anbindung

BSI IT-Grundschutz [NET.3.2 Firewall](#)

BSI [ISi-S Sichere Anbindung von lokalen Netzen an das Internet](#) (schon etwas älter aber gute detaillierte Beschreibung der P-A-P Struktur)

In Abbildung 1 ist eine solchen P-A-P Struktur mit beispielhafter Aufteilung in zwei Netzonen und einer DMZ dargestellt.

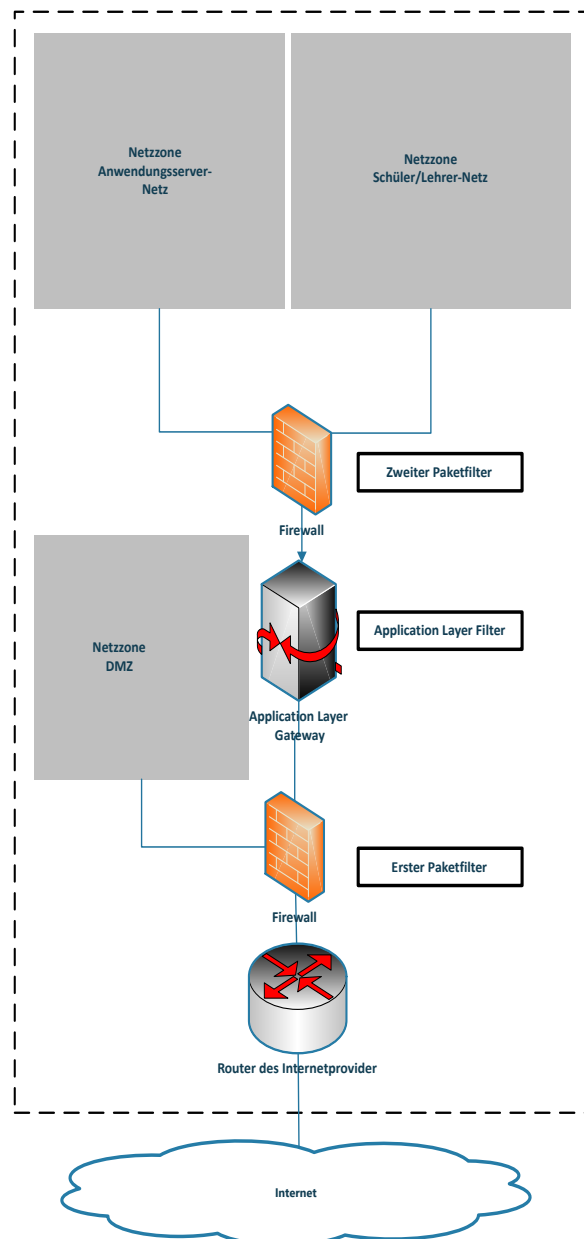


Abbildung 1: P-A-P Struktur mit beispielhafter Aufteilung in zwei Netzzonen und einer DMZ

## Erster Paketfilter – äußerer Paketfilter zum Internet

Dieser Paketfilter steht direkt am Übergang zum Internet. Er blockiert grundsätzlich alle eingehenden Verbindungen aus dem Internet.

Nur klar definierte, unbedingt notwendige Ausnahmen sind erlaubt (z. B. Zugriff auf einen öffentlichen Webserver). Dadurch wird verhindert, dass Angreifer ungefiltert Dienste im internen Netz oder der DMZ erreichen.

Der äußere P-Filter bildet die **erste Verteidigungslinie gegen Angriffe aus dem Internet**.

## A – Application Level Gateway (ALG) / Proxy-Firewall

Das ALG (auch Application Layer Firewall, Application Level Firewall genannt) befindet sich zwischen äußerem und innerem Paketfilter, in der Regel in der **DMZ**.

### Zu seinen Aufgaben gehört:

Es trennt Verbindungen vollständig: Ein externer Client verbindet sich zum ALG, das ALG verbindet sich wiederum separat zum internen Zielsystem. Der externe Client kennt damit nie die internen Kommunikationspartner (Server etc.), sondern immer nur den ALG.

--> Es gibt **keinen direkten Datenpfad** zwischen außen und innen.

Das ALG arbeitet auf Anwendungsebene (Layer 7), d. h. es kann Inhalte anhand von definierten Regeln prüfen (Header, Dateien, Protokolle) und Verbindungen zulassen. Es ist der am stärksten zu prüfende Teil der Firewallkette. Das ALG ist daher der **zentralste und kritischste Teil der P-A-P-Struktur**.

### Zweiter Paketfilter – innerer Paketfilter zu den internen Netzzonen

Der innere Paketfilter schützt das interne Netz, insbesondere sensible Systeme wie:

- Verwaltungsserver
- Identitätsdienste
- pädagogische Plattformen
- File-Server
- Lehrkräfte-/Schülerdaten

### Aufgaben des inneren Paketfilters:

- Er erlaubt nur klar definierte und kontrollierte Verbindungen vom ALG zu internen Systemen.
- Er verhindert, dass ein kompromittiertes System in der DMZ direkten Zugriff auf interne Ressourcen erhält.
- Er stellt sicher, dass BYOD-Geräte oder externe Angreifer nicht ungehindert ins Verwaltungsnetz gelangen.
- Er verhindert, dass aus einem kompromittierten System aus der internen Zone ungehindert Daten in das Internet abfließen können.

Der zweite Paketfilter bildet die **kritische letzte Schutzschicht** der Architektur.

### Was verhindert die P-A-P-Struktur?

Die Struktur schützt vor mehreren Gefahren:

- **Direkte Angriffe aus dem Internet auf interne Systeme:** Durch die doppelte Filterung und den ALG gibt es keine direkten Kommunikationswege.
- **Schadensausbreitung aus der DMZ ins interne Netz:** Sollte ein öffentlich erreichbarer Dienst (z. B. Videokonferenzsystem) kompromittiert werden, bleibt der Schaden auf die DMZ begrenzt.
- **Missbrauch unsicherer Geräte (z. B. BYOD-Geräte) als Sprungbrett ins interne Netz:** Schüler- oder Lehrergeräte können niemals direkt in Verwaltungsbereiche gelangen.
- **Manipulation oder Umgehung von Sicherheitsregeln:** Durch die klare Trennung der Zonen und die doppelte Sicherheitsstufe ist eine Umgehung praktisch ausgeschlossen.
- **Unkontrollierter Datenabfluss aus den inneren Zonen:** Schutz gegen Innentäter und unkontrolliertem Datenabfluss aus kompromittierten internen Systemen.

### Was ist eine DMZ und wie hängt sie mit der P-A-P-Struktur zusammen?

Die DMZ (Demilitarized Zone) ist ein Netzwerkbereich, in dem Dienste betrieben werden, die sowohl intern als auch extern erreichbar sein müssen, z. B.:

- Webserver
- E-Mail-Gateways
- Videokonferenzsysteme
- Lernplattformen
- Update-Server

Die DMZ liegt **zwischen den beiden Paketfiltern** der P-A-P-Struktur.

Durch diese Lage:

- bleibt das interne Netz isoliert, selbst wenn ein DMZ-Dienst angegriffen wird,
- können Dienste für Schüler, Eltern oder Lehrer sicher erreichbar bereitgestellt werden,
- wird verhindert, dass Schadsoftware direkt zu sensiblen Verwaltungsdaten gelangt.

## Warum ist die P-A-P-Struktur besonders für Schulen wichtig?

Schulen arbeiten mit sehr sensiblen Informationen, darunter:

- personenbezogene Schülerdaten
- Leistungsdaten
- Verwaltungs- und Personalinformationen
- interne pädagogische Systeme

Zusätzlich existiert eine besondere Herausforderung: **BYOD-Szenarien** bringen viele unsichere Geräte ins Netzwerk.

Die P-A-P-Struktur sorgt dafür, dass:

- Schülergeräte niemals direkten Zugriff auf Verwaltungsnetzbereiche haben,
- externe Angriffe abgefangen werden,
- interne Systeme auch bei DMZ-Problemen geschützt bleiben,
- rechtliche Anforderungen (Datenschutz, BSI-Grundschutz) erfüllt werden.

## Ausfallsicherheit und Redundanz

**Ausfallsicherheit** bedeutet, dass der Betrieb auch bei Fehlern weiterläuft: Ein defekter Switch, ein Stromausfall oder eine gestörte Internetleitung darf nicht sofort die gesamte Schule lahmlegen.

**Redundante Systeme** (z. B. doppelte Internetleitungen, doppelte Firewalls, Ersatz-Stromversorgungen) verringern das Risiko von Unterrichtsausfällen und Datenverlust aufgrund von Ausfällen von IT-Komponenten. Es ist kritisch zu prüfen welche Verfügbarkeit und damit welche Ausfallsicherheit benötigt wird. Redundanz erhöht die Komplexität und die Kosten.

## Anbindung einer Schule an einen externen IT-Dienstleister

Werden Teile der IT in der Schule durch den Schulträger oder einen externen Dienstleister erbracht und es wird hierfür eine Standort-Verbindung zwischen Schule und IT-Dienstleister benötigt, ist diese durch entsprechende kryptografische Verfahren abzusichern. Für die Umsetzung einer solchen Standortkopplung gibt verschiedene technische Möglichkeiten wie VPN (Virtual Private Network) L3/L3 Kryptierer. Welche Lösung verwendet werden kann, hängt letztendlich vom erwarteten Übertragungsvolumen ab. Gerade wenn Verwaltungsdaten außerhalb der Schule verarbeitet werden, ist eine solche Ende-zu-Ende-Verschlüsselung Pflicht nach BSI-Grundschutz.



## Hinweis

**Siehe hierzu:** BSI IT-Grundschutz [NET.1.1 Netzarchitektur und -design](#)

## Netz und Out-of-Band-Management (OOB)

Für eine sichere Schul-IT ist es notwendig, administrative Tätigkeiten in einem eigenen, besonders geschützten Netzwerkbereich durchzuführen. Das sogenannte Management-Netz erfüllt genau diesen Zweck. Es trennt den administrativen Datenverkehr strikt von den regulären Netzbereichen, in denen Schüler und Schülerinnen, Lehrkräfte oder BYOD-Geräte arbeiten. Im Management-Netz werden ausschließlich IT-Administrationsaufgaben für wichtige IT-Systeme ausgeführt, beispielsweise die Konfiguration von Servern, Firewalls, Switches, Storage-Systemen oder Virtualisierungsplattformen. Durch diese Trennung wird verhindert, dass Endgeräte aus dem pädagogischen Netz, die oft nicht vollständig kontrolliert oder gesichert sind, unbeabsichtigt administrative Schnittstellen erreichen oder Angreifer über studentische oder private Geräte Zugriff auf die IT-Infrastruktur erlangen.

Ein Management-Netz ist technisch durch starke Schutzmaßnahmen abgesichert. Dazu gehört in der Regel die Nutzung eigener VLANs, getrennte Firewalls, restriktiver Firewall-Regeln und gesicherter Verbindungswege, die ausschließlich autorisiertem IT-Personal zur Verfügung stehen. Zusätzlich werden häufig Methoden wie Multi-Faktor-Authentifizierung oder die Begrenzung der erlaubten Administrationsprotokolle eingesetzt, sodass die Verwaltung aller Systeme nachvollziehbar und zuverlässig abgesichert bleibt. Diese Struktur ermöglicht es zudem, administrative Aufgaben klar von der täglichen Nutzung der Schul-IT zu trennen und Schutzmechanismen gezielt auf die besonders sensiblen Verwaltungszugänge anzuwenden.

Ergänzend zum Management-Netz wird in professionellen IT-Umgebungen ein Out-of-Band-Management (OOB) eingesetzt. Während das Management-Netz Teil der normalen Netzwerkstruktur ist, besteht das OOB-Management aus einer davon vollständig unabhängigen Verbindung. Es dient dazu, administrative Zugriffe auch dann sicherzustellen, wenn das produktive Netzwerk gestört, fehlerkonfiguriert oder durch einen Angriff beeinträchtigt ist. Geräte wie Server, Firewalls oder Switches verfügen hierfür häufig über eigene Management-Ports oder separate Steuerungsschnittstellen, die unabhängig vom restlichen Datenverkehr funktionieren. In manchen Fällen wird ein zusätzliches, vom Schulnetz getrenntes Mobilfunk- oder Leitungsnetz dafür genutzt, um auch im Notfall auf zentrale Systeme zugreifen zu können.

Die Kombination aus Management-Netz und Out-of-Band-Management stellt sicher, dass die Schule selbst bei technischen Problemen jederzeit administrierbar bleibt und dass privilegierte Zugänge nicht über das pädagogische oder organisatorische Alltagsnetz erreichbar sind. Dies verhindert, dass Schadsoftware oder Angreifer auf kritische Systeme zugreifen können, die für den Betrieb der gesamten Schul-IT essenziell sind. Durch diese strenge Trennung bleibt das interne Netzwerk geschützt, selbst wenn ein Gerät im pädagogischen Umfeld kompromittiert wird, und die IT-Verantwortlichen behalten auch in Ausnahmesituationen die Kontrolle über die Infrastruktur. Diese Architektur ist daher ein zentrales Element der IT-Sicherheit in schulischen Umgebungen und entspricht den Anforderungen des BSI-Grundschutzes in besonderem Maße.

**Hinweis**

**Siehe hierzu:** BSI IT-Grundschutz [NET.1.2 Netzmanagement](#)

## RADIUS-Server und Authentifizierung im Schulnetz

Ein RADIUS-Server ist ein zentraler Bestandteil moderner Netzwerke – insbesondere in Bildungseinrichtungen mit vielen Geräten und wechselnden Nutzern, z. B. im Rahmen von „Bring Your Own Device“ (BYOD). RADIUS steht für Remote Authentication Dial-In User Service und übernimmt drei wesentliche Aufgaben: Authentifizierung (wer ist der Nutzer bzw. das Gerät), Autorisierung (zu welchen Diensten bekommt der Nutzer Zugang) und Accounting (wer hat wann welchen Dienst genutzt) – auch bekannt als AAA.

### Warum ein RADIUS-Server in Schulen?

In Schulen verbinden sich ständig Geräte: Schüler-Tablets, Laptops, Smartphones von Lehrkräften, Verwaltungsgeräte, IoT-Geräte. Ein RADIUS-Server sorgt dafür, dass alle Nutzende und jedes Gerät nach den Regeln des Netzwerks authentifiziert und autorisiert wird, bevor ein Zugang gewährt wird. So wird verhindert, dass beispielsweise ein fremdes oder unsicheres Gerät Zugang zum pädagogischen Netz oder gar zum Verwaltungsnetz erhält. Zudem ermöglicht RADIUS eine automatisierte VLAN-Zuordnung: Geräte von Schülern können automatisch ins pädagogische Netz gelegt werden, Lehr- oder Verwaltungsgeräte ins entsprechende Segment. Damit unterstützt der RADIUS-Server die Netztrennung und Mikrosegmentierung, die wir bereits in früheren Kapiteln behandelt haben.

### Wie funktioniert das in der Praxis?

Wenn sich ein Gerät mit dem WLAN oder LAN verbindet, wird die Anfrage – z. B. über einen Access Point oder Switch – an den RADIUS-Server weitergeleitet. Dort wird überprüft: Ist das Gerät bekannt? Gehört der Nutzende zur entsprechenden Gruppe (Schüler oder Schülerinnen, Lehrkräfte, Mitarbeitende)? Welche Rechte soll das Gerät haben? Anschließend wird entschieden, ob Zugriff gewährt wird und ggf. in welches VLAN oder welche Zone das Gerät einsortiert wird. Der Standard IEEE 802.1X ist hierbei häufig beteiligt, denn über ihn wird die Port-Authentifizierung umgesetzt: Nur nach erfolgreicher Authentifizierung erhält der Port Zugriff.

### Software-Beispiele mit integriertem oder besonders geeigneten RADIUS-Support

Für Schulträger stehen inzwischen mehrere deutsche Lösungen bereit, die einen RADIUS-Server integrieren oder sehr gut dafür geeignet sind (die hier genannten Anbieter werden nur exemplarische gelistet und stellen keine Empfehlung dar):

- **IServ Schulserver (IServ GmbH, Deutschland):** Mit dem WLAN-Modul von IServ kann ein RADIUS-Server direkt auf dem Schulserver betrieben werden. Laut Dokumentation unterstützt IServ eine benutzerspezifische Anmeldung im WLAN über RADIUS.
- **logoDIDACT (SBE network solutions GmbH, Deutschland):** Diese Schulserverlösung enthält explizit einen Authentifizierungsdienst (RADIUS) zur Einbindung von WLAN-fähigen Geräten wie Notebooks. Das bedeutet: Auch hier ist eine zentrale Zugangskontrolle über RADIUS möglich – ideal im BYOD-Szenario.
- **UCS@school (Univention GmbH, Bremen, Deutschland):** UCS@school bietet ebenfalls Unterstützung für die Integration eines RADIUS-Servers im Umfeld von Schule und Schulträgern.

Diese Beispiele zeigen, dass Schulen nicht zwingend eine reine Eigenlösung mit „von Grund auf“ RADIUS aufbauen müssen – oft ist die Funktion bereits im Schulserver enthalten oder kann als ergänzende Komponente aktiviert werden.



#### Hinweis

**Siehe hierzu:** BSI IT-Grundschutz [NET.3.4 Network Access Control](#)

## Backup und die 3-2-1-Regel – Schutz vor Datenverlust und Ransomware

Backups sind ein unverzichtbarer Bestandteil jeder IT-Sicherheitsstrategie. Sie stellen sicher, dass wichtige Daten auch dann wiederhergestellt werden können, wenn Geräte ausfallen, Fehler passieren oder Angriffe die Infrastruktur beeinträchtigen. Insbesondere im schulischen Umfeld, in dem personenbezogene Daten, Lernstände, Unterrichtsmaterialien, Verwaltungsunterlagen und Dokumentationen verarbeitet werden, ist eine zuverlässige und regelmäßig getestete Datensicherung von zentraler Bedeutung.

Ein Backup ist nicht nur eine Kopie wichtiger Daten, sondern ein Sicherheitsnetz, das den gesamten Schulbetrieb stabil hält. Ohne funktionierende Backups kann selbst ein kleiner technischer Vorfall gravierende Auswirkungen haben: Lehrkräfte verlieren Unterrichtsmaterialien, Verwaltungsstellen verlieren Akten und Dokumente, pädagogische Plattformen sind nicht mehr nutzbar und der Schulbetrieb ist massiv gestört.

### Backups im Kontext von Ransomware

In den letzten Jahren hat die Zahl der Ransomware-Angriffe stark zugenommen – auch auf Schulen, Bildungsverwaltungen und kommunale Einrichtungen. Ransomware verschlüsselt Daten und versucht anschließend, Lösegeld zu erpressen.

Oft werden dabei nicht nur Server und Arbeitsstationen verschlüsselt, sondern auch Netzlaufwerke und angeschlossene Speichersysteme.

Ein häufiger Irrtum besteht darin zu glauben, dass „ein Backup schon reichen wird“. Moderne Ransomware versucht jedoch gezielt:

- Backup-Server zu verschlüsseln,
- angebundene Backuplaufwerke zu zerstören,
- Netzwerkfreigaben zu überschreiben,
- Snapshot-Systeme zu löschen,
- Cloud-Backups zu manipulieren.

Deshalb schützt nur ein strukturiertes und mehrstufiges Backup-Konzept zuverlässig vor dem vollständigen Datenverlust.

### **Die 3-2-1-Regel – der zentrale Leitfaden**

Die international etablierte 3-2-1-Regel beschreibt eine robuste Backup-Strategie:

- 3 Kopien der Daten: Eine primäre Kopie + zwei Backups. Dadurch überlebt der Datenbestand auch den Ausfall eines Backup-Mediums.
- 2 unterschiedliche Speichermedien: Beispielsweise: Festplatte + Band, oder NAS + Cloud. Unterschiedliche Technologien reduzieren die Wahrscheinlichkeit eines gleichzeitigen Totalverlusts.
- 1 Kopie an einem externen oder komplett isolierten Standort: Dieser Punkt ist entscheidend gegen Ransomware: Ein Backup, das nicht im Schulnetz hängt, kann nicht verschlüsselt werden, selbst wenn das gesamte Schulnetz kompromittiert.

Gerade die Schul-IT, die in der Regel für Daten von bis zu 100 Schulen zuständig ist, muss sicherstellen, dass mindestens ein Backup physisch getrennt oder logisch isoliert ist – zum Beispiel in einem kommunalen Rechenzentrum, auf Bandlaufwerken, auf unveränderlichen Cloud-Speichern oder in einer Offline-Archivierung.

### **Warum externe und „Air-Gap“-Backups unverzichtbar sind**

Ein Air-Gap-Backup ist eine Sicherung, die technisch nicht erreichbar ist, wenn der Angriff stattfindet. Das kann erreicht werden durch:

- physisch getrennte Datenträger (z. B. externe Festplatten, die nur für die Sicherung angeschlossen werden),
- Bandlaufwerke (magnetische Bänder),
- externe Cloud-Systeme mit Schreibschutz-Funktion (Immutable Storage),
- Backup-Systeme beim Schulträger oder Rechenzentrum.

Air-Gap-Backups sind heute der wichtigste Schutz gegen Ransomware, da sie selbst von hochentwickelter Schadsoftware nicht erreicht werden können.

### **Backups müssen geplant, dokumentiert und getestet werden**

Viele Vorfälle zeigen: Ein Backup ist nur so gut wie seine letzte erfolgreiche Wiederherstellung. Deshalb gehören folgende Punkte zur Backup-Strategie einer Schul-IT:

- Regelmäßige Wiederherstellungstests (z. B. vierteljährlich)
- Dokumentierte Backup-Pläne und Verantwortlichkeiten
- Sicherung aller relevanten Systeme, einschließlich:
  - pädagogische Plattformen
  - Verwaltungssoftware
  - Identitätsdienste (z. B. Active Directory)
  - File-Server
  - Konfigurationsdaten von Firewalls, Switches und Servern
- **Versionierte Backups**, um auch ältere Zustände wiederherstellen zu können
- **Protokollierung und Monitoring** der Sicherungsläufe

Im schulischen Umfeld ist es essenziell, dass sowohl der Schulträger als auch die Schulleitung wissen, **wo die Backups liegen, wie sie geschützt sind und wer im Ernstfall Zugriff hat.**

### **Was passiert ohne funktionierendes Backup?**

Ohne strukturierte Backups drohen:

- vollständiger Verlust von Schüler und Schülerinnen sowie Verwaltungsdaten,
- Ausfall pädagogischer Plattformen,

- erhebliche organisatorische Schäden,
- Datenschutzvorfälle nach DSGVO (Meldepflicht!),
- langfristige Unterbrechung des Schulbetriebs,
- teure externe Wiederherstellungsversuche.

Ein erfolgreicher Ransomware-Angriff ohne aufrechterhaltene Backup-Strategie kann eine Schule über Wochen oder Monate lahmlegen.

### Warum BYOD-Geräte besonders risikobehaftet sind

Private Geräte weisen erhebliche Unterschiede hinsichtlich ihres Sicherheitsniveaus auf. Während einige Schüler oder Schülerinnen aktuelle Smartphones mit modernen Updates nutzen, arbeiten andere mit alten Geräten, die seit Jahren keine Sicherheitsaktualisierung mehr erhalten. Hinzu kommen vielfältige App-Installationen, persönliche Daten, offene WLANs, besuchte Websites und individuelle Nutzungsgewohnheiten – all das beeinflusst die Risiken für ein Schulnetzwerk.



#### Hinweise

**Siehe auch:** BSI IT-Grundschutz [CON.3 Datensicherungskonzept](#) und BSI IT-Grundschutz [Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept](#)

### Herausforderungen von Bring Your Own Device (BYOD) im schulischen Netzwerk

Bring Your Own Device (BYOD)/ Get Your own Device (GYOD) (im Folgenden unter BYOD zusammengefasst, da das BSI nur von BYOD spricht) beschreibt die Nutzung privater Endgeräte – wie Smartphones, Tablets oder Laptops – im Schulnetz. Dieses Modell bringt pädagogische Vorteile mit sich, da Lerninhalte flexibel, ortsunabhängig und differenziert angeboten werden können. Gleichzeitig stellt BYOD jedoch eines der größten sicherheitstechnischen Risiken für die gesamte Schul-IT dar. Private Geräte sind in der Regel nicht auf schulische Sicherheitsstandards vorbereitet und unterliegen keiner zentralen Kontrolle. Dadurch steigt die Wahrscheinlichkeit, dass Schadsoftware, Fehlkonfigurationen oder unzulässige Apps in das Netzwerk gelangen.

Die Herausforderung liegt darin, pädagogische Nutzung zu ermöglichen, ohne die Sicherheit des Verwaltungsnetzes oder der Schulserver zu gefährden. Schulen müssen daher technische, organisatorische und pädagogische Maßnahmen kombinieren, um ein ausgewogenes Verhältnis zwischen offener Lernumgebung und IT-Sicherheit herzustellen.

Folgende Faktoren machen BYOD besonders kritisch:

- **fehlende zentrale Kontrolle:** die Schul-IT kann Geräte nicht standardisiert konfigurieren oder absichern.
- **unvorhersehbare Softwareumgebungen:** Apps oder Hintergrundprozesse können unerwünscht in das Netzwerk wirken.
- **unklare Update- und Patchstände:** Viele Geräte sind veraltet, unsicher oder jailbrea-  
ked/rooted.
- **höhere Anfälligkeit für Schadsoftware:** ungesicherte WLAN-Nutzung im Alltag führt zu Infektionsrisiken.
- **Problem der „Schatten-IT“:** Geräte nutzen eigene Cloud-Dienste, Hotspots und Apps, die nicht in der schulischen IT-Strategie berücksichtigt sind.

Diese Vielfalt macht BYOD zu einem schwer kontrollierbaren Faktor und erklärt, warum BSI-Grundschutz und pädagogische IT-Richtlinien eine strikte Trennung der Netze fordern.

### Warum die Netztrennung mit BYOD unverzichtbar ist

Die Trennung des pädagogischen Netzes vom Organisations- und Verwaltungsnetz ist für Schulen zwingend erforderlich. BYOD-Geräte dürfen niemals direkten oder indirekten Zugriff auf Verwaltungsdaten, Schulbescheide, E-Mail-Systeme der Schulleitung oder Identitätsdienste erhalten.

Wenn private Geräte in Kontakt mit Verwaltungsdaten kommen, würden nicht nur technische Risiken entstehen, sondern auch schwerwiegende datenschutzrechtliche Verstöße:

- personenbezogene Schülerdaten könnten abgegriffen werden,
- interne Verwaltungsprozesse könnten manipuliert werden,
- Ransomware könnte das Verwaltungsnetz lahmlegen,
- es könnte zu DSGVO-Verstößen kommen.

Die Netztrennung wird über VLANs, Firewalls und klare Zugriffsregeln realisiert. BYOD ermöglicht pädagogisches Arbeiten, aber nur wenn das Gerät in einer streng kontrollierten Zone betrieben wird.

### Rolle von RADIUS und 802.1X im Kontext von BYOD

RADIUS-gestützte Authentifizierung ist ein zentraler Baustein, um BYOD sicher in das pädagogische Netz zu integrieren.

Über RADIUS lässt sich bestimmen:

- welcher Nutzer welche Rechte hat,
- in welches VLAN ein Gerät automatisch eingeordnet wird,
- ob das Gerät überhaupt zugelassen wird,
- wie Zugriffe protokolliert werden.

Durch 802.1X kann zudem an Access Points und Switches geprüft werden, ob ein Gerät gültige Anmeldedaten besitzt. Nur dann erhält es Zugriff. Geräte ohne gültige Berechtigungen werden blockiert oder in ein isoliertes Gäste-VLAN geleitet.

### Technische Maßnahmen zur Absicherung von BYOD

Damit BYOD sicher genutzt werden kann, sollten folgende Bausteine in der Architektur existieren:

Die Schul-IT muss sicherstellen, dass das pädagogische Netz stark segmentiert ist, sodass BYOD-Geräte nur den minimal notwendigen Zugriff erhalten. Der Datenverkehr sollte durch moderne Firewalls überwacht werden, die auch den Inhalt prüfen können. Ergänzend ist es sinnvoll, webbasierte Filter (Contentfilter) einzusetzen, um unerwünschten oder gefährlichen Datenverkehr zu blockieren. Die Nutzung eines RADIUS-Servers in Verbindung mit 802.1X erhöht die Sicherheit zusätzlich, weil jedes Gerät eindeutig identifiziert wird und automatisch in ein passendes Netzwerksegment eingeordnet werden kann (siehe oben). Um die Gefahr von Schadsoftware zu reduzieren, sollten Schulen zudem sichere Update-Mechanismen bereitstellen und den WLAN-Zugang so konfigurieren, dass er nur authentifizierte Verbindungen zulässt. Auch klar definierte Nutzungsrichtlinien, die von Lehrkräften und Schülern akzeptiert werden müssen, tragen dazu bei, das Risiko zu senken.

### Organisatorische Herausforderungen

BYOD erfordert klare Regeln und Kommunikation. Lehrkräfte müssen wissen, welche Geräte unterstützt werden, welche Einschränkungen gelten und wie sie mit technischen Problemen umgehen können. Schüler und Schülerinnen müssen verstehen, dass ihr eigenes Gerät im Schulnetz bestimmten Regeln unterliegt und dass Verstöße Konsequenzen haben können. Eltern müssen informiert werden, welche Daten verarbeitet werden und wie die Schule sicherstellt, dass die Nutzung privater Geräte DSGVO-konform bleibt.

Digitale Endgeräte können den Unterricht bereichern, strukturiertes Arbeiten fördern und differenziertes Lernen ermöglichen – aber nur, wenn die Nutzung durch klare Regeln, technische Schutzmaßnahmen und gut geschulte Fachkräfte begleitet wird.

### BYOD hat Vorteile – aber nur in klaren Sicherheitsstrukturen

BYOD bietet viele Chancen: personalisiertes Lernen, Medienkompetenz, digitale Kollaboration.

Doch ohne umfassende Sicherheitsmaßnahmen wird BYOD schnell zu einer erheblichen Gefahr, da sich die Angriffsfläche des Schulnetzes erhöht. Aus diesem Grund sind folgende Maßnahmen notwendig:

- klare technische Segmentierung.
- starke Authentifizierung notwendig.
- Sicherheitsmaßnahmen müssen mit Backups, Firewalls und DMZ-Strukturen zusammenspielen.
- koordinierte Zusammenarbeit zwischen Schule und Schulträger.

Erst wenn diese Bedingungen erfüllt sind, können BYOD-Geräte sinnvoll und sicher eingesetzt werden.

Das BSI macht zum BYOD-Modell nur einschränkende Aussagen, insbesondere über technische Kontrolle mittels MDM (Mobile Device Management, Containern etc.). Diese Ansätze sind bei einem uneingeschränkten BYOD-Modell nicht umsetzbar. Das BSI rät vom BYOD-Modell ab, wenn diese Kontrollanforderungen nicht durchsetzbar sind. Umso wichtiger ist die Umsetzung der oben beschriebenen Sicherheits- und organisatorischen Maßnahmen. Die zweite Säule ist neben den eigentlichen Schutzmaßnahmen das Detektieren von Sicherheitsvorfällen und Reaktion auf diese Vorfälle. Es ist empfehlenswert hier Automatisierungen einzusetzen, um der notwendige Zeitaufwand und Reaktionsgeschwindigkeit zu reduzieren.

Generell empfiehlt es sich einen IT-Grundschutz-Check über den Systemlandschaft der Schule durchzuführen, um einen Überblick über die vorhandenen Sicherheitsmaßnahmen zu haben und ggf. Lücken zu erkennen und zu schließen.



#### Hinweise

#### **Weitere Informationen zu einem IT-Grundschutzcheck**

[BSI - IT-Grundschutz-Kompodium mit weiterführenden Dokumenten:](#)

[BSI - IT-Grundschutz-Bausteine \(Edition 2023\)](#)

[BSI - Umsetzungshinweise](#)

[BSI - Bundesamt für Sicherheit in der Informationstechnik - Checklisten zum IT-Grundschutz-Kompodium \(Edition 2023\)](#)

Für einen einfacheren Weg in die Basis-Absicherung (WiBa) gibt es ein vereinfachtes Modell. Darüber hinaus werden auf dem Schul-IT Navigator Quickchecks angeboten, die auch den Einstieg erleichtern.

Hierüber ist es möglich einen schnellen Überblick über den Stand der Maßnahmenumsetzung und Defizite zu erhalten. Tiefere Kenntnisse der IT-Grundschutzmethodik sind nicht notwendig:



Hinweise

Siehe auch: [BSI - WiBA - Weg in die Basis-Absicherung](#)

## Darstellung der zwei Beispiele als Pläne mit Erklärung

Im Folgenden werden zwei Beispiele von Netzarchitekturen bezogen auf unterschiedliche Szenarien vorgestellt. Hier werden alle oben dargestellten Sicherheitsmaßnahmen berücksichtigt sowie diese bezogen auf das Beispiel erklärt. Obwohl die meisten Schulen über die Schul-IT an das Internet angebunden ist und die Schul-IT den Service, die Netze, Datensicherung sowie IT-Komponenten und Software stellen, gibt es Schulen, die aus der Coronazeit heraus noch autark agieren. Aus diesem Grunde wird das Beispiel 1 angeboten.

### Beispiel 1: Alleinstehende Schule mit direkter Internetanbindung

In diesem Beispiel führt die Schule den vollständigen Eigenbetrieb aller Fachanwendungen alleinverantwortlich durch.

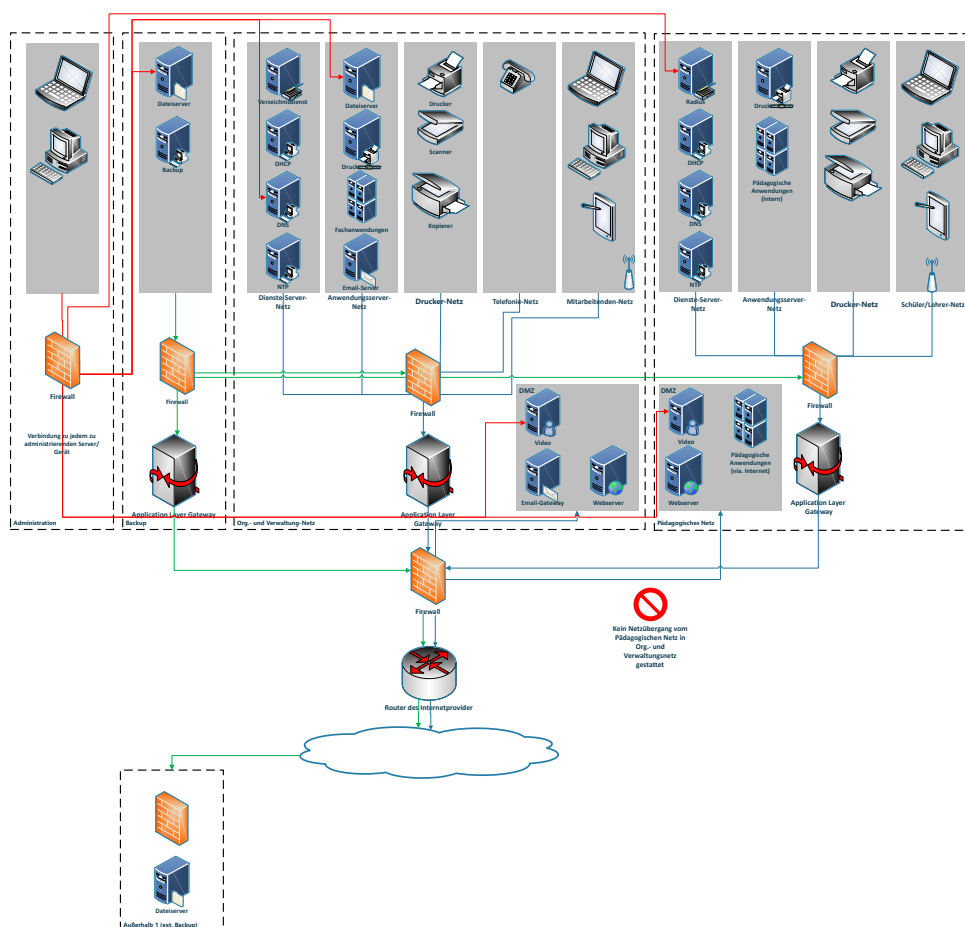


Abbildung 2: Alleinstehende Schule mit direkter Internetanbindung

Der Netzplan der alleinstehenden Schule (siehe Bilddarstellung) zeigt eine klar strukturierte Trennung verschiedener Netzbereiche, wie sie gemäß BSI-Grundsatz auch für Bildungseinrichtungen empfohlen wird. Sehr deutlich erkennbar sind die beiden Hauptsegmente:

1. Pädagogisches Netz
2. Organisations- und Verwaltungsnetz

Im Diagramm ist hervorgehoben, dass kein Übergang vom pädagogischen Netz zum Organisations- und Verwaltungsnetz erlaubt ist – diese Trennung ist kritisch, insbesondere im Kontext von BYOD. Schüler- und Lehrervergeräte im pädagogischen Bereich können durch private Nutzung oder unzureichende Absicherung ein Risiko darstellen. Daher muss das Verwaltungsnetz strikt isoliert bleiben.

Weiter zeigt der Plan:

- **DMZ-Zonen** (E-Mail-Gateway, Webserver, Videoanwendungen), die zwischen Internet und internen Netzen geschaltet sind. Dies schützt interne Systeme vor direkten Angriffen.
- **Mehrere interne Serverzonen**, darunter Verzeichnisdienst, DHCP, DNS, NTP, Dateiserver und Druckerserver. Diese werden in Funktionsgruppen gegliedert, die eine strikte Kontrolle des Netzverkehrs in diese Zonen ermöglicht.
- Separates Drucker-, Telefonie-, Mitarbeitenden und Schüler- Lehrernetz, was auf eine weitergehende Mikrosegmentierung umsetzt und eine Kontrolle des Netzverkehrs erlaubt.
- Firewall-Strukturen, die sowohl die Außengrenze als auch interne Segmente schützen. Der Plan zeigt mehrere Firewalls, die die Übergänge zwischen den Netzzonen absichern.
- Backup-Strategie, einschließlich "Außerhalb 1 (ext. Backup)", was zeigt, dass die 3-2-1-Regel beachtet wird, denn mindestens ein Backup liegt außerhalb des Gebäudes.
- Ein dediziertes Administrationsnetz inkl. Hinweis "Verbindung zu jedem zu administrierenden Server/Gerät". Der Netzübergang in die jeweiligen Netzzonen wird durch Firewalls abgesichert. Diese Struktur entspricht den Grundsätzen eines Out-of-Band-Managements.

Besonders wertvoll ist, dass pädagogische Anwendungen sowohl intern als auch über das Internet bereitgestellt werden können. Dies deckt hybride Unterrichtsformen ab (z. B. lokal installierte Lernsoftware und externe Lernplattformen). Damit werden die in der Einleitung beschriebene Netzstrukturen und Sicherheitsanforderungen in diesem Beispiel-Netzplan umgesetzt.

### Hinweis zur Vollständigkeit

Der Plan bietet eine beachtliche Detailtiefe. Dennoch ist anzumerken, dass in realen Umgebungen weitere Aspekte hinzukommen würden, etwa Monitoring-Systeme, SIEM-Dienste, Patch-Management, Intrusion Detection oder genauere Darstellungen von VLAN-Strukturen. Die vollständige Komplexität würde den Rahmen einer Bildungsdokumentation übersteigen, weshalb die Darstellung bewusst abstrahiert ist.

### Beispiel 2: Schule mit Anbindung an ein kommunales Rechenzentrum

In diesem Beispiel werden alle Fachwendungen durch die Schul-IT oder einen externen IT-Dienstleister für die Schule bereitgestellt.

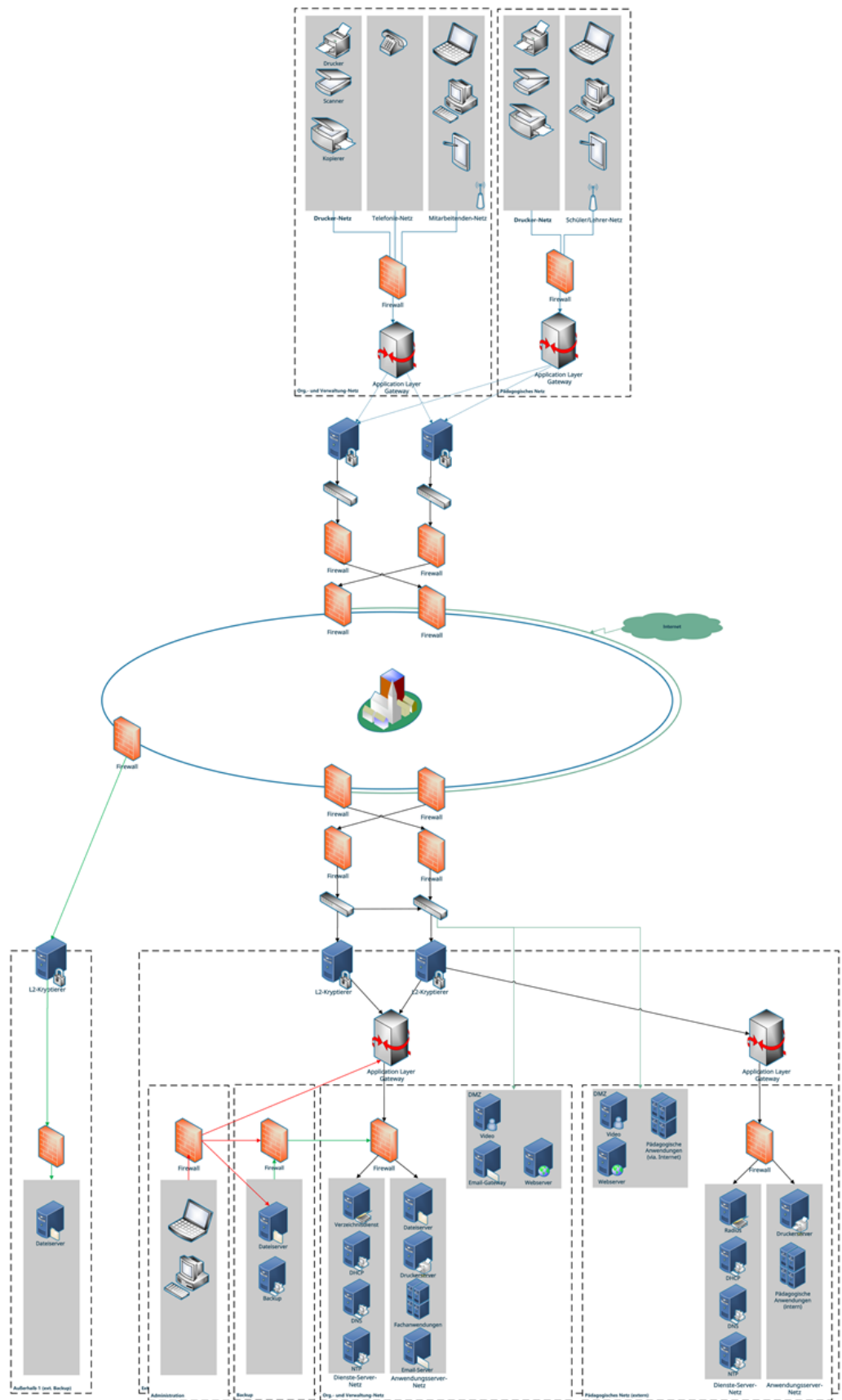


Abbildung 3: Schule mit Anbindung an ein kommunales Rechenzentrum

Der zweite Netzplan zeigt eine erweiterte Architektur, in der wesentliche IT-Dienste nicht mehr lokal in der Schule betrieben werden, sondern in ein **kommunales Rechenzentrum** oder die Schul-IT ausgelagert sind. Das Diagramm (siehe Seite 21) macht diese Struktur deutlich: Die Serverlandschaften für das Organisations- und Verwaltungsnetz sowie Teile der pädagogischen Infrastruktur sind in einem separaten Rechenzentrum dargestellt. Die Schule selbst agiert damit eher als „Netzknoten“ und nicht als vollständiges Hosting-Zentrum.

Ein wesentliches Element dieser Architektur ist der Einsatz von **Kryptierern**, die auf der Seite zwischen Schule und Schul-IT/Rechenzentrum dargestellt sind. Diese Geräte verschlüsseln die Verbindung, sodass die Kommunikation zwischen beiden Standorten vollständig vertraulich bleibt. Insbesondere bei der Übertragung personenbezogener Verwaltungsdaten ist dies ein wichtiger Baustein gemäß BSI-Grundschutz. Technisch kann diese Standortverbindung mit unterschiedlichen Mitteln realisiert werden, wie zum Beispiel VPN, L3/L2-Kryptierer. Die Entscheidung welche technische Umsetzung notwendig ist, hängt unter anderem vom Übertragungsvolumen zwischen Schule und IT-Dienstleister ab.

Deutlich erkennbar ist außerdem:

- **Die Trennung des pädagogischen Netzes vom Organisations- und Verwaltungsnetz** bleibt bestehen, auch wenn sich Serverdienste teilweise im Rechenzentrum befinden. Der Plan zeigt klar, dass Schüler-/Lehrer-Geräte keinerlei direkten Übergang in Verwaltungsbereiche erhalten.
- Die im Rechenzentrum dargestellten Serverrollen (z. B. Verzeichnisdienst, DHCP, DNS, NTP, Dateiserver, Fachanwendungen, E-Mail-Server) entsprechen einer vollständigen, zentralisierten IT-Infrastruktur, wie sie kommunale Anbieter bereitstellen.
- Mehrere **Firewall-Ebenen** sichern interne Serversegmente im Rechenzentrum sowie die Standortverbindung ab. Das Diagramm zeigt teilweise doppelte Firewalls, die Redundanz und Zonierung visuell unterstreichen und der höheren Verfügbarkeit des Rechenzentrums Rechnung trägt.
- Auch hier finden sich **DMZ-Bereiche**, unter anderem für Webserver, Video-Dienste und E-Mail-Gateways. Die DMZ trennt öffentlich erreichbare Dienste von internen Systemen, ein grundlegendes BSI-Schutzziel.
- Das Backup-Konzept bleibt auch im RZ erhalten: Ein externer Backup-Standort („Außerhalb 1“) wird ebenfalls dargestellt, womit die 3-2-1-Regel erfüllt wird.
- Der Plan zeigt ein **extern betriebenes pädagogisches Netz**, das über das Internet bereitgestellt wird. Dies kann z. B. Cloud-Lernplattformen umfassen oder externe digitale Dienste für Schülerinnen und Schüler.

Zudem ist gut zu erkennen, dass im Rechenzentrum weiterhin eine Management- und Administrationsstruktur existiert, getrennt vom Produktionsnetz. Der Plan führt entsprechende Firewallsegmente auf. Damit werden die in der Einleitung beschriebene Netzstrukturen und Sicherheitsanforderungen in diesem Beispiel-Netzplan umgesetzt.

### Hinweis zur Vollständigkeit

Wie bereits beim ersten Plan gilt: Auch dieses Diagramm bildet die Grundstruktur ab, jedoch nicht die gesamte Komplexität eines realen Rechenzentrums – oder Schul-IT-betriebs. In der Praxis kommen Aspekte hinzu wie Monitoring, Notfallmanagement (BCM/DR), Identity-Management-Systeme, Härtung der Server, Protokollierung nach BSI-Standards oder Intrusion Detection Systeme. Aus didaktischen Gründen ist die Darstellung reduziert gehalten – was hier jedoch völlig ausreichend und sinnvoll ist.

## Fazit – Ohne Netzarchitekturplan keine sichere Struktur

Eine moderne Schul-IT kann ohne eine klare, nachvollziehbare und dokumentierte Netzarchitektur nicht sicher und zuverlässig funktionieren. Netzpläne bilden die Grundlage für alle weiteren technischen und organisatorischen Maßnahmen: Sie zeigen, wo Daten fließen, welche Schutzmaßnahmen notwendig sind und welche Bereiche besonders sensibel sind. In einer Umgebung, in der Schüler und Schülerinnen und Lehrkräfte mit eigenen Geräten arbeiten, digitale Lernplattformen nutzen und die Schulverwaltung vollständig IT-gestützt arbeitet, nimmt die Bedeutung einer guten Netzplanung weiter zu.

Ein strukturierter Netzplan verhindert, dass Systeme „historisch gewachsen“ oder unsicher nebeneinander betrieben werden. Er sorgt dafür, dass Privates, Pädagogisches und Verwaltungsdaten voneinander getrennt sind, und dass BYOD-Geräte keine Risiken für sensible Informationen darstellen. Gleichzeitig ermöglicht er eine präzise Umsetzung der Anforderungen aus Datenschutz und BSI-Grundschutz, z. B. durch Zonierung, Mikrosegmentierung, Redundanz, Verschlüsselung, Management-Netze und klare Verantwortlichkeiten.

Natürlich bringt Digitalisierung auch Risiken mit sich: Cyberangriffe, Schadsoftware, technische Ausfälle oder Fehlkonfigurationen können den Schulbetrieb erheblich beeinträchtigen. Ein gut geplanter Netzaufbau minimiert diese Risiken, ohne unnötige Angst zu erzeugen. Er schafft eine stabile und sichere Grundlage, damit Pädagogik und Verwaltung sich auf ihre eigentlichen Aufgaben konzentrieren können – das Lehren, Lernen und Organisieren eines modernen Schulalltags.

Zusammengefasst gilt: Ein Netzplan ist nicht nur ein technisches Dokument – er ist ein zentrales Werkzeug, um die Schul-IT und die Schulen zukunftsfähig, sicher und datenschutzkonform zu gestalten. Ohne ihn bleibt die Digitalisierung instabil, riskant und schwer beherrschbar. Mit ihm dagegen wird der Schulbetrieb deutlich robuster, strukturierter und professioneller unterstützt.

Der Netzplan selbst ist ein wesentliches Element des IT-Sicherheitskonzeptes nach IT-Grundschutz und bildet die Grundlage für den IT-Grundschutz Check.

## Glossar

3-2-1-Regel	Backup-Leitlinie: 3 Kopien, 2 Medien/Technologien, 1 Kopie extern/isoliert.
AAA	Authentication, Authorization, Accounting; Kernfunktionen von RADIUS (Wer? Darf was? Protokollierung).
Access Point	WLAN-Komponente, die Endgeräte ins Funknetz bringt und Anfragen weiterleitet.
Active Directory	Verzeichnisdienst für Identitäten/Rechte; im Kontext von Backups/Identitätsdiensten genannt.
Äußerer Paketfilter	Erster Paketfilter am Internet-Übergang; blockiert grundsätzlich eingehende Verbindungen, erlaubt nur definierte Ausnahmen.
Air-Gap-Backup	Backup, das während eines Angriffs nicht erreichbar ist (physisch/logisch getrennt).
ALG (Application Level Gateway)	Proxy-Firewall auf Anwendungsebene; trennt Verbindungen und prüft Inhalte/Protokolle.
Ausfallsicherheit	Fähigkeit, den Betrieb auch bei Fehlern/Störungen aufrechtzuerhalten.
Backup	Datensicherung zur Wiederherstellung nach Ausfällen/Fehlern/Angriffen.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
BYOD	Bring Your Own Device; Nutzung privater Endgeräte im Schulnetz.
CC BY 4.0	Creative-Commons-Lizenz „Namensnennung 4.0 International“ (Nutzung/Lizenzangabe im Dokument).
Cloud-Backup	Datensicherung in einem Cloud-Speicher; im Dokument u. a. mit Schutzmechanismen erwähnt.
Contentfilter	Web-/Inhaltsfilter zur Blockade unerwünschter oder gefährlicher Inhalte/Verbindungen.
DMZ	„Demilitarisierte Zone“; Netzbereich für Dienste, die intern und extern erreichbar sein müssen.
DSGVO	Datenschutz-Grundverordnung; relevante Rechtsgrundlage bei personenbezogenen Daten in Schulen.
E-Mail-Gateway	Komponente zur Ein-/Ausleitung und Filterung von E-Mail-Verkehr (häufig in der DMZ).
Ende-zu-Ende-Verschlüsselung	Durchgehende Verschlüsselung zwischen Kommunikationsendpunkten (wichtig bei Verwaltungsdaten).
Firewall	Sicherheitskomponente, die Netzwerkverkehr anhand von Regeln zulässt/ablehnt.
GYOD	Get Your Own Device; im Dokument zusammen mit BYOD erwähnt (unter BYOD zusammengefasst).
IEEE 802.1X	Standard zur Port-Authentifizierung in LAN/WLAN; Zugriff erst nach erfolgreicher Authentifizierung.
Identity-Management	Verwaltung digitaler Identitäten/Accounts und Berechtigungen (als Praxisaspekt genannt).
Immutable Storage	Unveränderlicher Speicher mit Schreibschutz (Schutz gegen Manipulation/Überschreiben).
Innerer Paketfilter	Zweiter Paketfilter Richtung interne Zonen; schützt besonders sensible interne Systeme.
Intrusion Detection	Erkennung von Angriffen/Anomalien im Netz oder auf Systemen (als Ergänzung genannt).
IServ	Schulserver-Lösung mit WLAN-Modul und möglichem integriertem RADIUS-Betrieb.
ISi-S	BSI-Dokument/Leitfaden „Sichere Anbindung von lokalen Netzen an das Internet“ (im Dokument als Referenz genannt).

IoT	Internet of Things; vernetzte Geräte (z. B. Sensorik/Peripherie), im Schulkontext als Gerätetyp genannt.
IT	Informationstechnologie; Gesamtheit aus Systemen, Netzen, Software und Betrieb.
IT-Grundschutz	BSI-Methodik/Regelwerk zur strukturierten Absicherung von IT-Systemen.
Kryptierer (L3/L2, L3/L3)	Geräte/Lösungen zur Verschlüsselung von Standortverbindungen auf verschiedenen Netzebenen.
LAN	Local Area Network; kabelgebundenes lokales Netzwerk.
Layer 7	Anwendungsschicht im OSI-Modell; Ebene, auf der Inhalte/Anwendungsprotokolle geprüft werden können.
logoDIDACT	Schulserver-Lösung mit Authentifizierungsdienst (RADIUS) zur Geräteanbindung.
Management-Netz	Separates, besonders geschütztes Netz für administrative Tätigkeiten (Konfiguration/Verwaltung).
MDM	Mobile Device Management; Verwaltung/Absicherung mobiler Endgeräte (im BYOD-Kontext als eingeschränkt umsetzbar).
Mikrosegmentierung	Feingranulare Trennung innerhalb einer Zone (z. B. nach Diensten/Gerätegruppen) zur Reduktion von Angriffsflächen.
Monitoring	Überwachung von Systemzuständen, Verfügbarkeit und Ereignissen.
NAS	Network Attached Storage; netzwerkgebundener Speicher (als mögliches Backup-/Speichermedium).
Netzarchitektur	Gesamtkonzept des Netzwerkaufbaus (Zonen, Übergänge, Schutzmaßnahmen, Dienste).
Netzplan	Strukturierte Darstellung von Komponenten, Verbindungen, Zonen und Sicherheitsmechanismen eines Netzwerks.
Netztrennung	Technische/organisatorische Trennung von Netzen (z. B. pädagogisch vs. Verwaltung) mittels Regeln/Firewalls/VLANs.
NET.1.1 / NET.1.2 / NET.3.2 / NET.3.4	Verweise auf BSI-IT-Grundschutz-Bausteine (Netzarchitektur/-design, Netzmanagement, Firewall, Network Access Control).
OOB (Out-of-Band-Management)	Vom produktiven Netz unabhängiger Administrationszugang (für Notfälle/Störungen/Angriffe).
P-A-P-Struktur	Dreistufige Firewall-Architektur: Paketfilter – Application Level Gateway – Paketfilter.
Paketfilter	Firewall-Funktion, die auf Paket-/Transportmerkmalen filtert (z. B. IP/Port/Protokoll).
Patch-Management	Prozess zur planvollen Verteilung von Updates/Sicherheits-Patches.
PD	PD – Berater der öffentlichen Hand GmbH (Organisation/Autorenschaft im Dokument).
Proxy-Firewall	Firewall, die als vermittelnde Instanz agiert (kein direkter Datenpfad außen/innen).
Quickcheck	Schnellprüfung (im Schul-IT-Navigator erwähnt) zum Überblick über Maßnahmenstand/Defizite.
RADIUS	Remote Authentication Dial-In User Service; zentraler Dienst für Authentifizierung/Autorisierung/Accounting.
RADIUS-Server	Server, der RADIUS bereitstellt und z. B. WLAN/LAN-Zugänge zentral steuert.

Redundanz	Doppelte/mehrfache Auslegung kritischer Komponenten (z. B. Leitungen/Firewalls) zur Erhöhung der Verfügbarkeit.
Ransomware	Schadsoftware, die Daten verschlüsselt und Lösegeld erpresst; zielt oft auch auf Backups.
Schul-IT	IT-Umgebung einer Schule bzw. durch Schulträger bereitgestellte IT-Dienste.
Segment / Netzzone	Abgegrenzter Netzwerkbereich mit definierten Kommunikationsregeln.
SIEM	Security Information and Event Management; Sammeln/Korrelieren von Sicherheitsereignissen (als Ergänzung genannt).
Snapshot	Momentaufnahme eines Systems/Dateisystems; kann von Angreifern gezielt gelöscht werden (Risiko).
Standortkopplung	Sichere Verbindung zwischen Standorten (z. B. Schule ↔ Schulträger/Rechenzentrum).
Switch	Netzkomponente zur Kopplung von Geräten in einem LAN; kann Segmentierung/Ports steuern.
UCS@school	Schulserver-/Verzeichnisdienst-Lösung (Univention) mit RADIUS-Integration/Unterstützung.
Videokonferenzsystem	Dienst für Video-/Audio-Konferenzen; im Dokument als typischer DMZ-Dienst genannt.
VLAN	Virtuelles LAN; logische Segmentierung eines physischen Netzes in getrennte Broadcast-Domänen.
VPN	Virtual Private Network; verschlüsselte Verbindung über unsichere Netze (z. B. Standortkopplung).
Webserver	Serverdienst zur Bereitstellung von Webseiten/HTTP(S)-Diensten (häufig in der DMZ).
WiBA	„Weg in die Basis-Absicherung“; vereinfachter Einstieg in eine Grundabsicherung nach BSI-Logik.
WLAN	Wireless Local Area Network; drahtloses lokales Netzwerk.
Zonierung	Aufteilung eines Netzes in klar getrennte Bereiche (Zonen/Segmente) nach Funktion/Schutzbedarf.

## Haftungsausschluss

Dieses Dokument wurde mit größter Sorgfalt erstellt. Es wird aber kein Anspruch auf Vollständigkeit und Richtigkeit erhoben. Die Mitwirkenden an diesem Dokument haben keinen Einfluss auf dessen weitere Nutzung durch die einzelnen Anwenderinnen und Anwender und können daher hinsichtlich der Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen.

## Autorinnen und Autoren

Uta Fiedler (PD – Berater der öffentlichen Hand GmbH)

Dr. Jürgen Liebmann (PD – Berater der öffentlichen Hand GmbH)

Peter Lüttringhaus (PD – Berater der öffentlichen Hand GmbH)

PD – Berater der öffentlichen Hand GmbH Friedrichstr. 149, 10117 Berlin | [www.pd-g.de](http://www.pd-g.de) | [schuedigital@pd-g.de](mailto:schuedigital@pd-g.de)



### **Schon gewusst?**

Mehr Fachwissen zum Thema Schul-IT finden Sie auf unserer Webseite:

 [www.schul-it-navigator.de](http://www.schul-it-navigator.de)

### **Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen noch etwas?**

Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden. Wir freuen uns auf Ihre Rückmeldung.

 [feedback@schul-it-navigator.de](mailto:feedback@schul-it-navigator.de)