



IT-Ausstattungsempfehlungen für Schulen in Schleswig-Holstein

## Themenpapiere

### Internetnutzung in Schulen

# Internetnutzung in Schulen

## Grundlagen

An vielen Schulen stellt sich aufgrund zunehmender Medien- und Internetnutzung die Frage, welche organisatorischen, technischen und rechtlichen Aspekte zu beachten sind. Dieses ist insbesondere dann wichtig, wenn mobile und zunehmend auch schülereigene Geräte zum Einsatz kommen sollen.

Gerade beim Aufbau einer WLAN-Infrastruktur ist eine umfassende Planung von großem Vorteil, um eine zuverlässige und ausreichend leistungsfähige Funktionalität des Systems zu gewährleisten. Aufgrund des hohen Anteils aktiver Komponenten, die in der Schule verbaut werden und anschließend gewartet werden müssen, sind der Betreuungsaufwand und die damit verbundenen Kosten deutlich höher als bei einer reinen kabelgebundenen Vernetzung.

Wenn eine Schule Zugang zum Internet und insbesondere über ein WLAN für unterrichtliche bzw. dienstliche Nutzung zur Verfügung stellt, besteht die Gefahr, dass sie z.B. für Urheberrechtsverstöße der Nutzer in Haftung genommen werden kann. Um dieses zu verhindern, dürfen nur berechtigte Personen Zugriff auf das schulische Internet erhalten. In nicht bzw. weniger beaufsichtigten Unterrichtssituationen sind die Nutzeraktivitäten zudem zu protokollieren. Damit wird gewährleistet, dass im Falle einer missbräuchlichen Nutzung die betreffende Person ausfindig gemacht werden kann und im Falle straf- oder zivilrechtlicher Haftungsansprüche der Schüler bzw. seine Erziehungsberechtigten durch die Schule bzw. den

Schulträger in Regress genommen werden können.

Die kommunalen Landesverbände haben eine Handreichung für den Einsatz von WLAN in der Kommunalverwaltung veröffentlicht<sup>1</sup>. Im Gegensatz dazu trägt dieses Themenpapier dem besonderen Umstand Rechnung, dass an den Nutzerkreis Schülerinnen und Schüler strengere Maßstäbe als im Verwaltungsbereich anzulegen sind.

## Aufbau der Netzwerk-Infrastruktur

### Allgemeines

Grundsätzlich erscheint es sinnvoll, dass bei der Einrichtung des schulischen Netzwerkes die langfristige Perspektive mitbedacht wird, da sonst die Gefahr besteht in teure technologische Sackgassen zu geraten. Vor allem, wenn in zunehmendem Maße schülereigene Geräte zum Einsatz kommen sollen, sollten die Netzwerkstruktur im allgemeinen und die WLAN-Infrastruktur im speziellen so ausgelegt sein, dass sie ohne große Umbaumaßnahmen erweiterbar und an den jeweiligen Bedarf anpassbar sind. Insbesondere sollte überlegt werden, in welchen Räumen sowohl das kabelgebundene Netzwerk als auch das WLAN kurz-, mittel- und langfristig zur Verfügung stehen soll und für wie viele Nutzer es ausgelegt werden soll. Diese Überlegungen sollten im Rahmen der Erstellung oder Fortschreibung eines Mediennutzungsplanes einbezogen werden.

<sup>1</sup> Diese Handreichung kann unter [info@komfit.de](mailto:info@komfit.de) angefordert werden.



## Grundsätzliche Netzwerkstruktur

Um einen störungsfreien und datenschutzrechtlich einwandfreien Betrieb des schulischen Netzwerks zu gewährleisten, müssen die verschiedenen Bereiche sauber voneinander getrennt sein (Verwaltungsnetz, Lehrernetz, Schülernetz, WLAN etc.). Dieses kann man erreichen, indem man für jedes Netz eigene Switches in den Netzwerkschränken einbaut und auch leitungstechnisch physikalisch getrennt betreibt. Mit zunehmender Zahl an Netzen wird dieses jedoch aufgrund der Anzahl der benötigten Netzwerkleitungen und Switches sehr unpraktisch. Daher greift man auf so genannte VLANs (Virtual Local Area Network) zurück, bei denen ein physikalisches Netzwerk in mehrere logische Bereiche unterteilt wird. Jedes VLAN bildet dabei eine eigene Broadcast-Domain. Eine Kommunikation zwischen zwei unterschiedlichen VLANs ist nur über einen Router möglich, der mit beiden VLANs verbunden ist. VLANs verhalten sich also so, als ob sie jeweils mit eigenen, voneinander unabhängigen Switches aufgebaut wären. Über gemanagte Switches können dann den einzelnen Ports verschiedene getrennte VLANs zugewiesen werden. Für die verschiedenen VLANs sollten zur besserem Übersicht in den Netzwerkschränken einheitliche Farben verwendet werden. Bei der Nutzung von getaggten („tagged“) VLANs können diese auch über ein einziges Netzkabel transportiert werden, so dass der Aufwand für das sonst nötige Verlegen zusätzlicher Netzkabel durch die Schule z.B. für die Anbindung der einzelnen WLAN-Accesspoints entfällt. Bei einer solchen Lösung müssen alle (beteiligten) Netzwerkkomponenten VLAN-fähig sein.

Aufgrund der hohen Datenmengen, die bei einer intensiven Nutzung anfallen, sollten im kabelgebundenen

Netzwerk möglichst komplett Gigabit-LAN-fähige Komponenten eingesetzt werden.

## WLAN

Bei der Planung der WLAN-Vernetzung ist sicherzustellen, dass

1. eine zuverlässige Ausleuchtung in allen benötigten Bereichen erfolgt (hierzu ist eine Ausleuchtungsplanung erforderlich),
2. die zur Verfügung stehenden Accesspoint die maximale Anzahl der Schüler in den entsprechenden Bereichen der Schule versorgen können,
3. die Accesspoints in den einzelnen Räumen möglichst hoch in den Räumen positioniert werden (ggf. auch in Zwischendecken) → Schutz vor Zugriff der Schüler, bessere Ausleuchtung,
4. an den Installationspunkten der Accesspoints Stromanschlüsse zur Verfügung stehen oder die Stromversorgung durch Verwendung geeigneter Switches über POE (Power over Ethernet – Strom über das Netzkabel) erfolgen kann,
5. eine zentrale Steuerung der Accesspoints möglich ist, um Firmwareupdates (z.B. bei Sicherheitslücken) aufzuspielen und einzelne Einstellungen auf allen AP gleichzeitig vornehmen zu können (→ erhebliche Zeit- bzw. Geldersparnis),
6. eine spätere Erweiterbarkeit des Systems möglich ist (Verwaltung von mehr AP, Schülerkonten etc.),





7. getrennte WLAN-SSIDs für Schüler und Lehrer bereitgestellt werden können (von einem Accesspoint -> Multi-SSID-Fähigkeit),

8. die üblichen WLAN-Standards unterstützt werden (b/g/n oder neuer), WPA2-Business,

9. max. 2 Geräte der Schüler mit einer MAC-Adresse oder einem x509-Zertifikat hinterlegt sind, die sich verbinden können,

10. keine Mehrfachverbindung eines Nutzers möglich ist,

11. nur die unbedingt notwendigen Ports/Dienste nach außen freigeschaltet sind (u.a. dns, http, https) und Filesharingdienste grundsätzlich geblockt sind,

12. die Accesspoints „Client-Isolation“ unterstützen (-> kein Netzwerkverkehr zwischen angeschlossenen WLAN-Clients).

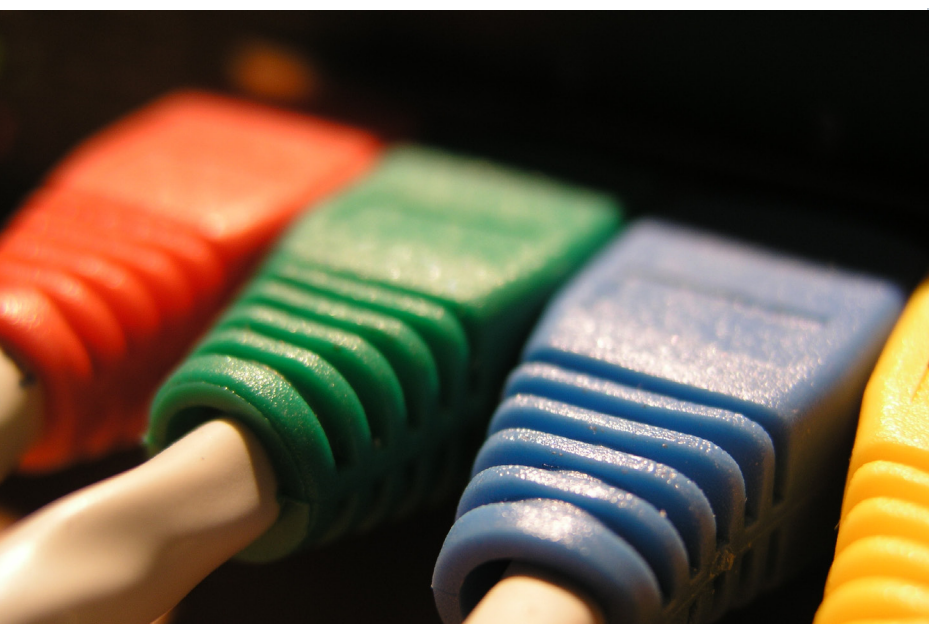
Günstige Consumergeräte erfüllen diese Anforderungen in der Regel nicht. Verschiedene Hersteller bieten aber WLAN Controller oder so genannte „Managed Accesspoints“ (Hybrid aus Controller und AP) an, welche die angeschlossenen AP steuern können. Hier müssen die Einstellungen nur einmal vorgenommen werden und können dann automatisch oder auf Knopfdruck an die angeschlossenen AP übertragen werden. Bei solchen Systemen ist aber auch auf eine ausreichende Erweiterbarkeit und Zukunftssicherheit zu achten. Das Verlegen von zusätzlichen Stromanschlüssen für die AP in den Räumen kann entfallen, wenn diese über PoE (Power over Ethernet) mit Strom versorgt werden können

(AP und Switches müssen dieses unterstützen).

#### Authentifizierungsverfahren

Grundsätzlich gibt es zwei Möglichkeiten das Internet und speziell das WLAN vor unbefugten Zugriffen zu schützen. Die erste Variante, die aus Hotels oder Flughäfen bekannt ist, ist eine so genannte „Captive Portal“-Lösung. Hierbei verbindet man sich im Regelfall mit einem unverschlüsselten WLAN oder dem kabelgebundenen Netzwerk und wird beim ersten Aufruf einer Internetseite auf eine Anmeldeseite umgeleitet, auf der man sich authentifizieren muss, um anschließend für eine gewisse Zeit Zugriff auf das Internet zu erhalten. Captive Portal-Lösungen sind in verschiedenen Schulroutern und Accesspoints bereits integriert und daher ohne großen Aufwand einsatzbereit. Um nur schulangehörigen Personen den Zugriff auf die Anmeldeseite zu ermöglichen, sollte das WLAN trotzdem auch mit einem Passwort gesichert sein und dieses regelmäßig geändert werden. Um das Ausspionieren von Kennwörtern zu unterbinden, sollte die Anmeldeseite (SSL-) verschlüsselt sein. Die Benutzerverwaltung kann innerhalb des Captive Portal-Systems erfolgen oder über eine separate Benutzerschnittstelle (z.B. Anbindung an einen RADIUS-Server – siehe unten).

Eine zweite Variante stellen mit WPA2-Business / IEEE802.1X / EAP über einen RADIUS-Server geschützte WLANs / LANs dar. Bei diesen erfolgt die verschlüsselte Authentifizierung der Nutzer bereits bei der Verbindungsherstellung zum WLAN / LAN. Dabei handelt es sich nicht um ein Passwort für alle Nutzer, sondern spezielle Zugangsdaten für jeden einzelnen.



Dadurch kann gewährleistet werden, dass die jeweiligen Internetzugriffe tatsächlich von der authentifizierten Person getätigt wurden und damit klar zugeordnet werden können. Die Benutzer werden über den jeweiligen RADIUS-Server der Schule authentifiziert, der diese z.B. in einer Textdatei, einem LDAP-Verzeichnis oder einem SQL-Server verwaltet. Auch ein Zugriff auf eine außerhalb der Schule befindliche Nutzerdatenbank wäre denkbar.

Voraussetzung für dieses Verfahren ist, dass die genutzten WLAN-Accesspoints alle 802.1X/EAP unterstützen und ein entsprechender RADIUS-Server samt hinterlegter Benutzerdatenbank vorhanden ist. Wenn zusätzlich auch die kabelgebundenen Netzwerkdaten vor einem unbefugten Zugriff geschützt werden sollen, müssen auch alle Komponenten (vor allem die Switches) im Netzwerk das Verfahren unterstützen.

Der RADIUS-Server kann dabei auf unterschiedliche Arten bereitgestellt werden. Er kann über eine vorhandene Benutzerdatenbank (Windows-AD + IAS, Schulserver) einen zentralen WLAN-Controller in der Schule oder auch als außerhalb der Schule befindlicher Dienst eingebunden werden.

Insbesondere wenn eine neue Nutzerdatenbank aufgebaut wird, entsteht bei beiden Varianten ein langfristiger nicht unerheblicher Pflegeaufwand (Passwörter zurücksetzen, neue Benutzer anlegen, Schuljahreswechsel). Die Benutzeroberfläche für die Verwaltung der Benutzerkonten sollte so gestaltet sein, dass Klassenlisten aus dem Schulverwaltungsprogramm importiert werden können und die Bedienung auch z.B. von einem weiteren Rechner aus dem Schulsekretariat oder dem Lehrerzimmer möglich ist. Für diese und weitere regelmäßig notwendige Tätigkeiten wie das Zurücksetzen von Passwörtern muss klar definiert

werden, welche Mitarbeiter der Schule die Berechtigung dafür haben und wie die Abläufe dafür geregelt sind. Aus Sicherheitsgründen sollte dieses möglichst nur über das kabelgebundene Netzwerk möglich sein.

### Internetanbindung

Abhängig von der angedachten Nutzerzahl eines schulischen Netzwerkes ist auch an die ausreichend breitbandige Versorgung mit Internet in der Planungsphase zu berücksichtigen. Gerade bei hohen Nutzerzahlen sind VDSL- und Glasfaseranschlüsse oder alternativ schnelle (Richt-)Funkverbindungen zu bevorzugen. Stehen diese nicht zur Verfügung, können auch mehrere ADSL-Anschlüsse über einen Router mit Load-Balancing-Funktion (mehrere WAN-Ports) gebündelt und über QoS (Quality of Service) sichergestellt werden, dass die verschiedenen Bereiche des schulischen Netzwerkes mit ausreichender Geschwindigkeit versorgt werden. Alternativ kann z.B. auch für das WLAN ein weiterer separater Internetanschluss genutzt werden.

Vorsicht ist geboten bei Tarifen, die eine Volumenbegrenzung oder ähnliche Einschränkungen vorsehen (häufig bei mobilfunkbasierten Tarifen). Entweder wird bei Überschreiten der Freivolumengrenze die Geschwindigkeit erheblich gedrosselt oder es fallen Zusatzkosten an.

### Jugendschutz

Über geeignete Lösungen ist durch die Schule mit einem vertretbaren Aufwand sicherzustellen, dass minderjährige Schüler möglichst keinen Zugriff auf jugendgefährdende Inhalte bekommen. Hierzu sind auf dem Markt verschiedene technische Lösungen vorhanden, die zentral im Schulnetzwerk gesteuert



werden können. Sie können entweder über den Router, das WLAN-Management, einen bestehenden Schulserver oder über ein separates Gerät integriert werden. In den Ausstattungsempfehlungen gibt es hierzu weitere Hinweise. Beachtet werden muss, dass weitere einmalige und jährliche Kosten entstehen können.

## Dokumentation

Um die Sicherheit, die Erweiterbarkeit und die Wartbarkeit des schulischen Netzwerkes sicherzustellen, sind die grundlegende Einrichtung und alle fortlaufenden Änderungen durch die ausführenden Personen bzw. Firmen schriftlich zu dokumentieren. Die jeweils aktuelle Fassung dieser Dokumentation sollte stets in der Schule abgelegt sein.

## Protokollierung

Wenn eine unbeaufsichtigte Nutzung des Internets erfolgt, sind alle Anmeldevorgänge und die anschließenden Nutzeraktivitäten im Internet (aufgerufene Seiten usw.) personenbezogenen zu protokollieren und für einen festgelegten Zeitraum zu speichern. Damit ist sichergestellt, dass die Schule bei strafrechtlichen Verstößen oder zivilrechtlichen Forderungen den Urheber der Schadens ermitteln kann.

Die Speicherdauer der Protokolldaten, die zugriffsberechtigten Personen im Rahmen der Protokollauswertung sowie die Fälle, in denen eine Protokollauswertung erfolgen darf, regelt die Schule in der Nutzungsordnung. Die Dauer der Aufbewahrungszeit muss auf Basis einer gesetzlichen Grundlage und der konkreten technischen und organisatorischen Verhältnisse vor Ort begründet werden. Der schulische Datenschutzbeauftragte muss (sofern vorhanden) einbezogen werden.

Die Speicherdauer der Protokolldaten, die zugriffsberechtigten Personen im Rahmen der Protokollauswertung sowie die Fälle, in denen eine Protokollauswertung erfolgen darf, regelt die Schule ebenfalls in der Benutzungsordnung.

## Nutzungsordnung

Jede Schule muss für die Internetnutzung der Schüler eine Nutzungsordnung erstellen, in der die wichtigsten Regeln und Vorgaben für die schulische Internetnutzung festgelegt sind. Die sollte durch die Schulkonferenz beschlossen werden. Alle Schüler und ihre Eltern müssen eine entsprechende Einverständniserklärung unterzeichnen, bevor der Zugang zum Internet freigeschaltet wird.

Eine in Zusammenarbeit mit dem ULD (Unabhängiges

Landeszentrum für Datenschutz Schleswig-Holstein) erstellte Musternutzungsordnung enthält alle wichtigen Punkte und kann die Grundlage für die individuelle Nutzungsordnung einer Schule bilden.

## Beratung

Das IQSH bietet Schulen eine Beratung zur Internetnutzung sowie der Netzwerk-/WLAN-Ausstattung an.

## Kontakt

Christoph Olsen  
Tel.: 0431-5403-227  
Mail: christoph.olsen@iqsh.de

## Impressum

Themenpapiere für Schulen  
in Schleswig-Holstein

Herausgeber:

Institut für Qualitätsentwicklung an Schulen

Schleswig-Holstein (IQSH)

Schreberweg 5

24119 Kronshagen

Gestaltung Deckblatt:

bdrops. Werbeagentur, Kiel