LANCOM Whitepaper

Anforderungen an Schulnetzwerke

Zur Gewährleistung eines zeitgemäßen Unterrichts und der Entfaltungsmöglichkeit pädagogischer Ziele, auch in digitaler Hinsicht, stellt die schulische Netzwerkinfrastruktur die notwendige Grundlage dar. Aufgrund der äußerst unterschiedlichen Voraussetzungen und Medienkonzepte in den Schulen werden in diesem Whitepaper Leitfäden für den Aufbau moderner schulischer Netzwerke illustriert. Auf dieser Basis kann jede Schule und ihr Träger ganz individuell entscheiden, welche Infrastruktur hinsichtlich des digitalen Lernens aktuell zu den Schülern und dem Lehrpersonal passt und umgesetzt werden soll.

Das Dokument ist in folgende Sektionen aufgeteilt:

Konzeptionelle Anforderungen an die Netzwerkinfrastruktur

Im Folgenden werden die grundsätzlichen Anforderungen an die Netzwerkinfrastruktur aufgeführt, die jedes zeitgemäße schulische Medienkonzept berücksichtigen sollte. Dies betrifft die Bereiche Netztrennung, Skalierbarkeit und Zukunftsfähigkeit sowie Vertrauenswürdigkeit und Datenschutz.

Sichere Netztrennung

Schulische Netzwerkanwender wie beispielsweise Schüler, Lehrer, IT-Management oder auch der Schulträger unterscheiden sich in den genutzten Daten und Inhalten, aber auch in Bezug auf Sicherheitsanforderungen. Aus diesem Grund muss die zugrundeliegende Infrastruktur eine Trennung verschiedener Netze ermöglichen. Seitens der Kultusministerien der Länder wird deshalb mindestens die Trennung von Verwaltungs- und pädagogischem Netzwerk (zumindest logisch über sog. virtuelle LANs kurz VLANs) verlangt.

Darüber hinaus sollte die Infrastruktur ein BYOD-Konzept („Bring your own Device“) ermöglichen, sodass externe Geräte von Schülern sowie Lehrkräften über ein eigenes (logisches) Netzwerk eingebunden werden können. So ergibt sich als Idealszenario ein Schulnetzwerk, das in mindestens drei logische Teilnetzwerke unterteilt wird:

- Verwaltungsnetzwerk
- Pädagogisches Netzwerk
- Gäste-Netzwerk für private Nutzung

Der Zugriff auf das Verwaltungsnetzwerk erfolgt in der Regel über einen externen Dienstleister bzw. ein kommu-

nales Schulamt, weshalb eine sicher verschlüsselte Anbindung über das Internet per VPN gegeben sein muss. Bei Einsatz eines Cloud-Management-Systems müssen die zu verwaltenden Komponenten eine sichere Verbindung per HTTPS/SSL initiieren können.

Skalierbarkeit und Zukunftsfähigkeit

Durch die Digitalisierung des Schulalltags ergeben sich gänzlich neue Anforderungen an die Leistungsfähigkeit und Erweiterbarkeit der Netzwerkinfrastruktur: Die der Infrastruktur zugrundeliegenden Komponenten sowie das Management-Konzept müssen zukünftige Entwicklungen abbilden können, wie zum Beispiel:

- Integration einer steigenden Anzahl mobiler (auch privater) Endgeräte wie Tablets, Notebooks und Smartphones (mind. zwei Endgeräte pro Person)
- Integration neuer kabelgebundener, IP-basierter Arbeitsgeräte wie Beamer, digitale Tafeln oder Server
- Bereitstellung von ausreichend Bandbreite für eine hohe Anzahl an Geräten in allen Klassenräumen
- Flexible, nachträgliche Inbetriebnahme zusätzlicher Netzwerkkomponenten wie beispielsweise WLAN Access Points und Switches für neue Räumlichkeiten

Vertrauenswürdigkeit und Datenschutz

Ein relevantes IT-Sicherheitsrisiko sind versteckte Zugangsmöglichkeiten (Backdoors) in Soft- und Hardware, die unbefugten Dritten das unbemerkte Eindringen in die Netze gestatten. Dieses Risiko kann bei der Auswahl der schulischen Netzwerkinfrastruktur grundlegend eliminiert werden, indem man sich für einen Hersteller mit konsequenter Anti-Backdoor-Politik entscheidet. Ein gutes Indiz dafür ist die erklärte volle Übereinstimmung mit Ziffer 2.4 der Ergänzenden Vertragsbedingungen über den Kauf von Hardware (EVB-IT Kauf AGB), Version 2.0 vom 17.03.2016[1]. Zudem muss sowohl die Schulinfrastruktur als auch die Administration des Netzwerks auf höchste Sicherheit und den Schutz personenbezogener Daten von Schülern, Lehrern und allen anderen Nutzern ausgelegt sein. Im Kern will das durch die Datenschutzgrundverordnung (DSGVO) heute europäisch kodifizierte Datenschutzrecht die von einer Datenverarbeitung betroffenen Personen schützen. Es geht also darum, die personenbezogenen Daten all derer zu schützen, die das Datennetzwerk einer Schule nutzen oder deren Daten entweder nutzungsbezogen oder aus anderen Gründen dort verarbeitet werden. Dabei muss der jeweilige Schulträger für die sorgfältige Auswahl und Implementierung und das Management der Netzwerkinfrastruktur Sorge tragen.

[1] Der Auftragnehmer liefert die Hardware frei von Schaden stiftender Software, z. B. in mitgelieferten Treibern oder der Firmware. Dies ist in geeigneter Form zu einem angemessenen Zeitpunkt vor der Lieferung zu prüfen. Der Auftragnehmer erklärt, dass die Prüfung keinen Hinweis auf Schaden stiftende Software ergeben hat. Diese Regelung gilt für jede, auch die vorläufige und Vorabüberlassung, z. B. zu Testzwecken. Der Auftragnehmer gewährleistet darüber hinaus, dass die von ihm zu liefernde Hardware frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Hardware, anderer Hard- und/oder Software oder von Daten gefährden und dadurch den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen durch
- Funktionen zum unerwünschten Absetzen/Ausleiten von Daten,
- Funktionen zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder
- Funktionen zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen.

Unerwünscht ist eine mögliche Aktivität einer Funktion, wenn die Aktivität so weder vom Auftraggeber in seiner Leistungsbeschreibung gefordert, noch vom Auftragnehmer unter konkreter Beschreibung der Aktivität und ihrer Auswirkungen angeboten, noch im Einzelfall vom Auftraggeber ausdrücklich autorisiert („opt-in") wurde.

Anforderungen an die eingesetzten Netzwerkkomponenten

Zur Realisierung aller im jeweiligen Medienkonzept einer Schule vorgesehenen Anforderungen ist die Auswahl geeigneter Netzwerkkomponenten essentiell. Im Folgenden werden die technischen Voraussetzungen für die einzelnen Netzsegmente in den Bereichen WAN/Security, LAN und WLAN aufgeführt. Zusätzlich helfen Checklisten bei der individuellen Geräteauswahl.

Internetzugang – Gateway / Firewall

Aktuelle Sicherheitstechnologien und keine Backdoors

Als Peripherie-Komponenten vom Internet ins interne Netz haben Gateways und Firewalls die sensibelste Funktion in einem Netzwerk inne. Insbesondere im Schulumfeld sollte daher das wichtigste Auswahlkriterium für Gateways und Firewalls auf Sicherheit, Vertrauenswürdigkeit und Datenschutz liegen. Der Hersteller sollte sich dazu verpflichten, dass die von ihm gelieferten Produkte keine extern nutzbaren, ungewollten Schnittstellen (Backdoors) mit sich bringen und den europäischen Datenschutzrichtlinien entsprechen. Zudem sollten seitens des Herstellers regelmäßige und automatische Software-Updates inkl. neuer Sicherheitstechnologien bereitgestellt werden, damit auch bei neuen Bedrohungen aus dem Internet das Schulnetzwerk geschützt ist.

Highspeed-Internet und Load Balancing

Im Zuge der Digitalisierung von Schulen steigt das Datenaufkommen aus dem und in das Internet und somit die erforderliche Bandbreite. Für die Unterstützung eines am jeweiligen Schulstandort verfügbaren Highspeed-Internetzugangs ist ein leistungsstarkes Gateway die notwendige Voraussetzung. Dabei sollte zwingend auf zukunftsfähige Komponenten gesetzt werden. Sollte die Bandbreite eines

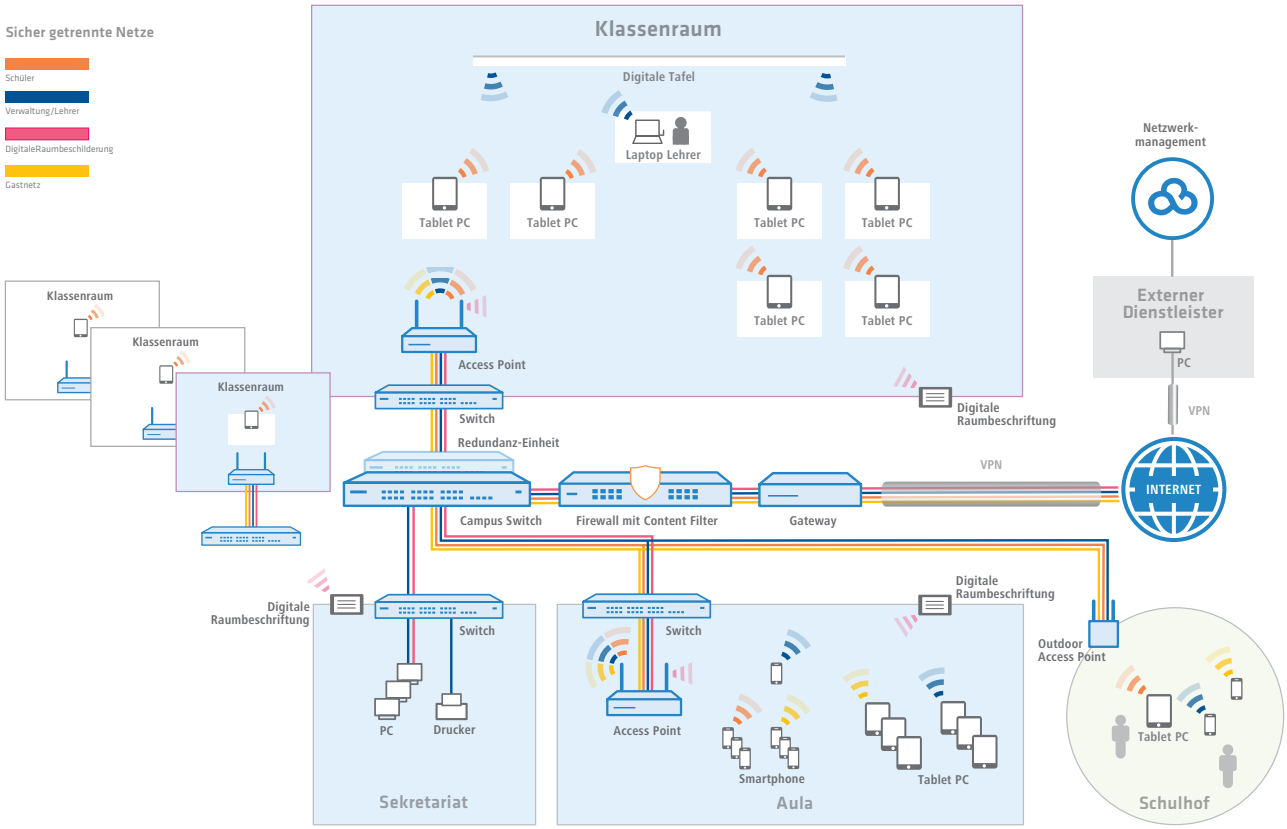

Abb. 1: Beispielszenario für ein Schulnetzwerk

einzigen Internetanschlusses nicht ausreichen, so muss das Gateway mehrere Internetanschlüsse simultan unterstützen, um beispielsweise Anwendungen mit hohem Datenaufkommen über die jeweils bestmögliche Leitung zu routen (Load Balancing). Zusätzlich sorgt die Nutzung mehrerer paralleler Internetanschlüsse für hohe Ausfallsicherheit, falls eine Leitung wegbricht.

VPN

Zur sicheren Anbindung externer Dienstleister oder an ein Rechenzentrum über das Internet müssen die Geräte die VPN-Verschlüsselungstechnologie unterstützen. Die bei vielen Endgeräten und Gegenstellen verbreitete und hochsichere Technologie IPSec-VPN (nach dem aktuellen Standard IKEv2) ermöglicht die komfortable und flexible Anbindung externer Netzwerk-User oder ganzer Standorte und Dienstleister. Dabei sollte das Gateway in der Lage sein, mehrere parallele VPN-Verbindungen ohne Leistungseinbußen zu terminieren.

Netzwerksegmentierung

Damit die verschiedenen logischen Teilnetzwerke (Verwaltungsnetzwerk, pädagogisches Netzwerk, Gäste-Netzwerk) auch WAN-seitig sicher getrennt werden, empfiehlt sich erneut die VPN-Technologie. Falls eine physikalische Trennung des Verwaltungs- und des pädagogischen Netzwerks gefordert ist, sollte ein Router zum Einsatz kommen, der mehrere Internetanschlüsse unterstützt (Multi-WAN).

Content Filter

Das Thema Jugendschutz ist bereits bei den Eltern der Schüler ein wichtiges Auswahlkriterium für oder eben gegen eine Schule. Der eingesetzte Router bzw. die eingesetzte Firewall müssen auch aus rechtlichen Gründen mit einem Jugendschutzfilter ausgestattet sein. Dieser erkennt Internetinhalte und blockiert diese bei Verstößen gegen die vorgegebenen Regeln. Ebenso können ganze Anwendungsgruppen wie Social Media blockiert (Blacklisting) oder erlaubt werden (Whitelisting), um unerwünschten Internetverkehr für Schüler zu unterbinden. Dabei gelten dank Netztrennung für andere Netzwerk-User wie z. B. Lehrer auch andere Regeln. Zudem sollte die Möglichkeit eines „autorisierten Overides“ gegeben sein, sodass aus begründeten Anlässen kurzzeitige Zugriffe auf eigentlich gesperrte URLs möglich sind.

Schutz vor Spam, Viren, Malware und Cyberangriffen

Die steigende Anzahl an Cyber-Angriffen auf Behörden und öffentliche Einrichtungen zeichnet ein bedrohliches Szenario für die Sicherheit und Verfügbarkeit von Daten und IT-Systemen und somit auch für die Sicherheit von Schulnetzwerken. Zum Schutz vor Spam, Viren, Malware

Checkliste Gateways / Firewalls

- ☐ Keine Backdoors, entspricht europäischen Datenschutzrichtlinien
- ☐ Regelmäßige, automatische und kostenfreie Software-Updates inkl. neuer Sicherheitstechnologien
- ☐ Unterstützung von Highspeed-Internetanschlüssen sowie Load Balancing
- ☐ Unterstützung von IKEv2-IPSec-VPN mit mindestens 5 Kanälen
- ☐ Unterstützung von Netzwerksegmentierung (mindestens logisch, ggfs. physikalisch)
- ☐ Internet-Content-Filter integriert inkl. Anwendungserkennung und -kontrolle, auch für verschlüsselte HTTPS-Verbindungen
- ☐ Schutz vor Spam, Viren, Malware und Cyberangriffen (Unified Threat Management)

und Cyberangriffen empfiehlt sich daher der Einsatz einer Firewall mit umfassenden UTM-Funktionen (Unified Threat Management). Um auch gegen neueste Gefährdungen gewappnet zu sein, muss die zugrundeliegende Sicherheits-Software sich ständig aktualisieren (Machine Learning). Wie beim Router sollte hier auf eine „No Backdoor Policy" des Herstellers geachtet werden sowie auf die strikte Einhaltung europäischer Datenschutzrichtlinien.

Interne Vernetzung – Switches

Hohe Leistung auf allen Ports

Switches sind die Verteilungsinstanz für zahlreiche kabelgebundene IP-Komponenten und werden daher oft zum Flaschenhals des Netzwerks: WLAN Access Points, PCs, Drucker, Telefone und Telefonanlagen oder auch weitere Switches zur Unterverteilung sowie die zunehmende Anzahl an IoT-Devices werden per Ethernet-Kabel angeschlossen und erfordern hohe Leistung. Zusätzlich setzen moderne Schulen nicht mehr auf klassische Kreidetafeln und Overheadprojektoren, sondern auf IP-basierte Arbeitsgeräte wie Beamer und digitale Tafeln. Darum ist bei der Auswahl der Switches auf entsprechende Performance-Reserven und eine ausreichende Anzahl an Ports zu achten. So sollten zukunftsfähige Switches neben 1-Gigabit-Ethernet-Ports mit zusätzlich 2,5-Gigabit-Ethernet-Ports („Multi-Gigabit") zum Einsatz kommen, damit beispielsweise leistungsstarke WLAN Access Points der neuesten Generation (Wi-Fi 6) vollen Durchsatz erhalten, denn: Die erhöhten Datenraten bei der Verwendung von Wi-Fi 6 erfordern bereits an den Anschlüssen der Access Points 2,5 Gigabit Ethernet, da die benötigten Performance-Ansprüche die eines einfachen Gigabit Ethernet-Ports übersteigen. Für den Anschluss an einen übergeordneten Aggregation Switch werden zudem 10G-Glasfaseranschlüsse (SFP+) benötigt.

Power over Ethernet

Die wachsende Anzahl an IP-Komponenten in Schulen erfordert auch ein Umdenken bei der Verkabelung, denn insbesondere in älteren, vielleicht sogar denkmalgeschützten Gebäuden ist eine nachträgliche Installation von Stromkabeln und Steckdosen nur mit hohen und kostenintensiven Aufwänden möglich. Daher empfiehlt sich der Einsatz von PoE-Switches (Power over Ethernet), welche die angeschlossenen Geräte direkt mit Strom versorgen. Dabei muss insbesondere die Versorgung besonders leistungsfähiger Komponenten mit einer erhöhten Leistungsaufnahme im Voraus eingeplant werden. Dazu eignen sich Switches mit PoE nach dem Standard IEEE 802.3at („PoE+") für bis zu 25,4 Watt Leistung pro Port. Nicht zuletzt sollte die zur Verfügung stehende PoE-Gesamtleistung der Switches mit Bezug auf die Gesamtanzahl aller anzuschließender PoE-Geräte kalkuliert werden.

Netzwerksegmentierung und Zugangskontrolle

Damit die verschiedenen Netze für unterschiedliche Anwendergruppen bereitgestellt werden können, ist eine VLAN-Zuweisung an den gewünschten Switch-Ports die technische Grundlage. Zusätzlich sollte der Switch sicherstellen, dass keine fremden bzw. unerwünschten Clients Zugriff auf das Schulnetzwerk erhalten. Ermöglicht wird eine solche Zugangskontrolle über den Netzwerksicherheitsstandard IEEE 802.1X (Port-based, Single, Multi und MAC-based) auf allen Ports.

Layer-3-Funktionen zur Entlastung des Netzwerks

Ein moderner Switch kann Aufgaben übernehmen, die in klassischen Netzwerken von einem Gateway ausgeführt

werden. Notwendige Voraussetzung: Die Unterstützung von Layer-3-Funktionalität im Switch. So ermöglicht statisches Routing über den Switch die Vordefinition von Netzwerkrouten durch ein oder mehrere Netzwerksegmente hinweg und somit einen schnelleren Datenaustausch insbesondere bei hohem internen Datenaufkommen. Das Gateway wird entlastet und freiwerdende Gateway-Kapazitäten stehen dann für die Bewältigung des externen Datenverkehrs zusätzlich zur Verfügung. Ebenso kann ein Switch als DHCP-Server eigenständig und automatisch IP-Adressen an Clients vergeben und den Router dadurch weiter entlasten.

Aggregation Switches für große, verteilte Netzwerke

In großen Infrastrukturen mit vielen Räumlichkeiten oder sogar verteilten Gebäudeteilen muss die Switch-Infrastruktur hierarchisch realisiert werden. Dafür dient ein übergeordneter hochperformanter Aggregation Switch als Distributions-Basis für untergeordnete Access Switches. Die Access Switches werden per Glasfaser (SFP+ für 10G) an den Aggregation Switch angeschlossen und übernehmen die Datenverteilung an die Clients. Da in einer solchen Topologie die Datenlast des gesamten Netzwerks am Aggregation Switch zusammenläuft, muss er für den Uplink an den zentralen Schulserver portseitig mit enormer Backhaul-Kapazität ausgestattet sein (z. B. QSFP+ für 40G oder SFP28 für 25G). Damit nicht genug: Ein solch zentrales Netzwerksegment sollte zukunftssicher und flexibel erweiterbar geplant werden: Über Stacking sind Netzwerk-Erweiterungen spielend einfach, da sich mehrere physikalische Switches als eine logische Einheit zusammenfassen und damit bequem warten und managen lassen. Sollte das Netzwerk nachträglich erweitert werden, erhält der neue Switch eine automatisierte Konfiguration vom Stack-Master und ist binnen Sekunden einsatzbereit. Darüber hinaus lassen sich per Stacking Geräte- oder Netzwerk-Redundanzen für höchste Ausfallsicherheit realisieren. Ein redundantes Netzteil, welches auch im laufenden Betrieb ausgetauscht werden kann („hot-swappable"), sorgt zusätzlich für unterbrechungsfreien Netzwerkbetrieb.

Checkliste Access Switches

- ☐ Hohe Portgeschwindigkeit (mind. Gigabit Ethernet, bei Einsatz von Wi-Fi 6 Access Points 2,5 Gigabit Ethernet)
- ☐ 10G-Glasfaseranschlussmöglichkeit (SFP+) für Uplink an weitere Switches der Aggregations-Ebene
- ☐ Stromversorgung angeschlossener Endgeräte via Power over Ethernet (IEEE 802.3at/PoE+)
- ☐ Netzwerksegmentierung über VLAN
- ☐ Portzugangskontrolle nach IEEE 802.1X
- ☐ Layer-3-Funktionen Static Routing und DHCP-Server zur Entlastung des Gateways

Checkliste Aggregation Switches

- ☐ Multi-Gigabit-Portunterstützung (10/5/2,5/1 Gigabit Ethernet bzw. SFP+)
- ☐ QSFP+ (40G)/SFP28 (25G) Uplink-Portunterstützung für ausreichende Backhaul-Kapazität
- ☐ Stacking-Unterstützung über eine „non-blocking" Backplane-Architektur
- ☐ Redundante Stromversorgung über „hot-swappable" Netzteil

Kabellose Vernetzung – WLAN Access Points

Hohe Leistungsfähigkeit für Schulumgebungen

Schulen oder Bildungseinrichtungen generell sind klassische „High-Density-Umgebungen". Dies bedeutet, dass Lehrer und Schüler teils mit mehreren (auch privaten) Endgeräten über WLAN eingebunden sind und arbeiten. Dabei kommen unterschiedlichste Endgeräte wie Notebooks, Tablet-PCs und Smartphones zum Einsatz – realistischer Weise rechnet man mit mindestens zwei Endgeräten pro Person. Hinzu kommt, dass das Datenaufkommen in Schulnetzwerken immens hoch ausfällt. Seien es Online-Recherchen, Videostreams von Lehrfilmen oder der Zugriff auf den Schulserver für den Down- und Upload von schulischen Unterlagen – ohne eine Leistungsfähigkeit der eingesetzten WLAN Access Points kann nicht ausreichend Bandbreite für

einen flüssigen Unterricht in allen Klassenräumen gewährleistet werden. Für höchste Effizienz und Geschwindigkeit in solchen High-Density-Umgebungen wurde der WLAN-Standard Wi-Fi 6 (IEEE 802.11ax) konzipiert, weshalb sich der Einsatz von Access Points mit Unterstützung dieses aktuellen Standards empfiehlt.

Netzwerksegmentierung über Multi-SSID

Für die sichere Trennung der verschiedenen Anwendungsnetze in beispielsweise Verwaltungsnetz, pädagogisches Netz sowie Gäste-Netzwerk für Schüler und externe Gäste kommen im WLAN-Betrieb separate SSIDs zum Einsatz (Multi-SSID). Die eingesetzten WLAN Access Points müssen daher die Bereitstellung mehrerer SSIDs über ein Gerät unterstützen.

Sichere Zugangskontrolle

Je nach Netzwerk (SSID) werden zur Nutzung unterschiedliche Anmeldeinformationen benötigt. So können sich schuleigene Endgeräte (Laptops oder Tablets der Lehrer oder auch der Schüler) mittels eines hierauf installierten Zertifikats via WPA2 Enterprise bzw. IEEE 802.1X am pädagogischen Netz automatisch anmelden und erhalten somit Zugriff auf pädagogische Inhalte des Schulservers. Private Endgeräte dagegen authentifizieren sich mit einer sicheren Passphrase (WPA2 / WPA3) oder idealerweise mit einer individuellen Benutzerkennung (Private Preshared Key, PPSK). Speziell die letzte Variante empfiehlt sich für den Schulalltag, da somit auch kurzfristige für die jeweilige Unterrichtssituation erstellte Zugangsdaten an die Schüler gegeben werden können. Für die Implementierung entsprechender Sicherheitskonzepte müssen die eingesetzten WLAN Access Points diese Sicherheitstechniken unterstützen.

Zeitgesteuerte WLAN-Netze

Damit die private Nutzung des schulischen WLANs über das Gäste-Netzwerk auf den Pausenbetrieb beschränkt bleibt, sollte die zugrundeliegende Infrastruktur eine zeitliche Steuerung der Ausstrahlung bestimmter WLAN-SSIDs ermöglichen. Genauso kann für bestimmte Unterrichtssituationen der Zugriff auf eine SSID mit erweiterten Internetzugriffsrechten (beispielsweise für den Geschichtsunterricht) erlaubt werden.

Access Point-Positionierung

Um ein leistungsfähiges WLAN-Netzwerk zur Verfügung zu stellen, muss an allen Stellen im Gebäude, an denen mit mobilen Endgeräten gearbeitet werden soll, ein stabiler WLAN-Empfang – auch im 5 GHz-Frequenzband – möglich sein. Durch die speziellen Anwendungsszenarien in Schulen kommt es immer wieder zu Lastspitzen in der Nutzung des Netzwerks (z. B. durch das gleichzeitige Schauen von Videos oder dem Abspeichern von Dateien auf einem Dateiserver). Auf der technischen Ebene teilen sich alle Endgeräte die Bandbreite eines Access Points. Durch die zuvor beschriebenen speziellen Nutzungsszenarien in Schulen wird deshalb perspektivisch in jedem Klassenraum ein Access Point installiert werden müssen. Speziell in älteren, evtl. denkmalgeschützten Gebäuden mit dickeren Wänden und Decken kann eine WLAN-Ausleuchtung zur exakteren Planung sinnvoll und notwendig sein.

Optional: WLAN im Freien

Auch auf dem Schulhof wollen Schüler und Lehrer flächendeckenden Zugriff auf das Netzwerk haben. Die hierfür notwendigen WLAN Access Points müssen bei jeder Witterung und auch bei sehr kalten oder sehr heißen

Temperaturen zuverlässig arbeiten. Spezielle Outdoor-geeignete Gehäuse der Schutzklasse IP67 sind vollständig staubdicht und auch gegen Strahlwasser geschützt. Zudem sollte ein Temperaturbereich zwischen -30°C bis +70°C in den Spezifikationen gekennzeichnet sein.

Optional: Digitale, funkgesteuerte Raumbeschilderung

Für eine deutlich erhöhte Transparenz im oft unübersichtlichen Schulalltag empfiehlt sich der Einsatz digitaler Displays für die Klassenraumbeschriftung. Durch eine Schnittstelle zum Schulkalenderverwaltungssystem können jederzeit die Unterrichtseinheiten im jeweiligen Klassenzimmer angezeigt werden. Dabei erhalten die Displays die anzuzeigenden Informationen per Funk (im 2,4 GHz-Frequenzbereich) über einen entsprechenden Access Point. Um Interferenzen im Funkfeld und somit eventuelle Paketverluste zu vermeiden, sollte die zum Einsatz kommende Infrastruktur für beide Funktechnologien – WLAN und die Ansteuerung der digitalen Displays – eine störungsfreie Koexistenz gewährleisten.

Checkliste WLAN Access Points

- ☐ Hohe Leistungsfähigkeit durch die Unterstützung des WLAN-Standards Wi-Fi 6, mindestens aber Wi-Fi 5 Wave 2
- ☐ Dualband-Fähigkeit (2,4 GHz und 5 GHz)
- ☐ DFS-Kanäle im 5 GHz-Band für insgesamt höhere Leistungsfähigkeit
- ☐ Möglichkeit für mehrere WLAN-Netzwerke über ein Gerät (Multi-SSID)
- ☐ Zugangskontrolle nach WPA2 Enterprise bzw. IEEE 802.1X, WPA2 / WPA3 und PPSK
- ☐ Möglichkeit zur Zeitsteuerung bestimmter WLAN-Netze
- ☐ Optional: Digitale, funkgesteuerte Raumbeschilderung
- ☐ Optional: Outdoor WLAN Access Points mit IP67-Schutzgehäuse und erweitertem Temperaturbereich (-30°C bis +70°C)

Management

Zentralisierung des Managements

In klassischen Netzwerkinfrastrukturen werden sämtliche Komponenten individuell in Betrieb genommen und konfiguriert. Die Voraussetzung: geschultes IT-Fachpersonal vor Ort – meist im normalen Schulbetrieb nicht vorhanden. Daher sollte bei der Auswahl eines Netzwerk-Management-Systems das oberste Kriterium die Vermeidung manueller Einzelgerätekonfigurationen sein. Die Lösung liegt in der Zentralisierung durch ein Controller-Management. Ein klassischer Hardware-Controller, beispielsweise für das WLAN-Management (WLAN-Controller, WLC), dient zur zentralen Konfiguration und Steuerung einer oder mehrerer Netzwerkkomponenten desselben Typs, z. B. Access Points. Diese Zentralisierung minimiert den Aufwand bei der Einrichtung und der Pflege des Funknetzes. Der große Nachteil: Nur ein Netzsegment wie z. B. das WLAN kann auf diese Weise verwaltet werden, die Konfiguration weiterer Komponenten wie Gateways, Firewalls oder Switches muss manuell erfolgen. Zudem benötigt man Zugriff auf diesen Hardware-Controller. Daher sollte ein modernes Schulnetz mit einer Vielzahl an Netzwerkkomponenten auf einen modernen Cloud-basierten Controller setzen.

Cloud-managed Networks

Hier befindet sich der „Controller" in einem Rechenzentrum bzw. der Cloud, welche über das Internet erreichbar ist. Der Administrator hat dabei über eine zentrale, grafische Benutzeroberfläche den vollständigen Überblick über alle Netzwerkkomponenten und den Zustand des Netzwerks – 24/7, historisch nachvollziehbar, einfach über einen Webbrowser. Der große Vorteil eines Cloud-basierten Management-Systems liegt insbesondere in der massiven Zeitersparnis: Große Teile der Konfiguration werden dem Administrator durch „Zero-touch Deployment" und „Auto-Konfiguration" abgenommen. Je nach Anbieter

unterscheiden sich die unterstützten Funktionen eines Cloud-Management-Systems – ein prüfender Blick in die Leistungsmerkmale lohnt sich!

Ganzheitliches Netzwerk-Management

Wie in diesem Whitepaper beschrieben haben die Planung und Implementierung sämtlicher Netzsegmente direkten Einfluss auf die Digitalisierung des Schulbetriebs. Daher ist ein Cloud-Controller mit Fokus auf einen einzelnen Bereich wie WLAN wenig sinnvoll, da ansonsten die Sicherheitseinstellungen der Switches manuell auf den einzelnen Geräten konfiguriert werden müssten. Ein modernes Cloud-Management-System verwaltet mehrere oder idealerweise sämtliche Netzwerkkomponenten (Gateways/Firewalls, Switches und WLAN Access Points) ohne Systembrüche.

Einhaltung europäischer Datenschutzbestimmungen

Schulträger müssen bei der Auswahl eines Herstellers und Cloud-Dienst-Anbieters für die schulische Netzwerkinfrastruktur darauf achten, dass diese die Einhaltung des gesetzlich vorgesehenen Datenschutzniveaus gemäß DSGVO gewährleisten.

Die Hersteller von Lösungen aus den USA erfüllen diese infrastrukturellen Voraussetzungen trotz bilateraler Zusicherungen und/oder Unterwerfung unter den sogenannten Privacy-Shield[2] nicht, weil die dortige Gesetzgebung einen unkontrollierbaren Zugriff amerikanischer Behörden auf die personenbezogenen Daten aller Nutzer ermöglicht und so in einem unauflösbaren Widerspruch zu den europäischen Regelungen steht[3].

Aufgrund des 2018 verabschiedeten CLOUD Acts[4] gilt dies ebenso für das Management der schulischen Netzwerkinfrastruktur, beispielsweise über einen US-amerikanischen Cloud-Dienst.

Ein Hersteller und Cloud-Dienst-Anbieter mit Sitz in der EU gewährleistet demgegenüber die Einhaltung des datenschutzrechtlichen Schutzniveaus, so wie es gesetzlich Pflicht ist. Nur so kann vor einer missbräuchlichen Nutzung der Daten maximaler Schutz erlangt werden.

Darüber hinaus sollte das Rechenzentrum, in welchem die netzwerkspezifischen Daten der Schule gehostet werden, bevorzugt den Sitz in der EU bzw. in Deutschland haben.

Betriebsmodelle

Eine öffentliche Cloud, die den oben beschriebenen Datenschutzbestimmungen entspricht, bietet aufgrund der hohen Rechenleistung des Hosting-Servers große Vorteile im Bereich Skalierbarkeit für alle Installationsgrößen. Entscheidet man sich für dieses (in den allermeisten Fällen zu bevorzugende) Modell, bieten vertrauenswürdige Hosting-Anbieter eine hohe Systemverfügbarkeit sowie ausreichend Kapazität für die Integration zusätzlicher Netzwerkkomponenten in das Management. Wird die Schulinfrastruktur durch einen Managed Service Provider (MSP) gemanagt, sollte seitens des Herstellers die Möglichkeit des Hostings der Cloud-Server im Rechenzentrum des MSPs (Private Cloud) gegeben sein.

Stand-alone-Fähigkeit

Für höchste Betriebssicherheit eines Cloud-managed Networks ist auf eine Stand-alone-Fähigkeit der verwalteten Netzwerkkomponenten zu achten, so dass ein autonomer Weiterbetrieb auch bei Verlust der Verbindung zur Cloud

[2] Der EU-U.S. Privacy Shield verpflichtet in den USA datenverarbeitende Unternehmen gegenüber den Betroffenen zwar zur Beachtung ihrer Rechte analog den europäischen Regelungen; er reflektiert aber nicht das gänzlich andere gesetzliche Umfeld mit behördlichen Zugriffsbefugnissen, die dem europäischen Recht fremd sind. Dies betrifft namentlich den USA Patriot Act, der als Reaktion auf die Terroranschläge bereits 2001 als Bundesgesetz vom amerikanischen Kongress verabschiedet wurde. Er ermöglicht US-Behörden wie dem FBI, der NSA oder der CIA, ohne richterliche Anordnung Zugriff auf die Server von US-Unternehmen zu nehmen. Bei Ermittlungsmaßnahmen gegen den Dienstleister könnten so etwa die Nutzungsdaten aus dem Schulnetz ausgelesen werden und zwar unabhängig davon, ob diese in den USA oder auf dem lokalen Netzwerk der Schule abgelegt sind.

[3] Vgl. Heitzer, Eric: Gilt das Recht auf Vergessenwerden auf für Hausaufgaben? https://www.dgc-integrity.de/digitalisierung-in-schulen-und-der-datenschutz.html

[4] Dieses Gesetz befasst sich explizit mit Daten, die nicht in den USA gespeichert sind. Es betrifft insbesondere IT-Dienstleister mit Sitz in den USA und verpflichtet diese bei behördlicher oder richterlicher Anforderung zur Herausgabe von Daten und zwar unabhängig davon, wo diese Daten gespeichert werden, also insbesondere auch dann, wenn diese im Fall der Schule auf einem Speichermedium in Deutschland liegen. Erforderlich ist auch nicht das Eigentum an den Daten, sondern lediglich, dass der Dienstleister die Daten „kontrolliert", was im Falle der Netzwerkadministration der Fall ist. Diese Herausgabeverpflichtung nach amerikanischem Recht kollidiert allerdings mit europäischem Datenschutzrecht.

gewährleistet ist. Ebenso sollte im Falle einer ausgelaufenen Cloud-Betriebslizenz eine manuelle Konfiguration der Komponenten sichergestellt sein, sodass zu keiner Zeit eine Abhängigkeit zu einer einzigen Managementinstanz besteht.

Checkliste Management

- ☐ Zentralisierung des Netzwerkmanagements über einen Cloud-basierten Controller
- ☐ Automatisierte Inbetriebnahme neuer Netzwerkkomponenten (Zero-touch Deployment und Auto-Konfiguration)
- ☐ 24/7-Monitoring, historisch nachvollziehbar
- ☐ Managementfähigkeit für Gateways/Firewalls, Switches und WLAN Access Points
- ☐ Einhaltung europäischer Datenschutzbestimmungen
- ☐ Hosting in der EU bzw. in Deutschland
- ☐ Optionales Hosting des Cloud-Servers im Rechenzentrum eines Managed Service Providers
- ☐ Stand-alone-Fähigkeit der Netzwerkkomponenten, kein „Cloud-only“

Fazit

Eine schulische Netzwerkinfrastruktur bedarf einer vorausschauenden Planung, um nicht nur aktuellen, sondern auch zukünftigen Anforderungen in den Bereichen Digitalisierung der Lehrmethoden und insbesondere Sicherheit der Schülerinnen und Schüler gerecht zu werden. Eine einseitige Investition in nur ein Netzsegment kann sich ebenso rächen wie die Entscheidung für ein Netzwerk, welches nicht den europäischen Datenschutzbestimmungen entspricht. Ebenso ist ein zentralisiertes und automatisiertes Management aller Komponenten essentiell für einen reibungslosen Schulbetrieb. Die zusammenfassende Checkliste im Anhang dient als eine gute Entscheidungsgrundlage für die sich durch das jeweilige Medienkonzept ergebenden Anforderungen an das Schulnetzwerk.

Übersicht Checklisten

Checkliste Gateways / Firewalls

- Keine Backdoors, entspricht europäischen Datenschutzrichtlinien
- Regelmäßige, automatische und kostenfreie Software-Updates inkl. neuer Sicherheitstechnologien
- Unterstützung von Highspeed-Internetanschlüssen sowie Load Balancing
- Unterstützung von IKEv2-IPSec-VPN mit mindestens 5 Kanälen
- Unterstützung von Netzwerksegmentierung (mindestens logisch, ggfs. physikalisch)
- Internet-Content-Filter integriert inkl. Anwendungserkennung und -kontrolle, auch für verschlüsselte HTTPS-Verbindungen
- Schutz vor Spam, Viren, Malware und Cyberangriffen (Unified Threat Management)

Checkliste WLAN Access Points

- Hohe Leistungsfähigkeit durch die Unterstützung des WLAN-Standards Wi-Fi 6, mindestens aber Wi-Fi 5 Wave 2
- Dualband-Fähigkeit (2,4 GHz und 5 GHz)
- DFS-Kanäle im 5 GHz-Band für insgesamt höhere Leistungsfähigkeit
- Möglichkeit für mehrere WLAN-Netzwerke über ein Gerät (Multi-SSID)
- Zugangskontrolle nach WPA2 Enterprise bzw. IEEE 802.1X, WPA2 / WPA3 und PPSK
- Möglichkeit zur Zeitsteuerung bestimmter WLAN-Netze
- Optional: Digitale, funkgesteuerte Raumbeschilderung
- Optional: Outdoor WLAN Access Points mit IP67-Schutzgehäuse und erweitertem Temperaturbereich (-30°C bis +70°C)

Checkliste Access Switches

- Hohe Portgeschwindigkeit (mind. Gigabit Ethernet, bei Einsatz von Wi-Fi 6 Access Points 2,5 Gigabit Ethernet)
- 10G-Glasfaseranschlussmöglichkeit (SFP+) für Uplink an weitere Switches der Aggregations-Ebene
- Stromversorgung angeschlossener Endgeräte via Power over Ethernet (IEEE 802.3at / PoE+)
- Netzwerksegmentierung über VLAN
- Portzugangskontrolle nach IEEE 802.1X
- Layer-3-Funktionen Static Routing und DHCP-Server zur Entlastung des Gateways

Checkliste Aggregation Switches

- Multi-Gigabit-Portunterstützung (10 / 5 / 2,5 / 1 Gigabit Ethernet bzw. SFP+)
- QSFP+ (40G) / SFP28 (25G) Uplink-Portunterstützung für ausreichende Backhaul-Kapazität
- Stacking-Unterstützung über eine „non-blocking“ Backplane-Architektur
- Redundante Stromversorgung über „hot-swappable“ Netzteil

Checkliste Management

- Zentralisierung des Netzwerkmanagements über einen Cloud-basierten Controller
- Automatisierte Inbetriebnahme neuer Netzwerkkomponenten (Zero-touch Deployment und Auto-Konfiguration)
- 24/7-Monitoring, historisch nachvollziehbar
- Managementfähigkeit für Gateways / Firewalls, Switches und WLAN Access Points
- Einhaltung europäischer Datenschutzbestimmungen
- Hosting in der EU bzw. in Deutschland
- Optionales Hosting des Cloud-Servers im Rechenzentrum eines Managed Service Providers
- Stand-alone-Fähigkeit der Netzwerkkomponenten, kein „Cloud-only“