LEITFADEN

NETZWERKINFRASTRUKTUR IN ÖSTERREICHISCHEN SCHULEN

Wie mit zeitgemäßer LAN und WLAN-Infrastruktur die Digitalisierung im Bildungswesen ermöglicht werden kann

aruba
a Hewlett Packard Enterprise company

INHALT

VORWORT

2018 wurde vom Bundesministerium für Bildung, Wissenschaft und Forschung ein Masterplan für die Digitalisierung im Bildungswesen verfasst. Der Hardware und dem IT-Management wurde dabei ein eigenes Handlungsfeld zugeordnet, in dem flächendeckend die Voraussetzungen geschaffen werden sollen, dass digitale Instrumente und Tools an Schulen zum Einsatz kommen können.

Ein zuverlässiges und für zukünftige Entwicklungen offenes Netzwerk bildet das Fundament dafür, diese Ziele erreichen zu können.

Die im September 2016 vom Bundesministerium für Bildung verfasste „Empfehlung für die Basis IT Infrastrukturausstattung an österreichischen Schulen“[1] bietet eine Grundlage für Entscheidungen bezüglich der vorzusehenden Anschlüsse. Dieser Leitfaden soll zur Konkretisierung der Netzwerkinfrastruktur im Detail beitragen und den Entscheidungsträgern in Schulen dabei helfen, im komplexen IT-Umfeld fundierte Entscheidungen treffen zu können.

ZUSAMMENFASSUNG – WAS IST DAS ZIEL DIESES LEITFADENS?

Der Leitfaden „Netzwerkinfrastruktur in Österreichischen Schulen“ von Aruba dient als Referenzdokument für Entscheidungsträger und Planer im Bildungsumfeld. Die Empfehlungen und Produktvorschläge sind konkret auf das Umfeld österreichischer Schulen und Bildungseinrichtungen abgestimmt und wurden aus den Erkenntnissen einer großen Anzahl bereits umgesetzter Projekte gesammelt. Begleitet wird dieser Leitfaden von einer Initiative von Aruba, einem weltweiten Marktführer für LAN- und WLAN-Produkte. Dies ermöglicht es, qualitativ hochwertigste Produkte und führende technologische Funktionalitäten dem Schulsektor zu günstigen Konditionen zugänglich zu machen. Dadurch werden die Arbeitskräfte von morgen schon heute fit für ein digitales Arbeitsumfeld.

Nach dem Studium des Leitfadens sollen die Herausforderungen und Lösungen im Netzwerkumfeld auch für Laien verständlich sein. Er schafft eine Entscheidungsgrundlage für den verantwortungsvollen Umgang mit Budget und Ressourcen. Damit wird das Ziel des Bundesministeriums für Bildung erreicht: Den Zugang zu digitaler Bildung für jeden einzelnen Schüler zu ermöglichen.

HERAUSFORDERUNGEN IM UMFELD DER DIGITALISIERUNG VON SCHULEN

Während die Mehrheit der Lehrer sich darüber einig ist, dass eine Digitalisierung den Unterricht bereichert, stehen viele vor der Herausforderung, wie eine Umsetzung dieser machbar ist. Dabei spielen viele Themen eine Rolle:

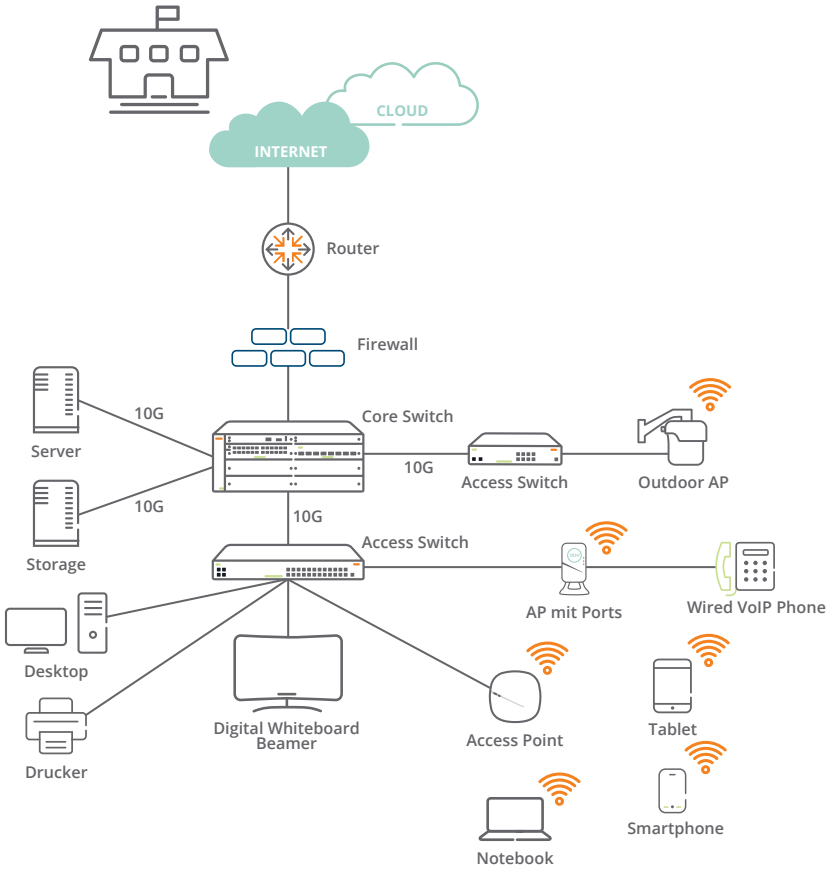
- Endgeräte für Lehrer und Schüler (Tablets, Notebooks, Smartphones, ...)
- Verwendung eigener Geräte durch Personal und Schüler (BYOD – Bring Your Own Device)
- Sicherheit im Netzwerk und Sicherheit der Daten vor Hackern
- Umsetzung und Einhaltung der Datenschutzgrundverordnung DSGVO
- Einbindung von elektronischen Tafeln, Beamern, Druckern, IP-Telefonen, Schließsystemen, Hausautomationssystemen, ... (IoT – Internet of Things)
- Begrenzte Bandbreiten ins Internet
- Begrenzte zeitliche Ressourcen und Know-How
- Budget für die Umsetzung

Aruba unterstützt Schulen und Lehrer mit ihren Produkten und Lösungen dabei, diese Hindernisse zu überwinden.

[1] https://bildung.bmbwf.gv.at/schulen/it/it_angebote/it_infrastruktur_empfehlung.pdf?6kdmfr Stand: 5.9.2019

BESTANDTEILE EINES MODERNEN NETZWERKS

Ein zeitgemäßes Netzwerk besteht üblicherweise aus folgenden Komponenten:



In Folge wird nun auf die einzelnen Komponenten eingegangen:

Router

Der Router wird zumeist vom jeweiligen Internet-Provider zu Verfügung gestellt und stellt die eigentliche Schnittstelle ins Internet oder zu anderen Netzwerken dar. Manche Router bieten neben der kabelgebundenen Leitung alternativ auch einen Uplink über UMTS oder LTE an, um im Fehlerfall eine Ersatzroute ins Internet aufbauen zu können.

Firewall

Die Firewall stellt eine wichtige Komponente dar, um die Sicherheit im Netzwerk zu gewährleisten. Man kann sie wie einen Filter sehen, den der ein- und ausgehende Datenverkehr passieren muss. Die Firewall erlaubt es, bestimmte Inhalte zu filtern – wenn diese z.B. aus dem Internet abgerufen werden. Aus der Grafik ist aber auch ersichtlich, dass Inhalte, die innerhalb des Netzwerkes ausgetauscht werden (also ohne den Weg zum Router zu passieren), diesen Beschränkungen nicht unterliegen. Daher stellt eine Firewall nur einen Teil der relevanten Maßnahmen zur Netzwerksicherheit dar.

Core Switch

Dieser stellt das „Herz" des Netzwerks dar, in dem alle Verbindungen zusammengeführt werden. Man spricht bei der Verbindung vom Core-Switch zum Router vom sogenannten „Uplink", während die Verbindungen zu den Verteilerswitches (Access Switches) als „Downlinks" bezeichnet werden.

Eine weitere Aufgabe des Core-Switches ist die zentrale Anbindung von lokalen Ressourcen wie Servern und Netzwerkspeichern. Meist befinden sich diese gemeinsam mit dem Core-Switch in einem gemeinsamen Serverraum.

Für eine zukunftssichere Installation sollten die Verbindungen zwischen Core-Switch und Access Switches Bandbreiten von 10 Gigabit/Sekunde unterstützen. Im Idealfall werden diese Verbindungen mit Glasfaserleitungen ausgeführt, da diese auch für zukünftige Technologien noch viel Spielraum betreffend der Bandbreite haben. Es wird zwischen Multimode-Leitungen für kürzere Verbindungslängen und Singlemode-Leitungen für längere Strecken unterschieden. Üblicherweise sind für Schulen Multimode-Verkabelungen nach dem OM3 oder OM4-Standard eine gute Wahl, wobei auch hier Singlemode mehr Kapazitäten für spätere Entwicklungen hat. Bei der Verbindung von unterschiedlichen Gebäuden bieten Glasfaserleitungen auch den Vorteil einer elektrischen Potentialtrennung. (Schutz bei Blitzschlägen, unterschiedliches Erdungspotential, ...)

Für sehr kurze Strecken innerhalb eines Raumes (<7 m) können alternativ zur Glasfaser auch günstigere so genannte DAC (Direct Attach Cable) eingesetzt werden. Eine weitere Möglichkeit bieten 10G Kupferverbindungen (10GBASE-T), bei denen jedoch die maximale Länge sowie die Verfügbarkeit von unterstützten Produkten eingeschränkt ist. Derartige Lösungen können vor allem zur Anbindung der Server und Storagesysteme Kosteneinsparungen bringen.

In kleineren Installationen mit limitierter Anzahl an Endgeräten und maximal 100 m Leitungslänge kann eventuell auf den Core-Switch verzichtet werden. Typischerweise trifft dies auf allgemein bildende Pflichtschulen (österreichweit durchschnittlich 7 Klassen je Schule) zu.

Access Switch

Über die Access Switches werden alle Endgeräte (PCs, Drucker, Beamer, elektronische Tafeln, IoT-Geräte, ...) sowie Access Points angeschlossen. Üblicherweise gibt es Access Switches in Ausführungen von 8 Ports bis maximal 48 Ports. Werden mehr als 48 Ports an einem Standort benötigt, besteht die Möglichkeit des „Stackings", bei dem mehrere Switches untereinander verbunden werden und nach außen hin wie ein einziger Switch wirken.

Um den heutigen Anforderungen gerecht zu werden, sollten die Ports alle eine Bandbreite von 1 Gigabit/Sekunde bieten (1000BASE-T). Alleine aus der Summe der dadurch möglichen Datenraten ergibt sich die Sinnhaftigkeit der 10 Gigabit-Leitungen für den Uplink zum Core-Switch. Diese sollten je Switch zumindest mit 2 Stück 10G-Ports, im Idealfall mit 4 Ports ausgeführt sein. Die 10G-Ports sind mit SFP+ Käfigen ausgestattet, in die dann entweder Multimode- oder Singlemode-Transceiver oder DAC eingesteckt werden. Der Transceiver (für 10G auch SFP+ genannt) stellt dann die Verbindung zu den Glasfaser-Kabeln her, die mit optischen LC-Duplex-Steckern ausgestattet sind.

LC Duplex Stecker Multimode

SFP+ Transceiver für 10G Glasfaserverbindungen

Power over Ethernet (PoE) 802.3af/at/bt hat sich als Technologie durchgesetzt, um Netzwerkgeräte über den Switch auch gleich mit Strom zu versorgen. So spart man sich die zusätzliche Installation einer Steckdose in unmittelbarer Nähe von Geräten wie z.B. Access-Points, VoIP-Telefonen oder Sicherheitskameras. Ein weiterer Vorteil ist, dass die Stromversorgung dieser Geräte somit über den Switch von einem zentralen Punkt (auch remote) ein- bzw. ausgeschaltet werden kann. Gerade bei Access-Points, die durch ihre erhöhte Montageposition oft schwerer zugänglich sind, kann dies von Vorteil sein.

Bei der Verwendung von PoE gibt es mehrere Leistungsklassen der Endgeräte, die bei der Wahl der Switches berücksichtigt werden müssen. Heute ist PoE Plus (802.3at, maximal 30 Watt) üblich und reicht für die meisten Geräte aus. 802.3bt ermöglicht sogar bis zu 60 Watt per Port, was den Betrieb von sehr leistungsstarken Access Points und sogar LED-Beleuchtung erlaubt.

Außerdem bietet jeder Switch ein begrenztes Power-Budget, welches zumindest der Summe der Leistungen der versorgten Geräte entsprechen muss. So muss die Leistung eines Access Points mit der Anzahl der am Switch angeschlossenen Access Points multipliziert werden, um den Gesamtbedarf abzuklären.

Bei diesen Planungen ist Voraussetzung, dass am Standort der Switches auch eine ausreichend starke Stromversorgung dimensioniert wurde. Sollte dies (z.B. in älteren Gebäuden) nicht der Fall sein, stellt die Verwendung von PoE-Injektoren oder lokalen externen Netzgeräten eine Alternative dar. Dazu sollten gegebenenfalls in unmittelbarer Nähe der Access-Points Steckdosen vorgesehen werden.

Lüfterlose Switches sollten vor allem in Betracht gezogen werden, wenn diese in einem Raum eingesetzt werden, in dem sich Personen länger aufhalten. Die stetige Geräuschbelastung durch Lüfter kann sonst als störend empfunden werden.

Bei allen Geräten muss eine ausreichende Wärmeabfuhr gewährleistet sein – entweder durch klimatisierte Bereiche oder ausreichende Luftzufuhr. Es sollte berücksichtigt werden, dass es in Netzwerkschränken zu keinem „Lüftungskurzschluss" kommt – wenn die Ventilatoren der Geräte in gegengleiche Richtungen blasen und so die warme Abluft der anderen Geräte ansaugen.

WLAN Access Points

Für einen reibungslosen digitalen Unterricht ist eine flächendeckende WLAN-Infrastruktur in den Lehrbereichen unverzichtbar. Um diese zu gewährleisten, empfiehlt sich eine professionelle Begutachtung der baulichen Situation,

im Idealfall mit entsprechenden Testaufbauten und Messgeräten. Man spricht von einer „WLAN-Ausleuchtung" des Gebäudes, diese wird von professionellen Unternehmen angeboten.

Grundsätzlich hat sich aus Erfahrungswerten ergeben, dass im Idealfall je Klassenraum ein Access Point installiert wird. Für Lehrerzimmern und Büros gibt es eigene Modelle, die neben der Ausstrahlung des WLAN-Signals zusätzliche Netzwerk-Ports aufweisen, die eine PoE-Weiterleitung und somit den Anschluss von zusätzlichen Geräten wie VoIP-Telefonen, Druckern und PCs erlauben. Für Veranstaltungsräume (Aula, Turnsaal, Festsaal, ...) empfiehlt es sich, leistungsstarke Access Points einzusetzen, da hier gegebenenfalls die Dichte der Endgeräte (z.B. Smartphones bei Veranstaltungen) sehr hoch sein kann. Zur besseren Anpassung der Abdeckung können auch Modelle mit verstellbaren externen Antennen im Einzelfall von Vorteil sein.

Wenn auch im Außenbereich (Schulhof, Sportplatz, ...) WLAN angeboten werden soll, gibt es eigene Outdoor Access Points. Qualitativ hochwertige Modelle können ohne zusätzlichen Schutz den tiefsten Temperaturen im Winter sowie der prallen Sonne im Sommer ausgesetzt werden, ohne Leistungseinbußen aufzuweisen. Eine professionelle Möglichkeit eines eventuell notwendigen Blitzschutzes (von Montagesituation und Leitungslängen abhängig) muss gegeben sein.

Bei der Wahl der Access Points sollte auch gleich die Montagemöglichkeit mit beachtet werden. Abhängig vom Ort der Installation kann dies als Deckenmontage (eventuell mit Montagekit für abgehängte Decken), Wandmontage oder Mastmontage erfolgen. Sind die Access Points für Schüler physisch zugänglich, ist auch eine sichere Anbringung anzudenken, die eine Demontage nur mit Spezialwerkzeug oder Schlüssel ermöglicht.

Namhafte Hersteller decken mit ihrem Portfolio alle angeführten Produkte ab, um ein einheitliches Management aus einem Guss zu gewährleisten.

WLAN STANDARDS

Seit den ersten WLAN-Installationen in den späten 1990er Jahren wurden bereits mehrere Standards definiert, die unter der Bezeichnung 802.11 in verschiedenen Ausprägungen zu finden sind. Da die Nomenklatur mit a/b/g/n/ac/ax usw. für Laien sehr kryptisch ist, wurde im Oktober 2018 eine vereinfachte Benennung beschlossen.

Wi-Fi 5 - 802.11ac

Dieser seit 2014 veröffentlichte Standard hat viele Vorteile und Leistungsverbesserungen gebracht und sollte den Mindeststandard bei WLAN-Netzen darstellen. Die Ausrollung erfolgte in zwei Wellen, wobei in Schulen eingesetzte Access Points zumindest „ac Wave 2" unterstützen sollten. Frühere Standards (Wi-Fi 1-4, 802.11a/b/g/n/ac Wave 1) sollten für Installationen nicht mehr in Betracht gezogen werden, da sie sowohl betreffend der Übertragungsbandbreite als auch bezüglich Sicherheit veraltet sind.

Wi-Fi 6 – 802.11ax

Dieser zuletzt vorgestellte Standard bringt viele weitere technologische Verbesserungen und Vorteile gegenüber Wi-Fi 5, die neben höheren Bandbreiten vor allem eine größere Nutzerdichte ermöglichen. Um alle Vorteile nutzen zu können, ist es essentiell, dass die Access Points die aktuellsten Chipsets verbaut haben. Einige Hersteller haben vor der Ratifizierung des Standards erste Produkte auf den Markt gebracht, die nicht alle Funktionen unterstützen. Da derzeit sehr wenige Endgeräte (Handys, Tablets, Notebooks) erhältlich sind, die Wi-Fi 6 implementiert haben, ist der Mehrwert für Schulen momentan noch eingeschränkt. Da auch bereits 802.11ac Wave 2 Bandbreiten von weit über 1 Gigabit unterstützt, liegt derzeit der Flaschenhals meist nicht im WLAN, sondern in der Anbindung der Access Points. Lässt der finanzielle Rahmen einer Schule die Anschaffung von Wi-Fi 6 Access Points zu, sind diese im Sinne des Investitionsschutzes natürlich sinnvoll.

Um eine zukunftsorientierte Installation zu gewährleisten, empfiehlt es sich, dass der gewählte WLAN-Hersteller alle bisher angeführten Technologien und Access Points auch im Mischbetrieb unterstützt. So ist später ein schrittweiser Upgrade möglich, und es muss nicht das gesamte Netz auf einmal getauscht werden, wenn ein Technologiewechsel ansteht.

Antennenanzahl in Access Points

Neben dem implementierten WLAN-Standard spielt die Anzahl der Antennen sowie der gleichzeitigen parallelen Funkverbindungen eine wichtige Rolle bei der Performance der Access Points. Modelle mit 2 Sendeantennen sowie 2 Empfangsantennen und 2 Streams (2x2:2) sind üblicherweise für Klassenräume ausreichend. Für Bereiche mit hoher Nutzerdichte, oder wo besonders hohe Performance benötigt wird, empfehlen sich Modelle mit 4x4:4 Ausstattung.

WLAN FUNKTIONEN

Den größten Unterschied im reibungslosen Betrieb von WLAN-Netzen machen die von den Herstellern implementierten Funktionen.

Dual Radio

Durch die sehr begrenzt verfügbaren Funkkanäle im 2,4 GHz Frequenzbereich (von den 13 Kanälen können nur 3 überlappungsfrei verwendet werden), sowie der Störanfälligkeit durch z.B. Mikrowellenherde etc. sollte simultan das 5 GHz Funkmodul genutzt werden können. Dieses ermöglicht auch größere Bandbreiten und eine bessere Verteilung der Endgeräte.

Kanal- und Sendeleistungseinstellung

Erfahrene WLAN-Planer können bei der ersten Inbetriebnahme die Kanäle und Sendeleistungen der Access Points vergeben, um eine gegenseitige Interferenz zu vermeiden. Damit kann aber nicht auf sich verändernde Umstände eingegangen werden. Noch praktischer ist daher eine dynamische, automatisch koordinierte Anpassung dieser Parameter durch die Intelligenz in der Steuerung des Netzwerks. Es ist wichtig, zu verstehen, dass es kontraproduktiv ist, die Leistung aller Access Points auf das Maximum einzustellen. Dies führt dazu, dass sich die Access Points gegenseitig stören und Frequenzen unnötig belegt werden. Daher ist die oft gestellte Frage nach der maximalen Leistung der Access Points zumeist nicht relevant (diese ist gesetzlich begrenzt), sondern die Möglichkeiten zur Optimierung der Sendeleistung in Abstimmung des gesamten Netzwerks. Aruba bietet zudem einen „Green-AP" Modus, der bei geringer Auslastung redundante Access-Points in einen Stromsparmodus versetzt.

Roaming zwischen Access Points

Aus dem Mobilfunk sind wir gewohnt, dass unsere Telefonate automatisch an die nächste Basisstation weitergegeben werden, wenn wir uns fortbewegen. Leider ist diese Funktionalität im WLAN-Standard nicht verankert. Dort verhält es sich standardmäßig so, dass ein Nutzer so lange mit dem ersten Access Point verbunden bleibt, bis sich die Signalstärke so weit senkt, dass es zu einem Abbruch der Verbindung kommt und ein neuer Access Point gesucht wird. Dies führt nicht nur bei diesem Nutzer zu schlechter Performance, sondern beeinflusst auch alle anderen Nutzer, die mit diesem Access Point verbunden sind. Diese so genannte „Sticky Client" - Problematik kann in vielen Netzwerken gut beobachtet werden, da die meisten Nutzer mit dem ersten Access Point verbunden bleiben, der sich z.B. im Eingangsbereich des Gebäudes befindet.

Aufbauend auf die zentralisierte Abstimmung der Access Points untereinander hat Aruba die patentierte ClientMatch - Funktionalität im Einsatz. Das Netzwerk beobachtet und bewertet die möglichen Verbindungen zu anderen Access Points und steuert von sich aus eine Übergabe des Nutzers. Bei dieser intelligenten Funktionalität wird nicht nur die Funkleistung in Betracht gezogen, es wird auch die Auslastung der Access Points und der verfügbare WLAN-Standard am Endgerät mit einbezogen. Somit erzielt ClientMatch die bestmögliche Netzwerkperformance für alle Teilnehmer. Es ist keine Installation von Software auf den Endgeräten erforderlich.

Erkennung und Klassifizierung von Inhalten

Während Firewalls vor schädlichen Inhalten schützen können, die von extern (aus dem Internet) kommen, benötigt es innerhalb des Netzwerkes anderer Mechanismen. Durch Technologien wie „Deep Packet Inspection", wo in den Datenverkehr hinein gesehen wird, kann Aruba AppRF den Datenverkehr von über 2800 Programmen bzw. Apps erkennen. Diese Zahl erhöht sich laufend. Sind bestimmte Apps in Verwendung, die noch nicht automatisch erkannt werden, können diese manuell hinzugefügt werden. Die leistungsstarken Prozessoren in den Access Points ermöglichen somit

- Priorisierung von Apps (z.B. Kommunikation via Skype, Unterrichtsapps, ...)
- Limitierung der Bandbreiten oder Sperre für Apps (z.B. Youtube, Facebook, ...)
- Unterschiedliche Einstellungen für Schüler vs. Lehrer möglich
- Optionale Firewall-Funktionalität mit Applikationserkennung und Inhaltsklassifizierung
- Blockieren bzw. Filtern von Verkehr (anstößige Inhalte, Rechtsextremismus, ...)

Einfache Installation

Durch den Mangel an qualifizierten IT-Fachkräften in Schulen sind eine einfache Installation und Wartung sehr wertvoll. Daher ist es wünschenswert, dass Netzwerkelemente „Zero Touch Provisioning" unterstützen. Das bedeutet, dass neue Access Points dem Netzwerk einfach hinzugefügt werden können bzw. im Fall eines Tausches dieser ohne aufwändige Installationsroutinen erfolgen kann.

Meshing und Serienschaltung von Access Points

Ist eine Anbindung eines Access Points mittels Ethernet-Kabel nicht möglich, besteht die Möglichkeit des „Meshings". Dabei werden Access Points untereinander über das 5 GHz Funkmodul miteinander verbunden, um den Datenverkehr der Nutzer so ins Netzwerk zu übertragen.

Sollte aus besonderen Gründen eine „Serienschaltung" von Access Points erwünscht sein (ein Ethernet Kabel geht zum ersten Access Point, von dort geht ein Kabel weiter zum nächsten), hat Aruba auch Sondermodelle. Dies spart Ports am Switch und Verkabelung.

Wenn möglich sollte jedoch immer eine eigene Leitung zu jedem Access Point verlegt werden, da Meshing und Serienschaltung die gesamt zu Verfügung stehende Bandbreite für User deutlich reduziert und Frequenzen für das Meshing belegt werden, die dann nicht für den User-Zugriff zu Verfügung stehen.

Für die besondere Herausforderung, geographisch abgesetzte Gebäude mit dem Schulnetz zu verbinden, ermöglichen spezielle Funk-Brücken wie der Aruba AP-387 Distanzen von bis zu 400 Metern mit einer Übertragungsrate von bis zu 3,37 Gigabit pro Sekunde zu überbrücken. Die automatische Ausrichtung der Antennen ermöglicht es, diese Richtfunkstrecke sehr einfach in Betrieb zu nehmen. Als Bestandteil des WLAN-Konzepts fügt sich diese Lösung – anders als herkömmliche Richtfunk-Strecken - nahtlos in das Gesamtportfolio ein.

Zusatzfunktionen

Moderne Access Points beschränken sich nicht nur auf WLAN, sondern unterstützen in vielen Fällen auch Bluetooth, ZigBee und zukünftig weitere Standards, die in der Steuerung von Lichtsystemen (Stichwort Smart Buildings) etc. eingesetzt werden. Auch wenn diese derzeit vielleicht nicht genutzt werden, sollte im Sinne der Zukunftssicherheit in die Überlegungen einbezogen werden, dass damit z.B. Asset-Tracking (Auffinden von Gegenständen wie mobilen Beamern im Gebäude, Warnung beim Verlassen des Gebäudes, ...), Indoor-Navigation, Steuerung von Schließsystemen etc. realisiert werden können.

Qualität - Limited Lifetime Warranty

Ein wichtiger Faktor in der Differenzierung von Netzwerkequipment ist die Qualität der Hardware und Software. Namhafte Hersteller bieten daher eine „Limited Lifetime Warranty" an. Das bedeutet, dass ein Austausch der Hardware bei unverschuldetem Defekt kostenlos stattfindet, nicht nur während des Gewährleistungszeitraumes von 12 Monaten im B2B-Bereich. Dies entspricht einer Investitionssicherung, die besonders für Schulen wichtig ist, da die Investitionszyklen meist länger sind als in anderen Branchen.

Die Limitierung der lebenslangen Garantie bezieht sich vorrangig darauf, dass diese für den ersten Endkunden gilt – daher ist es wichtig, bei autorisierten Partnern zu kaufen, welche die Schule dem Hersteller gegenüber als Endkunden anführen.

Unterstützung bei Fragen - Support

Auch in diesem Punkt trennt sich die Spreu vom Weizen. Eine Schule sollte sich eine Supportorganisation des Herstellers im eigenen Land erwarten, zusätzlich leisten Foren und das Know-How des installierenden Unternehmens einen wichtigen Beitrag.

Aruba bietet all das, mit einer über 80.000 Teilnehmer umfassenden Airheads-Community, die neben den Online-Veranstaltungen auch regelmäßige kostenlose Airheads-Meetings in Österreich veranstaltet.

WLAN-ARCHITEKTUR

Netzwerktechnik-Hersteller bieten unterschiedliche Konzepte für die Architektur und Verwaltung der Access Points an. Jedes der Konzepte hat Vorteile und Nachteile – daher ist es wichtig, dass alle Access Points des Herstellers flexibel eingesetzt werden können und die verschiedenen Konzepte unterstützen. Sonst führt eine spätere Anpassung bei Änderung der Bedürfnisse dazu, dass die gesamte Hardware getauscht werden muss – ein teures Unterfangen.

„Als eines der größten Gymnasien Österreichs hatten wir eine sehr diverse gewachsene Infrastruktur. Durch konsequente Planung und der Reduktion auf, im Wesentlichen, einen Hersteller, konnten wir nicht nur die Zuverlässigkeit im kabelgebundenen Netzwerk, sondern erstmals ein tatsächlich funktionierendes WLAN anbieten. In Zeiten, in denen Sicherheit in Netzwerken eine immer größere Rolle spielt, war die zusätzlich integrierte Firewall in den AccessPoints ein weiteres Kaufkriterium."

Thomas Baldauf
IT Manager GRG 21 Ödenburger Straße, Wien

Aruba Instant

Für kleinere Installationen bis 128 Access Points und maximal 2048 Endgeräte eignet sich Aruba Instant. Bei dieser Architekturvariante übernimmt der erste in Betrieb genommene Access Point die Rolle eines virtuellen Masters. Er koordiniert die Leistungs- und Kanalanpassung, steuert das automatische Roaming und ermöglicht die reibungslose Installation. Ist dieser Access Point mit den gewünschten Einstellungen in Betrieb genommen, fügen sich die weiteren Access Points, die an die gleichen Switches (Layer 2) angeschlossen werden, automatisch in den gleichen Cluster hinzu und übernehmen alle Einstellungen. Sollte der Master ausfallen übernimmt einer der verbleibenden Access Points diese Rolle.

Controllerbasierende Lösung

Für größere Netzwerke oder bei besonderen Anforderungen empfiehlt sich der Einsatz eines Hardware-Controllers. Dieser wird an den Core-Switch angeschlossen und kommuniziert mit allen Access Points, um die optimale Performance im Netzwerk zu gewährleisten. Zusätzlich ermöglicht der Einsatz eines Controllers auch die Verwendung von „Remote Access Points“. Diese können an einem beliebigen Ort mit Internetanbindung in Betrieb genommen werden (Home Office, Hotel, ...), bauen einen Tunnel zum Controller auf und stellen dann vor Ort exakt das gleiche Netzwerk mit allen Zugängen zu Verfügung, wie wenn man sich in der Schule befinden würde.

Eine Alternative zum Hardware-Controller bietet der Virtuelle Controller, der auf virtuellen Maschinen installiert werden kann.

Cloud-Management

Für verteilte Netzwerke oder schulübergreifendes Management bietet sich Aruba Central an. Hier sitzt das Management in der Cloud und kann von überall aus über einen gewöhnlichen Browser konfiguriert werden. So kann ein Systembetreuer mehrere Standorte oder Schulen verwalten, ohne physisch vor Ort sein zu müssen. Es werden nur die Managementdaten an ein hochsicheres Datacenter innerhalb der EU übertragen, weshalb diese Lösung auch vollkommen DSGVO-konform ist. Der Zugang zu den verwalteten Schulen lässt sich granular zuweisen. Änderungen können pro Access Point, pro Standort oder für multiple Standorte gleichzeitig vorgenommen werden.

Sollte es zu einem Ausfall der Internetanbindung bei der Schule kommen und somit keine Kommunikation zum zentralen Cloud-Management mehr möglich sein, wechselt das Netzwerk bis zur Wiederherstellung automatisch auf den Instant-Modus. Somit ist der weitere Betrieb in der Schule mit Zugriff auf alle lokalen Ressourcen vollständig gewährleistet.

NETZWERKMANAGEMENT UND MONITORING

Das Management von Netzwerken kann aufwändig sein und viel Zeit in Anspruch nehmen. Daher ist es für Netzwerkadministratoren wünschenswert, wenn damit möglichst wenig Aufwand verbunden ist und Änderungen so selten wir möglich vorgenommen werden müssen. Außerdem hilft ein gemeinsames Management von LAN und WLAN bei der raschen Aufdeckung von Problemen und einem raschen Überblick zur Gesundheit des Netzwerkes. Im Idealfall lassen sich auch Dritthersteller integrieren, um bestehende Infrastrukturen mit einbinden zu können und für die Zukunft offen zu sein.

Aruba bietet hier wieder unterschiedliche Modelle, um den individuellen Bedürfnissen von Schulen gerecht werden zu können.

Aruba AirWave

In Kombination mit Instant oder Controllern hat sich für Schulen AirWave bewährt. Dieses unterstützt neben den Aruba Switches und Access Points auch Produkte anderer Hersteller und ermöglicht einen Gesamtüberblick des Netzwerks in Echtzeit. Die grafische Aufbereitung der Monitoring-Ergebnisse mit der Möglichkeit, die Details aufzurufen, ermöglicht eine einfache und rasche Auffindung von Ursachen für Userprobleme.

Weitere Funktionalitäten beinhalten das Erkennen und Auffinden von unerwünschten externen Access Points, die Erkennung von diversen Angriffsmethoden auf WLANs sowie die Darstellung der Ergebnisse in einem Gebäudeplan.

Neben individuell konfigurierbarer automatischer Alarmierung bei Bedrohungen oder Fehlern im Netzwerk inkludiert AirWave eine Vielzahl verschiedener vordefinierte Report. Diese können angepasst und kombiniert werden, um in regelmäßigen Abständen über die Netzwerkdetails zu informieren.

Cloud Management

Wie bereits im Abschnitt der WLAN-Architektur angeführt ist Aruba Central die Lösung für schulübergreifende Anwendungen. Zusätzlich zur Konfiguration von Switches und Access Points ist auch ein Monitoring mit vergleichbaren Funktionen und Reports wie bei AirWave vorhanden.

Die volle Funktionalität im Browser wird ergänzt durch Apps für Android und iOS, die auch am Handy den sofortigen Überblick bieten. Es werden laufend weitere Funktionalitäten hinzugefügt, um das Leben des Netzwerkadministrators so einfach wie möglich zu machen.

SICHERHEIT IM NETZWERK

Die Sicherheit in Netzwerken lässt sich unter mehreren Aspekten betrachten.

Zugangskontrolle (Network Access Control)

War es früher üblich, die unterschiedlichen Zugriffsrechte über unterschiedliche Ports am Switch zu managen, wird heute eine rollenbasierende Rechteverwaltung präferiert. Dadurch wird jedem Nutzer dynamisch seine individuelle Rolle zugeordnet und dann die entsprechenden Ressourcen freigegeben. Wird ein Nutzer nicht im vordefinierten Verzeichnis gefunden oder schlägt die Anmeldung fehl, kann diesem ein Gastzugang zugewiesen werden oder er wird vollständig aus dem Netzwerk gesperrt.

Diese rollenbasierende Rechtezuweisung ist besonders durch die immer breitere Verwendung von „IoT"-Geräten relevant. Dabei handelt es sich um alle Geräte wie IP-Kameras, Sprachassistenten wie Amazon Alexa oder sogar Kaffeemaschinen und Kühlschränke. Intelligentes Fingerprinting zur Erkennung derartiger Geräte und Zuweisung der richtigen Netzwerkrechte schützt vor unberechtigten Zugriffen und vor Angriffen von Hackern.

Ein weiterer Vorteil ist, dass nicht für jede Usergruppe (Lehrer, Schüler, Administration) ein eigener Netzwerkname ausgestrahlt werden muss. Alle können sich mit dem allgemeinen Schul-WLAN verbinden und erhalten ihre individuellen Zugangsrechte.

Gästenetzwerk

Die Einrichtung eines Gästenetzwerks kann in Schulen sinnvoll sein, um Vertretungslehrern, Schülern, Eltern, Gästen oder anderen schulexternen Personen die Möglichkeit zu geben, das Internet über WLAN zu nutzen. Die Möglichkeiten der Zugangsgenehmigung reichen von einem Zugang ohne Passwort, einfacher Selbstregistrierung über „Sponsored" Zugänge (Der Zugang wird von einer definierten schulinternen Person freigegeben) bis hin zu zeitlich eingeschränkten Zugängen mit Username und Passwort.

Integrität der Access Points

Jedes Aruba Gerät wie z.B. Controller oder Access Point besitzt ein sogenanntes "Trusted Platform Modul (TPM)". Dieses TPM Modul ermöglicht es sicherzustellen, dass der Access Point weder gefälscht noch geklont wurde. Die Vertrauenswürdigkeit des Access Points wird somit garantiert. Passwörter und Zugangsdaten können aus den Geräten nicht ausgelesen werden, was zusätzliche Sicherheit bietet.

WLAN Verschlüsselung

Im Laufe der Jahre wurden verschiedene Verschlüsselungs- und Authentifizierungsverfahren entwickelt. Während WEP, WPA, WPA2 und WPS noch oft im Einsatz sind, gelten diese als unsicher und veraltet. Daher sollten Access-Points den aktuellen WPA3 Standard erfüllen, aber trotzdem abwärtskompatibel zu WPA2 sein, um auch ältere Geräte zu unterstützen.

Ausfallssicherheit und Redundanz

Auch wenn in Schulen ein kurzfristiger Netzwerkausfall üblicherweise keine schwerwiegenden Folgen nach sich zieht, sollte besonders in Anbetracht von Prüfungssituationen oder der Matura auf Computern die Ausfallssicherheit betrachtet werden.

Um eine möglichst hohe Verfügbarkeit des Netzwerks zu gewährleisten, empfiehlt es sich, den Core-Switch redundant auszuführen. Das bedeutet, dass alle Access-Switches, sowie andere Ressourcen wie Server und Storage, mit mindestens je einer Leitung an beide Core-Switches angeschlossen werden. Sinnvoll ist – so verfügbar – die beiden Core-Switches über unabhängige Stromkreise zu versorgen, sowie jeweils mindestens 2 redundante Netzteile pro Switch zu verwenden. Dies erlaubt bei einem Ausfall eines Core-Switches einen ungestörten Netzwerkbetrieb.

„An der digBiz HAK Imst betreiben wir seit 2018 ein feinmaschiges und flächendeckendes Campus-WLAN mit Aruba AP-303 bzw. AP-345 Access Points. Die Aruba-Lösung läuft äußert stabil und ist komfortabel einzurichten bzw. zu betreiben. Die APs können ohne dedizierte Controller-Hardware oder Cloud-Anbindung zentral verwaltet werden. Neue SSIDs (Gast, Schüler, Lehrer, Lab etc.) mit den verschiedensten Konfigurationen und Berechtigungen (Stichwort BYOD-Konzepte) sind schnell eingerichtet. Durch die Radius-Anbindung können sich unsere Benutzer mit ihren gewohnten AD-Credentials im WLAN authentifizieren. Die mächtigen Firewall-Features blockieren unerwünschten Datenverkehr bereits am AP und entlasten so das LAN bzw. die Internetbandbreite. Zusammen mit den äußerst effektiven Möglichkeiten der Bandbreitenoptimierung und dem perfekten Roaming-Verhalten können wir jedem Benutzer an unserer Schule ein ausgezeichnetes WLAN- bzw. Surf-Erlebnis bieten."

Mag. Dr. Claudio Landerer, Bakk.
digBiz HAK Imst

Für das WLAN ist eine Überlappung der Abdeckungsbereiche zumeist gegeben, wenn je Klasse ein Access-Point verwendet wird. Dadurch kann die Infrastruktur der benachbarten Klassen bis zum Tausch eines defekten Access-Points den Verkehr übernehmen. Diese Überlappung ermöglicht auch ein erfolgreiches lückenloses Roaming, wenn sich der User im Gebäude bewegt.

Bei besonderen Anforderungen können detailliertere Redundanzkonzepte erarbeitet werden.

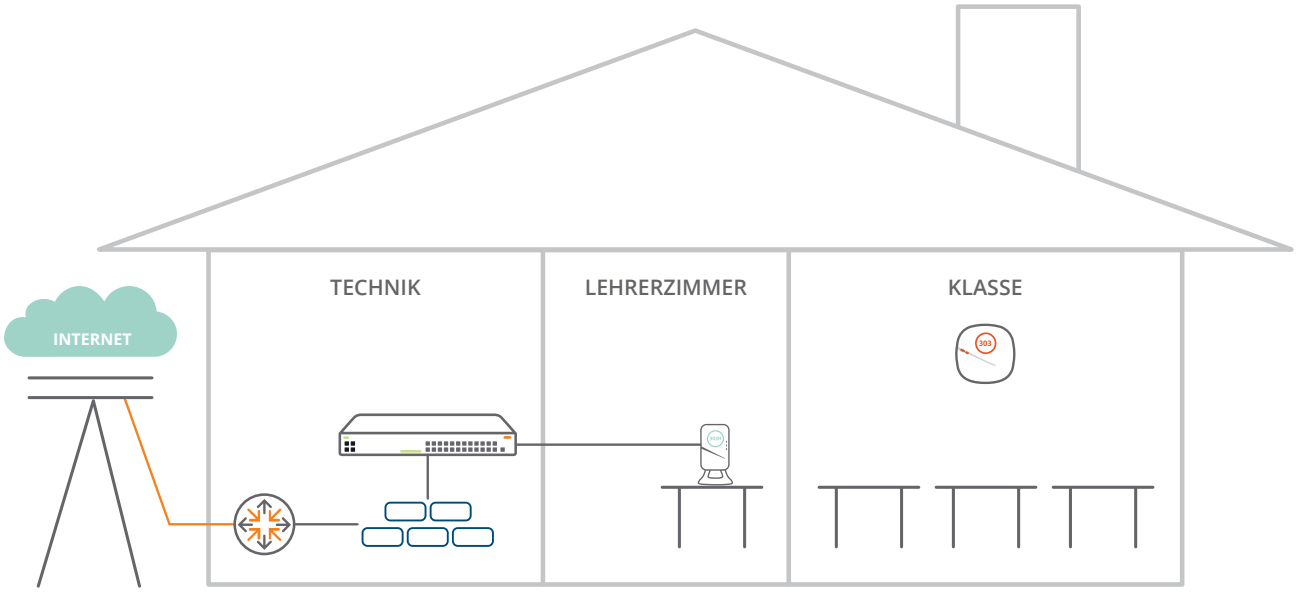
LÖSUNGEN FÜR KLEINE SCHULEN

Der Großteil der ca. 5700 Schulen in Österreich beherbergt weniger als 10 Klassen. Insbesondere Volksschulen haben oft keinen Bedarf an komplexer Netzwerkinfrastruktur mit Core-Switch und Verteilerswitches. Zudem sind die Anforderungen an diesen Schulen recht statisch und Netzwerke sollten aufgrund der begrenzten Ressourcen an IT-Know-How möglichst ohne regelmäßige Wartung funktionieren. Lange Garantiezeiten sorgen für geringes Investitionsrisiko bei gleichzeitiger Sicherheit.

Je nach Bedarf sollten in kleinen Schulen Switches mit 24 oder 48 Gigbit-Ports gewählt werden, die PoE unterstützen. Für das WLAN empfiehlt sich eine Architektur ohne Hardware-Controller.

Aruba bietet in diesem Umfeld mit der 2530 Switch Serie kostengünstige Einstiegsmodelle mit 8, 24 oder 48 Ports. Alternativ können der 2930F und 2930M in Betracht gezogen werden, wenn z.B. höhere PoE-Leistung erforderlich ist oder eine redundante Stromversorgung erwünscht wird.

Für WLAN empfiehlt sich der AP-303 für Klassenräume, in Lehrerzimmern der AP-303H, der gleichzeitig den Anschluss von bis zu 3 Geräten an die integrierten Ethernet-Ports erlaubt. Sollten Räumlichkeiten für Veranstaltungen mit mehr als 50 gleichzeitigen aktiven Nutzern verwendet werden empfiehlt sich das High-End Modell AP-345.

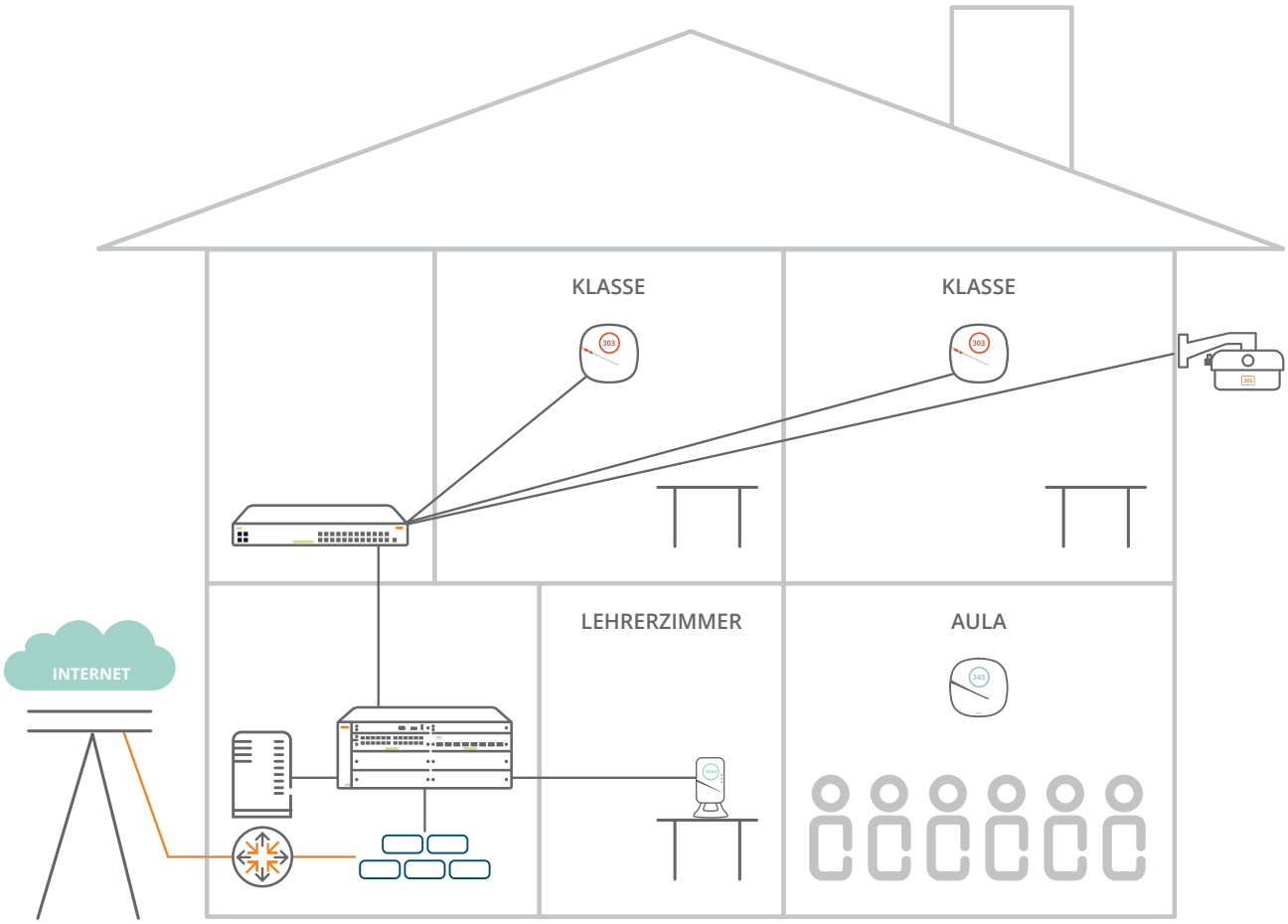


LÖSUNGEN FÜR GROSSE SCHULEN

Für große Installationen mit 70+ Access-Points können entweder mehrere Instant-Cluster oder eine Variante mit Controllern in Betracht gezogen werden. Als Core-Switch bietet die 54XX-Serie (redundant ausgeführt) durch die Modularität eine zukunftssichere Flexibilität. Die Access-Switches sollten entsprechend der Anforderungen an PoE-Leistung und eventueller Routing-Funktionalitäten getroffen werden. Die Serien 2540, 2930F, 2930M und 3810M bieten eine Vielzahl an Möglichkeiten, um die individuellen Bedürfnisse abzudecken.

Durch die homogene Kompatibilität der Access Points kann aus dem breiten Portfolio von Aruba gewählt werden. Bewährt haben sich die Modelle

- AP-303 für Klassenräume
- AP-345 für Bereiche mit hoher Userdichte (Aula, Veranstaltungsräume etc.)
- AP-303H mit Kupferports für Lehrerzimmer
- AP-360 Serie für Outdoor-Bereiche



LÖSUNG CAMPUS MEHRERE SCHULEN (ARUBA CENTRAL)

Für Schulen oder übergeordneten Organisationen mit mehreren räumlich verteilten Standorten stellt sich die besondere Herausforderung, das Netzwerk trotzdem mit wenig Aufwand zu managen. Muss bei vielen klassischen Ansätzen der Netzwerkadministrator entweder persönlich vor Ort sein oder sich auf unterschiedliche Arten einwählen, gibt es mit Aruba Central eine komfortable und sichere Lösung. Mit der Anmeldung im Browser über die Cloud sieht der Administrator alle Standorte, kann Änderungen bequem für einzelne oder gleichzeitig mehrere Standorte durchführen und erkennt Situationen, die ein Eingreifen erfordern auf einen Blick.

Dabei steht der störungsfreie Betrieb wieder an höchster Stelle – selbst bei einem Ausfall der Internetverbindung steht das lokale Netzwerk vollständig zu Verfügung und kann vor Ort gemanagt werden.

FÜR DIE BILDUNGSDIREKTION (EHEMALS LANDESSCHULRAT)

Die Bildungsdirektionen der Bundesländer sehen das IT-Management an den Schulen als wichtigen Bestandteil ihrer Aufgabe. Je nach Bundesland wird die Betreuung der Schulen unterschiedlich umgesetzt, es hat sich jedoch herausgestellt, dass eine schulübergreifende Betreuung der Netzwerke zu einer Effizienzsteigerung führt. Daher sind zumeist Organisationsstrukturen geschaffen, die mehrere Schulen betreuen.

Für diese Struktur bildet Aruba Central eine ideale Lösung, um kosteneffizient einen hohen Grad an Dienstleistung erfüllen zu können. Das Management der Netzwerke kann einerseits von den Schulen selbst, andererseits aber zentral von den betreuenden Organisationen durchgeführt werden. Aufgrund des zentralen Managements müssen Netzwerkbetreuer nicht lokal in der Schule anwesend sein, was speziell im Falle kurzfristig benötigter Änderungen von Vorteil ist. Durch die Möglichkeit, Funktionen gleichzeitig für mehrere Standorte zu bearbeiten, kann z.B. sehr rasch ein Gästenetzwerk auf allen Schulen aktiviert werden oder neue Sicherheitsstandards ausgerollt werden.

Die Flexibilität im Einsatz der Aruba-Lösungen ermöglicht alle Szenarien mit einer Hardware – mit der Option, klein anzufangen und später zu wachsen. Somit sind die Investitionen gesichert.

FÜR DEN DIREKTOR

Als Schulleiter steht die Sicherheit der Schüler und ein hoher Bildungsstandard an erster Stelle. Aruba unterstützt dabei mit einer sicheren und zuverlässigen IT-Infrastruktur, die eine Umsetzung von Tablet-Klassen und eine Digitalisierung der Pädagogik ermöglicht.

Die Expertise und Erfahrung von Aruba und unseren Partnern kommt der Schule zugute, was bereits in der Auswahl der geeignetsten Produkte ersichtlich wird.

Um dem starken budgetären Druck entgegenzuwirken, bietet Aruba spezielle Schulpreise, die über unsere Partner abgerufen werden können. Zusätzlich können die Produkte „as a Service“ bezogen werden, also gegen einen attraktiven regelmäßigen Betrag. Die Registrierung der Schule als Endkunde beim Hersteller ermöglicht nicht nur attraktive Projektpreise auch bei kleinen Stückzahlen, sondern stellt auch sicher, dass die Schule in den Genuss der Limited Lifetime Warranty kommt.

Die Investition in ein Aruba-Netzwerk garantiert eine zukunftssichere Lösung. Nicht umsonst wird die Vorreiterrolle von Aruba durch große Institutionen wie Gartner, IDC, Forrester und viele andere regelmäßig bestätigt. Als Teil von Hewlett Packard Enterprise ist eine langfristige Marktpräsenz gesichert.

FÜR DEN IT-SYSTEMBETREUER

Die Betreuung mehrerer Schulen stellt oft eine Herausforderung an das Zeitmanagement dar. Dabei kann der Einsatz der Aruba-Infrastruktur im Netzwerk eine entscheidende Rolle spielen. Einerseits ist das Management, Reporting und die Problembehandlung einfach und übersichtlich gestaltet, andererseits ermöglichen zentrale Managementlösungen wie Aruba Central eine Betreuung mehrerer Standorte, ohne vor Ort sein zu müssen. Änderungen müssen nur ein Mal durchgeführt werden und können leicht auf mehrere Netze ausgerollt werden.

Auch krankheitsbedingte Abwesenheiten oder ein Urlaub stellen keine Hürde mehr da, wenn Central als mandantenfähige Lösung eingesetzt wird. Vorübergehend können die betreuten Schulen Kollegen zugeordnet werden, die in einem gewohnten User Interface arbeiten können, ohne neue Systeme erlernen zu müssen.

FÜR DEN NETZWERKBETREUER AN DER SCHULE

Immer herausfordernde Sicherheitsanforderungen bringen steigende Anforderungen an das Know-How von IT-Administratoren. In den meisten Schulen werden die Netzwerke „nebenbei" gemanaged, oft nur unter großem persönlichem Einsatz. Netzwerkumstellungen erfordern Einsätze außerhalb der normalen Arbeitszeit und ohne zusätzliche Vergütung.

Aruba unterstützt Sie mit hochwertigsten und zuverlässigen Komponenten. Schon in der Installationsphase mit Plug-and-Play Funktionalitäten (Zero-Touch-Provisioning) besteht eine enorme Zeitersparnis, die sich im Betrieb durch Ausfallssicherheit und stabile Verbindungen fortsetzt. Weniger Beschwerden über die Netzwerkqualität bringt mehr Zeit für die wirklich relevanten Dinge. Mit Aruba haben Sie ein Netzwerk, das einfach läuft.

Regelmäßige, automatisierte Reports und Alarmierungsfunktionen zeigen Engpässe auf, bevor Probleme entstehen. Durch die vielfältigen Funktionen der Aruba Lösungen können die Anforderungen von Schulleitern und dem Lehrpersonal auf höchstem Niveau umgesetzt werden.

DSGVO

Alle Aruba Produkte unterstützen eine lückenlose Umsetzung der Datenschutzgrundverordnung. In der Cloud gehostete Lösungen wie Aruba Central erfüllen höchste Sicherheitsstandards und garantieren auch bei Audits volle Akzeptanz. Wir empfehlen für die Umsetzung der DSGVO die Rücksprache mit erfahrenen Organisationen und Partnern.

SECURITY

Die Sicherheit der Daten im Netzwerk sollte ein Hauptaugenmerk erhalten. Dies beginnt damit, den Zugang zum Netzwerk nur berechtigten Personen zu ermöglichen. Aber auch innerhalb des Netzwerks ist eine Unterscheidung bei den Zugangsrechten in Gruppen wie Administration, Lehrer, Schüler und Gäste sinnvoll. Die oft verwendete Variante von einem „geheimen" Zugangspasswort für das WLAN ist leider eine suboptimale Lösung.

Moderne Zugangslösungen setzen auf einen rollenbasierenden Zugriff. Jedes Gerät im Netzwerk bekommt bereits bei der Anmeldung eine Rolle zugewiesen, mit der dann die jeweiligen Berechtigungen verknüpft sind. So wird effektiv verhindert, dass Schüler auf Ressourcen zugreifen können, die Lehrern vorbehalten sind. Gleichzeitig unterstützen automatisierte Regeln den Netzwerkbetreuer, so dass dieser nicht jedes Gerät freischalten muss. User können ihre Geräte selbst administrieren, was besonders in Zeiten, in denen Mobiltelefone, Tablets oder Notebooks häufig getauscht werden, ein wichtiger Faktor ist.

Durch den Einsatz von Aruba ClearPass müssen sich Schulen keine Sorge um die Sicherheit der Zugänge machen. Um den Aufwand bei Schulen gering zu halten besteht die Möglichkeit, ClearPass als Service zu beziehen – es wird keine Security-Expertise an der Schule vorausgesetzt.

„Durch die Modernisierungsmaßnahmen mittels Access Points von Aruba Networks unter Berücksichtigung der Verwaltung der Geräte und User-Accounts konnten wir vor allem bei Tabletklassen eine deutlich spürbare Verbesserung feststellen.

Das Netzwerk wurde mittels VLANs in Teilnetze untergliedert, generischen Accounts wurden durch personalisierte Accounts für SchülerInnen und LehrerInnen ersetzt – was die Sicherheit der IT auf ein neues Level hebt.

Dies kommt vor allem den SchülerInnen und LehrerInnen der AHS Heustadelgasse zugute und ermöglicht einen zeitgemäßen Unterricht mit modernsten Lehrmitteln."

Mag. Claudia Varga,
EDV-Kustodin AHS Heustadelgasse

DER DIGITALISIERUNGSCHECK

Anbindung ans Internet und andere externe Netzwerke

- ☐ Die Bandbreite ist adäquat, um gleichzeitige Online-Arbeiten zu ermöglichen

Firewall

- ☐ Filterung von gefährdenden Inhalten
- ☐ Berücksichtigung der DSGVO Erfordernisse

Verkabelung

- ☐ Verbindungen zwischen Core-Switch und Access-Switches sind in Glasfaser (mindestens 10G) ausgeführt
- ☐ Verbindungen zu Access Points erfolgen mit mindestens 1000BASE-T (Gigabit Kupfer, AWG22 Kat.7)
- ☐ Stromversorgung der Verteilerswitches für PoE-Leistung der angeschlossenen Geräte dimensioniert (Alternativ je Access Point eine Steckdose)

Netzwerk

- ☐ Redundanz des Core-Switches mit unabhängigen Stromkreisen ist gegeben
- ☐ Es stehen ausreichend Ports zu Verfügung
  - Je Klasse 1x Access Point, 1x Beamer, 1x Lehrer-PC
  - Je Lehrerzimmer/Büro 1x Access Point, eventuell PoE-Telefonie, Drucker
  - Weitere Anwendungen wie Schließsysteme, elektronische Tafeln etc. berücksichtigt
- ☐ Das Power-over-Ethernet Budget entspricht den angeschlossenen Geräten

WLAN

- ☐ Access Points unterstützen automatische Kanal- und Leistungsabstimmung
- ☐ Automatisches Roaming zwischen Access Points (ClientMatch)
- ☐ Filterung und Priorisierung von Inhalten (AppRF) mittels Deep Packet Inspection (DPI)
- ☐ Bandbreitenbegrenzung für Schüler und Lehrer

WLAN Abdeckung

- ☐ Alle Klassenräume
- ☐ Lehrerzimmer und Büros
- ☐ Aula und Veranstaltungsräume
- ☐ Außenbereiche

Security

- ☐ Rollenbasierende Zugangskontrolle (Network Access Control) für alle Geräte im Netzwerk über 802.1x
- ☐ Trennung zwischen Lehrer- und Schülergeräte
- ☐ Gästenetzwerk getrennt vom Schulnetz (nur Internetzugang für Gäste)

Management

- ☐ Eine einheitliche Plattform zum Management von LAN und WLAN
- ☐ Einfache Installation durch Zero Touch Provisioning (Plug&Play)
- ☐ Cloud-basierendes Management zur einfachen Verwaltung mehrerer Schulen

Reporting und Alarmierung

- ☐ Regelmäßige Netzwerk-Health-Reports mit definierbaren Inhalten
- ☐ Konfigurierbare Alarmierung bei kritischen Netzwerkproblemen und Angriffen

aruba
a Hewlett Packard Enterprise company

WP_Netzwerkinfrastruktur_in_Österreichischen_Schulen_A4_110719