Handreichung: Unterricht drahtlos

WLAN-Clients einbinden

Unabhängig vom schulischen Einsatzkonzept – ob schülereigene Geräte oder primär einheitliche schulische Ausstattung – erfordern alle mobilen Endgeräte den Zugang zum Netzwerk der Schule bzw. Internet.

Als Standardzugangstechnik ist die **WLAN**-Schnittstelle (nach IEEE802.11 bzw. Wi-Fi) etabliert und wird nahezu von allen mobilen Clients und Betriebssystemen unterstützt. Das vereinfacht die Planung und den Betrieb. Vor dem Einsatz von WLAN sollte der erforderliche Schutzbedarf analysiert und grundlegende Anforderungen definiert werden. Diese betreffen insbesondere den Bereich des Datenschutzes.

Anders als in kabelgebundenen Netzwerken, verlassen die Daten das WLAN-fähige Endgerät über ein ungesichertes geteiltes Medium, die Luft. Das WLAN-Signal strahlt über das Gebäude hinaus und ist somit prinzipiell abhörbar.

Sicherheitsverfahren ermöglichen eine vertrauliche Kommunikation zwischen WLAN-Client und Access-Point. Die dort integrierten Kryptographie- und Authentifizierungsmechanismen gewährleisten den sicheren Datentransfer.

Sicherheitsverfahren

Mit WiFi-Protected-Access (WPA) wurde ein Standard definiert, der sowohl die Verschlüsselung der Daten als auch die Authentifizierung des Kommunikationspartners im WLAN ermöglicht. Empfohlen wird der Einsatz der aktuellen Version, WPA3. Aus Kompatibilitätsgründen kann die Verwendung von WPA2 weiterhin erforderlich sein. Komplexe bzw. lange Passwörter sichern in diesem Fall die Kommunikation.
Der frühere WEP-Standard gilt als unsicher und sollte nicht verwendet werden. Er wird in aktuellen Systemen deshalb mitunter auch nicht mehr angeboten.

Neben der Verschlüsselung, die aktuellen WPA-Versionen nutzen das Verfahren AES, ist auch die Authentifizierung des Kommunikationspartners für die sichere Datenkommunikation notwendig. Bei der Version WPA-Pre-Shared-Key (PSK) bzw. WPA Personal nutzen alle Netzwerkteilnehmer einen zuvor geteilten gleichen (WLAN-)Schlüssel. Diese Variante eignet sich wegen ihrer einfachen Handhabung besonders im Unterrichtsnetz der Schule.

Eine personenbezogene Authentifizierung kann die Sicherheit erhöhen. Unter WPA-Enterprise erfolgt eine Abfrage des WLAN-Access-Point gegen einen zentralen Authentifizierungsserver (RADIUS) bzw. Verzeichnisdienstserver. Diese Version ist mit einem deutlichen Mehraufwand bei Installation und Wartung verbunden. Ergänzend sei darauf hingewiesen, dass auch die Server selbst eine Absicherung benötigen. In Schulnetzwerken ist der Einsatz von WPA-Enterprise in aller Regel **nicht** notwendig. Gleiches gilt für die individuelle Authentifizierung per Private Pre Shared Key

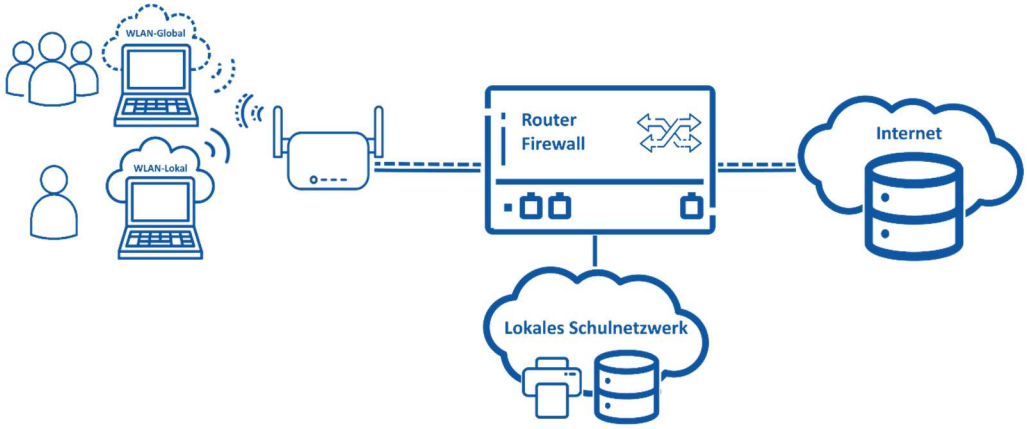
(PPSK) welches von einigen Herstellern unter verschiedenen Namen implementiert ist. Dieses Verfahren ist nicht standardisiert.

Netzbetrieb und Netztrennung

Mit der zunehmenden Nutzung cloudbasierter Dienste, wird das schulische WLAN mit Internetanschluss die primäre Zugangstechnik zu Lern- und Arbeitsmitteln. Cloudlösungen decken viele Anforderungen unterrichtlicher Prozesse ab. Der Zugang zum Internet über das WLAN sollte deshalb niederschwellig nutzbar sein. Der Schutzbedarf hinsichtlich Vertraulichkeit und Integrität ist hier als normal einzustufen.
Ein höherer Schutzbedarf ergibt sich, wenn auch lokale Ressourcen über das WLAN erreicht sein müssen. Drucker oder Datenspeicher werden insbesondere von Lehrkräften benötigt. Der Zugang zu diesen Diensten bedarf einer weiteren Absicherung.

Multi-SSID
Sowohl ein niederschwelliger Zugang als auch ein höherer Schutzbedarf beim Zugriff auf lokale Ressourcen kann über die Mehrfachnutzung der WLAN-Infrastruktur erfüllt werden. Die Technik „Multi-SSID“ ermöglicht die Konfiguration von zwei oder mehr virtuellen Netzen am Access-Point. Diese Netze werden mit unterschiedlichen Sicherheitseinstellungen versehen. Beispiel:

- SSID1: WLAN-Global[1]
  Funktion: Internetzugang für Schülerinnen und Schüler, Lehrkräfte sowie Gäste
  Sicherheit: WPA2/3-PSK, einfach nutzbares Passwort
- SSID2: WLAN-Lokal
  Funktion: Internetzugang und zusätzlich Zugriff auf Ressourcen im lokalen Netzwerk für Lehrkräfte
  Sicherheit: WPA2/3-PSK, komplexes Passwort mit vertraulicher/eingeschränkter Weitergabe



Die Anbindung der Funknetze erfolgt über Virtuelle LANs (VLAN) innerhalb der Schulnetzinfrastruktur. Der zentrale Router (L3-Switch) mit Firewall-Funktion übernimmt die zugriffskontrollierte Weiterleitung. Er hat eine zentrale Funktion im Sicherheitskonzept des Unterrichtsnetzes.

Der Zugang zum Verwaltungsnetz muss ausgeschlossen sein.

[1] WLAN-Global: Der SSID-Name weist auf die beabsichtigte Funktion hin, er kann beliebig gewählt werden.

Netzwerkzugänge (Konfiguration über Firewall-Router)

	Internet	Schulnetz (LAN)	Admin-VLAN
WLAN-Global	✔	✘	✘
WLAN-Lokal	✔	✔	✘
Systembetreuung	✔	✔	✔
Ext. Techniker	○	○	○

○ in Begleitung, bzw. in Einzelfällen

Access-Point und Administration

Leistungsfähige Hardware und eine gute WLAN-Abdeckung sichern den stabilen Betrieb auch zu Hochlastzeiten[2]. Störungen und Überlastungen im Netzzugang gefährden den Unterrichtsbetrieb und haben ggf. zur Folge, dass unsichere alternative private Zugänge, zum Beispiel Mobiltelefone der Schülerinnen und Schüler, genutzt und geteilt werden.

WLAN-Access-Points werden an funktechnisch günstigen Orten montiert. Die Stromversorgung erfolgt per Power-over-Ethernet (PoE) über den verbundenen Switch bzw. PoE-Adapter oder ein separates Netzteil. Um Manipulationen an der Hardware zu verhindern, sollte der Montageort so gewählt werden, dass er physisch allgemein nicht zugänglich ist.

WLAN-Controller
Die Administration des schulweiten WLAN bzw. der Access-Points erfolgt in aller Regel über einen WLAN-Controller. Notwendige Konfigurationen und Aktualisierungen der Firmware werden darüber durchgeführt und Ausfälle oder Überlastsituationen zentral angezeigt. Dies erhöht die Sicherheit und die Verfügbarkeit.
Der Zugriff auf die Access-Points bzw. den Controller muss auf den administrativen Nutzerkreis eingeschränkt sein. Nur die Systembetreuung und autorisierte Techniker bekommen Zugang zur passwortgeschützten Verwaltung. Eine Zwei-Faktor-Authentifizierung kann den Zugriff auf cloudbasierte Controller zusätzlich absichern.
Mit entsprechender Anforderungsdefinition und dem Einsatz eines WLAN-Controllers legt sich die Schule auf einen Hersteller fest. Access-Points und Controller müssen zueinander kompatibel sein.

Verfügbarkeit
Der Ausfall eines WLAN-Access-Points muss zeitnah behoben werden. Hersteller von Business-Hardware bieten mitunter erweiterte Garantieleistungen oder Serviceverträge für einen kurzfristigen Ersatz. Ein gut erreichbarer Support durch Dienstleister oder Hersteller unterstützt die Systembetreuung. Mögliche IT-Sicherheitslücken in der Firmware werden unverzüglich behoben und Aktualisierungen durch den Hersteller sichergestellt.

Für eine schnelle Wiederherstellung im Fehlerfall sollten Konfigurationsdateien von Access-Points bzw. des Controllers in einem externen passwortgeschützten Speicher gesichert werden.

Insgesamt können hier die gleichen Sicherheitsanforderungen bzw. Zugriffsbeschränkungen wie bei allen Netzwerkgeräten herangezogen werden.

Client-Absicherung
Die Absicherung des WLAN-Clients bzw. des Endgerätes obliegt in aller Regel dem Besitzer. Das WLAN-Netzwerk der Schule ist grundsätzlich als unsicher zu betrachten. Weder die Nutzer noch die Endgeräte können im einfachsten Fall hier individuell identifiziert oder behandelt werden.

[2] Schon im Regelfall kann vereinfacht von 60 WLAN-Clients pro Klassenzimmer-Access-Point ausgegangen werden. 30 Schülerinnen und Schüler: 30 x Smartphone + 30 x mobiles Endgerät

Eine Personal-Firewall kann die Client-Sicherheit erhöhen. Verbunden mit einer Anti-Viren-Software gewährleisten diese Maßnahmen einen Grundschutz am Endsystem. Sind diese Teil des Sicherungskonzepts, muss verhindert werden, dass die Funktionen an schuleigenen Geräten durch den Anwender deaktiviert werden.

Die Übertragung von sensiblen Daten muss durch weitere Mechanismen geschützt werden. Das Protokoll HTTP/S verschlüsselt die Nutzdaten bei einer Kommunikation über den Browser. Für andere Kommunikationsprozesse stehen VPN-Technologien zur Verfügung.

Erweiterte Sicherheit

Mit entsprechendem Aufwand ließen sich WLAN-Netzwerke grundsätzlich umfassend absichern. Individuelle Authentifizierung oder der Zugangsschutz per MAC-Adressfilterung sind weitere mögliche Ansätze.
Eine verbreitete WLAN-Authentifizierungstechnik ist Captive-Portal, ggf. kombiniert mit einem Ticketsystem. Diese von Hotspot-Systemen bekannte Variante erhöht den Verwaltungsaufwand, aber auch die Sicherheit durch die Limitierung der Zugriffsberechtigungen. Die Sicherheit der verschlüsselten Datenübertragung basiert auf WPA2/WPA3.

Die hier aufgeführten Maßnahmen widersprechen mitunter der Forderung nach einer niederschwelligen WLAN-Nutzung.

Erhöhte Sicherheitseinstellungen können auch mit einem Funktionsverlust verbunden sein. Mit „Client Isolation[3]“ – eine Einstellung auf dem Access-Point – kann die Kommunikation der WLAN-Clients untereinander innerhalb einer SSID-Funkzelle unterbunden werden. Diese, gerade in Gast-Netzen gerne verwendete Einschränkung, könnte jedoch zur Folge haben, dass - je nach System - die kabellose Bildschirmübertragung im Klassenzimmer oder der drahtlose Dateiaustausch zwischen den Endgeräten nicht möglich ist.

Pädagogisches Augenmaß

Das WLAN im Unterrichtsnetz der Schule dient primär pädagogischen Aufgaben. Es arbeitet als lokale Zugangstechnik zum weltweiten Internet. Mit einfachen Mitteln lässt sich ein grundlegender Schutzbedarf decken.

Zwischen den Sicherheitsanforderungen für ein Schüler-WLAN (auch Gäste), welches nur den Internetzugang bereitstellt, und einem WLAN für Lehrkräfte, mit Zugang zu lokalen Ressourcen, sollte unterschieden werden. Pädagogische, organisatorische und sicherheitsrelevante Vorgaben können weitere Umsetzungsvarianten erforderlich machen.
Die Funktionsstabilität, eine einfache Administration und die Absicherung der Netzwerkgeräte sollten von besonderer Bedeutung sein.

[3] herstellerspezifisch, auch genannt: AP Isolation/IP Isolation/Intra-cell Repeating (u.a.)