WLAN an Schulen

ÜBERLEGUNGEN ZUM TECHNISCH EINWANDFREIEN UND RECHTSSICHEREN BETRIEB VON WLAN-LÖSUNGEN MIT BYOD-OPTION

Übersicht
Elemente dieser Präsentation

- I. Grundsätzliches, Umfang
- II. Technische und infrastrukturelle Betrachtungen
  - Netzwerkstruktur
  - Hard- und Software
- III. Sicherheitsaspekte
  - Anmeldeverfahren
  - Filterung, Anti-Malware- und andere Sicherungsmechanismen
- IV. Nutzerverhalten und Rechtssicherheit
  - Nutzerordnung
  - "Logging"
  - Störerhaftung
- V. Ausblick
- VI. Fazit

BYOD Willicher Schulen
Volker Sternemann, Stadt Willich, GB I/2

I. Grundsätzliches, Umfang
Teil 1 – Eine „kleine Lösung“

- Kleine Lösung: Mobiler WLAN-Hotspot z.B. in einem Notebook-Wagen o.ä., der von Klasse zu Klasse transportiert wird.
  - Vorteil: Schnell einzurichten, kostengünstig
  - Nachteil 1: „Gebastel“, Lauffähigkeit kann nicht 100%-ig sichergestellt werden. Wartungsintensiv! Und Frage: Von wem soll gewartet werden?
  - Nachteil 2: Sicherheitsaspekte bleiben genauso wie bei „großer Lösung“, sind aber hiermit nur schwer umzusetzen (sh. Teil III)
  - Nachteil 3: Wenn dann nur in Grundschulen geeignet, wenig Flexibilität
  - Nachteil 4: Lehrpläne, „Bildung 4.0“, „Gute Schule 2020“ und Einführung des Medienpasses bilden eher die Grundlage für eine flächendeckende Lösung für alle Fachschaften und Bereiche, nicht für kleine Inseln

I. Grundsätzliches, Umfang
Teil 2 – Flächendeckendes WLAN

- Es werden in ausreichender Anzahl Access-Points installiert um eine flächendeckende Versorgung zu erreichen.
  - Vorteil 1: Sehr flexibel, kann plattformunabhängig viele User versorgen
  - Vorteil 2: Gibt langfristig Sicherheit für Lauffähigkeit. Wartungsarm!
  - Vorteil 3: Standortvorteil nicht auf die Schule bezogen sondern auf die gesamte Kommune (in Zeiten der aktuellen Medienlage nicht unwichtig!)
  - Vorteil 4: Einzige Möglichkeit, Datensicherheit und Datenschutz in vollem benötigten Umfang zu gewährleisten
  - Nachteil: Technisch aufwändiger (fest verkabelt), daher auch teurer
- BYOD ist **nicht** WLAN-abhängig! Vielmehr ist BYOD nur eine Entscheidung zum mobilen Lernen. **Aber:**
- Sicherheit und Nutzungskontrolle haben Vorrang! Daher kommen die „Kleine Lösung“ oder gar kein WLAN nicht in Frage (sh. auch V.)

II. Technische Überlegungen Teil 1 – Das Netzwerk an sich

- Basis sind die vorhandenen Netzwerkverkabelungen
  - „Hopping“ der Daten von AP zu AP nicht wirklich möglich
- Drittes Netz zusätzlich zum PN & VN der Schule sollte angelegt werden mit eigenem Bereich von IP-Adressen
  - Sonst droht Szenario ähnlich wie im Städtischen Krankenhaus in Neuss
- Da die Verkabelung mit der Zahl der Netze nicht automatisch mitwächst, werden VLAN-fähige Switche benötigt
  - alle Netze werden virtuell autark voneinander angelegt
- Zentrales AP-Management wird zwingend benötigt aufgrund der Menge von APs

II. Technische Überlegungen Teil 2 – Hard- und Software

- AP‘s müssen leistungsfähig sein: Viele User, hohe Datenmengen
- Hohe Anzahl von AP‘s: Zentrales Management nötig mindestens als Softwarelösung
- Seamless Roaming z.B. durch „Zero Handoff“-Technologie
- Automatische Umschaltung des von den Endgeräten jeweils benutzten Funkbandes (2,4 GHz / 5 GHz)
- WPS am besten gar nicht implementieren, zur Not wenigstens abschalten.
- Quotierung oder sogar Deaktivierung durch Zentralmanagement möglich

III. Sicherheitsaspekte
Teil 1 – Anmeldeverfahren

- „WPA2-Enterprise“-Authentifizierung
  - Personenbezogen
  - Höchste Verschlüsselungsstufe
- Zentraler RADIUS-Server übernimmt die Abfragen zur Userauthentifizierung beim LDAP-fähigen Domänencontroller (idealerweise Active-Directory)
  - Weitergabe der Daten an (externen) Radius-Server durfte bislang nicht stattfinden, nur ACK-/ NAK-Daten werden ausgetauscht
  - Vereinfachung des User-Managements über Pflege der AD (inkl. Anlage, Löschung und [De-]Aktivierung von Accounts)
  - Effizientes Logging des Nutzerverhaltens möglich (sh. Teil IV)
  - WLAN-Netze damit nicht mehr öffentlich (sh. Teil IV)
- MAC-Adressen-Filterung für Identifikation der Endgeräte möglich (für den Zugriff auf das VN oder PN mit hierfür zugelassenen Geräten)

III. Sicherheitsaspekte
Teil 2 – Filterung, Anti-Malware etc.

- Transparenter Proxy-Server übernimmt die Filterung zum/vom Internet
  - Filterung aller Netze (PN, VN, WLAN, evtl. weitere Netze z.B. für Haustechnik), ohne dass die Nutzer dies durch Änderung der Proxy-Einstellungen am Endgerät umgehen können.
- Zentrale Anti-Malware-Software übernimmt Überprüfung des Internet-Datenflusses per Bitstreaming
- Zentrale Firewall zwischen Internet und den einzelnen Netzen

IV. Nutzerverhalten
Teil 1a – Die Nutzerordnung

- „Digitale Hausordnung“ als letzte Stufe zur Rechtssicherheit
- Inhaltliche Abdeckung und Unterscheidung von:
  - Geräten des Schulträgers
  - BYOD-Geräten, die dem Eigentumsrecht des Nutzers unterliegen
  - Cloud-Nutzung (bei Bedarf)
- Klare Definition von:
  - Do‘s im Netz
  - Don‘ts im Netz
  - Sanktionen und Haftung
  - Vorratsdatenspeicherung: Was wird gespeichert und wie lange?

BYOD Willicher Schulen
Volker Sternemann, Stadt Willich, GB I/2

IV. Nutzerverhalten
Teil 1b – Die Nutzerordnung

- Muss im Einklang mit der gültigen Rechtslage sein (BDSG, DSG NRW, JuSchG, TMG, TKG, BGB, StGB, VO DV I, VO DV II...)
- Kurzer Exkurs in Sachen Cloud:
  - „Einklang mit Rechtslage“ bezieht sich natürlich auch auf die VO-DV I & II, was zu Problemen hinsichtlich der Cloud-Nutzung führte
    - Egal welcher „Cloud“-Dienst auch im weitesten Sinne hier gemeint ist
    - Datenweitergabe außerhalb des Schulnetzes war hier das Problem
    - Problem insoweit gelöst, als dass Datenweitergabe nunmehr grundsätzlich möglich ist, sofern die Datenschutzkonformität gegeben ist
  - Nutzung von Cloud-Diensten daher nur auf freiwilliger Basis

IV. Nutzerverhalten
Teil 2 – Das Logging

- Access-Log-Server aus Haftungsgründen
  - Im Falle von missbräuchlicher Nutzung Ihrer Netze müssen Sie Rede und Antwort stehen können
  - Eigenes Interesse daran zur Absicherung der Netze, aber auch zur Weitergabe der Haftung an die Missbrauchs-User
- Nutzungsordnung muss enthalten, welche Daten wie lange gespeichert werden und wer darauf zugreifen darf
  - stichprobenartige Überprüfung
  - oder komplette Darlegung auf richterliche Anordnung
- User **müssen** Kenntnis und sich einverstanden erklärt haben (bedeutet, dass Integration der Nutzungsordnung in Hausordnung der Schule eher problematisch sein dürfte).

IV. Nutzerverhalten
Teil 3a – Störerhaftung, Vorab…

Folgende Vorüberlegungen:

- Großes Angst-Thema bei allen Betreibern von öffentlichen Netzen, aber warum überhaupt?
- Einwand 1: Die Störerhaftung bezieht sich nur auf Missbrauchsfälle mit Auswirkungen auf Dritte
- Einwand 2: Da kein öffentliches Netz angeboten wird, gilt die Störerhaftung sowieso nicht
- Einwand 3: User wird mit gut überlegter Nutzungsordnung von vorn herein in die Pflicht genommen mit allen Konsequenzen

IV. Nutzerverhalten
Teil 3b – Störerhaftung, Definition

IV. Nutzerverhalten
Teil 3c – Störerhaftung, Userhandeln

- ***Ausgangsfrage***: Kann ein Netzbetreiber für das Verhalten eines Users direkt verantwortlich gemacht werden?
- Ausgangspunkt: Der Fall Tobias McFadden vs. Sony Music Entertainment Germany GmbH
- Statement des EuGH vom 16.03.2016 (noch VOR dem eigentlichen Urteil):

  „*...dass der Betreiber eines Geschäfts, einer Bar oder eines Hotels, der der Öffentlichkeit ein WLAN-Netz kostenlos zur Verfügung stellt, für Urheberrechtsverletzungen eines Nutzers nicht verantwortlich ist.*“
- Man merkt: Hier geht es konkret um Urheberrechtsverletzungen und kommerzielle Netzwerke, trotzdem betrachten wir das Thema dennoch einmal im übertragenden Sinne

IV. Nutzerverhalten
Teil 3c – Störerhaftung, Userhandeln

- Konkretisierung des o.g. Statements mit Urteil C484/14 des EuGH („McFadden"-Urteil) aus September 2016:

  „*...ein Geschäftsinhaber, der der Öffentlichkeit kostenlos ein WiFi-Netz zur Verfügung stellt, ist für Urheberrechtsverletzungen eines Nutzers nicht verantwortlich*".

- ***Antwort***: Nein! Rechtsverletzungen (analog gesehen) sind also nicht das Problem des Netzbetreibers, sondern des Nutzers. Und das bleibt auch so. Fachbegriff: „Providerprivileg"
- Dieser Teil der Störerhaftung wurde per Änderung des TMG am 21.07.2016 zugunsten der Netzwerkbetreiber durch Einführung des Providerprivilegs auch in Deutschland stark aufgeweicht, wenngleich (leider) nicht abgeschafft

IV. Nutzerverhalten
Teil 3d – Störerhaftung, Netzbetr.

- Trotzdem ist der Unterlassungsteil immer noch nicht aus der Welt, d.h. der Netzbetreiber könnte immer noch dafür Sorge tragen müssen, dass die Verstöße unmöglich gemacht werden
- Randnotiz 101 zum „McFadden"-Urteil sagt: „*Aufgrund der Vorgaben des EuGH darf nationales Recht dazu führen, dass WLAN-Betreiber ihr Netz verschlüsseln müssen und das Passwort nur an identifizierte Nutzer herausgeben.*"
- Was ist denn das? Nichts anderes als das Entfernen der Öffentlichkeit aus dem betroffenen Netzwerk
- Genau der Punkt wird aber schon erfüllt! Ergo verbleibt die Konsequenz für eine missbräuchliche Nutzung der Netze in Analogie zur Urheberrechtsverletzung in der Haftung des Users

IV. Nutzerverhalten
Teil 3d – Störerhaftung, Netzbetr.

- Vorsorglich für den Fall des - ohnehin schon illegalen – Eindringens in ein Netzwerk sei hier noch ein Urteil des BGH vom 24.11.2016 (Az.: I ZR 220/15) angesprochen:

  „*...dass die Störerhaftung für die Verbreitung von urheberrechtlich geschützten Medien [per Filesharing] nicht gilt, wenn sich Unbekannte unerlaubt Zugriff auf ein durch Passwort geschütztes WLAN verschaffen.*“

- Damit wird also auch der Fall der illegalen Benutzung von nicht-öffentlichen Netzen mit in die Überlegungen einbezogen.

IV. Nutzerverhalten
Teil 3e – Störerhaftung, Fazit

Fazit zur Störerhaftung

- Übergang der Haftung für das Userhandeln auf Netzbetreiber? Nein!
- Vorliegen der Haftung für zukünftigen Schutz gegen Missbrauch auf Netzbetreiber? Ja, ABER:
  1. Sofern die Netzwerke benutzerbezogen und ausreichend geschützt sind, liegt kein öffentliches Netz vor.
  2. Keine Haftung bei einem Betreiber, der sein Netz eben nicht der Öffentlichkeit zur Verfügung stellt und ausreichend schützt.
  3. Reduktion die Unterlassungsverpflichtung auf ein Maß, welches ohnehin schon erfüllt ist, wenn WLAN-Struktur professionell angelegt ist

V. Ausblick
Was kommt nach WLAN auf Sie zu?

- WLAN (und vor allem BYOD) erfordern drastische Geschwindigkeitssteigerungen der Internetleitungen von Schulen -> Ausbau der Breitbandanbindungen ist ein Muss
- Anpassung der Beschaffungs- und Finanzierungskonzepte aufgrund von:
  - Steigerung des Bedarfes an Präsentationstechnik (interaktive Bildschirme, interaktive Tafeln, Beamer in allen Klassenräumen etc.) durch Einsatz von mobilen Endgeräten
  - Einsatz von Tablet-Klassen (z.B. iPads)
  - Erweiterung der Support-Strukturen hinsichtlich des WLAN-Supports und des Supports von mobilen Endgeräten per MDM nötig
- Pädagogische Herausforderung an Schulen wird steigen. Insbesondere im Grundschulbereich häufig ein Problem

VI. Fazit
WLAN / BYOD an Schulen sinnvoll?

- Diskrepanz zwischen gelebter Wirklichkeit und Schulwirklichkeit viel zu hoch
- Sehr bald spürbare Auswirkungen auf Unterrichtsinhalte aufgrund der Hinwendung des Landes zu Bildung 4.0 und Digitalisierung des Unterrichts durch aktuelle Überarbeitung des Medienpass NRW
- Ja, WLAN-Netze sind – vernünftig aufgesetzt – technisch aufwändig und auch kostspielig
- Ja, es kommt noch ein ganzer Berg Arbeit und Kosten auf uns Schulträger zu
- Aber: Gute Schule 2020 hat als Kernthema den Ausbau der digitalen Infrastruktur, nichts anderes machen wir mit der Einführung von Funknetzen

Klare Empfehlung: WLAN-Netze JETZT und nicht später!

Herzlichen Dank für Ihre Aufmerksamkeit

SIE HABEN BESTIMMT NOCH FRAGEN, ODER?

IMMER HER DAMIT ☺

Kontakt:

Stadt Willich
GB I/2– Schule, Sport & Kultur
Volker Sternemann
email: volker.sternemann@stadt-willich.de
fon: 02154-949634