

Inhaltsverzeichnis

1	Management Summary	2
1.1	Ausschnitt aus der Sicherheits-Policy IG KOMSG	2
1.2	Allgemeine Hinweise / Redaktion	2
2	Konzepte	3
2.1	Grundlagen	3
2.1.1	Standards IEEE802.11a/b/g/n	3
2.1.2	Content Filtering im WLAN	5
2.1.3	Grundlegende Sicherheitsmassnahmen	5
2.1.4	Weiterführende Sicherheitsmassnahmen	7
2.1.5	Strahlungsbelastung	7
2.1.6	Fazit	8
2.2	Sicherheitsstufen	9
2.2.1	Gesichertes Unterrichtsnetzwerk (siehe Beispiel Volksschule Wattwil)	9
2.2.2	Halboffenes Netzwerk (siehe Beispiel BWZ Toggenburg)	9
2.2.3	Öffentliches Netzwerk (siehe Beispiel Hochschule Rorschach)	10
2.2.4	Zugriff auf das Verwaltungsnetzwerk	10
2.3	Beispiele	11
2.3.1	Volksschule Wattwil	11
2.3.2	Berufs und Weiterbildungszentrum Toggenburg	12
2.3.3	Pädagogische Hochschule Rorschach	13
3	Audit / Checkliste	14
4	Glossar	15
5	Weiterführende Informationen	18

1 Management Summary

Die IG Kommunikationsnetz St. Gallen (IG KOMSG) hat in ihrer Sicherheits- Policy für das Kantonale Netzwerk den Einsatz von drahtlosen Netzwerken (Wireless LAN, WLAN) gutgeheissen und in einem Abschnitt beschrieben.

Für das Erziehungsdepartement des Kantons geht aber dieser Abschnitt noch zu wenig weit. Es sind keine konkreten Beispiele, Checklisten und Audit-Richtlinien für den Einsatz solcher Netzwerke in Schulumgebungen aufgeführt. Die speziellen Bedürfnisse einer solchen Schulumgebung beinhalten diverse kritische Faktoren, wie zum Beispiel die Integration in den Schulbetrieb oder das Abschotten gegen Lauscher. Diese Aspekte werden in diesem Dokument ausführlich behandelt und Erfahrungen eingebracht. Es soll als Grundlage für weitere individuelle Konzepte für die Schulen dienen.

1.1 Ausschnitt aus der Sicherheits-Policy IG KOMSG

Der Einsatz von drahtlosen Netzwerken (WLAN) wird immer öfter zu einem Bedürfnis für die Erschliessung neuer Gebäudeteile. Grundsätzlich kann WLAN als öffentliches Netzwerk oder als eingeschränktes, sicheres Netzwerk betrieben werden. Der Einsatz dieser beiden Varianten unterscheidet sich neben der Sicherheit auch im Aufwand für den Betrieb und Unterhalt des Netzwerkes.

WLAN als öffentliches Netzwerk

Wird ein WLAN als öffentliches Netzwerk betrieben, hat grundsätzlich jedermann Zugriff auf das Netzwerk, die Benutzer werden nicht verwaltet. Die Daten werden nicht oder nur schwach verschlüsselt, es ist möglich den Datenverkehr eines anderen Benutzers aufzuzeichnen. Wegen der einfachen Zugriffsmöglichkeiten kann nicht kontrolliert werden, wer auf das Netzwerk zugreift. Aus diesem Grund müssen folgende Vorkehrungen getroffen werden:

- WLAN ist durch eine Firewall vom restlichen Netzwerk abgetrennt
- Keine direkten Zugriffe auf ein internes Netzwerk, allenfalls auf eine DMZ
- Die Firewall erlaubt nur den Zugriff mit den notwendigen Diensten ins Internet
- Die Benutzer müssen informiert werden, dass die Daten nicht oder nur schwach verschlüsselt sind und damit von anderen Benutzern aufgezeichnet werden können

Soll vom öffentlichen WLAN auf Daten innerhalb des Kundennetzwerks zugegriffen werden, muss dieser Zugriff über VPN erfolgen. Dabei gelten die in Kapitel 5 (Sicherheitsvorschriften IG KOMSG 040401) beschriebenen Bedingungen.

WLAN als sicheres Netzwerk

Damit vom Wireless LAN direkt auf Daten innerhalb des Kunden LAN zugegriffen werden darf, müssen die folgenden Bedingungen erfüllt sein:

- Die Benutzer müssen sich für den Zugriff auf das WLAN stark authentifizieren (SecureID, Zertifikat, gutes Passwort). Es wird eine gegenseitige Authentifizierung eingesetzt.
- Die Daten werden mittels eines starken Algorithmus verschlüsselt, die Verschlüsselung muss mit einem dynamischen Schlüssel erfolgen.

Diese Anforderungen werden heute von den Protokollen EAP-TLS (beschrieben im RFC 2716) und LEAP (Cisco proprietär) erfüllt. Beide Lösungen gelten heute als sicher und können damit auch für die Übertragung nicht öffentlicher Daten eingesetzt werden. Wichtig ist, dass die Daten nur auf der Luftstrecke verschlüsselt sind, nicht aber wenn sie über das Kunden LAN übertragen oder auf einem Gerät gespeichert werden. Die Benutzerverwaltung des WLAN muss kontinuierlich gepflegt werden, es ist insbesondere wichtig, dass austretende Mitarbeiter keinen Zugriff mehr auf das WLAN erhalten.

1.2 Allgemeine Hinweise / Redaktion

Fragen, allgemeine Hinweise sowie Verbesserungsvorschläge zu diesem Dokument oder den darin beschriebenen Richtlinien und Standards werden gerne entgegengenommen und sind an folgende Adresse zu richten:

Erziehungsdepartement Kanton St.Gallen
Dienst für Inneres und Informatik
Helmut Fürer (helmut.fuerer@sg.ch)
Davidstrasse 31
9001 St.Gallen

Freigabe	Technische Richtlinien WLAN (Funknetzwerk) <small>Techn. Richtlinie WLAN V 3.1</small>	Erziehungsdepartement Kanton St.Gallen		Seite 2 von 18
		Datum 01.09.2007	Version 3.1	

2 Konzepte

Für die Anwendung eines WLAN-Konzepts sind diverse Faktoren wichtig. Als erstes muss ein Standard (802.11a/b/g/n) gewählt werden. Zweitens ist die Sicherheitsstufe zu definieren. Drittens kann von bestehenden Anwendungsbeispielen gelernt werden. Die Anwendungsbeispiele beziehen sich auf die Problematik von Schulen, die schon WLAN erfolgreich einsetzen. Diese Beispiele sind von einer einfachen Lösung bis zu einer komplexen, skalierbaren Lösung beschrieben. Bevor WLAN eingeführt wird, müssen zuerst die Ziele des WLAN definiert sein, ein Konzept für die Umsetzung und den Betrieb erstellt, sowie Nutzungsrichtlinien erarbeitet werden.

2.1 Grundlagen

2.1.1 Standards IEEE802.11a/b/g/n

Früher war alles noch ganz einfach: Alle verfügbaren Funknetze basierten auf dem Standard 802.11b; Daten wurden mit theoretischen 11 MBit pro Sekunde übertragen. Jetzt plötzlich die Qual der Wahl: 11 Mbit (802.11b), 54 Mbit (802.11g und 802.11a) oder noch schneller? Und wenn es schon schneller sein soll, muss es dann auch noch kompatibel sein? Wer möglichst wenig Geld ausgeben will, steigt heute am besten mit einem 802.11b/g-Netz in die Wireless Welt ein. Für noch mehr Geschwindigkeit zahlt man immer noch mehr. In den nächsten Monaten werden weitere neue Geräte nach dem 802.11n-Standard auf den Markt kommen, sie versprechen noch höhere Übertragungsgeschwindigkeiten bei grösserer Reichweite.

Eine undankbare Rolle spielt 802.11a: nicht kompatibel zu aktuellen Netzen, deutlich teurer und weniger Reichweite. Für Privatanwender kommt 802.11a also kaum in Frage. Für Firmen bietet es jedoch einen entscheidenden Vorteil: Das Frequenzband ist breiter und bietet 8 parallele Kanäle. 802.11b/g-Netze müssen mit 3 parallelen Kanälen auskommen. Für grosse Funknetze mit hohen Benutzerzahlen ist 802.11a also besser geeignet. Wer 802.11a einsetzen will, sollte unbedingt eine Dualband-Karte in sein Notebook stecken. So kann er auch an öffentlichen Hotspots oder in den meisten anderen Wireless LANs ins Netz. Schulen, die bereits 802.11b-Netze einsetzen und nun auf 802.11a umsteigen wollen, können durch Dualband Access Points einen weichen Übergang mit einem sukzessiven Austausch der WLAN-Karten der Geräte erreichen

802.11b: Der billige Klassiker

Trotz neuer Standards unterstützt nach wie vor der grösste Teil der verkauften WLAN-Geräte dem Standard 802.11b

Auch wenn der Standard den Buchstaben "b" in der Bezeichnung trägt: Die erste ernstzunehmende Generation von Wireless-LAN-Geräten entsprach der Spezifikation 802.11b. Ihre Verbreitung ist in den vergangenen Jahren durch stark sinkende Preise auch im Privatbereich gestiegen; alle Hotspots, die drahtlose Verbindungen in Hotels, Flughäfen und anderen öffentlichen Plätzen erlauben, basieren auf diesem Standard.

Heute sind kaum noch Geräte auf dem Markt, welche nur den b-Standard unterstützen. Moderne Access Points und Karten fürs Notebook unterstützen meistens mindestens den b- und g-Standard.

802.11b	
Geschwindigkeit:	11 MBit/Sekunde brutto, in der Praxis 4 bis 6 MBit/Sek
Frequenz:	2,4 GHz – dieser Frequenzbereich ist stark genutzt, sodass Konflikte mit anderen Geräten wie Mikrowellen oder Bluetooth Handys den Datenverkehr stören und verlangsamen können
Reichweite:	In der Praxis sind Entfernungen von 25 bis über 50 Meter möglich. Wie bei allen Funkverbindungen hängt das stark von der Raumaufteilung und den verwendeten Baustoffen ab
Kompatibilität:	Kompatibel mit den meisten Hotspots und dem neuen Standard 802.11g; inkompatibel zu 802.11a
Kosten:	Router, Access Points ab ca. 150 CHF, Karte fürs Notebook ab ca. 50 CHF

Technische Richtlinien WLAN (Funknetzwerk)

802.11a: Die inkompatible Firmenlösung

Fast fünfmal so schnell, versprechen viele Hersteller – und verschweigen gerne, dass die teuren 802.11a-Geräte sich nicht mit ihren viel weiter verbreiteten 802.11b-Kollegen verstehen.

Gerne verweisen die Hersteller von 802.11a-Geräten auf das dicht gedrängte Frequenzband, das die wesentlich billigeren 802.11b-Geräte nutzen. Richtig ist, dass die Störung durch andere Geräte wesentlich geringer ist – gerne verschwiegen wird aber, dass simple Physik 802.11a teuer macht. Durch die höhere Frequenz wird das Funknetz wesentlich anfälliger für Rauschen, Abschattungen und Dämpfung. Dadurch ist die Reichweite von 802.11a-Netzen deutlich geringer als die von 802.11b, 802.11g oder gar 802.11n.

Ein weiteres Problem: In Europa dürfen 802.11a-Geräte nur mit einer Sendeleistung von 30 Milliwatt eingesetzt werden. So will man Störungen im Frequenzband vermeiden: Flugsicherung und Militär arbeiten teilweise im selben Frequenzbereich wie 802.11a-Funknetze. Mit einem erweiterten Standard 802.11h, der im September 2003 verabschiedet wurde, will man das Problem in den Griff bekommen: Darin sind bis zu 200 mW Sendeleistung vorgesehen, weil Frequenzkollisionen vermieden werden können (DFS, Dynamic Frequency Selection) und der Sender automatisch auf das benötigte Mass heruntergefahren wird (TPC, Transmit Power Control). Bis heute sind kaum Geräte des Standards 802.11h auf dem Markt.

Geräte, welche nur den a-Standard unterstützen sind heute bereits schwer zu erhalten, meistens sind die Geräte fähig Signale sowohl im 2,4 wie auch im 5 GHz Frequenzbereich zu verarbeiten, sie unterstützen den a-, b- und g-Standard.

802.11a	
Geschwindigkeit:	54 MBit/Sekunde brutto, in der Praxis ca. 15 MBit/Sek
Frequenz:	5 GHz – um Kollisionen auf der Frequenz zu vermeiden, ist die Sendeleistung der Geräte in Europa eingeschränkt und der Betrieb nur "indoor" erlaubt
Reichweite:	In der Praxis sind Entfernungen von 15 bis 20 Metern möglich. Wie bei allen Funkverbindungen hängt das stark von der Raumaufteilung und den verwendeten Baustoffen ab.
Kompatibilität:	Keine Kompatibilität mit anderen WLANs
Kosten:	Router, Access Points ab ca. 200 CHF, Karte fürs Notebook ab ca. 80 CHF

802.11g: Schnell und aktuell

Der g-Standard wird mittlerweile von den meisten angebotenen Geräten unterstützt, teilweise zusätzlich mit herstellerspezifischen Erweiterungen. Sie sind deutlich schneller und trotzdem voll rückwärtskompatibel zu 802.11b-Hardware.

Der g-Standard arbeitet problemlos mit bestehenden 802.11b-Wireless-Netzen zusammen und verspricht dieselbe Geschwindigkeit wie 802.11a. Wer also bereits drahtlose Hardware besitzt, kann problemlos mit schnellen Geräten nachrüsten. Für die Kompatibilität zu aktuellen WLANs gibt es eine simple technische Erklärung: 802.11b und 802.11g funken auf derselben Frequenz, nämlich 2,4 GHz. Eine Kommunikation mit 802.11a-Geräten ist nicht möglich, da diese auf 5 GHz arbeiten

802.11g	
Geschwindigkeit:	54 MBit/Sekunde brutto, in der Praxis ca. 20 MBit/Sek
Frequenz:	2,4 GHz – dieser Frequenzbereich ist stark genutzt, sodass Konflikte mit anderen Geräten wie Mikrowellen oder Bluetooth-Handys den Datenverkehr stören und verlangsamen können
Reichweite:	In der Praxis sind Entfernungen von 25 bis über 50 Metern möglich. Wie bei allen Funkverbindungen hängt das stark von der Raumaufteilung und den verwendeten Baustoffen ab
Kompatibilität:	Kompatibel mit den meisten Hotspots und anderen bestehenden Netzen nach 802.11b; inkompatibel zu 802.11a
Kosten:	Router, Access Points ab 150 CHF, Karte fürs Notebook ab ca. 50 CHF

Technische Richtlinien WLAN (Funknetzwerk)

802.11n: Die High Speed Zukunft

Neuerdings werden auch Geräte nach dem n-Standard zum Verkauf angeboten. Sie sind rückwärts kompatibel zu den Standards 802.11b und 802.11g.

Der n-Standard ist noch nicht verabschiedet, die Geräte sind entsprechend mit „802.11n (Draft)“ bezeichnet. Anfang 2006 haben sich die Standardisierungsgremien und die Gerätehersteller auf eine Vorabversion des Standards geeinigt, auf dessen Basis werden die Geräte hergestellt. 2007 soll der definitive Standard verabschiedet werden, die Hersteller verpflichten sich, dass Geräte nach dem Draft-Standard durch Softwareupdates die Anforderungen des definitiven Standards erfüllen werden. Durch die Bündelung von Kanälen verspricht 802.11n einerseits eine massiv höhere Übertragungsgeschwindigkeit, andererseits wird durch die Ausnutzung von Reflexionen auch eine bessere Abdeckung, insbesondere auch von verwinkelten Gebäuden, erreicht.

802.11n (Draft)	
Geschwindigkeit:	300 MBit/Sekunde brutto, in der Praxis bis 100 MBit/Sek
Frequenz:	2,4 GHz – dieser Frequenzbereich ist stark genutzt, sodass Konflikte mit anderen Geräten wie Mikrowellen oder Bluetooth-Handys den Datenverkehr stören und verlangsamen können
Reichweite:	In der Praxis sind Entfernungen von 50 bis über 200 Metern möglich. Wie bei allen Funkverbindungen hängt das stark von der Raumaufteilung und den verwendeten Baustoffen ab
Kompatibilität:	Kompatibel mit den meisten Hotspots und anderen bestehenden Netzen nach 802.11b und 802.11g; inkompatibel zu 802.11a
Kosten:	Router, Access Points ab ca. 200 CHF, Karte fürs Notebook ab ca. 140 CHF

2.1.2 Content Filtering im WLAN

Schulen tragen Verantwortung für schutzbedürftige Personen, also für alle minderjährigen Schülerinnen und Schüler. Da der Internetzugang in Funknetzwerken von allen Lernenden genutzt werden kann und soll (auch unbeaufsichtigt), sind Massnahmen zum Schutz vor rechtswidrigen Inhalten durch einen technischer Filter **unabdingbar**. Beim Content Filtering handelt es sich um einen Inhaltsfilter, der pornographische, rassistische und gewaltverherrlichende Seiten aus dem Internet herausfiltert.

Bei verschiedenen Schulen im Kanton St. Gallen stehen bereits Produkte für das Sperren von URLs und das Filtern von unerwünschten Inhalten im Einsatz.

Gemeinsam ist den Lösungen, dass das Surfen für die Benutzer nur über einen Proxy-Server, auf dem das Filterprogramm installiert ist, möglich ist. Auf dem Proxy-Server wird jede URL überprüft und zugelassen oder gesperrt. Neben dem Sperren von vordefinierten Kategorien von URLs ist es auch möglich eigene so genannte Black- (Liste von verbotenen URLs) und White-Lists (Liste von erlaubten URLs) zu definieren. Abhängig vom Benutzernamen des Surfers ist es zudem möglich verschiedene Filter anzuwenden.

Die bereits eingesetzten Produkte SurfControl Web Filter (www.surfcontrol.com) und WebWasher URL Filter (www.webwasher.com) können auf bereits bestehende Proxy-Server installiert werden. Neben der Filterfunktion bieten sie auch die Möglichkeit den Surfverkehr auszuwerten und so Rückschlüsse auf die Nutzung des Internet ziehen zu können.

2.1.3 Grundlegende Sicherheitsmassnahmen

Die ersten grundlegenden Massnahmen sind relativ einfach und ohne grössere Mehrkosten in der Installation und im Betrieb einzuführen:

Aktivierung der Sicherheitsarchitektur WEP (Wired Equivalent Privacy)

WEP ist ein Mechanismus, der WLAN Verkehr verschlüsselt, um unberechtigte Benutzer vom Lesen der während des Transports aufgefangenen Daten abzuhalten. WEP gilt heute nicht mehr als sicher und kann geknackt werden. Die meisten der WEP-Crack-Tools wie z.B. Aircrack laufen unter Linux und erfordern, dass der Benutzer ungefähr 4.000 Pakete mit schwachen Schlüsseln (Schlüssel sind die für die Erstellung des verschlüsselten Texts benutzten Geheimschlüssel) aus den Datenpaketen

Freigabe	Technische Richtlinien WLAN (Funknetzwerk) <small>Techn. Richtlinie WLAN V 3.1</small>	Erziehungsdepartement Kanton St.Gallen		Seite 5 von 18
		Datum 01.09.2007	Version 3.1	

Technische Richtlinien WLAN (Funknetzwerk)

des Netzverkehrs sammelt. Der Einsatz von WEP als Verschlüsselungsmethode wird heute nicht mehr empfohlen.

Einsatz von WPA (WiFi Protected Access) oder WPA2

In Drahtlosnetzwerken sollten die Daten auf jeden Fall verschlüsselt übertragen werden, damit diese vor dem Mitlesen durch andere Benutzer geschützt sind. Der WEP-Mechanismus bietet einen gewissen Schutz, gilt aber heute nicht mehr als sicher, resp. sollte nicht mehr verwendet werden.

Um das Netzwerk gegen unberechtigten Zugriff und das Abhören von Daten zu schützen, sollte heute zumindest WPA eingesetzt werden. WPA ist bei den eingesetzten Geräten heute nicht mehr eine Frage von Geld, sondern der Aktualität der Hardware und Firmware.

WPA arbeitet für den Schutz des Zugriffs auf das Netzwerk entweder mit vordefinierten Schlüsseln (Pre-Shared Keys PSK, WPA-PSK) oder authentisiert die Benutzer basierend auf dem Standard 802.1X auf einem RADIUS-Server (WPA-Enterprise) mittels Zertifikat oder SecurID. Für die Verschlüsselung wird TKIP verwendet, dieses Verfahren basiert auf WEP, es wird aber für jedes Datenpaket kryptographisch ein neuer Schlüssel erzeugt.

Kann in einem WLAN WPA2 eingesetzt werden, ist es sogar möglich die Daten mit dem als sicher geltenden AES-Algorithmus zu verschlüsseln. WPA2 erfüllt alle zwingenden Anforderungen des Standards 802.11i, ist allerdings nicht mehr abwärts kompatibel zu WEP.

Änderung der Standardeinstellungen des Access Points

Die Standardeinstellungen der Access Point - Service Set ID (SSID), SNMP Community String, Administrator-Passwort - sind Crackern weitgehend geläufig, und ein Cracker mit Know-how kann sich ziemlich leicht mit dem Netz verbinden und mit Standard-Passwörtern die Kontrolle über den Zugriffspunkt erlangen. (Leider sind Standard-Passwörter nicht ungewöhnlich.)

Senden der Service Set ID (SSID) nicht deaktivieren

Das Deaktivieren der Ausstrahlung der SSID bewirkt keinen Schutz.

Im Gegenteil: Bei deaktivierter SSID auf dem Access Point senden die WLAN Clients die SSID, auch wenn der entsprechende Access Point nicht in der Nähe ist. Diese SSID kann mit entsprechender Software einfach ausgelesen werden.

Testen des Umkreises

Identifizierung von Stellen und deren Abstand vom Access Point, an denen jemand auf das Netz zugreifen kann. Falls dies an ungewünschten Stellen vorkommt, können die Position des Access Points oder der Antennen Typ (z.B. Richtantenne) verändert werden, im Idealfall kann auch die Sendeleistung des Access Points auf das notwendige Minimum reduziert werden.

Die Überprüfung ob das WLAN beispielsweise auf dem Parkplatz empfangen werden kann, ist mit dem WLAN-Client des Betriebssystem bzw. des Hardwareherstellers möglich, es gibt auch Freeware-Tools die dafür eingesetzt werden können (z.B. NetStumbler).

MAC Adressfilterung am Access Point

Viele Access Points können so konfiguriert werden, dass sie MAC-Adressfilterung zur Einschränkung der Nutzung auf bestimmte Rechner einsetzen.

Die Filterung der MAC-Adressen ist insbesondere für mobile Klassenzimmer, bestehend aus einem Access Point und mehreren Laptops sinnvoll.

Deaktivieren des DHCP Protokolls des Access Point

In der Standardeinstellung sind die meisten Access Points als DHCP Server eingestellt und gewähren jedem anfordernden Rechner automatisch eine IP Adresse. Hierdurch ist es für Cracker sehr einfach, Informationen zu sammeln und sich mit dem Netz zu verbinden. Die Deaktivierung der DHCP-Funktion des Access Point verhindert das.

Freigabe	Technische Richtlinien WLAN (Funknetzwerk) <small>Techn. Richtlinie WLAN V 3.1</small>	Erziehungsdepartement Kanton St.Gallen		Seite 6 von 18
		Datum 01.09.2007	Version 3.1	

Technische Richtlinien WLAN (Funknetzwerk)

Die Deaktivierung der DHCP-Funktion ist insbesondere für mobile Klassenzimmer, bestehend aus einem Access Point und mehreren Laptops sinnvoll.

Gewährleistung der Nachvollziehbarkeit

Bei gewissen Geräten können Log-Informationen direkt an einen Syslog-Server gesendet werden. Damit liegen im Falle eines Missbrauchs oder einer Störung Informationen vor, welche die Nachvollziehbarkeit erleichtern. Log-Informationen, welche nach einem gewissen Zeitraum oder bei einer gewissen Grösse automatisch überschrieben werden, sind nur für diesen Zeitraum hilfreich.

2.1.4 Weiterführende Sicherheitsmassnahmen

Die nachfolgend beschriebenen, weiterführenden Massnahmen sollten wo immer möglich eingesetzt werden:

Einsatz von 802.11i

Der Standard 802.11i entstand, um die aufgetretenen Sicherheitslücken von WEP zu schliessen. Er umfasst die Bereiche Verschlüsselung, Authentisierung und Schlüsselmanagement. Weil der Standard auch Aspekte der Telefonie und des Roaming abdecken muss, dauerte es lange bis man sich auf die Spezifikation festgelegt hatte. Um bis dahin Lösungen anbieten zu können, die sicherer sind als WEP, wurde WPA als Übergangslösung eingesetzt. 802.11i ist ein von der IEEE definiertes, umfassendes WLAN-Sicherheitskonzept, WPA beinhaltet eine Teilmenge der in 802.11i enthaltenen Sicherheitsmassnahmen. Heute sind noch wenige Geräte verfügbar, welche 802.11i unterstützen.

Abtrennung des WLAN über eine Firewall

Die Abtrennung über einen Firewall hat den Vorteil, dass Zugriffe ins „sichere“ Netzwerk nur über die jeweiligen Sicherheits- Polycys erfolgen können. Somit ist das WLAN isoliert als unsicheres Netzwerk zu betrachten und stellt dementsprechend kein hohes Risiko mehr dar. Es sollten wenn möglich nur diese Dienste, die unbedingt nötig sind zur Verfügung gestellt werden.

Einsatz von Ausserband Benutzerauthentifizierung

Sollte das Konzept eine leistungsfähigere Authentifizierungsmethode fordern, kann eine Authentifizierung mittels eines separaten Authentifizierungs-Servers (z.B. RADIUS) auf einem verkabelten Segment neben dem Access Point eingesetzt werden. Diese Massnahme stellt sicher, dass nur autorisierte Benutzer sowohl zu verkabelten als auch zu kabellosen Ressourcen Zugang haben

Nutzung von verschlüsselten Protokollen

In Fällen, in denen vertrauliche Daten durch das WLAN geschickt werden müssen oder über das WLAN auf entsprechende Dienste zugegriffen wird, müssen die Verbindungen durch den Einsatz von aktuellen Verschlüsselungsprotokollen (IPSec, SSL, SSH) geschützt werden, so dass das erforderliche Mass an Vertraulichkeit gewahrt bleibt.

2.1.5 Strahlungsbelastung

Die Strahlungsbelastung ist immer wieder ein Thema für viele Personen. Generell kann gesagt werden, dass die gesetzliche Maximal-Leistung in der Schweiz für WLAN Geräte des Standards 802.11b/g/n bei 100mW EIRP (abgestrahlt) liegt. Das ist mehr als 20-mal weniger als ein Mobiltelefon, das beim Sprechen zudem oft direkt an den Kopf gehalten wird. Das benutzbare Frequenzband für den b/g/n-Standard liegt zwischen 2.400 und 2.484 GHz, beim a-Standard werden die Frequenzbänder von 5.15 bis 5.35 GHz und 5.47 bis 5.725 GHz genutzt. Weitere Aspekte über Störungen und Belastungen auf Mensch und Maschine sind im Internet zu finden.

Freigabe	Technische Richtlinien WLAN (Funknetzwerk) <small>Techn. Richtlinie WLAN V 3.1</small>	Erziehungsdepartement Kanton St.Gallen		Seite 7 von 18
		Datum 01.09.2007	Version 3.1	

2.1.6 Fazit

Wireless- LANs können auf der Grundlage der beschriebenen Sicherheitsmechanismen zuverlässig abgesichert werden - zumindest was die heutigen Angriffstechniken betrifft. Dies setzt aber voraus, dass die bereit stehenden Sicherheitsmassnahmen auch tatsächlich umgesetzt werden. Dabei ist die Situation weiterhin dadurch geprägt, dass die verfügbaren Lösungen teilweise proprietär sind und somit nur in einer homogenen Umgebung umgesetzt werden können und ein Teil der Lösungen (RADIUS Server, VPN) zwar praktikabel für grössere Netze ist, für kleinere Netzwerke aber kaum realisierbar erscheint.

Drahtlose Schulnetzwerke sollten daher, abhängig von der geforderten Sicherheit des WLAN, durch eine Auswahl der folgenden Massnahmen abgesichert werden:

- eine vorhandene Verschlüsselung unbedingt nutzen
- den statischen Schlüssel in regelmässigen Abständen aktualisieren
- eventuell vorhandene neue Treiber mit aufwändigerer Verschlüsselung vom Hersteller herunterladen
- WLANs eine eigene SSID geben und den SSID-Broadcast nicht unterbinden
- Zugangskontrolllisten auf MAC-Ebene pflegen
- die Log-Dateien regelmässig auf unbekannte MAC-Adressen überprüfen, um eventuelle Eindringversuche zu entdecken.

Bei grösserem Engagement (Kosten) kann man auch über ein Auftrennen des Netzwerkes in einen WLAN- und einen "sicheren" Teil nachdenken, wobei die Kopplung über eine Firewall erfolgt. All diese Massnahmen verringern das Risiko eines Eingriffs signifikant, auch wenn weiterhin Sicherheitslücken bestehen.

2.2 Sicherheitsstufen

Abhängig von der gewünschten Sicherheit des drahtlosen Netzwerks müssen verschiedene Massnahmen zur Minimierung des Risikos umgesetzt werden. Wie bereits weiter vorne beschrieben, gibt es grundlegende und weiterführende Sicherheitsmassnahmen, deren Einsatz mehr oder weniger Aufwand für den Betrieb bedeuten.

Die nachfolgenden Sicherheitsstufen wurden definiert, um eine Hilfe zu geben welche Sicherheitsmassnahmen für welchen Einsatz konfiguriert und aktiviert werden müssen.

2.2.1 Gesichertes Unterrichtsnetzwerk (siehe Beispiel Volksschule Wattwil)

Auf ein gesichertes drahtloses Netzwerk dürfen nur berechnigte Personen zugreifen, die Daten werden verschlüsselt übertragen.

Das WLAN ist nicht durch eine Firewall vom Schulnetzwerk getrennt, es muss ebenso gut geschützt sein wie das fest installierte Netzwerk der Schule.

Um das gesicherte WLAN zu schützen, müssen die folgenden Massnahmen umgesetzt werden:

- Verschlüsseln der Daten und Authentisierung mittels WPA
- Sendeleistung falls von den Access Points technisch unterstützt auf das Minimum reduzieren, damit der Zugriff nur im gewünschten Umfeld möglich ist
- Regelmässiger Wechsel der Pre-Shared Keys auf den Access Points und den Clients
- Sicherstellen, dass die Access Points nur vom fest installierten Netzwerk aus administriert werden können
- Regelmässiger Wechsel der Administrations-Passwörter aller WLAN-Komponenten
- LAN-Anschlüsse der Access Points falls möglich durch Einschalten von Port Security (Cisco-spezifisch) auf dem Switch vor unberechtigtem Zugriff schützen. Es kann so sichergestellt werden, dass nicht ein fremder Access Point an das Netzwerk angeschlossen werden kann.

2.2.2 Halboffenes Netzwerk (siehe Beispiel BWZ Toggenburg)

Auf ein halboffenes drahtloses Netzwerk dürfen nur berechnigte Personen zugreifen, die Daten werden verschlüsselt übertragen.

Das WLAN ist durch eine Firewall vom Schulnetzwerk getrennt, es sind vom WLAN nur Zugriffe auf die notwendigen und dafür vorgesehenen Dienste im Schulnetzwerk möglich.

Um das halboffene WLAN zu schützen, müssen die folgenden Massnahmen umgesetzt werden:

- Verschlüsseln der Daten und Authentisierung mittels WPA
- Sendeleistung falls von den Access Points technisch unterstützt auf das Minimum reduzieren, damit der Zugriff nur im gewünschten Umfeld möglich ist
- Regelmässiger Wechsel der Pre-Shared Keys auf den Access Points und den Clients
- Sicherstellen, dass die Access Points nur vom fest installierten Netzwerk aus administriert werden können
- Regelmässiger Wechsel der Administrations-Passwörter aller WLAN-Komponenten
- LAN-Anschlüsse der Access Points durch Einschalten von Port Security auf dem Switch vor unberechtigtem Zugriff schützen

2.2.3 Öffentliches Netzwerk (siehe Beispiel Hochschule Rorschach)

Auf ein drahtloses öffentliches Netzwerk haben alle freien Zugang (Hotspot), der Zugriff auf das Netzwerk ist nicht eingeschränkt, die Daten werden bei der Übertragung nicht verschlüsselt.

Das WLAN ist vom Schulnetzwerk durch eine Firewall getrennt, direkte Zugriffe sind nur auf öffentliche Dienste möglich. Für den Zugriff auf Dienste im Schulnetzwerk müssen sich die Benutzer am Netzwerkübergang authentisieren.

Um das öffentliche WLAN zu schützen, müssen die folgenden Massnahmen umgesetzt werden:

- Sicherstellen, dass die Access Points nur vom fest installierten Netzwerk aus administriert werden können
- Regelmässiger Wechsel der Administrations-Passwörter aller WLAN-Komponenten
- LAN-Anschlüsse der Access Points durch Einschalten von Port Security auf dem Switch vor unberechtigtem Zugriff schützen

Kann aus dem öffentlichen WLAN auf Dienste im Schulnetzwerk zugegriffen werden, ist es zwingend notwendig, dass sich die Benutzer an der Firewall oder beim Server, auf welchem die Dienste zur Verfügung gestellt werden, anmelden muss. Nur so kann nachvollzogen werden, wer auf einen Dienst zugegriffen hat und so kann auch gesteuert werden, dass nur berechnigte Benutzer auf einen Dienst zugreifen können.

Um sicherstellen zu können, dass nur berechnigte Benutzer auf einen Dienst zugreifen, müssen sich diese am Dienst authentisieren, beispielsweise durch den Einsatz von Zertifikaten, SecurID oder Benutzername und Passwort. Die Verbindung vom Endgerät zum Dienst über das WLAN muss verschlüsselt sein, damit die Daten bei der Übertragung nicht aufgezeichnet und mitgelesen werden können.

2.2.4 Zugriff auf das Verwaltungsnetzwerk

Wird von einem WLAN auf das Verwaltungsnetzwerk der IG KOMSG bzw. auf einen im Verwaltungsnetzwerk angebotenen Dienst zugegriffen, muss dieser Zugriff gemäss den Sicherheitsvorschriften der IG KOMSG zwingend mittels einer von der IG KOMSG angebotenen Lösung erfolgen (SSL-VPN, SSL).

Nur so kann die Forderung nach starker Authentisierung und Verschlüsselung der Daten in den oben beschriebenen Netzwerken erfüllt werden.

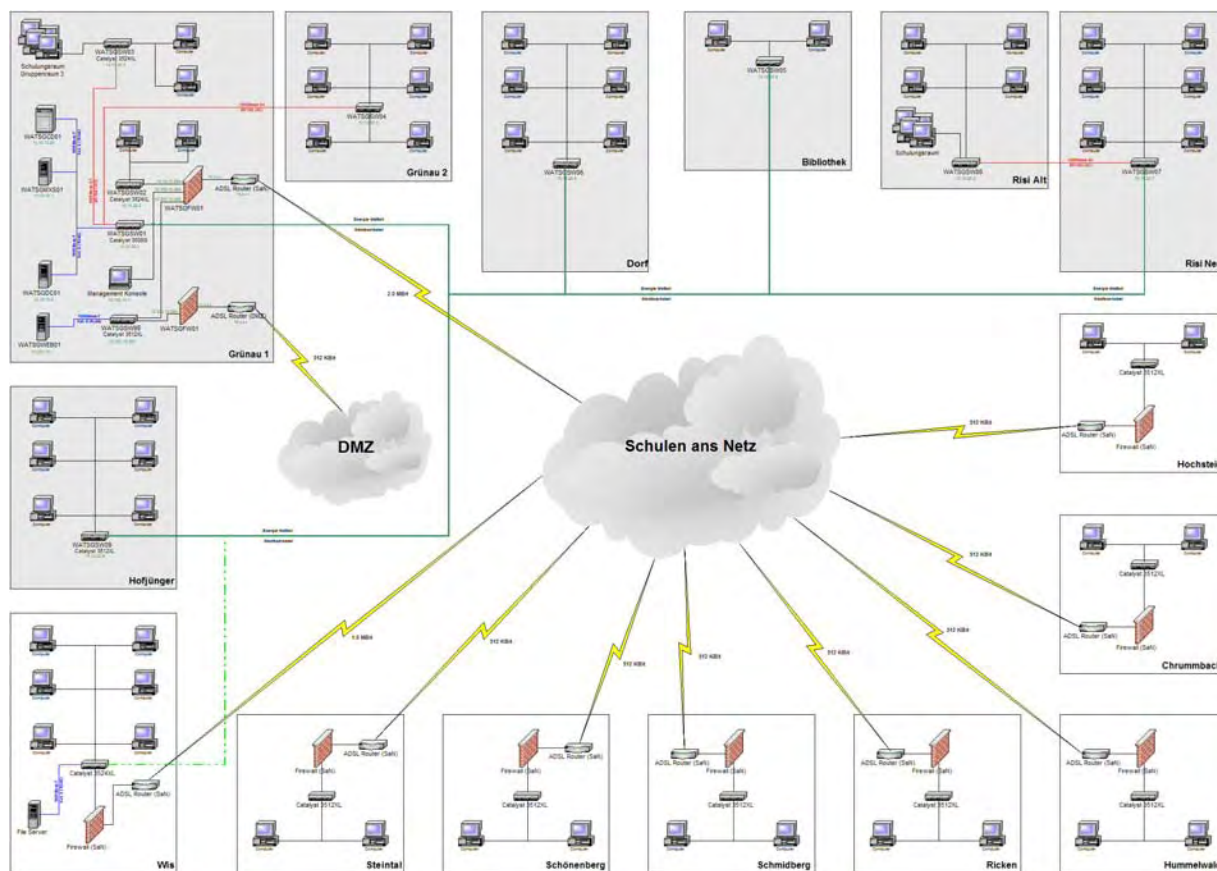
Technische Richtlinien WLAN (Funknetzwerk)

2.3 Beispiele

2.3.1 Volksschule Wattwil

In der Volksschule Wattwil werden im Moment zwei mobile Klassenzimmer mit Laptops eingesetzt. Mit dem mobilen Klassenzimmer wird je ein Access Point ausgefasst. Dieser wird, wenn benötigt am Netzwerk installiert (on demand). Dies hat zur Folge, dass die Strahlenbelastung sehr gering ist und nur kurze Zeit besteht. Als Sicherheitsmechanismen wurden eine SSID und ein WPA-Key zur Verschlüsselung installiert. Der Key wird halbjährlich gewechselt. Das WLAN ist nicht vom übrigen Netzwerk der Volksschule Wattwil getrennt.

Als WLAN-Standard wird im Moment 802.11b eingesetzt. Der Einsatz und die Migration auf 802.11g wird bei neuen Geräten ab dem Sommer 2004 in Erwägung gezogen.

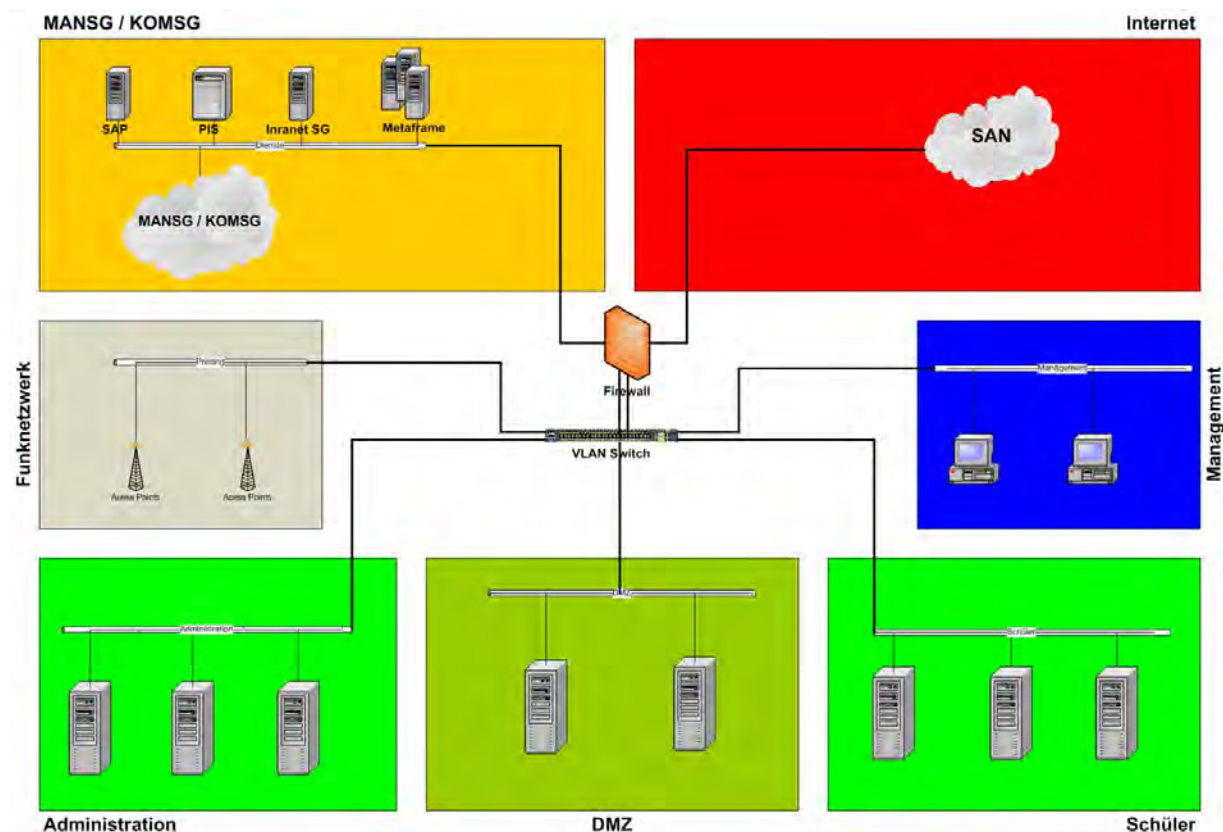


Technische Richtlinien WLAN (Funknetzwerk)

2.3.2 Berufs und Weiterbildungszentrum Toggenburg

Im BWZ Toggenburg werden im Moment drei mobile Klassenzimmer mit Laptops eingesetzt. Mit dem mobilen Klassenzimmer wird je ein Access Point ausgefasst. Dieser wird, wenn benötigt am Netzwerk installiert (on demand). Des weitern sind auf allen Etagen fixe Access Points montiert. Als Sicherheitsmechanismen wurden eine SSID und ein WPA-Key zur Verschlüsselung installiert. Der Key wird vierteljährlich gewechselt. Zusätzlich ist das WLAN in einem eigenen VLAN installiert und vom Rest des Netzwerks über eine Firewall getrennt. Zukünftig soll es für Berufsschüler auch möglich sein, sich über ihre eigenen Laptops ins Schulnetzwerk einzubinden. Im Verwaltungsnetzwerk wird kein WLAN eingesetzt.

Als WLAN-Standard wird im Moment 802.11b eingesetzt.



Technische Richtlinien WLAN (Funknetzwerk)

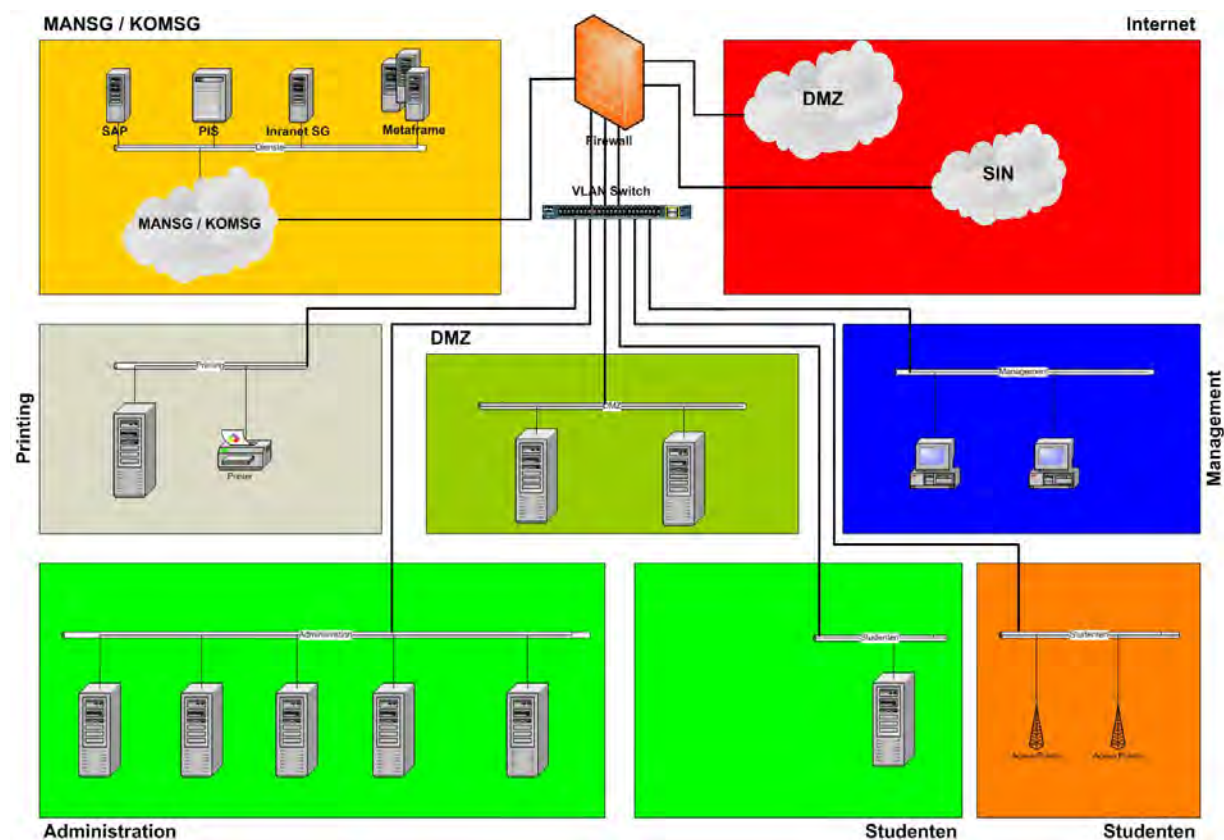
2.3.3 Pädagogische Hochschule Rorschach

In der PHR wird das WLAN als „öffentliches Netzwerk“ verwendet. Alle Studenten und Dozenten haben freien Zugang zum Studentennetzwerk. Laptops gehören zum Standard im Unterricht. Es wird kein WPA Key oder Ähnliches zur Authentifizierung oder Verschlüsselung eingesetzt. Dies vermindert den Support auf ein Minimum. Einzige Sicherheitsmassnahme ist, dass das WLAN in einem eigenen VLAN installiert ist und vom Rest des Netzwerks über eine Firewall getrennt wird. Im Vollausbau werden ca. 100 Access Points fix installiert sein.

Neu wird das Management der Access Points über eine Software durchgeführt. Diese Software erkennt räumlich an welchen Standorten sich die einzelnen Access Points befinden und kalibriert diese für eine flächendeckende Abdeckung automatisch.

Im Verwaltungsnetzwerk wird kein WLAN eingesetzt.

Als WLAN-Standard wird im Moment 802.11b eingesetzt. Die Migration auf 802.11a/g erfolgt im Mai 2004



3 Audit / Checkliste

Diese Checkliste kann sowohl für die Erstellung von WLANs oder für einen späteren Audit verwendet werden. Sie ist aber im Zusammenhang mit den weiteren Checklisten (Firewall, VLAN, usw.) der IG KOMSG oder anderen Stellen zu verwenden, da das Gesamtkonzept überprüft werden sollte.

	Ja	Teilweise	Nein	Bemerkung
01 Ist ein Inventar über die eingesetzten Netzwerkkomponenten vorhanden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
02 Besteht eine aktuelle Netzwerkdokumentation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
03 Ist ein aktuelles physisches oder logisches Netzwerkschema vorhanden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
04 Wird eine WPA-Verschlüsselung o.ä. eingesetzt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
05 Wird das senden der SSID unterdrückt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
06 Ist die neuste Firmware auf den Geräten installiert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
07 Sind die einzelnen Access Points vor Fremdmanipulationen geschützt.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8 Werden die Zugriffe und Zugriffsversuche auf die Netzwerkkomponenten aufgezeichnet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9 Wurde nach der Erstinstallation ein internes Audit durchgeführt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10 Wurde ein externes Audit durchgeführt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
11 Wird das Audit periodisch von intern oder von extern wiederholt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12 Sind alle Passwörter dokumentiert und an einem sicheren Ort hinterlegt (Safe)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
13 Wird das IT Personal über die möglichen sicherheitsrelevanten Probleme informiert und ausgebildet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
14 Werden für das gesamte WLAN Komponenten vom gleichen Hersteller eingesetzt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
15 Ist das WLAN von externen Standorten erreichbar?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16 Wurden Messungen für die Standortbestimmung der Access Points vorgenommen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
17 Sind alle Konfigurationen der Netzwerkkomponenten gesichert und dokumentiert?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
18 Entspricht die Installation den Richtlinien der IG KOMSG und den Vorgaben des Erziehungsdepartements?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

4 Glossar

Backbone	Das „Rückgrat“ des Datennetzes, ein Netz (oder mehrere Netze), das die Daten zwischen den lokalen Netzen weitergibt und somit die lokalen Netze verbindet
Broadcast	Rundsendung „an alle“; Verfahren, um alle angeschlossenen Geräte in einem LAN anzusprechen
Campus-Bereich	Mit diesem Begriff bezeichnen wir ein Areal aus mehreren Gebäuden, das durch Anbindungen an ein lokales Zentrum leitungstechnisch erschlossen wird
DMZ	De- Militarisierte Zone, bezeichnet hier ein Netz, in dem via Internet erreichbare Server stehen, die deswegen besonderer Pflege und Wartung sowie besonderer Sicherheitsanstrengungen bedürfen.
Ethernet	Paketorientierte Netzwerktechnik, die davon ausgeht, dass alle Teilnehmer ein gemeinsames Medium „als Äther“ verwenden, siehe Kollision; führende Technik im LAN, Übertragungsgeschwindigkeit 10 Mbit/s; zunächst durch Switching - Techniken, dann durch Fast Ethernet auf 100 Mbit/s und Gigabit Ethernet auf 1.000 Mbit/s wurde der mögliche Datendurchsatz kontinuierlich erweitert
FDDI	Fiber Distributed Data Interface; alte Technologie des HD-Net, Ende der achtziger Jahre die führende sichere und mit 100 Mbit/s schnelle LWL- Datenübertragungstechnik in Ring-Topologie
Firewall	Netzwerkfilter, der Datenpakete bis zur Ebene der Nutzdaten hinauf analysieren und filtern/verändern kann. Eine Massnahme, bestimmte Aspekte der Rechner- und Netzwerksicherheit zentral bereitzustellen
http, https	HyperText Transfer Protocol, Port 80/tcp, http-secure, Port 443/tcp. Das Protokoll, mit dem die Daten der Web-Seiten übertragen werden.
Hub, Konzentrat	einfacher Datensignalverteiler; eingehende Signale werden verstärkt und an alle angeschlossenen Geräte weitergegeben, an alle Ausgänge wird dasselbe Signal ausgegeben, das Netz wird von allen geteilt. Wer in einem solchen „shared network“ einen Rechner dazu bringen kann, den Datenverkehr an der Netzwerkkarte abzuhorchen, der hört allen Datenverkehr im ganzen Netz mit.
Internet-Dienste	Heute vor allem WWW, Email, aber auch Usenet-Diskussionsforen, zukünftig verteilte Datenbanken, Verzeichnisdienste, Multimedia-Angebote...
Intranet	Meist ein firmeninternes Netz, das besonders gegen das Internet abgeschottet ist und nicht die volle Internet-Funktionalität bietet.
IP, IPv4/6	Internet Protocol; früher vor allem zur Anbindung zwischen LANs entwickelt, ist es heute das auch im LAN führende Protokoll. IPv6 ist die erweiterte Version von IP, wird bislang nur im Probebetrieb eingesetzt
IPSec	IP Secure, verschlüsselte Version von IP, im IPv6-Standard enthalten, kann von modernen Komponenten auch unter/neben IPv4 eingesetzt werden
KOMSG	Kommunikationsnetzwerk des Kantons St. Gallen
L2, L3, L4	Layer 2/3/4, bezieht sich auf die Schichten des Datentransports gemäss dem OSI - Modell; siehe OSI; ein moderner Switch-Router kann auf allen diesen Ebenen arbeiten

Technische Richtlinien WLAN (Funknetzwerk)

LAN	Local Area Network; auf einen Nahbereich (z. B. ein Gebäude) beschränktes Netzwerk, z. B. in der Regel ein Institutsnetz
LWL	Lichtwellenleiter oder auch Glasfaser allgemein; wir unterscheiden Multi-Moden- (oder auch Gradienten-) Fasern (MMF) für kürzere Strecken mit relativ günstigeren Komponenten von den Singlemode-Fasern (SMF) für längere Strecken, mit relativ teureren Komponenten
MAN	Metropolitan Area Network; Netzwerk, das z. B. über eine Stadtfläche verteilt ist, und das viele LANs direkt anbindet
MANSNG	siehe KOMSG
Multimedia	Um Multimedia-Daten (Sprache, Bild...) z. B. ohne all zu grosse zeitliche Verzerrungen (siehe QoS) oder mit definierten (z. T. hohen) Bandbreiten übertragen zu können, wurden verschiedene Protokolle entwickelt, z. B. für Ressourcen-Reservierung, Multicasting-Verfahren für live-Sendungen, Streaming-Protokolle für „on-demand“-Abrufe
Netzwerk-Management	alle Tätigkeiten, die die Verwaltung, Überwachung und Instandhaltung der aktiven Komponenten (Router, Switches, Hubs) und der damit betriebenen Datenetze betreffen
OSI	Open Systems Interconnection, nur noch theoretisch genutztes Standardmodell der Datenübertragung, teilt den Übertragungsvorgang von der Anwendung (Layer 7) bis zum Kabel (Layer 1) in Schichten/Ebenen/Layer ein Paketfilter Netzwerkfilter, der bis zur Ebene der Transportdaten (Layer 4) analysieren und filtern kann; vergleiche Firewall
Peer-to-peer	Über das Internet hergestellter Anwendungsverbund, in dem jeder Rechner Client wie Server ist. Unter Verzicht auf zentrale Serverstrukturen wird ein dezentraler Datenaustausch zwischen den Nutzern betrieben.
Router	Datensignalverteiler zur Verbindung zwischen Subnetzen; muss die (z. B. TCP/IP- und IPX-) Adressfelder der Datenpakete („Layer 3“) sehr schnell lesen und auswerten können, trifft die Entscheidung, welche „Route“ ein Datenpaket nimmt; typischerweise die teuerste Komponente im Netz
Server	Rechner, der für andere Rechner über Netzwerk erreichbare Dienste bereitstellt.
ssh	Secure Shell; Anwendungsprogramm bzw. Serverdienst, das/der verschlüsseltes Arbeiten über das Datennetz ermöglicht, und dabei auch die „Identität“ des Servers überprüfen kann. Insbesondere sind hiermit auch - im Gegensatz zu telnet oder ftp - die Passwörter verschlüsselt, und werden - bei richtiger Handhabung - nur an den erwünschten Zielrechner vermittelt.
smtp	Simple Mail Transport Protocol, Port 25
Social Engineering	Informationsbeschaffung über ein Angriffsziel durch Ausfragen von Nutzern
Spam-Mail	unerwünschte Werbemails, die in grossen Mengen versendet werden
Strukturierte Verkabelung (UGV)	Verkabelungs-Norm, die, grob gesprochen, eine einheitliche Verkabelungsstruktur gemäss der Aufteilung in die drei Bereiche Campus/Backbone (LWL), Gebäudeverteilung/Steigbereich (LWL) und Stockwerksverteilung/Endanbindung (TP-Kupferkabel) vorschreibt. Eine solche Struktur ist auch unter Sicherheitsaspekten sinnvoll, zum Beispiel für die Betriebssicherheit.

Technische Richtlinien WLAN (Funknetzwerk)

Switch	Datensignal-Verteiler für ein Subnetz (oder mehrere, bei VLAN-fähigen Geräten), schaltet direkt auf „Layer 2“ zwischen den beteiligten Anschlüssen durch, dadurch ist im „switched network“ Möglichkeit kleiner, den Datenverkehr abzuhören. Durch entsprechende Konfiguration kann hier viel erreicht werden.
TCP/IP	Transport Control Protocol / Internet Protocol, die Standard-Regeln, um Daten mittels Datenpaketen zwischen Netzwerken transportieren zu können; der Standard zunächst im Internet, heute auch im LAN
Topologie	bezeichnet in diesem Zusammenhang die Art der Verbindung der Netzknoten in der grösseren Struktur, man unterscheidet hier Ring-, Stern- und Bustopologie
TP-Kabel	(UTP: unshielded, STP: shielded) twisted pair: Paarweise verdrehte abgeschirmte Kabel, kupferbasierte Kabeltechnik, 4 Paare werden in einem Kabel verlegt. Abhörmöglichkeit bei STP geringer
Unicast	Sendung „an einen“; direktes Ansprechen des Empfängers durch eine pazifische Adresse
USV/UPS	Unabhängige Strom-Versorgung / Uninterruptible Power-Supply: Netzteil mit Batterie, das die Stromversorgung bei einem Stromnetz-Ausfall aufrecht erhält, Element zur Erhöhung der Betriebssicherheit.
VLAN	Virtuelles LAN; Zusammenschaltung räumlich getrennter Bereiche zu einer, einem lokalen Netz (LAN) vergleichbaren Einheit; meist wird die Norm IEEE 802.1Q gemeint/erfüllt
VLAN-trunk	bezeichnet die Möglichkeit, die Signale mehrerer VLANs über eine gemeinsame Leitung zu geben, die dann zur Endverteilung entsprechenden Ausgängen zugeordnet werden; dies wird mittels Markierungen („tags“) der Datenpakete erreicht (VLAN- tagging)
VoIP	Voice over IP, von manchen Herstellern bereits verwirklichtes Konzept, Telefonie über Datenleitungen direkt zu betreiben. Um hier Störungen und Abhören bestmöglich auszuschliessen, sind detaillierte Konfigurationen der beteiligten Netzkomponenten nötig.
VPN	Virtuelles Privates Netzwerk, im Gegensatz zum VLAN wird hier mehr Wert auf Sicherheit/Nichtabhörbarkeit gelegt; kann z. B. mit IPSec umgesetzt werden
WAN	Wide Area Network; Weitverkehrsnetz über grosse Strecken, z.B. zwischen Städten oder Schulen
WEP	Wired Equivalent Privacy WEP ist Teil des IEEE WLAN-Standards 802.11 und bietet einen Basis-Schutz der übertragenen Daten, ähnlich demjenigen in einem herkömmlichen LAN. WEP gilt heute als unsicher und kann rasch geknackt werden.
WLAN	Wireless LAN; drahtlose Netzwerktechnologie mit Reichweite 25-200 Metern Alle Wireless-Techniken können im Prinzip leichter abgehört werden als kabelgebundene Verfahren, daher muss hier Wert auf Verschlüsselung gelegt werden.

Technische Richtlinien WLAN (Funknetzwerk)

WPA	Wi-Fi Protected Access WPA arbeitet für den Schutz des Zugriffs auf das Netzwerk entweder mit vordefinierten Schlüsseln (Pre-Shared Keys PSK, WPA-PSK) oder authentisiert die Benutzer basierend auf dem Standard 802.1X auf einem RADIUS-Server (WPA-Enterprise) mittels Zertifikat oder SecurID. Für die Verschlüsselung wird TKIP verwendet, dieses Verfahren basiert auf WEP, es wird aber für jedes Datenpaket kryptographisch ein neuer Schlüssel erzeugt.
WPA2	Entspricht dem Standard IEEE 802.11i Bei WPA2 ist es möglich die Daten für die Übertragung mit dem als sicher geltenden AES-Algorithmus zu verschlüsseln. WPA2 erfüllt alle zwingenden Anforderungen des Standards 802.11i, ist allerdings nicht mehr abwärts kompatibel zu WEP.
WWW	World Wide Web bezeichnet zunächst via http erreichbare Serverdienste, in denen vielfältige Informationsformate bereitgehalten und mittels Web-Browser abgerufen werden können. Für die einfache Vernetzung (web) sorgen dabei Verknüpfungselemente (links) und ein entsprechendes Adressformat (URL, Uniform Resource Locator). Für viele bedeutet die Nutzung von WWW-Diensten schlichtweg „das Internet.“

5 Weiterführende Informationen

Dokument „System- und Datensicherheit für Jedermann – Sicherheit in Funknetzwerken“
Einfaches Dokument vom Landesbeauftragten für den Datenschutz Niedersachsen, Deutschland.
Zielpublikum sind die Benutzer zu Hause, mit nur beschränktem Informatik-Knowhow.
http://cdl.niedersachsen.de/blob/images/C24074559_L20.pdf

Homepage „BSI für Bürger“

Homepage vom Bundesamt für Sicherheit in der Informationstechnik, Deutschland, die verschiedene Aspekte der Informationssicherheit verständlich beschreibt. Unter anderem auch die Sicherheit von WLAN (<http://www.bsi-fuer-buerger.de/wlan/index.htm>).

Dokument „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“
Vom Bundesamt für Sicherheit in der Informationstechnik, Deutschland. Sehr umfassendes Dokument, das nicht nur das Thema WLAN detailliert beschreibt.
<http://www.bsi.de/literat/doc/drahtkom/drahtkom.pdf>

Freigabe	Technische Richtlinien WLAN (Funknetzwerk) <small>Techn. Richtlinie WLAN V 3.1</small>	Erziehungsdepartement Kanton St.Gallen		Seite 18 von 18
		Datum 01.09.2007	Version 3.1	