8. Sicherheit Internetanbindung

Internet-Sicherheit ist ein sehr weiter Begriff. Er umfasst Themen wie

1. **Computer- und Netzsicherheit**, der Schutz der Infrastruktur vor Angriffen (Hacken, mutwillige automatisierte Überlastung, sowie Viren und anderem Schadcode)
2. **Datensicherheit**, der Schutz der Daten vor unerlaubtem Zugriff, Manipulation oder Verlust (Verschlüsselung, Datensicherung, etc.)
3. **Datenschutz**, der Schutz personenbezogener Daten vor Missbrauch (siehe Datenschutzgesetz)
4. **Schutz der Kinder, Jugendlichen und Lehrpersonen** vor problematischen Inhalten, problematischen Kontakten und Cybermobbing
5. **Schutz der Lehrer/innen und der Schule**, dass sie nicht in unangenehme und/oder rechtlich problematische Situationen geraten bzgl. der Internet-Nutzung in der Schule oder Internet-Einsatz im Unterricht (siehe Personalgesetz)
6. **Schutz der Schule** im Sinne, dass sie ihre Verantwortung bzgl. den obigen Punkten wahr nimmt.

Im Rahmen des Entwicklungsplans „Bildung im Netz 2010-2015“ wurde in erster Linie die Sicherheitsfragen des Internetzugangs betrachtet. da die Schulen ihre Internetanbindung den Lehrpersonen und Schüler/innen zur Verfügung stellen. Das Ergebnis dieser Arbeit sind die „Richtlinien Sicherheit Internet-Anbindung“ (siehe Anhang).

Stufengerechte Internet-Sicherheit

Die Internet-Sicherheit ist stufengerecht zu implementieren. Während ein volljähriger Schüler der Sekundarstufe 2 kaum vor Inhalten im Internet geschützt werden muss, sollen Kinderngartenkindern so gut wie nur möglich vor extremen Inhalten geschützt werden. Während die Sek2-Schüler/innen durchaus Hackeraktivitäten entwickeln können, ist dies bei Kindergartenkinder kaum zu erwarten. Wenn man von Internet-Sicherheit spricht ist es von Notwendig den Kontext zu klären von welcher Schulstufe gesprochen wird. Internet-Sicherheit ist stufengerecht zu betrachten.

Identitätsverwaltung, Authentisierung, Autorisierung, Abrechnung - IDAAA

Um den Zugang zum Internet und zu Ressourcen zu kontrollieren, wird ein System benötigt für die Identitätsverwaltung, Authentisierung, Autorisierung und evtl. für Abrechnungen benötigt.

Um eine bessere Vorstellung davon zu bekommen, was für Schulen ein geeignetes System ist, lohnt sich der metaphorische Vergleich wie der Zugang zu Ressourcen im Schulhaus.

Die Schule ist kein Flughafen und auch kein öffentlicher, rechtsfreier Raum. Es braucht keine Sicherheitsmassnahmen wie an einem Flughafen, wo jedes Paket durchleuchtet wird und jede Person mehrfach kontrolliert wird. Es ist aber auch nicht so, dass alle tun und lassen können was sie wollen. Und für einige Räume braucht es Schlüssel und der Zugang ist beschränkt auf Lehrpersonen. Vieles in der Schule geschieht über soziale Kontrolle, die Türen sind offen, doch wird geschaut ob man die Leute kennt. Ähnliches ist wünschenswert für die Nutzung des Internetzugangs und die Zugangskontrolle zu digitalen Ressourcen, Diensten und Anwendungen. Manchmal sind in den Schulen technische Umsetzungen zu finden die eher einem Eingangskontrollsystem eines Grossunternehmens erinnern oder dann ist der Internetzugang Tag und Nacht sperrangelweit offen,

beides ist so nicht zu empfehlen.

Unterscheidungen Internetzugänge und Zugangskontrolle

Für die Netzzugänge und die digitalen Räume muss unterschieden werden zwischen schulischem und persönlichem Internetzugang.

persönlicher Internetzugang
: Die Schule übernimmt keine Verantwortung für die Aktivitäten der Schüler/innen und Lehrpersonen, wenn diese persönliche Internetzugänge verwenden und sich in nicht-schulischen oder öffentlichen digitalen Räumen bewegen.

schulischer Internetzugang
: Die Schule übernimmt Schutz und zieht die SchülerInnen und Lehrpersonen zur Verantwortung für Aktivitäten die die Schüler/innen und Lehrpersonen in physischen oder logischen schulischen digitalen Räumen.

Die Netzzugangskontrolle kann (vereinfacht gesagt) auf drei Ebenen stattfinden, entweder durch das ICT-Gerät, das Betriebssystem oder das Web.

3) NZK Web
: ist die Art und Weise , welche digitalen Identitäten[1)] zu welchen digital-sozialen-Räumen Zugang haben (siehe Authentifizierung und Authorisierung z.B. AAI, Educa.ID, OpenID etc.)

2) NZK Betriebssystem
: Die Lehrperson oder Schüler/in meldet sich durch das Betriebssystem beim Netz an und hat damit meist zugang zu lokalen Ressourcen, Diensten und Anwendungen.

1) NZK ICT-Geräte
: Das ICT-Geräte der Lehrperson oder Schüler/in meldet sich an der IT-Infrastruktur an. Die Lehrperson oder Schüler/in hat damit Zugang zum Netz. Hier ist zu klären, welche Methode in den Schulen am einfachsten zu implementieren ist. (z.B. SSID + Passwort, MAC-Adresse, EAPOL(IEEE 802.1X)).

Aufgrund der im Orinertierungsbild aufgezeigten Entwicklungen ist tendenziell damit zu rechnen, dass die Netzzugangskontrolle auf der Ebene Web wichtiger wird und die Netzzugangskontrolle auf der Ebene Betriebssystem abnimmt.

Ein Netzwerkzugang ganz ohne Authentisierung sollte nicht mehr vorkommen. Jedoch kann in kleinen Schulen ein für die ganze Schule einheitliches Passwort für den Netzzugang zusammen mit der sozialen Kontrolle durchwegs genügen. In mittleren Schulen kann es auch über die Registrierung des Geräts gehen (z.B. MAC-Adresse). In grösseren Schulen ist die Implementierung einer komplexeren Netzwerkzugangskontrolle notwendig (z.B. eine Kombination aus Shibbolth und EAPOL).

Im Detail ist ideale Mischung aus technischer Lösung Abhängig von der Schulstufe und der Schulgrösse. Das folgende Diagramm bietet eine erste Orientierung.

	KGU	Mittelstufe	Sek1	Sek2
75	EducaID (optinal) SSID+PW	EducaID (optinal) SSID+PW	EducaID MAC-Adresse	
150	EducaID (optinal) SSID+PW	EducaID (optinal) SSID+PW	EducaID MAC-Adresse	Shibboleth EAPOL (802.1X)
300	EducaID (optinal) SSID+PW	EducaID (optinal) MAC-Adresse	EducaID EAPOL (802.1X)	Shibboleth EAPOL (802.1X)
600		EducaID (optinal) EAPOL (802.1X)	EducaID EAPOL (802.1X)	Shibboleth EAPOL (802.1X)
1200			EducaID EAPOL (802.1X)	Shibboleth EAPOL (802.1X)

Anonymität und Sichtbarkeit

Durch die digitalen Netze werden die Fragen von Anonymität und Sichtbarkeit neu aufgeworfen.

Schüler/inne und Lehrpersonen sollen im physischen (LAN) und logischen digitalen Raum (z.B. Lernplattform) der Schule bekannt sein. Die Schule unterstützt die Schüler/innen und Lehrpersonen beim Schutz der Privatsphäre im offenen Internet.

Der Schüler/in und die Lehrperson sind innerhalb des digital-sozialen Raumes der Schule nicht anonym (Ausnahmen, anonyme Abstimmungen etc.).

Zugangskontrolle bei Prüfungen

Eine der Fragen, die bezüglich Sicherheit und Netzwerk immer wieder auftauchen, ist, wie während Prüfungen der Zugang zu Ressourcen kontrolliert werden kann. Dies ist möglich durch Zugangsbeschränkung der Ressourcen oder/und Überwachung der Aktivitäten des Schülers und kann prinzipiell auf verschiedenen Ebenen geschehen. Eine 100% sichere technische Lösung ist durch realistischen Aufwand nicht realisierbar. Es ist eine Mischung aus sozialer und technischer Kontrolle notwendig.

In der folgenden Tabelle sind die verschiedenen Ebenen, auf denen die Zugangsbeschränkung durchgeführt werden kann, aufgezeigt.

Beschränkung durch …	**Für die Prüfung wird …**	**benötigt …**	**zu bedenken …**
Prüfungs-Netz	der Zugang für bestimmte Benutzer zum Internet für eine bestimmte Zeit beschränkt.	dass der Schüler oder sein Gerät sich beim Netz anmelden muss	Persönlicher Netzzugang (z.B. über UMTS) ist unkontrolliert.

Beschränkung durch …	Für die Prüfung wird …	benötigt …	zu bedenken …
Prüfungs-Gerät	ein Prüfungs-Gerät abgegeben oder ein Informatikzimmer mit Prüfungs-Geräten eingerichtet, bei denen der Zugang ins Internet beschränkt ist.	von der Schule gewartete Geräte	.
Prüfungs-Betriebssystem[2)]	ein Prüfungs-Stick oder ein Prüfungs-Image verteilt und ein Prüfungsbetriebssystem auf dem persönlichen ICT-Gerät gestartet.	USB-Stick-Ladestationen, Geräte der Schüler müssen von USB-Stick oder DVD-Laufwerk starten können	
Prüfungs-Browser[3)]	ein Prüfungs-Browser auf den persönlichen Geräten der SchülerInnen in ge'timeten Kioskmodus gestartet		Prüfungen müssen vollständig innerhalb eines Browsers durchführbar sein.

Bei all diesen Varianten, kann der Schüler nicht mit seiner gewohnten Lernumgebung arbeiten, bei der er unbeschränkten Zugang zu einem breiten Wissen der Menschheit hat. Deshalb und aus pädagogischen Gründen ist auch zu überlegen, inwieweit die klassische Vorstellung von Wissens-Prüfungen, in der Einzelpersonen ihr Wissen Nachweisen müssen aufrecht erhalten werden kann und soll.

Weitere Aspekte der Internet-Sicherheit

Alle weiteren Sicherheitsaspekte sind in weiterführenden Arbeiten zu klären (siehe auch Handlungsfelder).

1)
Schüler/innen und Lehrpersonen

2)
der Lernstick der FHNW http://www.imedias.ch/lernstick, könnte mit etwas Aufwand in einen Prüfungs-Stick umgebaut werden.

3)
siehe z.B. den Safe Exam-Browser http://www.safeexambrowser.org .