8. Sicherheit Internetanbindung

Dieses Kapitel zum Thema Internet-Sicherheit entstand einerseits aufgrund der neu entstehenden Kosten für die Web-Content-Screening-Dienstleistung bei den SAI-Angeboten der Swisscom und andrerseits aufgrund der Diskussion rund um das Thema Internet-Sicherheit an vielen Schulen. Die Schulen stehen vor der Entscheidung, für diese Dienstleistung der Swisscom zu bezahlen, sie selbst zu erbringen, sie von einem anderen Anbieter einzukaufen oder darauf zu verzichten.

Im Rahmen dieses Entwicklungsplans haben wir deshalb in erster Linie die Sicherheitsfragen des Internetzugangs betrachtet. Die Schulen stellen ihre Internetanbindung den Lehrpersonen und Schüler/innen zur Verfügung und tragen somit eine Mitverantwortung. In zweiter Linie wurde versucht zur weiteren Klärung der Diskussion rund um Internet-Sicherheit aus einem schulspezifischen Blickwinkel beizutragen.

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

1. **Computer- und Netzsicherheit**: Schutz der Infrastruktur vor Angriffen wie Hacken, mutwillige automatisierte Überlastung, sowie Viren und anderem Schadcode.
2. **Datensicherheit**: Schutz der Daten vor unerlaubtem Zugriff, Manipulation oder Verlust.
3. **Datenschutz**: Schutz personenbezogener Daten vor Missbrauch (siehe Datenschutzgesetz).
4. **Schutz der Kinder, Jugendlichen und Lehrpersonen**: Schutz vor problematischen Inhalten, problematischen Kontakten und Cybermobbing.
5. **Schutz der Lehrer/innen und der Schule**: Schutz vor unangenehmen und/oder rechtlich problematischen Situationen aufgrund der Internet-Nutzung in der Schule (siehe Personalgesetz)

Die Schule ist kein Flughafen und auch kein 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. Die Erarbeitung einer schulspezifischen Internet-Sicherheit ist eine ungelöste Aufgabe. Im Folgenden sind dazu einige Orientierungspunkte zu finden.

8.1 Stufengerechte Internet-Sicherheit

Die Internet-Sicherheit ist stufengerecht zu betrachten und umzusetzen.

Während eine volljährige Schülerin oder ein volljähriger Schüler der Sekundarstufe 2 kaum vor Inhalten im Internet geschützt werden muss, sollen Kindergartenkindern so gut wie nur möglich vor nicht-altersgerechten Inhalten geschützt werden. Während die Sek2-Schüler/innen durchaus Hackeraktivitäten entwickeln können, ist dies bei Kindergartenkinder kaum zu erwarten. Wenn von Internet-Sicherheit gesprochen wird, ist es wichtig klar zustellen, von welcher Schulstufe gesprochen wird.

Bezüglich der Zugangsbeschränkung auf Inhalte ist für den Kindergarten und die Primarstufe somit die Wahl des Web-Content-Screenings des SAI-Angebotes oder eines äquivalenten Angebotes empfehlenswert. Für die Schulen der Sekundarstufe 1 sind Verfahren, die auf einer einfachen Ressourcen-Filterung basieren angemessen. An den Schulen der Sekundarstufe 2 kann eine massvolle Ressourcen-Filterung die Diskussion vereinfachen. Es kann aber auch ganz auf die Filterung von Inhalten verzichtet werden.

8.2 Nicht-Anonymität in digitalen Schulräumen

Alle Personen sind innerhalb der digital-sozialen Räumen der Schule bekannt, d.h. nicht anonym[1)]. Sie können Gäste mitbringen.

Alle Personen sollen innerhalb des schulischen Netzes und der schulischen digitalen Räume (z.B. Lernplattform) der Schule bekannt sein. Die Schüler/innen und Lehrpersonen können temporär Gäste mitbringen. Die Schule unterstützt die Schüler/innen und Lehrpersonen beim Schutz der Privatsphäre im offenen Internet und kann dazu auch die Daten der Schüler/innen und Lehrpersonen anonymisieren.

Die technischen Verfahren sind einfach, benutzerfreundlich und bzgl. Aufwand der Schule angemessen zu wählen. D.h. in sehr kleinen Schulen kann es zum Beispiel durchaus angemessen sein, dass die Nicht-Anonymität über die soziale Kontrolle garantiert wird und alle Schüler/innen und Lehrpersonen die selben Anmeldungsdaten verwenden.

8.3 Identitätsverwaltung, Authentisierung, Autorisierung, Abrechnung

Die Gemeinde, ein Verbund von Schulen, der Kanton oder ein Verbund von Kantonen stellen die Infrastruktur zur Identitätsverwaltung, Authentisierung und Autorisierung zur Verfügung. Idealerweise ist ein solche Infrastruktur föderiert.

Um die Nicht-Anonymität, sowie die Zugangskontrollen zum Internet, sowie anderen Ressourcen als Schule wahrnehmen zu können, wird ein System für die Identitätsverwaltung, Authentisierung, Autorisierung benötigt. Es ist zu klären, welche Rollen, die verschiedenen Teilnehmer (Schulen, Gemeinden, Kanton, Kantonsverbunde) bei der Bereitstellung einer solchen Dienstleistung übernehmen. In einem späteren Schritt kann ein solches System um Abrechnungsverfahren erweitert werden, zum Beispiel um die Photokopierkosten zu verrechnen.

8.4 Zugangskontrolle zu Internet, Anwendungen und Ressourcen

Die Schulen sind verantwortlich für die Zugangskontrolle bei allen schulischen Anwendungnen und Ressourcen.

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

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.

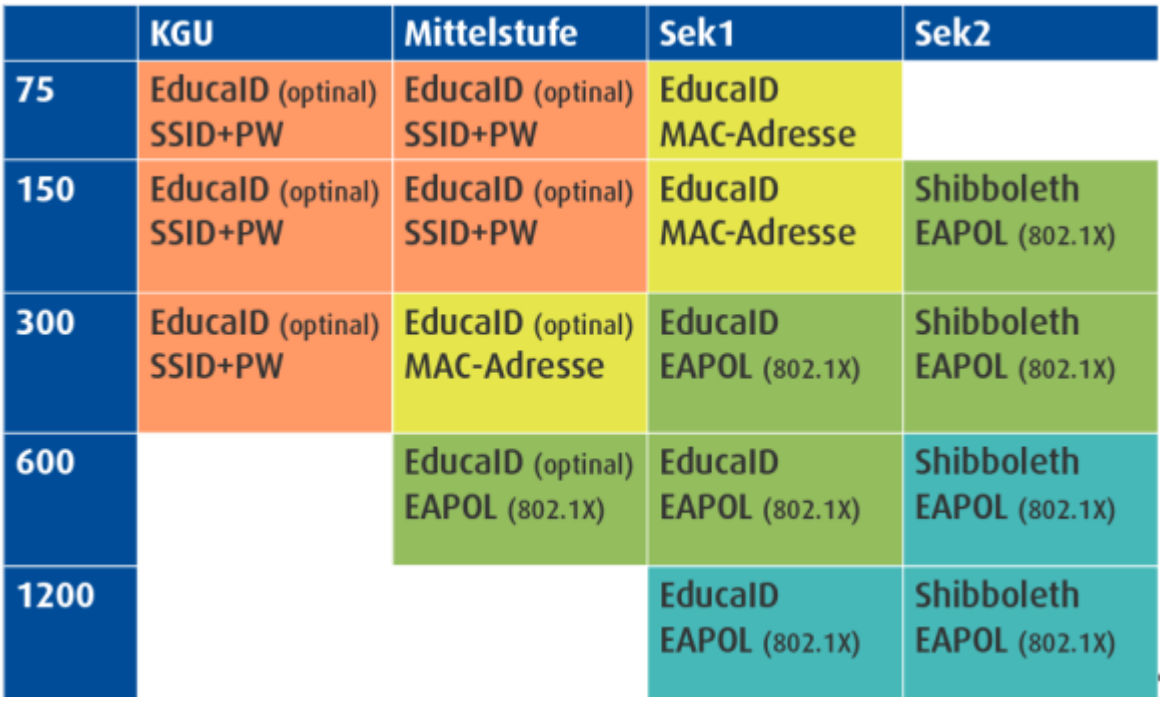
schulischer Internetzugang
: Die Schule übernimmt den Schutz und zieht die SchülerInnen und Lehrpersonen zur Verantwortung für deren Aktivitäten in schulischen digitalen Räumen.

Die Netzzugangskontrolle kann technisch (vereinfacht gesagt) auf verschiedenen Ebenen stattfinden, entweder durch das ICT-Gerät, das Betriebssystem oder den Browser.[2)]

Zugangskontrolle über …	**Beschreibung**	**Mögliche technische Verfahren**
Browser	Die Lehrperson oder Schüler/in meldet sich mit dem Browser direkt bei digital-sozialen Räumen und anderen Ressourcen an.	z.B. Switch-AAI, Educa.ID, OpenID etc.
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.	z.B. Active Directory + Kerberos
ICT-Gerät	Das persönliche ICT-Geräte der Lehrperson oder Schüler/in meldet sich am lokalen Netz an. Der Besitzer hat damit Zugang zum Netz, Internet und weiteren Ressourcen.	z.B. SSID + Passwort, Registrierung MAC-Adresse, EAPOL (IEEE 802.1X + Radius).

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 der Zugang über die Registrierung des ICT-Geräts kontrolliert werden (z.B. MAC-Adresse). In grösseren Schulen ist die Implementierung einer komplexeren Netzwerkzugangskontrolle notwendig (z.B. eine Kombination aus Shibbolth und EAPOL).

Das folgende Diagramm bietet eine erste Orientierung. Im konkreten Fall ist eine sinnvolle Mischung aus technischer und sozialer Kontrolle abhängig von der Schulstufe und der Schulgrösse zu wählen.



8.5 Zugangskontrolle bei Prüfungen

Eine häufige Frage bezüglich Sicherheit und Netzwerk 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 …	**Beschreibung**	**Mögliche technische Verfahren**	**Bemerkungen**
Prüfungs-Browser	Für die Prüfung wird ein Prüfungs-Browser auf den persönlichen Geräten der SchülerInnen in getimeten Kioskmodus gestartet.	Safe Exam-Browser [3)]	Prüfungen müssen vollständig innerhalb eines Browsers durchführbar sein.
Prüfungs-Betriebssystem	Für die Prüfung wird ein Prüfungs-Stick oder ein Prüfungs-Image verteilt und ein Prüfungsbetriebssystem auf dem persönlichen ICT-Gerät gestartet.	Prüfungs-Image auf USB-Stick oder DVD.[4)]	Geräte der Schüler müssen von USB-Stick oder DVD-Laufwerk starten können. Einrichtung um Prüfungs-Sticks oder Prüfungs-DVDs vorzubereiten.
Prüfungs-Gerät	Für die Prüfung wird ein Prüfungs-Gerät abgegeben oder ein Informatikzimmer mit Prüfungs-Geräten eingerichtet, bei denen der Zugang ins Internet beschränkt ist.	Prüfungsgerät	_
Prüfungs-Netz	Für die Prüfung wird der Zugang für bestimmte Benutzer zum Internet und andere Ressourcen für eine bestimmte Zeit beschränkt.	Firwall-Funktionalität	Persönlicher Netzzugang (z.B. über UMTS) ist unkontrolliert.

Bei all diesen Varianten kann der Schüler nicht mit seiner gewohnten Lernumgebung arbeiten, bei der er unbeschränkten Zugang zum breiten Informationsangebot im Internet hat. Die Schulen müssen sich überlegen, inwieweit die klassische Vorstellung von Wissens-Prüfungen aufrecht erhalten werden soll, in der Einzelpersonen ihr Wissen nachweisen müssen.

8.6 Weitere Aspekte der Internet-Sicherheit

Alle weiteren Sicherheitsaspekte sind in weiterführenden Arbeiten zu klären (siehe auch Anhang und

Handlungsfelder).

[1)]

Ausnahmen: anonyme Abstimmungen, Unterrichtsbefragungen etc.

[2)]

Der Browser ist hier als exemplarische Anwendung zu verstehen, die selben Methoden der Zugangskontrolle können auch von anderen Applikationen durchgeführt werden.

[3)]

siehe http://www.safeexambrowser.org

[4)]

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