
Swisscom Schulen ans Internet

Anleitung für eine sichere Nutzung des SAI Internetanschlusses

Aarau, 15. August 2010

Information aufgrund des neuen Swisscom Angebotes 2010

Mit dem neuen Angebot von Swisscom, welches die Nutzung hoher Bandbreiten ermöglicht, ändern Verantwortlichkeiten bei der Gewährleistung der Sicherheit des Internetzugriffs und Schulnetzwerks. Im neuen Swisscom - Angebot "Connectivity only" mit am lokalen Standort der Schule höchst möglichen Bandbreite ist die im Standardangebot von Swisscom kostenlos enthaltene Dienstleistung "Firewall und Inhaltsfilter" zur Gewährung der Sicherheit nicht mehr inbegriffen.

Massnahmen zur Gewährung der ICT Sicherheit an der Schule und beim Internetzugang der Schule sind obligatorisch.

Bei Bandbreiten bis 6'000/600 kbps übernimmt Swisscom im Standardangebot also weiterhin kostenlos den Schutz der Schule und deckt dabei die wichtigsten Anforderungen ab. Beim Wechseln zum Angebot "Connectivity only" hat die Schule verschiedene Möglichkeiten die Sicherheit zu gewährleisten:

Variante 1: Sicherheit kostenpflichtig durch die Swisscom

Variante 2: Betreiben der sicherheitsrelevanten Komponenten durch die Schule selbst oder eine beauftragte Drittfirma

Dieses Dokument gibt einige praktische Hinweise, die bei der Umsetzung eines sicheren Internetzugangs hilfreich sein können. Es dient als erläuternde Ergänzung zur „Checkliste für die Sicherheit des Internetzugangs“.

Die notwendigen Massnahmen werden für beiden Varianten vorgestellt mit Angabe der benötigten Komponenten. Sie finden Hinweise worauf bei einer eigenen Implementierung geachtet werden muss sowie auch konkrete Produktvorschläge. Die erwähnten Produkte stellen lediglich eine Auswahl aktuell möglicher Geräte dar. Selbstverständlich können auch andere Produkte dieselben Funktionen bieten. Beim Betreiben der sicherheitsrelevanten Komponenten durch die Schule selbst empfehlen wir die Unterstützung von Fachpersonen in Anspruch zu nehmen.

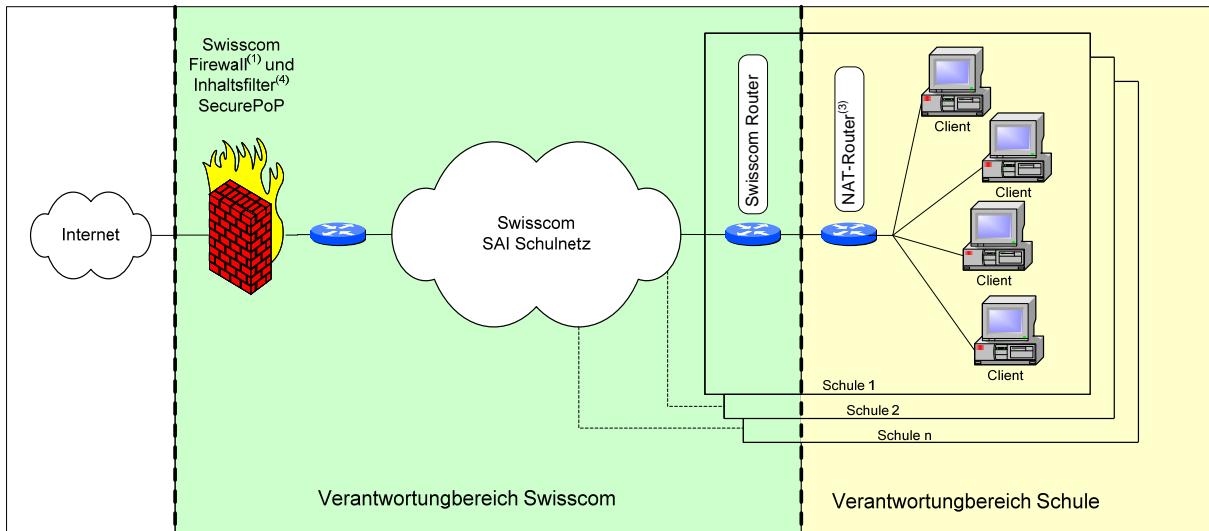
Neben rein technischen sind auch organisatorische Massnahmen zu treffen.

Inhalt:

Information aufgrund des neuen Swisscom Angebotes 2010	1
Firewall ⁽¹⁾	4
NAT-Router ⁽³⁾	4
Inhaltsfilter ⁽⁴⁾	4
Regelmässige Wartung und Aktualisierung der schulinternen Clients und Server ⁽⁵⁾	5
Betrieb eines aktuellen Virenschanners auf allen schulinternen Clients und Servern ⁽⁶⁾	5
Vereinbarung zum Umgang mit dem Internet und der ICT-Infrastruktur für Schülerinnen, Schüler, Eltern und Lehrpersonen ⁽⁷⁾	6
Exakte Dokumentation der Firewall- und Inhaltsfilter - Konfigurationen ⁽⁸⁾	6
Schutz der Systeme/Konfigurationen durch genügend komplexe Kennwörter ⁽⁹⁾	7
Nützliche Links ICT Sicherheit.....	7

Variante 1:

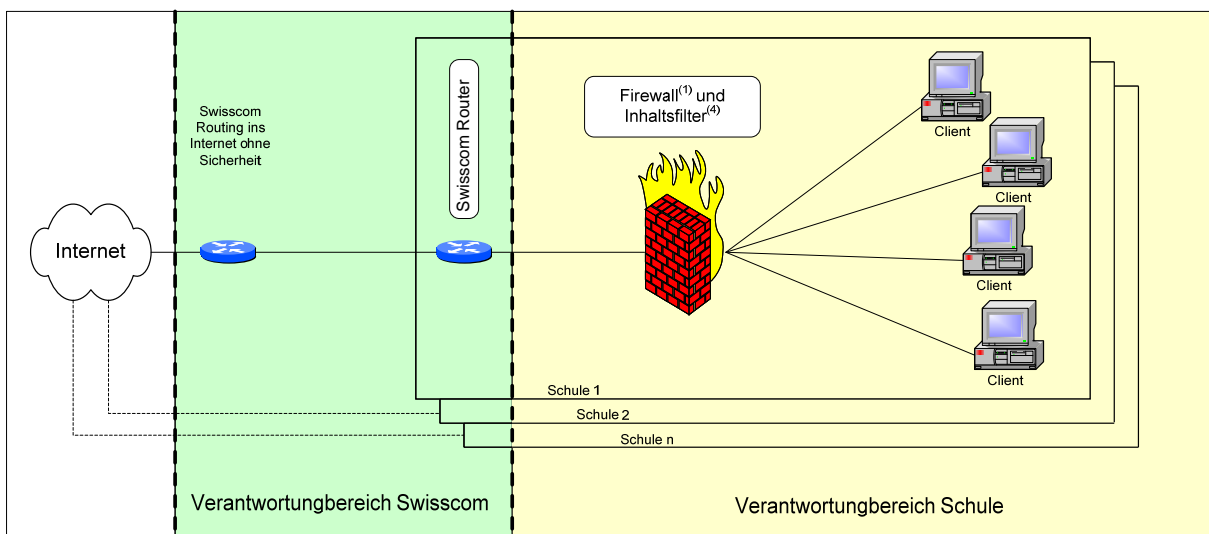
Die Swisscom bietet einen guten Schutz, kann jedoch nicht ganz alle Anforderungen selbst erfüllen. Die folgende Grafik zeigt die verschiedenen Komponenten sowie wer jeweils die Verantwortung dafür trägt:



Swisscom betreibt die Firewall und filtert den Internetverkehr auf unerwünschte Inhalte. Die Schule erhält einen IP-Adressbereich in einem Subnetz des in sich geschlossenen Swisscom Schulnetzes. Die Schule muss einen NAT-Router einsetzen, welcher das schulinterne Netz von den anderen Schulen im Swisscom-Netz trennt. Swisscom bietet diesen Dienst auf ihren Routern nicht.

Variante 2:

Verzichtet die Schule auf den Schutz durch die Swisscom, muss ein Firewall, möglichst mit Inhaltsfilter, in der Schule betrieben werden.



Swisscom stellt nur die Verbindung ins Internet zur Verfügung. Die Schule erhält öffentlich im Internet sichtbare IP-Adressen. Die Verantwortung über die Sicherheitskomponenten liegt bei der Schule.

Firewall ⁽¹⁾

Eine Firewall ist erforderlich um die internen Netzstrukturen zu verbergen und auch um ein- und ausgehende Verbindungen gezielt zuzulassen oder zu unterbinden (Firewall-Regeln⁽²⁾). Es muss darauf geachtet werden wirklich nur die benötigten ausgehenden Verbindungen zuzulassen. Eingehende Verbindungen sollten im Normalfall generell verboten werden. Eine Firewall sollte Verbindungsversuche protokollieren, um mögliche Probleme auch im Nachhinein identifizieren zu können. Network-Mapping (siehe auch NAT-Router bei „Sicherheit durch die Swisscom“) ist in einer Firewalllösung in der Regel ebenfalls eingeschlossen.

Bei kleineren Schulen mit bis etwa 10 Computern empfiehlt sich beispielsweise ein ZyXEL ZyWALL 2 plus. Dieses Gerät bietet die grundlegenden Funktionen und kann bis zu 34Mbps filtern. Ein weiterer Vorteil dieses Gerätes ist das verfügbare Abonnement für Inhaltsfilterung. Grösseren Schulen könnten auf eine ZyXEL ZyWALL USG 200 (bis 50 Benutzer) oder 300 (bis 75 Benutzer) setzen. Sollte dies nicht ausreichen gibt es verschiedene Security-Gateways, die auch mit sehr viel mehr Benutzern umgehen könnten. Beispiele eines solchen Gateways sind der Astaro Web Security Gateway, oder der als Open-Source frei erhältliche Gateway "Untangle".

NAT-Router ⁽³⁾

Ein NAT-Router ist erforderlich um die internen Netzstrukturen zu verbergen und auch um eingehenden Verbindungen zu verhindern. Die Swisscom kann die Schulen technologiebedingt nicht voreinander schützen.

Das Gerät muss in der Lage sein die IP Adressen der internen Clients auf externe Adressen der Swisscom umzuschreiben. Wir empfehlen nur Geräte einzusetzen, die die internen IP-Adressen auf mehrere externe IP-Adressen umschreiben. Oft wird dies als Network-Mapping bezeichnet. Nur durch diese Konfiguration kann die bestmögliche Geschwindigkeit des Inhaltsfilters sichergestellt werden.

Auf dem Markt sind verschiedenste Router mit NAT-Funktionalität, die günstigsten sind bereits unter hundert Franken erhältlich. Jedoch bieten diese meistens nicht die nötige Performance und „Network-Mapping“.

ZyXEL verkauft einige Geräte, die die Anforderungen erfüllen. Der ZyWALL 2 Plus, aber auch die grösseren ZyWALL USG Geräte beherrschen Network-Mapping und bieten genügend Performance für kleinere und mittlere Schulen.

Als Alternative könnte auch ein Gerät der Cisco ASA - Serie eingesetzt werden. Diese sehr leistungsfähigen Firewalls bieten einen sehr hohen Datendurchsatz, sind jedoch etwas komplexer in der Konfiguration als die ZyWALL Geräte.

Inhaltsfilter ⁽⁴⁾

Der Inhaltsfilter (Content-Filter) soll die Schüler vor unerwünschten Webseiten schützen. Ein hundertprozentiger Schutz ist leider nicht möglich. Trotzdem ist dieser Filter eine wichtige

Komponente zum Schutz der Schülerinnen und Schüler und sollte unbedingt eingesetzt werden. Im Zusammenhang mit der " Vereinbarung zum Umgang mit dem Internet und der ICT-Infrastruktur für Schülerinnen, Schüler, Eltern und Lehrpersonen ⁽⁷⁾" wird ein ausreichender Schutz vor unbeabsichtigt angezeigten oder unerwünschten Inhalten erreicht. Meistens basieren Inhaltsfilter auf vorbereiteten Listen mit tausenden unerwünschten Webseiten. Hier muss darauf geachtet werden, dass auch deutschsprachige Seiten in diesen Listen gut abgedeckt sind und diese Liste regelmässig aktualisiert wird. Setzt man als Firewall eine ZyWALL ein gibt es die Möglichkeit einen „iCard Content Filter“ zu beziehen. Dieses Abonnement ist jeweils ein Jahr gültig und lässt sich einfach installieren. Es kann aus 52 Kategorien (Pornographie, Games, usw.) ausgewählt werden. Diese Kategorien werden ständig aktualisiert und auch schweizer URLs sind enthalten. Auch der Astaro Web Security Gateway oder Untangle bieten ähnliche Filter wo Kategorien einzeln gesperrt werden können. Alternativ kann der Inhaltsfilter auch auf einem anderen Gerät als der Firewall betrieben werden. Dabei ist es wichtig sicherzustellen, dass die Schüler immer über den Inhaltsfilter ins Internet gelangen und keine Möglichkeit haben diesen zu umgehen.

Regelmässige Wartung und Aktualisierung der schulinternen Clients und Server ⁽⁵⁾

Sobald ein Gerät eine Internetverbindung aufbaut können gefährliche Daten über diese Verbindung in die Schule gelangen. Aus diesem Grund soll auf den Computern nur Software genutzt werden, die vom Hersteller noch aktiv mit Sicherheits-Updates unterstützt wird. Diese Updates müssen möglichst rasch nach der Veröffentlichung installiert werden. Hierbei ist es wichtig, dass neben dem Betriebssystem auch die anderen Komponenten nicht ignoriert werden. Dies gilt für alle Programme, die mit Daten aus dem Internet in Berührung kommen, unter anderem:

- Betriebssystem
- Internet-Browser-Plugins wie Adobe Flash
- Adobe Reader
- Multimedia-Player
- Microsoft Office

Auch andere Netzwerkgeräte wie Drucker, Kopierer, Switches und ähnliche Komponenten müssen regelmässig aktualisiert werden.

Wo verfügbar empfiehlt es sich die automatische Aktualisierung zu aktivieren. Für alle anderen Produkte muss regelmässig die Webseite des Herstellers auf Aktualisierungen geprüft werden. Sehr hilfreich ist in solchen Situationen ein Inventar der Geräte inklusive der installierten Produktversionen und der URL zum Herstellersupport. Siehe "Exakte Dokumentation der Firewall- und Inhaltsfilter - Konfigurationen ⁽⁸⁾"

Betrieb eines aktuellen Virenschanners auf allen schulinternen Clients und Servern ⁽⁶⁾

Trotz aller Vorsichtsmassnahmen können Viren in Dokumenten oder versteckt in Programmen aus dem Internet, Memory-Sticks oder CDs auf die Computer gelangen. Um die Viren so schnell als möglich zu erkennen und zu stoppen ist es unbedingt erforderlich

einen aktuellen Virenschanner auf jedem Computer zu installieren. Auch ist sicherzustellen, dass der Virenschanner die Virendefinitionsdateien laufend und möglichst automatisch aktualisiert. Periodisch müssen stichprobenartig einige Geräte geprüft werden ob die aktuelle Version der Virenschutz-Definitionsdatei installiert ist.

Es existieren auf dem Markt auch kostenlose Antivirusprogramme welche guten Schutz bieten. Beispiele für solche Software sind "Antivir", "Avast" oder "AVG" (nicht abschliessend). Um auch Spyware oder Malware zuverlässig zu entdecken reichen die kostenlosen Programme jedoch häufig nicht aus.

Vereinbarung zum Umgang mit dem Internet und der ICT-Infrastruktur für Schülerinnen, Schüler, Eltern und Lehrpersonen ⁽⁷⁾

"imediass", die Beratungsstelle für digitale Medien in Schule und Unterricht, hat eine Vorlage einer solchen Vereinbarung erarbeitet, welche von den Schulen ihren Bedürfnissen entsprechend angepasst und verwendet werden kann. Im Grundsatz geht es darum, dass Schülerinnen, Schüler und Eltern informiert sind über die an der Schule geltenden Regeln im Umgang mit ICT an der Schule. Mit ihrer Unterschrift bestätigen und akzeptieren sie dies.

Hauptthemen der Vereinbarung sind.

- Wir nutzen die Einrichtungen mit der nötigen Sorgfalt.
- Wir beachten den Datenschutz und schützen uns selber.
- Wir respektieren unsere Mitmenschen und achten die Menschenrechte.
- Wir berücksichtigen das Urheberrecht.
- Wir halten die Regeln ein.

Die Vorlage der Vereinbarung und andere nützliche Informationen bei "imediass" finden Sie unter <http://www.imediass.ch/service/vorlagen-ict-support>

Exakte Dokumentation der Firewall- und Inhaltsfilter - Konfigurationen ⁽⁸⁾

Wie die Dokumentation der allgemeinen schuleigenen ICT Infrastruktur, sollte auch der Aufbau und die Konfiguration der Sicherheitseinrichtungen in einem Dokument genügend ausführlich beschrieben werden. Konfigurationsänderungen sollen mit Änderungsdatum und Änderungsgrund nachführt werden. So können bei einem eventuellen Zwischenfall auftretende Fragen beantwortet werden. Die ausführliche Dokumentation der ICT Infrastruktur erleichtert zudem den Support, die Stellvertretung der ICT-Zuständigen und reduziert auch den Aufwand bei einer allfälligen "Amtsübergabe" an Nachfolger.

Schutz der Systeme/Konfigurationen durch genügend komplexe Kennwörter ⁽⁹⁾

Es existieren viele Programme, welche einfache Kennwörter schnell entdecken können. Daher ist bei sämtlichen Passwörtern darauf zu achten, dass diese gut gewählt, und bei Bedarf geändert werden. Falls möglich sollten Betriebssysteme, Programme und Netzwerkkomponenten so konfiguriert werden, dass die Anwender keine unsicheren Kennwörter nutzen können.

Ein sicheres Kennwort setzt sich aus mindestens 8 Zeichen verschiedener Zahlen, Satz- und Sonderzeichen zusammen. Ebenso sollten Groß- und Kleinbuchstaben gemischt verwendet werden. Wenn ein Kennwort im Duden oder in einem anderen Wörterbuch nachgeschlagen werden kann, ist es kein sicheres Kennwort - unabhängig von der Länge. Sie sollten keine Namen von Familienmitgliedern oder von Ihrem Haustier verwenden. Ebenso auch keine Telefonnummern, Autonummern oder andere Daten, die man leicht über Sie herausfinden kann. Verwenden Sie auch niemals einfache Tastaturmuster wie z.B. asdf oder jklö.

Viele Netzwerkfähige Geräte (Drucker, Kopierer, Switches, Netzwerk-Kameras, usw.) sind über das Netzwerk mittels Browser konfigurierbar. Um mögliche Risiken auszuschliessen müssen die Standardpasswörter der Hersteller ersetzt werden, oder bei Standardzugriff ohne Passwort ein solches gesetzt werden.

Auf dauerhafte Testbenutzer ist möglichst zu verzichten. Ist dies nicht möglich, müssen auch dort starke Kennwörter gewählt werden und es muss sichergestellt werden, dass diese Kontos nach Abschluss der Tests wieder gelöscht werden.

Nützliche Links ICT Sicherheit

IT-Sicherheit im Bildungswesen

<http://www.educa.ch/dyn/109337.asp>

Melde- und Analysestelle Informationssicherung MELANI

<http://www.melani.admin.ch/>

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Kinder, Jugendliche und die Tücken des Internets

<http://www.edoeb.admin.ch/themen/00794/01124/01602/index.html?lang=>

FHNW - imedias, IT-Sicherheit

<http://www.imedias.ch/service/pdfs-linklisten/it-sicherheit/?searchterm=datenschutz>

Elternet.ch - unterstützt Eltern in der Medienerziehung

<http://www.elternet.ch/alles-was-recht-ist/datenschutz-und-schutz-fuer-die-daten.html>