Minimale Sicherheitsanforderungen
für eine sichere Nutzung des SAI Internetanschlusses

Vorbemerkungen
Unternehmens- oder Bildungsnetzwerke ohne Schutz an das Internet anzubinden, ist in hohem Masse gefährlich, da immer mehr Prozesse und Informationen über das Internet abgewickelt und ausgetauscht werden. Es gilt, die Unternehmens- und Bildungsnetzwerke mittels zuverlässiger, auf dem Markt etablierter Systeme vor Hacker-Attacken zu schützen. Hinzu kommt, dass heute jeder ein am Internet angeschlossenes System angreifen kann. Es existieren dazu frei erhältliche Softwaretools, welche überall nach bekannten Hintertüren oder Betriebssystemfehlern suchen, um einen Systemeinbruch vorzubereiten oder aber ein ganzes System lahmzulegen (denial of service). An die Sicherheit des Netzwerkes denkt man meist erst dann, wenn die Kommunikation lahmgelegt wurde oder der Verdacht besteht, dass interne, wichtige Dokumente an unberechtigte Dritte gelangt sind. Es gilt, nebst dem kommerziellen Nutzen des Internet auch dessen Gefahren zu kennen und sich dagegen zu schützen. Jedes Unternehmen oder öffentliche Institut ist heute darauf angewiesen, dass seine EDV-Infrastruktur reibungslos funktioniert. Ein Teil- oder Totalausfall (verursacht durch Sicherheitsprobleme in Zusammenhang mit dem Internet) bedeutet meist einen hohen finanziellen Schaden. Nur, wenn Angriffe rechtzeitig erkannt und abgewehrt werden, erhöht sich der Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit der im Firmen- oder Bildungsnetzwerk befindlichen Informationen.

Verantwortung Kanton und Schule
Swisscom stellt allen Schweizer Volksschulen im Rahmen ihrer Initiative «Schulen ans Internet» einen kostenlosen Internet-Anschluss an. Teil dieses Angebotes ist für Anschlüsse mit einer maximalen Bandbreite von 6000/600KBit/s eine integrierte Sicherheitslösung, bestehend aus Firewall (FW) und Web Content Screening (WCS). Bei Bandbreiten von mehr als 6000/600 KBit/s (typischerweise VDSL- oder glasbasierte Anschlüsse) ist der Kanton verpflichtet, diese Sicherheit selbst zu gewährleisten. Er tut dies entweder mittels internem oder externem Dienstleister oder verpflichtet die einzelnen Schulen, für die Sicherheit des Internet-Anschlusses zu sorgen.
Der Kanton als Nutzer eines virtuellen privaten Netzwerks (VPN) ist sich bewusst, dass er und die derart angeschlossenen Schulen über den Zugang zum Internet beliebige Informationen verbreiten und abrufen können. Er bzw. die derart angeschlossenen Schulen übernehmen die Verantwortung für den Inhalt von Informationen (Daten, Bilder, Sprache), die berechtigter- oder unberechtigterweise über den ihm im Rahmen von «Schulen an Internet» von Swisscom zur Verfügung gestellten Internet-Zugang (inkl. Optionen) übermittelt oder abgerufen werden.
Der Kanton und die derart angeschlossenen Schulen sind sich bewusst, dass insbesondere der Zugang zu denjenigen Endgeräten, bei welchen ein Internet-Zugang besteht, in ihrer Verantwortung liegt und sie diese kontrollieren.
Der Kanton oder die derart angeschlossenen Schulen machen die Nutzer in geeigneter Weise (z.B. Ausbildung, Info-Veranstaltung, Merkblatt) auf die Gefahren des Internets aufmerksam und regeln insbesondere die Nutzung der vorliegenden Dienstleistungen durch Kinder und Jugendliche. Der Kanton und die berechtigten Schulen nehmen zur Kenntnis, dass Programme existieren, mit denen der Zugang zu bestimmten Websites blockiert werden kann; sie sind selbst für den allfälligen Einsatz solcher Programme besorgt.
In der Nachfolge formuliert Swisscom minimale Anforderung für die Sicherung dieser Internet-Zugänge.

Anforderungen an eine Firewall (FW) an einer Schule

Eine Firewall soll die Schule[1] gegen unberechtigte An- und Zugriffe von und nach aussen schützen.
Eine Firewall muss diese Minimalanforderungen erfüllen:

- in einer «Policy» ist zu definieren, welcher Netzverkehr nach bestimmten Regeln zugelassen oder verhindert werden soll. Diese Policy muss für eine gesamte Schule Gültigkeit haben.
- Diese Policy muss in regelmässigen Abständen von Dritten überprüft und den aktuellen Umständen angepasst werden (Audit).
- Die Firewall muss den Traffic unterbrechungsfrei protokollieren. Es muss in sinnvollen Abständen (täglich) geprüft werden, ob die Zugriffsbeschränkungen eingehalten werden und funktionieren. Nur durch eine hohe Analyse-Frequenz können Angriffe wie Port Scans, Smurf, Ping of Death, oder Teardrop in nützlicher Zeit erkannt und abgewehrt werden.
- Die Logdaten der Firewall müssen mindestens 6 Monate lang archiviert werden.
- Die Software-Komponenten müssen in regelmässigen Abständen ein Update erfahren. Es ist ein Qualitätsmerkmal der eingesetzten Lösung, wie häufig solche Updates zur Verfügung gestellt werden.
- Sämtliche Anpassungen der Konfiguration auf der Firewall müssen im System rückverfolgbar sein. Der Zugriff zum Ändern der Konfiguration muss eingeschränkt werden.
- Die Firewall muss wirksam die eigene Netzwerkstruktur verbergen. Nur nötige, öffentliche IP-Adressen sollen nach aussen (Internet) sichtbar sein
- Bei Angriffen von aussen und bei Missbrauch von innen ist ein Prozess zu sicherzustellen, der die notwendigen Gegenmassnahmen (z. B. Informationswege, Sichern von Beweisen, etc.) einleitet.
- Funktioniert die Firewall aufgrund von Hardware- oder Software-Problemen nicht oder nicht einwandfrei, muss der Zugang zum Internet unterbrochen werden können. Nur so kann die Sicherheit für das gesamte Bildungsnetz aufrechterhalten werden.
- Im Fall eines Ausfalls des Systems oder wichtiger Komponenten davon muss Ersatz-Material verfügbar sein, und das System muss mittels Backup/Restore-Funktion innert nützlicher Frist wiederhergestellt werden können.

Soll ein Web Content Screening-System (WCS) zum Einsatz kommen, muss es diese Bestimmungen erfüllen, wenn es wirksam und effizient sein soll:

- Die Schule definiert selber oder auf Empfehlung des Kantons, welche Kategorien unerwünschten Inhalts (Pornographie, Gewalt, etc.) sie blockieren will.
- Entweder verfügt das WCS über einen leistungsfähigen webbasierten Service, der laufend die Kategorisierung von Websites aktualisiert und mit dem WCS synchronisiert (URL-Filtering) oder das WCS vermag jede Seitenanforderung zur Laufzeit zu scannen. Wird URL-Filtering eingesetzt, so muss die zugrundeliegende Datenbank täglich aktualisiert werden. Wird ein Scanning zur Laufzeit eingesetzt, muss insbesondere auf eine genügende Performanz-Reserve geachtet werden.
- Requests via URL und via IP-Adressen müssen gleichermassen geprüft und allenfalls abgewiesen werden können.

[1] Mit Schule sind sowohl Institution, wie gebäudliche Ausprägungen mitgemeint. Das Netz umfasst alle Komponenten, die hinter einem Internet Access Point (typischerweise Router von Swisscom Schulen ans Internet) ein LAN ausmachen oder Teile davon sind.