
Swisscom "Schulen ans Internet"

Checkliste zur Gewährleistung der Sicherheit des Internetzugangs

Aarau, 15. August 2010

Information

Nebst den Vorteilen eines Internetzugangs dürfen auch die damit verbundenen Risiken nicht vernachlässigt werden. Dieses Dokument enthält eine Checkliste, welche die Schulen dabei unterstützen soll einen angemessenen Schutz sicherzustellen.

Bei Bandbreiten bis 6'000/600 kbps übernimmt Swisscom im Standardangebot kostenlos den Schutz der Schule und deckt dabei die Hauptanforderungen ab. Es sind nur noch minimale technische und organisatorische Massnahmen zur Netzwerktrennung an der Schule notwendig.

Für höhere Bandbreiten hat die Schule verschiedene Möglichkeiten die Sicherheit zu gewährleisten:

1. Kostenpflichtiges Angebot von Swisscom (Leistungen entsprechen "Standardangebot")
2. Betreiben der sicherheitsrelevanten Komponenten durch die Schule selbst oder eine beauftragte Drittfirma

Das Ziel dieser Checkliste ist es, den Schulen einen Leitfaden und Kontrollblatt über die für die Sicherheit notwendigen Massnahmen zu liefern. Die untenstehende Tabelle gibt dazu eine Übersicht.

Bezieht eine Schule die Sicherheit von Swisscom, sind ein grosser Teil der Anforderungen bereits erfüllt. In der Checkliste sind diese Anforderungen entsprechend markiert. Alle Punkte unter "Mindestanforderungen" sollen durch die Schule oder Swisscom abgedeckt werden.

Die aufgeführten "Optionale Möglichkeiten" können dazu beitragen, dass die Sicherheit erhöht wird, oder auch dass die zur Verfügung stehende Bandbreite optimaler genutzt werden kann. Je mehr Computer einen gemeinsamen Internetanschluss benutzen, desto wichtiger wird ein geordneter Betrieb aus technischer-, wie auch aus organisatorischer Sicht.

Checkliste

	Komponente	Im Swisscom Angebot enthalten	Erledigt
Mindestanforderungen	Firewall ⁽¹⁾	√	<input type="checkbox"/>
	<ul style="list-style-type: none"> • Firewall-Regeln ⁽²⁾ • (NAT) * ⁽³⁾ 	√ -	<input type="checkbox"/> <input type="checkbox"/>
	Inhaltsfilter ⁽⁴⁾	√	<input type="checkbox"/>
	Regelmässige Wartung und Aktualisierung der schulinternen Clients und Server ⁽⁵⁾	-	<input type="checkbox"/>
	Betrieb eines aktuellen Virenschanners auf allen schulinternen Clients und Servern ⁽⁶⁾	-	<input type="checkbox"/>
	Vereinbarung zum Umgang mit dem Internet und der ICT-Infrastruktur für Schülerinnen, Schüler, Eltern und Lehrpersonen ⁽⁷⁾ Vorlagen unter http://www.imedias.ch	-	<input type="checkbox"/>
	Exakte Dokumentation der Schul-ICT-Umgebung inkl. Firewall- und Inhaltsfilter - Konfigurationen ⁽⁸⁾	√ (Firewall)	<input type="checkbox"/>
Schutz der Systeme/Konfigurationen durch genügend komplexe Kennwörter ⁽⁹⁾	-	<input type="checkbox"/>	
Optionale Möglichkeiten	Betrieb eines Proxyservers	-	<input type="checkbox"/>
	Zentraler Virenschanner	-	<input type="checkbox"/>
	Bandbreitenverwaltung	-	<input type="checkbox"/>
	Zusätzlicher Internet-Anschluss als Reserve bei einem Ausfall des Hauptanschlusses	-	<input type="checkbox"/>

* Bei der Nutzung der zentralen Sicherheitslösung von Swisscom ist lokal zumindest ein NAT-Router zum Schutz vor Bedrohungen innerhalb des Schulnetzes notwendig.

Glossar

Firewall

Eine Firewall überwacht den durch sie hindurch eingehenden und ausgehenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Verbindungen oder Datenpakete zugelassen werden, oder nicht. Auf diese Weise schützt die Firewall das private Netzwerk vor unerlaubten Zugriffen.

Inhaltsfilter (Content-Filter)

Ein Inhaltsfilter ermöglicht die technische Kontrolle der zugreifbaren Informationen. Meist werden diese Bereiche mittels einer Kategorisierung konfiguriert. Ausnahmen können in der Regel verwaltet werden. Typische Beispiele für vordefinierte Kategorien sind Pornografie oder Rechtsextremismus. Ein Inhaltsfilter ist immer nur als technische Unterstützung zu betrachten und kann keinen hundertprozentigen Schutz garantieren (siehe Vereinbarung zum Umgang mit dem Internet für Schülerinnen, Schüler und Lehrpersonen)

NAT-Router (Network Address Translation - Router)

NAT ist ein Verfahren, das in Routern eingesetzt wird, welche lokale Netzwerke untereinander oder mit dem Internet verbinden. Der NAT-Router ersetzt in allen ausgehenden Datenpaketen die IP-Adressen der Stationen durch seine eigene(n), eingetragene(n) IP-Adresse(n). Damit die eingehenden Datenpakete dem richtigen Ziel zugeordnet werden, speichert der Router die aktuellen Verbindungen. Eine unkontrollierte Datenverbindung der physisch verbundenen Netzwerke untereinander ist so nicht mehr möglich.

Zweck dieses Gerätes ist es die Schule vor möglichen Gefahren (hauptsächlich Würmer) aus anderen Schulen innerhalb des SAI-Netzes zu schützen. Die zentrale Firewall der Swisscom kann diese lokal benötigte Funktion nicht übernehmen. Die von Swisscom gestellten Router haben diesen Dienst nicht implementiert.

Regelmässige Wartung der schulinternen Clients und Server

Immer wieder werden Sicherheitsrisiken bei Software bekannt. Daher ist es sehr wichtig, dass sämtliche Geräte (Server, Clients, Drucker, Netzwerkkomponenten) immer über die aktuellste Software verfügen. Sollte ein Produkt vom Hersteller nicht mehr unterstützt werden, soll dieses vom Netzwerk getrennt oder ersetzt werden.

Virens Scanner auf allen schulinternen Clients und Server

Nicht nur über das Internet sondern auch von Memory-Sticks oder CDs können Viren auf die Computer gelangen. Daher muss unbedingt ein regelmässig aktualisierter Virens Scanner auf sämtlichen Computern installiert sein.

Vereinbarung zum Umgang mit dem Internet für Schülerinnen, Schüler, Eltern und Lehrpersonen

Schule und Schüler regeln die Nutzung der ICT, sowie die Nutzung des Internet an der Schule mit einer Vereinbarung. Diese wird von den Erziehungsberechtigten mitunterzeichnet. Vorlagen und Informationen finden sich bei IMEDIAS, der Beratungsstelle für digitale Medien in Schule und Unterricht.

<http://www.imedias.ch/weiterbildung/pdfs-support/Schuelervereinbarung-ICT-2009-neu.pdf>

Exakte Dokumentation der Firewall- und Inhaltsfilterkonfiguration

Falls die Schule die Firewall und Inhaltsfilter selbst betreibt muss die aktuelle Konfiguration exakt dokumentiert werden. Änderungen sollen protokolliert werden.

Schutz der Systeme/Konfigurationen durch genügend komplexe Kennwörter

Sämtliche internen Systeme müssen durch geeignete Kennwörter geschützt werden. Auf Test-Benutzer ist wo immer möglich zu verzichten. Auch Netzwerkkomponenten, Drucker und ähnliche Geräte sollen mit einem Kennwort geschützt werden.

Proxyserver

Ein Proxyserver arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen. So werden Webinhalte zwischengespeichert, was zu einem spürbaren Performancegewinn führen kann. Weitere Informationen finden Sie z.B. in Wikipedia.

Bandbreitenverwaltung

Technologie, welche die zur Verfügung stehende Bandbreite auf bestimmte Netzwerkbereiche, Anwendungen oder Dienste aufteilen / reservieren kann, damit nicht einzelne Exponenten die gesamte Leistung für sich beanspruchen können.