*Infoblatt*

# Schulen ans Internet: Schutzmassnahmen für Ihren Internetzugang

Dieses Infoblatt richtet sich an Kantone, Schulen und Anwender und informiert sie über die verschiedenen Schutzmassnahmen, und wie alle Beteiligten zum Schutz der Jugendlichen beitragen können.

## Ausgangslage

Swisscom bietet den Kantonen und Schulen im Rahmen der Initiative "Schulen ans Internet" einen sicheren Zugang ins Internet an. Jugendlichen soll der Zugriff auf relevante Inhalte zum Schutz der Jugend, die von den Schulen und Kantonen vorgängig festgelegt wurden, verwehrt werden. Es existieren verschiedene Wege und jeder Weg deckt unterschiedliche Bedürfnisse ab, abhängig davon, wie umfangreich dieser Schutz ausgestaltet werden soll. Dabei sind zentrale Themen insbesondere der **Jugendmedienschutz**, **Schutz vor gefährlichen Inhalten** sowie **Datenschutz**.

## Jugendmedienschutz

Ziel des Jugendmedienschutzes ist es, die sichere, verantwortungsvolle und altersgerechte Nutzung von Medien zu fördern. Dies erfolgt über Massnahmen zur Förderung von Medienkompetenz oder über technische Massnahmen, um die Verbreitung und Nutzung von Medieninhalten einzuschränken. Bestimmte Inhalte sind für Kinder und Jugendliche unter 16 Jahren per Gesetz unzugänglich zu machen. Swisscom kann bei Bedarf den technischen Schutz vor Webseiten und Inhalten liefern, welche unter den Jugendmedienschutz fallen. Die Filterung umfasst dabei die Internetadressen und Kategorien, die vom Kanton festgelegt werden.

## Schutz vor gefährlichen Inhalten

Die für den Einsatz angebotene Lösung erlaubt den weitestmöglichen Schutz der Benutzer vor Malware und anderen gefährlichen Inhalten. Infizierte Geräte der Benutzer und in der Infrastruktur der Schulen können Schäden und grosse Aufwände in der Wiederherstellung verursachen.

Zu den häufigsten Bedrohungen gehören:

- Drive-by Exploits in Browsern und Browser-Plugins (Flash, Silverlight, etc.)
- Ransomware / Cryptotrojaner
- Viren und sonstige Malware (signaturbasiert)
- Bot-Netze (signaturbasiert, Command and Control-Kommunikation wird erkannt und blockiert)
- Cryptominer (Scripts auf Webseiten, Malware signaturbasiert)
- Phishing (Ausspähen von Benutzerkennungen und Passwörtern)

## Schutz von Personendaten und Daten aus der Internetnutzung

Ziel ist es, den Schutz von Personendaten der Benutzer sicherzustellen. Die Benutzer dürfen nicht ausgespäht werden, und die anfallenden Daten müssen unter Anderem nach dem Grundsatz der Datensparsamkeit bearbeitet werden. Swisscom "Schulen ans Internet" tut dies bereits heute. So werden keine Inhalte von Web-Zugriffen gespeichert, die gespeicherten Logdaten sind minimiert und der Zugriff auf Logdaten erfolgt nur durch autorisierte Administratoren zu Zwecken der Service-Erbringung. Weitere organisatorische und technische Massnahmen um das Anfallen, Speichern und Verarbeiten von Daten zu kontrollieren, sind umgesetzt. Die eingesetzte Lösung ist mit den anwendbaren Gesetzen zum Datenschutz konform.

## Überblick über verschiedene Massnahmen und deren Schutzwirksamkeit

Es gibt verschiedene Ansätze, bestimmte Inhalte zu filtern und die Benutzer zu schützen. Die nachfolgende Übersicht zeigt die verschiedenen Massnahmen auf, deren Wirksamkeit und die Einsehbarkeit der anfallenden Daten.

| Massnahme | Jugendmedienschutz | Schutz vor Malware | Diese Daten werden verarbeitet |
|---|---|---|---|
| **Nur Internetzugang, keine Filter** | Kein Jugendmedienschutz | Kein Schutz vor Malware | Der Internetprovider (Swisscom[1]) sieht die IPs der Benutzer bzw. der Schule und die aufgerufenen URLs sowie Konfigurationsdaten des Netzes. |
| **DNS Filter** | Jugendmedienschutz, aber leicht durch Benutzer zu umgehen. | Kein wirksamer Schutz vor Malware möglich. | Der Internetprovider (Swisscom) und der Betreiber des DNS Filters (Swisscom) sehen die IPs der Benutzer und die aufgerufenen URLs sowie Konfigurationsdaten des Netzes. |
| **HTTP Proxy Content Filter** | Schwacher Jugendmedienschutz, da 70% der Inhalte über HTTPS aufgerufen werden und ohne SSL Inspection keine Aussage über die Kategorie der Webseite getroffen werden kann. | Schutz vor Malware nur auf Webseiten über HTTP-Protokoll (ca. 30% der Verbindungen). | Der jeweilige Internetprovider und der Betreiber des Proxy (Swisscom) sieht die IPs der Benutzer (oder NAT-IP) und die aufgerufenen URLs sowie Konfigurationsdaten des Netzes. Die Inhalte der HTTP Webzugriffe fliessen durch den Proxy, werden aber nicht gespeichert. |
| **HTTP und HTTPS Proxy Content Filter** | Sicherer Jugendmedienschutz. | Wirksam auf allen Webzugriffen | Der jeweilige Internetprovider und der Betreiber des Proxy (Swisscom) sieht die IPs der Benutzer (oder NAT-IP) und die aufgerufenen URLs sowie Konfigurationsdaten des Netzes. |

[1] Swisscom behält sich im Rahmen der vertraglichen Vereinbarungen vor, zur Service-Erbringung mit technischen Sublieferanten zusammenzuarbeiten. Im vorliegenden Fall ist dies Zscaler. Dabei stellt Swisscom sicher, dass alle anwendbaren gesetzlichen Verpflichtungen auch dem Sublieferanten übertragen werden. Im Folgenden wird zur besseren Lesbarkeit lediglich "Swisscom" verwendet.

| | | | |
|---|---|---|---|
| | | | Die Inhalte aller Webzugriffe fliessen durch den Proxy, werden aber nicht gespeichert. |

Erläuterung:

- **DNS Filter:**

DNS-Filterung erlaubt die Namensauflösung von der URL einer Webseite zu deren IP-Adresse. Die DNS Filterung verhindert, dass eine URL vom Benutzer aufgerufen werden kann, und ist als zusätzliche Massnahme zum Proxy sinnvoll. Sie empfiehlt sich aber nicht als alleinige Massnahme, da sie zu leicht für Benutzer zu umgehen ist, und den Schutz der Nutzer und Malware-Abwehr nicht verlässlich sicherstellt.

- **HTTP/HTTPS Proxy:**

Ein Proxy (von englisch «Stellvertreter») arbeitet als Vermittler, der auf der einen Seite Anfragen der Benutzer entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen. Dadurch greift der Benutzer nie direkt auf Webseiten zu. Innerhalb des Proxy können Filterregeln für das Ausliefern von Webseiten an Benutzer umgesetzt werden. Zusätzlich kann der Proxy alle Inhalte auf Malware prüfen. Swisscom arbeitet für die Erbringung der Filter- und Schutzmechanismen mit dem Hersteller Zscaler[2] zusammen.

- **SSL Inspection und Whitelist:**

Um den Schutz der jugendlichen Nutzer und Schutz vor Malware für die verschlüsselten HTTPS-Verbindungen sicherzustellen, muss die Verschlüsselung aufgebrochen werden (SSL Inspection) und nach der Prüfung durch den Proxy neuerlich mittels des eingesetzten Zertifikats verschlüsselt werden. Dafür braucht es die Einwilligung der kantonalen Vertragspartner, damit Swisscom den HTTPS-Traffic (mit Ausnahme der vom Vertragspartner festgelegten Whitelist) entschlüsseln kann. Die Filterung und der Malware Schutz erfordern, dass die Web-Anfragen mittels SSL Inspection verarbeitet werden, damit unerwünschte Inhalte gesperrt werden können.
Nach Vorgabe des jeweiligen Kantons als Vertragspartner können beliebig viele Ausnahmen für die SSL Inspection festgelegt werden (Whitelist). Das heisst: die Kantone legen Whitelists fest, welche Kategorien von Webseiten, und welche einzelne Webseiten von der SSL Inspection auszunehmen sind. Die Whitelist kann jederzeit erweitert und angepasst werden.
Heute ist bei vielen Schulen ein Zertifikat von unserem Lieferanten Zscaler für diesen Prozess im Einsatz. Swisscom überlässt es den Kantonen, ein eigenes Zertifikat für die SSL Inspection zu erstellen und zu nutzen. Dies ist ohne Kostenfolge möglich und stellt sicher, dass das eingesetzte Zertifikat nur im jeweiligen Schulnetz für die SSL Inspection genutzt werden kann.

[2] Zscaler ist ein weltweit tätiger Lieferant für Content Filtering und Malware Protection mit Sitz in den USA. Die Einhaltung der gesetzlichen Vorgaben zum Datenschutz sowie den Vorgaben des EDÖB wird von Zscaler vertraglich zugesichert. Zscaler ist zudem dem Swiss-U.S. Privacy Shield Framework beigetreten, womit ein zugemessener Schutz der Personendaten im Sinne von Art. 6 Abs. 1 DSG gilt. Des Weiteren hat Swisscom mit Zscaler einen Vertrag zum Data Handling nach den Vorgaben des EDÖB abgeschlossen.

**HTTP und HTTPS:**

HTTP ist das Protokoll, über welches Internetseiten aufgerufen und ausgeliefert werden. Dabei wird der Inhalt der Webseite unverschlüsselt übertragen. HTTPS verwendet eine Verschlüsselung des Aufrufs und der Inhalte des Internetzugriffs. Aufgrund technologischer Entwicklungen nimmt der Anteil HTTPS-Traffic gegenüber HTTP stetig zu, und liegt Stand heute (Juli 2018) bei ca. 70%.

**Datenhaltung und Privacy:**

Swisscom identifiziert nicht die Person, die den jeweiligen Computer nutzt. Zugriffe auf Log-Daten werden nur zu Zwecken der Service-Erbringung gestattet und in einem Audit-Log protokolliert. Die autorisierten Administratoren unterliegen speziellen Auflagen (Segregation of Duty, regelmässige Schulungen, regelmässiges Vorweisen der Straf- und Betreibungsregisterauszüge, etc.).

- Inhalte aus Internetverbindungen via HTTP und HTTPS werden nicht gespeichert.
- Die eingesetzten Proxies verfügen über keinen physischen Speicherplatz (nur minimale Boot-Disk).
- Nur am Logserver werden Daten gespeichert, und die Log-Daten beinhalten ausschliesslich:
  - von welcher IP-Adresse der Internetzugriff kam
  - Zeitpunkt des Internetzugriffs
  - URL (Webadresse) des Internetzugriffs
  - Metadaten der Verbindung wie URL-Kategorie, Browserversion, Entscheid anhand der Filterregeln (blockiert/erlaubt).

## Wer tut was in Sachen Jugendmedienschutz?

***Kantone***

Wünscht der Kanton für das entsprechende Schulnetz keine Ausdehnung der Filterung auf HTTPS-Traffic, sind ausser der Mitteilung des Entscheids an Swisscom (s. Punkt a)) keine weiteren Schritte nötig. Im Falle eines Entscheids für die Ausdehnung der Filterfunktion auf HTTPS-Traffic gilt:

An den Kantonen in ihrer Rolle als Vertragspartner von Swisscom für die Bildungsnetze ist es:

a) die Frage zu entscheiden: Soll Swisscom nur den HTTP-Traffic oder auch zusätzlich den HTTPS-Traffic filtern?
b) falls auch eine HTTPS-Filterung gewünscht ist: Welche Inhaltskategorien und URLs sollen von dieser Filterung in jedem Fall ausgeschlossen werden (Whitelist)?
c) Zu entscheiden, ob der Kanton ein kantonsspezifisches Zertifikat einsetzen möchte. Falls ja, stellt er dies Swisscom zur Verfügung, und Swisscom hinterlegt es für dieses Netz/für diese Netze als anwendbar. Der Kanton verteilt das Zertifikat an die Schulen.
d) allenfalls die Nutzer/Nutzerinnen betreffend getroffener Schutzmassnahmen zu informieren. Dies ist insbesondere zu empfehlen, weil der Nutzer über den Sachverhalt informiert werden muss, wenn verschlüsselter Traffic entschlüsselt wird.

***Schulen***

- Es ist Aufgabe der Schulen, gemeinsam mit den Kantonen eine Liste spezifischer URLs zu definieren, die von der Filterung ausgeschlossen werden sollen (Whitelist).
  *(Dies sind z.B. Gemeinde-interne Applikationen, weitere Services im Internet wie Tools, Applikationen, etc. Die Kantone können solche Services aus eigenen Internet-Infrastrukturen anbieten. Viele Schulen werden keine solchen spezifischen Services in Betrieb haben.)*
- Soll in einem Kanton ein kantonsspezifisches Zertifikat genutzt werden, installieren die Schulen dieses Zertifikat auf den schuleigenen Computern und weisen die Berechtigten, die eigene Computer verwenden, dieses Zertifikat ebenfalls zu installieren.

***Swisscom***

An Swisscom ist es,

- die Filterung im Auftrag der Kantone auf HTTP- und HTTPS-Traffic gemäss den getroffenen Vereinbarungen vorzunehmen;
- die von den Kantonen gemeldeten Whitelist-Einträge in der Filter-Konfiguration zu hinterlegen;
- die allenfalls von den Kantonen bereitgestellten kantonsspezifischen Zertifikate im System als zulässiges Zertifikat zu konfigurieren[3]. Wünscht der Kanton kein kantonsspezifisches Zertifikat einzuführen, kann weiterhin das von Swisscom bereitgestellte Zscaler-Zertifikat genutzt werden.

Für weitere, detailliertere Informationen stehen wir Ihnen über unseren kantonalen Vertragspartner gerne zur Verfügung.

[3] Das System akzeptiert das kantonseigene Zertifikat als vertrauenswürdig und setzt es für den SSL Inspection Prozess ein.