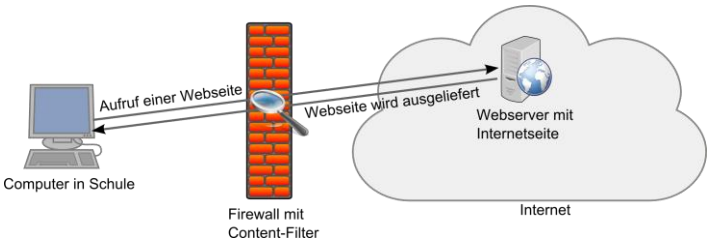
Content-Filter

Grundlagen

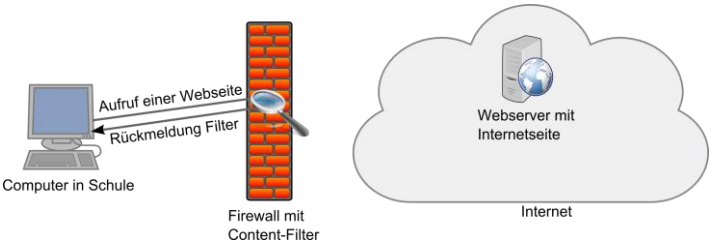
Der Kanton verlangt von den Schulen, dass sie Schülerinnen und Schüler vor unerwünschten Inhalten im Internet schützen:

> *„Das Schulnetz ist mit einem zuverlässigen Inhaltsfilter zu sichern. Dieser stellt sicher, dass Seiten mit unerwünschtem Inhalt (Pornografie, Rassismus, Gewalt) gesperrt sind.“*

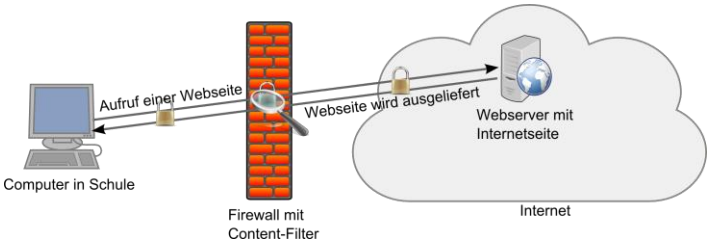
Wir haben einen solchen Content-Filter. Wenn von einem Computer in der Schule eine Webseite aufgerufen wird, überprüft dieser Filter, ob es sich um eine Seite mit unerwünschtem Inhalt handelt. Im Normalfall wird die Anfrage weitergeleitet, so dass der Webserver die Seite ausliefern und der Computer in der Schule sie anzeigen kann.



Wenn es sich nun um eine Seite mit unerwünschtem Inhalt handelt, blockiert der Content-Filter die Anfrage und liefert statt der Webseite eine eigene Rückmeldung.



Wenn es sich aber um eine verschlüsselte Seite handelt, kann der Content-Filter nicht auf unerwünschten Inhalt überprüfen. Dass es sich um eine verschlüsselte Seite handelt, erkennt man am https und am Schlosssymbol in der Adresszeile.

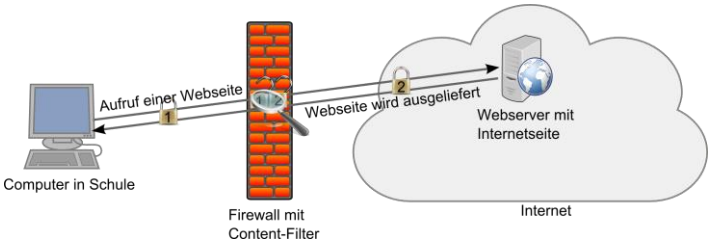


Google verwendet seit einiger Zeit das https Protokoll für seine Suchanfragen. Somit kann ein Content-Filter nicht verhindern, dass in den Vorschaubildern der Google Suche auch unerwünschte Inhalte angezeigt werden. Wer nach Seiten mit unerwünschtem Inhalt sucht und die Bilder anzeigen lässt, sieht sofort, dass dies nicht den Forderungen des Kantons entspricht. Neben Google haben aber viele andere Seiten auch begonnen, standardmässig auf https zu setzen, was eigentlich eine

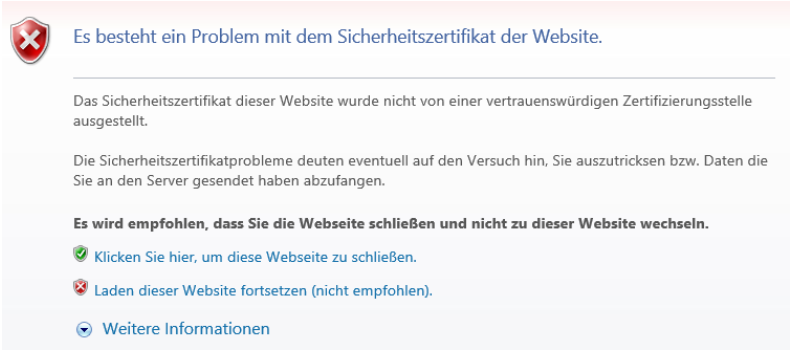
gute Entwicklung ist, da dies Sicherheit und Persönlichkeitsschutz des Anwenders verbessert. Dadurch werden aber neben dem Content-Filter auch alle Sicherheitsmassnahmen auf der Firewall ausgehebelt. Diese kann https Verkehr auch nicht mehr auf Malware überprüfen, um das interne Netzwerk zu schützen.

SSL aufbrechen

Es gibt aber eine Möglichkeit, auch verschlüsselten https Verkehr zu filtern. Dazu muss die Verschlüsselung auf der Firewall aufgebrochen werden. Die Verbindung zwischen Computer und Firewall wird mit einem „falschen" Zertifikat (1) verschlüsselt, die zwischen Firewall und dem Webserver im Internet mit dem richtigen (2). Dadurch, dass die Firewall nun von beiden Teilen ein Endpunkt ist, kann sie den Verkehr entschlüsseln, filtern und wieder verschlüsseln.



Dies entspricht einem sogenannten Man-in-the-Middle-Angriff. Daher wird man als Benutzer darauf hingewiesen, dass das Zertifikat (1) nicht vertrauenswürdig ist.



Damit man diese Meldungen nicht mehr erhält, kann man das Zertifikat auf dem Gerät installieren. Danach wird auch diesem Zertifikat vertraut. Für die Computer der Schule wird dies automatisch gemacht, bei den privaten Geräten muss man das Zertifikat selber importieren.

Abwägungen

Das oben erwähnte Aufbrechen der verschlüsselten https Verbindung ist ein Eingriff in die Privatsphäre des Benutzers. Normalerweise kann ein Benutzer davon ausgehen, dass eine https Verbindung Ende-zu-Ende-Verschlüsselt und damit „abhörsicher" ist, auch gegenüber der Firewall. Argumente gegen das Aufbrechen wurden z.B. von Beat Döbeli in seinem Beitrag „Das schulische Content-Filter-Dilemma" aufgeführt.

Die Schule Altstätten hat trotzdem beschlossen, den Forderungen des Kantons nachzukommen und genau gleich wie die Schulen, die über das Schulen ans Internet Angebot der Swisscom ins Internet gehen, auch verschlüsselte Verbindungen zu filtern. Wichtig erscheint uns, die Benutzer angemessen auf diesen Umstand hinzuweisen, damit sie selber entscheiden können, ob sie weiterhin z.B. die Weboberfläche des privaten Mailaccounts in der Schule öffnen wollen.

Ich hoffe, es ist mit diesem Dokument gelungen, verständlich zu erklären, um was es geht. Bei Fragen kann man sich gerne an mich wenden.
Christian Krüsi, Informatikverantwortlicher Schule Altstätten