Akademie für
Lehrerfortbildung
und Personalführung

Webfilter in der Schule

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen
Autor:	SCHULNETZ, Akademie Dillingen
URL:	https://schulnetz.alp.dillingen.de
Mail:	schulnetz@alp.dillingen.de
Stand:	März 2024

Inhalt

Webfilter in der Schule

Ein Webfilter ist eine Technik, die es ermöglicht, unerwünschte Internetseiten zu filtern. Die Empfehlungen zur IT-Ausstattung von Schulen (Votum) sehr vor, dass keine grundsätzliche Verpflichtung für Schulen zum Einsatz dieser Technologie besteht.

1. Allgemein

1.1. Herausforderung

Schulen stehen vor der Herausforderung, digitale Medien im Unterricht einzubinden und auch die Schulverwaltung benötigt Möglichkeiten, die Digitalisierung zu nutzen. Ein ständig verfügbarer Internetzugang ist dabei obligatorisch. Daraus ergeben sich besondere Herausforderungen:

- Wie können die Kinder und Jugendliche vor jugendgefährdenden Darstellungen oder Inhalten geschützt werden?
- Wie kann sichergestellt werden, dass über die Internetverbindung keine Schadsoftware in Schulnetzwerke eindringt?
- Gibt es Techniken, die einen Schutz von schuleigenen Geräten auch außerhalb des Netzwerks der Schule sicherstellen, z.B. von Lehrerdienst- oder Schülerleihgeräten zu Hause?
- Wie können Lehrerdienstgeräte vor betrügerischen Websites geschützt werden?
- Wie können Schulleitungen und die Schulverwaltung vor Verschlüsselungstrojanern geschützt werden?
- Wie flexibel ist der Webfilter auf mobilen Geräten einsetzbar?
- Wie lassen sich Apps filtern?

1.2. Schulische Szenarien für einen möglichen Einsatz eines Webfilters

In der Schule gibt es unterschiedliche Anwendungsfälle für eine Webfilter:

- Einsatz eines Webfilters bei stationären schuleigenen Geräten im pädagogischen Netzwerk, z.B. in Computerräumen oder Klassenzimmern
- Einsatz eines Webfilters im stationären Geräten Verwaltungsnetz
- Einsatz eines Webfilters auf Lehrerdienstgeräten oder Referendarsgeräten
- Einsatz eines Webfilters bei Schülerleihgeräten
- Einsatz eines Webfilters bei elternfinanzierten Geräten
- Einsatz eines Webfilters bei privaten Geräten im Gast-WLAN

1.3. Webfilter als Teil der Sicherheitsinfrastruktur der Schule

Die Sicherheitsinfrastruktur einer Schule besteht im Allgemeinen aus folgenden Elementen:

- Internetzugangsrouter mit NAT, Firewall und der Möglichkeit, verschiedene Netzwerke voneinander zu trennen.
- Webfilter (optional)
- Clients mit Virenscanner und Firewall

Der Internetzugangsrouter bietet Sicherheit auf Netzwerkebene. Er verbindet das Schulnetzwerk mit dem Internet. Die Technologie NAT (network adress translation) sorgt dafür, dass private Quell-IP-Adressen aus dem Schulnetz in die öffentliche IP-Adresse des Internetzugangsrouters übersetzt werden. Dank dieser Technik ist es nicht möglich, aus dem Internet eine Verbindung ins Schulnetz aufzubauen. Die Verbindungen werden immer nur aus der Schule heraus aufgebaut.

Der Internetzugangsrouter kann verschiedene Teilnetze verwalten. Diese sind mit einer Firewall voneinander getrennt. Das sorgt für eine Trennung z.B. zwischen dem Verwaltungsnetzwerk und dem pädagogischen Netzwerk. Die Anzahl der Teilnetze in einer Schule kann stark variieren.

Der Webfilter wird eingesetzt, um den Lernenden ungeeignete Inhalte im Internet nicht verfügbar zu machen. Er wird ebenfalls eingesetzt, um Bedrohungen im Internet, wie z.B. Spam, Phishing, Ransomware, Verschlüsselungstrojaner oder ähnliches zu minimieren. Dies ist vor allem zum Schutz des Verwaltungsnetzes sinnvoll. Der Webfilter kann dabei mit verschiedenen Technologien umgesetzt werden. Neben der Proxy-Technologie ist Webfilterung ebenfalls mit DNS-Filterung möglich.

Die Clients sind ebenfalls Teil des Sicherheitskonzeptes der Schule. Sie verfügen über einen Virenscanner, der Schadsoftware erkennt und blockiert. Die Berechtigungen auf den Clients sind so gewählt, dass Nutzern administrative Rechte fehlen. Die Firewall verhindert unautorisierte Zugriffe aus dem Netzwerk auf den Client.

2. Anwendungsfälle eines Webfilters

Die Anwendungsfälle eines Webfilters haben in den letzten Jahren zugenommen und umfassen heute u.a. folgende Bereiche:

- URL-Filterung: Die URL-Filterung umfasst die Filterung von Webseiten nach vorgegebenen Kategorien. Nutzer sollen daran gehindert werden, Websites aufzurufen, die unerwünschte Inhalte zeigen oder Schadsoftware verteilen.
- Drive-by-Downloads von Schadsoftware: Beim Besuch manipulierter Webseiten laden sich Internetnutzer unbewusst Schadsoftware auf den eigenen Rechner.
- App-Filterung: Nicht alle Apps sind für den Unterricht wertvoll. Man kann mobile Geräte entweder über ein schuleigenes MDM verwalten, so dass nicht pädagogisch nicht sinnvolle Apps in der Schule nicht funktionieren. Alternativ kann man nicht wertvolle Apps sperren.
- Software aus unsicheren oder unbekannten Quellen: Ist es Nutzern möglich, Software auf Computern zu installieren, können Programme aus unbekannten oder unsicheren Quellen ein Risiko darstellen.

- Spam oder Phishing-Mails: Spam oder auch Phishing-Mails sind unerwünschte elektronische Nachrichten, die teilweise massenhaft versendet werden. Der Inhalt dieser Nachrichten können Werbung, irreführende Inhalte oder Betrugsversuche sein.
- Trojaner / Würmer: Würmer und Trojaner gehören zu Klassikern unter den Schadprogrammen. Die Programme nisten sich unerkannt in einem Computersystem ein und führen dann gefährliche Aktionen aus, zum Beispiel übertragen sie Passwörter, die der Nutzer am Gerät eingibt.
- Botnetze: Ein Botnetz ist ein Netzwerk infizierter Computer. Rechner werden über das Internet zusammengeschaltet und kontrolliert. Aus Botnetzen können Spam- und Phishing-Mails versendet oder Webserver mit massenhaften Anfragen lahmgelegt werden. Zudem können Cyberkriminelle auf den befallenen Computern Passwörter und andere Daten abgreifen.

3. Anforderungen an einen Webfilter

Wenn sich eine Schule für einen Webfilter entscheidet, um die kontinuierliche und präventive Aufsicht der Schule zu unterstützen, kann die Berücksichtigung folgender Kriterien bei der Auswahl hilfreich sein:

- Deutscher Jugendschutz-Filter: Der Deutsche Jugendschutz-Filter blockiert Inhalte, die als jugendgefährdend gelten. Diese Liste wird nicht vom Hersteller des Webfilters kontrolliert, sondern von der BPjM (Bundesprüfstelle für jugendgefährdende Medien), um dem deutschen Recht zu entsprechen.
- Verhinderung von DoH und DoT: Applikation wie z.B. Internetbrowser können DNS über HTTPS (DoH) und DNS über TLS (DoT) verwenden, um verschlüsselte DNS-Anfragen direkt an voreingestellte DoH oder DoT Name Server zu senden. Hiermit kann die Namensauflösung umgangen werden. Eine Filterlösung sollte daher in der Lage sein, die Verwendung von fremden DoH und DoT Servern zu erkennen und verhindern.
- Performanz: Der Webfilter darf die Internetverbindung oder das Aufrufen von Webseiten (Latenz) nicht merklich verlangsamen und muss mit allen Desktop-Computern, Notebooks, Tablets und weiteren mobilen Endgeräten funktionieren.
- Zuverlässigkeit und Verfügbarkeit: Ein Webfilter kann entweder als Hardware in der Schule oder als Softwaredienst, z.B. in der Cloud verwendet werden. Daher sollte entweder die Hardware eine hohe MTBF (z.B. > 100.000 Stunden) besitzen oder der Dienst in der Cloud z.B. über ein Anycast-Verfahren arbeiten. Sobald ein Server unter seiner Adresse nicht erreichbar ist, wird via dem Anycast-Routing Verfahren der nächstgelegene Server, bei gleichbleibender IP-Adresse angesprochen.
- Weltweite Sicht auf Internetbedrohungen: Internetbedrohungen sind nicht auf Deutschland begrenzt. Je mehr Angriffe ein Security-Anbieter weltweit sieht, analysiert und auswertet, umso besser kann er den einzelnen Anwender vor aktuellen Gefahren schützen. Der Security-Anbieter sollte daher mehrere Milliarden Internetanfragen am Tag sehen, analysieren und innerhalb kurzer Zeit in seine Security-Lösungen implementieren.
- Kurze Aktualisierungszeiten: Die Zeitspanne für das Kategorisieren und Auswerten von Internet-Anfragen sollte unter 24 Stunden liegen. Für Hardware-Webfilter sollten tägliche Updates angeboten werden.
- Integration in das Unterrichtsnetz: Auf den schüler- bzw. lehrereigenen Geräten sollte der Webfilter funktionieren, ohne dass dort Änderungen an der Konfiguration vorgenommen werden müssen.

- Speicherung von Log-Daten: Wünscht die Schule eine Speicherung von Webanfragen, sollten diese nach den Vorgaben der Schule gespeichert und in vorgegebenen Zeiträumen automatisiert gelöscht werden. Aufgrund der in der EU geltenden Bestimmungen zum Datenschutz und bezüglich des Aufbewahrungsorts von Daten ist eine Speicherung der Log-Daten innerhalb der EU anzustreben.
- Inhaltliche Zuverlässigkeit: Bei der bestimmungsgemäßen Arbeit im Unterricht sollte man den Webfilter nicht bemerken. Üblicherweise werden Webfilter danach bewertet, wie zuverlässig diese unerwünschte Webseiten sperren. Ebenso wichtig ist, dass Webfilter erwünschte Webseiten und Dienste zulassen und den Unterricht nicht behindern.
- Globale Einstellung durch die Schule: Die Schule sollte eine Möglichkeit haben, die Filterung zu beeinflussen (z. B. Auswahl der zu filternden Kategorien, eigene Blacklist/Whitelist). Sinnvoll ist es, wenn die Filterregeln entsprechend dem Alter, der Medienkompetenz, der Selbstverantwortung, der Einsichtsfähigkeit der Schülerinnen und Schüler und der jeweiligen Einsatz und Beaufsichtigungssituation global voreingestellt werden können.

4. Technische Umsetzung

Im Folgenden sollen verschiedene Webfilter-Technologien miteinander verglichen werden.

Merkmal	Proxy-Server	DNS-Filterung mittels App	DNS-Filterung über Router
Filtertechnik	Ein Proxy-Server wird in Netzwerk einer Schule an zentraler Stelle platziert. Der gesamte Internet-Traffic wird über den Proxy-Server geleitet. Ein Client im Schulnetzwerk baut bei einer Anfrage ins Internet zunächst nur eine Verbindung bis zum Proxy auf, dort wird anschließend der Inhalt nach bestimmten Filterkriterien untersucht. Wird die Verbindung nicht geblockt, baut der Proxy-Server anschließend eine Verbindung zum Ziel auf. Der Proxy-Server kann zudem bei unverschlüsselter Übertragungsprotokolle (z.B. http) die Inhalte der Antworten an den Client auf kategorisierte Inhalte prüfen und ggf. blockieren. Die Proxy-Technologie erlaubt sehr differenzierte Einstellungen. Der Proxy-Server erhält regelmäßige Updates mit kategorisierten Websites, mit diesen Informationen werden Filter-	Der DNS-Dienst (Domain Name Service) ist einer der zentralen Dienste im Internet, ohne den kein Webzugriff und auch nahezu kein Zugriff auf einen anderen Dienst möglich ist. Die Kontrolle des DNS-Dienstes kommt damit der Kontrolle des Internetzugangs gleich. Adressen im Internet werden von DNS-Filter-Anbietern klassifiziert und kategorisiert. Macht ein Client eine DNS-Anfrage, wird diese von der DNS-Filter-App zum DNS-Filter-Anbieter umgeleitet. Soll die Adresse nicht gefiltert werden, wird die IP-Adresse zurückgegeben, ansonsten findet keine Namensauflösung statt. Die DNS-Filterung geschieht vor dem Aufbau z.B. einer http/ https -Verbindung. Daher findet keine Unterbrechung der Verbindung wie beim Proxy statt. Die DNS-Filterung über Filter-App ist stets aktuell, da auf die Daten des Filter-Anbieters in der Cloud zugegriffen wird. Es finden keine Updates mit Filterlisten auf die Geräte statt.	Der DNS-Dienst (Domain Name Service) ist einer der zentralen Dienste im Internet, ohne den kein Webzugriff und auch nahezu kein Zugriff auf einen anderen Dienst möglich ist. Die Kontrolle des DNS-Dienstes kommt damit der Kontrolle des Internetzugangs gleich. Auf dem Internetzugangsrouter der Schule wird der DNS-Server eines Anbieters mit DNS-Filterung eingetragen. Andere DNS-Server ohne Filterung müssen von der Firewall des Internetzugangsrouters blockiert werden. Adressen im Internet werden von DNS-Filter-Anbietern klassifiziert und kategorisiert. Macht ein Client eine DNS-Anfrage, wird diese vom Router zum DNS-Filter-Anbieter umgeleitet. Soll die Adresse nicht gefiltert werden, wird die IP-Adresse zurückgegeben, ansonsten findet keine Namensauflösung statt. Die DNS-Filterung geschieht vor dem Aufbau z.B. einer http/ https -Verbindung. Daher findet keine Unterbrechung der Verbindung wie beim Proxy statt.

	entscheidungen getroffen. Die Aktualisierungsrate ist entscheidend für die Webfilterung.		Die DNS-Filterung ist stets aktuell, da auf die Daten des Filter-Anbieters in der Cloud zugegriffen wird. Es finden keine Updates mit Filterlisten auf die Geräte statt.
Erforderliche Ressourcen für die Einrichtung	Ein Proxy-Webfilter wird entweder als Proxyserver (Hardware) oder als Software auf einem Server eingesetzt. Um technische Engpässe bei den Verbindungen ins Internet zu vermeiden, muss die einzusetzende Hardware an die Anzahl der Benutzer und die zur Verfügung stehende Bandbreite ins Internet entsprechen.	Für die Installation ist keine Hardware erforderlich.	Für die Einrichtung wird der Internetzugangsrouter der Schule verwendet.
Einrichtung und Konfiguration des Webfilters	Hoher zeitlicher Aufwand sowie vertiefte IT-Kenntnisse, um einen Proxyserver zu installieren und zu konfigurieren.	Für den Betrieb der DNS-Filterung mittels App ist meist ein Konto incl. Lizensierung bei einem Anbieter einzurichten. Hier können die Filterregeln definiert werden.	Für den Betrieb der DNS-Filterung über einen Router ist meist ein Konto incl. Lizensierung bei einem Anbieter einzurichten. Hier können die Filterregeln definiert werden. Im Router muss die IP-Adresse des DNS-Servers geändert werden. Der Kunde wird meist anhand seiner externen (öffentlichen) IP-Adresse erkannt. Besitzt die Schule keine statische öffentliche IP-Adresse, muss ggfs. ein dynDNS-Dienst verwendet werden. Um Clients daran zu hindern, einen anderen DNS-Server zu verwenden, ist eine Firewall-Regel einzurichten, damit keine anderen DNS-Server verwendet werden können.

Einrichtung am Client	Ein nicht transparenter Proxy muss an jedem Client im Netzwerk eingetragen werden. Für das Aufbrechen der HTTPS Verschlüsselung (siehe oben), muss ggf. auf allen Geräten das Root Zertifikat des jeweiligen Proxy Servers ausgerollt und installiert werden. Ein transparenter Proxy muss am Client nicht weiter eingerichtet werden, kann aber ggfs. verschlüsselte Verbindungen nicht filtern.	Die DNS-Filter-App wird entweder selbst oder mit Hilfe eines MDM installiert. Für den Betrieb der App ist oft eine Konfigurationsdatei erforderlich. Diese wird entweder mit einem MDM oder mittels Link / QR-Code auf die Geräte verteilt.	Am Client sind keine Änderungen notwendig.
Ende zu Ende Verschlüsselung	Teilweise. Teilweise muss verschlüsselter Web-Verkehr (der größte Teil des heutigen Datenverkehrs) aufgebrochen werden, um Filterregeln anwenden zu können.	Ja. Keine Auswirkung, da http/HTTPS Web Daten nicht "angefasst" werden (es wird schon vorher auf DNS-Ebene gefiltert).	Ja. Keine Auswirkung, da http/HTTPS Web Daten nicht "angefasst" werden (es wird schon vorher auf DNS-Ebene gefiltert).
Auswirkungen auf Internetbandbreite und Latenz	Die Leistungsfähigkeit eines Proxyservers ist stark von der verwendeten Hardware abhängig. Die zur Verfügung stehende Internetbandbreite kann durch einen zu klein dimensionierten Proxyserver verringert sein. Meist erhöht die Verwendung eines Proxyservers die Latenz deutlich, manchmal sogar um ein Mehrfaches.	Keine	Keine
Auswirkungen auf Apps	Einige Apps funktionieren bei Einsatz eines Proxyservers u.U. nicht wie gewünscht (u.a. Office und Videokonferenz-Dienste, deren Verschlüsselung	Keine	Keine

	nicht ohne weiteres aufgebrochen werden darf).		
Unterstützte Clients	Auf allen gängigen Desktop und mobilen Betriebssystemen ist die Konfiguration eines Web Proxy Servers möglich. Auf vielen anderen Systemen (Drucker, Telefone, Smart Boards, etc.) ist es oft nicht möglich, einen Proxy Server einzustellen. Diese Systeme sind damit entweder vor Angriffen ungeschützt und stellen eine potenzielle Gefahr für alle Netzteilnehmer dar oder sind über das Internet nicht mehr managebar.	Auf allen gängigen Desktop und mobilen Betriebssystemen ist die Installation einer DNS Filter App möglich.	Alle
Geschützte Applikationen / Protokolle	Ausschließlich Web-basierte Anwendungen bzw. Deren Protokolle (z.B. http) können gefiltert werden. Apps oder andere Protokolle werden nicht gefiltert.	Alle. Es wird schon vor dem Verbindungsaufbau – unabhängig von der verwendeten App bzw. Protokoll – gefiltert.	Alle. Es wird schon vor dem Verbindungsaufbau – unabhängig von der verwendeten App bzw. Protokoll – gefiltert.
Verfügbarkeit außerhalb der Schule	Nein. Ein Proxyserver, der innerhalb der Schule eingesetzt wird, ist außerhalb der Schule nicht verfügbar.	Ja. Die Webfilterung per DNS-Filter-App funktioniert überall. Es muss lediglich eine Internetverbindung vorhanden sein. Damit sind Geräte außerhalb der Schule (z.B. in heimischen Netzwerken) geschützt.	Nein. Wenn sich Geräte außerhalb der Schule mit einem anderen Netzwerk (z.B. Heimnetzwerk) verbinden, ist die Webfilterung nicht mehr verfügbar. Damit sind Geräte zu Hause nicht geschützt.
Möglichkeit, auf einzelnen Geräten im Schulnetzwerk	Ja. Die Anwendung unterschiedlicher Filterregeln auf bestimmten Geräten im	Ja.	Nein.

abweichende Filterregeln zu realisieren	Schulnetzwerk ist möglich durch eine Registrierung von Geräten im Proxyserver, für die andere Filterregeln gelten. Ebenfalls ist es möglich, für verschiedene Subnetze unterschiedliche filterregeln zu konfigurieren.	Die Webfilterung geschieht mittels App auf dem Endgerät. Damit ist die Webfilterung unabhängig davon, in welchem Netzwerk der Schule sich das Gerät sich gerade befindet. Die Webfilterung kann individuell angepasst werden.	Sollen auf bestimmten Geräten im Schulnetzwerk andere Filterregeln angewendet werden, müssen diese manuell mit einem anderen DNS-Server mit Webfilterung konfiguriert werden.
Möglichkeit verschiedene Filteregeln innerhalb eines Subnetzes zu realisieren	Ja. Die Anwendung unterschiedlicher Filterregeln innerhalb eines Subnetzes ist möglich durch eine Registrierung von Geräten im Proxyserver, für die andere Filterregeln gelten.	Ja. Die Webfilterung geschieht mittels App auf dem Endgerät. Damit ist die Webfilterung unabhängig davon, in welchem Netzwerk der Schule sich das Gerät sich gerade befindet. Die Webfilterung kann individuell angepasst werden.	Nein. Sollen auf bestimmten innerhalb eines Subnetzes verschiedene Filterregeln angewendet werden, müssen diese manuell mit einem anderen DNS-Server mit Webfilterung konfiguriert werden.
Möglichkeit interne Domänen oder Adressen von der Webfilterung auszunehmen	Durch Verwendung einer Whitelist ist dies möglich.	Durch Verwendung einer Whitelist ist dies möglich.	Durch Verwendung einer Whitelist ist dies möglich.
Auswirkungen auf die Verwendung von MDM-Systemen	Proxyserver können die Verwendung von MDM-Systemen behindern bzw. einschränken. Die Zeit, die Clients zum Aktualisieren benötigen kann ggfs. deutlich erhöht sein. Ebenfalls kann es vorkommen, dass eine Aktualisierung von Clients in einem MDM nicht mehr funktioniert.	Die Verwendung von MDM-Systemen wird nicht beeinflusst.	Die Verwendung von MDM-Systemen wird nicht beeinflusst.
Anpassbarkeit der Leistungsfähigkeit	Eine Anpassung der Leistungsfähigkeit eines Hardware-Proxyservers ist nicht möglich. Steigen z.B. die Anforderungen an den Webfilter durch die Erhöhung der Anzahl der Clients ist ein Austausch der Hardware nötig.	Die Leistungsfähigkeit ist unabhängig von der Anzahl der Clients. Die Leistungsfähigkeit ist lediglich durch die Bandbreite der Internetanbindung begrenzt.	Die Leistungsfähigkeit ist unabhängig von der Anzahl der Clients. Die Leistungsfähigkeit ist lediglich durch die Bandbreite der Internetanbindung begrenzt.

	Die Anpassung der Leistungsfähigkeit eines Software-Proxyservers ist durch Virtualisierung in gewissen Umfang möglich.		
Redundanz	Eine Redundanz eines Proxyservers (Software) kann durch Virtualisierung erreicht werden. Der Einsatz eines redundanten Proxyservers (Hardware) verursacht deutlich höhere Kosten und Konfigurationsaufwand.	Eine Redundanz einer Webfilterung mittels DNS-Filter-App kann erreicht werden mit einem DNS-Filter mit Redundanz (z.B. mehrere Rechenzentren oder Verwendung von Anycast-Adressen)	Eine Redundanz einer Webfilterung mittels DNS-Filter auf dem Router kann erreicht werden mit einem redundanten Internetzugangsroutern und einem DNS-Filter mit Redundanz (z.B. mehrere Rechenzentren oder Verwendung von Anycast-Adressen)
Skalierbarkeit auf verschiedene Standorte	Soll ein Proxyserver an verschiedenen Standorten eingesetzt werden, müssen die Standorte miteinander vernetzt sein, damit der Proxyserver erreicht werden kann. Dies kann einen hohen Aufwand bedeuten.	Die Webfilterung geschieht mittels App auf dem Endgerät. Damit ist die Webfilterung unabhängig davon, an welchem Standort sich das Gerät gerade befindet. Die Webfilterung kann auf beliebig viele Standorte skaliert werden.	Die Einrichtung und Konfiguration der Internetzugangsrouter muss für jeden Standort durchgeführt werden. Eine Skalierung auf mehrere Standorte kann einen hohen Aufwand bedeuten.
Verwaltung	Die Verwaltung eines Proxy-Servers geschieht über das Interface des Servers. Dies kann vor Ort oder über VPN geschehen. Eine Verwaltung über die Cloud kann nur mit zusätzlichem Aufwand erreicht werden.	Die Verwaltung der DNS-Filterung per App ist in der Cloud und ortsunabhängig. Sie kann für eine einzelne Schule, für einen Schulverbund, für einen Sachaufwandsträger oder landesweit angewendet werden.	Die Verwaltung der DNS-Filterung über einen Router geschieht in der Cloud für jeden Standort. Die Verwaltung mehrere Standorte kann aufwändig sein.
Erkennung und Auswertung von Vorfällen	Die Erkennung und Auswertung von Vorfällen geschieht durch Auswertung von Logfiles. Dies kann bei umfangreichen Logfiles z.T. sehr aufwändig sein.	Die Erkennung und Auswertung von Vorfällen geschieht automatisiert in der Cloud.	Die Erkennung und Auswertung von Vorfällen geschieht automatisiert in die Cloud.

		Vorfälle können ortsunabhängig und standortbergreifend erkannt und ausgewertet werden.	Vorfälle können für den Standort, an dem der Webfilter auf dem Router eingesetzt wird, ausgewertet werden. Vorfälle für mehrere Standorte müssen oft für jeden Standort einzeln ausgewertet werden.
Logging	Ein Proxyserver kann entweder lokal oder remote loggen. Eine Auswertung von Logs mehrerer Proxyserver kann aufwändig sein.	Das Logging findet in der Cloud statt. Das Logging ist ortsunabhängig und damit für mehrere Standorte verfügbar.	Das Logging findet in der Cloud statt. Es ist für den Standort, an denen der Webfilter eingesetzt wird, verfügbar. Eine Auswertung von Logs mehrerer Standorte kann aufwändig sein.

5. Einsatz und Grenzen eines Webfilters

5.1. Anwendung von Webfilter-Technologien auf schulische Szenarien

Die o.g. Webfilter-Technologien eignen sich unterschiedlich für schulische Szenarien. Die folgende Tabelle zeigt beispielhaft die Anwendung der Webfilter-Technologien auf verschiedene schulische Szenarien.

Proxy-Server	DNS-Filterung mittels App	DNS-Filterung über Router
	• Lehrerdienstgeräte oder Referendarsgeräte • Schülerleihgeräte	• stationäre schuleigene Geräte im pädagogischen Netzwerk, z.B. in Computerräumen oder Klassenzimmern • stationäre Geräte im Verwaltungsnetz • elternfinanzierte Geräte • private Geräte im Gast-WLAN

Die Webfilterung mittels DNS-Filterung auf einem Router ist für stationäre schuleigene Geräte zweckmäßig. Die Geräte sind nicht mit unterschiedlichen Netzwerken (z.B. Verwaltungsnetz oder pädagogisches Netz) verbunden. Eine Webfilterung für diese Geräte ist über eine DNS-Filterung am Router vorzuziehen.

Für elternfinanzierte Geräte bzw. private Geräte in einem Gast-WLAN ist eine Webfilterung mittels DNS-Filterung über einen Router zweckmäßig. An den Geräten sind keinerlei Einstellungen zu verändern.

Schuleigene mobile Geräte, wie z.B. Lehrerdienstgeräte oder Schülerleihgeräte, werden z.T. in unterschiedlichen Netzwerken innerhalb der Schule und außerhalb der Schule, z.B. zu Hause, verwendet. Sie profitieren von einer Webfilterung mittels DNS-Filter-App. Die Webfilterung geschieht mittels App auf dem Endgerät und ist überall verfügbar, wo das Gerät mit dem Internet verbunden ist. Die Webfilterung ist unabhängig davon, mit welchem Netzwerk innerhalb und außerhalb der Schule das Endgerät verbunden ist.

5.2. Abdeckung möglichst vieler Anwendungsfälle

Die im vorigen Kapitel vorgestellten Techniken sollten möglichst viele Anwendungsfälle eines Webfilters abdecken. Der Vergleich mit den Anwendungsfällen zeigt, dass der DNS-Filter eine Mehrheit dieser Anwendungsfälle abdeckt:

- URL-Filterung
- Drive-by-Downloads von Schadsoftware
- Software aus unsicheren oder unbekannten Quellen
- Spam oder Phishing-Mails (nur darin enthaltene Links)
- Trojaner / Würmer (sofern DNS zur Namensabfrage genutzt wird)
- Botnetze (sofern DNS zur Namensauflösung genutzt wird)
- App-Filterung

Trotzdem sollte auch mit Webfilterung eine gewisse kritische Vorsicht, vor allem bei E-Mails, vorhanden sein. Social engineering stellt für Webfiltertechnologien weiterhin eine Herausforderung dar.

5.3. Effizienter und flexibler Einsatz von Ressourcen

Die Abdeckung einer großen Anzahl an Anwendungsfällen einer Webfilterung durch einen DNS-Filter zeigt, dass der geringe Aufwand zum Einrichten eines DNS-Filters mit einem großen Gewinn an IT-Sicherheit verbunden ist. Werden schuleigene Geräte auch außerhalb der Schule verwendet, bietet sich der Einsatz einer DNS-Filter App an.

Da in den nächsten Jahren die Anforderungen an eine Webfilterung sich durch die zunehmende Zahl mobiler elternfinanzierter Geräte in den nächsten Jahren erhöhen könnte, sollte auf den Einsatz von Hardware in der Schule zur Webfilterung verzichtet werden und stattdessen flexiblere und leichter skalierbare Technologien zum Einsatz kommen.

5.4. Steigerung der IT-Sicherheit und Förderung der Medienkompetenz

Der Einsatz eines Webfilters ist aus den oben genannten Gründen sinnvoll.

Der Einsatz eines Webfilters ist eine Entscheidung, die von möglichst vielen Beteiligten der Schulfamilie mitgetragen werden sollte. Bei dieser Entscheidung sind auch lokale Gegebenheiten zu berücksichtigen (Budget, zeitlicher Aufwand,…).

5.5. Grenzen der Webfilterung am Beispiel der DNS-Filterung

DNS-Filterung kann nur dann unterstützen, wenn vor dem Verbindungsaufbau eine DNS-Namensauflösung stattfindet, um ein Ziel (ein Name) in IP-Adresse zu übersetzen. Daher gibt es bei der DNS-Filterung Grenzen:

- Sollte eine IP-Adresse in einer Applikation statisch verankert sein, so wäre es möglich, das Ziel direkt über die IP-Adresse - ohne vorangehende DNS-Namensauflösung – anzusprechen. In der Praxis kommt dieser Anwendungsfall allerdings so gut wie nie vor.
- Sollte eine Website mehrere Anwendungen anbieten, so ist es nicht möglich für diese Website differenziert zu blockieren. Subdomains werden bei der DNS-Filterung nicht einzeln gefiltert.
- DoH (DNS over HTTPS) oder DoT (DNS over TLS) ermöglichen es, den DNS-Dienst zu umgehen. Dies kann verhindert werden, indem DoH bzw. DoT Server, welche wiederum über eine normale DNS-Anfrage aufgelöst werden, per DNS-Filterung zu blocken.
- Eine Webfilterung – unabhängig davon welche - kann mittels VPN theoretisch umgangen werden. Allerdings ist zum Aufbau eine DNS-Anfrage nötig. Wird diese gefiltert, ist ein Verbindungsaufbau nicht möglich.

6. Beispiele für Filter-Regeln

Für unterschiedliche Personengruppen innerhalb der Schule sollten angepasste Filterregeln konfiguriert werden. Bei den Filterregeln wird zwischen Sicherheitskategorien und URL-Filter-Kategorien unterschieden. Sicherheitskategorien decken Sicherheitsrisiken unabhängig von Websites ab, während URL-Filter-Kategorien Websites in Kategorien klassifizieren.

Für die Personengruppe der **Lehrkräfte** können beispielhaft Inhalte aus folgenden Sicherheits- und URL-Filter-Kategorien geblockt werden:

Sicherheitskategorien:

- Malware: Blockiert Anfragen zum Zugriff auf Server, die Malware hosten, und auf kompromittierte Websites über jede Anwendung, jedes Protokoll oder jeden Port.
- Neue Domains: Dies ist eine Sicherheitskategorie, die Domains identifiziert, die innerhalb der letzten 24 Stunden zum ersten Mal von einem Nutzer abgefragt wurden.
- Command-and-Control-Server: Verhindert, dass kompromittierte Geräte über eine beliebige Anwendung, ein beliebiges Protokoll oder einen beliebigen Port mit Befehls- und Kontrollservern kommunizieren.
- Phishing Attacken: Blockiert den Zugang zu betrügerischen Websites, die darauf abzielen, persönliche Daten zu stehlen.
- DNS Tunneling VPN: Blockiert VPN-Dienste, die es Benutzern ermöglichen, ihren Datenverkehr zu verschleiern, indem sie ihn durch das DNS-Protokoll tunneln.
- Crypto Mining: Blockiert den Zugang zu Krypto-Mining-Pools, in denen sich „Miner" zusammenschließen und Ressourcen (Rechenleistung) teilen, um besser Kryptowährungen zu sammeln und zu teilen.

URL-Filter-Kategorien:

- Adult: Richtet sich an Erwachsene, ist aber nicht unbedingt pornografisch. Dazu gehören Clubs für Erwachsene (Stripclubs, Swingerclubs, Begleitservice, Stripperinnen), allgemeine Informationen über Sex, die nicht pornografischer Natur sind, Genitalpiercing, Produkte oder Grußkarten für Erwachsene, Informationen über Sex, die nicht im Zusammenhang mit Gesundheit oder Krankheit stehen
- Child Abuse Content: Weltweit illegale Inhalte zum sexuellen Missbrauch von Kindern.
- DoH und DoT: DNS über HTTPS (DoH) und DNS über TLS (Transport Layer Security) – Verschlüsselte DNS-Anfragen
- Extreme: Material sexuell gewalttätiger oder krimineller Natur, Gewalt und gewalttätiges Verhalten, geschmacklose, oft blutige Fotos, z. B. Autopsiefotos, Fotos von Tatorten, Verbrechens- und Unfallopfern, übermäßig obszönes Material, Schock-Websites.
- Filter Avoidence: Förderung und Unterstützung der nicht nachweisbaren und anonymen Webnutzung, einschließlich anonymer CGI-, PHP- und Glype-Proxy-Dienste.
- Pornography: Sexuell eindeutige Texte oder Darstellungen. Dazu gehören explizite Anime und Cartoons, allgemein explizite Darstellungen, sonstiges Fetischmaterial, explizite Chatrooms, Sexsimulatoren, Strip-Poker, Filme für Erwachsene, anzügliche Kunst, webbasierte explizite E-Mails.

Für die Personengruppe der Schüler können beispielhaft Inhalte aus folgenden Sicherheits- und URL-Filter-Kategorien geblockt werden:

Sicherheitskategorien:

- Malware: Blockiert Anfragen zum Zugriff auf Server, die Malware hosten, und auf kompromittierte Websites über jede Anwendung, jedes Protokoll oder jeden Port.
- Neue Domains: Dies ist eine Sicherheitskategorie, die Domains identifiziert, die innerhalb der letzten 24 Stunden zum ersten Mal von einem Nutzer abgefragt wurden.
- Command-and-Control-Server: Verhindert, dass kompromittierte Geräte über eine beliebige Anwendung, ein beliebiges Protokoll oder einen beliebigen Port mit Befehls- und Kontrollservern kommunizieren.
- Phishing Attacken: Blockiert den Zugang zu betrügerischen Websites, die darauf abzielen, persönliche Daten zu stehlen.
- DNS Tunneling VPN: Blockiert VPN-Dienste, die es Benutzern ermöglichen, ihren Datenverkehr zu verschleiern, indem sie ihn durch das DNS-Protokoll tunneln.
- Crypto Mining: Blockiert den Zugang zu Krypto-Mining-Pools, in denen sich „Miner" zusammenschließen und Ressourcen (Rechenleistung) teilen, um besser Kryptowährungen zu sammeln und zu teilen.
- Deutscher Jugendschutz-Filter: Diese Kategorie hilft dabei, das Ansehen von jugendgefährdenden Inhalten in Deutschland zu verhindern. Gesperrte Seiten für diese Kategorie enthalten deutschen Text. Diese Liste wird von der BPjM (Bundesprüfstelle für jugendgefährdende Medien) kontrolliert, um dem deutschen Recht zu entsprechen.
- Aktivierung von Safe Search im Browser: SafeSearch ist ein automatischer Filter für Pornografie und andere anstößige Inhalte, der in Suchmaschinen integriert ist. Wenn jemand einen unangemessenen oder anzüglichen Begriff eingibt, werden keine Ergebnisse angezeigt, die als unsicher oder problematisch angesehen werden könnten.

URL-Filter-Kategorien:

- Adult: Richtet sich an Erwachsene, ist aber nicht unbedingt pornografisch. Dazu gehören Clubs für Erwachsene (Stripclubs, Swingerclubs, Begleitservice, Stripperinnen), allgemeine Informationen über Sex, die nicht pornografischer Natur sind, Genitalpiercing, Produkte oder Grußkarten für Erwachsene, Informationen über Sex, die nicht im Zusammenhang mit Gesundheit oder Krankheit stehen
- Child Abuse Content: Weltweit illegale Inhalte zum sexuellen Missbrauch von Kindern.
- DoH und DoT: DNS über HTTPS (DoH) und DNS über TLS (Transport Layer Security) – Verschlüsselte DNS-Anfragen
- Extreme: Material sexuell gewalttätiger oder krimineller Natur, Gewalt und gewalttätiges Verhalten, geschmacklose, oft blutige Fotos, z. B. Autopsiefotos, Fotos von Tatorten, Verbrechens- und Unfallopfern, übermäßig obszönes Material, Schock-Websites.
- Filter Avoidence: Förderung und Unterstützung der nicht nachweisbaren und anonymen Webnutzung, einschließlich anonymer CGI-, PHP- und Glype-Proxy-Dienste.
- Pornography: Sexuell eindeutige Texte oder Darstellungen. Dazu gehören explizite Anime und Cartoons, allgemein explizite Darstellungen, sonstiges Fetischmaterial, explizite Chatrooms,

Sexsimulatoren, Strip-Poker, Filme für Erwachsene, anzügliche Kunst, webbasierte explizite E-Mails.