Google Safesearch und HTTPS Scanning

OctoGate / Schulamt

OctoGate
EINFACH. SICHER. GESCHÜTZT.-

Version 1.2

OctoGate Dokumentation

OctoGate IT Security Systems GmbH, Friedrich-List-Straße 42
33100 Paderborn

Tel.: ++49 5251 18040 0
Fax: ++49 5251 18040 39
Email: info@octogate.de
Internet: www.octogate.de

Verantwortlicher für den Inhalt: Frank Menne

Versionshistorie

Datum	Person	Version	Kommentar
21.2.2017	Frank Menne	0.9	Initial-Dokument
21.2.2017	Uwe Kauffoldt	1.0	Final abgestimmt
22.2.2017	Frank Menne	1.1	Tests mit INL
28.2.2017	Frank Menne	1.2	Speicheraufrüstung RVWBK

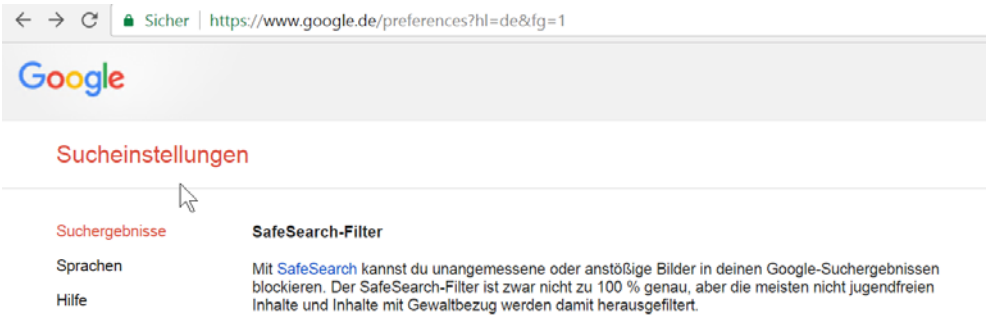
Inhalt

Google Safesearch und HTTPS Scanning 4
Was ist Google Safesearch ? 4
Google und HTTPS 5
https – Wie funktioniert das ? 5
Wie funktioniert dann https – Scanning in einer Firewall ? 6
Warum so kompliziert ? Warum kauft man nicht ein Zertifikat für die Firewall wie es die Websitebetreiber tun ? 7
Ist das nur bei OctoGate so kompliziert ? 7
Was heist das nun konkret für das HWBK und den Google Safesearch ? 7
Wir müssen transparentes HTTPS – Scanning auf der Firewall aktivieren und die Safesearch Funktion aktivieren. Das sollte aber nicht im laufenden Betrieb und nur für die Schuleigenen Geräte passieren, da wir sonst – wie oben beschrieben auf Zertifikatsfehler laufen. 7

Google Safesearch und HTTPS Scanning

Was ist Google Safesearch ?

Auf der Google Seite kann man in den Sucheinstellungen die Option “Safesearch” einschalten. Damit werden zusätzlich zu den Filter und Blacklisten der Firewall auch seitens Google die Suchergebnisse gefiltert.



Natürlich kann ein Schüler die Safesearch Funktion selbständig ein- und ausschalten. Hier kommt nun die OctoGate ins Spiel: Ist in unserem Produkt der SafeSearch Filter aktiviert, kann der Nutzer die Google Option nicht mehr ausschalten.

Safesearch gilt für Google Suchergebnisse – nicht für direkte von uns gefilterte Webzugriffe. Aber auch diese werden natürlich auf jugendgefährdende Inhalte geprüft.

Google und HTTPS

Gibt man im Browser “google.de” ein, so wird man automatisch auf die HTTPS – Variante der Google Seite umgeleitet. Also auf HTTPS://www.google.de.

Das heißt: Nur wenn eine Firewall den “sicheren” HTTPS – Datenstrom analysieren kann, lässt sich auch google SafeSearch firewallseitig erzwingen wie oben beschrieben.

https – Wie funktioniert das?

Das sichere https – Protokoll für das Ausliefern von Webseiten erfüllt zwei Aufgaben. Einerseits wird der Datenstrom verschlüsselt, so dass es im Normalfall nicht möglich ist, mitzulesen.

Es wird aber noch eine zweite Aufgabe wahrgenommen: Die Verifizierung der Gegenseite. Beispiel: Ich verbinde mich mit der Webseite meiner Bank. Dort fragt man für eine Überweisung nach meiner PIN Nummer. Wer sagt mit aber, dass ich gerade technisch wirklich mit dem Webserver der Bank kommuniziere und sich nicht ein Hacker dazwischengeschaltet hat, der so tut als ob er der Webserver der Bank wäre und somit an meine PIN gelangt?

Für diese Aufgabe kann https die Gegenseite verifizieren. Der Inhaber der Webseite (Bank) hat sich von einer “vertrauenswürdigen Stelle” zertifizieren lassen und ein technisches Zertifikat für seine Webseite bekommen. Der Browser des Users vertraut ebenfalls dieser “vertrauenswürdigen Stelle”. Somit kann der Browser verifizieren, dass der Webserver mit welchem gerade kommuniziert wird, wirklich die Sparkasse ist.

Wie funktioniert dann https – Scanning in einer Firewall?

Eine Firewall tut genau das, was wir im vorherigen Abschnitt vermeiden wollten: Sie gibt sich als der gegenläufige Webserver aus (Bank), um die Kommunikation mitlesen zu können.

Die Daten werden nicht gespeichert und somit ist die Lösung konform zum Datenschutz. Die Firewall scannt die Daten auf Viren, Trojaner und jugendgefährdende Inhalte – und natürlich kann Google – Safesearch somit eingeschaltet werden.

Aber was passiert mit dem Browser? Dieser erkennt, dass da etwas nicht passt und warnt den Browser.

Um dies zu verhindern, muss der Browser der OctoGate ebenso vertrauen wie der “vertrauenswürdigen Stelle” auf dem vorherigen Abschnitt.
Oder Technisch: Das Stammzertifikat der OctoGate muss im Browser des Clients bereits eingetragen worden sein. Dies ist im HWBK für die schuleigenen Geräte bereits der Fall.

Im Falle der BYOD – Geräte ist dies ggf. schwierig. In der Regel verzichtet man hier auf das HTTPS – Scanning oder setzt eine MDM (Mobile Device Management) - Lösung ein um die Zertifikate zu distribuieren.

Warum so kompliziert? Warum kauft man nicht ein Zertifikat für die Firewall wie es die Websitebetreiber tun?

Die Zertifikate für die Webseitebetreiber sind auf eine Web – Domain ausgestellt. Z.B. www.octogate.de. Der Client hinter der Firewall fragt natürlich viele verschieden Websites an. Ein “Zertifikat für alle” kann man aber nicht kaufen – damit würde man ja auch jedem mit genügend finanziellen Mitteln die Möglichkeit geben, den o.g. HTTPS – Schutz auszuhebeln.

Ist das nur bei OctoGate so kompliziert?

Nein. Die technologische Basis und der Schutz den HTTPS – bietet kann erfreulicherweise aktuell durch niemanden ausgehebelt werden. Dadurch ist die Sicherheit im Netz ein Stück weit gewährleistet.

Google Safesearch

Wir müssen transparentes HTTPS – Scanning auf der Firewall aktivieren und die Safesearch Funktion aktivieren.
Das sollte aber nicht im laufenden Betrieb und nur für die Schuleigenen Geräte passieren, da wir sonst – wie oben beschrieben auf Zertifikatsfehler laufen.