



# WebFilter

Sicher im Netz unterwegs



© Rob - fotolia.com

Erhöhen Sie die Online Sicherheit! Der WebFilter blockt automatisch gefährliche Webseiten und bietet Ihnen die Möglichkeit unerwünschte Seiten zu sperren. Sie setzen so konsequent Firmenrichtlinien zur Internetnutzung um und haben zusätzlich eine Online-Bandbreitenüberwachung.

## Schutz vor Gefahren

Es lauern im Internet einige Gefahren. Infizierte Webseiten und versteckte Downloads sind ein existentes Risiko für Ihr Computer Netzwerk und bedrohen die System- und Datensicherheit. Vorhandene Standard Schutzmaßnahmen wie z.B. eine Firewall und ein AntiVirus Programm sind jedoch nicht immer ausreichend (z.B. bei Userfehlern).

Zu den häufigsten Angriffsvektoren gehören mit

- ➔ 54 % Online-Interaktionen
- ➔ 16,6 % Internetzugang durch Download
- ➔ 37,4 % eMails mit schadhafte Link (Quelle: Verizon DBIR 2015)

Angriffe verlaufen heute meist über verschiedene Kanäle (Blended Threats), entsprechend macht es Sinn, mehrstufige Schutzmechanismen zu implementieren.

Der Brauner Telecom WebFilter ergänzt ideal Ihre vorhandene Security Struktur und...

- bietet Schutz vor mit Malware, Phishing, Trojaner, Proxys, Spyware, Adware, Botnets oder Spam infizierten Webseiten
- bietet Schutz vor versteckten Downloads
- blockt als unsicher gekennzeichnete und bereits als gefährlich identifizierte Websites.

## Webfilterung

Firmenrichtlinien zur Nutzung des Internets können Sie mit dem WebFilter einfach und sicher durchsetzen und überwachen.

Nutzerprofile lassen sich individuell anpassen, damit z.B. das Marketing immer auf soziale Netzwerke zugreifen kann, während die übrigen Mitarbeiter nur in der Mittagspause Zugriff auf diese Kategorie erhalten. So reduzieren Sie nicht arbeitsbezogene Internetaktivitäten.

- ➔ **Zeitbeschränktes Internetsurfen**  
z.B. Freigaben in der Mittagspause)
- ➔ **Filterung unerlaubter Internetseiten**  
z.B. soziale Netzwerke, Spiele, Versteigerungsseiten, Erotik ...
- ➔ **Risiko von Sicherheitsverletzungen und gesetzlichen Haftungsansprüche werden verringert**  
z.B. da unseriöse Seiten oder illegale Up- und Downloads verhindert werden.
- ➔ **Jugendschutzbestimmungen werden eingehalten**  
z.B. bei jugendlichen Auszubildenden

So zentral wie möglich und so individuell wie nötig, erstellen Sie zentrale Sicherheitsrichtlinien, können aber jederzeit individuell Freigaben und Sperrungen für einzelne Rechner vornehmen.

## Bandbreitenüberwachung

Erhalten Sie automatisierte Warnmeldungen bei übermäßiger Bandbreitennutzung im Netzwerk und verhindern Sie so Geschwindigkeitseinbußen im Netzwerk oder ungewollte Kosten.

### INTERNET SECURITY



© arrow - fotolia.com

## Einfache Administration

Bei der Einrichtung und Verwaltung des WebFilters haben Sie viele Möglichkeiten. Sie können zentrale oder gruppenbasierte Richtlinien erstellen und diese auf einfache Art und Weise zentral ins Netzwerk bzw. auf die gewünschten Rechner ausrollen. Anpassungen sind individuell je Rechner möglich.

- ➔ Blockieren Sie als unsicher gekennzeichnete und bereits als gefährlich identifizierte Websites.
- ➔ Verwenden Sie die Webfilterung, um die Firmenrichtlinien für den Arbeitsplatz durchzusetzen.
- ➔ Definieren Sie Whitelists und Blacklists für Websites als Ergänzung der vorhandenen kategoriebasierten Filterung.
- ➔ Begrenzen Sie Firmenrichtlinien zeitlich, damit private Seiten außerhalb der Arbeitszeiten aufrufbar sind.
- ➔ Nutzen Sie die Bandbreitenüberwachung und erhalten Sie automatisierte Warnmeldungen bei übermäßiger Bandbreitennutzung in einem Netzwerk.
- ➔ Filtern Sie die Internetaktivität nach Tag, Kategorie und URL um Trends, Hochverbrauch und Unregelmäßigkeiten zu erkennen, jeweils mit oder ohne Anzeige der URL, je nach Datenschutzerfordernissen.

Der WebFilter ist eine benutzerfreundliche und wartungsfreie Lösung, die eine einfache Integration bei minimalen Administrationsaufwand bietet.



## Einfach & sicher für Nutzer

Einmal installiert, läuft der WebFilter automatisch bei jedem Start des Rechners im Hintergrund – der Nutzer muss sich nicht am WebFilter anmelden.

Das Eingreifen oder Ändern des WebFilters durch den Nutzer ist nicht möglich, möchte er auf eine gesperrte Webseite zugreifen, muss er dies dem Administrator melden.

Auf diese Weise ist sichergestellt, dass Firmenrichtlinien nicht umgangen werden können. Der Administrator kann Websites individuell für jeden Rechner gezielt freigeben oder sperren. Damit bietet unser WebFilter größtmögliche Flexibilität bei gleichzeitiger Einhaltung der Firmenrichtlinien gegeben.

## Sicherheit

Mit den gehosteten Security Lösungen von Brauner Telecom steigern kleine- und mittelständische Unternehmen die Sicherheit, denn mit den Angeboten erhalten Sie Zugang auf Technologien, die sich bislang nur Großfirmen leisten konnten.

Wie bei allen unseren gehosteten Lösungen, gilt auch hier:

- Serverstandort Deutschland
- Deutsches Recht
- Deutscher Datenschutz

## Tarif

Preislich sehr attraktiv und faire Bedingungen sind weitere Vorteile des Brauner Telecom WebFilters.

- Kostengünstiger Service
- Monatliche Abrechnung je Gerät
- Kein Kauf von Software
- Nie wieder Lizenzen verlängern
- Keine Laufzeiten (zum Monatsende kündbar)
- Keine einmalige Einrichtungsgebühr

### WebProtection WebFilter

- ➔ Je Rechner
- ➔ 1,79 € / Monat\*

30 Tage Try-Before-You-Buy

Testen Sie unser WebProtection WebFilter 30 Tage ohne Verpflichtung. Die ersten 30 Tage werden Ihnen nur berechnet, wenn Sie den WebProtectionWebFilter weiter nutzen wollen.

\*alle Preise netto zzgl. Gesetzlicher MwSt.

So erreichen Sie uns:

**Brauner Telecom**

☎ 0800 220 50 220

@ support@brauner-telecom.de

www.brauner-telecom.de

Weitere Security, eMail und Teamwork Lösungen finden Sie auf [www.cloud-systempartner.de](http://www.cloud-systempartner.de)