The Internet you deserve

https://feeltr.io

Warum Feeltr nutzen?

Feeltr hat die Aufgabe, die Verbindungen in **Ihrem Netwerk zu filtern**, unabhängig davon, ob es sich um ein LAN (Local Area Network) oder ein WAN (Wide Area Network) handelt.

Das Filtern hat drei Ergebnisse:

- Ein **schlankeres Netzwerk**, da Feeltr unnötige Anfragen blockiert, was zu mehr Bandbreite und somit zu einer schnelleren Verbindung führt;
- Ein **sichereres Netzwerk**, da Feeltr bestimmte Arten von Datendiebstahl und Malware blockiert;
- Ein **weniger umweltschädliches Netzwerk**, da Feeltr durch die Verringerung der Bandbreitenbelegung und das Stoppen von Malware den gesamten C02-Verbrauch senkt.

Feeltr ist daher eine angemessene Antwort auf die qualitativen, sicherheits - und umweltbezogenen Herausforderungen der Computernetzwerke von großen Unternehmen, Gesundheitszentren, Schulen und akademischen Einrichtungen, Staaten, öffentlichen WIFI-Verbindungen, IOT-Betreibern, Internetdienstanbietern usw.

Wie verbessert Feeltr Ihr Netzwerk?

Feeltr ist ein sicherer **DNS-Server.**

Die Aufgabe von Feeltr ist es, so weit wie möglich die:

- Biometrische Erhebungen
- Diebstahl von privaten Daten
- Missbrauch durch Werbung
- Adwares
- Ransomwares
- Malwares
- Minerwares
- Spywares

Biometrische Erhebungen

Biometrische Daten sind technische Informationen, die von einer Software an das Unternehmen, das sie entwickelt hat, gesendet werden.

Eine Anwendung auf einem Mobiltelefon sendet z. B. das Modell des Telefons, die Seriennummer, den Netzbetreiber, die Anzahl der Ladezyklen des Akkus etc.

Bei einem Internetbrowser auf einem Computer kann dies z. B. die Adressen der besuchten Webseiten sein.

Diebstahl von privaten Daten

Diebstahl privater Daten ist die Weitergabe von Daten, die sich auf Ihren Geräten befinden, durch eine Software an das Unternehmen, das die Software entwickelt hat.

Beispielsweise wird eine Anwendung auf einem Mobiltelefon, der Sie den Zugriff auf die Kontakte Ihres Smartphones gestattet haben, Ihr gesamtes Adressbuch (und de facto alle privaten Daten Ihrer Kontakte) übertragen, dessen Inhalt dann an Informationsbroker weiterverkauft wird, die Datenbanken zu Marketingzwecken vermarkten.

Für Computer gilt die gleiche Logik.

Missbrauch durch Werbung

Für den Begriff des Werbemissbrauchs gibt es zwei mögliche Definitionen:

- Entweder es handelt sich um eine Überbelichtung durch Werbung, die das Surferlebnis verschlechtert oder sogar unmöglich macht ;
- Oder es handelt sich um Werbung, die nicht den Standards entspricht, die von der ACC (« Acceptable Ads Committee » https://acceptableads.com/committee/).

ÜBERBELASTUNG: Übermäßige Werbebelastung liegt vor, wenn eine Internetseite zu viele Werbeanzeigen enthält, oder wenn die Werbeanzeigen den Zugang zum Inhalt verhindern, oder wenn eine Kampagne zu stark auf Sie abzielt (d. h. mehr als 5 Werbeanzeigen für ein und dasselbe Produkt pro Tag).

STANDARD FÜR AKZEPTABLE WERBUNG: Akzeptable Werbeanzeigen sind Werbeanzeigen, die nicht aufdringlich oder störend sind. Sie sind respektvoll, mischen sich nicht in den Inhalt ein und sind deutlich mit dem Wort "Werbung" oder einem Äquivalent gekennzeichnet. Werbeanzeigen dürfen den normalen Lesefluss des Nutzers nicht unterbrechen. Diese Werbeanzeigen müssen über, seitlich oder unter dem Hauptinhalt platziert werden.

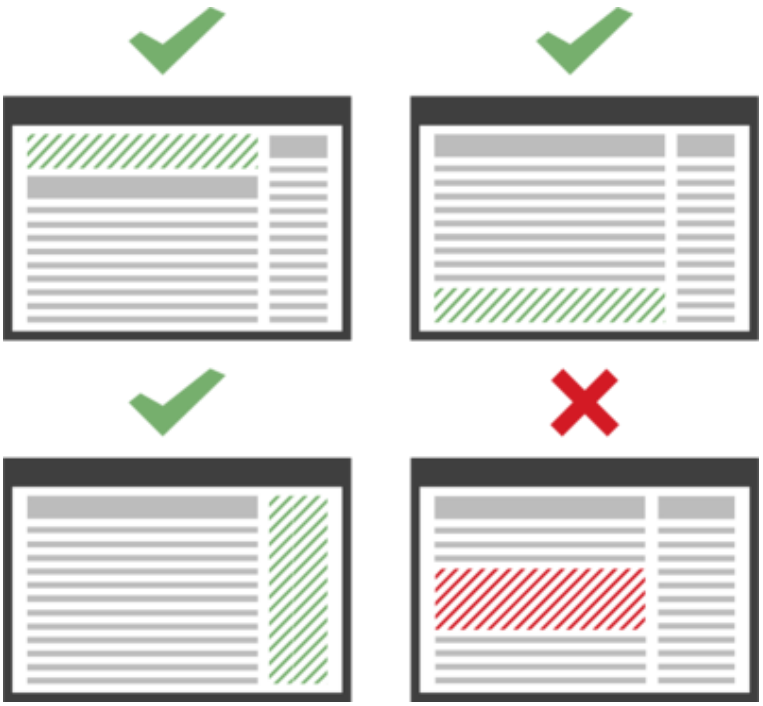

Figure 1- source : https://acceptableads.com/committee/

Die Anforderungen an die Größe hängen davon ab, wo die Werbeanzeige platziert wird:

- Wenn sie über dem Hauptinhalt platziert wird, beträgt die maximale Höhe der Anzeige 200 Pixel.
- Wenn sie neben dem Hauptinhalt platziert wird, betragt die maximale Breite der Anzeige 350 Pixel.
- Wenn sie unter dem Hauptinhalt platziert wird, beträgt die maximale Höhe der Anzeige 400 Pixel.

Werbeanzeigen müssen auf der Standardbildschirmgröße ausreichend Platz für den Hauptinhalt lassen: 1366 x 768 für Computer, 360 x 640 für Mobilgeräte und 768 x 1024 für Tablets.

Alle Werbeanzeigen, die oberhalb der Wasserlinie platziert werden (der Teil der Internetseite, der beim Öffnen einer Seite zuerst im Browserfenster erscheint, je nach Standardbildschirmgröße), sollten weniger als 15 % des sichtbaren Teils der Internetseite einnehmen. Werbeanzeigen, die unterhalb der Wasserlinie platziert werden, sollten weniger als 25 % des sichtbaren Teils der Internetseite einnehmen.

Figure 2- source : https://acceptableads.com/committee/

Adware

Ein ADWARE ist ein Computerprogramm, das auf der Oberfläche einer Software oder über den Internetbrowser Werbung in Form von chronisch aufspringenden Pop-up-Fenstern einblendet.

Ransomware

Ein RANSOMWARE ist eine bösartige Computersoftware, die Daten oder vielmehr den Besitzer dieser Daten als Geisel nimmt. Dazu verschlüsselt und sperrt sie die Dateien auf Ihrem Computer und verlangt ein Lösegeld für einen Schlüssel, mit dem die Dateien wieder entschlüsselt werden können. Ransomware ist ein großes Risiko für die Cybersicherheit von Unternehmen.

Malware

Ein MALWARE ist ein bösartiger, aggressiver Virentyp, dessen Ziel es ist, Computer, Computersysteme, Tablets oder mobile Geräte zu beschädigen oder außer Betrieb zu setzen.

Minerware

Eine MINERWARE ist ein Code, der ohne Ihr Wissen fortgeschrittene Berechnungen auf Ihren Geräten durchführt, um für Gruppen von Cyberkriminellen Kryptowährungen wie Bitcoin zu generieren. Die Auswirkungen der MINERWARE sind eine Verlangsamung Ihrer Geräte, deren Ressourcen von dieser speziellen Art von Malware monopolisiert werden.

Spyware

Eine SPYWARE ist eine Software, die Sie ausspioniert, indem sie z. B. Fotos von Ihrer Webcam macht oder alles kopiert, was Sie auf der Tastatur eingeben, und die Informationen dann an diese Cyberkriminellen weiterleitet.

Welche Angebote hat Feeltr?

Feeltr kann entweder ein einzelnes Gerät schützen oder ein ganzes Netzwerk, wie LAN oder WAN, und damit de facto alle Geräte, die mit diesem Netzwerk verbunden sind.

Unter einem Gerät verstehen wir:

- Computer
- Tablet
- Telefon
- Verbundene Geräte (Geräte zur Erfassung des Gesundheitszustands, medizinische Geräte, private IOT wie ein verbundener Kühlschrank, professionelle IOT wie eine Sonde oder Kamera usw.).

Wenn Sie einen individuellen Schutz realisieren möchten, abonnieren Sie bitte die Software über: https://feeltr.io/index.html

Wenn Sie ein Netzwerk schützen wollen, genügt es, Feeltr als Standard-DNS für Ihr Netzwerk einzustellen. Es handelt sich also um eine extrem einfache Konfiguration, die Sie an Ihren Routern vornehmen können. Für ein individuelles Angebot auf der Grundlage Ihrer spezifischen Bedürfnisse kontaktieren Sie uns bitte per E-Mail unter feeltr@simpl.team

Feeltr ist gut für den Planeten

Laut GREENPEACE würde der weltweite Internetverkehr **+/- 500 Millionen Tonnen CO2** verursachen, was dem **doppelten CO2-Fußabdruck eines Landes wie Spanien** entspricht.

Indem Sie Ihre Bandbreite durch die Nutzung von Feeltr verringern, verringern Sie den CO2-Fußabdruck Ihres Computers.

Wenn wir beispielsweise **25% des weltweiten Datenverkehrs** über Feeltr blockieren könnten, würde dies **175 Millionen Tonnen CO2** einsparen.

Zum Vergleich: Die während der COP21 festgelegte weltweite Anstrengung, die nicht einmal dadurch erreicht wurde, dass die Welt während der COVID19-Krise stillstand, besteht darin, **die Emissionen um etwa 150 Millionen Tonnen zu senken.**