Disable and Remove Google Fonts

Disable and Remove Google Fonts

Von Fonts Plugin

Beschreibung

Verbessert die Leistung der Website, indem Google Fonts deaktiviert werden, die von Themes oder Plugins geladen werden.

While this plugin removes Google Fonts from as many themes and plugins as possible, some require additional steps, we have detailed those here: Remove Google Fonts from WordPress

Plugin-Kompatibilität

Dieses Plugin funktioniert mit allen WordPress-Themes. Speziell getestet wurde es für folgende Themes:

- Twenty Twelve
- Twenty Thirteen
- Twenty Fourteen
- Twenty Fifteen
- Twenty Sixteen
- Twenty Seventeen
- Twenty Nineteen
- Twenty Twenty
- Avada
- Enfold

- Sydney
- Hestia
- Hueman
- Vantage
- ColorMag
- Shapely
- OnePress
- JupiterX
- Storefront
- Divi Extra
- Zerif Lite

Es entfernt auch Google Fonts, die von den folgenden Plugins geladen werden:

- Divi
- MailPoet
- Elementor
- Beaver Builder
- Revolution Slider
- WPBakery (Visual Composer)

Neben der Verbesserung der Ladezeit kann das Entfernen der Google Fonts auch dazu beitragen, die Bestimmungen der DSGVO einzuhalten.

Fehler

Wenn du ein Problem mit diesem Plugin feststellst, melde dich bitte hier!

Mitwirkende

Jeder ist willkommen, zu diesem Plugin beizutragen.

Es gibt verschiedene Arten, wie du dich beteiligen kannst:

1. Melde uns Fehler, die du feststellst.

2. Übersetze „Disable and Remove Google Fonts“ in verschiedene Sprachen
3. Gib uns Feedback und mache Vorschläge für Verbesserungen

FAQ

Wird mein Theme mit „Disable and Remove Google Fonts“ funktionieren?

Site Kit by Google – Analytics, Search Console, AdSense, Speed

Site Kit by Google – Analytics, Search Console, AdSense, Speed

Von Google

Version: **1.87.0** Zuletzt aktualisiert: **vor 3 Tagen** Aktive Installationen: **2+ Millionen** WordPress-Version: **4.7 oder höher** Getestet bis: **6.1** PHP-Version: **5.6 oder höher** Sprachen: Schlagwörter:

adsenseanalyticsgooglepagespeed insightsSearch Console

Beschreibung

Site Kit is the official WordPress plugin from Google for insights about how people find and use your site. Site Kit is the one-stop solution to deploy, manage, and get insights from critical Google tools to make the site successful on the web. It provides authoritative, up-to-date insights from multiple Google products directly on the WordPress dashboard for easy access, all for free.

Bringt die besten Google-Dienste zu WordPress

Site Kit includes powerful features that make using these Google products seamless and flexible:

- Easy-to-understand stats directly on your WordPress dashboard
- Offizielle Statistiken verschiedener Google-Werkzeuge, alle in einem Dashboard
- Quick setup for multiple Google tools without having to edit the source code of your site
- Metrics for your entire site and for individual posts
- Easy-to-manage, granular permissions across WordPress and different Google products

Unterstützte Google-Tools

Site Kit shows key metrics and insights from different Google products:

- **Search Console:** Understand how Google Search discovers and displays your pages in Google Search. Track how many people saw your site in Search results, and what query they used to search for your site.
- **Analytics:** Explore how users navigate your site and track goals you've set up for your users to complete.
- **AdSense:** Keep track of how much your site is earning

you.

- **PageSpeed Insights:** See how your pages perform compared to other real-world sites. Improve performance with actionable tips from PageSpeed Insights.
- **Tag Manager:** Use Site Kit to easily set up Tag Manager- no code editing required. Then, manage your tags in Tag Manager.
- **Optimize:** Use Site Kit to easily set up Optimize- no code editing required. Then, set up A/B tests in Optimize.

FAQ

Für weitere Informationen, besuche die offizielle Site Kit Website.

Ist Site Kit kostenlos?

What are the minimum requirements for Site Kit?

Why is my dashboard showing “gathering data” and none of my service data?

Why aren’t any ads appearing on my site after I connected AdSense?

Is Site Kit GDPR compliant?

Where can I get additional support?

Mitwirkende & Entwickler

„Site Kit by Google – Analytics, Search Console, AdSense, Speed“ ist Open-Source-Software. Folgende Menschen haben an diesem Plugin mitgewirkt:

Sperren (Schützen) von Dateien mit PMPro

Paid Memberships Pro bietet Ihnen viele Optionen zum Sperren Ihrer WordPress-Beiträge und -Seiten direkt nach dem Auspacken – aber vielleicht möchten Sie auch den Zugriff auf geschützte Dateien einschränken. Vielleicht möchten Sie den Mitgliedern beispielsweise den Zugriff auf eine PDF-Arbeitsmappe oder einen begleitenden Audioguide als Upselling anbieten.

Dieses Rezept zeigt Ihnen, wie Sie Dateien in Ihrer WordPress-Medienbibliothek mit Paid Memberships Pro sperren.

Inhaltsverzeichnis

Dateischutz verstehen

Der Schutz von Dateien auf Ihrer WordPress-Site erfordert einige zusätzliche Einschränkungsschritte auf Serverebene. Aufgrund dieser Serverüberlegungen aktivieren wir den Dateischutz nicht standardmäßig in Kern-PMPro. Um Dateien zu schützen, benötigen Sie:

1. Die Möglichkeit, Umschreibungsregeln hinzuzufügen, indem Sie die .htaccessDatei.
2. Die Möglichkeit, WordPress zu bearbeiten wp-config.phpDatei.

3. Genügend Speicherplatz auf Ihrem Server, um Dateien über ein PHP-Skript bereitzustellen.
4. Um sicherzustellen, dass Ihr Uploads-Ordner nicht von einem CDN bereitgestellt wird (z. B. mit WP Engine und einigen anderen Hosts)

In Bezug auf Punkt 3 oben begrenzt die Menge an Speicherplatz, die Ihrer Website zur Verfügung steht, wie groß eine Datei ist, die Sie geschützt bereitstellen können. Beispielsweise können Sie nach dem Aktivieren des Dateischutzes möglicherweise ein 1-MB-Bild, aber kein 50-MB-PowerPoint-Dokument bereitstellen. Wir empfehlen, einige Dateien in der Größe zu testen, die Sie freigeben möchten, um sicherzustellen, dass Ihr Server über genügend Speicher verfügt, um den Dateischutz zu unterstützen.

Beachten Sie, dass diese Methode nur für Dateien gilt, die über die „Medien“-Bibliothek auf Ihrer WordPress-Site hochgeladen wurden. Bei Bedarf haben wir ein begleitendes Tutorial zum Sperren von Dateien und Verzeichnissen außerhalb von WordPress .

So sperren Sie Dateien nur für Mitglieder

Führen Sie die folgenden Schritte aus, um Dateischutz nur für Mitglieder zu Ihrer WordPress-Mitgliederseite hinzuzufügen.

1. Fügen Sie diese Zeile zu Ihrer hinzu wp-config.php Datei

```
define('PMPRO_GETFILE_ENABLED', true);
```

2. Fügen Sie für Sites, die mit Apache gehostet werden, diesen Code zu Ihrer hinzu .htaccessDatei, über der # BEGIN WordPressLinie.

```
RewriteBase /
RewriteRule     ^wp-content/uploads/(.*)$     /wp-
```

content/plugins/paid-memberships-pro/services/getfile.php [L]

Stellen Sie sicher, dass es keine Zeilenumbrüche/Textumbrüche gibt, nachdem Sie diese Regel zu Ihrer .htaccess-Datei hinzugefügt haben. Diese Regel muss möglicherweise für Websites angepasst werden, auf denen WordPress in einem Unterverzeichnis installiert ist, oder wenn die Pfade in Ihrem Setup unterschiedlich sind.

Fügen Sie für Websites, die mit NGINX gehostet werden, diesen Code zu Ihrer NGINX-Konfigurationsdatei unter den anderen WP-Regeln hinzu. Auch diese Regel muss möglicherweise für Websites angepasst werden, auf denen WordPress in einem Unterverzeichnis installiert ist, oder wenn die Pfade in Ihrem Setup unterschiedlich sind.

rewrite ^/wp-content/uploads/(.*)$ /wp-content/plugins/paid-memberships-pro/services/getfile.php last;

3. Passen Sie alternativ die an .htaccessRegel, nur bestimmte Dateitypen zu sperren.

Die folgende Regel sperrt nur pdf, doc, docx, ppt, und zipDateien. Diese Anpassung vermeidet das Ausführen von Bildern und anderen statischen Dateien, die sich möglicherweise in Ihrem befinden uploadsOrdner durch die getfile.phpSkript, das Websites verlangsamen kann.

Sie können die geschützten Dateierweiterungen in die spezifischen Dateitypen ändern, die Sie schützen müssen.

RewriteBase /
RewriteRule ^wp-content/uploads/.*(\.pdf|\.doc|\.docx|\.ppt|\.zip)$ /wp-content/plugins/paid-memberships-pro/services/getfile.php [L]

4. Hier ist die Version dieser Regel, die Sie für NGINX-Server verwenden würden:

rewrite ^\/wp-content\/uploads\/(.*[\.pdf|\.doc|\.docx|\.ppt|\.zip])$ /wp-

content/plugins/paid-memberships-pro/services/getfile.php last;

5. Stellen Sie sicher, dass Ihre Dateien an geschützte Posts „angehängt“ sind.

Dateien, die über den Bildschirm zum Bearbeiten von Beiträgen hochgeladen wurden, werden an diesen Beitrag angehängt. Dateien, die direkt in die Medienbibliothek hochgeladen werden, sind nicht angehängt. Um den Anhang einer Datei zu überprüfen, suchen Sie sie in der Medienbibliothek und überprüfen Sie die Registerkarte „Hochgeladen auf“. Von dort aus können Sie es lösen oder am richtigen geschützten Pfosten anbringen.

6. Dateischutz testen.

Nachdem Sie diese Schritte ausgeführt haben, testen Sie den Schutz, indem Sie eine Datei auf eine Seite oder einen Beitrag hochladen, für deren Zugriff eine Mitgliedschaft erforderlich ist. Für die Anzeige der angehängten Datei sind dieselben Mitgliedschaftsstufen erforderlich.

Seien Sie vorsichtig, wenn Sie versuchen, Bilder zu schützen. Abgesehen davon, dass Sie möglicherweise Ihren Server belasten, wenn Sie viele Bilder haben, die keinen Schutz benötigen, erstellt WordPress verkleinerte Versionen von Bilddateien, und PMPro ist noch nicht schlau genug, um die verkleinerten Versionen mit dem angehängten Beitrag zu verknüpfen.

Wie diese Methode des Dateischutzes funktioniert

Was hier passiert, ist, dass jeder Link zu einer Datei in /wp-content/uploads/.../wird durch die geleitet getfile.phpSkript, bevor es im Browser geladen wird. Dieses Skript ermittelt den Beitrag, an den die Datei angehängt ist, und prüft dann, ob

der angemeldete Benutzer Zugriff auf diesen Beitrag hat. Wenn dies der Fall ist, wird die Datei über das Skript bereitgestellt. Wenn nicht, wird ein 503-Fehler angezeigt.

Holen Sie sich Expertenunterstützung für Ihre Fragen zum Dateischutz

Lassen Sie mich wissen, wie das für Sie funktioniert. Wenden Sie sich bei Problemen an unser Support-Team . Wir werden versuchen, Ihnen bei allen Problemen zu helfen, die Sie haben.

Beachten Sie, dass diese Art von Funktionalität stark von Ihrem Server-Setup abhängt und Sie möglicherweise einen Entwickler einstellen oder extra bezahlen müssen, um dies vollständig einrichten zu lassen.

Autor: Jason Coleman

Jason ist Mitbegründer von Paid Memberships Pro, dem 100 % Open Source Mitgliedschafts-Plugin für WordPress. Er treibt WordPress seit vielen Jahren an seine Grenzen und ist ein Befürworter der Verwendung von WordPress als Anwendungsframework zum Erstellen von Websites und Apps, die über die typischen Blog- oder CMS-Sites hinausgehen. Gepostet in Code-Rezepte . Setzen Sie ein Lesezeichen auf den Permalink . Zuletzt aktualisiert: 19. Oktober 2011 .

E-Mail-Adresse zur Kontaktaufnahme

Markt + Trends | IT-Recht & Datenschutz

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Das Landgericht Düsseldorf hat erneut bestätigt, dass eine kommerzielle Webseite eine **E-Mail-Adresse zur Kontaktaufnahme** durch Internetnutzer enthalten muss (LG Düsseldorf, Beschluss vom 17.08.2022 – 12 O 219/22). Bei Verstößen können

Webseitenbetreiber auf Basis der Regelung des § 5 Telekommunikationsgesetz erfolgreich abgemahnt werden.

Neueste Entwicklungen im Datenschutzrecht

Markt + Trends | IT-Recht & Datenschutz

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein

etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Das Arbeitsgericht Baden-Württemberg hat zu zwei **Fragen des Auskunftsrechts** nach der Datenschutz-Grundverordnung entschieden (ArbG Baden-Württemberg, Urteil vom 10.08.2022, 2 Sa 16/21 ab Rdnr. 96). Zum einen genügt nach dessen Auffassung eine Auskunftserteilung per E-Mail, da die DSGVO keine besondere Form hierfür vorgibt. Zum anderen stellte das Gericht klar, dass der Auskunftsverpflichtete sich des Datenschutzbeauftragten als Erfüllungsgehilfen bedienen darf.

Wegen der **missbräuchlichen Verwendung von Grundbuchdaten** hat der Datenschutzbeauftragte Baden-Württembergs ein Bußgeld in Höhe von 55 000 Euro verhängt. Ein Vermessungsingenieur hatte von seiner gesetzlichen Erlaubnis zur Einsicht in Grundbücher Gebrauch gemacht und die dadurch gewonnenen Erkenntnisse an einen Bauträger übermittelt. Dieser wiederum hat den Eigentümern Kaufangebote für ihre Grundstücke unterbreitet. Beide beteiligten Parteien mussten einen Teil des Bußgeldes bezahlen.

Ein Bußgeld von über 500 000 Euro hat der Berliner Datenschutzbeauftragte verhängt, weil er in der **Bestellung eines Datenschutzbeauftragten** in einem E-Commerce-Konzern einen Interessenkonflikt sieht. In dieser Unternehmensgruppe

war eine Person zum Datenschutzbeauftragten ernannt worden, die gleichzeitig in zwei weiteren Unternehmen als Geschäftsführer tätig war. Diese Unternehmen waren noch dazu Auftragsdatenverarbeiter für das betroffene Unternehmen.

Das Bundesamt für Arzneimittel und Medizinprodukte hat seine Prüfkriterien für den **Datenschutz für digitale Gesundheitsanwendungen** überarbeitet. Sie sind Grundlage für die Zertifizierung der Datenschutzkonformität entsprechender Medizinprodukte. Konkret geht es dabei um Apps auf Rezept, die seit etwa zwei Jahren von Ärzten verschrieben werden können. Neben diesen digitalen Gesundheitsanwendungen hat das Amt als erste EU-Behörde nun auch digitale Pflegeanwendungen in den Geltungsbereich aufgenommen. In die Überarbeitung waren der Bundesdatenschutzbeauftragte sowie das Bundesamt für Sicherheit in der Informationstechnik eingebunden.

Der bekannte IT-Rechtsprofessor Thomas Hoeren aus Münster hat gemeinsam mit Mitarbeitenden der Forschungsstelle des DFN-Vereins eine **überarbeitete Musterdatenschutzerklärung** veröffentlicht (siehe ix.de/zcph). Sie darf von allen Webseitenbetreibern als Mustertext herangezogen und verwendet werden. Allerdings weisen die Autoren darauf hin, dass sie keine Gewähr für Richtigkeit und Vollständigkeit übernehmen, und warnen vor einem unbedachten Übernehmen. *Tobias Haar* (ur@ix.de)

Mehr IT-Sicherheit für KMU

Zwei neue Publikationen sollen

kleinen und mittleren Unternehmen zu mehr Widerstandsfähigkeit gegen Angriffe verhelfen.

Markt + Trends | IT-Sicherheit

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Kleine und mittlere Unternehmen haben in der Regel nur wenige Ressourcen für IT-Sicherheit. Trotzdem müssen sie den mit der Digitalisierung einhergehenden Bedrohungen begegnen und individuelle Schutzmaßnahmen ergreifen. Für das Entwickeln einer unternehmensweiten Sicherheitsstrategie und das

systematische Etablieren von Sicherheit in allen Prozessen ist ein Informationssicherheitssystem (ISMS) hilfreich. Gerade bei KMU ist dieses Werkzeug jedoch noch wenig bekannt oder scheidet aus Mangel an finanziellen und personellen Mitteln aus.

Hier setzt die Broschüre „Kleine und mittlere Unternehmen mit Sicherheit digitalisieren“ des BMWi-geförderten Netzwerks Mittelstand-Digital an. Mittels einer Umfrage erforschten die Autoren, wie verbreitet oder bekannt ISMS bei kleinen Unternehmen sind, welche Hindernisse oder Motivationen es für eine Einführung oder Zertifizierung gibt und welche Effekte es hat, ein ISMS zu implementieren. Die Broschüre stellt die gängigsten ISMS vor, gibt Handlungsempfehlungen für KMU und nennt weitere kostenlose Angebote – beispielsweise zum Ermitteln des Status quo der IT-Sicherheit, einen Leitfaden

zum Implementieren eines ISMS, Erfahrungsberichte von KMU, Checklisten zum IT-Sicherheitsmanagement oder eine interaktive Plattform zur Entwicklung eines eigenen Sicherheitskonzepts.

Einen anderen Ansatz fährt die jüngste Publikation aus dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Dort hat man im Jahr 2020 ein eigenes Referat für kleine und mittlere Unternehmen eingerichtet, die (nach EU-Klassifikation) 99,4 Prozent aller Unternehmen in Deutschland ausmachen. Jenseits von ISO-Normen und IT-Grundschutz-Kompendium vermittelt die Broschüre die wichtigsten Grundlagen der IT-Sicherheit in 14 Fragen. Geschrieben sind sie so, dass auch nicht mit der Technik befasste Geschäftsführer nach der Lektüre wissen, was sie in ihrem Unternehmen umsetzen müssen – oder, wenn das nicht selbst zu stemmen ist, durch einen Dienstleister umsetzen lassen sollten. Beide Broschüren sind über ix.de/zjqs zu finden. (ur@ix.de)

Bundesnetzagentur will digitale Plattformen beaufsichtigen

Markt + Trends | World Wide Web

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Die Bundesnetzagentur (BNetzA) bringt sich für die Rolle des nationalen Koordinators für Digitalisierung nach dem Digital Services Act (DSA) in Stellung. Dieser soll Onlineplattformen mit mehr als 45 Millionen aktiven Nutzern beaufsichtigen und als Schnittstelle zur EU-Kommission dienen. In einer Onlinediskussion bekräftigte BNetzA-Vizepräsident Wilhelm Eschweiler, seine Behörde sei für die Plattformaufsicht gut gerüstet, man habe Informatiker und Datenwissenschaftler eingestellt und sei auf dem Weg, sich von einer sektorspezifischen Aufsichtsbehörde zu einer Digitalagentur zu

entwickeln.

Auch sei die BNetzA bereits jetzt dafür zuständig, Bußgelder gegen Provider zu verhängen, und sie sei politisch unabhängig. Derzeit sind viele konkrete Zuständigkeiten bei der Umsetzung des DSA noch offen. Eschweiler sprach von einem „Schaulaufen der Behörden“, das derzeit stattfinde. (ulw@ix.de)

Chrome-Browser bekommt Root-CA-Speicher

Markt + Trends | World Wide Web

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…
Google hat seine Pläne für eine im Chrome-Browser eingebaute Verwaltung von Root-CAs konkretisiert und das bereits 2020 angekündigte Chrome Root Program offiziell gestartet. Bislang verwendet Chrome für die Überprüfung von HTTPS-Zertifikaten das Betriebssystem als Vertrauensanker und lässt alle Zertifikate gelten, deren digitale Unterschrift sich auf eines der vom Betriebssystem installierten Root-CA-Zertifikate zurückführen lässt. Künftig soll ein Chrome Root Store im Browser diese Zertifikate verwalten. Google bestimmt dann selbst, welche Root CA (Certification Authority) als vertrauenswürdig gilt, und verstärkt so seinen Einfluss auf die Herausgeber der Root CAs.

Chrome Root Store soll lokal verwaltete Zertifikate berücksichtigen. Wenn also ein Zertifikat zum Beispiel via Windows Group Policy verteilt wird, soll es Chrome als vertrauenswürdig einstufen. Den Übergang will Google allmählich vollziehen, bereits der im September erschienene Chrome 105 wird laut Google für manche Nutzer mit aktiviertem Root Store ausgeliefert. Wer das Feature testen will, kann beim Browserstart ein entsprechendes Flag setzen. (ulw@ix.de)

Ethereum-Blockchain arbeitet

jetzt mit Proof of Stake

Markt + Trends | World Wide Web

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Die Ethereum-Blockchain hat den Wechsel zum Proof-of-Stake-Verfahren offiziell vollzogen. Bei dem als Merge bezeichneten Übergang integrierten die Ethereum-Entwickler die Beacon Chain, auf der man das Konsensverfahren seit 2020 erprobte, mit dem Ethereum Mainnet. Der erste Schritt des lange erwarteten Merge war ein Update der Beacon Chain Anfang

September. Nach Erreichen der vorher bestimmten Gesamtschwierigkeit für das Erzeugen neuer Blöcke fand das Mining von Ethereum Mitte September ein Ende.

Statt mit Proof of Work am schnellsten einen mathematischen Beweis auszurechnen, erzeugt nun ein ausgeloster Validierer den neuen Block. Um einen Block zu validieren (zu staken), muss man einen Full Node betreiben und eine Sicherheitssumme in der Kryptowährung von Ethereum hinterlegen. Derzeit beträgt die Sicherheit mindestens 32 Ether, die dem Besitzer im Falle eines Betrugs aberkannt werden. Durch den Wechsel des Konsensverfahrens entfällt das umweltschädliche Mining. Der Energiebedarf der Ethereum-Blockchain soll sich damit um 99,95 Prozent verringern. Im Zuge des Merge fiel der Preis von Ether um mehr als 20 Prozent auf etwa 1330 US-Dollar. (pst@ix.de)

Cloudflare will mit Turnstile reCAPTCHA ablösen

Mit dem neuen Human-Validierungsdienst Turnstile will Cloudflare bisher gängige CAPTCHA-Verfahren ersetzen. Das soll die User Experience verbessern.

Markt + Trends | World Wide Web

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Cloudflares CAPTCHA-Alternative Turnstile soll das Suchen nach Zebrastreifen, Bussen und Ampeln für Nutzer in Zukunft obsolet machen. Turnstile ist in der offenen Beta und soll für Internet-User unsichtbar deren Menschsein bestätigen. Dafür soll Turnstile die Validierung automatisch aus einer Reihe von nicht intrusiven Browseraufgaben vollziehen – basierend auf der Telemetrie und dem Kundenverhalten während einer Sitzung.

Ein weitere Validierungsmöglichkeit bei Turnstile sind Private Access Tokens, die die Gerätehersteller vergeben und mit denen

sich das Gerät als legitim ausweist. Das Token bürgt dabei für die Validität der Nutzer. Das will Cloudflare über Kollaborationen mit Herstellern erreichen, Apple sei bereits an Board. Damit könne man die Datenerhebung für Turnstile minimieren: Statt Geräte selbst auszulesen, erledige das nun der Hersteller.

Bestehende Dienste bei Nutzern unbeliebt

Neben der Konkurrenz zum eigenen Dienst CAPTCHA, bekannt vom Klick auf „Ich bin ein Mensch“, hofft Cloudflare Googles reCAPTCHA ablösen zu können. In der Bekanntmachung der Beta von Turnstile hebt Cloudflare vor allem die schlechte User Experience der bestehenden Validierungsdienste hervor: „Wir hassen es, ihr hasst es, alle hassen es.“

Dabei ist Turnstile nicht der erste Validierungsdienst, der keine Interaktion erfordert. Auch Googles reCAPTCHA existiert bereits in einer Variante, die im Verborgenen basierend auf dem Benutzerverhalten eine Entscheidung trifft. Zum Einsatz kommt diese reCAPTCHA-Version aber selten. Cloudflare hebt ihr gegenüber die komfortablere Bedienung des eigenen Produkts hervor.

Turnstile steht ab sofort allen Webseitenbetreibern kostenlos über eine API zur Verfügung. Cloudflare-Kunde muss man nicht sein. Die Anmeldung erfolgt über eine eigene Website. (jvo@ix.de)