Web Application Firewalls

Marc Nilius

WordPress Online Meetup, 23. Oktober 2019

Über mich

- Diplom-Informatiker, selbständig
- WordPress-Wartung und WordPress-Sicherheit
- @marcnilius oder @wpsicherheit
- https://www.wp-wartung24.de
- Organizer diverser Meetups und WordCamps

Wird meine Website angegriffen?

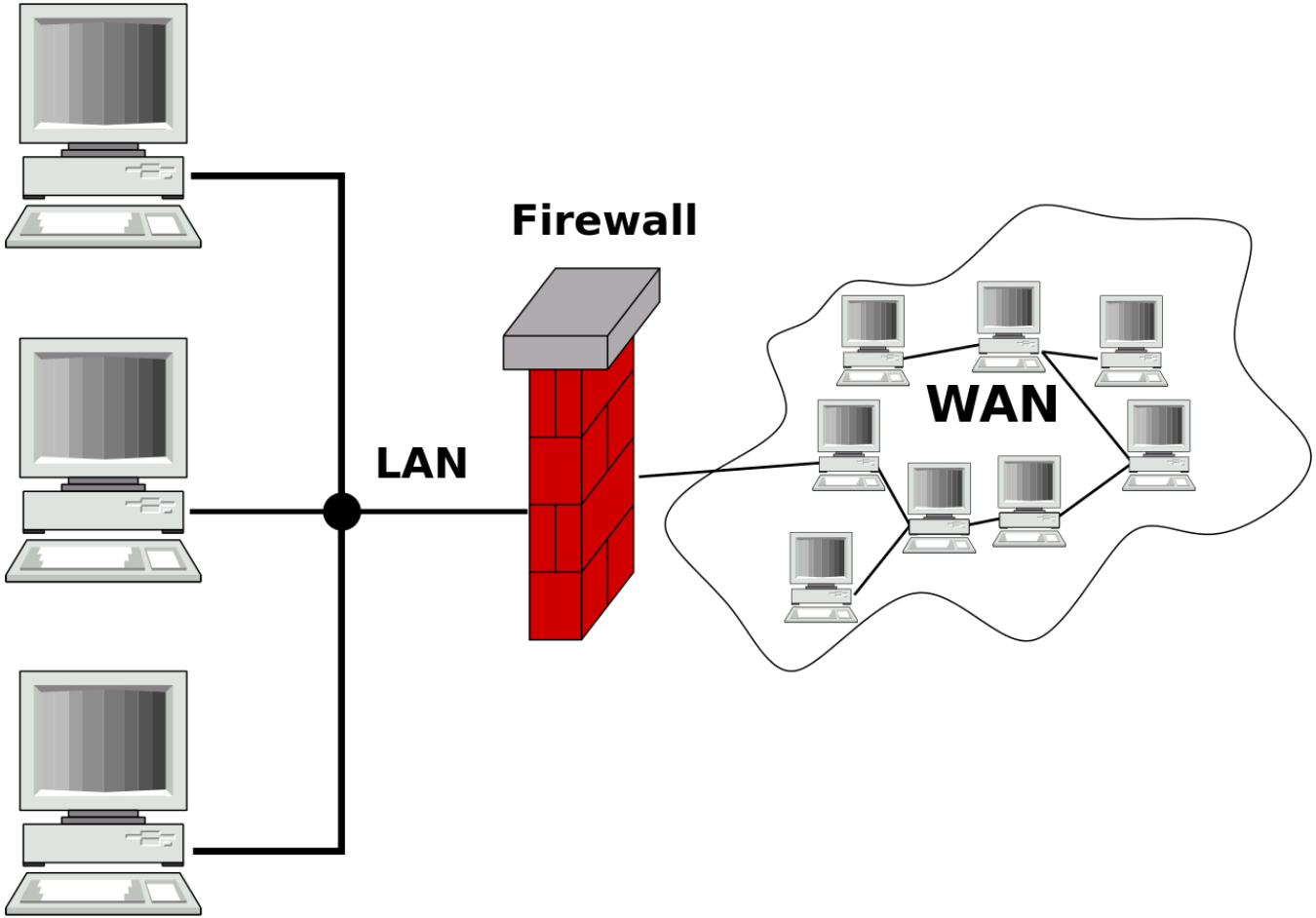
Basics der Website-Sicherheit

Basics der Website-Sicherheit

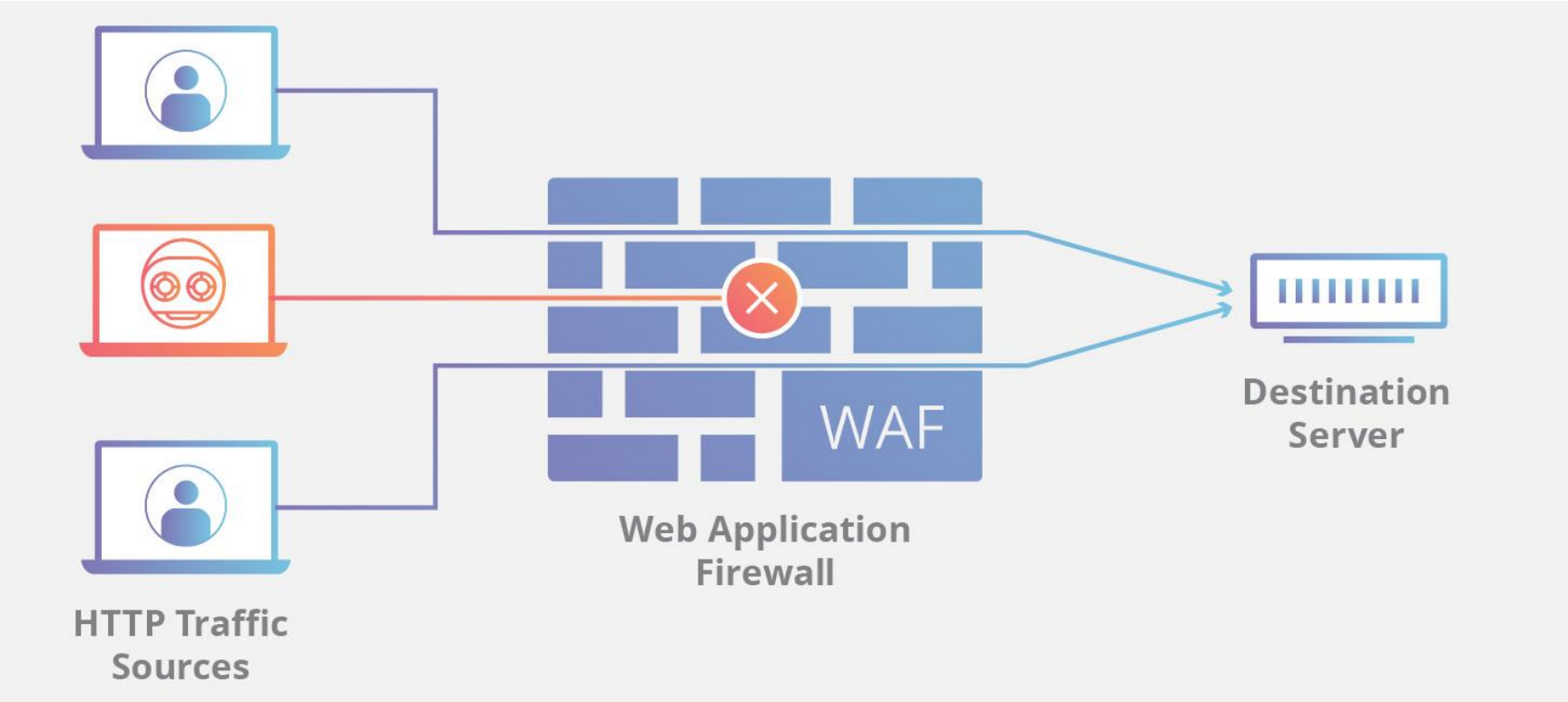
- Regelmäßige Updates
- Regelmäßige Backups auf externe Server
- Sichere Passwörter

- Unnütz: Security by Obscurity / Schlangenöl
  - Login-Sperren
  - WordPress-Verwendung verstecken

Was sind Web Application Firewalls?



Quelle: Wikipedia - Harald Mühlböck – CC BY-SA 3.0



Quelle: cloudflare.com

Web Application Firewalls

- Werden bei jedem Aufruf vorgeschaltet und überprüfen den Aufruf auf Angriffe/Gefahren
- Basierend auf definierten Regeln

- Obwohl eine Sicherheitslücke in der Website ist, kann diese wegen der Firewall nicht ausgenutzt werden
- Aber: obwohl eine Firewall vorhanden ist, kann eine Seite trotzdem gehackt werden, wenn die Firewall für die Art des Angriffs keine Regel hat

Web Application Firewalls

- FW-Regeln erkennen allgemeine Angriffe wie zB
  - Cross-Site Scripting
  - SQL Injections
- Aber auch spezifische Angriffsvektoren zu bekannten Sicherheitslücken in WP oder Plugins
- Somit können sowohl explizit bekannte Sicherheitslücken geblockt werden
- … aber auch allgemeine unspezifische Angriffe

Arten von WAFs

- Netzwerk-WAFs
  - Hardware in großen Infrastrukturen
  - Heute kein Thema für uns
- Cloud-basierte WAFs
- Host-basierte WAFs

Cloud-basierte WAFs

- von einem Dienstleister auf einem anderen Server bereitgestellt
- Daten werden erstmal auf anderen Server umgeleitet, dort überprüft und dann weitergeleitet
- Anbieter kann sehr schnell auf Bedrohungslagen reagieren und Regeln anpassen
- Weitere Zusatzleistungen möglich
  - DDoS-Schutz
  - Bildoptimierung

Cloud-basierte WAFs

- Nachteil:
  Zweiter "Point of Failure" - zwei Server müssen fehlerfrei laufen, damit Website angezeigt werden kann
- Technik: Mittels DNS-Anpassung werden Daten umgeleitet

- Beispielanbieter: Cloudflare, Sucuri

Host-basierte WAFs

- Installation auf eigenem Server, z.B. mithilfe eines WP-Plugins
- Alle Aufrufe werden durch die Firewall geprüft, basierend auf der Serverkonfiguration
- Regeln müssen aktualisiert werden (z.B. WP-Plugin-Update, individuelles Nachladen durch das Plugin)
- Technik: PHP-Konfiguration (auto_prepend_file) auf dem Server selbst
- Beispiele: Wordfence, Ninja Firewall

Eigenheiten, Vor- und Nachteile

- system-unabhängige Überwachung
- funktional autark
- wordpress-seitige Integration nur für Konfiguration
- echter Schutz vor Sicherheitslücken und Angriffsvektoren

Eigenheiten, Vor- und Nachteile

- zumindest theoretisch:
  Verlangsamung durch Server-Umleitung und/oder Programmausführung
- False Positives, also fehlerhafte Blockaden von Requests
- Konfiguration erfordert technische Kenntnisse (DNS- oder PHP-Konfiguration)

Cloud- oder host-basierte Firewall?

Beispiel: Ninja Firewall

- Fallback-Modus „WordPress-WAF“ mit eingeschränkter Funktion und Sicherheit
- Art der Konfiguration Hoster-abhängig

NinjaFirewall (WP Edition)

Dashboard | Statistics | About...

Firewall Dashboard

Firewall	Enabled
Mode	NinjaFirewall is running in WordPress WAF mode. For better protection, click here to enable its Full WAF mode.
Edition	WP Edition ~ Need more security? Get Premium!
Version	4.0.4 ~ Security rules: 2019-06-10.1
PHP SAPI	FPM-FCGI ~ 7.2.23
Admin user	`WP-Wartung24` : You are whitelisted by the firewall.
Help & configuration	Securing WordPress with NinjaFirewall (WP Edition)

Upgrade to Full WAF mode

In **Full WAF** mode, all scripts located inside the blog installation directories and sub-directories are protected by NinjaFirewall, including those that aren't part of the WordPress package. It gives you the highest possible level of protection: security without compromise. It works on most websites right out of the box, or may require some very little tweaks. But in a few cases, mostly because of some shared hosting plans restrictions, it may simply not work at all. If this happened to you, don't worry: you could still run it in **WordPress WAF** mode. Despite being less powerful than the **Full WAF** mode, it offers a level of protection and performance much higher than other security plugins.

Select your HTTP server and your PHP server API (`SAPI`)

Apache + CGI/FastCGI or PHP-FPM (recommended)

- Apache + PHP7 module
- Apache + CGI/FastCGI or PHP-FPM (recommended)
- Apache + suPHP
- Nginx + CGI/FastCGI or PHP-FPM
- Litespeed
- Openlitespeed
- Other webserver + CGI/FastCGI or PHP-FPM

Select the PHP initialization file supported by your server

- (•) Let NinjaFirewall make the necessary changes (recommended).
- ( ) I want to make the changes myself.

Ensure that you have FTP access to your website so that, if there were a problem during the installation of the firewall, you could easily undo the changes.

Finish »

Hoster-Unterschiede

Select the PHP initialization file supported by your server

- (•) `.user.ini` (recommended)
- ( ) `php.ini`

- .user.ini-Dateien werden nicht von allen Hostern interpretiert
- php.ini sind bei den meisten Hostern nicht möglich

- Hetzner: Einstellung kompliziert über htaccess
- Hosting.de: manuelle Eingabe im Hoster-Backend

WordPress-WAF-Modus

- Nur eingeschränkt empfehlenswert, da für die Überprüfung der Aufrufe WordPress bereits bereits aktiv sein muss
  => nicht alle Angriffe können blockiert werden
- Als Notmaßnahme
  (bei Hostern ohne Konfigurationsmöglichkeit)
  oder
  als Modus vor der endgültigen Einrichtung

Ergänzungen zur WAF

- Hilfreich z.B. der NinjaScanner zur Suche nach Malware

- Andere Sicherheitsplugins sind in Kombination mit einer WAF selten sinnvoll
  - Überschneidungen
  - Unnötige Einstellungen, die das System stören oder langsamer machen

Web Application Firewall – Wat willste mehr? ;-)

Vielen Dank!

Zeit für Fragen und Diskussion!

Vortragsfolien auch unter
https://www.marcnilius.de

Marc Nilius
@marcnilius / @wpsicherheit
https://www.wp-wartung24.de