

Updates in WordPress - Wie? Wo? Was? Warum?

Marc Nilius

WordCamp Frankfurt, 4. September 2016



Über mich

- Diplom-Informatiker
- Selbständiger Web-Entwickler
- Spezialgebiet
WordPress-Wartung und
WordPress-Sicherheit
- @marcnilius oder
@wpsicherheit
- <https://www.wp-wartung24.de>



Updates in WordPress? Grundlagen



Welche Updates gibt es?

- Updates von WordPress selbst (Core)
 - Major Release (4.3, 4.4, 4.5, 4.6, ...)
 - Alle 4-5 Monate
 - Neue Features und Funktionen
 - Minor Release: Maintenance / Security Release (4.5.1, 4.5.2, ...)
 - Security Releases auch noch für ältere Release-Äste (4.4.x, 4.3.x, ...)
- Updates von Plugins
- Updates von Themes
- Updates der Übersetzungen



Updates sind mir egal!



Warum und wann sollte ich updaten?

- Updates so schnell wie möglich
 - aber nicht überstürzt!
 - Updates liefern mehr Sicherheit!
 - Updates liefern Kompatibilität
 - Updates bringen Fehlerbehebung
- Vor dem Update Backup anlegen
- Bei großen Systemen: Updates auf Test-/ Staging-System testen



Warum und wann sollte ich updaten?

- Für Test-Systeme: WP Rollback



<https://de.wordpress.org/plugins/wp-rollback/>



Woher weiß WP, dass es Updates gibt?

- Jede WordPress-Installation fragt alle 12 Stunden bei den WordPress-Servern nach (api.wordpress.org)
- System basiert auf wp-cron.php
 - Funktioniert nur, wenn jemand die Website auch aufruft!
- Anfrage liefert Infos über neue WP-Updates, Plugin- und Theme-Versionen (sofern im WP-Repository)
- Plugins / Themes aus anderen Quellen sind außen vor
 - Außer, die jeweiligen Autoren bilden den Abfrage-Mechanismus nach (per Hook möglich)



Welche Daten werden gesendet?



Website



api.wordpress.org

- Aktuelle WP-Version
- PHP-Version
- Locales (Sprachen)
- MySQL-Version
- Local Package: lokalisiertes WP-Paket
- Anzahl Websites (relevant bei Multisites)
- Anzahl Benutzer
- Multisite?
- Initiale DB-Version (erste installierte WP-Version)
- Installierte Plugins
(Name, Title, Description, Author, Author URI, Version, Textdomain, DomainPath, nur netzwerk-weit aktivierbar, aktiv)
- Installierte Themes
(Name, Title, Version, Author, Author URI, Template, Stylesheet)
- Installierte Übersetzungen für Plugins und Themes



Welche Daten werden gesendet?

- Angabe "Aktive Installationen" im Plugin-Verzeichnis
- Informationen über die genutzte PHP-Versionen bei WordPress (PHP 5.2 immer noch bei ca. 7%)
- Mehr Statistiken?
<https://wordpress.org/about/stats/>

Requires: 4.1 or higher

Compatible up to: 4.5.3

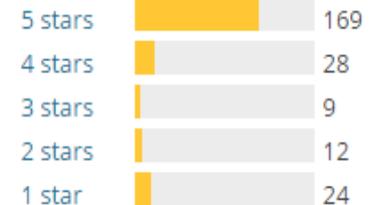
Last Updated: 7 days ago

Active Installs: 200,000+

Ratings



4.3 out of 5 stars



Auto-Updates



Was sind Auto-Updates?

- Security- und Maintenance-Releases können automatisch installiert werden
 - Installation, sobald verfügbar
 - Nur Bugfixes und Sicherheitslücken
 - Keine Kompatibilitätsprobleme (normalerweise)
- Seit WordPress 3.7 ist die automatische Installation von Minor Releases der Standard
- Major Releases (4.5, 4.6) werden niemals (per default) automatisch installiert



Auto-Updates für den Core

- Auto-Updates können abgeschaltet werden (in wp-config.php):

```
define( 'WP_AUTO_UPDATE_CORE', false );
```

- `true` = Auto-Updates für Major und Minor Releases
`false` = Keine Auto-Updates
`'minor'` = Auto-Updates nur für Minor-Releases
- Oder per Filter



Auto-Updates für Übersetzungen

- Standardmäßig eingeschaltet
- Für WordPress selbst
- Für Plugins und Themes (soweit angeboten)
- Abschalten nur via Filter:

```
add_filter( 'auto_update_translation', '__return_false' );
```



Auto-Updates für Plugins und Themes

- Generell sind Auto-Updates für Plugins und Themes deaktiviert
- Aus berechtigten Gründen kann ein Auto-Update angestoßen werden (z.B. Sicherheitslücken)
 - Nur individuell auslösbar, kein Mechanismus
 - Von WordPress.org nach Rücksprache mit dem Plugin-Autor



Auto-Updates für Plugins und Themes

- Auto-Updates anschalten (per Filter):

```
add_filter( 'auto_update_plugin', '__return_true' );  
add_filter( 'auto_update_theme', '__return_true' );
```

- Auch Zwangs-Updates verhindern (nicht empfohlen):

```
add_filter( 'auto_update_plugin', '__return_false' );  
add_filter( 'auto_update_theme', '__return_false' );
```



Updates aus anderen Quellen



Updates aus anderen Quellen

- Kein einheitliches Update-System
- Plugins / Themes können das WP-Update-System imitieren
 - Per Hook an den Update-Check hängen
- Viele Kauf-Plugins und -Themes haben keine eigene Update-Technik
 - Manuelles Update (per FTP) notwendig
 - Abschreckend für technisch Unerfahrene
 - Aufwendiges Verfahren verhindert regelmäßige Updates



Updates aus anderen Quellen

- Hilfs-Plugin für Plugins und Themes von Envato
 - ThemeForest
 - CodeCanyon
- Plugin "Envato Market"
<https://github.com/envato/wp-envato-market>
 - Nach Angabe eines Envato API-Keys werden alle möglichen Updates angezeigt
 - Plugins von Themeforest
 - Themes von CodeCanyon

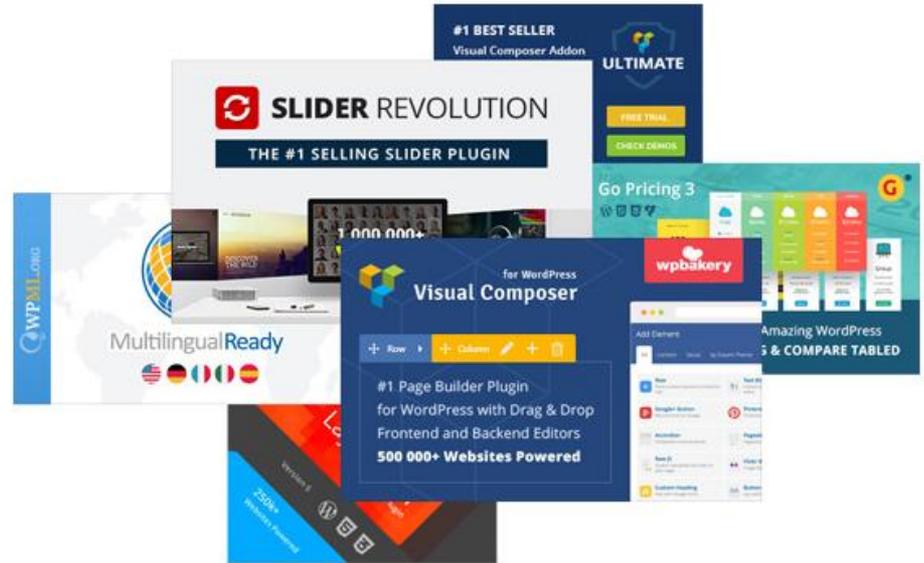


Updates aus anderen Quellen

- Themes mit Bundle-Plugins
- Benutzer abhängig vom Theme-Update, um Plugins aktualisieren zu können
- Eventuell ist der Kauf einer eigenständigen Plugin-Lizenz sinnvoll
- Generell rate ich von Themes mit Bundle-Plugins ab

Expand & Optimize

Best in class plugins compatibility. \$99 value premium plugins included.
Translation and multilingual ready.



Child-Theme-Problematik

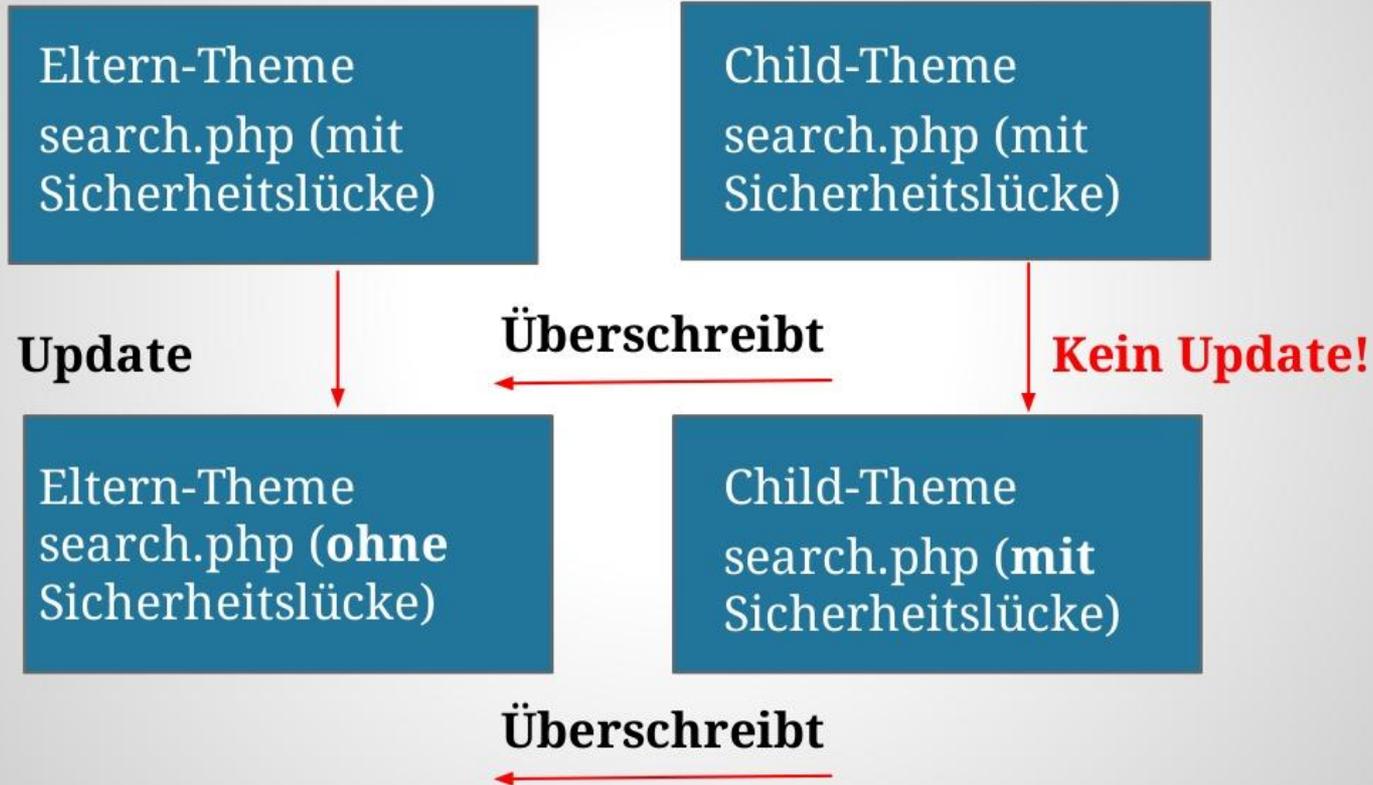


Child-Theme-Problematik

- Update eines Themes lässt Child-Theme unangetastet
- Änderungen in kopierten Dateien werden nicht übernommen
 - Bugs und Sicherheitslücken bleiben bestehen
- Child-Theme muss manuell geprüft und aktualisiert werden
- Zwischenzeitlich ggf. Inkompatibilität zwischen Parent und Child Theme



Sicherheitsprobleme



Thorsten Landsiedel, WordCamp Köln 2015



Child-Theme-Problematik

- Torsten Landsiedel auf dem WordCamp Köln 2015
<http://de.slideshare.net/zodiac1978/child-themedilemma>
- Child-Theme Check
 - Prüft Templates von Child-Themes auf Aktualität
 - Voraussetzung: Parent-Theme muss Versionsnummer im Template angeben
- <https://github.com/Zodiac1978/tl-template-checker>



Tipps & Tricks



Maintenance Mode

- Während eines Updates versetzt sich WP in einen Wartungsmodus:

Wegen geplanter Wartungsarbeiten kurzzeitig nicht verfügbar. Schau gleich noch einmal vorbei.

- WordPress legt eine Datei `.maintenance` ins Hauptverzeichnis
 - Beinhaltet eine Variablendefinition `$upgrading = "Zeit d. Starts"`
 - WordPress zeigt obige Meldung an, solange die Datei existiert und die Startzeit weniger als 10 Minuten her ist
- Bei Problemen nach dem Update: einfach `.maintenance` löschen



Maintenance Mode

- Die angezeigte Seite kann umgestaltet werden
- Datei `maintenance.php` in `wp-content` anlegen
- Theme- und Plugin-unabhängig
- Wird bei Updates nicht überschrieben



Was machen, wenn das Update schief geht?

- Per FTP
 - Verzeichnis des Plugins oder Themes umbenennen
 - "pluginname" -> "_pluginname"
 - Damit wird das Plugin nicht mehr ausgeführt
 - Testen, ob Seite wieder funktioniert
 - Plugin neu installieren
 - Verzeichnis "_pluginname" löschen



Nochmal: Auto-Update

- Update-Check ist nicht einfach per Filter abschaltbar

Nur per Workaround

```
add_filter( 'pre_http_request', array($this, 'block_request'), 10, 3 );
function block_request($pre, $args, $url) {
    $url_data = parse_url( $url );

    /* block request */
    if(
        false !== stripos( $host, 'api.wordpress.org' ) &&
        (
            false !== stripos( $url_data['path'], 'update-check' )
            || false !== stripos( $url_data['path'], 'browse-happy' )
        )
    ) {
        return true;
    }

    return $pre;
}
```



Nochmal: Auto-Update

- Per Plugin



<https://wordpress.org/plugins/disable-wordpress-updates/>



Nochmal: Auto-Update

- E-Mail bei verfügbaren Updates
 - WP Updates Notifier
 - <https://wordpress.org/plugins/wp-updates-notifier/>



- Mail on Update
- <https://de.wordpress.org/plugins/mail-on-update/>



Ausblick: Management-Lösungen

- InfiniteWP
- ManageWP
- MainWP
- Jetpack
- iThemes Sync
- WPRemote
- ...

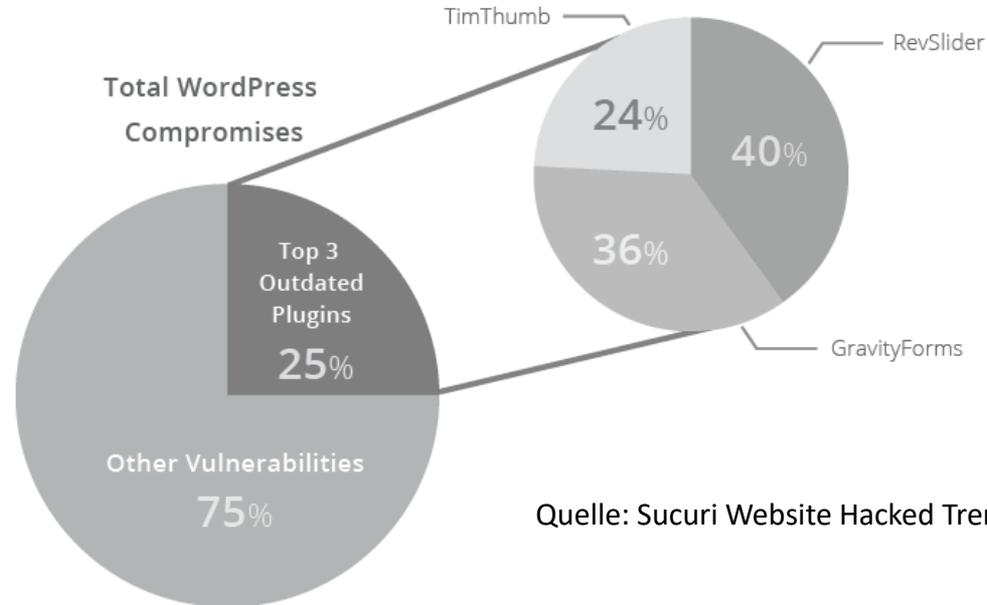


Ein Wort zur Sicherheit



Ein Wort zur Sicherheit

Top 3 Out of Date WordPress Plugins Contributing to Site Hacks Q1 - 2016



Quelle: Sucuri Website Hacked Trend Report 2016 - Q1

- Laut einer Studie sind hauptsächlich nicht aktualisierte Plugins an gehackten Websites schuld
 - Häufig im Bundle mit einem Theme
 - An 25% aller Hacks sind 3 Plugins Schuld



Ein Wort zur Sicherheit

- Der Hauptgrund für gehackte Websites sind Plugins mit Sicherheitslücken
 - Regelmäßige und zeitnahe Updates sind der beste Schutz

Für die Sicherheit der eigenen Website ist jeder WordPress-Admin selbst verantwortlich



Vielen Dank!

(Hoffentlich) Zeit für Fragen und Diskussion!

Folien gibt's unter
<https://www.wp-wartung24.de/wcfra2016>

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

