WP Sicher betreiben

Grundlagen

WP Meetup München – 23.10.2018

Speaker – Dietmar Leher

- Xing: http://www.xing.com/profile/Dietmar_Leher
- LinkedIN: https://www.linkedin.com/in/dietmarleher/
- Facebook: https://www.facebook.com/dietmarleher

- Twitter: https://twitter.com/spacehostDE
- Webseite: https://spacehost.de
- Blog: https://spacehost.de/blog

Inhalt

- Sicherheitslücken / Angriffe /Hacks
  - Warum wird man angegriffen?
  - WordPress ist nicht (un-)sicherer als andere CMS
- Hauptangriffe auf WordPress
- Informationen über unsichere Plugins und Themes finden
- WordPress absichern – Wie?
  - WordPress sicher aufsetzen und betreiben
  - Regelmäßige Aktionen
  - Welche Plugins helfen können
- Was soll ich tun, wenn die Seite gehackt wurde?
- Beyond WordPress - Absicherung außerhalb von WP

Sicherheitslücken / Angriffe / Hacks

Sicherheitslücke:

Eine Schwachstelle von IT-Komponenten oder IT-Endgeräten. Sie wird durch Fehler in der Programmierung oder Codierung verursacht und lässt sich ausnutzen, um beispielsweise Schadcode auf Rechnersystemen einzuschleusen.

*Quelle:
https://www.security-insider.de/was-ist-eine-sicherheitsluecke-a-648842/

Verizon 2018 Data Breach Investigation Report

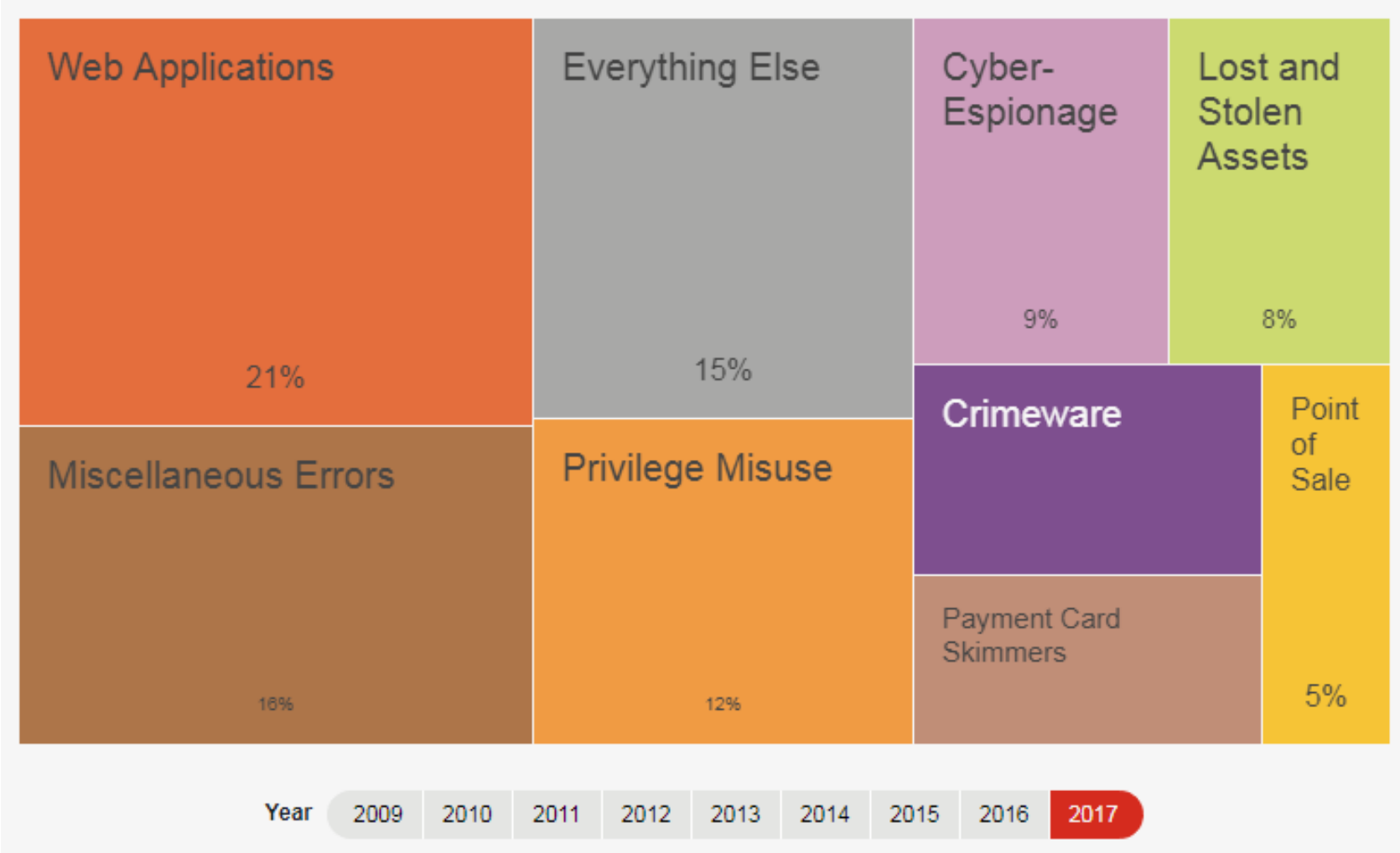
- 81 Prozent der Hacking-bedingten Verstöße nutzen gestohlene und/oder schwache Passwörter.
- 73 Prozent der Datenverstöße wurden von Außenstehenden begangen.
- Etwa 20% der "Eintrittsstellen" waren Web-Applications

*Quelle:
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Google blacklisted etwa 20.000 Webseiten mit Malware and etwa 50.000 aufgrund von Phishing jede Woche. (*Google Angabe)

Laut Sitelock werden aber nur 19 Prozent der infizierten Webseiten überhaupt von Suchmaschinen gekennzeichnet.

Verizon 2017 DBIR



*Quelle: http://www.verizonenterprise.com/verizon-insights-lab/dbir/tool/

SIWECOS Report Sept.2019

SIWECOS untersuchte 1.142 Webseiten kleiner und mittelständischer Unternehmen hinsichtlich Sicherheitslücken

Rund jede zehnte Webseite hat eklatante Sicherheitsmängel

* Quelle: Sichere Webseiten und Content Management Systeme ist ein Projekt des Verbandes der Internetwirtschaft eco e.V. in Kooperation mit der Ruhr-Universität Bochum und den Partner CMS Garden e.V. und der Hackmanit GmbH.

https://siwecos.de/news/64-siwecos-weist-sicherheitsluecken-auf-webseiten-im-mittelstand-nach

How WordPress websites get hacked

- 29% vulnerable themes
- 22% vulnerable plugins
- 8% weak passwords
- 41% hosting vulnerabilities

*Quelle: The Hacker News, March 2014
http://thehackernews.com/2014/03/162000-vulnerable-wordpress-websites.html

Sucuri 2017 Hacked Website Report

"WordPress infections rose from 74% in 2016 Q3 to 83% in 2017."

"At the end of Q3 2016, 61% of hacked WordPress sites recorded outdated installations, however, this has since decreased. In 2017, only 39.3% of clean up requests for WordPress had an outdated version."

TOP 3 - modified files:

- 28% index.php
- 10% .htaccess
- 8% functions.php

*Quelle: https://sucuri.net/reports/2017-hacked-website-report

Warum wird man angegriffen?

Gründe für einen Angriff

- Um persönliche Informationen von Benutzern zu stehlen (z.B. Erstellung von Profile, zum Identitätsdiebstahl, gezielte Phishing-Attacken)
- Maskieren von bösartigen Links auf der Seite oder in Kommentaren (z.B. Phishing, Malware-Download)
- Zur Speicherung und Verteilung von Malware
- Traffic-Klau
  (Umleitung des Traffics auf andere Webseiten, z.B. "BabaYaga" 06/2018)

Gründe für einen Angriff

- Pornografische Inhalte verstecken (nicht verlinkte/verwaiste Seiten die nur per Direktlink erreichbar sind)
- Hacktivismus, meist politisch (z.B. Ersetzung der Seite durch "Hacked by " Information)
- DDoS Account, dient als Angriffsserver für eine DDoS-Attacke auf Dritt-Seite

Info:
Malware-Links und Seiten werden von Google hart bestraft
=> erhebliche Rückstufung bei SEO und Domain-Reputation

WordPress ist nicht (un-)sicherer als andere CMS

Andere CMS sind auch gefährdet

Auswahl von Artikeln, ohne Wertung:

- Drupalgeddon 2: Angreifer attackieren ungepatchte Drupal-Webseiten (16.04.2018)
  https://www.heise.de/security/meldung/Drupalgeddon-2-Angreifer-attackieren-ungepatchte-Drupal-Webseiten-4024700.html

- Sicherheitsupdates: Angreifer könnte Passwörter in Typo3 überschreiben (17.07.2018)
  https://www.heise.de/security/meldung/Sicherheitsupdates-Angreifer-koennte-Passwoerter-in-Typo3-ueberschreiben-4111640.html

- Jetzt patchen: Gefährliche Sicherheitslücke in Joomla (17.05.2017)
  https://www.heise.de/security/meldung/Jetzt-patchen-Gefaehrliche-Sicherheitsluecke-in-Joomla-3716175.html

WordPress ist weit verbreitet

- Unter den 10 Millionen meistbesuchten Webseiten werden 30 Prozent mit WordPress betrieben.

*Quelle:
https://www.heise.de/newsticker/meldung/WordPress-dominiert-die-Content-Management-Systeme-3986486.html

Die weite Verbreitung ist der Hauptgrund, warum automatisierte Angriffe über Skripte existieren.
Unabhängig davon, ob die Ziel-Webseite wirklich relevante Informationen bereitstellt, ist sie grundsätzlich gefährdet.

Hauptangriffe auf WordPress

Hauptangriffe auf WordPress

- Brute force Passwort-Attacken
- Sicherheitslücken in Plugins (auch nicht mehr weiterentwickelte Plugins)
- Kürzlich bekannt gewordene Schwachstellen

Was ist somit besonders gefährdet?

- Login
- Plugins
- Themes
- Drittsoftware

Informationen über unsichere Plugins + Themes finden

Informationsquellen Lücken

- Offensive Security's Exploit Database Archive: https://www.exploit-db.com/
  - https://www.exploit-db.com/search/
  - https://www.exploit-db.com/webapps/
- WPScan Vulnerability Database: https://wpvulndb.com/
- Veröffentlichte Lücken: https://www.cvedetails.com/product-search.php

Welche Version und welches Plugin wird angegriffen?

z.B. https://hackertarget.com/100k-top-wordpress-powered-sites/

WordPress absichern – Wie?

WordPress absichern - Einstieg

Offizielle Hinweise auf wordpress.org

https://codex.wordpress.org/de:Hardening_WordPress

- Sichere Passwörter
- Rechte-/Benutzermanagement
- Verschlüsselung
- FTP-Zugang
- Computer: Browser aktuell halten
- ...

WordPress Security

WordPress sicher aufsetzen und betreiben

WordPress Security – 20 Punkte

1) Backup erstellen, regelmäßig

2) Als Datenbankpräfix nicht 'wp_' verwenden
3) Den Admin-Benutzer nicht "admin" nennen
4) Komplexe Passwörter verwenden, 2FA (Zwei-Stufen-Authentifizierung)
5) Die aktuelle Version von WordPress betreiben
6) Themes und Plugins in der aktuellen Version betreiben
7) Bei der Wahl von Plugins und Themes: Weniger ist mehr
8) Rechte-/Benutzermanagement: Benutzer nur mit benötigten Rechten ausstatten

WordPress Security – 20 Punkte

8) Security Keys von WordPress nutzen (wp-config.php)
9) Dateiberechtigungen prüfen (max. Verzeichnisse 755, Dateien 644, wp-config auf 600)
10) .htaccess - Directory Listing ausschalten

```
Options -Indexes
```

11) HTTPS für alle Logins und wp-admin forcieren, benötigt SSL-Zertifikat / wp-config.php

```
define('FORCE_SSL_LOGIN', true);
define('FORCE_SSL_ADMIN', true);
```

WordPress Security – 20 Punkte

12) Debug-Modus deaktivieren (falls aktiv) / wp-config.php

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

13) wp-admin und wp-config.php schützen (.htaccess)

```
<files wp-config.php>
  Order allow,deny
  Deny from all
</files>
```

Evtl. (abhängig von Theme und Plugins) aber erlauben:

```
<Files wp-admin/admin-ajax.php>
  Order allow,deny
  Allow from all
</Files>
```

WordPress Security – 20 Punkte

14) PHP Ausführung in wp-includes und wp-content/uploads verhindern / .htaccess

```
<Files *.php>
  Deny from all
</Files>
```

15) Bearbeitung von Theme-Files über das Admin-Panel verbieten

    Hat ein Hacker sich Zugang zum Admin-Panel verschafft, kann er über den Design- und Plugin-Editor Änderungen vornehmen und Malware installieren. Dann funktionieren allerdings auch Plugins wie der Theme Editor, WP-Editor u.a. nicht mehr / wp-config.php

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

WordPress Security – 20 Punkte

16) Auflistung/Ausgabe der WordPress Usernamen unterbinden / .htaccess

```
RewriteCond %{QUERY_STRING} author=d
RewriteRule ^ /? [L,R=301]
```

17) XML-RPC-Pingbacks deaktivieren / .htaccess

```
<Files xmlrpc.php>
  Order deny,allow
  Deny from all
</Files>
```

WordPress Security – 20 Punkte

18) Skriptverkettung für WordPress-Administrator-Panel deaktivieren / wp-config.php

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

19) Zugriff verweigern auf .htaccess und .htpasswd verweigern / .htaccess

```
<FilesMatch "(\.htaccess|\.htpasswd)">
    Order deny,allow
    Deny from all
</FilesMatch>
```

WordPress Security – 20 Punkte

20) Weitere Punkte ?

Z.B. vorsorglich einen "Notfallplan" erstellen:

- Backup-Strategie (z.B. Full / Inkrementell, Backups an verschiedenen Orten, verschlüsselt, Backup schnell zugreifbar/wiederherstellbar
- Eskalationsweg, wer wird wann informiert
- Veröffentlichungen (BSI-Meldung, Newsletter an Kunden, Pressemeldung)
- ...

Regelmäßige Aktionen

- Plugins aktualisieren
- Alte / nicht benötigte Plugins + Themes löschen
- Webspace ausmisten, z.B. Testinstallation, Tools
- Passwörter/Tokens zu Drittsoftware erneuern (API-Keys)
- Inaktive Benutzer löschen
- ergänzende Scans
- Backup erstellen

Welche Plugins bei der Absicherung helfen können

Sicherheits-Plugins

- Gegen Kommentar-Spam, Links und Schadcode darin

  Antispam Bee

  https://de.wordpress.org/plugins/antispam-bee/

- Login absichern, Fehlversuche begrenzen

  Login LockDown

  https://wordpress.org/plugins/login-lockdown/

- Limit Login Attempts Reloaded

  https://de.wordpress.org/plugins/limit-login-attempts-reloaded/

Sicherheits-Plugins

- All In One WP Security & Firewall
  https://de.wordpress.org/plugins/all-in-one-wp-security-and-firewall/

- Security Ninja – WordPress Security Plugin
  https://de.wordpress.org/plugins/security-ninja/
  - Umfangreiche Scan-Funktion, Pro-Version für Einstellungen

- NinjaFirewall (WP Edition) / NinjaFirewall (WP+ Edition) Kostenpflichtig
  https://de.wordpress.org/plugins/ninjafirewall/
  https://nintechnet.com/ninjafirewall/wp-edition/?comparison

Sicherheits-Plugins

- iThemes Security (formerly Better WP Security)

  https://wordpress.org/plugins/better-wp-security/

- Sucuri Security

  https://de.wordpress.org/plugins/sucuri-scanner/

  - Viele Features kostenlos, nach Anmeldung auch API-Key und in Verbindung mit einem Sucuri-Tarif nutzbar

- SiteLock Security - Dashboard Connection

  https://de.wordpress.org/plugins/sitelock/

  - benötigt SiteLock-Account

Sicherheits-Plugins

- Wordfence - https://wordpress.org/plugins/wordfence/

  - DSGVO-Konformität stark zweifelhaft
  (speichert IP-Adressen und sendet diese an Wordfence-Server)

- Jetpack - https://jetpack.com/pricing/

  - derzeit **nicht** DSGVO-Konform

Für alle aufgeführten Plugins gilt:

Gemäß DSGVO sind IP-Adressen schützenswert. Daher ist die Speicherung und Übertragung von IP-Adressen nicht problemlos möglich und einige Plugins benötigen separate Einstellungen zur Deaktivierung!

Einschätzung zahlreicher Plugins auf DSGVO-Konformität unter:
https://www.blogmojo.de/wordpress-plugins-dsgvo/

Was soll ich tun, wenn die Webseite gehackt wurde?

Webseite gehackt?

Mögliche Schritte, weniger/mehr können individuell erforderlich sein.

- Ruhe bewahren
- Dokumentieren
  - -- Aktuellen Stand der Daten sichern
  - -- Wann habe ich den Hack bemerkt? Datum+Uhrzeit
- Überlegen und identifizieren
  - -- Was wurde zuletzt auf der Seite gemacht, ein neues Plugin installiert, Theme geändert, Widget modifiziert, ... ?
  - -- Gab es neue User oder geänderte Berechtigungen an den Bestehenden?
  - -- Funktioniert der Login ins WordPress-Backend?
  - -- Leitet die Webseite zu einer anderen um?

Webseite gehackt?

- Webseite prüfen und Details identifizieren
  - -- z.B. https://www.virustotal.com/#/home/url
  - -- z.B. https://sitecheck.sucuri.net/
  - -- z.B. https://quttera.com/#online%20url%20malware%20scanner
  - -- Kürzlich geänderte Dateien überprüfen
- Webseite offline nehmen
- Entwicklungsumgebung prüfen
  - -- Ist diese ebenfalls betroffen?
  - -- Falls ja: Computer prüfen, ob dort evtl. Trojaner oder Malware die Seite infiziert hat

Webseite gehackt?

- Alle Zugriffe zurücksetzen
  - -- WordPress Security Tokens
  - -- Verbindungen zu anderen Diensten über API-Tokens o.ä.
  - -- Zugangsdaten Administrator und andere User
  - -- FTP/SSH + MySQL-Passwörter
- Den Webhoster kontaktieren
  - > Evtl. Zugriff auf weitere Logfiles, z.B. FTP-Logins
  - > Evtl. Hilfe bei der Ursachenfindung und/oder Beseitigung
  - > Unwahrscheinlich, aber evtl. gibt es eine ganz neue Sicherheitslücke und bei euch war es das Erste/frühe auftreten = Vorwarnung für den Hoster und andere Kunden
  - > Sollte auf der Seite schon eine Phishing-Seite o.ä. installiert worden sein, werden sog. Abuse-Meldungen bei ihm eintreffen

Webseite gehackt?

- A) Variante: Bereinigen

  -- Integrität der WordPress Core Files prüfen

  -- Veränderte/Befallene Einzeldateien können mit einer sauberen Version ersetzt werden

  -- Tipps des Google-Safe-Browsing umsetzen
  https://transparencyreport.google.com/safe-browsing/search

  -- Auch in der Datenbank aufräumen, verdächtige Links etc. entfernen. Hier helfen die Ergebnisse der Malware-Scanner

- Updaten (WP, Plugins, Themes)

- Manuell ein neues Backup erstellen

- Zusätzliche, noch fehlende Schutzmaßnahmen vornehmen

- Sofern die Website in Blacklists ist, die Austragung beantragen

Webseite gehackt?

- B) Variante: Ersetzen
  - Sauberes Backup einspielen
  - Updaten
  - Zusätzliche, noch fehlende Schutzmaßnahmen vornehmen
  - Manuell ein neues Backup erstellen
  - Sofern die Website in Blacklists ist, die Austragung beantragen

Beyond WordPress

Absicherung außerhalb des WordPress-Systems

Webhosting und Serverumgebung

- Die jeweils aktuellen angebotenen Versionen von PHP und MySQL/MariaDB verwenden. Bei vielen Webhostern mehrere Versionen auswählbar.

- WordPress empfiehlt mittlerweile:

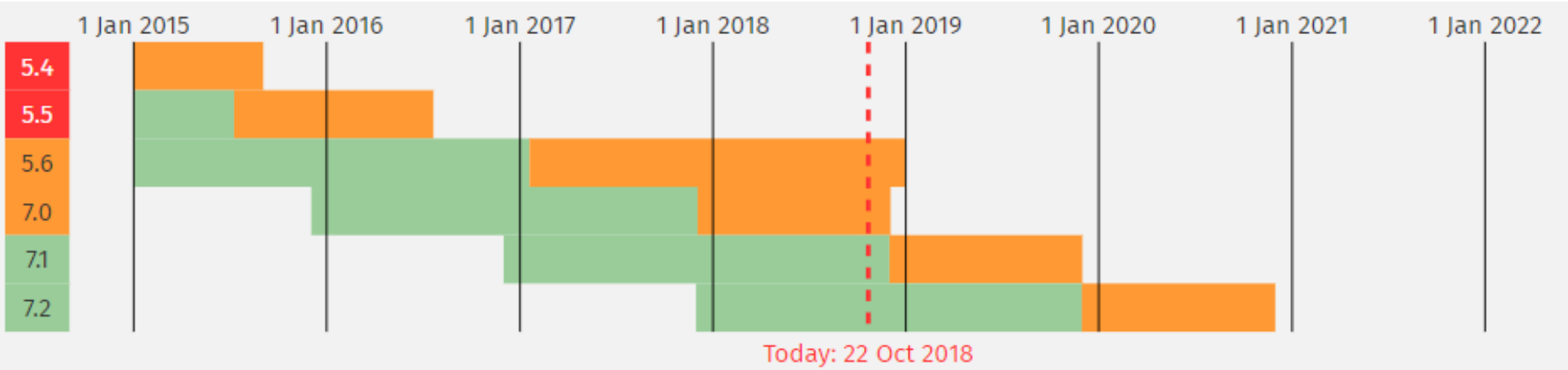
  - PHP-Version 7.2+

  - MySQL-Version 5.6+ oder MariaDB-Version 10.0+

  *Quelle: https://de.wordpress.org/about/requirements/

- Aktueller Webserver (Apache, NGINX etc.)

Unterstützte PHP-Versionen



Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

*Quelle: http://php.net/supported-versions.php

Webhosting und Serverumgebung

- Eine Web Application Firewall (WAF) verwenden

  - ".htaccess Firewall"

  - Firewall auf dem selben Server

  - Firewall bei einem externen Anbieter (meist mit zusätzl. Services wie CDN)

  Zahlreiche Unterschiede in Details+Preis: z.B. nur OWASP TOP10 Schutz, Schutz vor bekannten Lücken, spezialisiert auf CMS, vordefinierte Regeln und/oder auch Eigene, Aktualisierungsrate etc.

- DoS/DDoS - Schutz

  Anbieter-Test des BSI aus 2018:
https://www.heise.de/security/meldung/BSI-gibt-Empfehlungen-zum-Schutz-vor-DDoS-Angriffen-4168894.html

TLS/SSL und HTTP-Header

- TLS/SSL - SSL ist nicht gleich SSL
  - unterschiedliche TLS Standards
  - Ciphern
  - Weitere Konfigurationen

- SecurityHeaders

  https://securityheaders.com/

TLS/SSL und HTTP-Header

Empfehlenswerte Online-Scanner in Bezug auf SSL und weitere Punkte:

- Qualys, SSL Labs - https://www.ssllabs.com/ssltest
- Mozilla, Observatory - https://observatory.mozilla.org
- High-Tech Bridge - https://www.htbridge.com/ssl
  - SSL Certificate Analysis
  - Test for Compliance with PCI-DSS Requirements (PCI DSS 3.2.1 / Mai 2018)
  - Test for Compliance with HIPAA (HIPAA of 1996)
  - Test for Compliance with NIST (Publication 800-52 Revision 1 / April 2014)
  - Test for Industrie Best Practise (z.B. DNS-CAA, server cipher suites preference, PFS, http > https redirect)
  - Third-Party Content analysis (SSL-Test eingebundener Ressourcen wie z.B. Googlefonts)

Vielen Dank

Fragen?