WordPress-Sicherheit: Grundlagen, Hosting, "Ask me anything"

Marc Nilius

WordCamp Köln, 29. Oktober 2016

Über mich

- Selbständig, Diplom-Informatiker
- Spezialgebiet WordPress-Wartung und WordPress-Sicherheit
- Newsletter "WordPress Sicherheit"
- @marcnilius oder @wpsicherheit
- https://www.wp-wartung24.de
- Co-Organizer WordCamp Köln, Co-Organizer WordPress-Meetup Köln

Warum wird meine Seite gehackt?

Arten von Angriffen

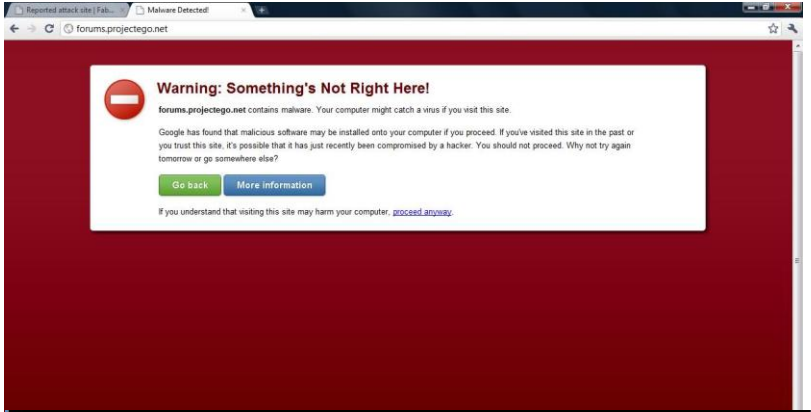
- Die meisten Angriffe geschehen automatisch und nicht zielgerichtet
- Bewusste Angriffe auf bestimmte Websites meistens nur bei größere Firmen
- Automatisierte Angriffe von Bots auf kleine und mittlere Websites sind sehr viel häufiger
- Angriffe aus Langeweile oder wegen politischen & gesellschaftlichen Statements

Ökonomische Gründe

- **Drive-by-Downloads:** Infizierung der Website mit Malware, die sich beim Besuch der Seite auf den Computer des Besuchers herunterlädt / installiert
- **Blackhat SEO**: Einbinden von (unsichtbaren) Links, damit die Websites in Google oder Bing gefunden werden. Häufig Affiliate-Links (Provision)
- **Systemressourcen**: Nutzung des Servers für Aufgaben wie Botnetze, Spam, etc. Die Website muss dabei keine Auffälligkeiten zeigen

Folgen von Angriffen und Hacks

- Aussendung von Spam oder Malware hat direkte Folgen für die Website-Besucher - Fahrlässigkeit?
- Blocken der Website durch Google
- Abschalten der Website durch den Hoster
- Blocken durch Anti-Virus-Programme
- Folge: keine Besucher, keine Bestellungen, verlorene Reputation
- Neues IT-Sicherheitsgesetz (seit 25.07.2015):
  Unter Umständen sogar relevant, Bußgelder drohen



Grundregeln WP-Sicherheit

Grundregeln

- Sicheres Passwort (> 12 Zeichen)
- Benutzertrennung (1 x Admin, 1 x Redakteur)
- Updates aller Komponenten (WP, Plugins, Themes)
  - Bei kostenpflichtigen Komponenten: gültige Lizenz!
- Regelmäßiges Backup
  - Mindestens 1 x pro Woche
  - Am besten automatisch
  - Auf ein externes System (anderer Server, Cloud, eigener Rechner)
- Zusätzliche Sicherheitsmaßnahmen
  - Generell auch ohne Sicherheits-Plugins möglich
  - Bei wenig Wissen: lieber Sicherheitsplugin als gar nichts

Praxistest: Das weiß ich über deine Seite

Praxistest

- Benutzernamen
  - Author-Enumeration (?author=1)
  - Ein gutes Passwort schützt
  - Plugin "Edit Author Slug"
- WordPress-Version
- Pfad auf dem Server
  - wp-includes/rss-functions.php
  - Rückschluss auf Hoster und ggf. Benutzernamen möglich

Praxistest

- Informationen sind weitgehend nutzlos,
  wenn System gut abgesichert ist
- Trotzdem kann die Installation gehärtet werden, um die Informationen nicht offensichtlich rumliegen zu lassen
- Anpassung htaccess-Datei ist ein Weg:
  https://gist.github.com/zottto/608a18d109bd22e76aa4

Ask Me Anything

Vielen Dank!

Diese Folien, alle Links und Plugin-Empfehlungen gibt es in Kürze in meinem Blog zum Nachlesen.

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