Dem Hacker keine Chance – Grundlagen der WordPress-Sicherheit

Marc Nilius

WordPress-Meetup Bonn, 3. Mai 2017

Über mich

- Diplom-Informatiker und selbständiger Web-Entwickler
- WordPress-Wartung und WordPress-Sicherheit
- @marcnilius oder @wpsicherheit
- https://www.wp-wartung24.de
- Co-Organizer diverser Meetups und WordCamps

Warum werde ich gehackt?

Wie werde ich gehackt?

Wie kann ich mich schützen?

Warum werde ich gehackt?

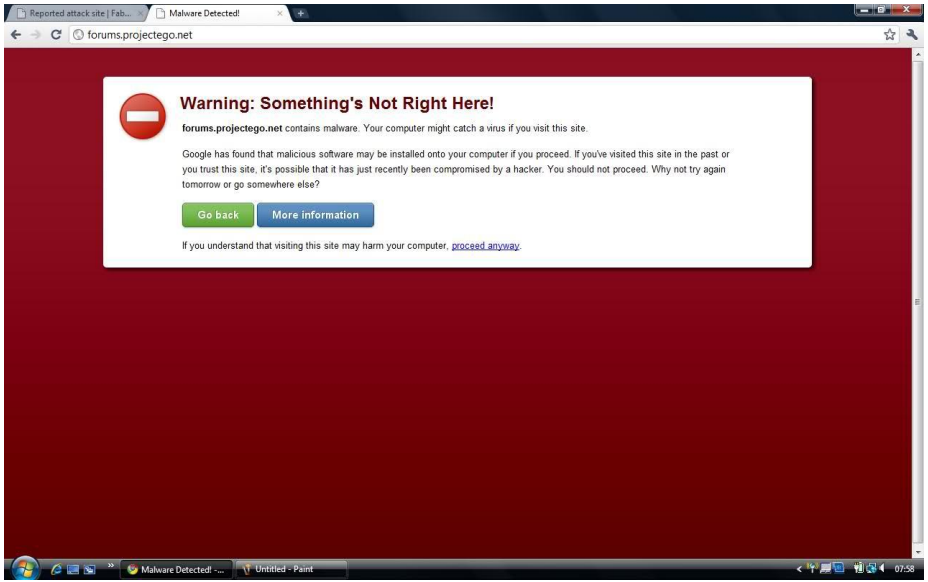
Warum werde ich gehackt?

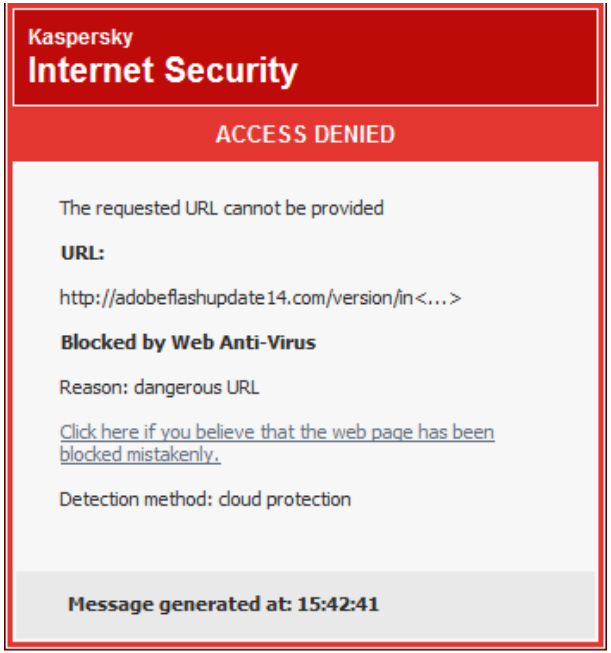
- Die meisten Angriffe geschehen automatisch und nicht zielgerichtet
- Automatisierte Angriffe von Bots auf kleine und mittlere Websites sind sehr viel häufiger als gezielte Angriffe
- Selten aber möglich: Angriffe aus Langeweile oder wegen politischen & gesellschaftlichen Statements

Ökonomische Gründe für Angriffe

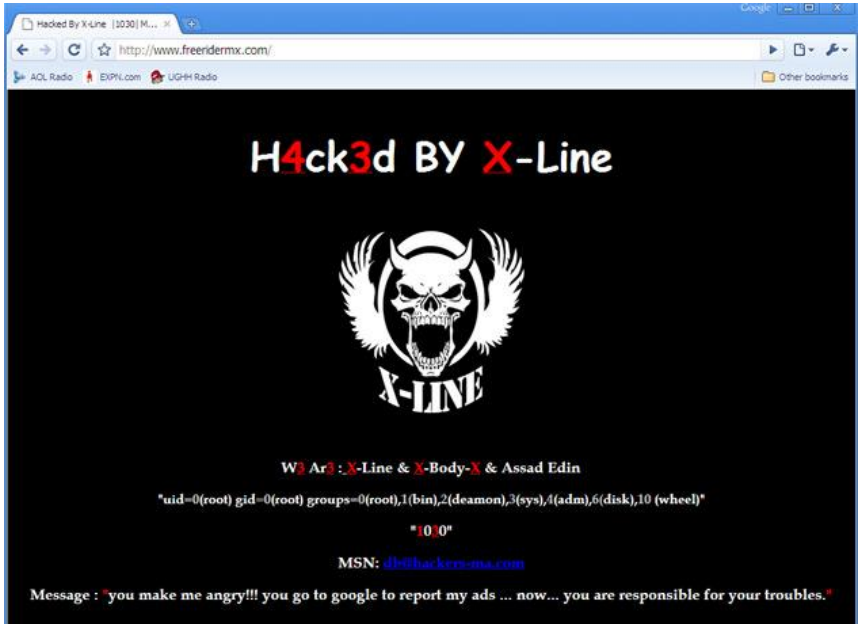
- **Systemressourcen**: Nutzung des Servers für Aufgaben wie Botnetze, Spam, etc. Die Website muss dabei keine Auffälligkeiten zeigen
- **Drive-by-Downloads:** Infizierung der Website mit Malware, die sich beim Besuch der Seite auf den Computer des Besuchers herunterlädt / installiert
- **Blackhat SEO**: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

Folgen von Angriffen und Hacks





Folgen von Angriffen und Hacks



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
- IT-Sicherheitsgesetz: Unter Umständen drohen Bußgelder

IT-Sicherheitsgesetz

- **Betreiber von Web-Angeboten sind verpflichtet, ausreichende, dem Stand der Technik entsprechende technische und organisatorische Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme zu ergreifen.**
- Ggf. drohen Abmahnungen

Wie werde ich gehackt?

Wie werde ich gehackt?

- Sicherheitslücken in WordPress, Plugins, Themes
  - Cross-Site-Scripting
  - SQL Injections
  - Unauthenticated File Uploads
- Server-Zugangsdaten (FTP)
- WordPress-Login geknackt

Wie werde ich gehackt?

- Grundsätzlich gilt: jede (!) Website, insbesondere WordPress-Website, wird täglich (!) angegriffen
- Dabei sind die meisten Angriffe aber wenig zielgerichtet und mit einfachen Mitteln abzuwehren
- 3 einfache Regeln erhöhen die Sicherheit der Seite immens!

Wie kann ich mich schützen?

Wie kann ich mich schützen?

- Regel Nummer 1: Immer aktuelle Backups haben
  - Mindestens wöchentlich
  - Sowohl alle Dateien als auch die Datenbank
  - Die Export-Funktion von WordPress reicht nicht aus!
  - Entweder über den Hoster oder mit Backup-Plugin
  - Backup muss auf externer Quelle liegen
    - Beim Hoster auf anderem Server
    - Bei einem anderen Hoster
    - In der Cloud
    - Zuhause auf dem PC

Wie kann ich mich schützen?

- Regel Nummer 2: Sichere Passwörter für alle!
  - Ein sicheres Passwort ist mindestens 12 Zeichen lang
  - Zeichenklassen: Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen
  - Je weniger Zeichenklassen, desto längeres Passwort
  - 20 Zeichen sind gut!
  - Für alle (!) WP-Benutzer
  - Für FTP und Datenbank
  - Für den Login beim Hoster

Wie kann ich mich schützen?

- Regel Nummer 3: Komponenten aktuell halten
  - Updates mindestens wöchentlich (für WP, Plugins und Themes)
  - Auto-Update für Minor-Versions aktiviert lassen
    - Bei One-Click-Installationen ggf. vom Hoster deaktiviert
  - Kauf-Plugins und Themes nur mit gültiger Lizenz
    - Lizenz auch im Backend eintragen für Auto-Updates
    - Bei Lizenz-Abo: Abo regelmäßig verlängern
  - Vor den Updates: natürlich ein Backup machen
  - Ausnahme: Bei größeren Versionssprüngen von WordPress (4.6.x auf 4.7.x) oder großen Plugins (WooCommerce) kann man eine Woche abwarten

Wie kann ich mich schützen?

- Ergänzend (Regel 3,5):
  - Keine alten Plugins verwenden (letztes Update max. 2 Jahre her)
  - Aktuelle PHP-Version nutzen (mind. 5.6, besser 7)
  - Nur einen Administrator-Benutzer (der darf sogar admin heißen)
  - Arbeiten an Seiten und Beiträgen nur mit einem Nicht-Admin
  - So wenige Benutzer wie möglich, insbesondere Admins
  - Nicht genutzte Plugins und Themes löschen (nicht nur deaktivieren)

Verbesserter Schutz

- Es gibt viele Härtungsmaßnahmen, die Standard-Angriffe besser abwehren können
- Nicht zwingend Plugin notwendig
- Einsatz aber bitte nur mit entsprechender Erfahrung
- Mehr Sicherheit mit der .htaccess-Datei: https://gist.github.com/zottto/608a18d109bd22e76aa4
- Über Autorenseiten Benutzernamen herausfinden: https://de.wordpress.org/plugins/edit-author-slug/

Verbesserter Schutz

- Standard-Sicherheitsplugins können eine gute Möglichkeit sein
- Problem: viele Funktionen und falsche Anwendung durch Laien
- Beispiele:
  - iThemes Security
  - Wordfence (mit einfacher Web Application Firewall) und Dateiscan
  - All-In-One Security

Profi-Schutz

- Web Application Firewall
  - Eine "Mauer" vor der eigentlichen Anwendung (WordPress)
  - Verhindert mit intelligenten Regeln die Ausnutzung von bekannten Sicherheitslücken
  - Lokale WAFs
    - Ninja Firewall: https://de.wordpress.org/plugins/ninjafirewall/
    - Eingeschränkt auch Wordfence
  - Cloud-WAFs
    - Cloudflare, Sucuri
    - Datenschutzrechtlich in Deutschland nicht einwandfrei

Profi-Schutz

- Überwachung aller Dateiänderungen
  - Angreifer hinterlegen Schadcode und Backdoors
  - Überprüfung aller Dateiänderungen ermöglicht schnelle Erkennung
  - Aufwendig und viel Erfahrung notwendig, um Auffälligkeiten zu erkennen
  - Beispiele:
    - Ninja Firewall
    - iThemes Security

Mehr zum Thema WP-Sicherheit

- Kostenloser Newsletter alle zwei Wochen: https://www.wp-sicherheit.info
- Facebook-Gruppe: "WordPress-Sicherheit"

Vielen Dank!

Zeit für Fragen und Diskussion!

Vortragsfolien auch unter
https://www.wp-wartung24.de/blog

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