WordPress-Sicherheit in a nutshell

Marc Nilius

WordPress-Meetup Dortmund, 10. Juni 2021

Über mich

- Inhaber WP-Wartung24
- Technik und Support für WordPress-Websites, Wartung & Sicherheit, https://www.wp-wartung24.de
- Anzutreffen auf den Meetups in Köln, Bonn und Koblenz
- Diplom-Informatiker

Warum werde ich gehackt?

Frage ans Meetup: Ja, warum denn?

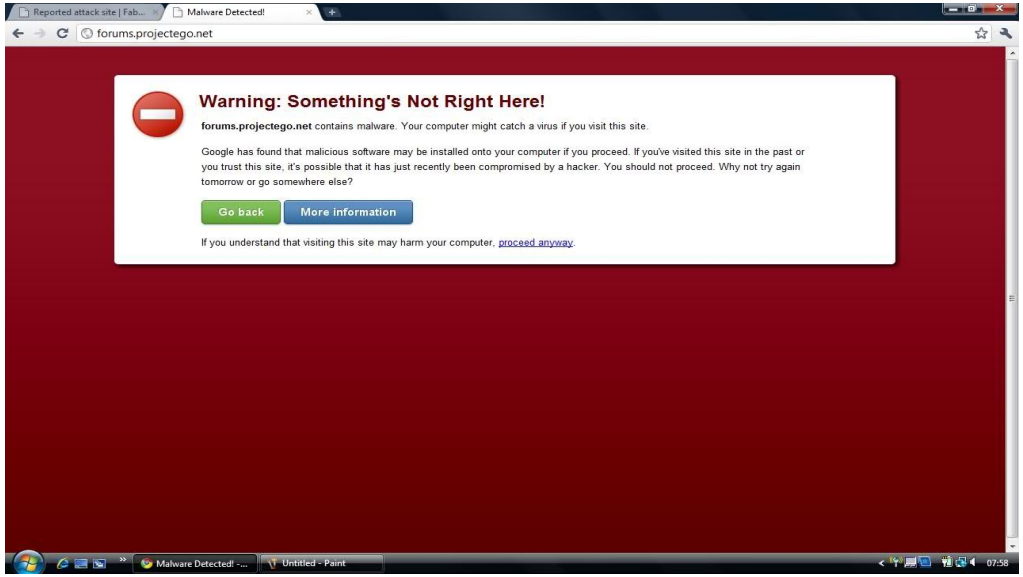
Warum werde ich gehackt?

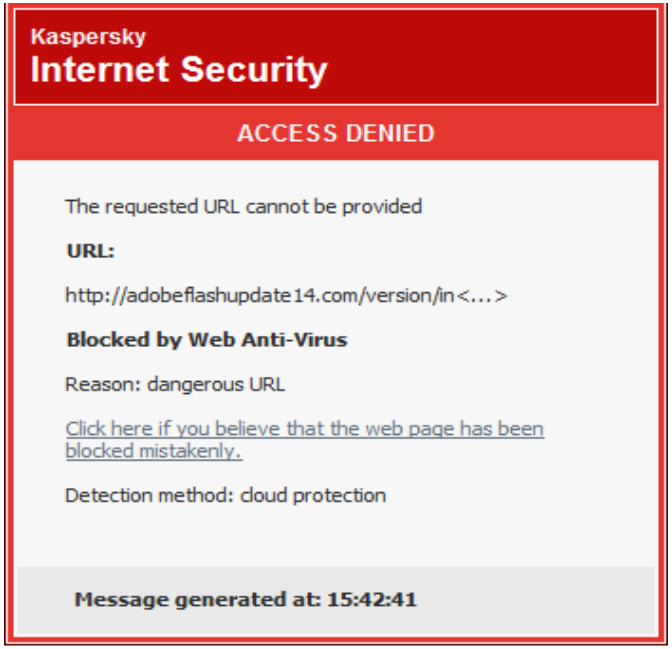
- Angriffe automatisch und nicht zielgerichtet
- Häufig: automatisierte Angriffe von Bots auf kleine und mittlere Websites
- Selten aber möglich: Angriffe aus Langeweile oder wegen politischen & gesellschaftlichen Statements

Ökonomische Gründe für Angriffe

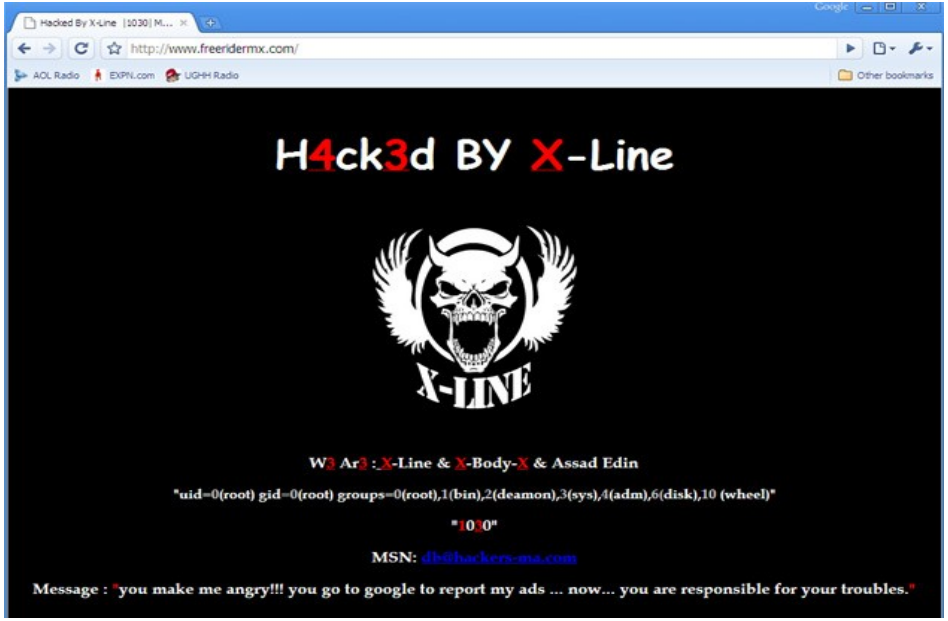
- **Systemressourcen**: Nutzung des Servers für Aufgaben wie Botnetze, Spam, etc. Die Website muss dabei keine Auffälligkeiten zeigen
- **Drive-by-Downloads:** Infizierung der Website mit Malware, die sich beim Besuch der Seite auf den Computer des Besuchers herunterlädt / installiert
- **Blackhat SEO**: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

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.**

DSGVO

- Fehlende Absicherung Grund für Untersuchungen / Bußgelder
- Meldepflicht bei den Datenschutzbehörden, wenn personenbezogene Daten in der Website gespeichert sind! (72h)
- Informationspflicht an betroffene Personen!
- Reputationsverlust!

Welche Schutzmaßnahmen habt ihr?

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?

- Jede (!) Website wird täglich (!) angegriffen
- Angriffe sind wenig zielgerichtet und mit einfachen Mitteln abzuwehren
- 3 einfache Maßnahmen erhöhen die Sicherheit der Seite immens!

Wie kann ich mich schützen?

Was nichts bringt (oder sehr wenig)

- Login-Versuche sperren
- Verstecken von WordPress-Version, Verzeichnisnamen, Uploads-Verzeichnis, verwendeten Plugins, o.ä.
- Kryptischer Benutzername oder Benutzername verstecken
- Passwort andauernd wechseln
- 5 Sicherheitsplugins gleichzeitig

Wie kann ich mich schützen?

- **Maßnahme 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?

- **Maßnahme Nummer 2:** Sichere Passwörter für alle!
  - Ein sicheres Passwort ist mindestens 16 Zeichen lang
  - Zeichenklassen: Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen
  - Je weniger Zeichenklassen, desto längeres Passwort
  - > 20 Zeichen sind gut!
  - Für alle (!) WP-Benutzer, nicht nur Admins
  - Für FTP und Datenbank
  - Für den Login beim Hoster

Wie kann ich mich schützen?

- **Maßnahme Nummer 3:** Komponenten aktuell halten
  - Updates mindestens wöchentlich (für WP, Plugins und Themes)
  - Auto-Update für Core-Minor-Versions aktiviert lassen
    - Bei One-Click-Installationen ggf. vom Hoster deaktiviert
    - Auto-Update für Plugins ist diskutabel
  - 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 (4.9.x auf 5.x) oder großen Plugins (WooCommerce) kann man etwas abwarten

Wie kann ich mich schützen?

- **Ergänzend (Maßnahmen 3+):**
  - Keine alten Plugins verwenden (letztes Update max. 2 Jahre her)
  - Aktuelle PHP-Version nutzen (mind. 7.3)
  - 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*

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

Profi-Schutz

- Login mit Zwei-Faktor-Authentifizierung
  - Neben Benutzername und Passwort ist noch Eingabe eines weiteren Codes nötig
    - Entweder per SMS
    - Per App (zB Google Authenticator)
    - Oder per Hardware-Dongle (Yubikey)
  - Plugin „TwoFactor“
  - Vortrag von Matthias Kurz auf WordPress.TV: *https://wordpress.tv/2017/05/16/matthias-kurz-absicherung-von-wordpress-durch-zwei-faktor-authentifizierung-mit-security-keys/*

Vielen Dank!

Zeit für Fragen und Diskussion!

Vortragsfolien auch unter https://marcnilius.de

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