Wie schütze ich meine Webseite vor Hacker-Angriffen?

Wie schütze ich meine Webseite vor Hacker-Angriffen?

Heute ist es möglich, eine eigene **Webseite** auch ganz **ohne Programmierkenntnisse** zu erstellen und zu betreiben. Dabei helfen sogenannte **Web-Apps wie Joomla oder WordPress**, in die Inhalte ganz einfach eingefügt werden können. Als **Webseitenbetreiber** sind Sie jedoch auch **selbst für Ihre Webanwendungen verantwortlich**. Sollte Ihr System dann von **Hackern angegriffen** werden, ist es notwendig die Sicherheitslücken auf schnellstem Wege zu schließen. Andernfalls kann es dazu kommen, dass unsere **Abuse-Abteilung** eingreifen und Ihre **Seite vorübergehend sperren** muss, bis die Sicherheit wiederhergestellt ist. Wir haben deshalb einige **Tipps zum Schutz Ihrer Webpräsenz** zusammengestellt.

So geht’s Schritt für Schritt:

1. **Führen Sie regelmäßige Updates durch!**

Die zwei Open-Source-Programme Joomla und WordPress gehören aktuell zu den meistgenutzten Content-Management-Systemen. Leider verwenden viele Nutzer veraltete Versionen und riskieren somit ungewollte Zugriffe durch Hacker. Daher bitten wir Sie Ihre Webapplikationen stets auf dem neuesten Stand zu halten. Bei WordPress gibt es die Möglichkeit, **Updates automatisch** im Hintergrund ausführen zu lassen.

2. **Plugins und Erweiterungen müssen ebenfalls aktualisiert werden!**

Da Plugins und Erweiterungsmodule als eigenständige Programme arbeiten, werden diese nicht zwangsläufig mit dem Update der Webanwendung aktualisiert. Dies kann ebenfalls zu einem Sicherheitsrisiko für User werden, weshalb wir auch hier regelmäßige Updates dringend empfehlen. Bei den beiden Webanwendungen WordPress und Joomla ist dies ganz einfach **über das Dashboard** möglich.

3. **Sichern Sie Ihre Daten rechtzeitig!**

Sollten SIe einmal Opfer eines Hacker-Angriffs werden, hält sich der Schaden in Grenzen, wenn Sie Ihre wichtigsten Daten und Einstellungen von vornherein gesichert haben. Daher ist es ratsam ein **regelmäßiges Backup** Ihrer Daten und Datenbanken, sowie Systemdateien Ihrer Webanwendung durchzuführen. WordPress stellt dazu z.B. das kostenlose Plugin „BackupWordPress“ zur Verfügung und auch Joomla gibt den Nutzern mit „Akeeba Backup“, „Easy Joomla“ oder „LazyDbBackup“ wichtige Tools mit an die Hand. Über Ihren 1blu Kundenservicebereich haben Sie ebenfalls die Möglichkeit ein Backup durchzuführen und einzuspielen.

4. **Verwenden Sie sichere und komplexe Passwörter!**

Trotz des Allgemeinwissens um die wichtige Bedeutung von Passwortsicherheit werden immer noch Passwörter verwendet, die für Hacker keine große Hürde darstellen. Daher denken Sie bitte daran, ein Passwort zu generieren, das aus **mindestens 12 Buchstaben unter Gebrauch von Groß- und Kleinschreibung** besteht. Des Weiteren sollten Zahlen und Sonderzeichen enthalten sein.

Vermeiden Sie Wörter, die man in einem Wörterbuch finden kann und kombinieren Sie die einzelnen Elemente miteinander (Buchstaben, Zahlen, Sonderzeichen). Sie können dazu auch ein entsprechendes Tool wie z.B. den kostenlosen Passwort-Generator „GaiJin“ verwenden.

5. Wählen Sie einen sicheren Benutzernamen!

Zusätzlich zu einem sicheren Passwort können Sie mit einem eher untypischen Benutzernamen einen Hacker-Angriff erschweren. **Vermeiden Sie** deshalb obligatorische Bezeichnungen wie „**Administrator**“ **oder** „**admin**“ oder Ihren Namen. Gestalten Sie Ihren Benutzernamen eher komplex und fügen Sie ebenfalls Zahlen oder sonstige Kürzel hinzu.

6. Verwenden Sie Captchas!

Besonders häufig sind Gästebücher und Kontaktformulare von automatisierten Zugriffen durch Hacker betroffen. Eine einfache Möglichkeit dem entgegenzuwirken ist die Verwendung von Captchas, also „Completely Automated Public Turing test to tell Computers and Humans Apart.“ Viele Erweiterungen enthalten diese Option bereits, aber Sie können alternativ auch schauen, ob Ihnen ein **Captcha-Plugin** zur Verfügung steht.

7. Überprüfen Sie Ihre Webseite!

Da Sie als Webseitenbetreiber oft gar keine Kenntnis über einen Hacker-Angriff haben oder diesen erst zu spät bemerken, sollten Sie in regelmäßigen Abständen überprüfen, ob Ihre Seite gehackt wurde. Dafür stehen Ihnen verschiedene **kostenlose Tools** zur Verfügung, wie beispielsweise von „SIWECOS“, einem deutschen Projekt zur Webseitensicherheit.

8. Tipps für WordPress!

- **WordPress und PHP aktuell halten**
  WordPress regelmäßig updaten (ggf. „Automatisches Update“ in der easyApp-Verwaltung aktivieren) und eine aktuelle, offiziell unterstützte PHP-Version verwenden.
- **Plugins und Themes verwalten**
  Updates zeitnah installieren. Veraltete oder nicht benötigte Erweiterungen löschen, statt sie nur zu deaktivieren.
- **Sicherheits-Plugins einsetzen (WAF)**
  Login-Versuche begrenzen (z.B. max. 3 Fehlversuche), Sperrzeiten festlegen und bekannte Angriffsmuster blockieren.
- **XML-RPC absichern**
  Zugriff auf xmlrpc.php nur erlauben, wenn unbedingt nötig. Andernfalls per Sicherheits-Plugin oder .htaccess-Konfiguration blockieren. Meist reicht die REST-API als Alternative aus.
- **Formulare schützen**
  Captchas für Kontakt-, Kommentar- oder Gästebuch-Formulare einsetzen. Nicht benötigte Formulare deaktivieren.
- **Starke Zugangsdaten verwenden**
  Lange, komplexe Passwörter nutzen und den Standard-Benutzernamen „admin“ durch einen individuellen Benutzernamen ersetzen. Optional eine Zwei-Faktor-Authentifizierung einrichten.
- **HTTPS konfigurieren**

SSL-Zertifikat anlegen und Webseite vollständig auf HTTPS umstellen (inkl. WordPress- und Website-Adresse auf „https://“ anpassen).

- **Datenbank modernisieren**
  Falls noch MySQL 5 im Einsatz ist, kann eine Migration auf eine MySQL-Datenbank der Version 8 oder höher die Sicherheit erhöhen.
- **Dateien im Webspace kontrollieren**
  Regelmäßig alle Verzeichnisse auf unbekannte oder ungewöhnlich große Dateien prüfen (vgl. Backups). Schadcode ist oft verschleiert (alphanumerischer Code in Dateien).
- **Logfiles überwachen**
  Regelmäßig Logfiles im logfiles-Ordner auf ungewöhnliche Zugriffe prüfen. Aus DSGVO-Gründen werden diese nach kurzer Zeit gelöscht.
- **Langfristige Backups erstellen**
  Regelmäßig Sicherungen von WordPress (Dateien und Datenbank) z.B. über ein Backup-Plugin oder ggf. über die easyApp-Verwaltung anfertigen. Die automatischen Backups im _backup_-Ordner reichen nur 14 Tage zurück.
- **Aktuelle Informationen nutzen**
  Regelmäßig Sicherheitshinweise und Empfehlungen recherchieren (z.B. online nach „WordPress absichern“ suchen).

Eindeutige ID: #1821
Verfasser: 1blu Support-Team
Letzte Änderung: 2025-09-26 18:53