

Sicherheitshinweise CMS Systeme

Sicherheitshinweise CMS Systeme wie: Joomla, Wordpress usw.

- Mosillus.com übernimmt keine Haftung für einen Hack ihrer Webseite, Sicherheitslücken in CMS Systemen sowie unsicheren Passwörtern in CMS Systemen, FTP usw. Bitte beachten Sie, dass ein normaler Name oder ein Wort als Passwort keine Sicherheit vor Trojanern und Malware sowie Spam darstellt. Es ist daher von Vorteil ein PW von mindestens 12 Zeichen / Gross & Kleinbuchstaben, Zahlen und Sonderzeichen wie " * , & , %" oder ähnlich in das Passwort einzubauen und dieses an einem sicheren Ort aufzubewahren.
- Beachten sie auch, dass sie die CMS Systeme wie Wordpress, Drupal, Joomla etc. immer wieder auf den neusten Stand bringen (Update der Systemversion) , um einen optimalen Schutz vor Hacks zu gewährleisten. Sie können das Update selbst durchführen, wenn Sie sich das zutrauen und ein wenig Erfahrung mit dem jeweiligen System haben.
- Das CMS Admin, E-Mail PW sowie FTP PW sollte alle 1-2 Jahre erneuert werden. (Bitte verwenden Sie unterschiedliche Passwörter für die jeweiligen Systeme).
- Speichern Sie **keine** Passwörter in Ihrem e-Mail Programm. Versenden Sie keine Passwörter per e-Mail (Oder ändern Sie diese anschliessend). Seien Sie im Umgang mit Passwörter immer vorsichtig.
- Passwörter müssen nach unserer Empfehlung mind. 12 Zeichen enthalten. Hier ein Beispiel eines sicheren Passworts: „xXrZ982-3324-1sAydd-ww“
- Wie alt ist ihre Webseite? Grundlegend gilt; Je älter das System der Webseite ist, desto gefährdeter ist es.
- Wordpress scheint als CMS System weltweit am meisten betroffen zu sein, da es am meisten verbreitet und das beliebteste CMS System ist.
- Mosillus.com beauftragt für das Hosting (Webseiten Datenhosting) seiner Kunden die Metanet AG. Schauen Sie in Ihren Metanet.ch Unterlagen (Einrichtungsbestätigung) wie viele Zeichen Ihr Admin für Wordpress, Joomla sowie FTP und Webmail PW enthält. Früher galten 8 Zeichen als ausreichend, Mosillus.com empfiehlt eine Änderung des Passwortes auf mindestens 12 Zeichen falls Sie nur 8 oder weniger haben.
- Optional und auf Aufpreis kann ein "Login Lockdown" installiert werden. Das Login von Wordpress ist so nach 3 missglückten Login versuchen für 60 Minuten gesperrt.
- Falls Sie nicht sicher sind auf welchem Stand ihre Wordpress Version oder ihr PW auf dem FTP sind, fragen Sie uns. Wir können Ihnen bestimmt weiterhelfen.
- Untersuchen Sie Ihren PC und Ihr CMS regelmässig auf Malware und Viren. Meisten gelangt Malware durch einen bereits angegriffenen PC ins System.
- Die Konsequenzen von **nicht** Einhalten dieser Regeln kann dazu führen, dass Sie den Inhalt der Webseite nach einem Maleware Angriff löschen müssen. Dabei gehen meistens alle Daten der Webseite verloren. Die Löschung der Nameserver-Zuordnung wird durch die Switch im Auftrag für den Bund (Schweizer Registrierstelle) geregelt.

Der Ablauf **nach** einem Angriff auf Ihre Webseite durch Malware sieht folgend aus:

1. Löschung der Name-Server-Zuordnung, gestützt auf AGB Ziff. 3.2.3 lit. b in Verbindung mit Ziff. 3.3.2 Abs. 2 lit. e. Dies bedeutet, dass Ihre Website nicht mehr erreichbar ist.
<http://www.nic.ch/de/terms/agb.html>
 2. Blockierung des Domain-Namens, gemäss AEFV Art. 14f bis.
http://www.admin.ch/ch/d/sr/784_104/a14bisi.html
 3. Verständigen der zuständigen Behörden, um eine richterliche Verfügung zu beantragen.
- Wir gehen davon aus, dass Sie den schädlichen Code schnellstmöglich beseitigen oder die betreffenden Websites von Ihrem Server entfernen. Unterstützung erhalten Sie dabei von Ihrem Hosting-Anbieter sowie auf der SWITCH-Website:
<http://www.nic.ch/de/faq/malware.html>

- Weitere Hilfe gibt es Hier: <http://www.nic.ch/de/faq/malware.html>
- Eine 100% Sicherheit gibt es **nie**, aber mit diesen Massnahmen erschweren sie es den Malware - Urhebern bereits erheblich.