Meine Webseite ist gehackt - was tun?

1. Ruhe bewahren :-)) und - systematisch und gründlich vorgehen. Bei den folgenden Schritten muss die Reihenfolge eingehalten werden.

Anmerkung: Die folgenden Schritte funktionieren immer und sind die einfachste und schnellste Methode. Voraussetzung ist allerdings, dass Sie eine nicht infizierte Sicherung Ihres Dateisystems und Ihrer Datenbanktabellen haben.

Falls Sie dies nicht haben wird es schwierig (und unsicher). Sie müssen dann Ihr Dateisystem nach dem Datum der Dateiänderungen durchgehen, die Dateien entsprechend ersetzen und in Ihrer Datenbank nach Änderungen suchen.

Es gibt spezialisierte Anbieter, die mit Skripten Dateisystem und Datenbanktabellen nach typischen Hackangriffen durchgehen und entsprechend Änderungen vornehmen.

2. Die eigene Arbeitsumgebung überprüfen - ist Ihr PC sicher?
Grund: eventuell werden Passwörter **auch von Ihrem derzeitigen** PC abgegriffen. Wenn Sie in den Folgeschritten Passwörter abändern, ist so alle Mühe umsonst.

3. Die Zugriffspasswörter für Ihre Webseite ändern - FTP Passwörter, Datenbank-Passwörter
Grund: Wie bei 2. - eventuell wurden FTP-Passwörter zusammen mit den Domainnamen beim Hochladen von Ihrem PC aus abgefangen. Mit dem FTP Passwort kann das Hackerskript alle weiteren Passwörter auslesen.

4.FTP Übertragung ist nie völlig sicher - Sie können die Sicherheit jedoch verbessern - mit SFTP. Ihr Hoster sollte diese Möglichkeit anbieten. Sie stellen Ihren **FTP Client** **also auf "Passwörter nicht speichern" und SFTP** und laden Ihre letzte nicht infizierte Dateisystemsicherung in **einen neuen Ordner** Ihres Webspace.
Grund: Es nützt nichts Ihre Dateien zu überschreiben - eventuell hat der Hacker neue Dateien angelegt, die er aufrufen kann, um so auf Ihrem Webspace Skripte auszuführen.

5. Sie passen in der Konfigurationsdatei Ihres Content-Management-Systems das

Datenbankpasswort an. (Sie hatten es in Schritt 3 geändert).

6. Sie löschen alle Datenbanktabellen und importieren Ihre Datenbanksicherung.

7. Sie legen jetzt Ihre Domain auf den neuen Ordner (im Kundenmenü des Hosters).

8. Ihre Webseite funktioniert jetzt wieder auf dem Stand Ihrer Sicherung.

9. Sie überprüfen die Version Ihres Content-Management-Systems und machen ein Update auf die neueste Version.
Grund: Alte Versionen haben bekannte Sicherheitslücken. Hackerskripte suchen im Netz gezielt nach diesen Sicherheitslücken.

10. Sie können Ihre Webseite bei der SIWECOS der Internetwirtschaft, unterstützt vom Bundesministerium für Wirtschaft und Technologie, anmelden für das Monitoring von eventuell eingeschleuster Malware.

11. Überprüfen Sie, ob Google bei einem Durchlauf bemerkt hat, dass Ihre Webseite gehackt wurde und in den Suchergebnissen die Webseite als schädlich markiert und Aufrufe blockiert. Sie können Ihre Seite in den Google Webmastertools anmelden, überprüfen wie der Google Roboter Ihre Seite sieht und die Löschung des Eintrags beantragen. Google löscht den Eintrag innerhalb eines Tages.

Barbara Funke - Online Publizistik und -PR - www.bfunke.de
