Webseiten-Sicherheit

Fertige Systeme wie Content-Managing-Systeme, Forensoftware, Bildergalerien und vieles mehr, sind in we

nigen Klicks am Webserver installiert. Viele zusätzliche “Plug-Ins“ werden in Sekunden hinzugefügt, Social-Medi

a Plattformenüberberreitsverfügbare Schnittstellen eingebunden. Webseiten oder Shops, die auf diese Weise

Nachteil: Es kann auch ein großer Laie alles schnell einrichten, haben nicht den Vorteil, dass selbst ein Laie alles schnell einrichten kann, auch ein großen

	Diese Konstrukte sind unsicher!

Da viele der genannten „Web-Apps“ und Erweiterungen als kostenlose Open-Source-Lösung verfügbar und millionenfach im Einsatz sind, werden diese auch bevorzugt angegriffen. Die Gründe dafür sind vielfältig, von harmlosen Textänderungen bis hin zu gefährlichen Maßnahmen wie Phishing-Seiten, Spionagetools, Identitätsdiebstahl, „drive-by download“ – Besucher laden unbemerkt Trojaner oder Viren herunter und dem Klassiker: Spamversand – Hier wird die eigene Webseite dazu genutzt, um massenhaft Spammails zu verschicken. Diese Liste könnte man noch sehr lange fortsetzen.

Die Entwickler der jeweiligen Systeme möchten dies natürlich verhindern, indem regelmäßig Updates veröffentlicht werden, um bekannte Schwachstellen sofort schließen zu können. Diese müssen aber erst einmal installiert werden. Einige Maßnahmen die Ihre Webseite und Ihren Webauftritt schützen können, möchten wir nun aufzeigen:

1 Aktualität
Die wohl beliebtesten Webanwendungen sind die Content-Managing-Systeme (CMS) Wordpress und Joomla. Gravierend dabei ist, dass zum Beispiel 3 von 4 WordPress-Installationen überaltert sind. Bei Joomla sind es sogar über 90 % der Webseiten, die mit einer veralteten Joomla-Version laufen. Sei es aus Gründen der Bequemlichkeit oder einfach nur Unwissen, Updates werden viel zu selten genutzt..
Halten Sie Ihre Systeme aktuell!

2 Plug-Ins und Erweiterung aktualisieren
Durch ein Update der Web-Anwendung werden diese nicht automatisch mitaktualisiert. Kriminelle wissen das und nutzen für ihre Angriffe oft gezielt Sicherheitslücken in Plug-Ins und Erweiterungsmodulen. Aktualisieren Sie deshalb Ihre Plug-Ins und Erweiterungen regelmäßig! Bei WordPress und Joomla können Sie diese Updates bequem über das Dashboard ausführen.

3 Backup
Wenn Ihre Webseite gehackt wurde, ist es meist zu spät. Wichtige Daten und Einstellungen, die sich auf dem betroffenen System befunden haben, können dadurch unwiederbringlich zerstört sein. Auch Systemdateien werden teilweise durch Updates überschrieben. Das ist besonders ärgerlich, wenn Sie zum Beispiel individuelle Theme- oder Template-Anpassungen vorgenommen haben. Bei WordPress betrifft das hauptsächlich die folgenden Dateien: index.php, style.css und wp-config.php, während bei Joomla-Template-Änderungen vor allem die Dateien index.php, template.css und template_rtl.css angepasst werden. Führen Sie deshalb regelmäßig ein Backup der Daten, Datenbanken und Systemdateien Ihrer Webanwendung durch. Es gibt für Joomla und Wordpress kostenlose Plug-Ins, die Ihnen dabei helfen, die Datenbank und Ihre Webseitendateien regelmäßig zu sichern. Es ist empfehlenswert, diese Sicherungsdateien nicht am Webspace liegen zu lassen, sondern lokal zu speichern!

Wenn Sie als Telematica-Kunde das Verwaltungsportal cPanel verwenden, können auch hier Backups angelegt und verwaltet werden.

4 Der Klassiker, verwenden Sie nicht 12345 als Passwort
Über Passwortsicherheit ist bereits so viel geschrieben worden, dass die Verwendung sicherer, komplexer Passwörter eigentlich eine Selbstverständlichkeit sein sollte. Doch praktisch werden häufig immer noch Passwörter verwendet, die einfach zu knacken sind und das nicht nur von versierten Technik-Nerds. Ein sicheres Passwort sollte mindestens 10 Zeichen oder mehr enthalten. Verwenden Sie Klein- und Großbuchstaben, Zahlen und Sonderzeichen gemischt und vermeiden Sie Ausdrücke, die in einem Wörterbuch zu finden sind. Zur Generierung eines sicheren Passworts können Sie auch ein Tool nutzen, wie z.B. den kostenlosen Passwort-Generator von GaiJin. Leichter ist es jedoch, dass man sich einen Satz zurechtlegt, den man nicht vergessen kann und einige Buchstaben darin durch Sonderzeichen austauscht. Beispiel: iCh_verWENd3EiNsicH3res!Pass /ort*
(Dieses Passwort aber bitte nicht verwenden;))

5 Benutzernamen

Neben einem sicheren Passwort sollten Sie auch einen Benutz

Wetten, dass Ihre Kollegen und Kolleginnen Ihr Geburtsjahr herausfinden oder bereits wissen ?

ernamenwählen, dernichteinfachzuerratenist. Verwenden Sie stattdenStandards „Administrator“, „admin“ oder Ihr

en Klarnamen lieber komplexere Benutzernamen. Bedenken Sie dabei, dass diese nicht allzu leicht zu erraten sein

s ol lt e.	

6 Sichern Sie Kontaktformulare und Gästebücher
Äußerst beliebte Angriffspunkte für automatisierte Angriffe auf Ihre Webseite sind Kontaktformulare und Gästebücher. Diese sollten Sie daher besonders absichern. Eine einfach und praktische Möglichkeit, um sich vor automatisierten Anfragen zu schützen, sind Captchas (Completely Automated Public Turing test to tell Computers and Humans Apart.) Achten Sie bei der Recherche nach Erweiterungsoptionen am besten direkt darauf, ob diese entweder schon ein Captcha enthält oder ob ein passendes Captcha Plug-In zur Verfügung steht.

7 Erweiterte Sicherheitsvorkehrungen für Experten

Neben den vorgestellten Basic-Tipps gibt es natürlich noch weitere Vorkehrungen, die Sie treffen können, um Hacking und das Einschleusen von Schadprogrammen zu unterbinden. Erstellen Sie einen eigenen „.htaccess“-Zugriffsschutz für den Administrationsbereich und verstecken Sie den Loginbereich. Jeder weiß mittlerweile, dass man sich bei wordpress unter der Adresse meineseite.at/wp-admin und bei Joomla unter meineseite.at/administrator einloggen kann. Optimieren Sie die Rechtevergabe für Ihre Dateien und Verzeichnisse und unterbinden Sie die Ausführung von PHP-Dateien in bestimmten Verzeichnissen.

8 Prüfen Sie regelmäßig, ob Ihre Seite gehackt wurde
Wie Sie sehen, können Sie sehr viel tun, um Ihre Webseite zu schützen. Aber selbst die besten Vorkehrungen können Ihnen keine 100% Sicherheit vor Hacking/Cracking bieten. Als Websitebetreiber merken Sie oft gar nicht oder zu spät, dass Ihre Webseite gehackt wurde. Deshalb sollten Sie Ihre Webseite regelmäßig prüfen. Im Netz gibt es eine ganze Reihe kostenloser Tools, mit denen Sie Ihren Webauftritt auf Manipulationen checken lassen können oder Ihre Webseite direkt zu regelmäßigen Überprüfungen anmelden können.

Seite gehackt? Was tun?

Ihre Seite wurde gehackt? Dann sollten Sie schnell handeln – Melden Sie sich bei uns - Unsere Spezialisten geben Ihnen hilfreiche Tipps, damit Sie diese Situation rasch wieder in den Griff bekommen.