Web Sicherheit

So schützen Sie Ihre Webseite vor Hackern

1. Regelmäßig die Software des Webservers aktualisieren (CMS, Plugins, Themes, Forum, Shop, …)

Für alle weit verbreiteten CMS Systeme (WordPress, Joomla, Typo3 …) gibt es regelmäßig (mehrmals jährlich) Updates. Es ist wichtig, diese Updates so bald wie möglich einzuspielen, da dadurch bekannte Sicherheitslücken geschlossen werden.
Plugins und Themes sollen ebenfalls regelmäßig upgedatet werden. Und vergessen Sie nicht auf 3rd Party Software für das Forum, Shop oder Helpdesk.
Der häufigste Weg, wie Hacker Zugriff auf eine Webseite bekommen, ist durch bekannte Schwachstellen in alter Software oder Scripts. Hacker suchen gezielt nach nicht upgedateten, unsicheren Webservern.

2. Sichere Passwörter verwenden!

Die häufigsten Passwörter in der Welt sind “password” und “1234567”. Auch Passwörter wie „Passw0rd$“ sind nicht sicher und werden in Sekunden von modernen Hacker Tools geknackt.
Verwenden Sie einen Password-Manager (wie z.B. Keypass, Lastpass oder 1Password) und lassen Sie sich sichere Passwörter mit 10 oder mehr Buchstaben, Symbolen und Zahlen generieren.

Passwörter, die für Hacker interessant sind, gibt es bei einer Webseite mehrere:

- ⇨ Datenbank
- ⇨ Administrator Zugriff für CMS
- ⇨ FTP
- ⇨ Zugriffsplattform des Providers (Plesk, cPanel usw.)
- ⇨ E-Mail

Diese sind auf jeden Fall zu ändern, wenn man bereits gehackt wurde!

3. Regelmäßiges Backup von allen Dateien und der Datenbank

Machen Sie regelmäßig Backups Ihrer Datenbank und aller Dateien am Webserver und behalten Sie immer mehrere Versionen auf. Sie merken oft nicht sofort wenn Ihre Webseite gehackt wurde und so können Sie auch auf eine ältere Version zurückgehen.

4. Alle alten, nicht verwendeten Programme am Webserver entfernen – vor allem alte CMS / Plugins

Nicht verwendete Plugins, Themes und vergessene Test-Installationen sind Schwachstellen am Webserver. Jede Software, die nicht in Verwendung ist, soll vollständig deinstalliert werden! Auch ein deaktiviertes Plugin kann von einem Hacker genutzt werden.

5. Gute Anti-Virus- und Schadsoftware-Scanner auf allen eigenen Computern installieren

Sie müssen sicherstellen, dass Ihre Computer, alle Ihre Passwörter und der Zugriff auf Ihren Webserver sicher bleiben. Viele Webserver werden gehackt, weil das FTP Passwort über Keylogger Software (Virus, Trojaner am eigenen Computer) gestohlen wird. Bei anderen wird das Passwort mitgeloggt, wenn sie auf den Webserver über ein öffentliches, nicht sicheres WLAN zugegreifen.

Gute Freeware in diesem Bereich ist z.B.:

- ⇨ Zum Scannen für Malware: *Malwarebytes* – http://de.malwarebytes.org/
- ⇨ Anti-Virus-Programm *Avast*, *Avira* oder ähnliche

6. Geeignete Berechtigungen am Webserver verwenden

Grundsätzlich sollen nur jene Personen ein Login für den Webserver bekommen, die sie auch wirklich brauchen.
Geeignete Berechtigungen sind:

- ⇨ für Verzeichnisse: 755
- ⇨ für Dateien: 644

Dadurch kann nur der Administrator Verzeichnisse und Dateien ändern.
Hinweis: Die Wartung der Webseite über das CMS ist davon nicht betroffen.

7. Vorsicht bei Auskünften am Telefon oder per E-Mail

Viele Hacker nehmen auch persönlich Kontakt auf. Sie rufen an und geben vor, vom Support Ihres Website-Hosting-Providers zu sein oder von der Domain-Registrierungsstelle. Sie fragen nach Ihren Passwörtern oder persönlichen Daten (Geburtstag, Name der Haustiere etc.) um Zugriff auf Ihr Website-Konto zu bekommen. Geben Sie nur Personen, denen Sie vertrauen, per E-Mail oder am Telefon diese Daten bekannt.

8. Zusatzschutz

Zusätzlich kann ein technischer Spezialist:

- ⇨ Überprüfen, ob der Server des Providers aktuell upgedatet ist
- ⇨ Die häufigsten Angriffsmethoden von Hackern über eigene Scripts abwehren