SAFE BLOGGING GUIDE

TIPS AND TRICKS ON HOW TO KEEP YOUR BLOG AND YOUR IDENTITY SAFE

BOGDAN BOTEZATU
E-THREATS ANALYSIS AND COMMUNICATION TEAM

HOME USERS

bitdefender

Inhaltsverzeichnis

147 Millionen Blogs, Tendenz steigend

Es war das Jahr 1999, als eine neue Art Journalismus anfing, um sich zu greifen, in erster Linie gefördert durch das Aufkommen einiger kostenloser Online-Plattformen. Damals ahnte noch niemand, dass Blogs einmal zu einer der wichtigsten Ausdrucksformen im Internet werden würden oder dass sie den gängigen Journalismus, wie wir ihn kannten, für immer verändern würden.

Zurzeit gibt es etwa 147 Millionen Blogs (nach Analysen von BlogPulse), und weitere 54.000 kommen nach derselben Statistik jeden Tag hinzu. Die meisten Blogs sind etwas sehr Persönliches und werden nur von einer oder zwei Personen gepflegt, andere hingegen sind Teil komplexer Kommunikationsstrategien von Unternehmen, die alle ihre spezifische Zielgruppe ansprechen.

Dieser Leitfaden enthält grundlegende Tipps zum sicher Bloggen und befasst sich insbesondere mit persönlichen Blogs, die privat oder bei einer der großen Blog-Plattformen gehostet werden.

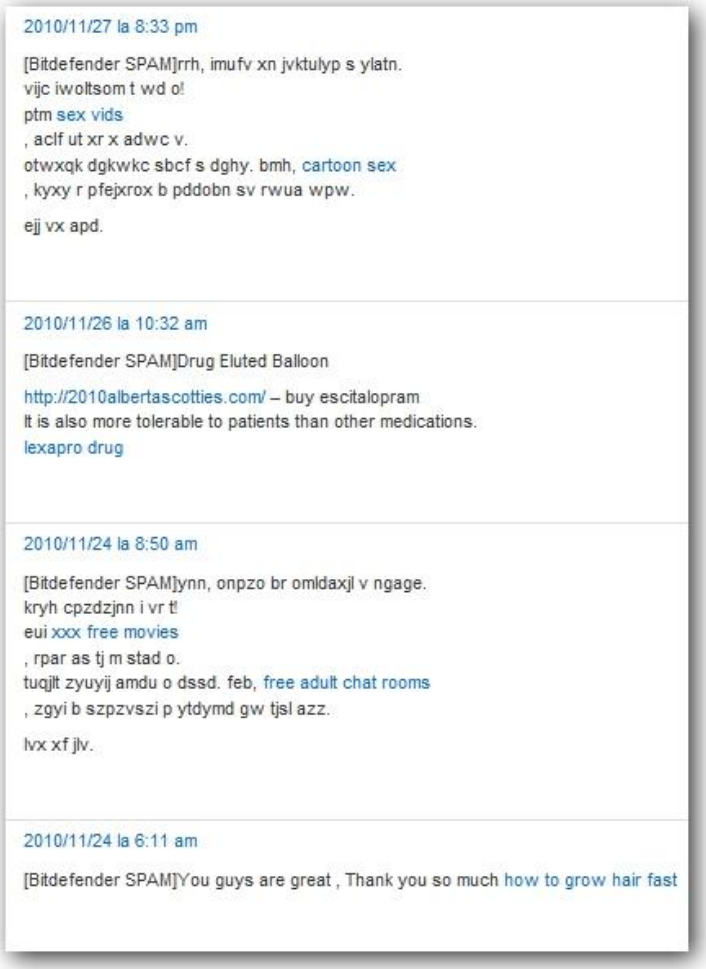
Blogs für jeden Geschmack: eigenes Hosting vs. SaaS

Manche Blogger entscheiden sich für ein Konto bei einer der großen Blog-Plattformen, ideal zum Bloggen für Anfänger, darum sind es meistens diejenigen, die gerade erst das „Fieber“ gepackt hat. Andere hingegen hosten ihr Blog selbst, was mehr Flexibilität sowohl bei der Verwaltung als auch bei der Gestaltung bedeutet, allerdings auch mehr Aufwand mit sich bringt, wenn man sicher bloggen will.

Blogspot®, Wordpress® und LiveJournal® sind die drei beliebtesten Anbieter kostenloser Blogs. Diese werden als Dienstleistung angeboten und professionell vom Anbieter verwaltet, was bedeutet, dass der Nutzer sich nicht um Patches oder andere serverbasierte Sicherheitsvorkehrungen kümmern muss, da der Anbieter sie automatisch zur Verfügung stellt. Ein solches Blog ist zwar deutlich besser vor Angriffen geschützt, aber nicht unbedingt vor Bedrohungen wie Spam oder Phishing und somit zum sicher Bloggen.

Blogs und der Bumerang-Effekt

Unabhängig von der Art des Hostings und dem Inhalt hat ein Blog meistens den Zweck ein Unternehmen oder eine Person darzustellen. Die Person kann sogar selbst ein Unternehmen sein. Werbefinanzierte Blogs sind weit verbreitet und stellen für einen Großteil der Blogger eine Einkommensquelle dar. Es kann jedoch dazu kommen, dass ein Blog gewissermaßen nach hinten losgeht – z. B. dann, wenn es missbraucht wird, z. B. um dem Betreiber zu schaden.



Das Bitdefender-Spamschutz-Plug-in erkennt Spam-Kommentare und meldet sie den Moderatoren.

Blog-Spam

Spam in Blogs wird oft eingesetzt, um dem Image des Blog-Eigentümers zu schaden. Spam-Kommentare beinhalten meist Links zu schädlichen oder (zumindest) obszönen Inhalten. Wenn die Spam-Beiträge überhandnehmen, sinkt der Nutzen des Blogs rapide, denn die sinnvollen Informationen werden dann nur schwer gefunden. In Beiträge eingebettete Links zu dubiosen Websites schaden darüber hinaus dem Stellenwert des Blogs bei den verschiedenen Suchmaschinen – ein herber Schlag im harten Konkurrenzkampf des Online-Business. Außerdem werden Leser ein Spam-überfülltes Blog meiden, was eine Verringerung der treuen Leserschaft nach sich zieht. Leider betrifft das Problem des Blog-Spams sowohl selbst gehostete Blogs als auch die bei den großen Anbietern.

Anmerkung

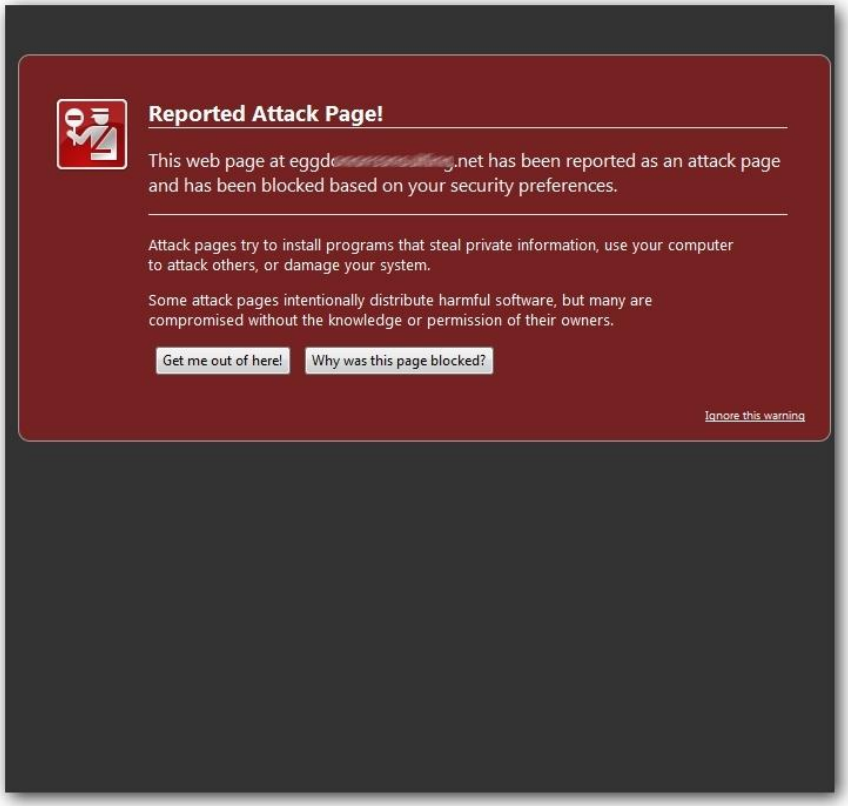
Etwa 99 Prozent aller Spam-Beiträge in Blogs und Foren werden über Spam-Bots gepostet – kleine in einer Skriptsprache wie Perl oder Python geschriebene Programme. Diese Bots sind sehr geschickt und effektiv, aber zum Glück auch sehr leicht zu bekämpfen. Oft zum Beispiel dadurch, dass JavaScript oder Cookies zum Posten eines Beitrags aktiviert sein müssen. Da Spam-Bots weder JavaScript noch Cookies verwenden können, können sie dann auch keine Beiträge schreiben. Eine andere Methode für sicheres Bloggen ist, über CSS ein verstecktes Textfeld einzubauen, das leer bleiben muss, damit der Beitrag gepostet werden kann. Die Bots erkennen dieses Textfeld und versuchen es mit Spam zu füllen, wodurch der Beitrag nicht gepostet werden kann.

Zum Glück lässt sich Blog-Spam sehr leicht bekämpfen, wenn man die richtigen Tools hat und das Blog entsprechend eingerichtet ist. Folgend finden Sie einige Tipps zum sicheren Bloggen und wie Sie Spam-Beiträge auf Ihrem Blog verhindern können.

1. Legen Sie fest, dass der erste Beitrag jedes neuen Benutzers erst veröffentlicht wird, wenn ein Administrator ihn genehmigt. So können ehrliche Benutzer nach ihrem ersten, genehmigten Beitrag weitere Beiträge schreiben, die dann automatisch veröffentlicht werden.

2. Legen Sie fest, dass jeder Beitrag erst veröffentlicht wird, wenn ein Administrator ihn genehmigt hat. Dieser Ansatz ist deutlich sicherer als der erste, bedeutet bei Blogs mit einer großen Benutzergemeinde aber einen erheblichen Mehraufwand.

3. Installieren Sie ein Spamschutz-Plug-in. Wenn Sie Wordpress als Blog-Plattform nutzen, sollten Sie das Spamschutz-Plug-in von Bitdefender einsetzen. Diese völlig kostenlose Lösung prüft über eine API beim Spamschutz-Cloud-Dienst von Bitdefender, ob ein Beitrag Spam ist oder nicht.



Warnungen vor bösartigen Inhalten schrecken Besucher des Blogs ab und bewirken meist, dass sie nie wiederkommen.

Blog-Malware

Wenn der Eigentümer des Blogs nicht gerade selbst schädliche Dateien auf sein Hosting-Konto hochgeladen hat, wird Malware in Blogs meist dadurch eingeschleust, dass das Blog oder der Server, auf dem es liegt, gehackt wurde.

Ein Angreifer kann auf verschiedenen Wegen die Kontrolle über ein Blog und sein FTP-Konto erlangen. In einigen Fällen sind diese Angriffe sehr sorgfältig geplant und erfordern ein hohes Maß an Computerkenntnissen. In anderen Fällen melden sich die Angreifer einfach mit dem richtigen Benutzernamen und Passwort an.

1. Oft passiert es, dass Bloggern ihre Zugangsdaten gestohlen werden, weil sich auf ihrem Computer Malware eingeschlichen hat. Bestimmte Trojaner wie iStealer oder der berüchtigte Facebook Hacker greifen Kombinationen von Benutzernamen und Passwörtern direkt im Passwort-Manager des Browsers ab. Gängige Keylogger (kleine Programme, die Tastenanschläge protokollieren) können ebenfalls Zugangsdaten abgreifen und an den Eindringling senden. Und nicht zuletzt können Passwörter auch ausgelesen werden (sog. Sniffing), wenn unbedachte Blogger sich per öffentlichem WLAN in einem Café in ihrem Blog anmelden. Dasselbe gilt für FTP-Zugangsdaten, die eine wahre Goldmine für Cyber-Kriminelle darstellen, da sie dann infizierte Dateien, Malware und Phishing-Seiten unter dem gestohlenen Konto speichern können.

2. Blogs können auf verschieden Weise gehackt werden, und gegen manche sind Benutzer auch nahezu machtlos. So können Hosting-Konten beispielsweise über eine schlechte Server-Konfiguration oder Software mit ausnutzbaren Schwachstellen geknackt werden. Andere Angriffe wiederum folgen direkt aus fehlerhaften Blog-Installationen oder angreifbaren Plug-ins. Sogenannte Zero-Day-Fehler in einer Blog-Software können auch dazu führen, dass Eindringlinge Zugangsdaten stehlen oder unachtsame Benutzer ihre Systeme mit Malware infizieren.

Egal, wie Malware in ein Blog gelangt, sie wird in jedem Fall das Ansehen und die Funktionalität des Blogs beschädigen. Die meisten Suchmaschinen prüfen die indizierten Seiten durchgehend auf Malware, die Besuchern der Seiten schaden könnte. Wenn bösartige Inhalte gefunden werden, wird die Seite intern sofort als gefährlich gekennzeichnet, was heißt, dass Benutzer, die diesem Link folgen, gewarnt werden, dass der angeklickte Inhalt Gefahren für die Besucher und ihre Computer birgt.

Blog-Malware beschränkt sich jedoch nicht auf Bedrohungen, die ein einzelnes Benutzerkonto betreffen, sondern kann auch in Form von Skripten daherkommen, die im Blog hinterlegt werden und Benutzer auf Websites mit gefährlichen Inhalten umleiten können, oder in Form von Pseudo-Virenschutzskripten, die einen System-Scan vortäuschen. Unabhängig von der Art der Malware wird ein infiziertes Blog höchstwahrscheinlich von Suchmaschinen nicht mehr angezeigt, und die treuen Benutzer werden vermutlich für immer abgeschreckt aus Furcht, beim Besuch des Blogs den eigenen Computer zu infizieren.

```
Registration Service Provided By: GLOBEHOSTING EUROPE
Contact: +040.312249495

Domain Name: DOWN[redacted]

Registrant:
    [redacted]
    Botezatu Bogdan          (bogdan.botezatu@[redacted])
    5B Basarabi St.
    Iasi
    [redacted]
    RO
    Tel. +040.[redacted]1233424

Creation Date: 20-Sep-2010
Expiration Date: 20-Sep-2011

Domain servers in listed order:
    ns24.roserve.net
    ns23.roserve.net

Administrative Contact:
    [redacted]
    Botezatu Bogdan          (bogdan.botezatu@[redacted])
    5B Basarabi St.
    Iasi
    [redacted]
    RO
    Tel. +040.[redacted]1233424
```

Die WHOIS-Registrierungsdatenbanken beinhalten Kontaktdaten des Eigentümers der Domain.

Phishing und Vishing

Blogger, die viel über sich selbst schreiben, sollten nicht nur ihre Online-Konten und Zugangsdaten, sondern auch ihre personenbezogenen Daten und Konto- bzw. Kreditkarteninformationen schützen.

Viele Blogger schreiben ausufernd über Themen wie ihre Lieblingsmusik, Filme, Freunde, Hobbies und andere Themen, die auf den ersten Blick harmlos wirken. Über diese Themen zu schreiben oder über Erlebnisse zu bloggen ist sicher sehr einfach. Diese Texte können potenziellen Angreifern jedoch unter Umständen genug Informationen über den Blogger liefern, um einen Phishing- oder Vishing-Angriff (Phishing per Telefon) zu starten.

Um die damit verbundenen Risiken deutlich zu machen, wollen wir ein Beispiel betrachten: Ein Blogger kauft sich ein neues moderneres Smartphone. Es kann PDF-Dokumente anzeigen, hat einen WLAN-Adapter (oder kann zumindest über GPRS eine Verbindung zum Blog herstellen), wodurch der Benutzer auch von unterwegs sein Blog aktualisieren kann. Viele Blogger lassen sich gerne im Detail und mit viel Gusto über ihre coolen neuen Anschaffungen aus. Das folgende Beispiel basiert auf einem tatsächlichen Blog-Eintrag, wurde jedoch abgeändert, um die Identität des Autors zu schützen.

„Ich habe mir gerade ein neues Handy zugelegt, um auch unterwegs über die Dinge bloggen zu können, die mir so passieren. Gestern habe ich mir das neue Smartphone von Marke X in einem Laden des Anbieters Y gekauft. Ihr glaubt nicht, wie cool das Ding ist."

Ein wirksamer Privatsphärenschutz versteckt die personenbezogenen Daten und bieten eine sichere Methode, den Eigentümer einer Website zu kontaktieren.

Jetzt stellen Sie sich vor, dass der obige Beitrag von einem Kriminellen gelesen wird, der den Blogger anruft und sich als Mitarbeiter des Anbieters Y ausgibt. Blogger, die einen eigenen Domainnamen haben, haben meist auch ihre Telefonnummer, ihren Namen, eine Postadresse und eine E-Mail-Adresse in der Datenbank des Domain-Registrars hinterlegt.

„Guten Tag. Hier spricht [Name] von der Firma Y. Ich würde Ihnen gerne ein paar Fragen zu Ihrem neuen Smartphone der Marke X stellen, das Sie gestern in unserer Filiale gekauft haben. Zunächst muss ich Sie jedoch bitten, Ihre Identität zu bestätigen. Bitte nennen Sie mir Ihren Namen, Ihre Adresse und Ihr Geburtsdatum."

Dies ist nur ein Beispiel für die vielen möglichen Szenarien, wie Betrüger an personenbezogene Daten gelangen können. Die Faustregel: Je mehr Sie über sich preisgeben, desto leichter wird es für Kriminelle, andere Informationen zu erraten. Wer etwas über Vorlieben, Hobbies und Tagesablauf eines anderen weiß, kann deutlich leichter Passwörter erraten oder Sicherheitsfragen beantworten, um ein angeblich vergessenes Passwort zugeschickt zu bekommen.

Sicher Bloggen – Tipps wie Sie sich schützen können

Wenn Sie eine Domain auf Ihren Namen registriert haben, gehen Sie beim Kontakt mit Unbekannten stets mit äußerster Vorsicht vor. Wenn Sie in einem Gespräch, in dem Sie nach personenbezogenen Daten gefragt werden, auch nur die geringsten Bedenken haben, ob Ihr Gesprächspartner tatsächlich für die Firma arbeitet, die er angibt, sollten Sie die Informationen nicht herausgeben, sondern sich selbst bei der entsprechenden Firma melden.

Oder Sie bitten Ihren Domain-Name-Registrar, den WHOIS-Privatsphärenschutz für Ihr Konto zu aktivieren, wodurch Ihre Kontaktdaten komplett durch die der Privatsphärenschutzorganisation ersetzt werden. Ihre Daten werden dann gesichert aufbewahrt und nur im Zusammenhang mit staatlichen Ermittlungen preisgegeben.

Blog gehackt. Was tun?

Von den Auswirkungen eines erfolgreichen Hacks des eigenen Blogs erholt man sich nur schwer und langsam; doch je eher Sie die Schwachstellen finden und beheben, desto weniger Schaden kann Ihr Blog nehmen. Hier folgt eine kurze Liste von Sofortmaßnahmen, die nach einem vermuteten Angriff auf das eigene Blog ergriffen werden können.

1. Zunächst sollten Sie Ihr Blog sowohl für menschliche Benutzer als auch für Suchmaschinen-Crawler unerreichbar machen. Da Sie sämtliche Dateien für eine Analyse des Problems und (vermutlich) für die Wiederherstellung des ursprünglichen Zustands benötigen, sollten Sie erst mal keine löschen. Sie können sämtlichen Datenverkehr einfach unterbinden, indem Sie die Datei index.php umbenennen und stattdessen eine leere erstellen. Doch Vorsicht: Die leere Kopie müssen Sie unbedingt erstellen, da Sie sonst Gefahr laufen, andere Dateien auf Ihrem FTP-Konto dem Zugriff freizugeben. Suchmaschinen zu blockieren verhindert, dass diese sehen, dass Ihr Blog infiziert wurde, und es somit als gefährlich kennzeichnen.

2. Erstellen Sie über einen FTP-Client eine vollständige Sicherheitskopie Ihres Start-Ordners, und exportieren Sie dann manuell die Datenbank als SQL-Datei.

3. Entfernen Sie die Zugriffsprotokolle von Ihrem Webserver, und speichern Sie sie an einem sicheren Ort. Sie brauchen die Protokolle für eine spätere Analyse, um nachvollziehen zu können, was genau die Eindringlinge auf Ihrem Blog unternommen haben.

4. Erstellen Sie Kopien von allen benutzerdefinierten Dateien, soweit Sie welche angelegt haben. Benutzerdefinierte Dateien können Themes, Plug-ins oder als Inhalt hochgeladene Dateien sein – also im Prinzip alles, was nicht über das Internet heruntergeladen werden kann. Speichern Sie einfach alles, von dem Sie glauben, dass Sie es für einen Neustart Ihres Blogs brauchen können.

5. Untersuchen Sie jedes Plug-in und Theme auf verdächtig wirkende Textstücke. Achten Sie dabei besonders auf Zeilen wie „eval(base64_decode(“ gefolgt von einer Reihe willkürlich wirkender Zahlen und Buchstaben und auf Skript-Einbettungen von Domains, die Ihnen unbekannt sind wie z. B. <script src="http://[unbekannterDomain-Name]/scriptname.php">.

6. Gehen Sie die Datenbank Tabelle für Tabelle durch und suchen Sie nach verdächtigen Links. Durchsuchen Sie mit besonderer Sorgfalt die Tabellen mit den Administratoren, den Konfigurationseinstellungen und den Blog-Artikeln. Wenn Sie einen Administrator finden, der Ihnen unbekannt vorkommt, löschen Sie ihn umgehend.

7. Nach der Überprüfung und Säuberung sollten Sie alle Dateien vom Webserver löschen. Wenn die Datenbank ebenfalls infiziert war, sollten Sie sie löschen und manuell die Kopie der Datenbank wiederherstellen, die Sie selbst überprüft haben.

8. Laden Sie Ihr Blog-Skript wieder auf den Server. Vergewissern Sie sich, dass Sie es von einer offiziellen Quelle heruntergeladen haben. Auf jeden Fall sollten Sie die aktuellste Version des Blog-Skripts herunterladen. Ändern Sie die Config-Datei dahingehend, dass sie auf Ihren Webserver passt (SQL-Benutzer, Datenbank, Passwort, Dateipfad und weitere Einstellungen).

9. Die Datei- und Ordnerberechtigungen sollten nicht höher eingestellt sein, als es zur reibungslosen Ausführung des Skripts absolut notwendig ist. Die Einstellung CHMOD 777 für Dateien und Ordner kann ein Eindringling z. B. dazu ausnutzen, bösartigen Code einzuschleusen. Legen Sie neue Passwörter für Administratoren und für den FTP-Zugang fest.

10. Legen Sie alle Dateien über FTP wieder an Ihre Ursprungsorte. Löschen Sie den Browser-Cache, und rufen Sie Ihre Website im Browser auf. Suchen Sie auch über eine Suchmaschine mit Ihrem Namen oder dem Namen des Blogs als Suchwörter nach Ihrem Blog, und sehen Sie sich die Treffer genau an. Meistens liest Blog-Malware den Referrer aus, um zu sehen, ob der Besucher direkt auf die Website zugegriffen hat oder ob er über eine Suchmaschine dorthin gelangt ist, und wird nur im letzteren Fall aktiv.

Tipps zum sicher Bloggen

Sie können das Risiko eines Hackerangriffs auf Ihr Blog minimieren, indem Sie ein paar ganz einfache Sicherheitsmaßnahmen ergreifen und Tipps zum sicheren Bloggen umsetzen:

• Verwenden Sie niemals Blog-Skripte, die aus dubiosen oder inoffiziellen Download-Quellen stammen. Und verwenden Sie auf keinen Fall sogenannte genullte Skripte, da sie nicht nur gesetzeswidrig, sondern auch riskant für Ihr Blog und Ihren Webserver sind.

- Halten Sie Ihr FTP-Konto übersichtlich: Speichern Sie unter dem Konto, auf dem Sie Ihr Blog betreiben, keine anderen Skripte, die Sie nur testen möchten. Die kleinste Sicherheitslücke in einem Drittanbieter-Skript kann verheerende Folgen für Ihr Blog haben. Testen Sie neue Skripte immer auf einem lokal installierten Webserver.

- Nutzen Sie in Ihrem Blog nur so viele Plug-ins und Themes wie nötig. So minimieren Sie das Risiko, ein angreifbares Plug-in oder Theme zu installieren. Und vergewissern Sie sich stets, dass alle Plug-ins, die Sie einsetzen möchten, aus vertrauenswürdigen Quellen stammen; fragen Sie im Zweifel die Blogger-Gemeinde.

- Legen Sie in regelmäßigen Abständen Sicherheitskopien Ihrer SQL-Datenbanken an. Über ein Plug-in können Sie diesen Vorgang automatisieren und sich die Kopien per E-Mail oder über ein separates FTP-Konto zuschicken lassen. Sicherheitskopien unter demselben Konto wie das Original zu speichern, ist keine gute Idee, da Sie im Falle eines Angriffs auf Ihr Blog ebenfalls Schaden nehmen oder gar gelöscht werden können.

- Verwenden Sie sichere Passwörter für Ihr FTP-Konto und für Administratorenzugänge. Verraten Sie diese Passwörter niemals irgendjemandem. Sie können auch eine Rundum-Malwareschutzlösung installieren, die Ihr Blog garantiert frei von Trojanern hält. Eine Reihe von erfolgreichen Blog-Hacks wurden über bestehende Benutzernamen und Passwörter durchgeführt, die mit Hilfe von Keyloggern oder Trojanern abgegriffen wurden.

- Besonders wichtig beim Bloggen für Anfänger: Seien Sie besonders sorgfältig bei der Auswahl Ihres Hosting-Anbieters. Kostenpflichtiges Hosting ist normalerweise deutlich besser als kostenlose Angebote; achten Sie darauf, dass in Ihrem Hosting-Paket automatische tägliche Backups, Zugriffsstatistiken und eine solide Webserver-Konfiguration enthalten sind.

bitdefender