E-Mails autorisieren: So verhindern Sie, dass WordPress-E-Mails im Spam landen

Sie möchten E-Mails direkt über WordPress an eine große Empfängerzahl schicken? Dann sollten Sie diesen Beitrag unbedingt lesen – denn die Gefahr ist groß, dass Ihre Nachrichten im Spam landen!

Inhalt

Das Problem

Eines direkt vorweg: In diesem Beitrag geht’s ans Eingemachte. Wenn Sie gerade kurz angebunden sind, sollten Sie definitiv wann anders wiederkommen. Es wird technisch, komplex und viel. Wir gehen nämlich der Frage auf den Grund, wie man verhindern

kann, dass E-Mails, die direkt über WordPress verschickt werden (z. B. Newsletter), im Spam landen.

Das passiert unglücklicherweise recht häufig, sobald eine kritische Empfängerzahl erreicht ist. Hält sich diese in überschaubaren Grenzen und werden nur vereinzelnd E-Mails verschickt (z. B. bei der Benachrichtigung über einen Kommentar), gibt es in der Regel keine Schwierigkeiten.

Da Sie das hier gerade lesen, haben Sie aber wahrscheinlich genau das Problem – tauchen wir also ein in die Welt des WordPress-E-Mail-Versands!

E-Mails über WordPress verschicken

Es gibt etliche Plug-ins, die das Verschicken von E-Mails über WordPress ermöglichen. Dafür wird typischerweise der Webserver Ihrer CMS-Installation genutzt – und nicht, wie wir später noch ausführlich betrachten, der Mailserver. Technisch gesehen kommt dabei das Script „*PHP mail()*“ zum Einsatz.

Der Vorteil: Die Nutzer werden nicht damit belastet, sich über die Funktionsweise im Hintergrund Gedanken machen oder technische Einstellungen vornehmen zu müssen. Leider ist genau das jedoch notwendig, um das Spam-Problem zu lösen. Bei großen Mengen stößt der Webserver einfach an seine Grenzen.

Das hat vor allem drei Ursachen:

- Viele Shared-Webhoster limitieren die Anzahl der E-Mails, die per PHP-Script verschickt werden können – oder die Funktion ist gänzlich deaktiviert.
- Webserver verfügen häufig nicht über die notwendige Konfiguration sowie die erforderlichen Zertifikate, um als vertrauenswürdig eingestuft zu werden.
- In manchen Fällen wird vom Empfänger – u. a. aus Gründen des Spam-Schutzes – per Einstellung verlangt, dass E-Mails nicht sofort zugestellt, sondern zu einem späteren

Zeitpunkt noch mal verschickt werden, wozu viele Webserver nicht in der Lage sind.

Webserver vs. Mailserver

Auch wenn Sie Ihre Domain und Ihr E-Mail-Postfach vom selben Anbieter haben, hat der Webserver erst mal nichts mit Ihrer E-Mail-Adresse zu tun. Es kann also sein, dass eine E-Mail mit dem Absender info@ihre-domain.de, die vom Webserver verschickt wird, beim Empfänger als Spam angesehen wird, da sie nicht von Ihrem offiziellen Mailserver stammt.

Dieser ist für nichts anderes da, als sich um das Verschicken, Entgegennehmen, Weiterleiten und Bereithalten Ihrer E-Mails zu kümmern. Er wird auch SMTP-Server genannt, wobei „SMTP“ für „Simple Mail Transfer Protocol“ steht und das Standard-Netzwerkprotokoll des Internets zum Übermitteln von E-Mails darstellt.

Sie ahnen es wahrscheinlich bereits: Die erste Maßnahme, um das Spam-Problem zu lösen, sollte sein, dafür zu sorgen, dass E-Mails aus WordPress heraus mittels Mailserver verschickt werden. Dazu benötigen Sie bestimmte Zugangsdaten, die Sie von Ihrem Webspace-Anbieter erhalten:

- SMTP-Host: Domain oder IP-Adresse zu Ihrem Mailserver
- Port zum Mailserver: das „Tor“ zur richtigen Anwendung auf dem Server (Standard: Port 587)
- Art der Verschlüsselung: meistens SSL/TLS
- SMTP-Benutzername
- SMTP-Passwort

Wohin nun mit diesen Daten? Natürlich, in ein Plug-in!

Nutzen Sie bereits ein modernes Plug-in für den Versand von Newslettern (z. B. Mailster), finden Sie dort die Möglichkeit,

die entsprechenden Einstellungen vorzunehmen.

Für den reinen Versand von WordPress-E-Mails empfehlen wir Easy WP SMTP, auch wenn es nur das zweitbeliebteste Plug-in im WordPress-Verzeichnis nach WP Mail SMTP von WPForms ist. Easy WP SMTP ist sehr übersichtlich und beschränkt sich aufs Wesentliche. Außerdem ist hier alles gut ins Deutsche übersetzt.

Nach der Installation sowie Aktivierung gelangen Sie über *„Einstellungen“ –> „Easy WP SMTP“* zu den Einstellungsmöglichkeiten. Die Zugangsdaten vom Mailserver können Sie direkt unter dem ersten Reiter eintragen. Den zweiten Reiter („Weitere Einstellungen“) können Sie ignorieren, sofern Sie kein Entwickler sind. Sind Sie einer, wissen Sie, was zu tun ist.

Testen Sie den E-Mail-Versand über Ihren SMTP-Server
Der letzte Reiter ist wiederum für alle relevant. Hier haben Sie die Möglichkeit, eine Test-E-Mail zu verschicken, was Sie unbedingt tun sollten. Ist der Test erfolgreich, haben Sie einen wichtigen Schritt getan, um sicherzustellen, dass E-Mails, die in Verbindung mit Ihrer Domain stehen, fortan nicht mehr als Spam klassifiziert werden.

Einstellungen SMTP-Server anhand des Beispiels Easy WP SMTP
Sie können aber noch mehr tun!

Bounce-Mails vermeiden

Je älter Ihre Empfängerliste, desto mehr E-Mail-Adressen existieren bereits nicht mehr. Kann ein Newsletter nicht mehr zugestellt werden, erhält Ihr Mailserver eine Benachrichtigung darüber, dass das anvisierte Postfach verschwunden oder voll ist.

Solche sogenannten Bounce-Mails („bounce“ = „abprallen“) darf man auf keinen Fall ignorieren! Senden Sie weiterhin Newsletter an die entsprechenden E-Mail-Adressen, wird das beim Anbieter des Empfängers (z. B. Gmail) negativ registriert und die Wahrscheinlichkeit, dass Sie als Spammer eingestuft und damit alle Ihre Nachrichten blockiert werden, steigt.

Daher sollten Sie Ihre Empfängerliste stets aufräumen, sobald Sie eine Bounce-Mail erhalten.

E-Mails autorisieren

Eines der größten Probleme im Zusammenhang mit dem E-Mail-Versand sind Kriminelle, die E-Mails im Namen anderer verschicken. Heutzutage sind fast alle missbräuchlichen E-Mail-Nachrichten mit gefälschten Absenderadressen versehen.

Werden Sie Opfer, führt das nicht selten zu Vertrauensverlust und E-Mails mit Ihrer Domain-Adresse landen im Spam-Ordner oder werden komplett abgelehnt.

Um dieses Problem zu begrenzen, kann man dem Empfänger mitteilen, wer zum Versand berechtigt ist. Der Mailserver des Empfängers kann dann beim Mailserver des Senders nachfragen, welche Server zum Versand von E-Mails einer bestimmten Domain autorisiert sind.

Diese Vorgehensweise verhindert zwar nicht direkt einen Identitätsklau, macht Ihre E-Mail-Adresse für Cyberkriminelle jedoch uninteressanter. Deshalb ist es absolut sinnvoll, dass Sie die entsprechenden Einstellungen vornehmen und Ihre E-Mails autorisieren.

Zugegeben, jetzt wird’s sehr technisch! Die grundsätzliche Voraussetzung für die folgenden Maßnahmen ist, dass Ihr Hoster Ihnen die Bearbeitung der DNS-Einträge gestattet – und Sie sich bestenfalls ein bisschen mit dem Thema auskennen, um keinen Schaden anzurichten. Falls das nicht der Fall ist,

geben Sie die Aufgabe besser in vertrauensvolle Hände.

Sender Policy Framework (SPF)

SPF (Sender Policy Framework) ist ein Verfahren zur Identitätsprüfung des Absenders einer E-Mail. Um daran teilnehmen zu können, müssen Sie die Informationen darüber, welche Mailserver senden dürfen, in den DNS-Einträgen Ihrer Domain hinterlegen.

Es gilt, den DNS-Eintrag vom Typ TXT oder – falls vorhanden – SPF zu konfigurieren. Und zwar nur diesen einen – er wird entweder erweitert oder gekürzt, Sie können nicht mehrere SPF-Records anlegen.

Der Eintrag startet immer mit der Angabe der SPF-Version, die genutzt wird:

v=spf1

Es folgen sogenannte „Mechanismen“, die angeben, welche Server zum Versenden von E-Mails mit einer bestimmten Domain berechtigt sind. Dies geschieht wiederum mithilfe von „Ergebnissen“.

Die wichtigsten Mechanismen:

- a = berechtigt den Server, der als A-Record für die Domain hinterlegt ist
- mx = berechtigt den Server, der als MX-Record hinterlegt ist
- ip4 = berechtigt das IPv4-Netz zur darauffolgenden Adresse (Beispiel: ip4:188.94.26.162)
- ip6 = berechtigt das IPv6-Netz zur darauffolgenden Adresse (Beispiel: ip6:2101:688:4:74::2)
- include = berechtigt zur Übernahme der SPF-Einstellungen der darauffolgenden externen Domain (Beispiel: include:mailchimp.com)

- all = definiert, was in allen anderen Fällen passieren soll (muss immer am Ende stehen)

Die wichtigsten Ergebnisse:

- + = Absender ist autorisiert
- – = Absender ist nicht autorisiert (Hard Fail)
- ~ = Absender ist nicht autorisiert, E-Mail darf aber durchgelassen werden (Soft Fail)

Wird nichts angegeben, wird automatisch von einem „+“ ausgegangen. Eine Übersicht aller Parameter gibt es hier: SPF Record Syntax

Beispiel: ***v=spf1 a mx ip4:188.94.26.162 ip6:2101:688:4:74::2 include:mailchimp.com ~all***

Achtung: Die eigene Domain darf im SPF-Record nicht auftauchen, sonst wird dieser ungültig!

Unterstützung bei der Erstellung des für Sie richtigen Eintrags erhalten Sie in der Regel auch bei Ihrem Webhoster. Im Netz gibt es darüber hinaus einen SPF-Generator.

Wenn Sie nun vor Interesse brennen und noch tiefer in die Thematik einsteigen möchten, können Sie sich u. a. folgenden Beitrag anschauen: „Häufige Fehler beim Erstellen eines SPF-Datensatzes“

Oder Sie lesen erst mal hier weiter, denn wir sind – es tut uns leid – noch immer nicht am Ende der Möglichkeiten angelangt.

DomainKeys Identified Mail (DKIM)

Puh, noch so ein kryptischer Name! Hinter DKIM (DomainKeys Identified Mail) verbirgt sich ebenfalls ein Identifikationsprotokoll zur Sicherstellung der Authentizität

von E-Mail-Absendern. Es funktioniert nach einem ähnlichen, aber doch anderen Prinzip als SPF.

Auch das DKIM-Verfahren basiert auf der Kommunikation zwischen dem sendenden und empfangenden Mailserver, wobei der sendende Server den E-Mails eine digitale Signatur hinzufügt, die vom empfangenden Server überprüft werden kann. Dabei wird ein zur Signatur passender öffentlicher Schlüssel abgerufen. Gibt es keine Übereinstimmung, werden die entsprechenden E-Mails blockiert.

Das ist zugegebenermaßen eine sehr vereinfachte Darstellung des Funktionsprinzips, aber wir möchten schnell zur Sache kommen und Sie nicht mit technischen Spezifikationen überfrachten. Wie also wird DKIM eingerichtet?

Zunächst müssen Sie ein Schlüsselpaar generieren, was Sie u. a. mithilfe des DKIM Record Generator von EasyDMARC tun können. Dieser erzeugt einen privaten und einen öffentlichen Schlüssel.

Der private Schlüssel muss auf dem Mailserver hinterlegt werden, was häufig nur Ihr Webhoster erledigen kann. Leider gibt es allerdings beim Erscheinen des Beitrags noch einige Hoster, wie zum Beispiel HostEurope, die noch kein DKIM unterstützen.

Der öffentliche Schlüssel wird – wie der SPF-Record – per DNS-Eintrag (TXT) hinzugefügt. Damit kennen Sie sich ja nun bereits bestens aus!

Erledigt? Gut, denn einen haben wir noch.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

In Sachen Bezeichnung schießt DMARC (Domain-based Message Authentication, Reporting and Conformance) schon mal den Vogel ab. Doch was bewirkt diese Spezifikation?

Während die beiden vorab genannten Verfahren beschreiben, wer eine E-Mail versenden darf (SPF) bzw. dass eine E-Mail unverändert vom angegebenen Absender stammt (DKIM), können via DMARC zusätzliche Empfehlungen über die Art und Weise des Umgangs mit einer E-Mail abgegeben werden, die nicht den SPF- und DKIM-Regeln entsprechen (z. B. in Quarantäne schieben oder als Spam markieren). DMARC baut demnach auf SPF sowie DKIM auf und steht nicht für sich allein.

Auch das DMARC-Verfahren wird mithilfe eines TXT-Eintrags in der DNS-Zone Ihrer Domain integriert. Wie der Code aussehen kann und welche Parameter Ihnen für die gewünschten Einstellungen zur Verfügung stehen, hat u. a. Google gut zusammengefasst: „DMARC-Eintrag hinzufügen“

Haben Sie DMARC erfolgreich eingerichtet, erhalten Sie beispielsweise Berichte darüber, welche Server oder Dritte von Ihrer Domain aus E-Mails verschicken, ob diese die Authentifizierung bestanden und wie die jeweiligen Eingangsserver auf nicht authentifizierte Nachrichten reagiert haben. Wertvolles Wissen, um möglichen Spam-Problemen auf den Grund gehen und angemessene Maßnahmen ergreifen zu können!

Kann ich DMARC ohne DKIM einrichten?

Ja, Sie können DMARC ohne DKIM einrichten und nur DMARC und SPF nutzen. In diesem Fall schlägt die DKIM-Prüfung immer fehl und das DMARC-Authentifizierungsergebnis hängt von der SPF-Prüfung und dem SPF-Kennungsabgleich ab, was zwar funktioniert, aber nicht optimal ist.

Eine E-Mail besteht die DMARC-Authentifizierung, wenn SPF-Authentifizierung oder die DKIM-Authentifizierung bestanden ist. Gibt es keine DMARC-Authentifizierung hängt also alles an SPF. Funktioniert SPF nicht, dann gibt es ein Problem.

Bei einem Eigentest gab es bei einer automatischen Weiterleitung ein Problem: Vermutlich wurde bei der

Weiterleitung die SMTP-From-Adresse (MAILFROM) verändert, so dass die deren Domain nicht mehr gleicht der Header-From-Domain (elbnetz.com) ist. Das diese beiden übereinstimmen ist aber ein Erfordernis der DMARC-Prüfung.

Das Probleme wäre nicht so schlimm, wenn noch eine gültige DKIM-Signatur (von elbnetz.com) in der Mail wäre. Dann würde die DMARC-Prüfung trotzdem positiv enden. Für diese Weiterleitungsfälle sollte man also eine DKIM-Signatur mitsenden. Geht bei uns leider nicht; wir nutzen einen E-Mail-Server bei HostEurope und die können DKIM nicht.

Da aber die meisten E-Mail-Dienste die Möglichkeit bieten, sowohl SPF als auch DKIM einzurichten, sollten Sie auf jeden Fall DKIM neben SPF einrichten.

Fazit

Zunächst einmal großen Respekt: Sie haben es geschafft, diesen Beitrag durchzulesen!

Wenn Sie die darin vorgestellten Möglichkeiten umsetzen, haben Sie gute Chancen, Herr Ihrer Spam-Probleme zu werden. Lassen Sie sich von der Menge des Inputs nicht erschlagen und gehen Sie Schritt für Schritt vor – die Angelegenheit ist zu wichtig, um sie nicht in Angriff zu nehmen.

Und: Testen Sie unbedingt Ihre Konfigurationen. Eine gute Anlaufstelle dafür ist EasyDMARC Domain Scanner.

Wie bereits erwähnt: Sollten Sie Bedenken haben, dass Sie es selbst schaffen, wenden Sie sich am besten an einen Experten (z. B. uns).

Viel Erfolg!
Ihre WordPress Agentur

+

FAQ’s zum Thema Autorisierung von E-Mails

+

Warum E-Mails Autorisieren

Eines der größten Probleme im Zusammenhang mit dem E-Mail-Versand sind Kriminelle, die E-Mails im Namen anderer verschicken. Heutzutage sind fast alle missbräuchlichen E-Mail-Nachrichten mit gefälschten Absenderadressen versehen. Um dieses Problem zu begrenzen, kann man dem Empfänger mitteilen, wer zum Versand berechtigt ist. Der Mailserver des Empfängers kann dann beim Mailserver des Senders nachfragen, welche Server zum Versand von E-Mails einer bestimmten Domain autorisiert sind.

+

Was ist DKIM?

Das DKIM-Verfahren (DomainKeys Identified Mail) basiert auf der Kommunikation zwischen dem sendenden und empfangenden Mailserver, wobei der sendende Server den E-Mails eine digitale Signatur hinzufügt, die vom empfangenden Server überprüft werden kann. Dabei wird ein zur Signatur passender öffentlicher Schlüssel abgerufen. Gibt es keine Übereinstimmung, werden die entsprechenden E-Mails blockiert. Erfahren Sie mehr hier.

+

Was ist SPF?

SPF (Sender Policy Framework) ist ein Verfahren zur Identitätsprüfung des Absenders einer E-Mail. Um daran

teilnehmen zu können, müssen Sie die Informationen darüber, welche Mailserver senden dürfen, in den DNS-Einträgen Ihrer Domain hinterlegen. Erfahren Sie mehr hier.

+

Was ist DMARC?

DMARC (Domain-based Message Authentication, Reporting and Conformance) bietet zusätzliche Empfehlungen über die Art und Weise des Umgangs mit einer E-Mail, die nicht den SPF- und DKIM-Regeln entsprechen (z. B. in Quarantäne schieben oder als Spam markieren). DMARC baut demnach auf SPF sowie DKIM auf und steht nicht für sich allein. Erfahren Sie mehr hier.

+

Kann ich DMARC ohne DKIM einrichten?

Ja. DKIM ist für DMARC nicht erforderlich. Durch die Einrichtung von DKIM werden jedoch falsch negative Ergebnisse bei der DMARC-Authentifizierung auf ein Minimum reduziert. Erfahren Sie mehr hier.
