WP Mail SMTP als Spam Schleuder? How to fix it.

Warum Ihre WordPress-E-Mails im Spam landen (+ So beheben Sie das Problem)

Sie fragen sich, wie Sie verhindern können, dass WordPress-E-Mails im Spam landen? Befolgen Sie einfach diese Schritte:

In diesem Artikel

Schauen wir uns zunächst einige häufig auftretende Probleme genauer an.

1. Fehlerbehebung bei WordPress-E-Mails, die im Spam landen

Wenn Sie sich fragen, warum die E-Mails Ihrer Website im Spam landen (oder verschwinden), führen Sie zunächst die folgenden Schritte zur Fehlerbehebung durch.

Befindet sich Ihr Server auf einer Spam-Blacklist?

Wenn Ihr Server auf der schwarzen Liste steht, bedeutet das, dass er in der Vergangenheit wegen Spam markiert wurde. Das bedeutet, dass Ihre E-Mails nicht vertrauenswürdig sind.

Dies ist ein häufiges Problem beim Shared Hosting. Wenn nur ein Kunde wegen Spam auf die schwarze Liste gesetzt wird, haben alle anderen Kunden auf demselben Server Probleme beim Senden von E-Mails.

Dies kann auch passieren, wenn Ihre Website mit Malware infiziert ist oder ein Hacker Ihren Server als E-Mail-Relay nutzt.

So erkennen Sie, ob Ihre E-Mails im Spam landen

Wenn Sie überprüfen möchten, ob Ihre E-Mails im Spam landen, können Sie prüfen, ob Sie auf einer Spam-Blacklist stehen.

Testen Sie dazu die IP-Adresse Ihres Servers mit dem Blacklists-Checker von MXToolbox . Klicken Sie einfach auf **„Blacklist Check“** , um über 100 Blacklists gleichzeitig zu scannen.

Wenn Sie feststellen, dass Sie auf einer schwarzen Liste

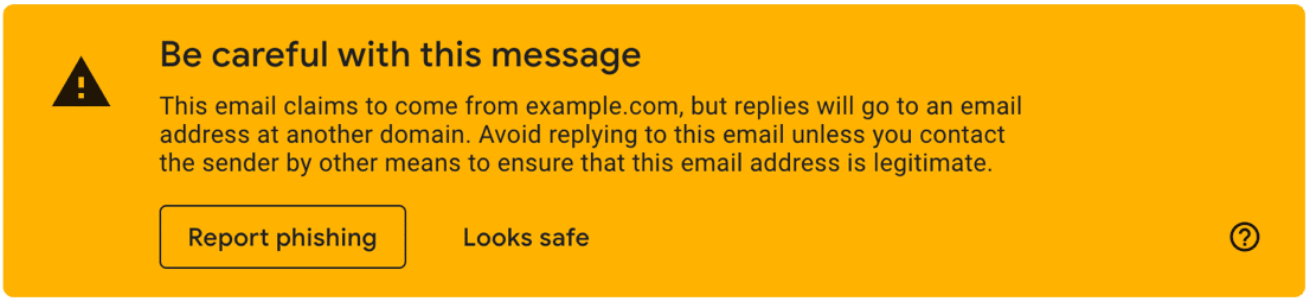
stehen, wenden Sie sich an Ihren Host und bitten Sie ihn, Sie auf einen anderen Server zu verschieben.

Werden einige WordPress-E-Mails im Spam landen, andere jedoch nicht?

Manchmal werden Sie feststellen, dass E-Mails für einen Empfänger im Spam landen, andere sie jedoch problemlos empfangen können.

Dies kommt sehr häufig bei Empfängern vor, die AOL, Yahoo oder Gmail verwenden. Diese Anbieter neigen dazu, deutlich strengere Spam-Prüfungen durchzuführen. Yahoo kann beispielsweise jede E-Mail von einer Domain ohne DMARC-Eintrag ablehnen.

Gmail zeigt möglicherweise auch die Warnung „ Seien Sie vorsichtig mit dieser Nachricht an “ an, wenn in Ihren E-Mail-Headern etwas Ungewöhnliches festgestellt wird.



Normalerweise können Sie dieses Problem beheben, indem Sie Ihre DNS-Einträge überprüfen , worauf wir später im Tutorial eingehen.

Wenn jedoch nur eine Person Ihre E-Mails nicht erhält, sollten Sie auch überprüfen, ob diese Ihre vorherigen E-Mails nicht als Spam markiert hat. In diesem Fall sollten Sie sich an Ihren E-Mail-Dienstanbieter wenden und fragen, ob Sie diese Person aus der Unterdrückungsliste entfernen können.

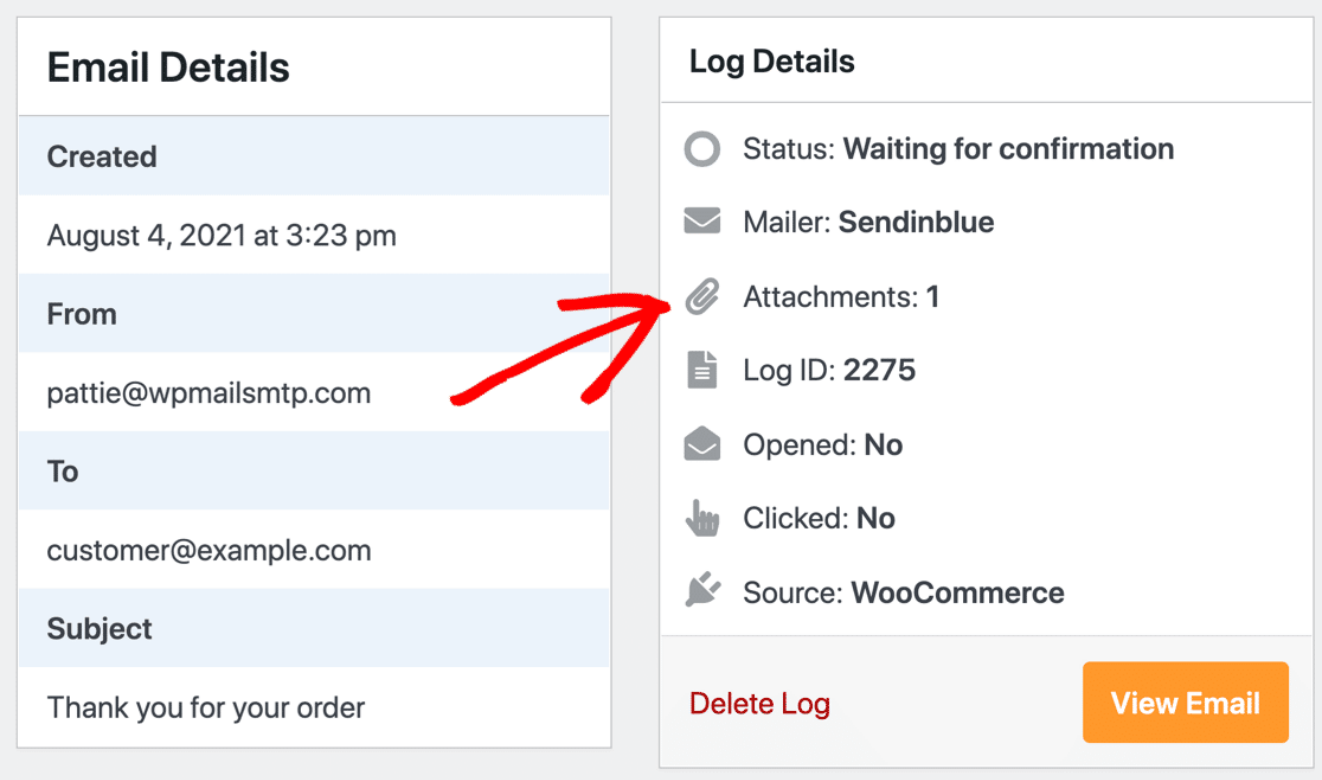
Senden Sie Bilder oder Anhänge?

Jede E-Mail, die Sie senden, hat einen Spam-Score, und das

Einfügen von Bildern oder Anhängen erhöht diesen Score.

Obwohl Sie in WordPress E-Mails mit Anhängen versenden können , spielt die Größe der Anhänge eine Rolle. Mehrere Anhänge können dazu führen, dass Ihr E-Mail-Inhalt noch mehr als Spam aussieht.

Sie sind sich nicht sicher, ob das auf Sie zutrifft? Wenn Sie bereits über WP Mail SMTP Pro verfügen , wird die Anzahl der Anhänge im E-Mail-Protokoll angezeigt.



Darüber hinaus können große Bilder oder Anhänge dazu führen, dass E-Mails aufgrund der vom Postfach des Absenders oder Empfängers festgelegten Sendebeschränkungen fehlschlagen. Mit WP Mail SMTP können Sie gesendete Anhänge speichern, um den Verlust wichtiger Dateien zu vermeiden.

Verwenden Sie eine ungewöhnliche TLD?

Spam-Scores werden anhand einer Reihe von Faktoren berechnet, und die Top-Level-Domain (TLD) kann einer davon sein.

Die Top-Level-Domain ist der Teil der Domain nach dem letzten Punkt.

Laut Spamhaus gehören zu den am häufigsten von Spammern missbrauchten TLDs: .work, .shop, Und .biz. (Dies sind alles gTLDs, was bedeutet, dass sie nicht zu einem bestimmten geografischen Standort gehören.)

Durch die Verwendung einer nicht-traditionellen gTLD werden Sie nicht unbedingt als Spammer eingestuft. Wenn Ihre E-Mails jedoch bereits Spamfilter auslösen und den Spam-Score Ihrer E-Mails erhöhen, kann der Besitz einer dieser gTLDs dazu führen, dass Sie einen höheren Spam-Score erreichen.

Dies ist einer der Gründe, warum WPBeginner die Verwendung einer traditionellen TLD wie empfiehlt .combei der Auswahl des besten Domainnamens .

Ist Ihre E-Mail-Liste veraltet?

Ein weiterer Grund, der Ihren Spam-Score erhöhen und die Reputation Ihrer Domain beeinträchtigen kann, ist eine veraltete E-Mail-Liste.

Die E-Mail-Adressen in Ihrer E-Mail-Liste werden möglicherweise nicht mehr von Ihren Abonnenten verwendet. Oder einige Personen auf Ihrer Liste möchten möglicherweise einfach keine E-Mails mehr von Ihnen erhalten.

Wie dem auch sei: Wenn Ihre E-Mails ständig von Personen auf Ihrer Liste ungeöffnet bleiben, besteht die Gefahr, dass Sie als Spam gekennzeichnet werden.

Es ist eine gute Idee, Ihren Abonnenten hin und wieder eine Check-in-E-Mail zu senden. Auf diese Weise können Sie bestätigen, ob sie weiterhin an Ihrem Newsletter interessiert sind und ob ihre E-Mail-Adressen aktiv sind.

Anschließend können Sie inaktive Abonnenten entfernen und Ihre E-Mail-Liste bereinigen, um eine hohe Domänenreputation aufrechtzuerhalten und zu vermeiden, als Spam markiert zu werden.

Stellen Sie außerdem sicher, dass Ihre Abonnenten jederzeit eine einfache Möglichkeit haben, sich von Ihrem Newsletter abzumelden. Sie können beispielsweise einfach am Ende Ihrer E-Mail einen Abmeldelink hinzufügen.

WordPress-E-Mails landen immer noch im Spam?

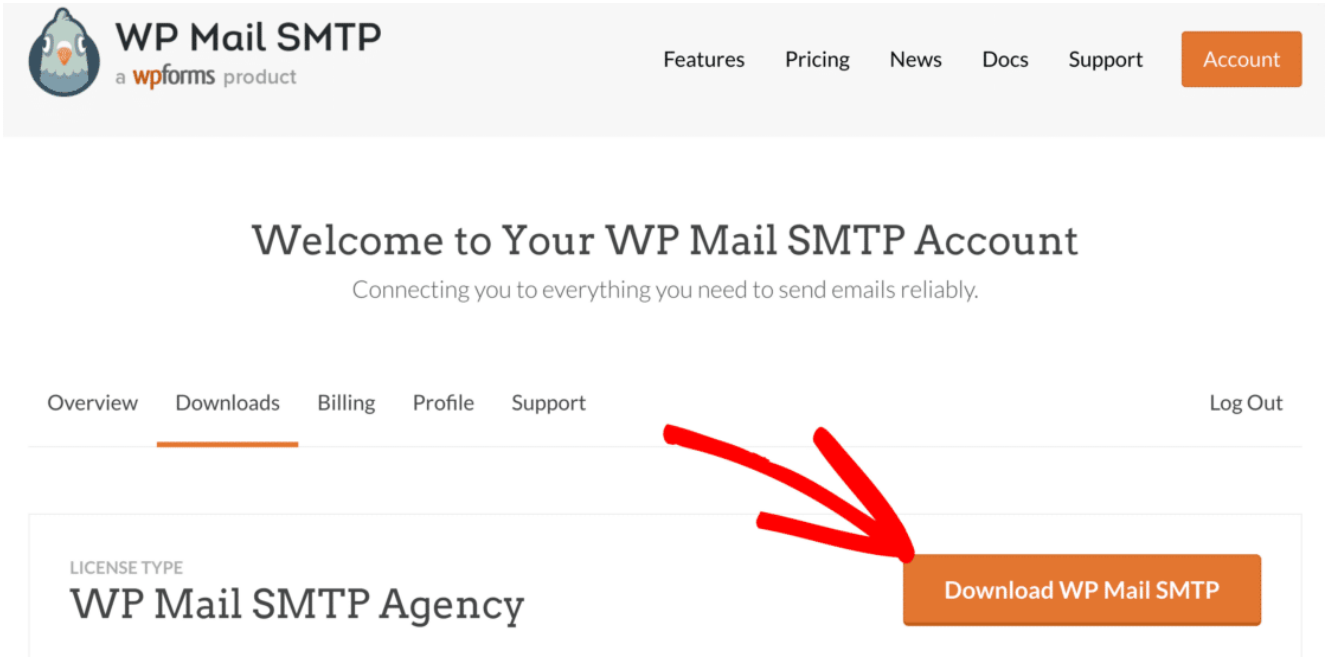
Wenn keines dieser Probleme auf Sie zutrifft, liegt das Problem wahrscheinlich einfach an der fehlenden Authentifizierung. Wir können das mit WP Mail SMTP beheben. Diese Lösung funktioniert für alle auf Ihrer Website installierten Plugins, die E-Mails versenden.

Unabhängig davon, ob WooCommerce-E-Mails im Spam landen oder ein anderes WordPress-Plugin, sollte WP Mail SMTP dabei helfen, Ihre Zustellbarkeitsprobleme ein für alle Mal zu beheben.

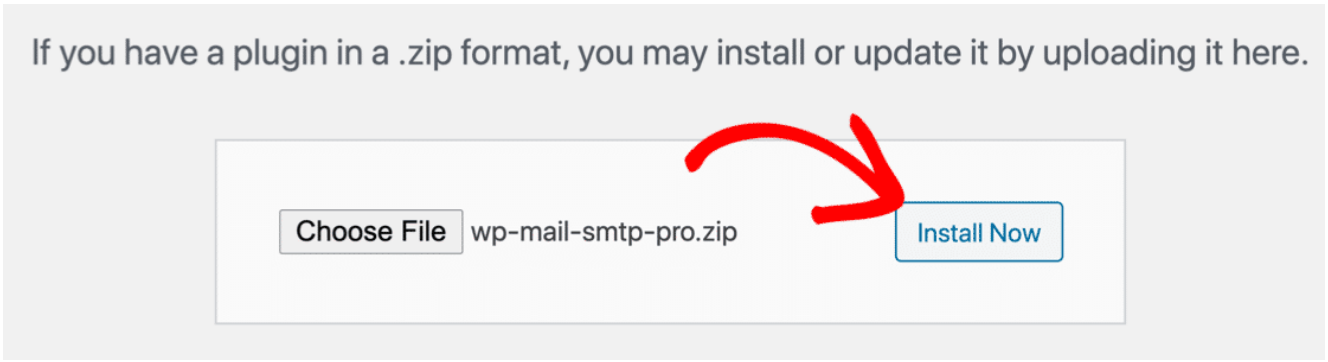
2. Installieren Sie das WP Mail SMTP-Plugin

WP Mail SMTP ist das beste SMTP-Plugin für WordPress. Es unterstützt kostenlose und Premium-E-Mail-Anbieter, die Ihre WordPress-E-Mail-Probleme lösen.

Um das Plugin herunterzuladen, gehen Sie zur WP Mail SMTP-Website und melden Sie sich bei Ihrem Konto an. Wechseln Sie zur **Registerkarte „Downloads“** , um die neueste Version der Plugin-Datei herunterzuladen.



Gehen Sie zu Ihrer Website und melden Sie sich beim WordPress-Dashboard an. Navigieren Sie nun zur Plugins-Seite und laden Sie die ZIP-Datei hoch, die Sie gerade heruntergeladen haben, um sie zu installieren.



Sobald das Plugin installiert ist, müssen Sie es unbedingt aktivieren. Sobald Sie dies tun, wird der Setup-Assistent des Plugins in Ihrem Browser gestartet.

Es ist wichtig, den gesamten Setup-Assistenten abzuschließen, um das Problem zu beheben. Denken Sie daran: Wenn Sie das Plugin installieren und es nicht einrichten, hat es keine Auswirkungen.

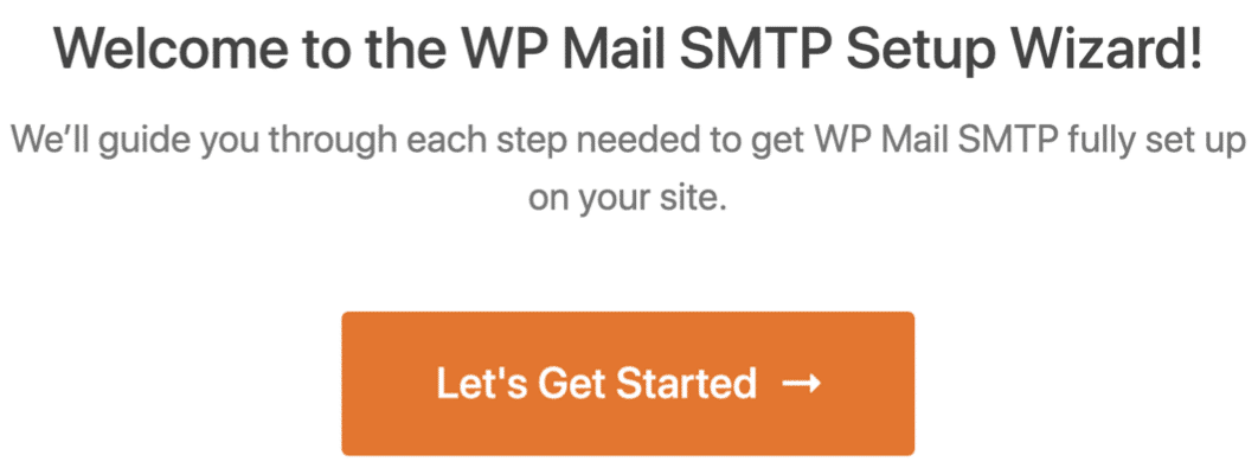
Brauche Hilfe?

Unsere Elite-Lizenz beinhaltet das White Glove Setup für WP Mail SMTP.

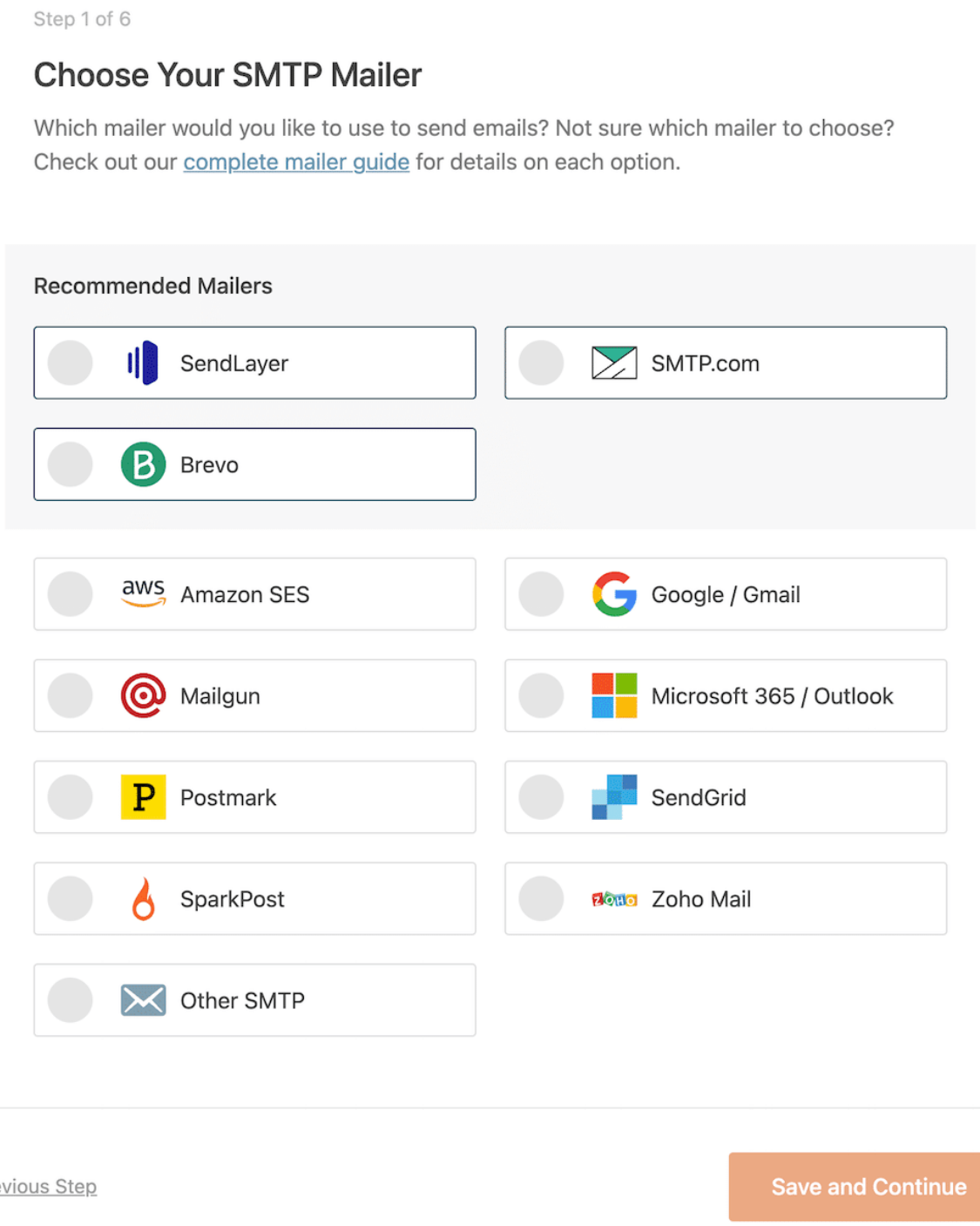
3. Wählen Sie einen E-Mail-Anbieter für WordPress

In diesem Schritt wählen wir den E-Mail-Anbieter aus, der Ihre WordPress-E-Mails zustellt.

Klicken Sie im ersten Bildschirm des Assistenten auf die **Schaltfläche „Los geht's“** , um zu beginnen.



WP Mail SMTP zeigt eine Liste der unterstützten Mailer-Dienste an.



Jeder dieser E-Mail-Anbieter hilft dabei, zu verhindern, dass Ihre WordPress-E-Mails im Spam landen. Sie haben jedoch alle unterschiedliche Sendelimits und Zulagen für Anhänge.

Darüber hinaus sind einige einfacher einzurichten als andere.

Wenn Sie einen zuverlässigen, professionellen und erschwinglichen Service wünschen, empfehlen wir SendLayer , SMTP.com oder Brevo (ehemals Sendinblue). Hierbei handelt es sich um Transaktions-E-Mail-Anbieter , das heißt, sie sind für

die Verarbeitung einer großen Anzahl automatisierter Benachrichtigungs-E-Mails ausgelegt.

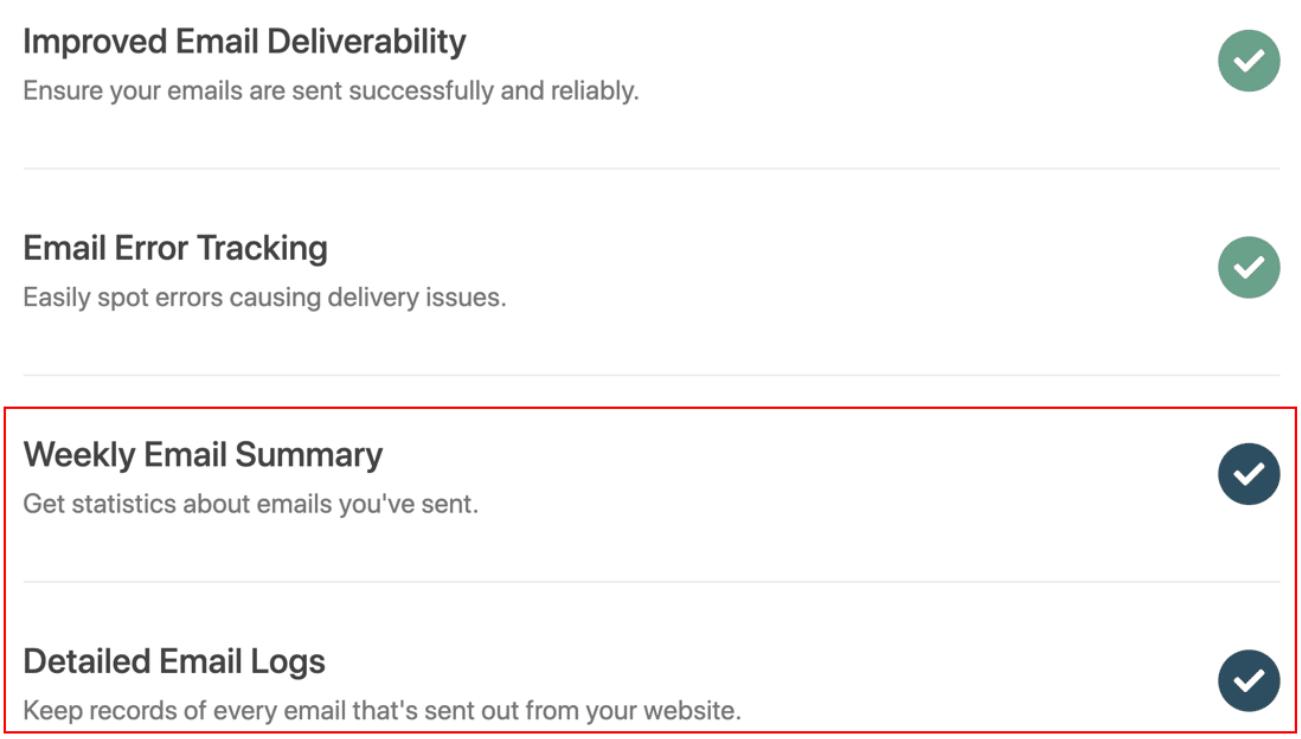
Im Vergleich zu Gmail oder Outlook sind sie auch einfach einzurichten.

Nachdem Sie Ihren E-Mail-Anbieter ausgewählt haben, klicken Sie auf den Link unten, um die entsprechende Dokumentation zu öffnen. Wir haben für jeden Mailer eine vollständige Anleitung erstellt, damit Sie Ihre WordPress-Site ganz einfach verbinden können:

Mailer in allen Ausführungen erhältlich	**Mailer in WP Mail SMTP Pro**
SendLayer	Amazon SES
SMTP.com	Microsoft 365 / Outlook.com
Kurz	Zoho Mail
Google Workspace / Gmail	
Postpistole	
Stempel	
SendGrid	
SparkPost	
Anderes SMTP	

Sobald Sie fertig sind, können Sie mit dem Assistenten fortfahren.

Wenn Sie über eine Pro-Lizenz zu aktivieren . **die detaillierten E-Mail-Protokolle** und die **wöchentliche E-Mail-Zusammenfassung** verfügen, empfehlen wir Ihnen dringend, im letzten Schritt

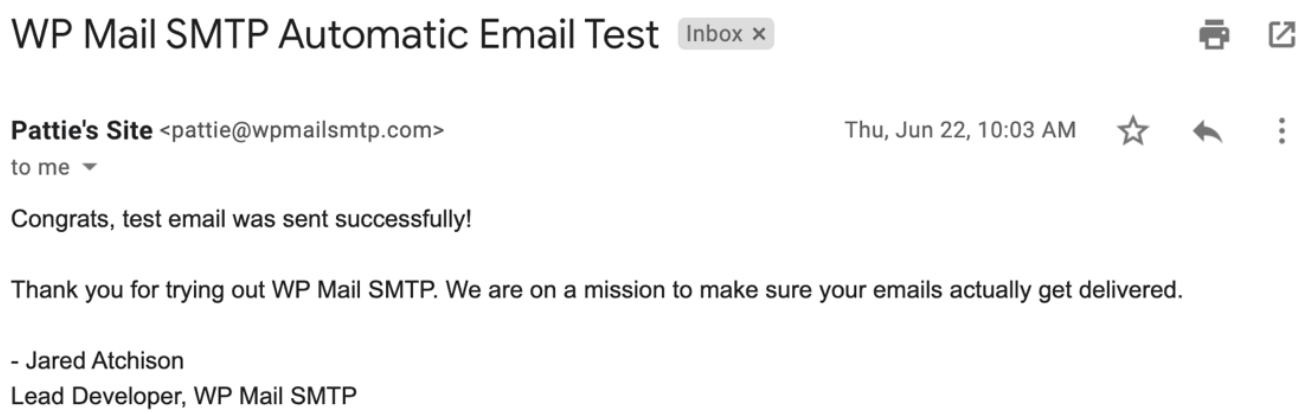


Wenn Sie diese Funktionen aktivieren, schalten Sie eine Menge zusätzlicher Funktionen in WP Mail SMTP frei:

- **Vollständige E-Mail-Protokollierung** : Speichern Sie eine Kopie des Textkörpers jeder E-Mail zusammen mit den Kopfzeilen
- **Öffnungs- und Klickverfolgung** : Sehen Sie sich Öffnungs- und Klickanalysen für Ihre WordPress-E-Mails an
- **E-Mail-Anhänge speichern** : Speichern Sie jeden von WordPress gesendeten Anhang
- **E-Mail-Protokolle exportieren** : Exportieren Sie Details gesendeter E-Mails und aller Anhänge
- **Export im EML-Format** : Speichern Sie eine vollständige Kopie einer gesendeten E-Mail und ihrer Anhänge
- **E-Mail erneut senden** : Senden Sie fehlgeschlagene E-Mails einzeln oder in großen Mengen erneut – ideal, wenn Sie die E-Mail zur Registrierung neuer Benutzer in WordPress erneut senden möchten
- **Wöchentliche Updates** : Erhalten Sie jeden Montag einen E-Mail-Bericht mit Ihren E-Mail-Zustellbarkeitsstatistiken , Öffnungsraten und Klickraten.

unserem Artikel [zum Protokollieren von WordPress-E-Mails .] Weitere Informationen finden Sie in

Und das ist es! WP Mail SMTP sendet eine automatische Test-E-Mail, damit Sie überprüfen können, ob alles funktioniert.

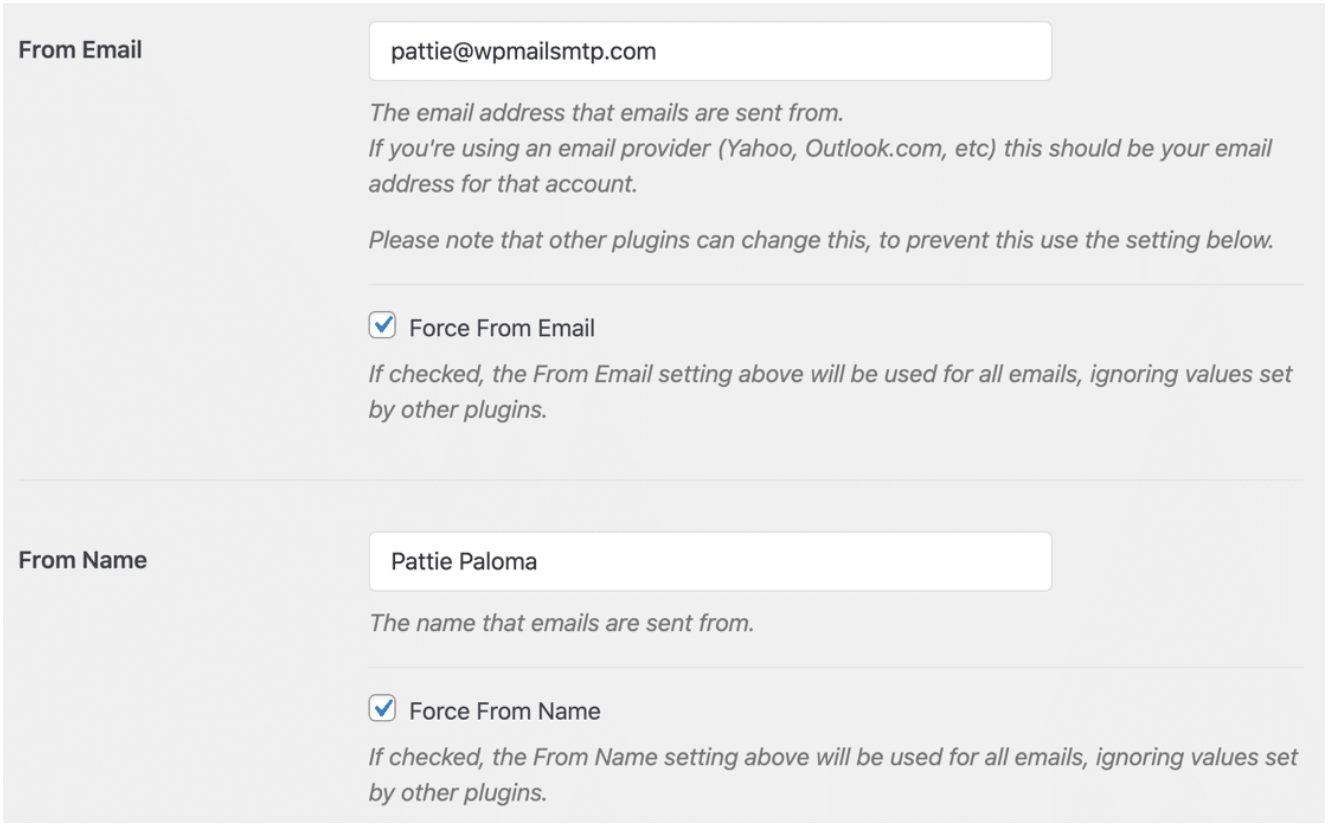


Sie werden feststellen, dass WP Mail SMTP Sie gefragt hat, ob Sie den Formularnamen erzwingen möchten. Werfen wir einen Blick darauf, was das bedeutet.

4. Legen Sie den Absendernamen und die Absender-E-Mail in WordPress fest

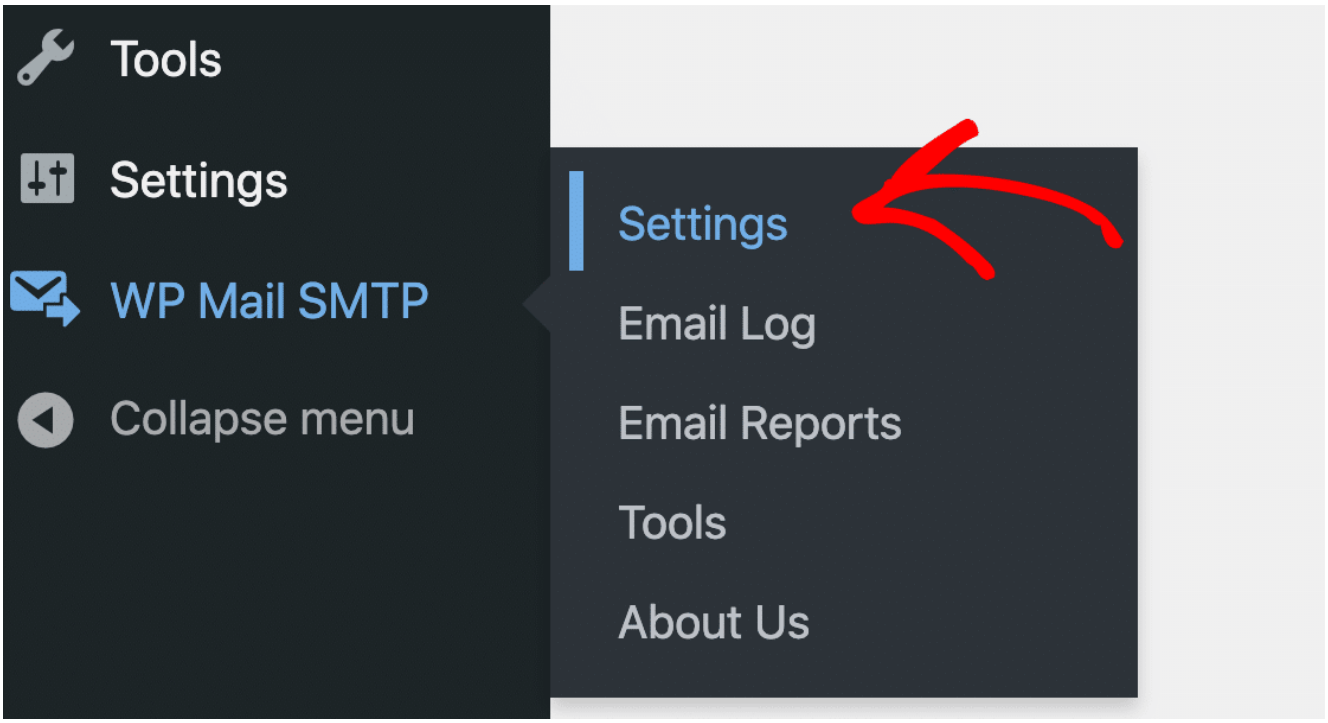
Der **Absendername** und **die Absender-E-Mail** sind wichtige Einstellungen beim Versenden von E-Mails von Ihrer WordPress-Website.

Der **Absendername** ist der Name des Absenders und die **Absender-E-Mail** ist die E-Mail-Adresse, von der die Warnung oder Benachrichtigung gesendet wird.



Die **Absender-E-Mail** ist hier die wichtige Einstellung. Es ist äußerst wichtig, dass die **Absender-E-Mail** korrekt eingerichtet ist, um zu verhindern, dass WordPress-E-Mails im Spam landen.

überprüfen **Sie können Ihre Absender-E-Mail** in **WP Mail SMTP » Einstellungen** .

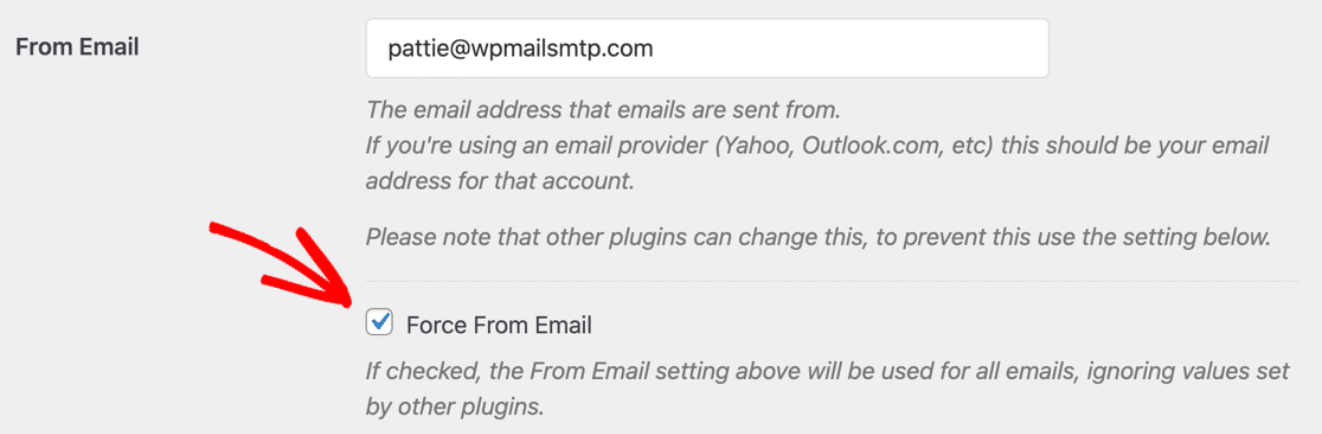


eingeben **Absender-E-Mail** Bei einigen Mailprogrammen können Sie

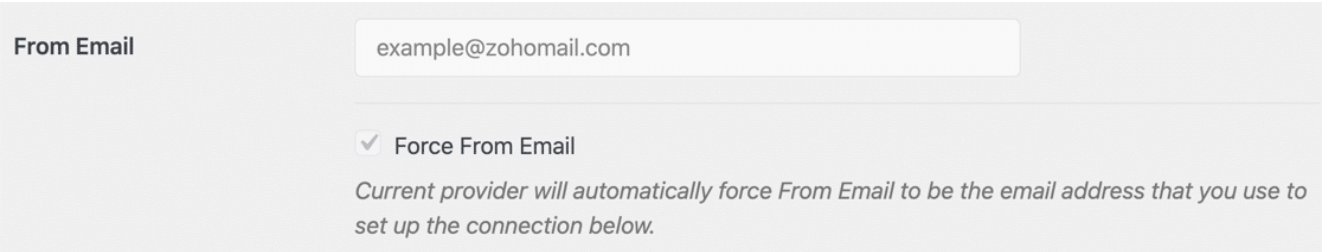
eine beliebige . In diesem Fall sollten Sie eine E-Mail-Adresse der Domäne verwenden, die Sie bei Ihrem E-Mail-Anbieter authentifiziert haben.

Zum Beispiel, wenn Sie sich authentifiziert haben example.comWenn Sie SendLayer einrichten, sollte Ihre E-Mail-Domäne ebenfalls mit enden example.com.

Wenn Sie dies auf Ihrer gesamten WordPress-Site erzwingen, können Sie sicher sein, dass alle Ihre E-Mails authentifiziert sind.



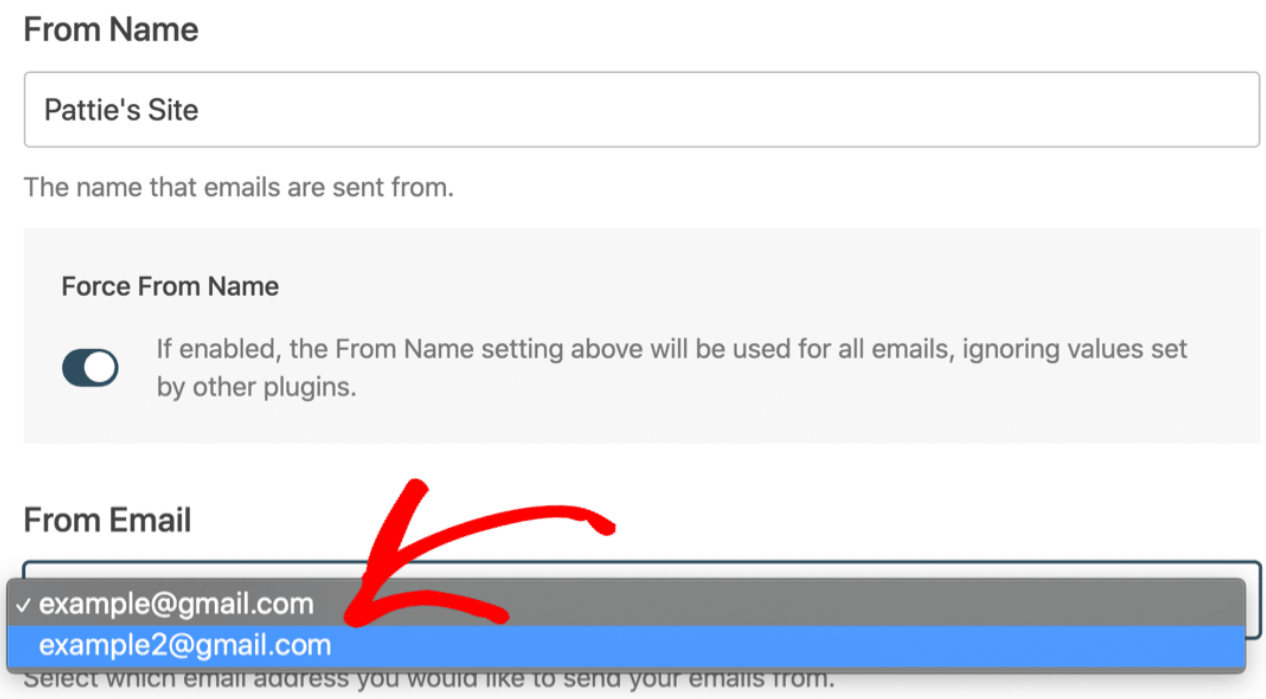
Wenn die **Absender-E-Mail** ausgegraut ist, können Sie sie nicht ändern.



Bei einigen E-Mail-Anbietern (einschließlich Zoho Mail) können Sie nicht eine andere **Absender-E-Mail-Adresse** verwenden als die, die Sie bei der Einrichtung des Plugins authentifiziert haben. Deshalb haben wir diese Einstellung ausgegraut, um sicherzustellen, dass Ihre E-Mails nicht fehlschlagen.

Wenn Sie Gmail oder Google Workspace verwenden, können Sie einen beliebigen Gmail-Alias verwenden, um E-Mails von WordPress aus zu senden . Ihre primäre **Absender-E-Mail-Adresse**

auswählen können. In diesem Fall wird ein Dropdown-Menü angezeigt, in dem Sie beim Ausführen des Einrichtungsassistenten



Sie können jeden dieser Aliase verwenden, um E-Mails von WordPress aus zu versenden. Beachten Sie, dass der primäre Google-Alias □□als **Absender-E-Mail** verwendet wird , wenn Sie versuchen, eine E-Mail-Adresse zu verwenden, die in Ihrem Gmail-Konto nicht vorhanden ist.

5. Smart Routing einrichten (optional)

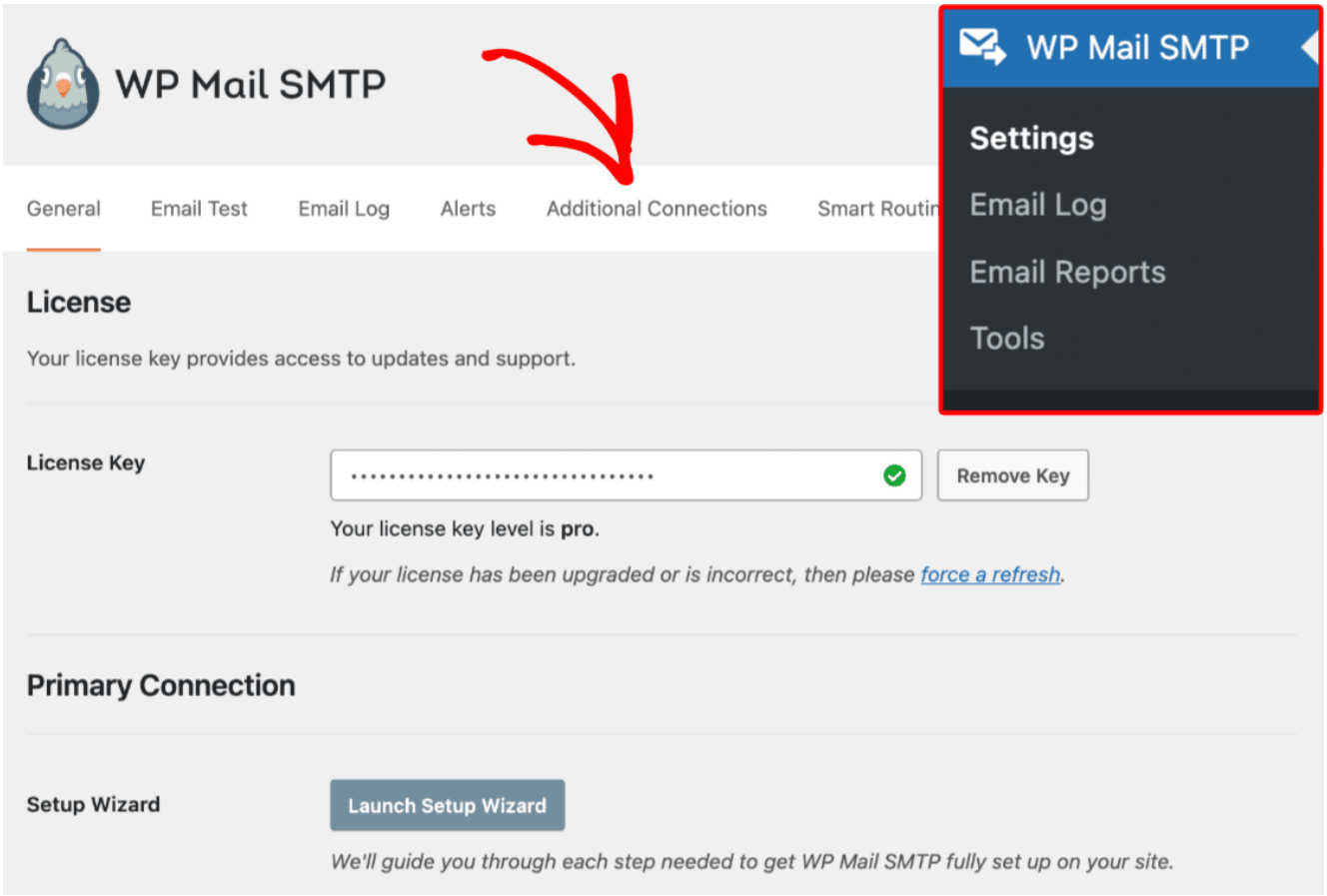
Mit WP Mail SMTP Pro können Sie Smart Routing einrichten. Mit dieser Funktion können Sie unterschiedliche Mailer für unterschiedliche E-Mail-Typen verwenden.

Dies kann die Zustellbarkeit von E-Mails verbessern, da bestimmte Mailer für unterschiedliche E-Mail-Typen am besten geeignet sind. Beispielsweise wird häufig empfohlen, für E-Commerce-Bestellbenachrichtigungen einen Transaktionsmailer zu verwenden.

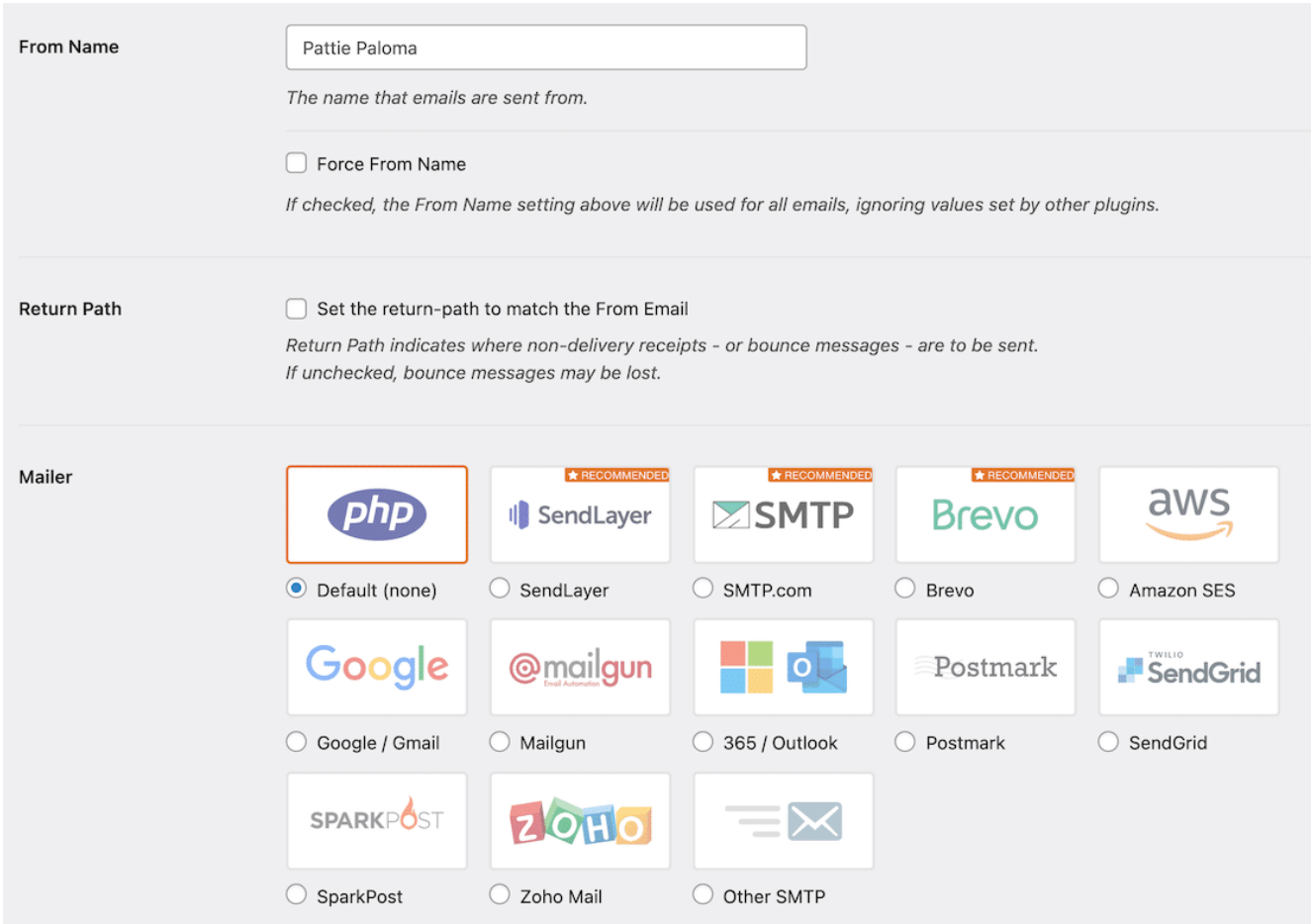
Wenn Sie den richtigen Mailer für die Art der E-Mails auswählen, die Sie versenden möchten, können Sie verhindern,

dass Ihre E-Mails im Spam landen.

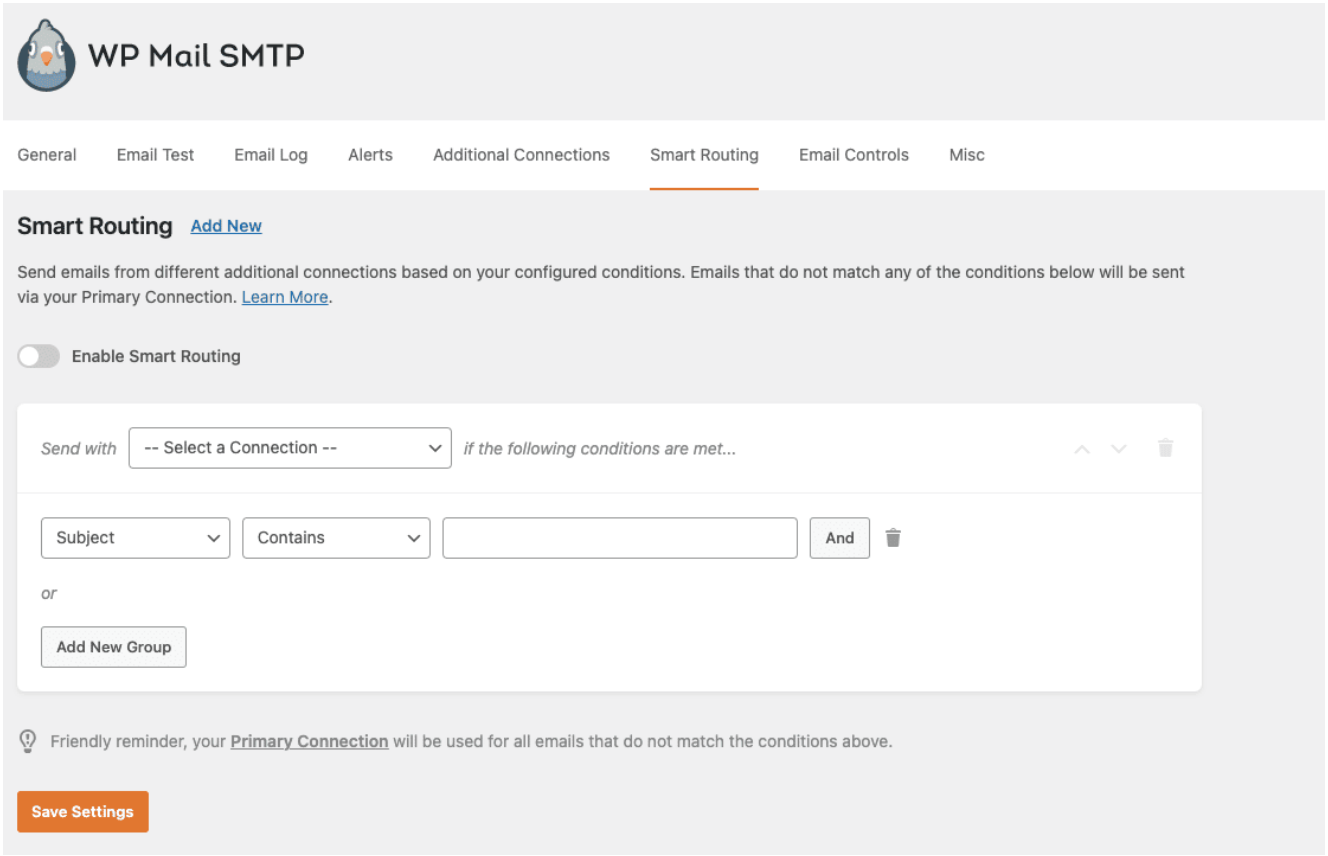
Um Smart Routing einzurichten, müssen Sie zunächst eine zusätzliche Verbindung hinzufügen. Gehen Sie zu **WP Mail SMTP » Einstellungen** und klicken Sie auf **Zusätzliche Verbindungen** .



Fügen Sie dann eine neue Verbindung hinzu und füllen Sie die Einstellungen aus. Dies sind die gleichen wie die Optionen für Ihre primäre Verbindung, die Sie zuvor in diesem Tutorial eingerichtet haben.



Sobald Sie mindestens eine zusätzliche Verbindung haben, können Sie Smart Routing aktivieren. Gehen Sie zur **Seite „Smart Routing-** Einstellungen“ und verwenden Sie die Dropdown-Listen, um eine bedingte Regel zu erstellen.



Dadurch wird WP Mail SMTP mitgeteilt, wann E-Mails über Ihre zusätzliche Verbindung gesendet werden sollen. Alle E-Mails, die die hier festgelegten Anforderungen nicht erfüllen, werden über Ihre primäre Verbindung gesendet.

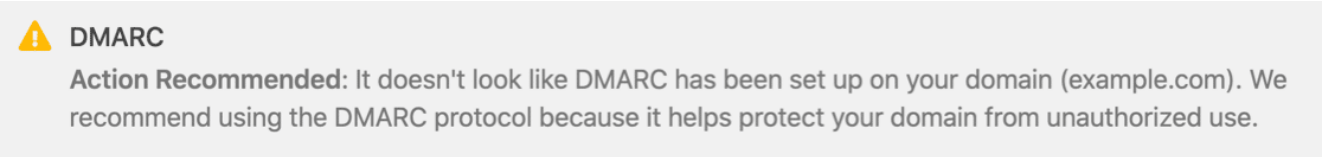
Weitere Einzelheiten finden Sie in unserem Leitfaden zu Smart Routing .

6. Richten Sie Ihr E-Mail-DNS ein

Manchmal landen WordPress-E-Mails im Spam, selbst nachdem Sie WP Mail SMTP eingerichtet haben. Dies wird fast immer durch falsche DNS-Einstellungen in Ihrer Domain verursacht.

einrichten Möglicherweise müssen Sie bei Ihrem E-Mail-Anbieter SPF-, DMARC- und DKIM-Einträge , um Ihre WordPress-E-Mails zu authentifizieren. Wenn Sie diesen Schritt überspringen, landen Ihre WordPress-E-Mails wahrscheinlich immer noch im Junk-Mail-Ordner.

Glücklicherweise verfügt WP Mail SMTP über einen integrierten DNS-Prüfer, der Ihr DNS automatisch auf Probleme überprüft.



Achten Sie auf alle SPF-, SKIM- oder DMARC-Warnungen, die Sie in WP Mail SMTP erhalten. Die richtigen Einstellungen sind ein entscheidender Schritt, um zu verhindern, dass WordPress-E-Mails im Spam landen.

Sie wissen nicht, wo Sie anfangen sollen? Wir haben vollständige Schritte zur DNS-Einrichtung in unsere Mailer-Dokumentation aufgenommen, um Sie auf den richtigen Weg zu bringen. Beginnen Sie mit dieser Anleitung zum Erstellen eines DMARC-Eintrags .

Korrigieren Sie jetzt Ihre WordPress-E-Mails

Als nächstes stoppen Sie Spam in Ihrem Kontaktformular

Da Sie nun die Spam-Ordnung Ihrer WordPress-E-Mails behoben haben, besteht möglicherweise ein weiteres Problem: Sie erhalten Spam von Ihrem Kontaktformular.

Schauen Sie sich die besten Kontaktformular-Plugins an , um zu erfahren, wie Sie Kontaktformular-Spam mithilfe von CAPTCHAs und geheimen Formular-Tokens stoppen können.

Sind Sie bereit, Ihre E-Mails zu reparieren? Beginnen Sie noch heute mit dem besten WordPress-SMTP-Plugin. WP Mail SMTP Elite umfasst das vollständige White Glove-Setup und bietet eine 14-tägige Geld-zurück-Garantie.

Wenn Ihnen dieser Artikel weitergeholfen hat, folgen Sie uns bitte auf Facebook und Twitter für weitere WordPress-Tipps und Tutorials.

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.

Reaktion nach Sperrung der Mail-Domain ct.de von Google

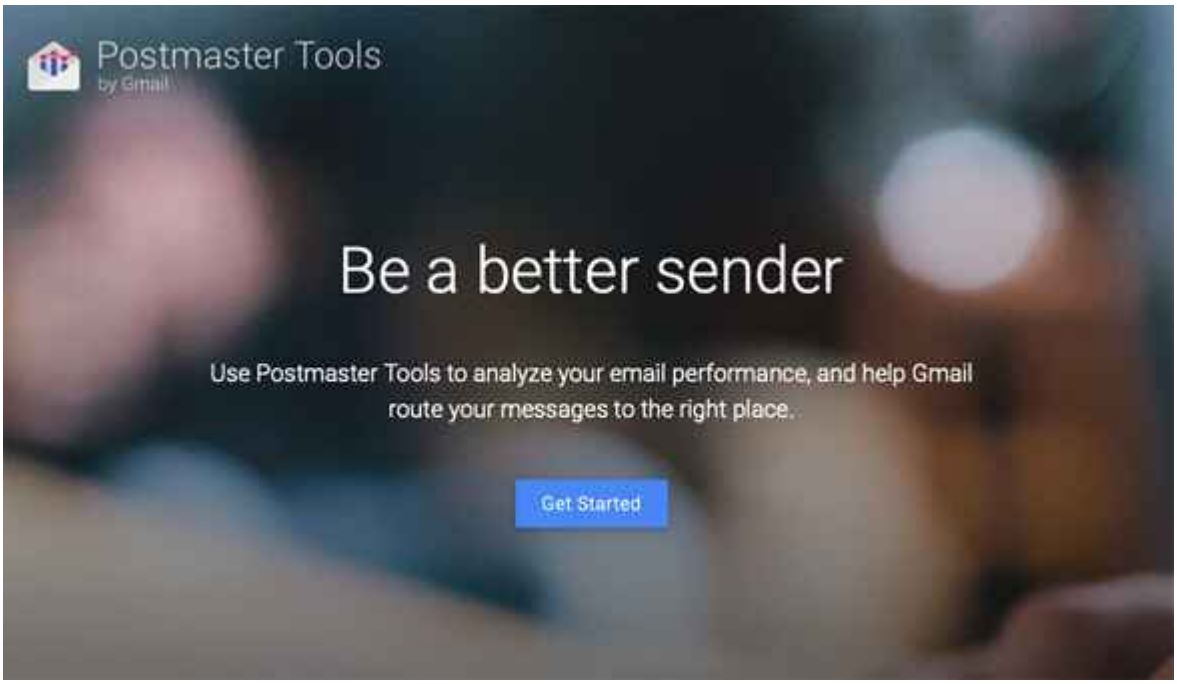
Google sagt: Microsoft ist schuld

Mitte Juni nahm Google plötzlich keine Mails von ct.de mehr an, die Reputation der Domain sei zu gering. Jetzt hat sich das Unternehmen geäußert und zeigt mit dem Finger auf Microsoft.
Mitte Juni nahm Google plötzlich keine Mails von ct.de mehr an, die Reputation der Domain sei zu gering. Jetzt hat sich das Unternehmen geäußert und zeigt mit dem Finger auf Microsoft.

Von Michael Fischer von Mollard und Jan Mahn

Fast einen Monat lang konnten Mitarbeiter der c’t mit einer

@ct.de-Adresse nicht an Server von Google mailen – weder an @gmail.com noch an die zahlreichen Unternehmen, die ihre Mails bei Google verwalten lassen. In der Fehlermeldung beklagten sich die Server über mangelnde Reputation der Domain ct.de [1]. Die Postmaster-Tools, die Google für solche Fälle für Mail-Admins bereitstellt, halfen nicht weiter. In seinen FAQ spricht Google selbst davon, dass die Informationen erst bei einer Größenordnung von Hunderten Mails pro Tag aussagekräftig sind – und diese Grenze erreicht die Domain nicht. Im Juli war das Problem dann so plötzlich verschwunden, wie es gekommen war.



Postmaster-Tools von Google: Die Anlaufstelle für Mailserverbetreiber liefert nicht immer aussagekräftige Informationen, wenn es bei der Zustellung Probleme gibt.

Mit einer Erklärung ließ sich Google bis Ende August Zeit, doch die hatte es in sich: Schuld sei Microsoft. Weil der Verlag für Videotelefonie Teams einsetzt, enthielt der SPF-Eintrag (Sender Policy Framework) im DNS für ct.de den Eintrag: include:spf.protection.outlook.com

Empfangende Mailserver können diesen Eintrag auswerten und ihm entnehmen, wer Mails im Namen einer Domain versenden darf. Dass Microsofts Server berechtigt wurden, ist Standard für Unternehmen, die Teams nutzen und das System zum Beispiel

Termineinladungen verschicken lassen wollen. Zum Problem wurde der SPF-Eintrag, weil Microsofts Server eine extrem ungewöhnliche Art der direkten Weiterleitung einsetzen, die Spammer ausnutzen können. Beschrieben wird das Problem auch in einem wissenschaftlichen Paper aus dem April [2].

Um das Problem zu verstehen, muss man wissen, dass es auf Ebene des Mailprotokolls SMTP einen für die Nutzer meist unsichtbaren Envelope-Absender gibt, der von dem Absender abweichen kann, den Sender und Empfänger in ihren Mailprogrammen sehen (dem From-Header). Für SPF ist der Envelope-Absender entscheidend.

Offene Weiterleitung

Die Spammer nutzen aus, dass Microsofts Mailserver sogenanntes Open Forwarding erlauben – als Nutzer kann man eine dauerhafte Weiterleitung einrichten. Bei Accounts von Privatnutzern, die über outlook.com senden, setzt Microsoft in dem Fall den Envelope-Absender auf die Domain outlook.com, bei Geschäftskunden jedoch nicht. Bei ihnen wird beim Weiterleiten der Absender aus dem From-Header als Envelope-Absender übernommen und die Mail so an die eingestellte Adresse gesendet. Spammer brauchen also Zugriff auf ein Geschäftskundenkonto, hinterlegen dort die Adresse ihres Spam-Opfers (in diesem Fall ein Konto bei Google) als Weiterleitungsadresse.

Dann müssen sie sich nur eine beliebige Domain aussuchen, die den gängigen SPF-Eintrag für Microsoft-Server enthält. Von ihrer eigenen Adresse senden sie Mails an das Konto bei Microsoft, setzen aber als From-Header zum Beispiel eine ct.de-Adresse. Microsoft nimmt die Mail an, ändert den Envelope-Absender und leitet sie direkt an das Opfer weiter. Genau das ist laut Google mit der Domain ct.de passiert: Am 15. Juni stieg das Mailvolumen von der Domain um rund den Faktor 2000, alle problematischen Mails kamen über Microsoft-Server. Anstatt diese Server auszubremsen, entschied sich

Google dafür, die Reputation der Domain zu senken.

Googles Reaktion ist teilweise verständlich, die nicht funktionierenden Postmaster-Tools, die Reaktionszeiten und das Kommunikationsverhalten sind für Mail-Admins jedoch extrem unbefriedigend. Microsofts Vorgehen dagegen ist ein echtes Sicherheitsproblem: Weil Teams-Admins den entsprechenden SPF-Eintrag massenhaft setzen, haben Microsofts Mailserver eine exponierte Rolle – die spammerfreundliche Weiterleitung ist dann schlicht unangemessen. Mitte August erfuhren wir über DMARC-Reports von einem ähnlichen Vorfall – diesmal schickten die Microsoft-Server im Namen von ct.de an Yahoo-Adressen. Der SPF-Eintrag für ct.de ist seitdem geändert und Microsofts Server sind entfernt.

Der Vorfall macht aber auch deutlich, dass SPF aus einer anderen Zeit stammt, in der es noch üblich war, dass Mailserver dezentral von Organisationen betrieben werden. Heute ist es dagegen üblich, dass große Provider die Mails für ihre Kunden abwickeln und mit dem dann unvermeidlichen include: im SPF-Eintrag gibt man als Admin die Kontrolle über die ausgehenden Server aus der Hand – das verwässert den Wert eines SPF-Eintrags.

1. Literatur
2. Jan Mahn, Google stufte ct.de als Spamschleuder ein, c’t 19/2023, S. 35
3. E. Liu et al., Forward Pass: Onthe Security Implications of Email Forwarding Mechanism and Policy, arXiv, 19. April 2023, https://arxiv.org/pdf/2302.07287.pdf

Verdächtige Mailanhänge risikolos untersuchen und entschärfen

Erfolgreicher Exorzismus

Wie Sie verdächtige Mailanhänge risikolos untersuchen und entschärfen

Mailanhänge zu öffnen, ist ein riskantes Unterfangen – aber oft unumgänglich. Wir stellen Tools vor, mit denen Sie Anhänge in risikofreie Kopien verwandeln und eingehend untersuchen können, bevor Sie sie öffnen.

Von Sylvester Tremmel

Mailanhängen dürfen Sie nicht vertrauen. Doch egal wie vorsichtig Sie Ihren Posteingang auf Phishing-Attacken untersuchen und wie misstrauisch Sie E-Mails begegnen: Früher oder später taucht ein Anhang auf, dessen Absichten unklar sind und den Sie nicht ignorieren können, weil der Inhalt verspricht, wichtig zu sein.

Also müssen Sie irgendwie das Risiko verringern, das von dem Anhang ausgeht, bevor Sie ihn öffnen. Dazu haben Sie eine Reihe von Handlungsoptionen; die einfachste vorweg: Sehen sie nach, ob ein Online-Virenscanner wie virustotal.com den Anhang kennt. Allerdings nicht, indem Sie dort einfach die Datei hochladen, sonst haben Sie allzu leicht ein Datenschutzproblem am Hals (siehe dazu den Artikel auf S. 18). Berechnen Sie

stattdessen lokal einen eindeutigen Hash der Datei und geben Sie diesen in die Suche von VirusTotal ein. Aus dem Hash lassen sich keine Daten rekonstruieren, aber falls es sich um eine bereits bekannte Datei handelt, bekommen Sie so eine Einschätzung des Dienstes. Viren-Dokumente werden in der Regel breit gestreut, mit etwas Glück liegt daher zu einer verseuchten Datei bereits ein Report vor.

Auf VirusTotal muss man nicht unbedingt eigene Dateien hochladen. Man kann auch per Hash nach bereits bekannten Dateien suchen.
Einen passenden Hash berechnen Sie am schnellsten auf der Kommandozeile, unter Windows mit dem PowerShell-Befehl Get-FileHash DATEI, unter Linux per sha256sum DATEI und unter macOS mit shasum -a 256 DATEI. Es gibt aber auch diverse Tools mit grafischer Oberfläche, die Hashes berechnen können; VirusTotal findet Hashwerte der Verfahren MD5, SHA-1 und SHA-256. (Nutzen Sie am besten das letzte, es gilt als uneingeschränkt sicher.)

Wenn gleich mehrere namhafte Scanner bei VirusTotal anschlagen, sollten Sie den Anhang direkt in den Orkus schicken. Falls der Onlinedienst die Datei nicht kennt oder darin nichts findet, dann ist das nur ein erster Hinweis, aber noch keine Unbedenklichkeitserklärung, und Sie sollten

weiterforschen.

Ab in die Quarantäne

Zum Beispiel, indem Sie eine von Ihrem Arbeitsrechner isolierte Umgebung nutzen, aus der Malware nicht ausbrechen kann. Dafür eignet sich unter anderem eine virtuelle Maschine (VM). Wenn man darin ein bösartiges Dokument öffnet, geht höchstens diese VM zugrunde. Zwar gibt es auch in VM-Software Lücken, aber das Risiko, dass eine Malware aus der Virtualisierung herauskommt, ist sehr, sehr gering.

VMs sind gut, um gelegentlich eine Datei zu analysieren. Dann bootet man darin am besten ein frisches Spezialsystem wie Kali Linux oder Parrot Security [1, 2] und löscht nach der Analyse die ganze VM. Sie können virtuelle Maschinen auch zur Absicherung der täglichen Arbeit nutzen, zum Beispiel, indem Sie darin ein wartungsarmes Linux wie Debian [3] installieren und damit Ihre Mails abrufen. Das ist eine gute Methode, aber wenn man täglich so arbeitet, stößt man schnell an die Grenzen, die durch die Isolierung entstehen. Wer dann keine eiserne Disziplin zeigt, bohrt über kurz oder lang Löcher in die Isolation, um leichter Dateien in die VM hinein und aus ihr heraus zu bekommen. Schlimmstenfalls wird aus der Isolations-VM allmählich die normale Arbeitsumgebung und der Schutzeffekt ist perdu.

Praktikabler sind Tools, die automatische Isolationsumgebungen nutzen, um Dateien zu entschärfen, wie das Werkzeug Dangerzone (https://dangerzone.rocks). Es steht für Windows, macOS und Linux zur Verfügung und nutzt Container zur Isolation. Unter Windows und macOS kommt dafür Docker Desktop zum Einsatz unter Linux podman. Container bieten eine weniger gute Isolation als echte virtuelle Maschinen, stellen für Malware aber dennoch eine massive Hürde dar.

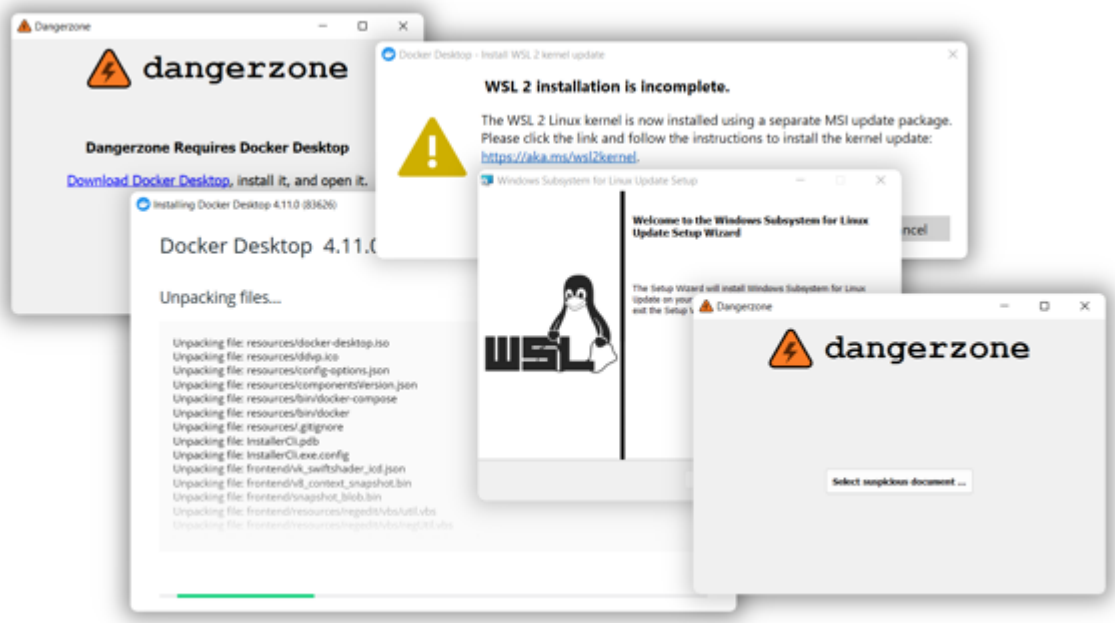
Die isolierten Container nutzt Dangerzone, um einen Anhang zu öffnen und in Bilddaten zu konvertieren. Malware können diese

Pixelbilder nicht enthalten und nur diese Daten lässt Dangerzone aus dem Container. In einem zweiten Schritt wird aus den Pixeldaten ein PDF erzeugt, damit man keine lose Bildsammlung als Ergebnis erhält. Das Resultat ist ein PDF mit optisch gleichem Inhalt wie das Eingangsdokument, aber garantiert ohne Malware, Makros, versteckte Inhalte, verheimlichte Linkziele und viele andere Arten von Bedrohung. Als Betriebssystem im Container nutzt Dangerzone Linux (auch unter Windows und macOS). Da die meisten Schädlinge auf Windows abzielen, ist es unwahrscheinlich, dass etwaiger Schadcode überhaupt ausgeführt wird, selbst wenn die Programme im Container Sicherheitslücken aufweisen sollten. Und auch wenn Malware die Software im Container kompromittiert und mit Linux zurande kommt, dann müsste sie immer noch aus dem Container ausbrechen, um Schaden anzurichten.

Bei so vielen Hürden kann man es verschmerzen, dass sich die Software im Container leider nicht leicht aktualisieren lässt: Der Installer von Dangerzone bringt ein fertiges Containerimage mit, damit die Software auch auf Rechnern ohne Internetzugang funktioniert. Wer sich nicht zutraut, das Containerimage selbst neu zu bauen – und eventuelle Inkompatibilitäten zu beheben –, bekommt erst mit einer neuen Dangerzone-Version ein neues Image. Das ist ein akzeptabler Kompromiss, aber wem er nicht reicht: Nichts spricht dagegen, noch eine Barriere hinzuzufügen und Dangerzone innerhalb einer VM zu betreiben.

Die Installation von Dangerzone erfordert unter Windows und macOS diverse Schritte, aber die sind relativ simpel: Zuerst laden Sie den Installer herunter und führen ihn aus. Danach können Sie Dangerzone bereits starten, erhalten aber den Hinweis, dass die Applikation Docker Desktop erfordert, sofern es nicht bereits installiert ist. Also folgen Sie dem angezeigten Link, laden Docker Desktop herunter und führen auch diesen Installer aus, was unter macOS mit ein paar Sicherheitsabfragen einhergeht, die Sie bestätigen müssen.

Danach starten Sie Docker und sind unter macOS nach ein paar Sekunden Startzeit einsatzbereit.



Die Installation von Dangerzone erfordert zwar eine Reihe von Schritten, ist aber nicht kompliziert.
Unter Windows beschwert sich Docker Desktop eventuell, falls das „Windows Subsystem for Linux 2“ (WSL 2) nicht bereitsteht. Aber auch in diesem Fall zeigt die Problemmeldung direkt den nötigen Link an. Sie müssen also nur eine weitere Runde aus Klick, Download und Installation drehen und nun ist Docker auch unter Windows zufrieden und zur Arbeit bereit. Nach einem Klick auf „Check again“ merkt das auch Dangerzone und macht sich daran, das Container-Image zu installieren. Das geht vollautomatisch vonstatten.

Die Installation unter Linux ist leichter oder schwerer, je nachdem, um welche Distribution es geht. Für einige Distributionen betreiben die Dangerzone-Entwickler eigene Repositories, was die Installation sehr einfach macht. Unter Debian genügen beispielsweise folgende Befehle:

```
curl -s https://packagecloud.io/install/repositories/firstlookmedia/code/script.deb.sh | sudo bash
sudo apt update
sudo apt install -y dangerzone
```

Ein Skript per curl herunterzuladen und direkt auszuführen, gilt allerdings zu Recht als höchst fragwürdige Installationsmethode. Wer dem Braten nicht traut, kann die Repositories manuell einrichten, die Dokumentation von Dangerzone erklärt, wie das geht (siehe ct.de/yw2x).

Leider unterstützt Dangerzone im Moment nur bei Debian aktuelle Versionen (11 und 12), bei Ubuntu und Fedora funktionieren von Haus aus nur etwas ältere Ausgaben (20.10, 21.04 und 21.10 beziehungsweise 33, 34 und 35). Auch bei anderen Distributionen sollten Sie sich nicht zu früh freuen: Beispielsweise findet sich Dangerzone zwar im User Repository von Arch Linux, allerdings ist das Paket aktuell nicht funktionstüchtig.

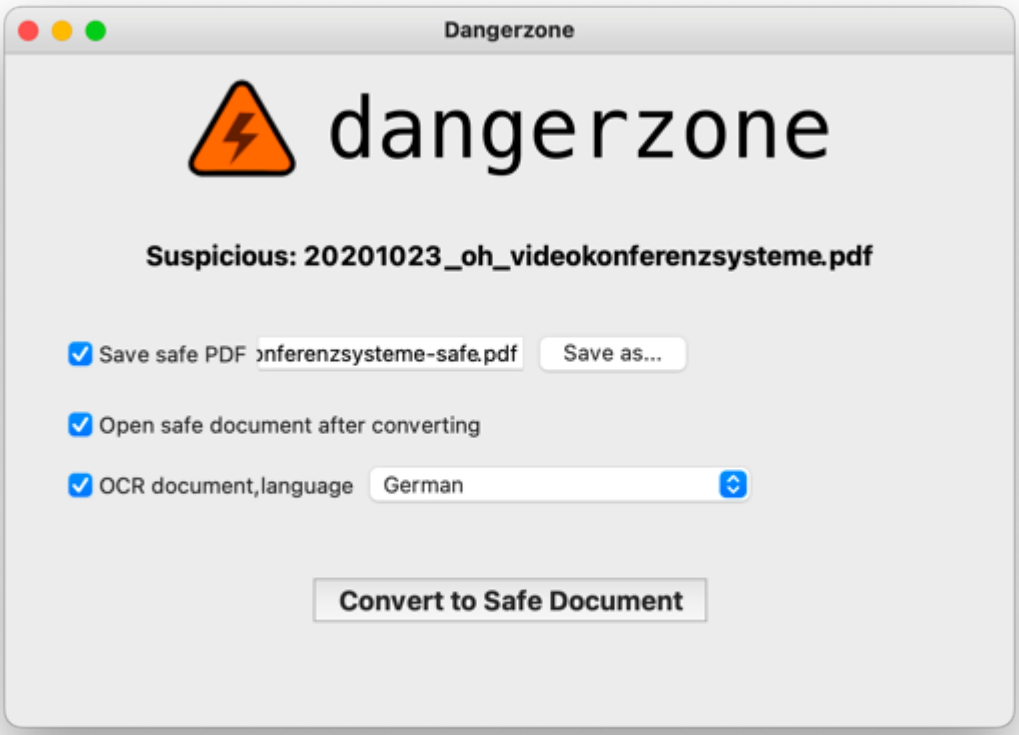
Statt sich unter Linux mit dem Paketbau oder Versionsinkompatibilitäten herumzuschlagen, bietet es sich an, einfach eine Debian-VM aufzusetzen und Dangerzone darin zu betreiben.

In der Gefahrenzone

Einmal fertig installiert, fällt die Bedienung von Dangerzone sehr leicht: Das Programm präsentiert nach dem Start nur eine Schaltfläche, die Sie drücken, um eine Datei zu konvertieren. Dangerzone kann diverse Office-Formate unschädlich machen, die ein Haupteinfallstor für Malware sind. Dazu startet das Programm im Container LibreOffice, um aus dem Office-Dokument ein PDF zu machen. Aus dem PDF werden dann Pixelgrafiken und daraus wieder ein – garantiert harmloses – PDF. Daneben können Sie mit Dangerzone auch PDFs und sogar Bilddateien entschärfen. Von letzteren geht nur eine geringe Gefahr aus, aber sicher ist sicher.

Nachdem Sie ein Dokument ausgewählt haben, bietet das Programm noch ein paar Einstellungen an. Dangerzone hat eine Texterkennung integriert (Optical Character Recognition, OCR) und fragt dafür nach der Sprache, in der das Dokument

vermutlich verfasst ist. So kann das Tool im zweiten Schritt die Bilddaten analysieren, um den Textinhalt eines Dokumentes zu rekonstruieren. OCR erhöht den Komfort erheblich, weil Sie dadurch im sicheren PDF Texte wieder markieren und kopieren können. Ein Klick auf „Convert to Safe Document“ stößt die Umwandlung an. Unter Linux und macOS erlaubt Dangerzone darüber hinaus, das Ergebnis-PDF automatisch zu öffnen, was Ihnen noch ein paar Klicks erspart.



Ein Klick und Dangerzone erzeugt eine garantiert harmlose Dateikopie mit dem gleichen (sichtbaren) Inhalt. So wird beispielsweise aus einem verseuchten Word-Dokument eine entschärfte PDF-Version.
Diese Bequemlichkeit können Sie unter Windows leicht nachrüsten, indem Sie die Kommandozeilenvariante von Dangerzone einspannen. Die wurde automatisch mitinstalliert, Sie können sie in der Eingabeaufforderung mit dem Befehl dangerzone-cli (für „command-line interface“) starten. Der Aufruf dangerzone-cli DATEI erstellt aus DATEI ein sicheres PDF, mit den Parametern --ocr-lang deu und --output-filename NEU.PDF schalten Sie die Texterkennung für Deutsch ein und

legen den Namen der Ergebnisdatei fest.

Damit kann man leicht ein Skript basteln, das Dateien konvertiert und öffnet. Unter ct.de/yw2x haben wir Ihnen drei Varianten bereitgestellt: Eine Batch-Datei, ein AutoHotkey-Skript und eine daraus erstellte EXE-Datei. Es ist eine gute Idee, eines der Skripte als Standardanwendung für Office-Dateien festzulegen. In Zukunft genügt dann ein Doppelklick auf die Datei, um Dangerzone zu starten, eine sichere Version zu generieren und diese zu öffnen. So vermeiden Sie auch, gefährliche Dateien versehentlich direkt zu öffnen. Bei Bedarf können Sie die Originaldokumente über das Kontextmenü weiterhin mit der üblichen Anwendung öffnen – wenn Sie sicher wissen, dass sie harmlos sind.

Qubes OS

Wenn man willens ist, aus Sicherheitsgründen das Betriebssystem zu wechseln, stehen noch bessere Lösungen als Dangerzone zur Verfügung. Nahe am Nonplusultra liegt Qubes OS, das VMs nutzt, um das gesamte System in Sicherheitszonen zu unterteilen. Im Detail haben wir Qubes OS in Ausgabe 11/2022 vorgestellt [4].

Unter Qubes OS können Sie beliebige Dateien weitgehend gefahrlos öffnen, indem Sie im Kontextmenü „View in disposable“ oder „Edit in disposable“ auswählen. Das System startet dann automatisch eine aktuelle VM und öffnet darin den Anhang mit der Standardanwendung. Wenn Sie die schließen, verwirft Qubes OS die komplette VM. Einzig die Änderungen an der Datei werden zurückgeschrieben, sonst nichts, und auch die Änderungen nur, wenn Sie die „Edit“-Option gewählt haben.

Schon das liefert mehr Sicherheit und Komfort, als man mit normalen VM-Lösungen erreicht. Zusätzlich gibt es die Tools qvm-convert-pdf und qvm-convert-img. Diese Werkzeuge waren die Vorlage für Dangerzone und funktionieren im Prinzip genauso. Allerdings nutzen die Qubes-OS-Befehle echte VMs und keine

Container. Das bietet noch mehr Schutz und ist leicht implementiert, wenn das Betriebssystem ohnehin alles in VMs verpackt.

Mit spitzen Fingern

Trotz solcher Helferlein ist Dangerzone mit Einschränkungen verbunden. Zum einen stellt das LibreOffice im Container Office-Formate nicht unbedingt so dar, wie Microsoft Office unter Windows sie anzeigt; zum Beispiel, weil im Container Schriftarten fehlen. Sie müssen also damit leben, dass die Ausgabedokumente von Dangerzone eventuell ein bisschen anders aussehen, als die Eingabedateien.

Zum anderen holpert die Texterkennung von Dangerzone gelegentlich, besonders wenn die Schrift im Dokument schlecht lesbar ist, etwa weil es sich um eine schnörkelige Schreibschrift handelt. Längere kopierte Passagen sollten Sie daher Korrektur lesen.

Das Hauptproblem von Dangerzone folgt aber aus seiner Funktionsweise: Als Ergebnis erhalten Sie immer ein PDF. Das reicht, wenn Sie das Dokument nur betrachten wollen, aber wenn Sie ein Word-Dokument bearbeiten, eine Excel-Tabelle für Berechnungen nutzen oder ein PDF-Formular ausfüllen wollen, dann kommen Sie so nicht weiter.

Immerhin können – und sollten – Sie in solchen Fällen das Dokument erst einmal mit Dangerzone konvertieren und öffnen, um den Inhalt auf Plausibilität zu prüfen. Ein angeblicher Geschäftsbericht gehört direkt in die Tonne, wenn der sichtbare Inhalt laut Dangerzone nur aus einem aufwendigen Banner besteht, das Sie auffordert, Makros zu aktivieren.

Aber was, wenn der Dateiinhalt plausibel aussieht? In diesem Fall kommen Sie nicht darum herum, das Dokument zu öffnen – allerdings nicht mit der Standardanwendung! Als absolutes Minimum können Sie beispielsweise den PDF-Reader im Browser

statt des Adobe Reader einspannen oder LibreOffice statt Microsoft Office. Das verringert zumindest die Chance, dass eventuell im Dokument eingebetteter Schadcode korrekt ausgeführt wird (siehe S. 21).

Deutlich sicherer ist es aber, verdächtige Dateien mit Werkzeugen zu öffnen, die den Inhalt analysieren und nicht direkt anzeigen. Was für Werkzeuge sich dafür eignen, hängt vom Typ der fraglichen Datei ab. Wir beschränken uns im Folgenden auf die beiden verbreitetsten Arten von Anhängen: Office- und PDF-Dateien. Bilder werden zwar ebenfalls sehr häufig verschickt, aber von üblichen Formaten wie JPG oder PNG geht nur eine geringe Gefahr aus. Wer solche Dateien weiterverarbeiten will, kann sie – nach einer Inspektion per Dangerzone – in der Bildbearbeitung seiner Wahl öffnen. Das verbleibende Restrisiko ist sehr gering.

Zur Analyse von PDFs und Office-Dateien stellen wir Ihnen zwei Werkzeugsammlungen vor, die beide auf der Kommandozeile laufen. Lassen Sie sich davon nicht abschrecken, eine erste Analyse ist wirklich nicht schwer.

PDF-Tools

Der Sicherheitsforscher Didier Stevens hat eine Reihe von Werkzeugen geschrieben, um PDF-Dateien zu analysieren und bietet sie auf seiner Webseite als Zip-Archive zum Download an (siehe ct.de/yw2x). Um eine Datei grob einzuschätzen, eignet sich das Tool pdfid. Laden Sie das zugehörige Archiv von Didiers Website und entpacken Sie den Inhalt in ein beliebiges Verzeichnis. Das Tool ist in Python geschrieben; wie Sie die dafür nötige Laufzeitumgebung installieren, haben wir in c’t 5/2022 ausführlich erklärt [5].

Wenn Sie zum Beispiel die PDF-Datei verdaechtig.pdf mit

```
python pdfid.py verdaechtig.pdf
```

öffnen, gibt das Programm eine Liste von Schlüsselwörtern

zurück, die es im PDF gefunden hat:

```
PDFiD 0.2.8 verdaechtig.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

Im Grunde sucht pdfid lediglich in der Datei nach diesen Schlüsselwörtern, die als ASCII-Zeichen vorliegen müssen. Wie so oft ist es in Praxis komplizierter: PDFs erlauben die Zeichenketten unterschiedlich zu kodieren, womit pdfid aber zurande kommt.

Achten sollten Sie besonders auf die Schlüsselwörter /JS und /JavaScript, die einen Wert größer 0 anzeigen, wenn das PDF vermutlich JavaScript-Code enthält. JavaScript kommt auch in einigen gutartigen PDFs vor, wo es beispielsweise Formulareingaben validiert. Nichtsdestotrotz sollten Sie JavaScript-Code als deutliches Warnsignal betrachten.

Ebenfalls Warnsignale stellen die Schlüsselwörter /AA,

/OpenAction und /AcroForm dar. Werte größer 0 bedeuten dort, dass der PDF-Reader automatische Aktionen starten soll, wenn man ein Dokument öffnet. Auch das kann harmlos sein und den Reader beispielsweise anweisen, eine bestimmte Seite des Dokuments anzusteuern – oder es führt Skriptcode aus und platziert Malware auf dem Rechner.

Wenn Sie auch nur eines dieser Schlüsselwörter entdecken, löschen Sie das verdächtige PDF, um auf Nummer sicher zu gehen. Wenn es dafür zu wichtig und dringend ist, dann hilft der Parameter --disarm (oder -d) von pdfid:

```
python pdfid.py -d verdaechtig.pdf
```

Das Programm produziert damit eine Kopie der Datei mit der Endung „.disarmed.pdf“. In der Kopie ist die Groß- und Kleinschreibung kritischer Schlüsselwörter vertauscht, aus /JavaScript wird /jAVAsCRIPT, aus /OpenAction wird /oPENaCTION und so weiter. So geschrieben handelt es nicht um gültige Schlüsselwörter und PDF-Reader sollten sie ignorieren. Diese entwaffnete Variante der Datei können Sie risikoarm öffnen.

Wem auch das nicht reicht, der kommt um eine detaillierte Analyse der internen Struktur des Dokuments nicht herum. Nur so findet man gefahrlos heraus, welche Aktionen genau ausgeführt würden und was genau der JavaScript-Code täte. Das erfordert allerdings Programmierkenntnisse, Wissen über den internen Aufbau von PDFs und mehr Platz, als dieser Artikel bietet. Wir werden in einer der folgenden Ausgaben zeigen, wie man bei so einer Analyse vorgeht.

Office-Dateien

Auch um Office-Dateien zu untersuchen, gibt es Kniffe und Werkzeuge in der Art von pdfid, aber nicht immer benötigen Sie dergleichen: Microsofts neuere Formate, die auf X enden (DOCX, XSLX, PPTX), sind im Grunde Zip-Archive, die lediglich einen speziellen Inhalt haben. Das hilft, falls Sie beispielsweise nur an den Bildern in einem Word-Dokument interessiert sind.

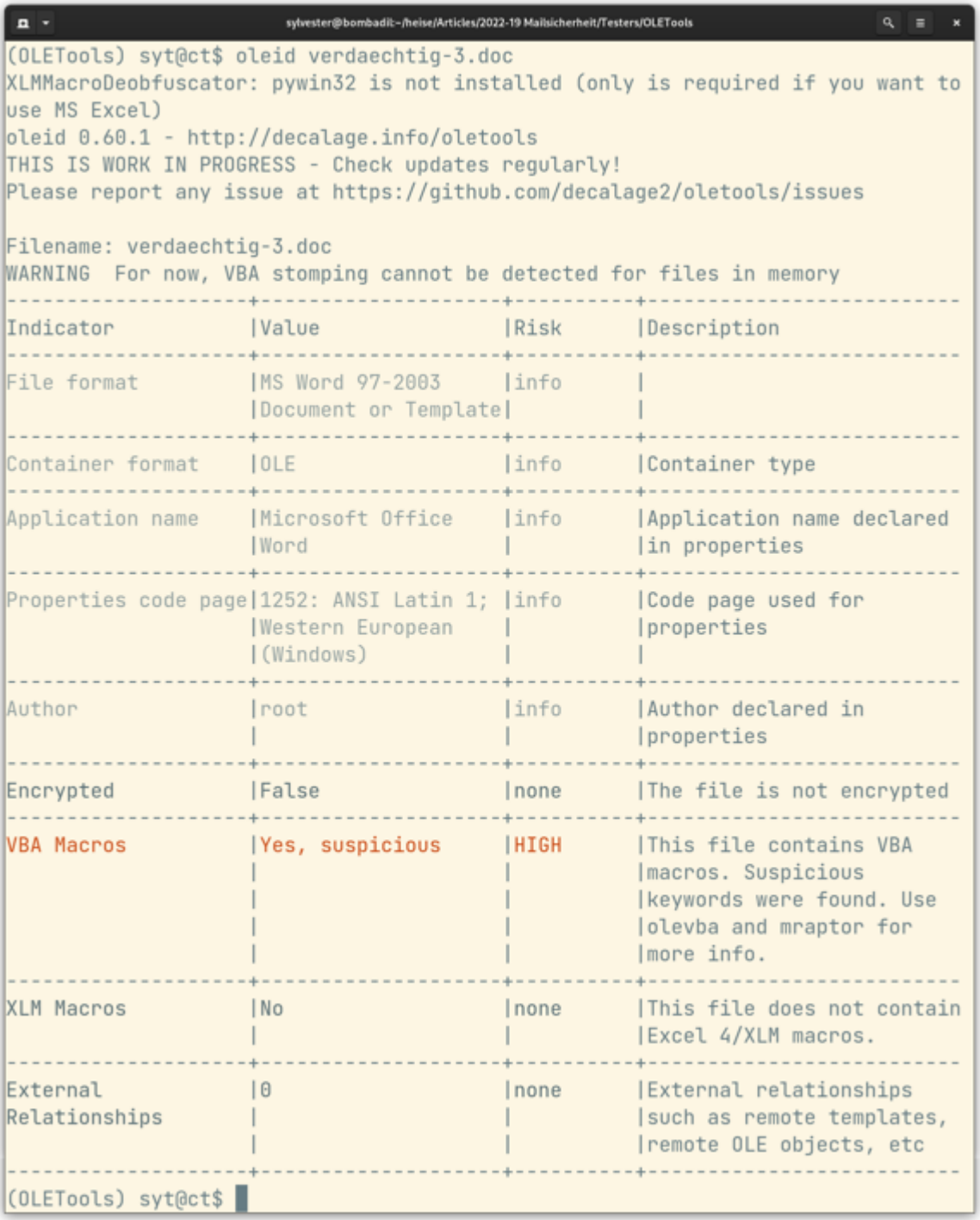
Dann ändern Sie einfach die Endung von .docx in .zip, öffnen das Archiv mit dem Zip-Programm Ihrer Wahl und inspizieren die Bilder im entpackten Verzeichnis /word/media/.

Wenn Sie die Office-Dateien aber auf Unbedenklichkeit prüfen und letztlich in Word oder Excel bearbeiten wollen oder wenn es um ältere Formate geht (DOC, XLS …), dann funktioniert dieser Trick nicht. Was funktioniert, sind die oletools des Programmierers Philippe Lagadec (siehe ct.de/yw2x). Auch dieser Werkzeugkasten nutzt Python, am einfachsten installieren Sie ihn über die Paketverwaltung pip [5]:

```
pip install -U oletools[full]
```

Die oletools lesen sowohl die alten Office-Binärformate (wie DOC) als auch die aktuelleren auf XML-Basis (etwa DOCX). Für eine Einschätzung einer verdächtigen Datei ist das Programm oleid gedacht. Wie pdfid gibt es einen Überblick über relevante Aspekte einer Office-Datei. Statt einer bloßen Liste liefert oleid allerdings eine Tabelle samt Risikoeinschätzung der Elemente und schreibt im Fall der Fälle auch noch Handlungsanweisungen dazu (siehe Bild auf S. 31) Einer Word-Datei ohne Makros, externe Objekte oder andere Spezialitäten attestiert das Programm beispielsweise ein geringes Risiko: In der Spalte Risk sind alle Werte „info“ oder „none“.

Im Testdokument des heise Mailchecks (siehe S. 21) erkennt oleid korrekterweise ein VBA-Makro und bewertet es mit dem Risiko „Medium“. In der letzten Spalte steht, warum und was Sie jetzt tun können: „No suspicious keyword was found. Use olevba and mraptor for more info.“ Es wurden also keine Alarmsignale im Makro selbst gefunden, für Details soll man die Werkzeuge olevba oder mraptor nutzen.

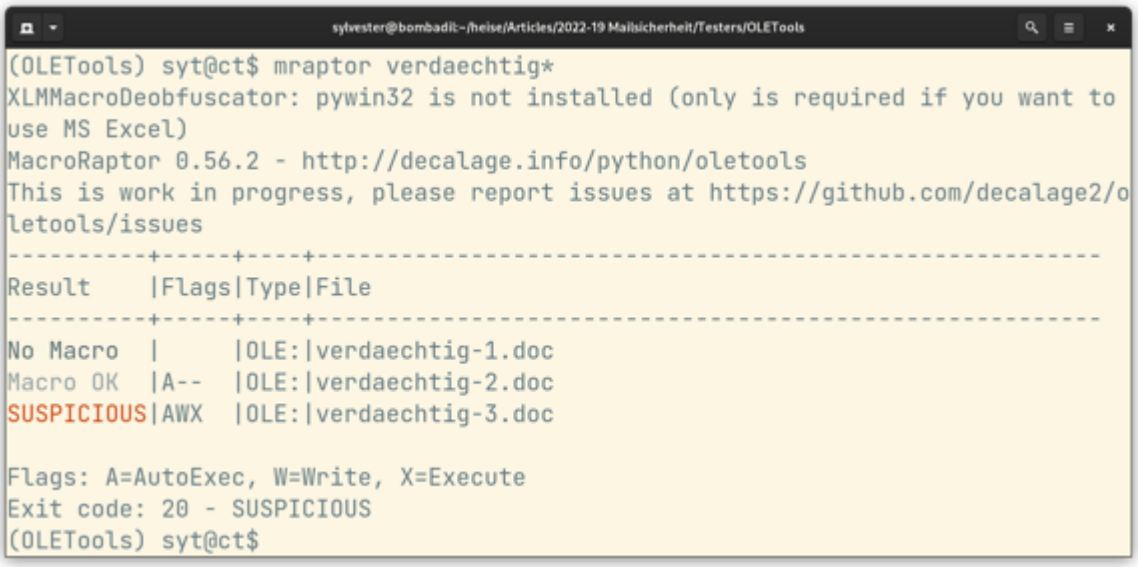


„VBA Macros: Yes, suspicious; Risk: HIGH“ meldet oleid und hat recht. Diese Datei ist tatsächlich höchst suspekt.
Ein Dokument mit einem höchst suspekten Makro, das versucht, eine Datei auf die Festplatte zu schreiben, bewertet oldid in Rot als „suspicious“ (verdächtig) und warnt in Großbuchstaben vor dem hohen Risiko, weil es verdächtige Schlüsselwörter im Makro gefunden hat.

Der wieder empfohlene Aufruf von mraptor erklärt den Verdacht näher: Das Makro wird automatisch ausgeführt („AutoExec“),

schreibt Daten („Write“) und versucht etwas außerhalb des Makro-Codes aufzurufen („Execute“). Folgerichtig kommt mraptor zu dem Schluss, dass die Datei verdächtig ist.

Wer es noch genauer wissen will, greift zum Werkzeug olevba. Es zeigt den enthaltenen Makrocode an, was aufschlussreich ist, wenn man Programmierkenntnisse hat. Zudem liefert olevba eine noch detailliertere Tabelle mit gefundenen problematischen Schlüsselwörtern und was sie bedeuten (siehe Listing auf S. 32).



mraptor kann man auch mehrere Dateien auf einmal vorwerfen. Er liefert dann eine Tabelle, ob Makros gefunden und als verdächtig bewertet wurden.

Listing: Output von olevba

```
+----------+--------------------+----------------------------
---------------+
|Type      |Keyword             |Description
|
+----------+--------------------+----------------------------
---------------+
|AutoExec  |AutoOpen            |Runs when the Word document
is opened      |
|Suspicious|Environ             |May read system environment
variables      |
|Suspicious|Open                |May open a file
```

```
|
|Suspicious|Write                  |May write to a file (if
combined with Open)  |
|Suspicious|Put                    |May write to a file (if
combined with Open)  |
|Suspicious|Binary                 |May read or write a binary
file (if combined |
|              |                                |with Open)
|
|Suspicious|CreateObject           |May create an OLE object
|
+----------+---------------------+-----------------------------
----------------+
```

Das Helferlein olevba extrahiert nicht nur Makrocode aus Office-Dateien (hier nicht gezeigt), sondern meldet auch, welche interessanten Begriffe sich im Code finden und worauf sie hindeuten.

Fazit

Auch ohne weitere Analyse müssen Sie keine Angst vor bösartigen Anhängen haben, wenn Sie die in diesem Artikel vorgestellten Werkzeuge einsetzen. Das Risiko, dass etwas den Filter von Dangerzone passiert, ist extrem gering. Übrigens sammeln sich unter Windows und macOS mit der Zeit immer mehr „Containers“ (mit Status „Exited“) und „Volumes“ in Docker Desktop an, zwei für jeden Aufruf von Dangerzone. Sie können die Einträge einfach ignorieren – oder aufräumen, wenn Sie die Unordnung stört. Löschen Sie einfach alle Exited-Container, die zugehörigen Volumes entsorgt Docker Desktop gleich mit. Dangerzone benötigt lediglich den Eintrag unter „Images“ und falls sie diesen versehentlich löschen sollten, legt das Programm ihn automatisch neu an.

Wenn Sie ein Dokument doch im Original öffnen müssen, dann reichen pdfid, oleid und Konsorten, um Gefahren zu wittern, bevor es zu spät ist. Das genügt für den Eigenschutz, aber wenn Sie die Neugierde packen sollte, dann sehen Sie sich

weiter in den Werkzeugkisten von Stevens und Lagadec um. Die enthalten noch viele weitere Programme, mit denen man den Inhalten von Office- und PDF-Dateien auf den Grund gehen kann. Ein Beispiel dafür werden wir in einer der kommenden Ausgaben beschreiben. *(syt@ct.de)*

1. Literatur
2. Ronald Eikenberg, Hacking-Stick, Kali Linux auf USB-Stick einrichten, c't 23/2021, S. 30
3. David Wolski, Buntes Hacker-Linux, Linux-Distribution: Parrot Security für Pentester und Hacker, c't 14/2020, S. 98
4. Sylvester Tremmel, Neue Stammkneipe, Wie Sie die passende Distribution für sich finden, c't 3/2022, S. 30
5. Knut von Walter, Von Snowden empfohlen, Das sicherheitsorientierte Betriebssystem Qubes OS im Test, c't 11/2022, S. 94
6. Ronald Eikenberg, Jan Mahn, Draufgebeamt, Python schnell und einfach einrichten, c't 5/2022, S. 20

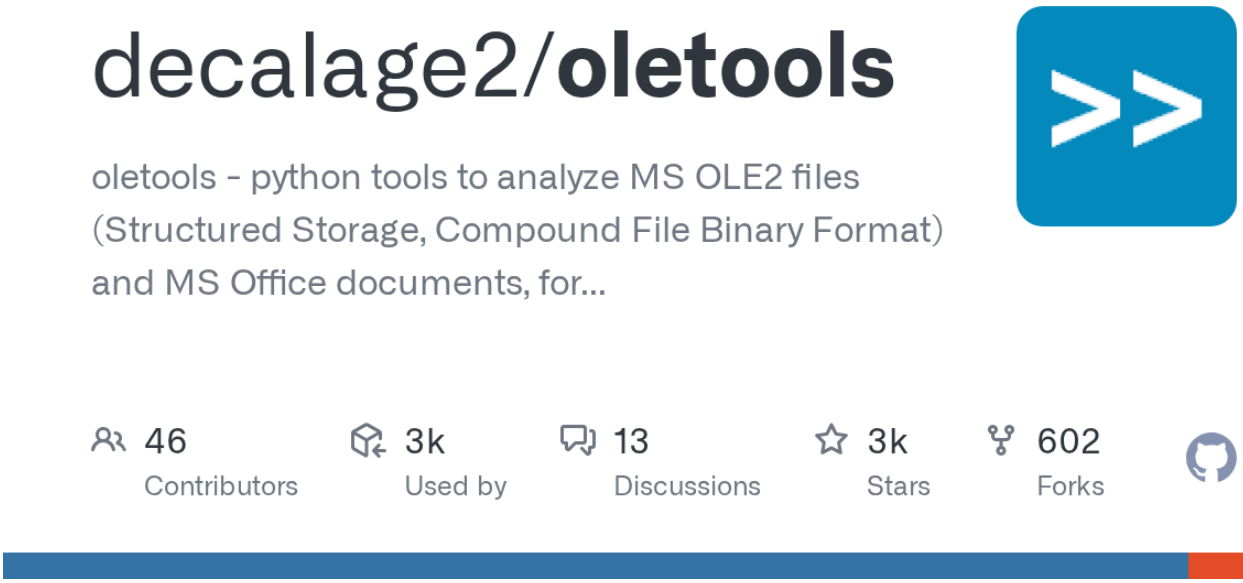
Downloads: ct.de/yw2x

Installing Dangerzone · freedomofpress/dangerzone Wiki

Take potentially dangerous PDFs, office documents, or images and convert them to safe PDFs — Installing Dangerzone · freedomofpress/dangerzone Wiki

PDF Tools

Here is a set of free YouTube videos showing how to use my tools: Malicious PDF Analysis Workshop. pdf-parser.py This tool will parse a PDF document to identify the fundamental elements used in the…



GitHub – decalage2/oletools: oletools – python tools to analyze MS OLE2 files (Structured Storage, Compound File Binary Format) and MS Office documents, for malware analysis, forensics and debugging.

oletools – python tools to analyze MS OLE2 files (Structured Storage, Compound File Binary Format) and MS Office documents, for malware analysis, forensics and debugging. – GitHub – decalage2/oleto…

E-Mails richtig versenden

Verschickt und für gut befunden

Mails so verschicken, dass man Ihnen vertraut

Damit Ihre Mails nicht ungeöffnet als Spam oder Phishing aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie folgende Tipps beherzigen, verschicken Sie Mails, die einen guten Eindruck hinterlassen und auch tatsächlich gelesen werden.

Von Ronald Eikenberg

Absender, Betreff und Anrede

Der erste Eindruck zählt. Stellen Sie sicher, dass Sie einen aussagekräftigen Absendernamen in Ihrem Mailkonto eingestellt haben, etwa Vorname Nachname (Firma). Geben Sie Ihrer Mail einen sinnvollen, möglichst konkreten Betreff: anstatt „Anfrage“ beispielsweise „Kundenanfrage Ersatzteil XY für Modell Z“.

Beginnen Sie die Mail nach Möglichkeit mit einer individuellen Ansprache mit Person oder Firma, die Sie erreichen möchten. Stellen Sie eine Signatur mit Ihrem Namen, der Firma und Rufnummer für Rückfragen ein. So können die Adressaten Ihre Mails zumindest von plumperen Fälschungen leicht unterscheiden.

Auf Empfänger achten

Überprüfen Sie vor dem Abschicken die Empfängerfelder „An“, „CC“ und „BCC“. Durch die automatische Vervollständigung Ihres Mailclients schleicht sich hier schon mal ein falscher Empfänger ein. Beim Beantworten von Mails sollten Sie in den Feldern gründlich ausmisten. Das gilt insbesondere für Antworten auf Mails, die an einen großen Empfängerkreis gerichtet waren. Denn die Antwort auf die Rundmail des Chefs

muss in vielen Fällen nicht erneut die große Runde machen.

Wenn Sie mehrere Empfänger anmailen, die nichts miteinander zu tun haben, sollten Sie die Empfängeradresse unbedingt in das Feld BCC (Blindkopie) eintragen, damit die Empfänger nicht die gesamte Adressliste einsehen können. Wenn Sie „An“ oder „CC“ nutzen, geben Sie die Empfängerliste preis und handeln sich ein Datenschutzproblem ein.

Text statt HTML

HTML-Mails bergen unnötige Risiken: Der Empfänger sieht nicht auf den ersten Blick, auf welche Webadresse ein Link wirklich zeigt und von externen Servern eingebettete Inhalte sind entweder ein Datenschutzrisiko oder werden vom Empfängerclient nicht angezeigt. Verfassen Sie Ihre Mails daher besser im Textformat. Falls Sie auf eine URL verweisen möchten, sollten Sie Linkverkürzer wie TinyURL meiden, damit der Empfänger der Mail auf Anhieb weiß, wohin Sie ihn schicken möchten.

Vorsicht bei Anhängen

Von Mailanhängen geht eine große Gefahr aus. Phisher verschicken insbesondere Office-Dokumente und ausführbare Dateien, um neue Opfer in die Falle zu locken. Verschicken Sie Dokumente deshalb am besten im PDF-Format. Es hat sich als risikoarmes Austauschformat durchgesetzt. Microsoft Office und viele andere Anwendungen können Ihre Dokumente im PDF-Format speichern, zum Beispiel über die Druckfunktion. Falls es doch mal ein Office-Format sein muss, dann wählen Sie bevorzugt die Formate, die auf X enden: DOCX, PPTX, XLSX. Diese können keine Makros enthalten.

Vermeiden Sie insbesondere ausführbare Dateiformate wie EXE. Dabei handelt es sich häufig um Malware, weshalb Mails mit ausführbaren Anhängen oft aussortiert werden. Kündigen Sie unerwartete und ungewöhnliche Mailanhänge am besten über einen anderen Kommunikationskanal an. Vermeiden Sie große Anhänge,

da diese oft nicht ankommen.

Mails signieren

Im besten Fall signieren Sie ausgehende Mails digital vor dem Versand mit OpenPGP oder S/MIME. So hat der Empfänger die Chance, zu verifizieren, dass die Mail tatsächlich von Ihnen stammt. Mailverschlüsselung sollten Sie nur nutzen, wenn Sie sicher sind, dass der Empfänger die Mail tatsächlich entschlüsseln kann. Die Verbindung zum Mailserver sollte in jedem Fall transportverschlüsselt sein (möglichst SSL/TLS), was bei den meisten Mailanbietern inzwischen jedoch Standard ist.

Andere Kanäle nutzen

E-Mails sind ein denkbar schlechtes Transportmedium für wichtige Informationen: Sie werden meist unsigniert übertragen, deshalb kann der Empfänger Ihre Mail nur mit Mühe zweifelsfrei von Phishing unterscheiden. Nutzen Sie daher auch andere Kommunikationskanäle, die Ihnen zur Verfügung stehen. Diese sind häufig besser geeignet.

In Unternehmen gibt es für interne Kommunikation oft Chat- oder Kollaborationssoftware wie Teams, Slack oder Rocket.Chat, im Zweifel können Sie auch zum Telefonhörer greifen. Messenger-Apps wie Signal oder WhatsApp sind ebenfalls besser als Mail, da die Nachrichten automatisch Ende-zu-Ende-verschlüsselt sind und der Empfänger den Absender überprüfen kann. Auch Dateien können Sie gut über diese Kanäle weitergeben.

Kurzlink zu diesem Artikel für Ihre Mail-Signatur: ct.de/sicher-mailen

(rei@ct.de)

26.08.2022 06:00 Uhr

c’t Magazin

Von

- Ronald Eikenberg

Damit Ihre Mails nicht ungeöffnet als Spam oder Phishing aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie folgende Tipps beherzigen, verschicken Sie Mails, die einen guten Eindruck hinterlassen und auch tatsächlich gelesen werden.

Absender, Betreff und Anrede

Der erste Eindruck zählt. Stellen Sie sicher, dass Sie einen aussagekräftigen Absendernamen in Ihrem Mailkonto eingestellt haben, etwa Vorname Nachname (Firma). Geben Sie Ihrer Mail einen sinnvollen, möglichst konkreten Betreff: anstatt „Anfrage“ beispielsweise „Kundenanfrage Ersatzteil XY für Modell Z“.

Beginnen Sie die Mail nach Möglichkeit mit einer individuellen Ansprache mit Person oder Firma, die Sie erreichen möchten. Stellen Sie eine Signatur mit Ihrem Namen, der Firma und Rufnummer für Rückfragen ein. So können die Adressaten Ihre Mails zumindest von plumperen Fälschungen leicht unterscheiden.

Auf Empfänger achten

Überprüfen Sie vor dem Abschicken die Empfängerfelder „An“,

„CC“ und „BCC“. Durch die automatische Vervollständigung Ihres Mailclients schleicht sich hier schon mal ein falscher Empfänger ein. Beim Beantworten von Mails sollten Sie in den Feldern gründlich ausmisten. Das gilt insbesondere für Antworten auf Mails, die an einen großen Empfängerkreis gerichtet waren. Denn die Antwort auf die Rundmail des Chefs muss in vielen Fällen nicht erneut die große Runde machen.

Wenn Sie mehrere Empfänger anmailen, die nichts miteinander zu tun haben, sollten Sie die Empfängeradresse unbedingt in das Feld BCC (Blindkopie) eintragen, damit die Empfänger nicht die gesamte Adressliste einsehen können. Wenn Sie „An“ oder „CC“ nutzen, geben Sie die Empfängerliste preis und handeln sich ein Datenschutzproblem ein.

Text statt HTML

HTML-Mails bergen unnötige Risiken: Der Empfänger sieht nicht auf den ersten Blick, auf welche Webadresse ein Link wirklich zeigt und von externen Servern eingebettete Inhalte sind entweder ein Datenschutzrisiko oder werden vom Empfängerclient nicht angezeigt. Verfassen Sie Ihre Mails daher besser im Textformat. Falls Sie auf eine URL verweisen möchten, sollten Sie Linkverkürzer wie TinyURL meiden, damit der Empfänger der Mail auf Anhieb weiß, wohin Sie ihn schicken möchten.

Vorsicht bei Anhängen

Von Mailanhängen geht eine große Gefahr aus. Phisher verschicken insbesondere Office-Dokumente und ausführbare Dateien, um neue Opfer in die Falle zu locken. Verschicken Sie Dokumente deshalb am besten im PDF-Format. Es hat sich als risikoarmes Austauschformat durchgesetzt. Microsoft Office und viele andere Anwendungen können Ihre Dokumente im PDF-Format speichern, zum Beispiel über die Druckfunktion. Falls es doch mal ein Office-Format sein muss, dann wählen Sie bevorzugt die Formate, die auf X enden: DOCX, PPTX, XLSX. Diese können keine Makros enthalten.

Vermeiden Sie insbesondere ausführbare Dateiformate wie EXE. Dabei handelt es sich häufig um Malware, weshalb Mails mit ausführbaren Anhängen oft aussortiert werden. Kündigen Sie unerwartete und ungewöhnliche Mailanhänge am besten über einen anderen Kommunikationskanal an. Vermeiden Sie große Anhänge, da diese oft nicht ankommen.

Mails signieren

Im besten Fall signieren Sie ausgehende Mails digital vor dem Versand mit OpenPGP oder S/MIME. So hat der Empfänger die Chance, zu verifizieren, dass die Mail tatsächlich von Ihnen stammt. Mailverschlüsselung sollten Sie nur nutzen, wenn Sie sicher sind, dass der Empfänger die Mail tatsächlich entschlüsseln kann. Die Verbindung zum Mailserver sollte in jedem Fall transportverschlüsselt sein (möglichst SSL/TLS), was bei den meisten Mailanbietern inzwischen jedoch Standard ist. Lesen Sie auch

- Gefahrloser Umgang mit E-Mails

Andere Kanäle nutzen

E-Mails sind ein denkbar schlechtes Transportmedium für wichtige Informationen: Sie werden meist unsigniert übertragen, deshalb kann der Empfänger Ihre Mail nur mit Mühe zweifelsfrei von Phishing unterscheiden. Nutzen Sie daher auch andere Kommunikationskanäle, die Ihnen zur Verfügung stehen. Diese sind häufig besser geeignet.

In Unternehmen gibt es für interne Kommunikation oft Chat- oder Kollaborationssoftware wie Teams, Slack oder Rocket.Chat, im Zweifel können Sie auch zum Telefonhörer greifen. Messenger-Apps wie Signal oder WhatsApp sind ebenfalls besser als Mail, da die Nachrichten automatisch Ende-zu-Ende-verschlüsselt sind und der Empfänger den Absender überprüfen kann. Auch Dateien können Sie gut über diese Kanäle weitergeben.

Geben Sie die Tipps weiter! Kurzlink zu diesem Artikel für Ihre Mail-Signatur: **https://ct.de/sicher-mailen**