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

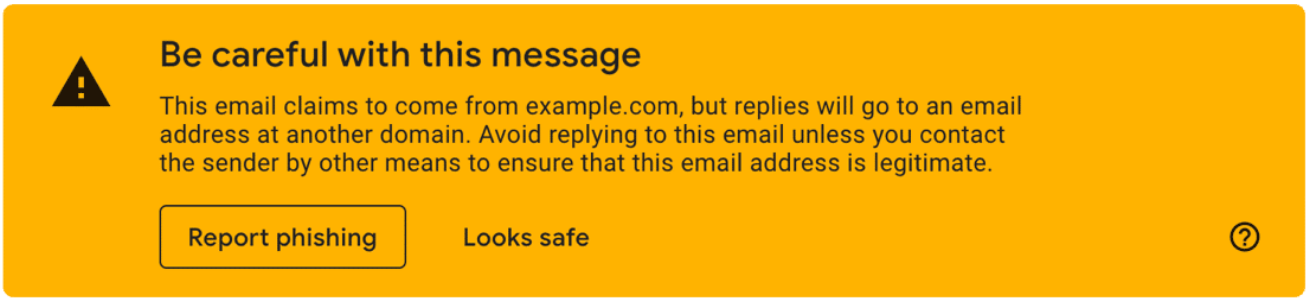
stehen, wenden Sie sich an Ihren Host und bitten Sie ihn, Sie auf einen anderen Server zu verschieben.

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.

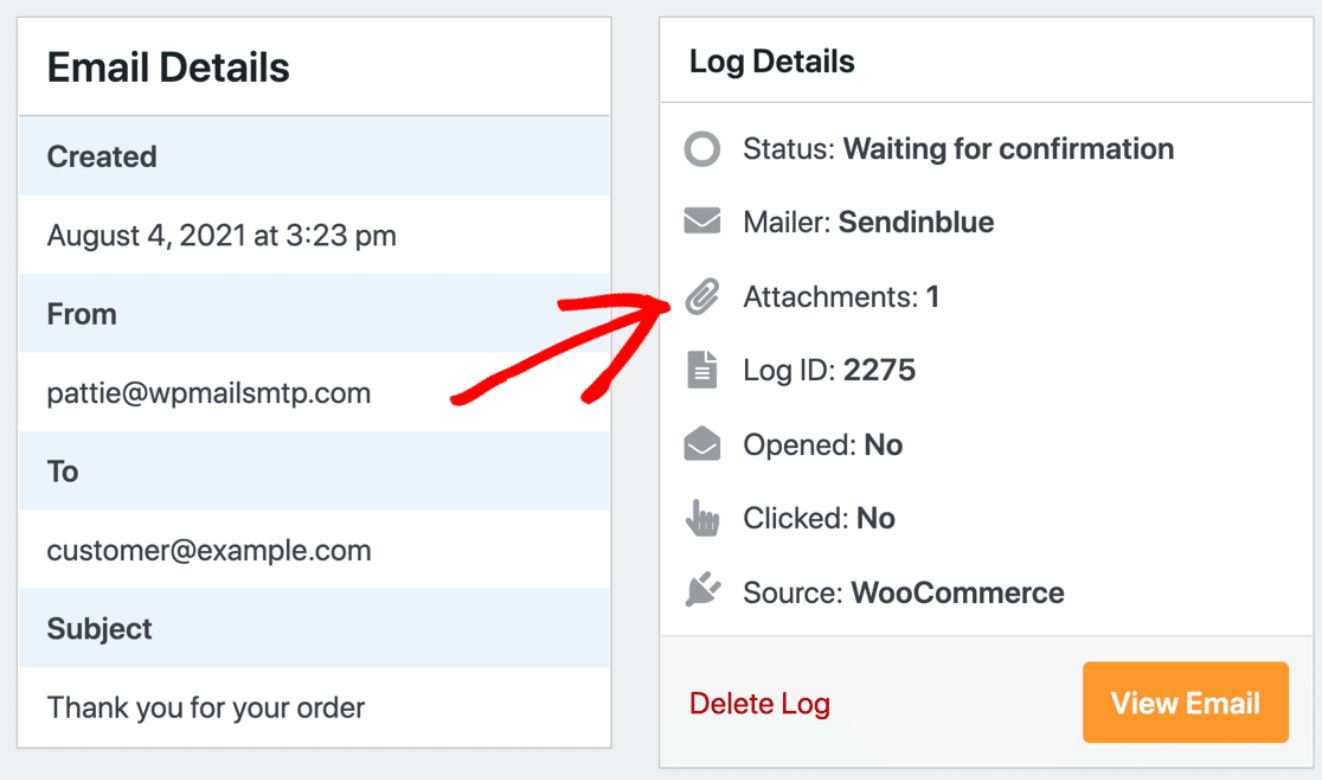
Senden Sie Bilder oder Anhänge?

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?

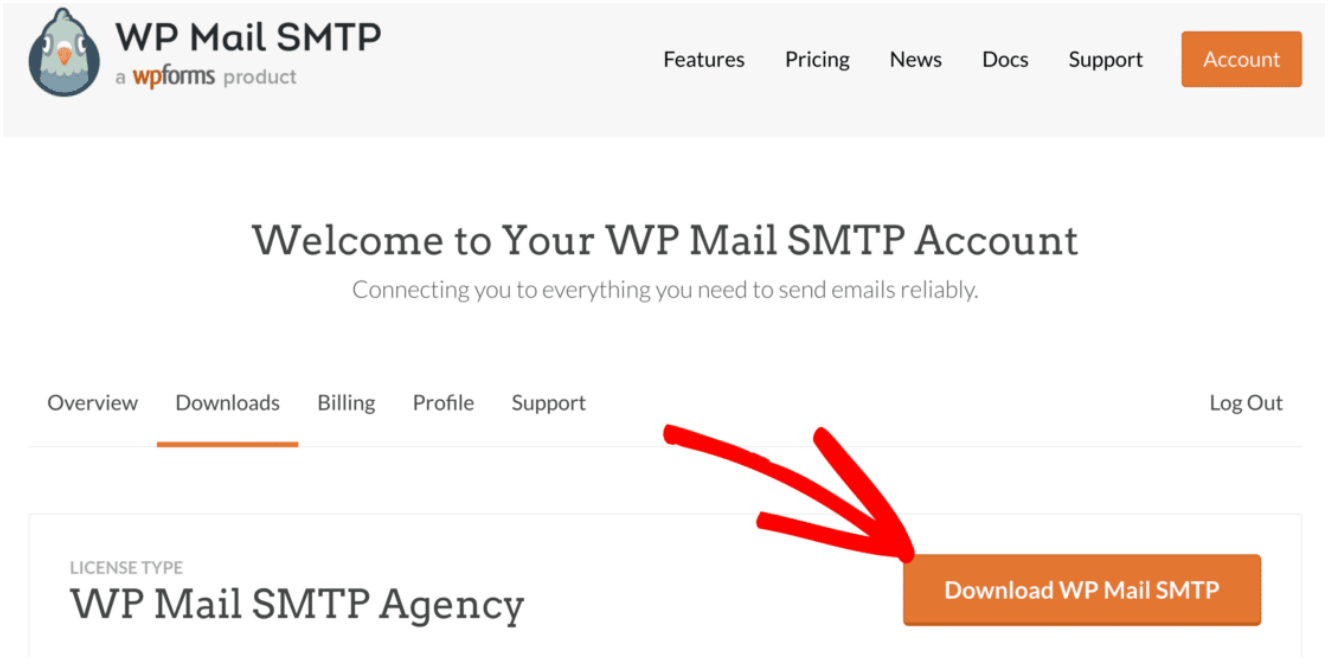
Wenn keines dieser Probleme auf Sie zutrifft, liegt das Problem wahrscheinlich einfach an der fehlenden Authentifizierung. Wir können das mit WP Mail SMTP beheben. Diese Lösung funktioniert für alle auf Ihrer Website installierten Plugins, die E-Mails versenden.

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.

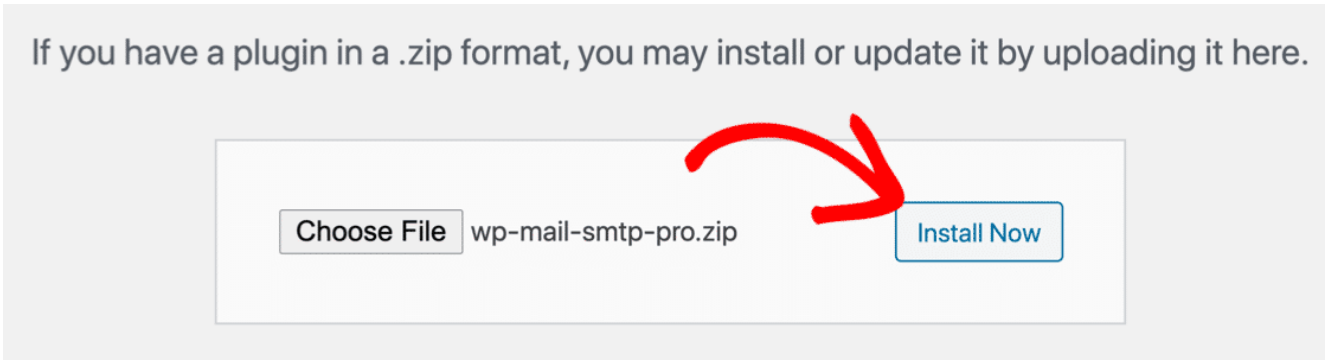
2. Installieren Sie das WP Mail SMTP-Plugin

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.

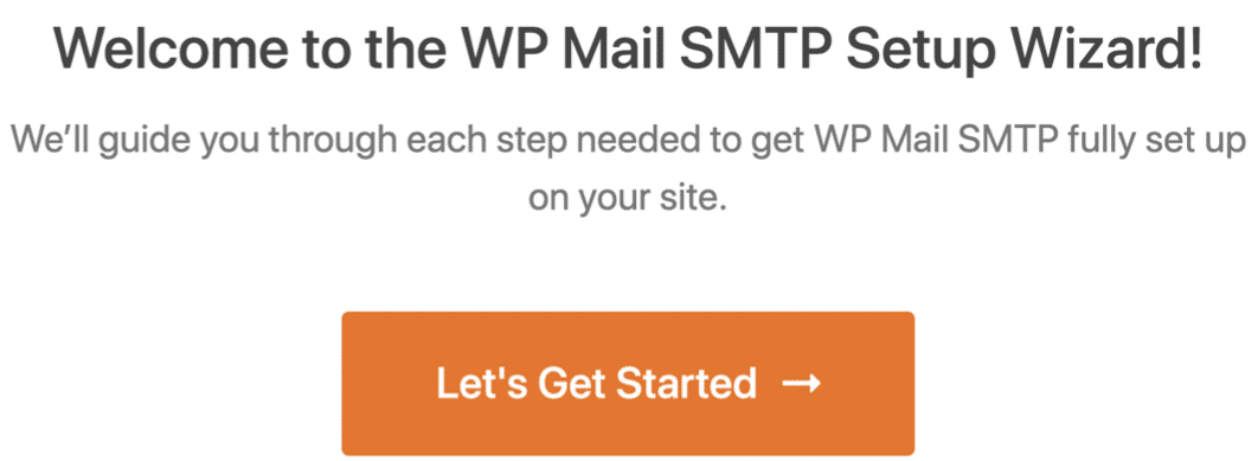
Brauche Hilfe?

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

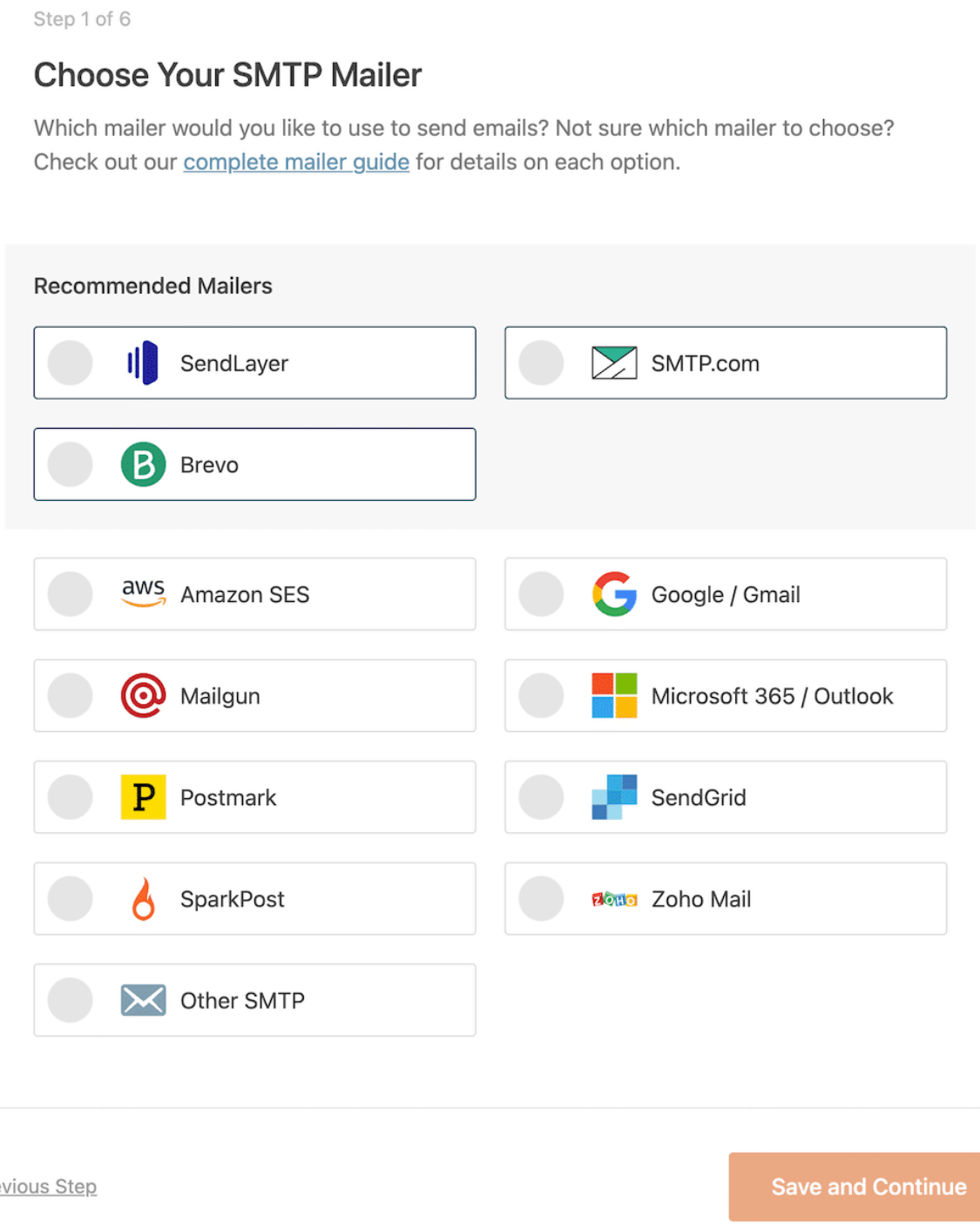
3. Wählen Sie einen E-Mail-Anbieter für WordPress

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.

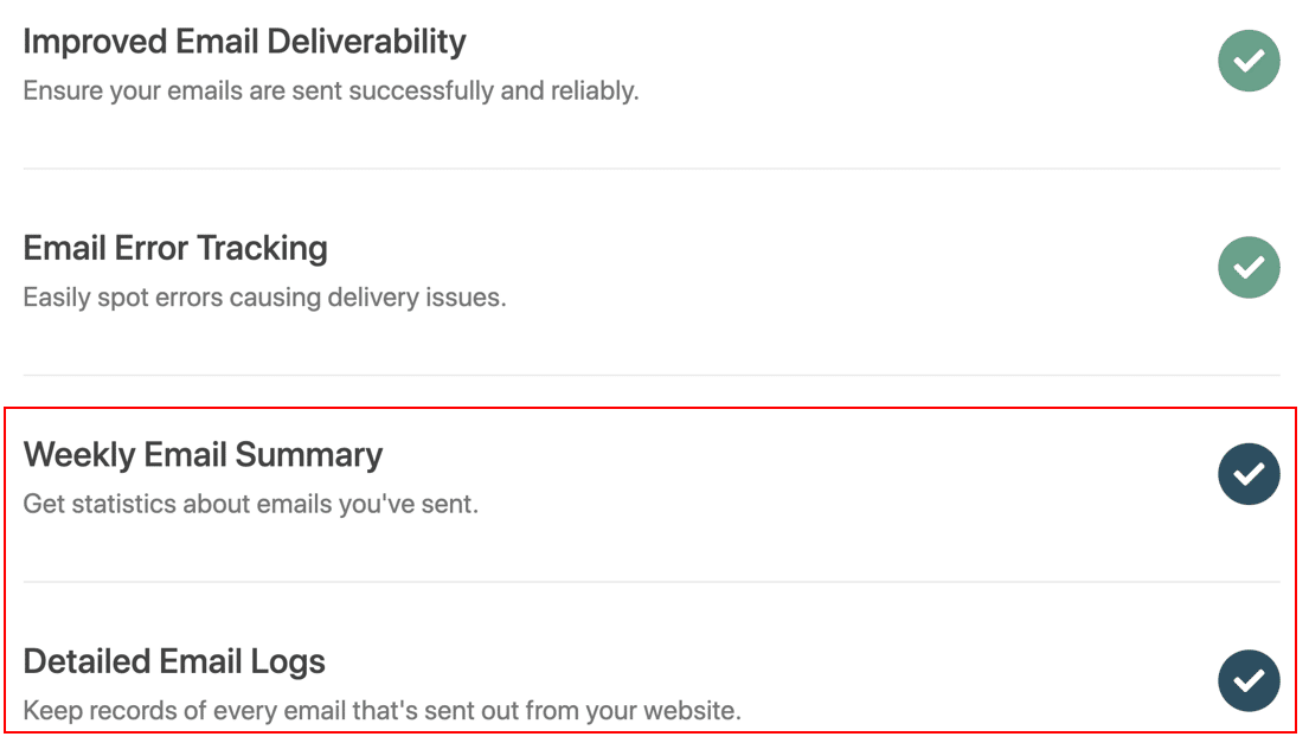
Im Vergleich zu Gmail oder Outlook sind sie auch einfach einzurichten.

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

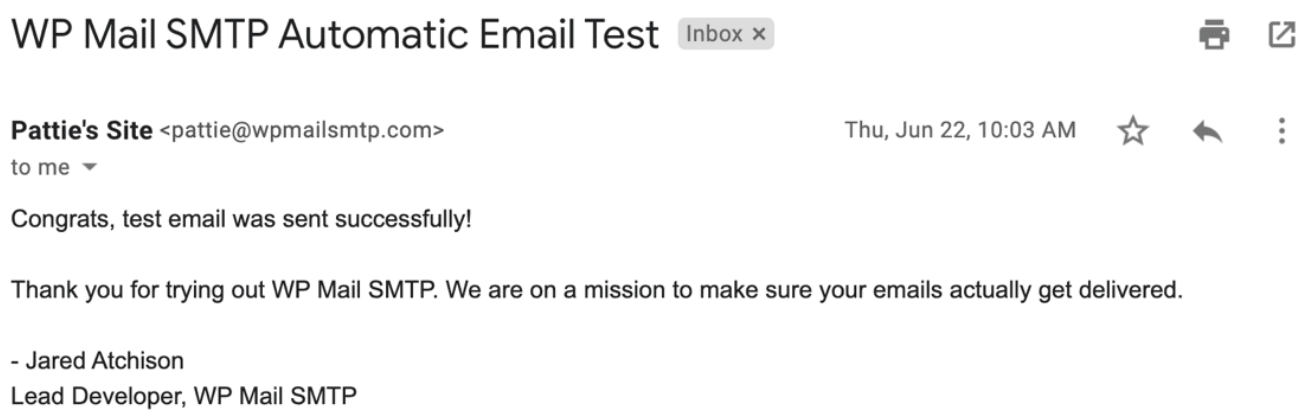


Wenn Sie diese Funktionen aktivieren, schalten Sie eine Menge zusätzlicher Funktionen in WP Mail SMTP frei:

- **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.

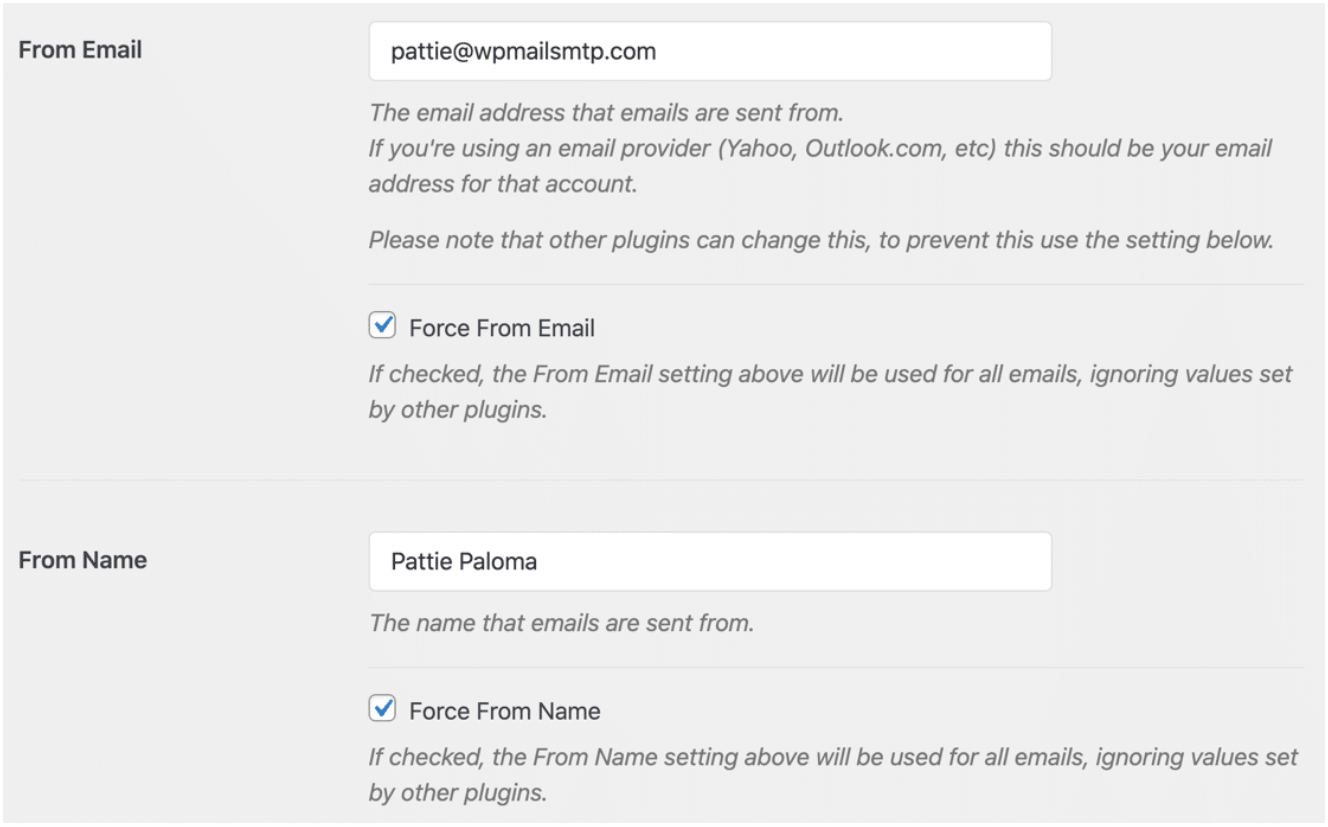


Sie werden feststellen, dass WP Mail SMTP Sie gefragt hat, ob Sie den Formularnamen erzwingen möchten. Werfen wir einen Blick darauf, was das bedeutet.

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

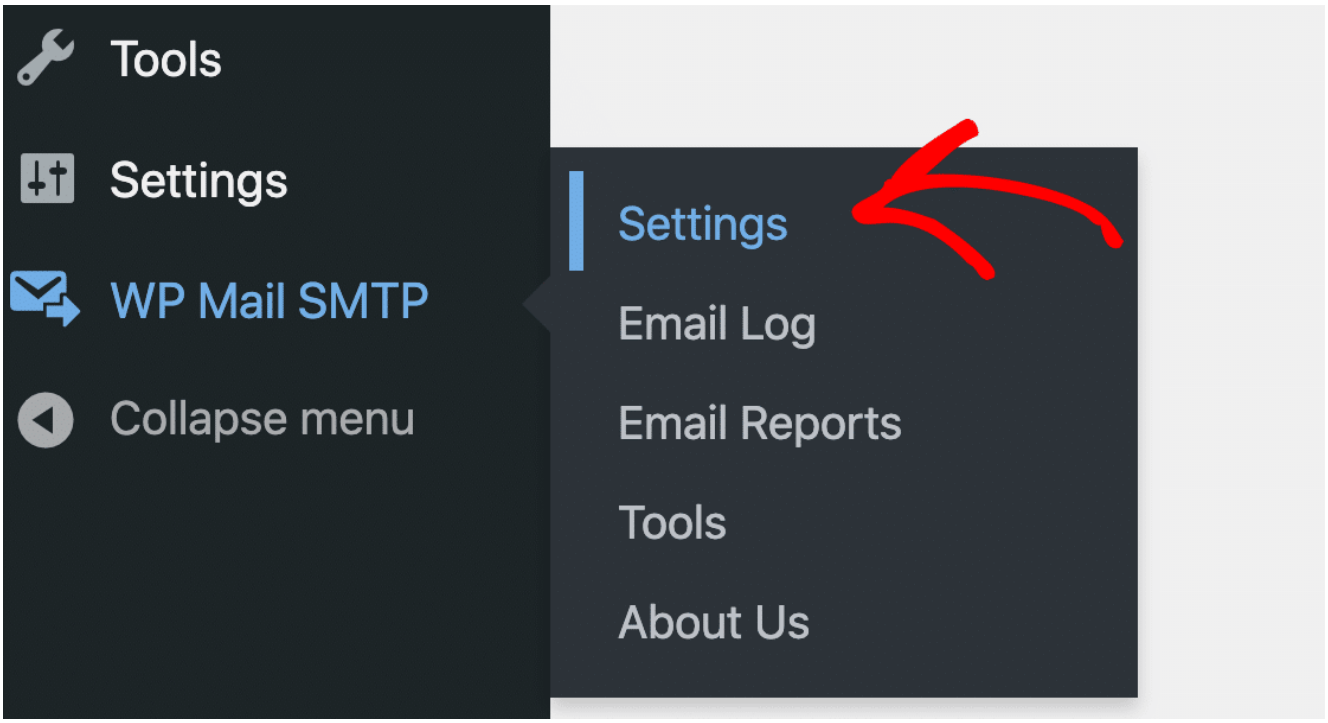
Der **Absendername** und **die Absender-E-Mail** sind wichtige Einstellungen beim Versenden von E-Mails von Ihrer WordPress-Website.

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** .

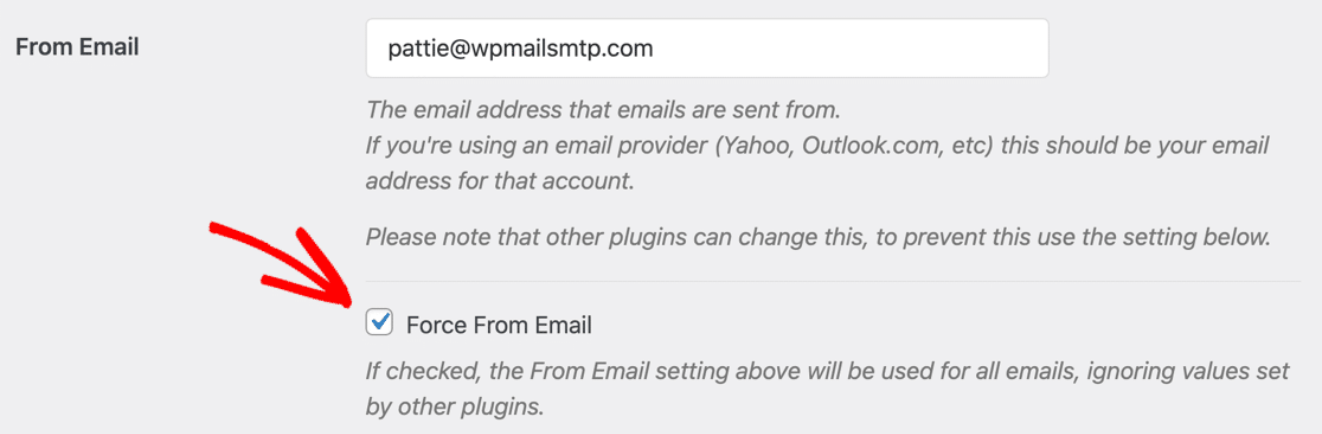


eingeben **Absender-E-Mail** Bei einigen Mailprogrammen können Sie

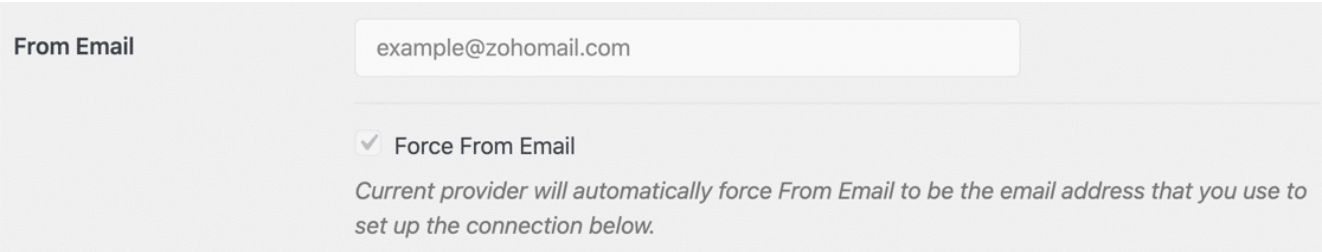
eine beliebige . In diesem Fall sollten Sie eine E-Mail-Adresse der Domäne verwenden, die Sie bei Ihrem E-Mail-Anbieter authentifiziert haben.

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.



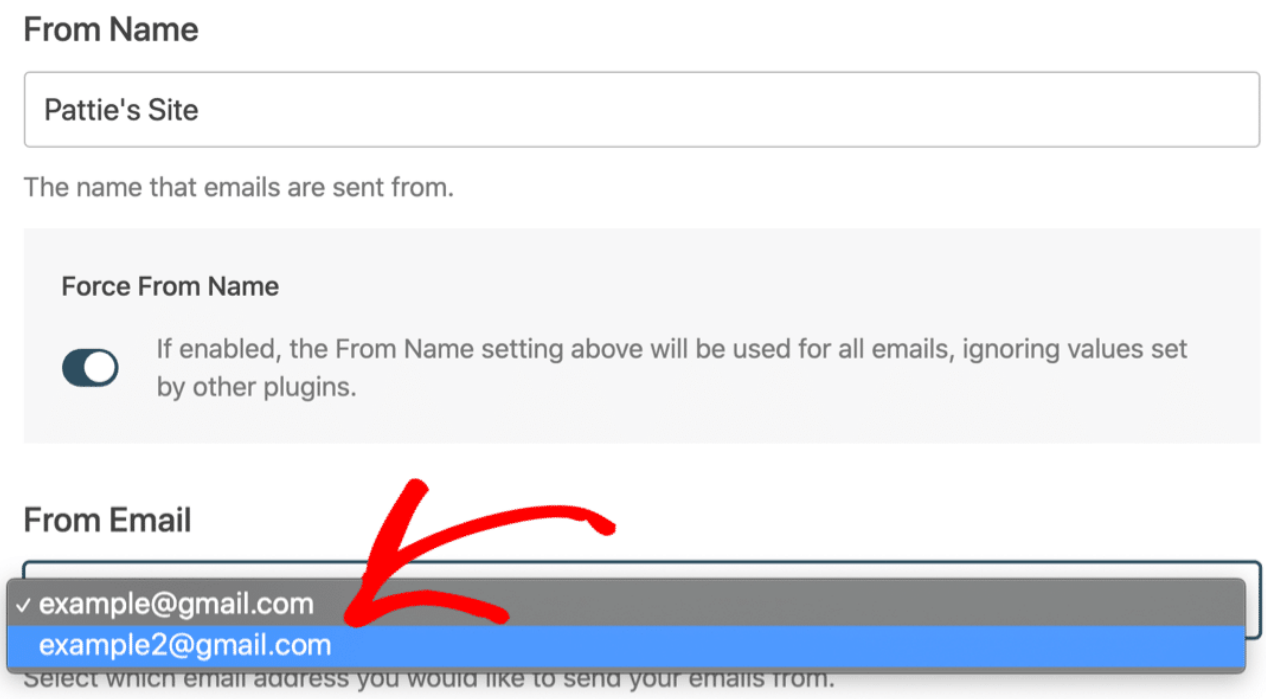
Wenn die **Absender-E-Mail** ausgegraut ist, können Sie sie nicht ändern.



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)

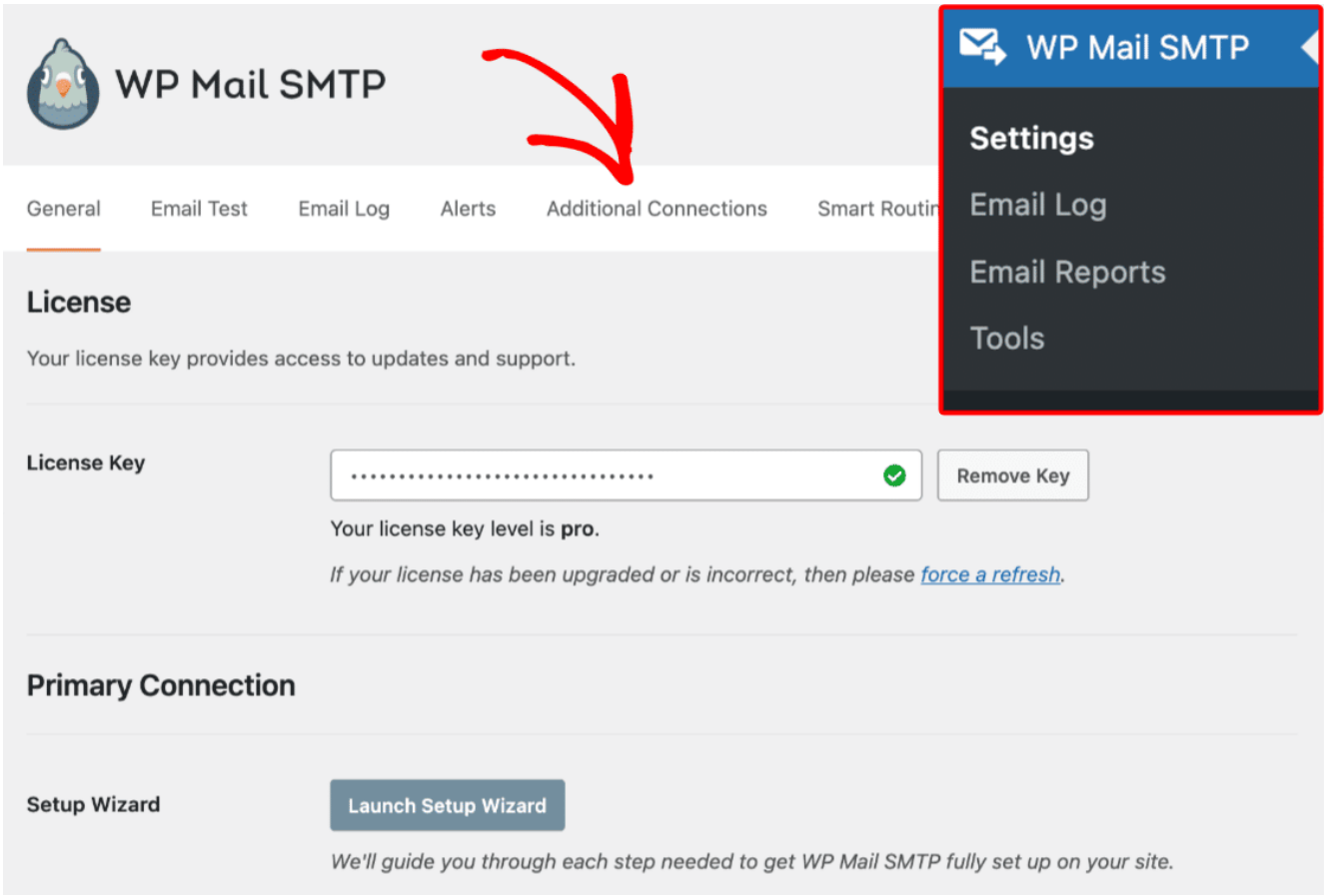
Mit WP Mail SMTP Pro können Sie Smart Routing einrichten. Mit dieser Funktion können Sie unterschiedliche Mailer für unterschiedliche E-Mail-Typen verwenden.

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.

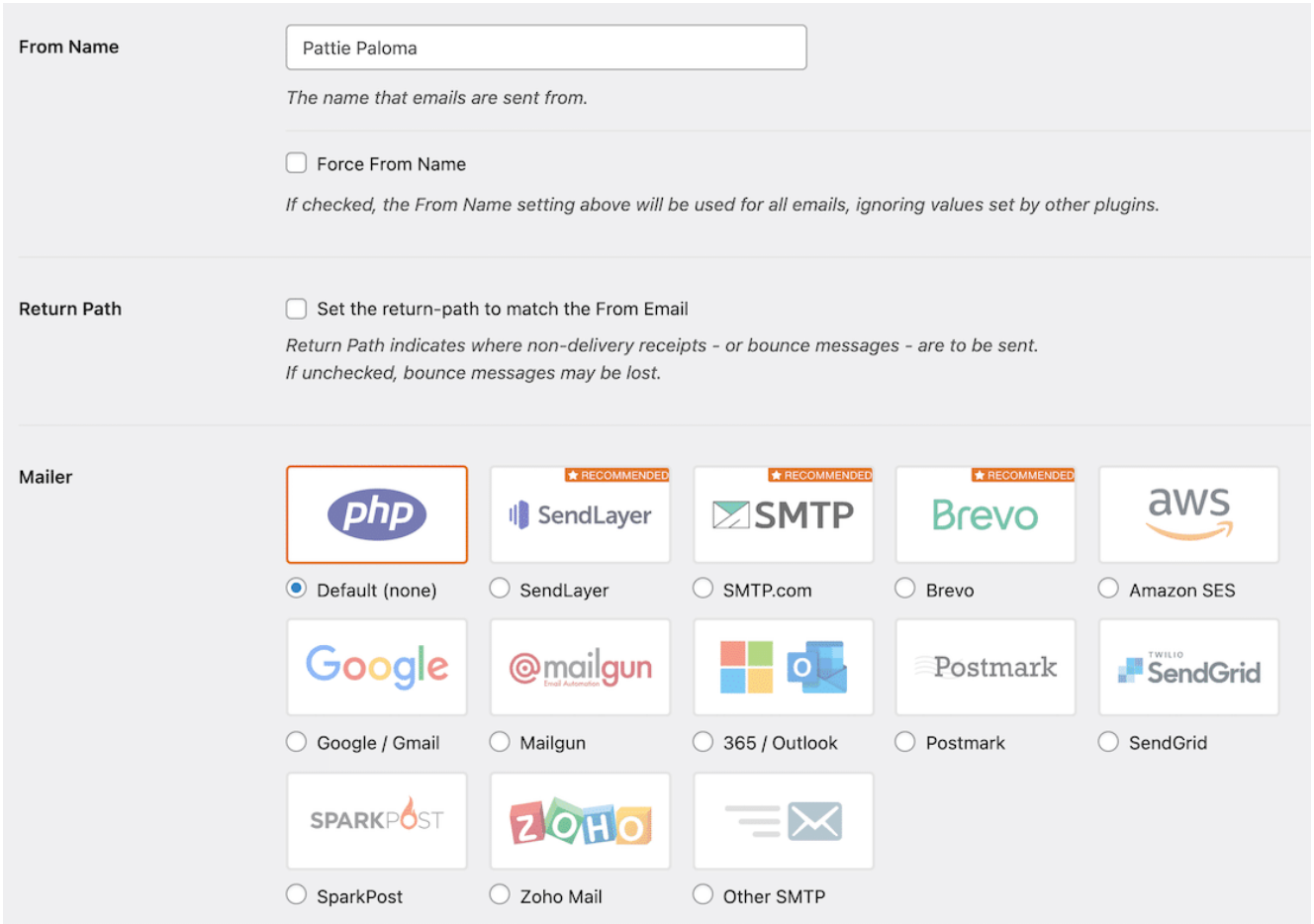
Wenn Sie den richtigen Mailer für die Art der E-Mails auswählen, die Sie versenden möchten, können Sie verhindern,

dass Ihre E-Mails im Spam landen.

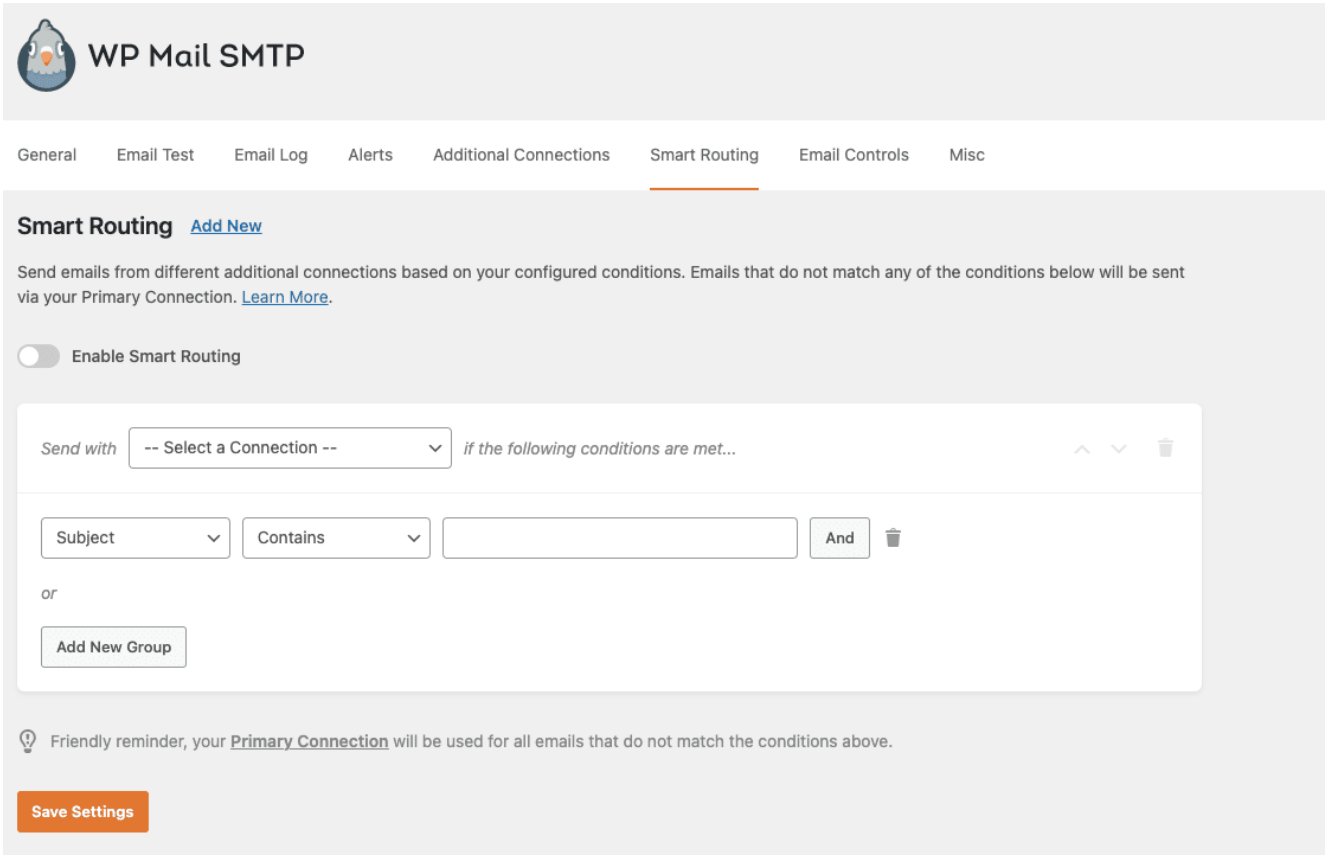
Um Smart Routing einzurichten, müssen Sie zunächst eine zusätzliche Verbindung hinzufügen. Gehen Sie zu **WP Mail SMTP » Einstellungen** und klicken Sie auf **Zusätzliche Verbindungen** .



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.

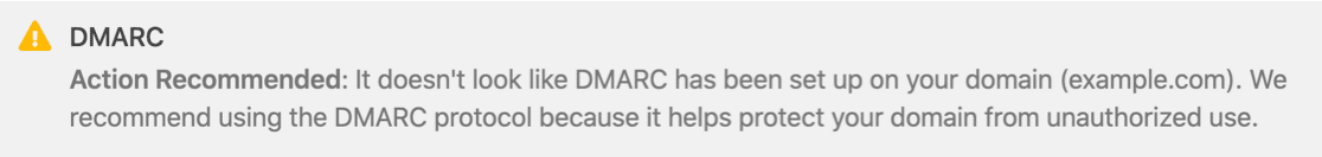
Weitere Einzelheiten finden Sie in unserem Leitfaden zu Smart Routing .

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.

Spuren kompromittierter E-Mail-Konten analysieren

Spuren kompromittierter E-Mail-Konten analysieren

Nachdem der erste Teil des Playbooks zu gekaperten E-Mail-Accounts zeigte, wie man die Logs mithilfe von Microsofts zentraler Logfunktion einsammelt, erklärt der zweite Teil, wie man sie auf verdächtige Vorgänge auswertet und welche Rückschlüsse sich daraus ziehen lassen.
Nachdem der erste Teil des Playbooks zu gekaperten E-Mail-Accounts zeigte, wie man die Logs mithilfe von Microsofts zentraler Logfunktion einsammelt, erklärt der zweite Teil, wie man sie auf verdächtige Vorgänge auswertet und welche Rückschlüsse sich daraus ziehen lassen.

- Beim ersten Anzeichen verdächtiger Aktivität rund um E-

Mail-Accounts sollte man IT-forensische Untersuchungen anstoßen, um zu verstehen, was genau passiert ist. Ausgangspunkt der Analyse sind die gesammelten Logdaten und Artefakte.

- Aussagekräftig im Hinblick auf Eindringlinge ins Firmennetz sind unter anderem fehlgeschlagene Anmeldevorgänge, eingerichtete Mailweiterleitungen oder neu vergebene Berechtigungen. Solche Hinweise sollten sorgfältig untersucht werden.
- Die Ursachenforschung und eine Nachbereitung sind das A und O nach der Bewältigung von Sicherheitsvorfällen. Daraus abgeleitete technische Maßnahmen sowie die Sensibilisierung von Mitarbeitenden sollen künftige Angriffe zumindest erschweren.

Die umfassendste Datenquelle zur Analyse von Unregelmäßigkeiten oder Verdachtsmomenten für einen Sicherheitsvorfall bietet Microsofts zentrale Logfunktion Unified Audit Log (UAL). Hier werden Benutzer- und Administratoraktivitäten auch unabhängig vom Einsatz zusätzlicher Produkte wie Microsoft Sentinel oder Microsoft Defender for Identity aufgezeichnet (wie die Logdaten im Detail gesichert werden, beschreibt [1]). Die nachfolgenden Schritte zeigen, wie man bei der Analyse vorgeht und die Logdaten sinnvoll durchsuchen kann.

Schritt 4: Untersuchen der Anmeldeaktivitäten

Jedes Mal, wenn sich ein Benutzer bei seinem Konto anmeldet, wird ein Ereignis im UAL erstellt. Dieses Ereignis enthält wichtige Informationen, etwa die Quell-IP-Adresse, die sich unter anderem für eine geografische Suche verwenden lässt. Die Ergebnisse lassen sich mit den erwarteten geografischen Standorten eines Unternehmens und seiner Nutzer vergleichen. Wenn zum Beispiel ein Unternehmen in Deutschland ansässig ist

und keine Niederlassung in Asien hat oder das VPN des Unternehmens nicht zu einer IP-Adresse in Asien auflöst, würde man keine Ereignisse aus Asien erwarten. Daher wären Anmeldungen aus Asien in diesem Fall verdächtig.

Natürlich kann es auch sein, dass ein Mitarbeiter sich im Urlaub in Asien befindet und sein Firmenhandy dabeihat, dennoch erfordern diese Ausreißer Aufmerksamkeit. Verdächtige Anmeldungen kann man durch die Suche nach bestimmten Schlüsselwörtern im UAL entdecken. Neben der IP-Adresse liefern auch die Uhrzeit sowie Informationen zum verwendeten Gerät (UserAgent: Betriebssystem, Browser et cetera) gute Anhaltspunkte. Ob das verwendete Gerät dem Unternehmen bekannt ist und von der IT verwaltet wird oder nicht, lässt sich ebenfalls den Ereignissen entnehmen. Für die Suche nach verdächtigen Anmeldeereignissen kann man folgende Schlüsselwörter verwenden:

Schlüsselwort	**Bedeutung des Logeintrags**
MailboxLogin	Hinweis auf einen erfolgreichen Log-in-Vorgang
UserLoggedIn	Hinweis auf einen erfolgreichen Log-in-Vorgang
UserLoginFailed	Hinweis auf einen fehlgeschlagenen Log-in-Vorgang
IdsLocked	Hinweis auf einen Brute-Force-Angriff. Der Account wurde gesperrt, da zur viele fehlgeschlagene Anmeldeversuche unternommen wurden.
UserKey=“Not Available“	Hinweis auf einen Brute-Force-Angriff. Die Anmeldung ist fehlgeschlagen, da der Benutzeraccount nicht existiert.

Neben Ereignissen rund um das Log-in können auch Fehlermeldungen zur Multi-Faktor-Authentisierung (MFA) Indikatoren für mögliche schädliche Aktivitäten sein. Ein Angreifer könnte das Passwort eines Anwenders ausgespäht

haben, um dann an der MFA-Abfrage zu scheitern. UAL-Einträge mit den folgenden Schlüsselwörtern sollten näher untersucht werden:

Schlüsselwort	Bedeutung des Logeintrags
UserStrongAuthClientAuthNRequired	Der Benutzer wird zur Bestätigung einer MFA-Abfrage aufgefordert.
UserStrongAuthClientAuthNRequiredInterrupt	fehlgeschlagene MFA-Abfrage

Schritt 5: Untersuchen von Weiterleitungsregeln

Nachdem ein Angreifer einen Benutzeraccount kompromittiert hat, erstellt er häufig Weiterleitungsregeln, um eingehende E-Mails an ein externes Postfach zu schicken. Auf diese Weise kann er die Aktivitäten eines Opfers kontinuierlich überwachen, ohne sich aktiv in das Konto einzuloggen. Selbst wenn das Passwort eines kompromittierten Kontos zurückgesetzt wird, kann der Angreifer weiterhin E-Mails mitlesen.

Ebenfalls beliebt ist der Einsatz von Weiterleitungsregeln zum automatisierten Löschen von E-Mails, um Spuren, die auf Unregelmäßigkeiten hinweisen, zu verwischen. Auch können Weiterleitungsregeln dazu dienen, Spuren vor dem Anwender zu verstecken, indem E-Mails automatisch als gelesen markiert und in einen anderen Ordner (zum Beispiel in den Junk- oder den RSS-Ordner) verschoben werden.

Einem Angreifer bieten sich in einer Microsoft-365-Umgebung gleich mehrere Möglichkeiten, E-Mails an ein externes Postfach umzuleiten. Er kann zunächst einmal Inbox-Regeln anlegen, um E-Mails auszuleiten. Verfügt das Konto zudem über administrative Berechtigungen, ist auch eine Ausleitung über

die globalen Postfacheinstellungen oder Exchange-Transportregeln möglich.

Aktive Inbox-Regeln lassen sich mit der Exchange-Management-Shell auffinden, falls sie nicht bereits mittels des im ersten Artikel vorgestellten Tools Hawk extrahiert wurden:

```
Get-InboxRule -Mailbox | ? {$_.forwardto -or $_.forwardasattachmentto -or $_.redirectto}
```

Auch aktive Mailbox-Weiterleitungen kann die Exchange-Management-Shell anzeigen:

```
Get-Mailbox <identity> | Format-List ForwardingSMTPAddress,DeliverToMailboxandForward
```

Der Powershell-Befehl Get-TransportRule liefert eine Übersicht über alle bestehenden Weiterleitungsregeln.

Des Weiteren kann man im UAL potenzielle Angreiferaktivitäten im Zusammenhang mit Weiterleitungsregeln analysieren. Hier lassen sich auch Regeln nachvollziehen, die der Angreifer schon wieder gelöscht hat. Folgende Schlüsselwörter führen zu den relevanten Logeinträgen:

Schlüsselwort	**Bedeutung des Logeintrags**
New-InboxRule	Anlegen einer neuen Weiterleitungsregel (Inbox-Ebene)
New-TransportRule	Anlegen einer neuen Transportregel (Mail Flow Rule)
Set-Mailbox	Änderungen an den Einstellungen einer Mailbox; kann zum Einrichten einer Weiterleitung auf Mailbox-Ebene verwendet werden
Set-InboxRule	Änderung an einer bestehenden Weiterleitungsregel (Inbox-Ebene)
Set-TransportRule	Änderung an einer bestehenden Transportregel (Mail Flow Rule)

Schlüsselwort	Bedeutung des Logeintrags
DeliverToMailboxAndForward	Hinweis darauf, dass eine E-Mail an eine andere Mailbox weitergeleitet wurde
ForwardingSMTPAddress	Hinweis auf eine erfolgte Weiterleitung einer E-Mail
ForwardingAddress	Hinweis auf eine erfolgte Weiterleitung einer E-Mail
SentTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde
BlindCopyTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde
ForwardTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde

Schritt 6: Persistent Access – Hintertüren entdecken

Im nächsten Schritt gilt es zu prüfen, ob der Angreifer Hintertüren eingerichtet hat. Das würde ihm auch im Fall einer Entdeckung noch Zugriff auf die erbeuteten Konten gewähren. Hier gibt es im Wesentlichen drei beliebte Techniken: App-Kennwörter, das Einrichten schädlicher OAuth-Applikationen und die Manipulation von Berechtigungen.

App-Kennwörter dienen eigentlich der Absicherung von Netzwerkprotokollen, die Microsofts „Modern Authentication“ nicht unterstützen. Um die Sicherheit eines Kontos nicht durch die Verwendung des Kennwortes über ein Protokoll, das nicht dem aktuellen Sicherheitsstand entspricht, zu gefährden, bietet Microsoft die Möglichkeit, ein spezifisches Kennwort einzurichten. Es gilt nur für dieses Protokoll.

Wird es kompromittiert, erhält der Angreifer nur Zugriff zu einem einzelnen Protokoll, zum Beispiel IMAP oder POP, nicht aber zum gesamten Nutzerkonto. Doch Angreifer können diese Funktion auch missbrauchen, damit sie über ein selbst eingerichtetes App-Kennwort auch nach Änderung des Kennworts im Azure AD noch Zugriff auf die Mails eines Nutzers haben und gegebenenfalls auch weiterhin illegitime Mails verschicken können.

Zur Prüfung auf App-Passwörter sollten Administratoren zum einen im Azure AD die für den jeweiligen Benutzeraccount hinterlegten Authentifizierungsmethoden sichten und zum anderen im Kontext des Kontos selbst die Liste der App-Kennwörter abrufen (siehe ix.de/z2y8).

Anwendungen als Hintertür missbrauchen

Auch Enterprise-Applikationen, die sich mittels OAuth authentifizieren, können als Hintertür zu einem kompromittierten Konto genutzt werden. Berechtigt der Angreifer eine von ihm kontrollierte Enterprise-Applikation zum Zugriff auf das übernommene Konto, erlaubt er damit der Applikation, Aktionen im Kontext des Benutzers durchzuführen.

So ist über diese Applikation auch nach Änderung des Kennworts ein Zugriff mit den gewährten Berechtigungen möglich. Um zu prüfen, ob im Rahmen eines Angriffs Enterprise-Applikationen Berechtigungen erhielten – Microsoft spricht in diesem Zusammenhang von „Illicit Consent Attacks“ –, gibt es mehrere Möglichkeiten.

Administratoren können die Berechtigungen über das Azure-Active-Directory-Portal über den Menüpunkt „Nutzer“ und Auswahl des betroffenen Nutzerkontos prüfen. Eine globale Liste zeigt im Azure AD der Unterpunkt Enterprise-Applikationen. Wer lieber mit PowerShell arbeitet, kann das Skript AzureADPSPermissions.ps1 (siehe ix.de/z2y8) verwenden, um sämtliche OAuth-Berechtigungen eines Tenant in eine CSV-

Datei zu exportieren und anschließend zu überprüfen.

Das Hinzufügen von Enterprise-Applikationen beziehungsweise das Erteilen von Berechtigungen für sie im Analysezeitraum wird im UAL erfasst. Das Werkzeug Hawk extrahiert die Artefakte automatisch (Azure_Application_Audit.csv und Consent_Grant.csv).

Eine Variante zum Phishing mittels OAuth-Applikationen ist das sogenannte Device-Code-Phishing, mit dem sich Office-365-Konten übernehmen lassen. Details zu dieser Angriffstechnik sowie Hinweise zur Detektion und Aufklärung finden sich in einem Artikel des Sicherheitsforschers Nestori Syynimaa (siehe ix.de/z2y8).

Schlüsselwort	Bedeutung des Logeintrags
Add 0Auth2PermissionGrant	Einer Enterprise-Applikation wurden Berechtigungen erteilt.
Consent to application	Einer Enterprise-Applikation wurden Berechtigungen durch einen Admin erteilt.
Add app role Assignment grant to use	Ein Benutzer wurde einer Applikation hinzugefügt.

Hat ein Angreifer mehrere Konten eines Unternehmens kompromittiert, kann er sie dazu missbrauchen, Hintertüren einzurichten, indem er den anderen kompromittierten Konten Zugriff auf eine Mailbox gibt. Solange die Verteidiger nicht sämtliche betroffenen Konten identifizieren, behält der Angreifer weiter Zugriff.

Ereignisse im Zusammenhang mit Berechtigungsänderungen lassen sich durch die Suche nach den folgenden Schlüsselwörtern im UAL ausfindig machen:

Schlüsselwort	Bedeutung des Logeintrags
Add-MailboxPermission	Neue Berechtigungen auf ein Postfach wurden vergeben.

Schlüsselwort	Bedeutung des Logeintrags
Add-MailboxFolderPermission	Neue Berechtigungen auf einen Order in einem Postfach wurden vergeben.
Add-RecipientPermission	Hinweis darauf, dass einem Benutzer die „Senden als“-Berechtigung zugewiesen wurde.
Set-MailboxFolderPermission	Bestehende Berechtigungen eines Ordners in einem Postfach wurden geändert.

Hat ein Angreifer sogar ein Konto mit administrativen Berechtigungen gekapert, kann er zudem eigene neue Benutzerkonten anlegen, die dann als Hintertür dienen. Auch das hinterlässt Spuren im UAL.

Schlüsselwort	Bedeutung des Logeintrags
Added user	Ein neuer Benutzer wurde angelegt.

Schritt 7: Datenexfiltration analysieren

Bestätigt es sich, dass jemand Unbefugtes Zugriff auf das Unternehmensnetzwerk hatte, stellt sich in erster Linie die Kernfrage: Worauf hat der Angreifer zugegriffen? Dem zugrunde liegt oft die (späte) Erkenntnis über Art und Umfang der Informationen, die mit einem Benutzerkonto prinzipiell erreichbar wären, verbunden mit dem Wunsch, dieses Worst-Case-Szenario irgendwie einzugrenzen.

Hier zunächst die schlechte Nachricht vorweg: Es ist in der Praxis selten möglich, einen Negativbeweis zu führen, also festzustellen, was die Angreifer nicht mitgenommen haben. Die Aussagekraft der Artefakte ist meist begrenzt, da schlicht nicht alles protokolliert wird. In der Regel muss bei einer gesicherten Kompromittierung eines Kontos unterstellt werden, dass der Angreifer alle erreichbaren Inhalte ausgespäht hat. Das hat erhebliche Konsequenzen beispielsweise für die

datenschutzrechtliche Bewertung eines Vorfalls.

Die gute Nachricht ist, dass auch Microsoft das erkannt hat. Konten, die mit einer E5-Lizenz ausgestattet sind, verfügen über eine „erweiterte Überwachung“. Diese Funktion protokolliert unter anderem Zugriffe auf einzelne E-Mails, was die Chance auf den seltenen Negativbeweis zumindest für die Inhalte des Postfachs deutlich verbessert.

Im UAL finden sich dann Einträge der Art MailItemsAccessed. Diese haben unter anderem ein Attribut MailAccessType, das zwischen Bind und Sync unterscheidet.

Operation	Bedeutung des Logeintrags
MailItemsAccessed	Hinweis auf den erfolgten Zugriff auf Inhalte eines Postfachs

Bind-Einträge werden erzeugt, wenn eine einzelne E-Mail abgerufen wird. Die ID der Nachricht steht dann im Attribut InternetMessageId. Die Protokollierung unterliegt jedoch einer wichtigen Einschränkung: Werden innerhalb von 24 Stunden mehr als 1000 Zugriffe dokumentiert, wird die Protokollierung für Bind-Ereignisse für 24 Stunden ausgesetzt (Throttle).

Zuerst sollte also geprüft werden, ob das UAL Einträge des Typs MailItemsAccessed für die zu untersuchende Mailbox enthält. Anschließend gilt es auszuschließen, dass ein Throttling stattgefunden hat. Dazu schaut man, ob es bei den MailItemsAccessed-Ereignissen welche gibt, die beim Attribut IsThrottled den Wert True vermerkt haben. Im Idealfall gibt es keinen solchen Eintrag.

Welche Sitzung gehört zu wem?

Der nächste Schritt besteht darin, die zum Angreifer gehörenden Sitzungen zu ermitteln. Dafür gleicht man die MailItemsAccessed-Vorgänge im UAL mit den Informationen des Angreifers (verdächtige Log-in-Aktivitäten, IP-Adressen, Zeitstempel, Art des Zugriffs) und den Informationen über den

legitimen Anwender ab. Die Einträge haben mitunter mehrere Session-IDs und IP-Adressen für ein Benutzerkonto. Anhand der in den vorangegangenen Schritten ermittelten Kompromittierungsindikatoren lässt sich feststellen, welche Sitzungen wahrscheinlich legitim oder gültig sind. Einige Sitzungen haben möglicherweise keine Session-ID, weil für die Anmeldung eine alte (Legacy-)Authentifizierung verwendet wurde. Die verdächtigen MailItemsAccessed-Einträge werden dann weiter analysiert.

Sync-Einträge entstehen immer dann, wenn ein E-Mail-Client, beispielsweise Outlook, ein Postfach synchronisiert und dabei Inhalte auf einen lokalen Computer herunterlädt. Hierbei entsteht kein Logeintrag pro Element, sondern pro Ordner des Postfachs. Finden sich im UAL MailItemsAccessed-Einträge mit dem MailAccessType Sync, die dem Angreifer zugeordnet werden, so muss man davon ausgehen, dass alle E-Mails im synchronisierten Ordner kompromittiert wurden.

Zuletzt bleiben die Bind-Vorgänge, die dem Angreifer zugeordnet werden. Diese enthalten eine InternetMessageID. Um damit auf die eigentlichen Nachrichten schließen zu können, ist es notwendig, das Message Trace Log mit den IDs abzugleichen. Leider reicht das Message Trace Log nicht so weit zurück wie die Einträge im UAL, sondern lediglich zehn Tage. Auch lässt sich die InternetMessageID nicht als Suchparameter im Rahmen einer Suche nach Beweismitteln (E-Discovery) verwenden.

Können E-Mails nicht mehr über das Message Trace Log zugeordnet werden, bleibt lediglich der Weg, das Postfach selbst zu exportieren und die E-Mails zu durchsuchen. Die ID ist in den Eigenschaften der E-Mails gespeichert. Der Export des Postfachs lässt sich außerdem über die E-Discovery-Funktion realisieren, die auch bereits gelöschte Elemente berücksichtigt (sofern entsprechende Aufbewahrungsrichtlinien konfiguriert sind und die Elemente noch vorgehalten werden).

Rekonstruieren, was geklaut wurde

Wie beschrieben können E-Mails auch über Weiterleitungsregeln abgegriffen werden. Findet man bei einer Untersuchung solche Regeln, kann sowohl das UAL (siehe Schritt 5) wie auch die Logik der Regeln selbst Aufschluss über die betroffenen Inhalte geben. Neben dem Abgleich der Einträge im UAL mit dem Message Trace Log sollte die Mailbox nach den Parametern der Regel(n) durchsucht werden.

Sofern ein Angreifer Zugang zu einem Konto mit administrativen Berechtigungen und der E-Discovery-Suche hatte, kann er auch auf diesem Weg Inhalte gesucht und exportiert haben. Hinweise darauf lassen sich wieder im UAL finden.

Analog zu den E-Mails sind alle weiteren Inhalte zu berücksichtigen, die mit dem kompromittierten Konto für den Angreifer erreichbar waren. Das beinhaltet sowohl in OneDrive geteilte Dateien wie Teams-Nachrichten und SharePoint-Seiten als auch sämtliche nachgelagerten Applikationen, die Azure AD zur Authentifizierung verwenden. Die Analyse ist allerdings oft sehr individuell und würde den Rahmen dieses Artikels sprengen.

Schritt 8: Remediation

Nachdem die Aktivitäten eines Angreifers nachvollzogen wurden, gilt es, alles rückgängig zu machen, also alle gefundenen Weiterleitungsregeln, Enterprise-Applikationen, App-Kennwörter et cetera zu entfernen und die Kennwörter der betroffenen Konten, falls noch nicht geschehen, zurückzusetzen. Auch sollten alle Analysen und eingeleiteten Maßnahmen dokumentiert und mit den zugehörigen Logdateien aufbewahrt werden.

Zeigte die Untersuchung einen unberechtigten Zugriff auf Postfächer, handelt es sich um einen meldepflichtigen Vorfall gemäß der DSGVO. Dementsprechend ist eine Erklärung an den zuständigen Landesdatenschutzbeauftragten verpflichtend. Dabei

gilt es, die gesetzlichen Fristen zu beachten. Binnen 72 Stunden ab dem Zeitpunkt der Kenntnisnahme muss die Meldung erfolgen. Zu diesem Zeitpunkt ist gegebenenfalls noch nicht das gesamte Ausmaß des Vorfalls bekannt. In diesem Fall sollte die Meldung einfach alle bisher gesicherten Informationen enthalten. Die Meldung sollte durch den benannten Datenschutzbeauftragten des betroffenen Unternehmens erfolgen.

Neben den Datenschutzbehörden müssen gegebenenfalls auch die betroffenen Personen informiert werden. Dies ist dann der Fall, wenn besonders heikle personenbezogene Daten gemäß Art 9 DSGVO – also beispielsweise religiöse oder weltanschauliche Überzeugungen oder Gesundheitsdaten – betroffen sind. In diesem Fall sind die betroffenen Personen direkt zu benachrichtigen. Die Prüfung einer solchen Meldepflicht obliegt dem Datenschutzbeauftragten. Gegebenenfalls sollte bei Verdacht auf einen solchen Fall juristischer Beistand hinzugezogen werden.

Schritt 9: Root Cause Analysis – woran liegts?

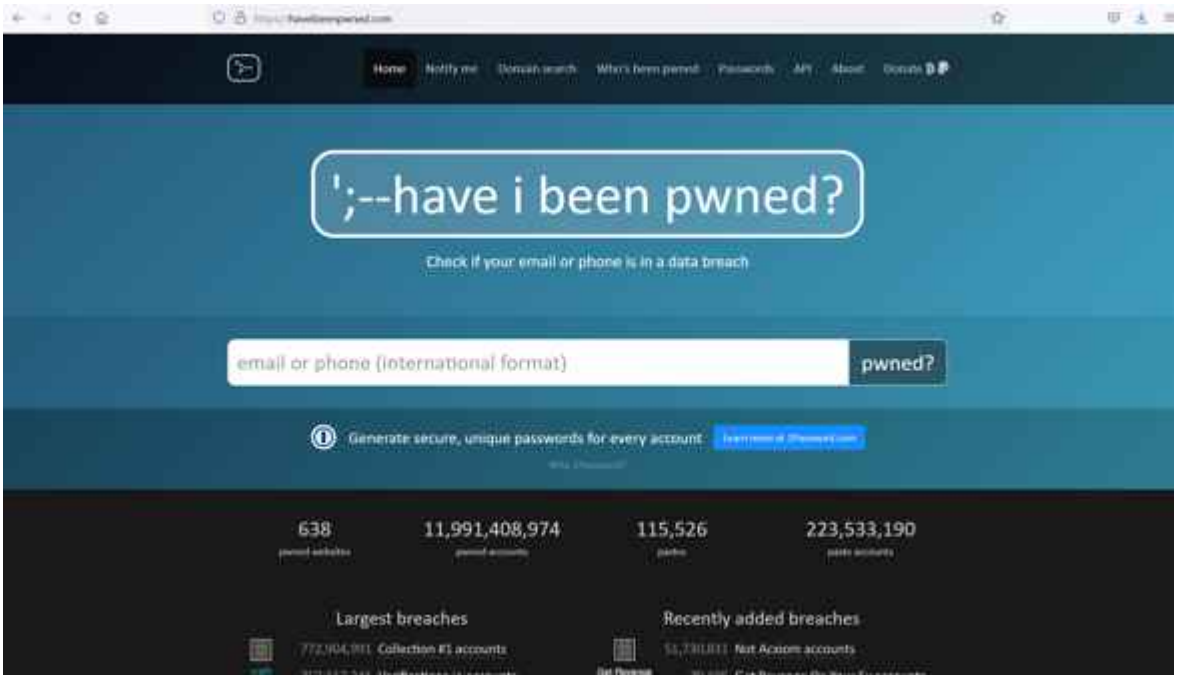
Nachdem aufgeklärt ist, wie ein Angreifer vorgegangen ist und was er genau getan hat, bleibt noch die Frage, wie das passieren konnte. Wie hat er initial Zugang erhalten?

Auch hier ist leider keine pauschale Anleitung möglich, doch die häufigsten Ursachen sind folgende:

- Password Spraying / Brute Force / einfach zu erratende Passwörter: Allen drei Szenarien ist gemeinsam, dass sie in der Regel mit mehrfachem Ausprobieren einhergehen. In den Logs äußert sich dies durch multiple fehlgeschlagene Log-in-Versuche bei einem oder mehreren Konten, ausgehend von derselben IP-Adresse und/oder ähnlichen Parametern wie User-Agent, Protokoll und Zeitpunkt.
- (Spear-)Phishing: Bei einem Phishingangriff erhält das

Opfer eine E-Mail, die einen Link oder einen Anhang enthält, über den die Zugangsdaten abgegriffen werden (funktioniert teilweise auch bei MFA) oder eine Enterprise App via OAuth-Berechtigungsanfrage untergeschoben wird. In dem Fall sind keine gehäuften fehlgeschlagenen Log-in-Versuche zu beobachten. Stattdessen gilt es, die Phishingmail im Postfach oder den aufgerufenen Link ausfindig zu machen.

- Password Re-use / Leaked Credentials: Oft verwenden Anwender ein Passwort für mehrere Dienste und Konten oder recyceln ein privates Passwort für Firmenzwecke. In dem Fall kann es sein, dass das Kennwort bei einem der anderen Dienste ausgespäht wurde und dann für die Anmeldung am Microsoft-365-Account ausprobiert wird. Auch hier ist nicht unbedingt eine gehäufte Anzahl an Fehlversuchen zu beobachten, sofern nicht zusätzlich MFA aktiviert ist. Um der Ursache in dem Fall näherzukommen, empfiehlt es sich, mit dem Benutzer ein offenes Gespräch zu führen oder die Unternehmens-E-Mail des Anwenders bei seriösen Diensten wie haveibeenpwned.com einzugeben (siehe Abbildung).



Ob ein Passwort geleakt wurde, kann man beispielsweise bei Diensten wie „Have I Been Pwned“ herausfinden. Dieser Dienst

des australischen Sicherheitsforschers Troy Hunt hat einen guten Ruf, da er nicht das Passwort selbst, sondern nur den Benutzernamen abfragt.
Nach der erfolgreichen Bewältigung des potenziellen oder realen Sicherheitsvorfalls sollte immer auch geprüft werden, welche Lektionen man daraus lernen kann und welche Maßnahmen zu ergreifen sind, damit ähnliche Vorfälle in Zukunft seltener oder gar nicht mehr vorkommen. Dabei soll es explizit keine Schuldzuweisungen geben, das Stichwort lautet hier vielmehr „Blameless Post Mortem“.

Awareness-Maßnahmen und Schulungen können gängige Betrugsmuster vermitteln und damit die Anfälligkeit der Mitarbeitenden für solche Angriffe verringern. Klar definierte Prozesse zur Veranlassung von Zahlungen helfen außerdem, bestimmte Arten von finanziellem Betrug zu erschweren. Häufig werden aber im Rahmen der Vorfallsbehandlung vor allem technische Gegebenheiten identifiziert, die die Kompromittierung erleichtert oder die Untersuchung des Vorfalls erschwert haben. So ist es hilfreich, die SPF-, DKIM- oder DMARC-Konfiguration (Sender Policy Framework; DomainKeys Identified Mail; Domain-based Message Authentication, Reporting and Conformance) nachzurüsten, falls sie im Vorfeld des Vorfalls noch nicht aktiv war, die Protokollierung lässt sich verbessern, wenn Logs für die Aufklärung des Angriffs fehlten, oder das Installieren von OAuth-Anwendungen kann für Nutzer des Tenants eingeschränkt werden, falls Angreifer solche Anwendungen als Hintertür installiert haben.

Microsoft gibt im Rahmen einer Referenzarchitektur zahlreiche Hinweise für das Absichern von Microsft-365- und Azure-AD-Umgebungen (siehe ix.de/z2y8), die im Nachgang eines Vorfalls (re-)evaluiert werden und bei Bedarf in das Sicherheitskonzept des Unternehmens integriert werden können. Dedizierte Dienste wie Microsoft Defender for Office, Microsoft Defender for Identity oder Microsoft Defender for Cloud Apps können gegen Angriffe schützen oder bei ihrer Entdeckung und Aufbereitung helfen. Allerdings sind sie häufig nur in den teureren

Lizenzen der Microsoft-Produkte enthalten oder müssen sogar separat lizenziert werden. (ur@ix.de)

1. Quellen
2. Jens Lüttgens, Dominik Oepen; E-Mail-Betrug in MS-365-Umgebungen; iX 12/2022, S. 102
3. Vertiefende Microsoft-Artikel, das erwähnte PowerShell-Skript sowie die Microsoft-Referenzarchitektur sind über ix.de/z2y8 zu finden.

Introducing a new phishing technique for compromising Office 365 accounts

The ongoing global phishing campaings againts Microsoft 365 have used various phishing techniques.
Currently attackers are utilising forged login sites and OAuth app consents. In this blog, I'll introduce a new phishing technique based on Azure AD device code authentication flow.
I'll also provide…

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.

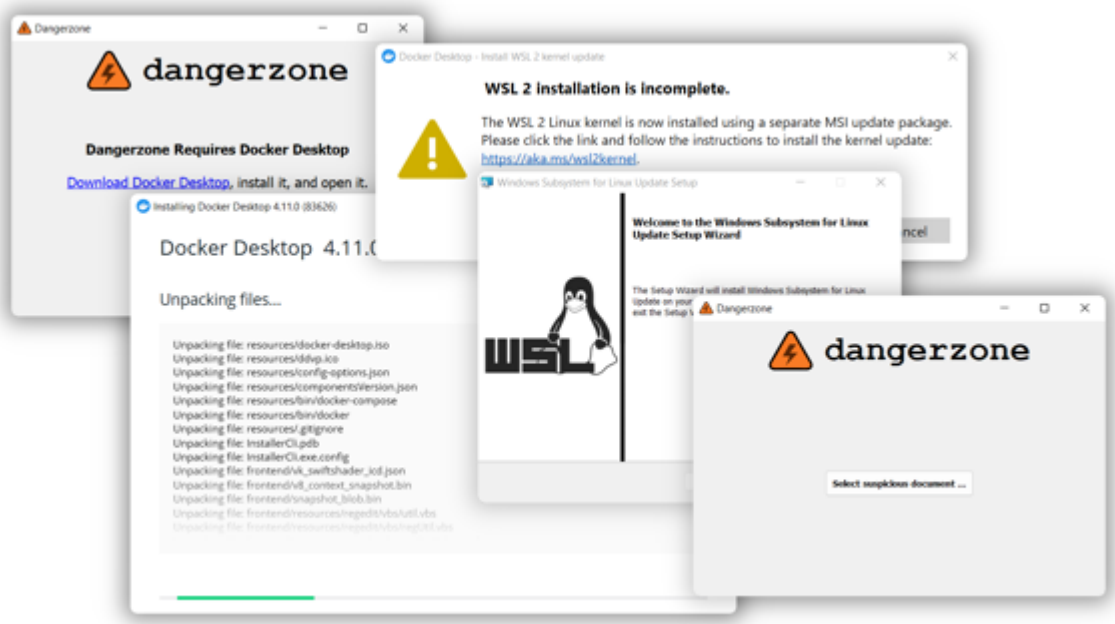
Praktikabler sind Tools, die automatische Isolationsumgebungen nutzen, um Dateien zu entschärfen, wie das Werkzeug Dangerzone (https://dangerzone.rocks). Es steht für Windows, macOS und Linux zur Verfügung und nutzt Container zur Isolation. Unter Windows und macOS kommt dafür Docker Desktop zum Einsatz 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/co
```

```
de/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.

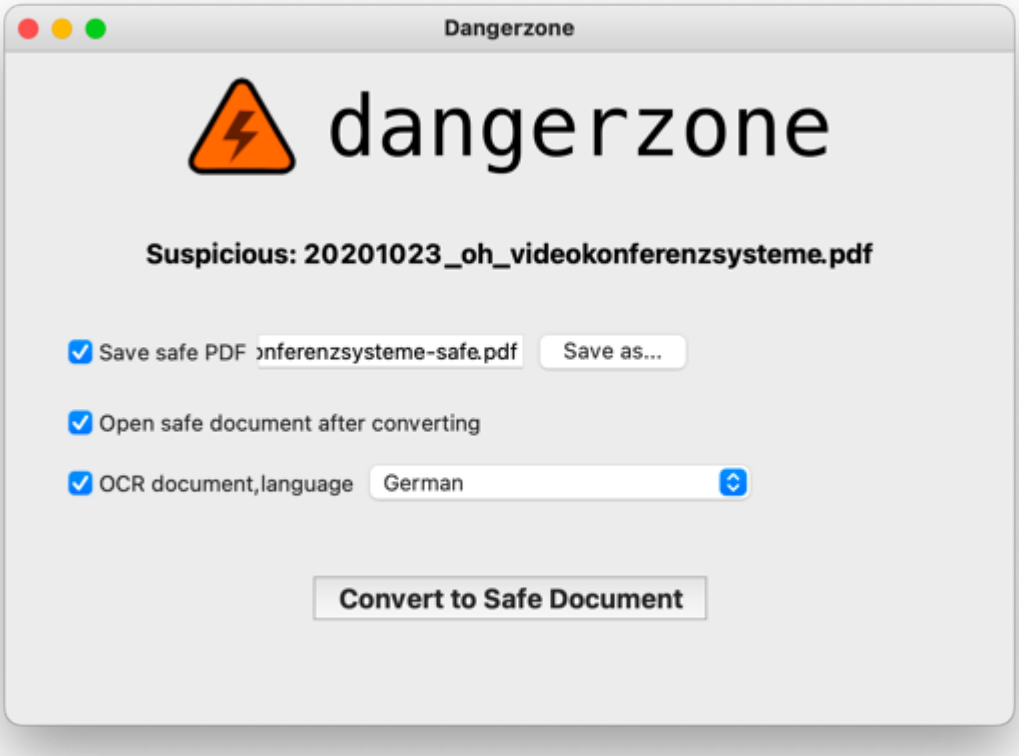
Statt sich unter Linux mit dem Paketbau oder Versionsinkompatibilitäten herumzuschlagen, bietet es sich an, einfach eine Debian-VM aufzusetzen und Dangerzone darin zu betreiben.

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,

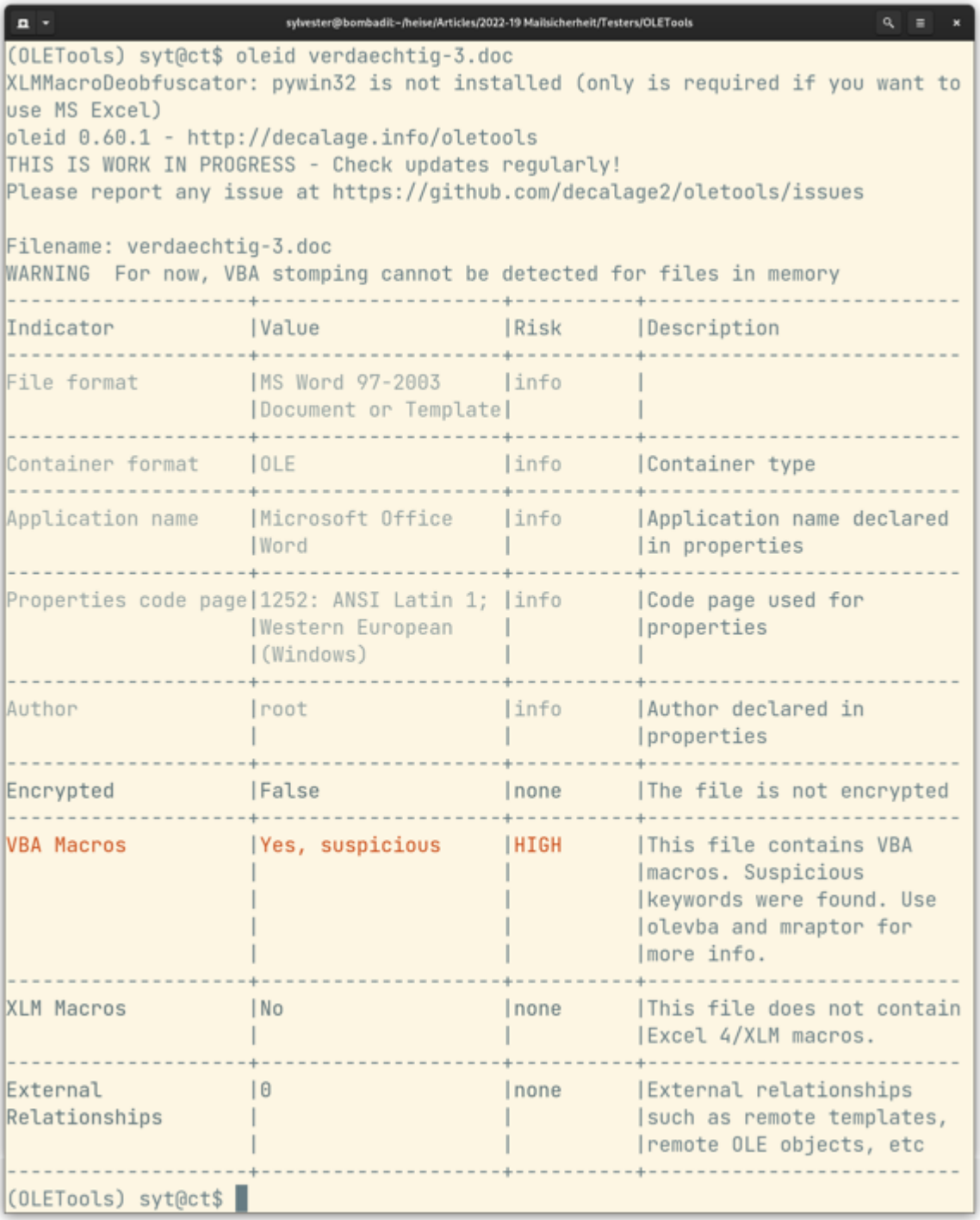
XSLX, PPTX), sind im Grunde Zip-Archive, die lediglich einen speziellen Inhalt haben. Das hilft, falls Sie beispielsweise nur an den Bildern in einem Word-Dokument interessiert sind. Dann ändern Sie einfach die Endung von .docx in .zip, öffnen das Archiv mit dem Zip-Programm Ihrer Wahl und inspizieren 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.

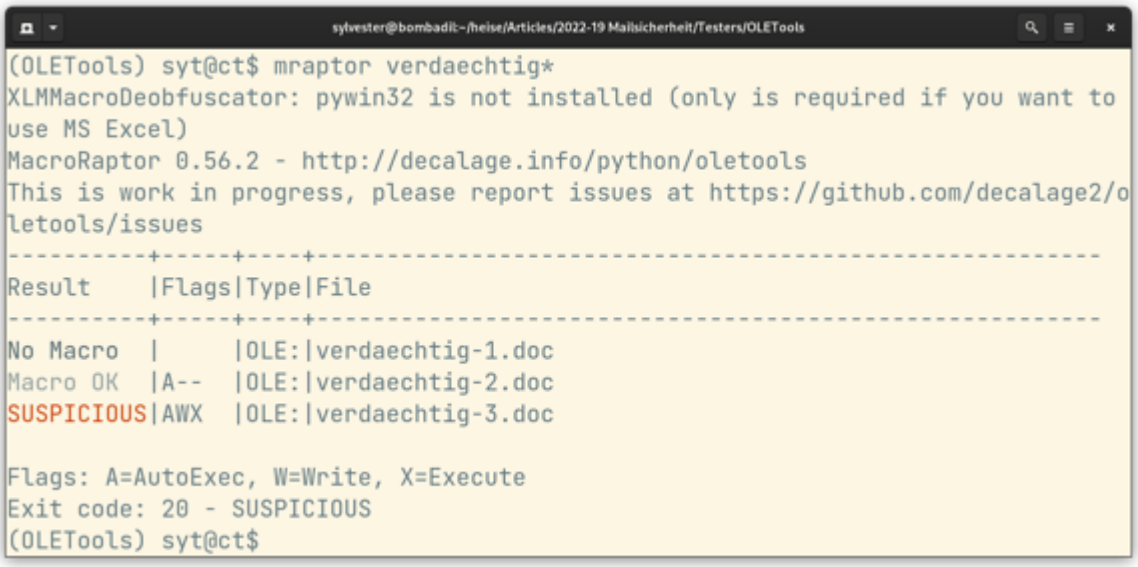


„VBA Macros: Yes, suspicious; Risk: HIGH“ meldet oleid und hat recht. Diese Datei ist tatsächlich höchst suspekt.
Ein Dokument mit einem höchst suspekten Makro, das versucht, eine Datei auf die Festplatte zu schreiben, bewertet oldid in Rot als „suspicious“ (verdächtig) und warnt in Großbuchstaben vor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