Website Sicherheits-Check: Sichere deine Webseite gegen Malware und Spam

Es ist keine große Überraschung, dass Sicherheit ein wichtiges Thema für Webentwickler und Betreiber von Webseiten geworden ist. Da das Internet immer beliebter wird und die neue Methode zur Kommunikation, Recherche und zum Einkaufen ist, sind Sicherheitschecks für Webseiten entscheidend, um die Verbreitung von Malware und Spam zu verhindern.

Egal ob du einen kleinen persönlichen Blog oder einen riesigen multinationalen Online-Shop betreibst, die Gefahr, gehackt zu werden, ist immer gegeben. Einige Leute werden deine Webseite verunstalten und Malware darin einbetten, versuchen, deine Daten oder die deiner Kunden zu stehlen und wichtige Inhalte auf deinem Server zu löschen. Du musst dich und deine sensiblen Informationen schützen.

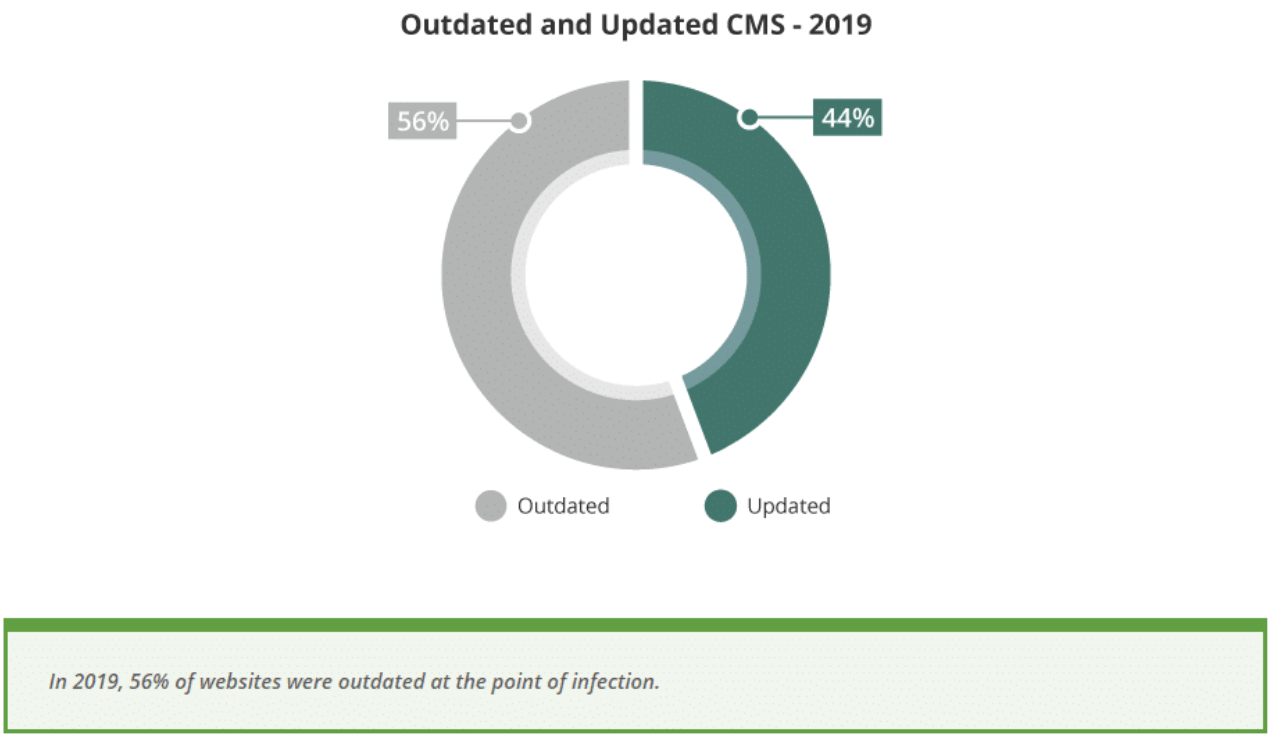
Lass uns genau herausfinden, wie sicher deine Webseite im Moment ist. Außerdem geben wir dir ein paar Tipps, wie du die niedrig hängenden Früchte entfernen kannst, die sich Malware-Autoren zunutze machen. WordPress ist von Haus aus sicher, aber es braucht ein wenig Arbeit, um es komplett zu reparieren.

Schau dir unseren Video-Leitfaden zur Überprüfung der Sicherheit deiner Webseite an

Webseiten Sicherheitscheck: Warum ist es wichtig?

Du denkst vielleicht, dass deine Webseite so klein und unwichtig ist, dass sich niemand die Mühe machen würde, sie ins Visier zu nehmen. Oder vielleicht hast du noch nie über Sicherheit nachgedacht und denkst, dass es nicht wichtig genug ist, um sich damit zu beschäftigen.

So zu denken ist der Grund, warum im Jahr 2013 mehr als 70% der WordPress Installationen anfällig für Angriffe waren. Viele dieser Angriffe waren auf veraltete Software zurückzuführen – weil die meisten Leute entweder nicht genug wissen oder sich nicht genug darum kümmern, ihre Webseiten zu sichern, was zu einer massiven Welle von Hackern führte, die es auf WordPress Installationen abgesehen hatten.



Veraltetes vs. aktualisiertes CMS im Jahr 2019.

Was könnte also passieren, wenn deine Webseite ein unerwünschtes Ereignis erlebt? Es ist nicht nur ein einfaches Ärgernis, das leicht durch das Ändern deines Passworts gelöst werden kann.

- In deine Webseite könnte Code eingeschleust sein, der Besucher dazu bringt, sich mit Malware zu infizieren, die extrem schwer zu finden und zu entfernen sein könnte.
- Deine kritischen Seiten können verunstaltet, ausgeblendet oder mit Links zu illegalen Webseiten gefüllt sein.
- Es kann zur Löschung von Inhalten wie Blogposts und Seiten führen.
- Sensible Daten wie Login- oder Kreditkarteninformationen, die dir, deinen Nutzern oder Kunden gehören, können gestohlen und online verkauft werden.
- Angriffe können sich auf andere Webseiten auf deinem Server ausbreiten.
- Wenn Google Malware auf deiner Webseite entdeckt, wird es den Zugang blockieren und sie aus den Suchergebnissen entfernen, was deine Bemühungen zur Suchmaschinenoptimierung (SEO) zunichte macht.
- Der Benutzername und das Passwort des Admin-Accounts könnten geändert werden, sodass du überhaupt keinen Zugriff mehr auf dein Backend hast.

Gehackte Webseiten können ein großes Problem darstellen, wenn du einen E-Commerce-Shop betreibst.

Und während du vielleicht sagst, dass deine Webseite nicht wichtig genug ist, sind nicht alle Angriffe gezielt. Viele WordPress Angriffe sind automatisiert – ein Bot sucht deine Webseite nach Schwachstellen ab und startet einen Angriff ohne menschliches Zutun.

Deshalb musst du Maßnahmen ergreifen, um deine Webseite zu sichern, egal was passiert.

Warum wird WordPress gehackt?

Hacking ist weit verbreitet, aber was sind die häufigsten Schwachstellen, die Hacker ausnutzen, um in deine Webseite einzubrechen?

Du stellst dir vielleicht vor, dass es ein schwieriger Prozess ist, in eine Webseite einzudringen, der Tage oder Wochen an Arbeit und ein enormes Wissen über Computer, Codierung und Server erfordert. Diese Situation könnte für gezielte Versuche zutreffen, die Verteidigungsanlagen einer großen, gut geschützten Webseite zu überwinden, aber die Geschichte sieht ganz anders aus, wenn es um kleine WordPress Domains geht.

Die überwiegende Mehrheit der Angriffe auf WordPress sind erfolgreich, weil die Leute leicht zu erratende Passwörter benutzen und ihre Themes und Plugins nicht aktualisieren. Hacker brechen in die meisten solcher Webseiten mit Hilfe von automatisierten Programmen ein.

Passwort-Cracking ist die einfachste Form des Hackens, die möglich ist, aber es ist so verbreitet, weil es funktioniert. Viele Leute belassen ihr WordPress Login auf dem Standard „admin“, was die Hälfte des Rätselraten ausschaltet, und benutzen dann ein einfaches, erratbares Passwort.

Wenn das nicht funktioniert, nutzen Hacker häufige Schwachstellen in beliebten Plugins oder veralteten Versionen von WordPress aus. Deshalb ist es so wichtig, alles auf dem neuesten Stand zu halten.

Es gibt viele kompliziertere, komplexere Wege, um in eine Webseite „einzubrechen“. Dennoch nutzen die meisten WordPress-Angriffe die niedrig hängenden Früchte eines unsicheren Passworts und veralteter Software, die es extrem einfach macht, auf deine Webseite zu gelangen.

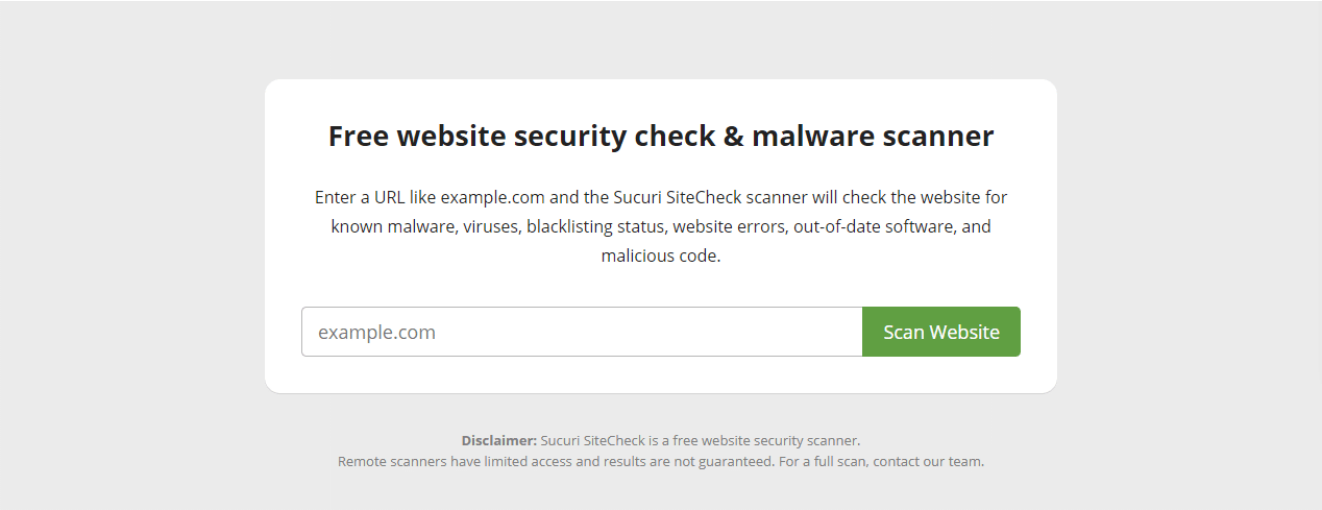
Wie man einen Sicherheitscheck der Webseite durchführt

Der erste Schritt zur Absicherung deiner Webseite: Feststellen, wie sicher deine Webseite bereits ist. Gibt es irgendwelche eklatanten Schwachstellen in deinem Backend, die du sofort flicken musst, oder irgendwelche einfachen Korrekturen, die du jetzt vornehmen kannst?

Verwende ein Online Tool

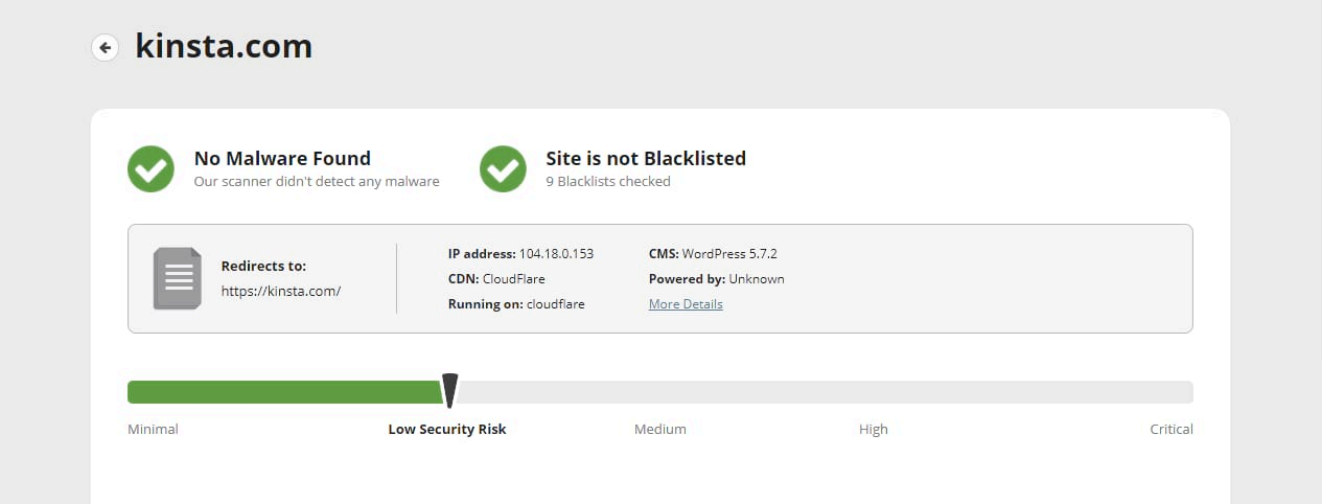
Eine schnelle und einfache Möglichkeit, deine Webseite auf Malware und Schwachstellen zu überprüfen, ist die Verwendung eines Online-Scanners. Diese scannen deine Webseite aus der Ferne und identifizieren häufige Probleme. Es ist super bequem, da es keine Software oder Plugins benötigt und nur ein paar Sekunden dauert.

Es gibt Dutzende von Online-Scannern zur Auswahl und wir werden ein paar weitere in unserem Tool-Bereich weiter unten auflisten, aber für den Moment nehmen wir einen beliebten, der einfach zu benutzen ist: Sucuri SiteCheck.



Sucuri SiteCheck.
Dieses Tool ist eine gute Wahl, denn du kannst das Sucuri Plugin installieren und dich direkt an die Behebung der Probleme machen, die es erkennt.

Sobald du deine Webseite gescannt hast, gleicht Sucuri sie mit Blocklisten ab, sucht nach offensichtlichen Problemen wie eingeschleustem Spam oder veralteter Software und scannt kurz jeden Code, auf den es zugreifen kann, auf Malware. Sucuri bietet auch einige Vorschläge, um deine Webseite gegen Angriffe zu schützen.



Scannen einer Webseite mit dem Sucuri Plugin.
Tools wie dieses sind ein hervorragender Ausgangspunkt für die Erkennung versteckter Malware und anderer Probleme.

Scanne deine Webseite mit einem WordPress Plugin

Während Online-Scanner gut genug funktionieren, ist es noch besser, ein Plugin zu installieren, das in der Lage ist, tief in die Wurzel deines Codes zu graben und Schwachstellen oder schwer zu entdeckende Malware herauszufischen.

Wir haben bereits Sucuri als eine Option erwähnt. Es gibt auch zwei noch populärere Sicherheits Plugins: All in One WP Security & Firewall und das meist heruntergeladene im Repository, Wordfence Security.

Sobald du das Plugin deiner Wahl installiert hast, wird es dich wahrscheinlich anweisen, sofort einen Scan durchzuführen. Der Vorteil dieser Plugins gegenüber Remote-Scannern ist, dass sie Malware entfernen und Änderungen automatisch vornehmen

können.

Suche nach seltsamen Änderungen

Wenn du den Verdacht hast oder weißt, dass deine Webseite mit Malware infiziert wurde, kann es manchmal schwierig sein, die Quelle zu lokalisieren. Hier sind ein paar unerklärliche Änderungen, die dir auffallen könnten, sowie die Dateien, auf die es Hacker typischerweise abgesehen haben:

- Plötzliche Links zu fremden Webseiten, die du nicht selbst hinzugefügt hast
- Neue Artikel und Seiten, die du nicht erstellt hast, oder der Inhalt bestehender Seiten ändert sich plötzlich
- Änderungen an Einstellungen, die du nicht vorgenommen hast
- Ein neuer Benutzer, besonders einer mit hohen Rechten, den du nicht hinzugefügt hast
- Plugins oder Themes, die du nicht installiert hast
- Malware kann oft bösartigen Code in deine Dateien einschleusen. Überprüfe Plugin- und Theme-Dateien, den Ordner **wp-content/uploads**, WordPress-Core-Dateien, die sich in einem falschen Verzeichnis befinden, **wp-config.php** und **.htaccess**. Du solltest ein Backup deiner Webseite machen und den Code verstehen, bevor du sensible Änderungen vornimmst.

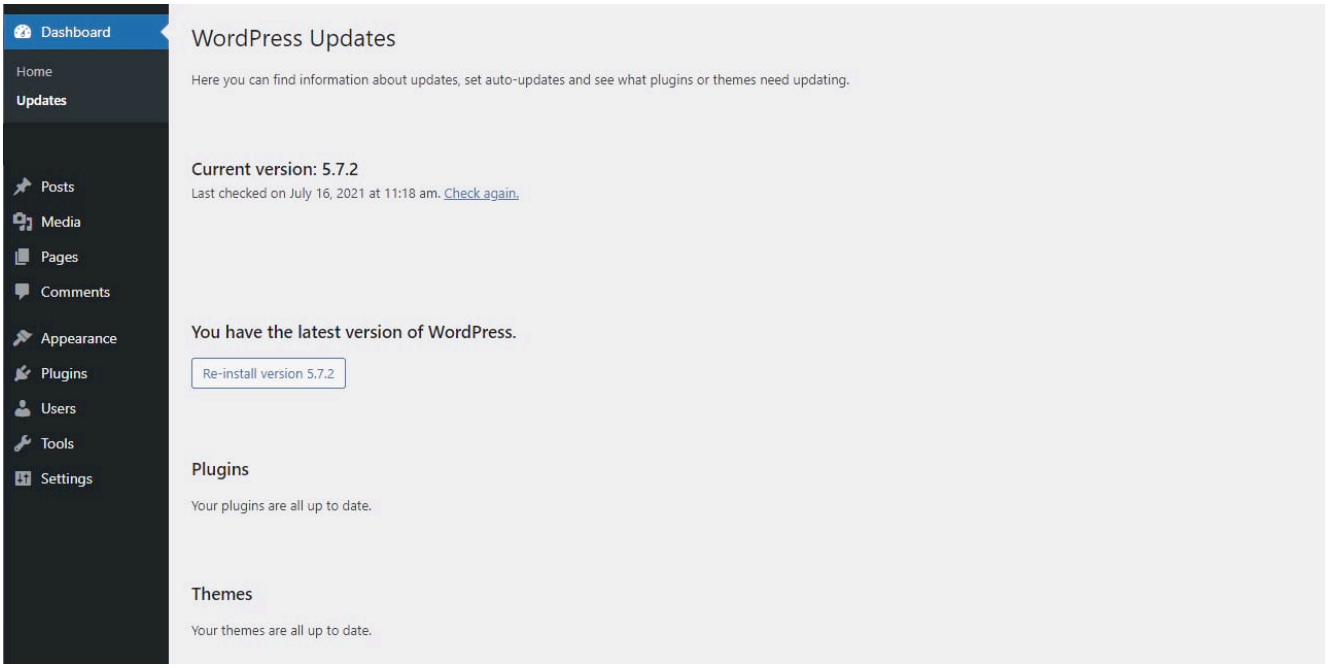
Wenn du dich mit FTP mit deiner Webseite verbindest, kannst du nach kürzlich geänderten Dateien sortieren, um Code zu finden, der dort nicht sein sollte.

Wenn deine Webseite regelmäßig mit Malware infiziert wird und du keine Ursache in den Dateien finden kannst, kann das Problem bei deinem Server oder einer anderen Webseite auf deinem Server liegen.

Stelle sicher, dass alles auf dem neuesten Stand ist

Wie wir bereits erwähnt haben, ist veraltete Software der mit Abstand häufigste Infektionsvektor in WordPress. Wenn es nur eine Sache gibt, die du tun kannst, um deine Webseite sicher zu halten, dann sollte es sein, WordPress auf dem neuesten Stand zu halten.

Der einfachste Weg, den Status aller Software auf deiner Webseite zu überprüfen, ist das **Dashboard > Updates**, welches dich darauf hinweist, wenn dein Core, Theme oder Plugins veraltet sind.



WordPress Updates

Da WordPress nun seit Version 5.5 automatische Updates durchführt, sollte nichts veraltet sein, es sei denn, du hast eine veraltete Version von WordPress. Wenn das nicht der Fall ist, kannst du alles von diesem Bildschirm aus aktualisieren.

Wenn du weißt, dass es eine neue Version von WordPress gibt, sie aber nicht angezeigt wird, klicke auf den Button **Erneut** prüfen unter **Aktuelle Version**.

Du kannst auch auf den Seiten **Plugins** > **Installierte Plugins**

oder **Erscheinungsbild** > **Themes** nach Updates suchen.

Important

Es ist wichtig, PHP auf dem neuesten Stand zu halten, besonders wenn du eine Version älter als 7.3 verwendest, da es erhebliche Sicherheitslücken aufweisen kann.

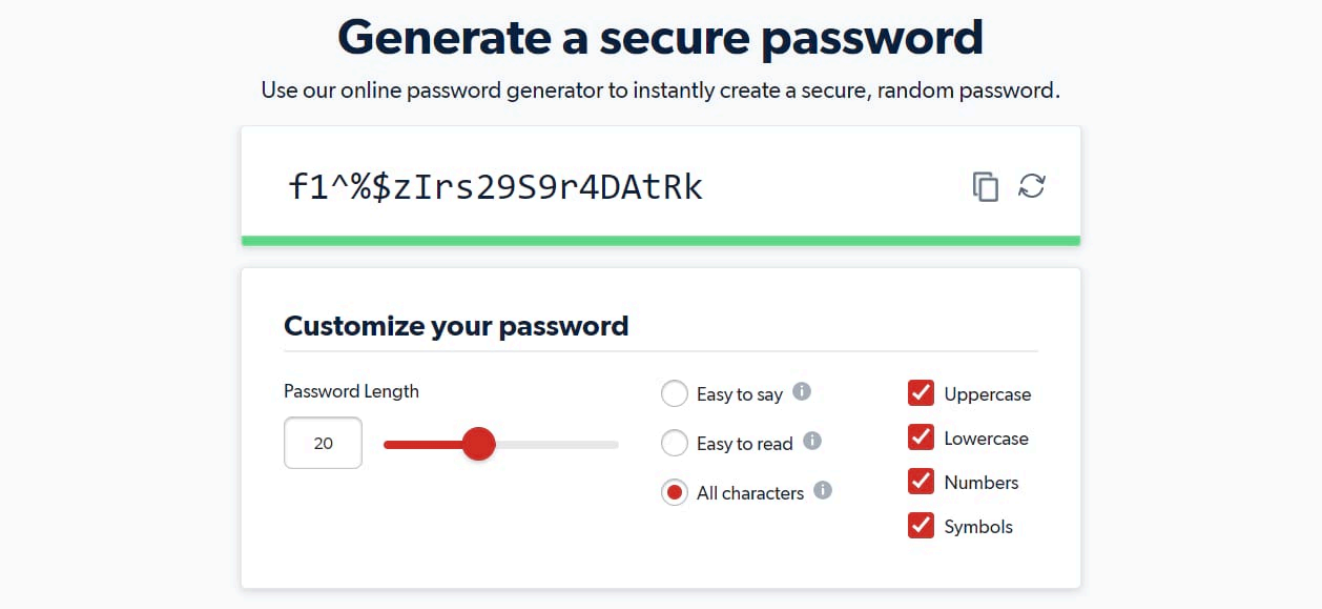
Sichere Konten und Passwörter

Ein schwaches Passwort für deinen Hauptaccount macht es jedem leicht, mit Brute-Force-Programmen in deine Webseite einzubrechen, ihnen Administrator-Zugang zu geben und die Möglichkeit, alles zu ändern.

Während ein kompliziertes Passwort mühsam zu merken ist und das Einloggen weniger bequem macht, ist es noch unangenehmer, wenn du deine Webseite nach einem Hack wiederherstellen musst. Es lohnt sich auf jeden Fall, ein sichereres Passwort zu verwenden, selbst wenn du es aufschreiben musst.

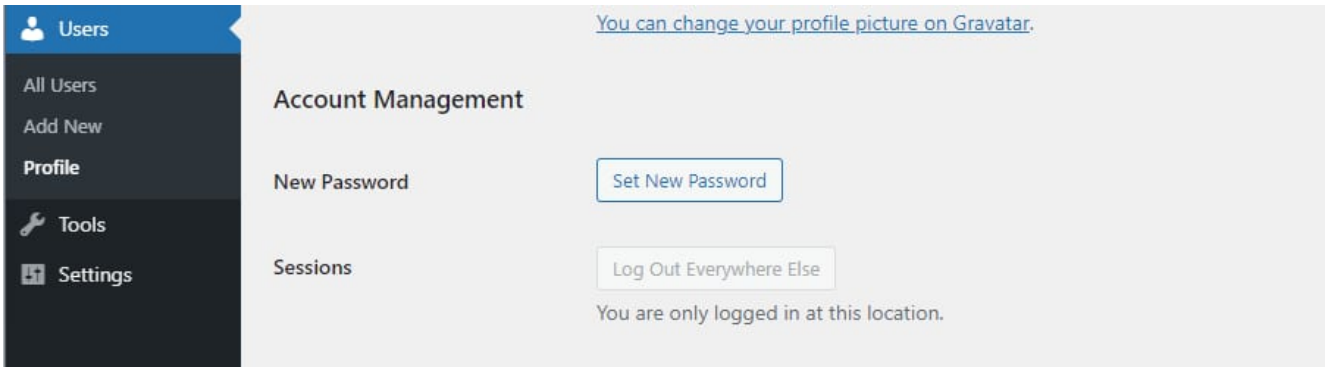
Dein Passwort sollte eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Symbolen verwenden. Am besten wäre es, wenn du es nicht auf Wörterbuchwörtern oder persönlichen, erratbaren Informationen wie deiner Adresse oder dem Namen eines Familienmitglieds basieren würdest.

Im besten Fall ist dein Passwort eine lange, verworrene Kette aus zufälligen Zeichen. Wir empfehlen dir dringend, einen Passwort-Manager zu verwenden. Verwende eine Webseite wie 1Password oder LastPass, um ein sicheres, nicht zu erratendes Passwort zu generieren.



Generiere ein sicheres Passwort mit LastPass.

Du kannst dein Passwort und deine E-Mail in WordPress aktualisieren, indem du zu **Benutzer** > **Alle Benutzer** oder direkt zu **Benutzer** > **Profil** gehst. Scrolle nach unten und finde **E-Mail** unter **Kontaktinformationen** und **Neues Passwort** unter **Kontoverwaltung**.



Ein neues Passwort in WordPress setzen

Wenn du auf der **Benutzerseite** bist, schaue dir alle deine Benutzer an und stelle sicher, dass niemand dabei ist, den du nicht kennst oder der unangemessene Berechtigungen hat. Du solltest jeden nicht identifizierten Benutzer mit Admin-Rechten sofort entfernen.

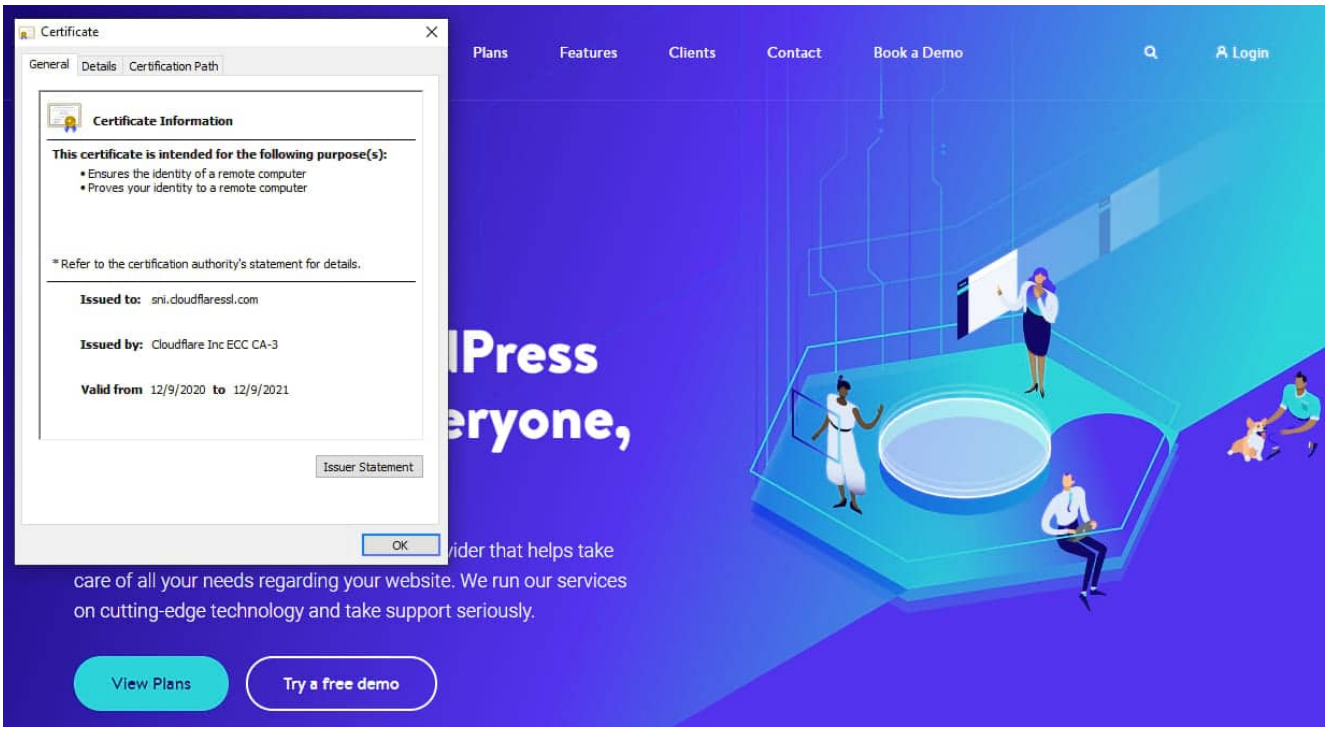
Wir empfehlen dir auch diesen Leitfaden zur Einschränkung von Benutzerrechten, damit nur dein Konto sensible Dateien auf deiner Webseite ändern kann.

Überprüfe dein SSL Zertifikat

Wenn dein SSL-Zertifikat veraltet ist, merkst du das in der Regel sofort; Browser wie Google Chrome blockieren den Zugriff auf deine Webseite mit einer großen Warnung über das abgelaufene Zertifikat. Wenn du dir nicht sicher bist oder bereits diesen Fehler bekommst, überprüfe dein SSL Zertifikat, um zu sehen, ob es auf dem neuesten Stand ist und ob du die neueste Version von SSL/TLS verwendest.

Wenn du eine Webseite besuchst, siehst du in den meisten Browsern ein Schloss-Symbol in der Adressleiste. Wenn dein Zertifikat abgelaufen ist, kann dieses Schloss rot sein oder einen Schrägstrich haben.

Klicke auf das Schlosssymbol und dann erneut, um Informationen zum Zertifikat zu erhalten, einschließlich des Ablaufdatums.



Überprüfe das SSL Zertifikat einer Webseite.

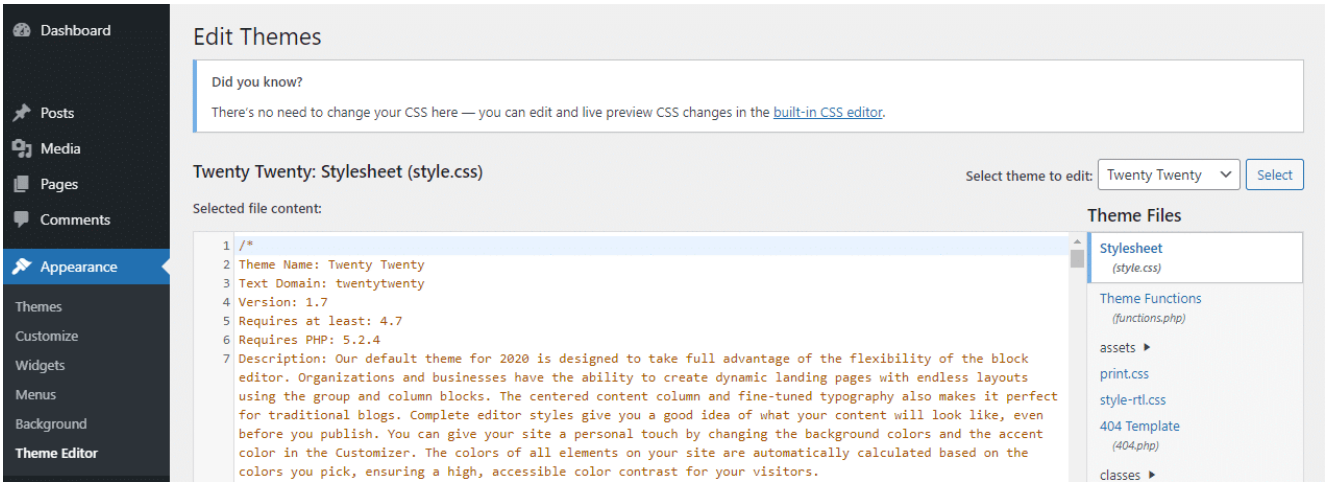
Du kannst auch einen SSL-Zertifikatschecker verwenden, um deine Webseite zu scannen und sicherzustellen, dass dein Zertifikat nicht abgelaufen ist und keine Schwachstellen in deinem SSL-Protokoll vorhanden sind.

Häufige Schwachstellen

Viele WordPress Seiten sind voll von winzigen Angriffsvektoren, die zwar harmlos erscheinen, aber mehr Informationen liefern können, als du teilen willst.

Eine sichtbare WordPress-Version in deinem Frontend verrät Hackern genau, welche Schwachstellen auf deiner Webseite vorhanden sind. Besonders, wenn du eine veraltete Version von WordPress verwendest, solltest du diese Informationen verstecken.

In deinem Backend findest du Dateieditoren unter **Appearance** > **Theme Editor** und **Plugins** > **Plugin Editor**.



Hinzufügen von Code zum Theme Editor

Diese Tools sind zwar sehr praktisch, aber es macht sie auch für jeden geeignet, der deine Webseite hackt, um etwas zu kaputt zu machen, also solltest du sie vielleicht abschalten. Du kannst dies tun, indem du diese Funktion in die **wp-config.php** einfügst:

```
define( 'DISALLOW_FILE_EDIT', true );
```

SQL-Injektionen sind eine gängige Methode, um in eine Webseite einzubrechen. Wenn du Formulare oder andere Benutzereingaben hast, schränke die Verwendung von Sonderzeichen ein und erlaube nur sichere, gebräuchliche Dateitypen, die hochgeladen werden können.

Für einen zusätzlichen Schutz kannst du Dateiverzeichnisse mit einem Passwort schützen.

Wie du deine Webseite sicher machst: Tipps und Tools

Wenn deine Webseite mit Malware infiziert ist, sollte ein gutes Sicherheits-Plugin ausreichen, um es zu entfernen. Und wir haben oben ein paar Sicherheitslücken beschrieben, auf die du achten solltest.

Schau dir unseren Video-Leitfaden zur Absicherung deiner Webseite an

Wir haben noch ein paar andere schnelle Tipps, um deine Webseite zu sichern und eine Infektion zu verhindern, bevor sie passieren kann. Die meisten dieser Tipps kannst du in wenigen Minuten umsetzen, so dass sie auch dann einfach einzurichten sind, wenn du dich mit WordPress und Websicherheit nicht auskennst.

Wähle einen sicheren Host

Wenn Hacker nach einem Weg auf deine Webseite suchen, wenden sie sich oft an den Server, um nach Exploits zu suchen. Es gibt viele billige Hosts, aber sie investieren nicht immer in die sichersten Server.

Shared Hosting kann ein Vektor für Infektionen sein. Wenn eine Webseite mit Malware infiziert ist, kann es sich potenziell auf alle Webseiten auf dem Server ausbreiten. Du könntest also mit einer Webseite voller Viren und SEO-Spam enden, und es wäre nicht einmal deine Schuld.

Deshalb ist es wichtig, dass du einen Hoster wählst, der sich um die Sicherheit kümmert und in sichere Server investiert. Du wirst immer noch Arbeit investieren müssen, um deine Webseite zu sichern, aber auf Server-Ebene sind deine Daten sicher.

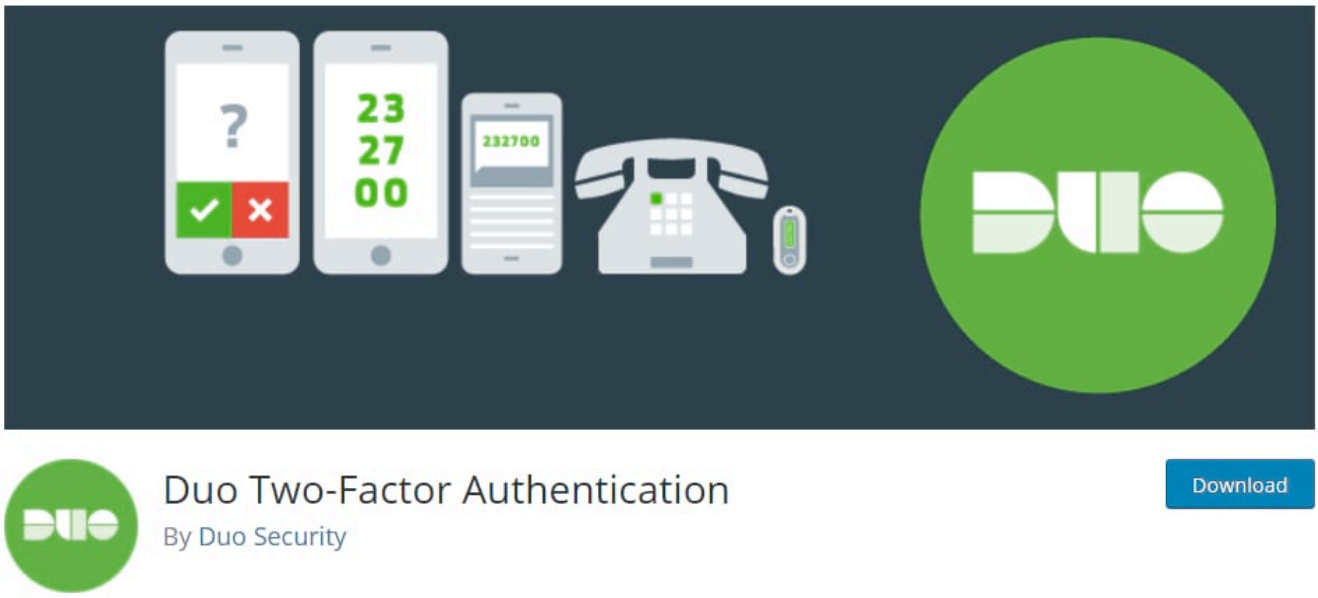
Aktiviere die Zwei-Schritt-Authentifizierung (2FA)

Die zweistufige Authentifizierung (auch bekannt als Zwei-Faktor-Authentifizierung oder 2FA) fügt einen weiteren Anmeldeschritt hinzu. Neben Benutzername und Passwort brauchst du oder jemand, der sich für dich ausgibt, noch eine weitere Information: einen einzigartigen Zusatzcode.

Es könnte ein Zahlencode sein, der an dein Telefon geschickt wird, was deinen WordPress-Account durch Brute-Force nahezu unknackbar machen kann. Alternativ kann es auch eine E-Mail-Verifizierung oder eine Information sein, die nur du kennst.

Während es keine eingebaute Möglichkeit gibt, die Zwei-Faktor-Authentifizierung zu aktivieren, fügen viele Plugins die Funktionalität zu WordPress hinzu.

Kinsta bietet die Zwei-Faktor-Authentifizierung für alle Kunden an. Wenn du kein Kinsta-Kunde bist, kannst du auch das bereits erwähnte Wordfence Plugin mit integrierter 2FA nutzen. Du kannst auch andere Tools für die Sicherheit deiner Webseite ausprobieren, wie z.B. das Two-Factor Plugin für E-Mail-Codes oder Duo, um eine Zwei-Faktor-Authentifizierung per Telefon über eine App einzurichten.



Duo Zwei-Faktor-Authentifizierung Plugin

Mache jeden Tag Backups

Ein Backup deiner Webseite kann sie nicht vor Hackern schützen, aber falls doch einmal etwas passiert, ist ein Backup von unschätzbarem Wert. Es kann den Unterschied ausmachen, ob du Wochen oder sogar Jahre an Arbeit verlierst oder ob du einfach ein Backup von vor dem Hack wiederherstellst.

Wenn du bei Kinsta bist, sichern wir dich mit täglichen automatischen Backups ab, die zwei Wochen lang gespeichert werden (30 Tage für diejenigen mit Kinstas Agenturpartnerprogramm). Zusätzlich kannst du fünf manuelle

Backups und ein herunterladbares Backup pro Woche erstellen und es gibt optionale Add-Ons, um stündlich Backups zu erstellen oder in die Cloud zu exportieren.

Plugins wie UpdraftPlus können ebenfalls helfen. Am besten ist es, einen Dienst zu wählen, der mindestens täglich ein Backup erstellt, um den Datenverlust zu minimieren.

Verwende eine Web Application Firewall

Eine Web Application Firewall (WAF) filtert mit strengen Regeln den eingehenden Traffic und blockiert IPs, die bekanntermaßen mit Hacker- oder DDoS-Angriffen in Verbindung gebracht werden. Es verhindert, dass viele Angriffe deinen Server überhaupt erreichen.

Obwohl du WAFs auf Serverebene einsetzen kannst, ist es am einfachsten, einen Cloud-basierten Service zu kaufen, wie zum Beispiel von Cloudflare oder Sucuri.

Verbindung über SSH oder SFTP

Manchmal musst du dich per FTP mit deiner Webseite verbinden, um dort Dateien hinzuzufügen oder zu ändern. Es ist immer besser, SFTP gegenüber FTP zu verwenden; der Unterschied ist einfach: SFTP ist sicher und FTP ist es nicht.

Bei FTP sind deine Daten nicht verschlüsselt. Wenn es jemandem gelingt, die Verbindung zwischen dir und deinem Server abzufangen, kann er alles sehen, von deinen FTP-Zugangsdaten bis zu den Dateien, die du hochlädst. Verbinde dich immer mit SFTP.

Du könntest auch einen SSH-Zugang in Betracht ziehen, der es dir erlaubt, dich mit einer Aufforderung zu verbinden und deine Webseite direkter zu verwalten. Es ist sicher und kann einfache Aufgaben aus der Ferne erledigen. Unser Guide zu SSH kann dir helfen, wenn du nicht weiterkommst.

Verhindere DDoS-Attacken

DDoS-Attacken verlangsamen deine Webseite zu einem Kriechgang, indem sie deinen Server mit tausenden von gefälschten Anfragen überschwemmen und so verhindern, dass potenzielle Leser oder Kunden auf sie zugreifen können. Hier sind ein paar Tipps, um sie zu stoppen, bevor sie passieren:

- Habe einen Plan für den Fall, dass ein DDoS-Angriff zuschlägt. Du willst nicht in Panik geraten, wenn du deinen Host alarmieren und die Attacke stoppen musst.
- Verwende eine Web Application Firewall, die möglicherweise gefälschten Traffic erkennen kann.
- Verwende speziell zugeschnittene Anti-DDoS-Software.
- Deaktiviere xmlrpc.php, um zu verhindern, dass Apps von Drittanbietern deinen Server nutzen.
- Deaktiviere die REST API für allgemeine Benutzer.

Brute-Force-Attacken verhindern

Brute-Force-Angriffe können ähnlich wie DDoS-Attacken sein, aber das Ziel ist es, dein Admin-Passwort zu erraten und in deine Webseite einzubrechen, anstatt deinen Server zum Absturz zu bringen. Trotzdem können sie auch deine Webseite ausbremsen.

- Auch hier kann eine WAF Bot-Traffic und krasse Brute-Force-Versuche herausfiltern.
- Verwende eine zweistufige Authentifizierung für deinen Admin-Account.
- Richte ein Aktivitätsprotokoll ein und behalte unautorisierte Login-Versuche im Auge.
- Ändere die URL der Login-Seite und begrenze die Anzahl der Login-Versuche.
- Schütze deine Anmeldeseite mit einem Passwort.
- Verwende ein langes, zufällig generiertes Passwort und

ändere es etwa alle Jahre.

Webseiten Security Tools, die du kennen solltest

Neben den bereits erwähnten Tools gibt es noch ein paar weitere Online-Sicherheitstools, die dir dabei helfen werden, deine Webseite abzusichern:

- Intruder.io: Scanne nach den neuesten Sicherheitslücken.
- SSL Server Test: Entwickler-Tool, das dein SSL Zertifikat analysiert und Schwachstellen identifiziert.
- HTML Purifier: Filtert bösartigen Code/XSS heraus, toll, wenn du infizierten Code hast, den du bereinigen musst.
- Mozilla Observatory: Umsetzbare Ratschläge, um deinen Code von häufigen Schwachstellen zu bereinigen.
- sqlmap: Ein Penetrationstest Tool, um Exploits in deinem SQL Code zu identifizieren.
- Detectify: Scanne deine Web-Apps mit der Hilfe von ethischen Hackern.
- WPScan: Ein CLI-basierter WordPress-Scanner.
- SonarQube: Schreibe standardkonformen Code frei von Sicherheitslücken.

Webseiten Sicherheit Checkliste

Ist deine Webseite sicher vor Angriffen? Stelle sicher, dass du fast alles auf dieser Checkliste angekreuzt hast:

- Nutzt du eine sichere, qualitativ hochwertige Hosting Umgebung?
- Hast du deine Webseite mit einem Plugin oder Online-Scanner auf Viren überprüft?
- Hast du ein Aktivitätsprotokoll installiert und

überwachst du es auf ungewöhnliche Änderungen?
- Verwenden du und alle Benutzer mit hohen Privilegien sichere Passwörter und Zwei-Faktor-Authentifizierung? Sind alle Emails korrekt?
- Sind WordPress, seine Themes und Plugins sowie die zugrunde liegenden Systeme wie PHP auf dem neuesten Stand?
- Ist dein SSL Zertifikat sicher und auf dem neuesten Stand?
- Hast du deine Webseiten, Einstellungen und Dateien auf unerklärliche Änderungen, das Löschen oder Hinzufügen von Inhalten oder Links, die du nicht hinzugefügt hast, überprüft?
- Ist deine Login-Seite durch ein Passwort und begrenzte Login-Versuche geschützt?
- Hast du nach neuen Benutzern gesucht, die du nicht hinzugefügt hast?
- Sind Formulare, Kommentarboxen und andere Quellen für Benutzereingaben gesichert? (Verbiete Sonderzeichen und beschränke Datei-Uploads auf bekannte Dateitypen).
- Hast du **xmlrpc.php** und die REST API deaktiviert, um DDoS-Angriffe zu verhindern?
- Hast du die Bearbeitung von Themes und Plugins im Dashboard deaktiviert?
- Hast du einen täglichen Backup-Service eingerichtet?
- Hast du eine Web Application Firewall eingerichtet?

Zusammenfassung

Die Sicherheit einer Webseite ist keine Nebensache. Wenn du dich also noch nicht darum kümmerst, ist es jetzt an der Zeit, es zu einer Priorität zu machen. Wenn du gehackt wirst, ist das nicht nur ärgerlich – es kann in beschädigter SEO, verheerendem Datenverlust, verlorenem Vertrauen der Nutzer und Malware enden, die immer wieder zurückkommt.

Du musst kein erfahrener Entwickler sein, um ein paar zusätzliche Schritte zu unternehmen, um deine Webseite zu sichern. Und das beginnt mit einem ordentlichen Sicherheitscheck der Webseite. Selbst etwas so Einfaches wie die Wahl eines besseren Passworts oder der Wechsel zu einem sichereren Host kann den Unterschied ausmachen.

Brauchst du mehr Sicherheitstipps? Erfahre mehr über 19 weitere Möglichkeiten, deine Webseite zu sichern. Und teile deine Vorschläge gerne in den Kommentaren unten!

So testen Sie Ihre WordPress-Site auf Funktionalität, Geschwindigkeit und

Sicherheit

Warum sind WordPress-Tests wichtig?

Es gibt viele Vorteile, wenn du deine WordPress-Website regelmäßig testest. Wie bereits erwähnt, kannst du mit dem Design und den Elementen der Benutzeroberfläche (UI) experimentieren, ohne dass dies Auswirkungen auf deine Live-Site hat.

So kannst du deine aktuelle Website beibehalten und den Geschäftsbetrieb aufrechterhalten, während du neue Ideen ausprobierst. Wenn in der Testumgebung etwas schief geht, musst du dir keine Sorgen über die Auswirkungen machen, die ein Ausfall auf deinen Webverkehr und deine Einnahmen haben könnte.

Andererseits kannst du deine WordPress-Website auch testen, um Probleme zu erkennen, die Besucher/innen haben könnten, wenn sie versuchen, deine Seiten aufzurufen. Zum Beispiel kann es sein, dass deine Seite in einem bestimmten Browser langsam läuft oder dass dein Menü auf mobilen Geräten nicht richtig angezeigt wird.

Außerdem kann eine Testumgebung eine gute Möglichkeit sein, um Sicherheitslücken zu vermeiden. Vielleicht möchtest du neue Plugins und Themes ausprobieren, bevor du sie auf deiner Website installierst. In der Zwischenzeit kannst du Updates auf deiner Testseite durchführen, um sicherzustellen, dass sie sicher sind.

Während viele Anfänger/innen davon profitieren können, mit WordPress in einem sicheren, privaten Umfeld zu experimentieren, ist das Testen auch für fortgeschrittene Entwickler/innen sehr wichtig. Mit den richtigen Tools können Entwickler/innen eine permanente Testumgebung einrichten, um

die Funktionalität ihrer Produkte zu testen, bevor sie sie der Öffentlichkeit zugänglich machen.

Was sind die gängigsten Arten von Tests?

Da du nun weißt, warum es wichtig ist, WordPress sicher zu testen, werfen wir einen Blick auf einige der gängigsten Methoden.

- **Funktionstests.** So kannst du dir ein genaues Bild davon machen, wie sich die Nutzer/innen auf deiner Seite bewegen. Du kannst zum Beispiel überprüfen, ob Formulare, Buttons und Checkout-Seiten richtig funktionieren.
- **Leistungs- und Geschwindigkeitstests.** Wenn du sicherstellst, dass deine Website schnelle Ladezeiten hat, kannst du die Benutzerfreundlichkeit verbessern, die Suchmaschinenoptimierung (SEO) unterstützen und deine Core Web Vitals verbessern.
- **Sicherheitstests.** Dazu gehört die Analyse der Sicherheitsmechanismen auf deiner Website, wie SSL-Zertifikate, HTTPS, Web Application Firewalls und mehr. Sie hilft dir, sensible Daten zu schützen, böswillige Angriffe zu verhindern und WordPress-Schwachstellen zu erkennen.

Unabhängig davon, welche Art von Website du betreibst, solltest du dir angewöhnen, regelmäßig Funktions-, Leistungs- und Sicherheitstests durchzuführen.

Best Practices für WordPress-Tests

Es ist wichtig, den Wert der Tests deiner Website in verschiedenen Umgebungen zu erkennen. Wenn du den Unterschied

zwischen den verschiedenen Umgebungen kennst, ist es einfacher, die richtige Option für deine Bedürfnisse zu wählen.

Eine lokale Umgebung wird auf deinem eigenen Computer gehostet. Daher hat nichts, was du dort tust, Auswirkungen auf deine Live-Site. Für den allgemeinen Gebrauch bietet sie eine gute Möglichkeit, neue Funktionen und Features zu testen. Für Entwicklerinnen und Entwickler ist eine lokale Umgebung der ideale Ort, um Bugs und Fehler in deinem Code zu finden.

Eine Staging-Umgebung hingegen bietet eine Kopie der Daten deiner Website auf einem Server (und nicht auf einem lokalen Rechner). Sie ist der ideale Ort, um größere Versions-Updates, Konfigurationsänderungen und Datenbankmigrationen durchzuführen. Wenn du Websites für Kunden entwirfst, eignet sich eine Staging-Site außerdem gut als Demo-Site, um den Kunden zu zeigen, wie die Website aussehen wird.

Wie du Testumgebungen einrichtest

Jetzt, wo du die verschiedenen Arten von Testumgebungen besser kennst, schauen wir uns an, wie du sie einrichtest!

So richtest du eine Testumgebung mit einer Staging-Site ein

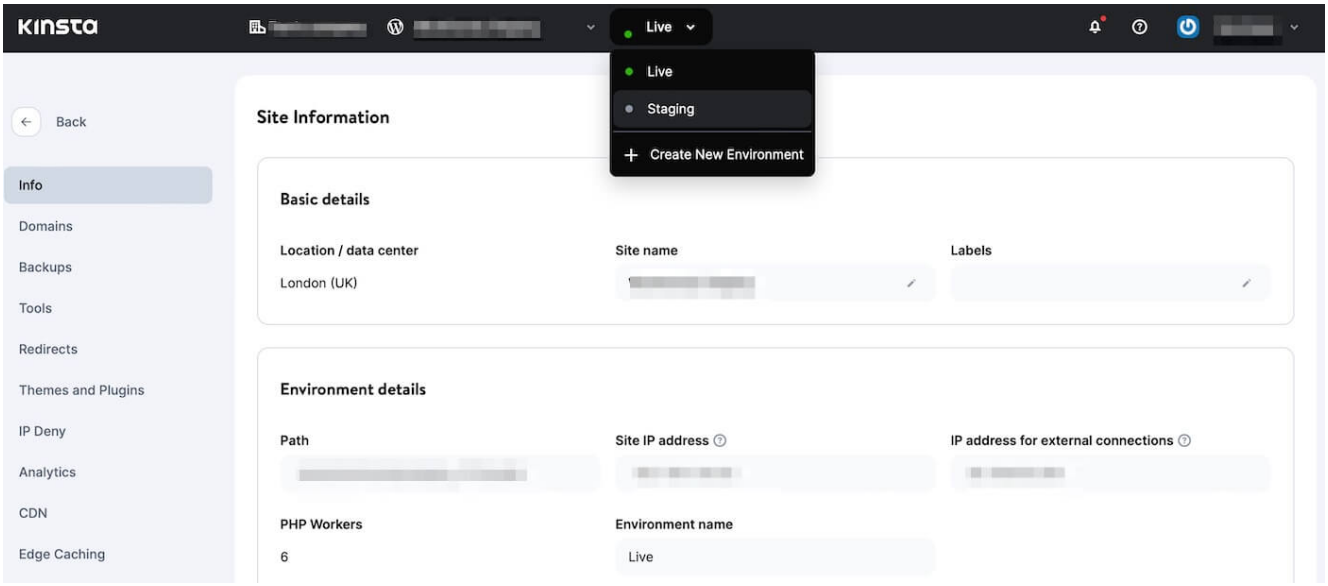
Wie bereits erwähnt, ist eine Staging-Site im Grunde eine vollständige Kopie deiner Live-Website. Normalerweise wird sie auf demselben Server gehostet wie deine Live-Website. Der einzige Unterschied besteht darin, dass Besucher/innen nicht auf sie zugreifen können.

Das Beste am Staging ist, dass es einem realen Aufbau folgt. So kannst du genau nachvollziehen, wie sich die Kunden auf deinen Seiten bewegen.

Der einfachste Weg, eine Staging-Site einzurichten, führt über deinen Webhoster. Nicht alle Webhoster bieten Staging-

Umgebungen mit ihren Hosting-Diensten an. Aber bei Kinsta ist es super einfach, die integrierte WordPress-Staging-Umgebung zu erstellen und zu konfigurieren.

Du kannst auf deine Staging-Site zugreifen, indem du dich in dein MyKinsta-Dashboard einloggst. Wähle einfach deine Website aus der Liste aus. Oben auf dem Bildschirm kannst du dann über das Dropdown-Menü von **Live** zu **Staging** wechseln:



Eine Staging-Site mit Kinsta einrichten

Denke daran, dass es bis zu fünfzehn Minuten dauern kann, bis deine Staging-Site zum ersten Mal erstellt wird. Danach wird sie als Subdomain deiner Hauptdomain existieren (beide nutzen denselben Server).

Sobald du bereit bist, die Änderungen auf deine Live-Website zu übertragen, kannst du einfach die Schaltfläche **Push-Umgebung** in deinem Dashboard verwenden.

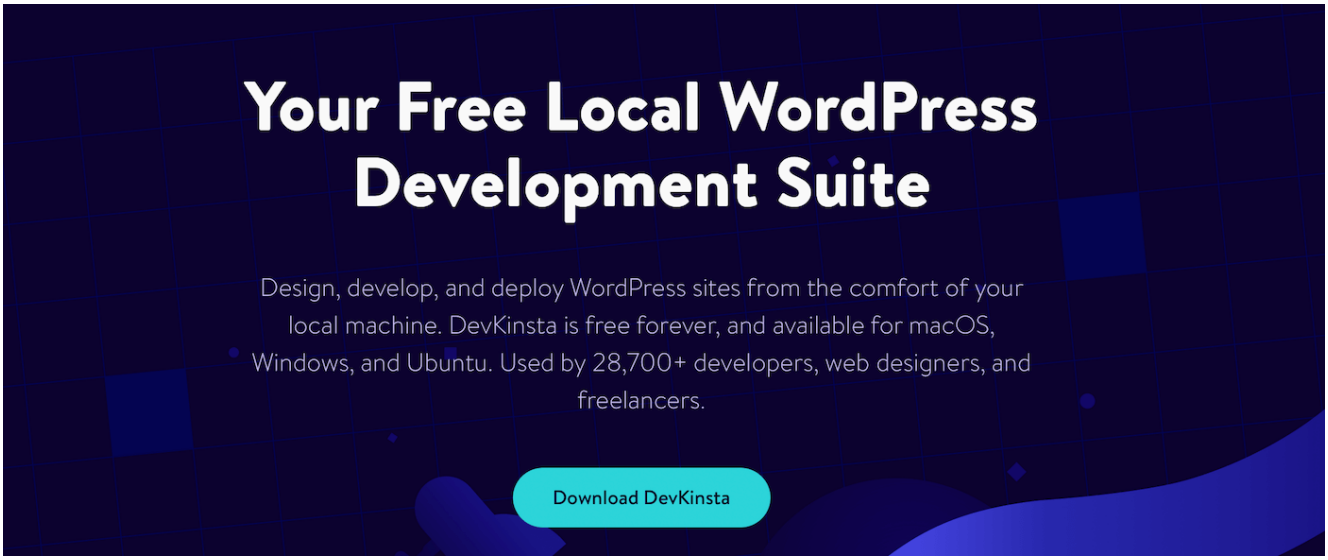
Wie du eine lokale Testumgebung einrichtest

Eine lokale Umgebung funktioniert ähnlich wie eine Staging-Site, allerdings musst du die Umgebung nicht extern hosten. Stattdessen befindet sich deine lokale Umgebung auf einem lokalen Rechner (meistens auf deinem Computer).

Um eine WordPress-Testumgebung lokal zu installieren, musst du dir einen AMP-Stack für deinen Computer besorgen. Diese

Software (Apache, MySQL und PHP) wird verwendet, um deine echte WordPress-Website zu imitieren.

Einige der beliebtesten Möglichkeiten, WordPress lokal zu installieren, sind WAMP und XAMPP. Der einfachste Weg ist jedoch die Verwendung von DevKinsta:



Verwende DevKinsta, um eine lokale Umgebung zu erstellen

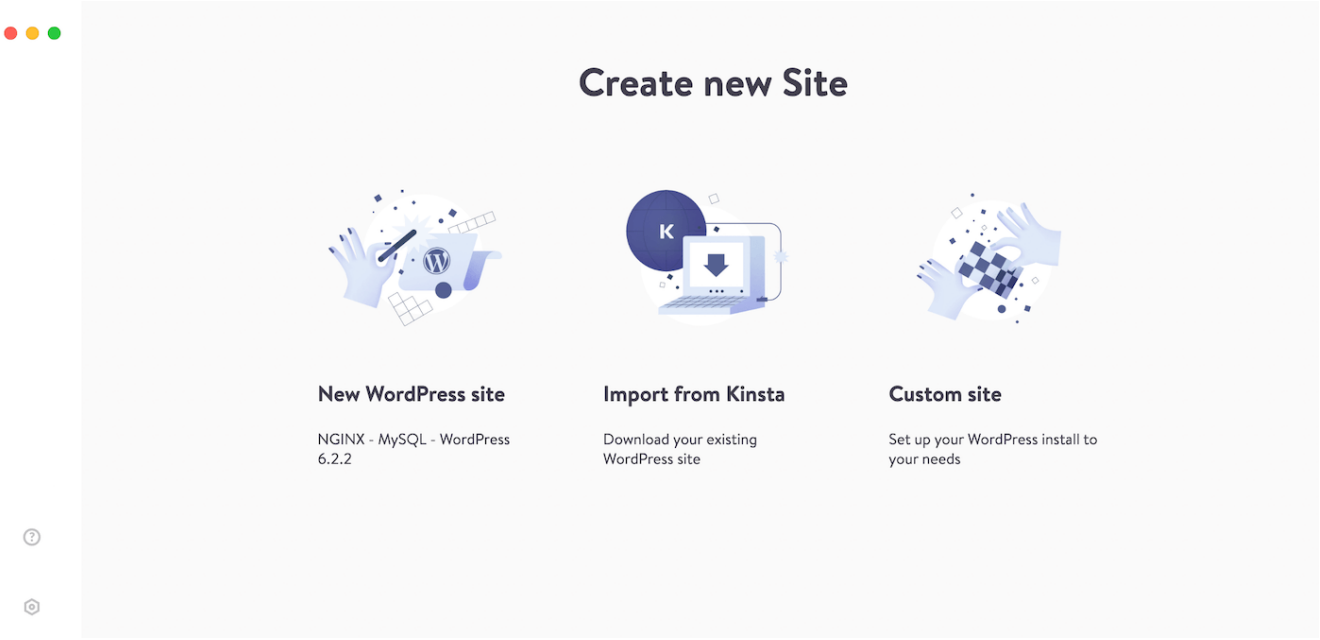
DevKinsta ist ein kostenloses lokales Entwicklungstool für WordPress Single oder Multisite. Mit DevKinsta erhältst du Zugang zu einer Vielzahl von Datenbank- und E-Mail-Verwaltungstools. Außerdem lässt es sich nahtlos in MyKinsta integrieren (du musst allerdings kein Kinsta-Kunde sein, um DevKinsta zu nutzen).

Um loszulegen, musst du die neueste Version von DevKinsta herunterladen. Auf dem Mac fügst du DevKinsta zu **Programme** hinzu und öffnest die DevKinsta-App mit einem Doppelklick.

Der Installationsprozess unterscheidet sich leicht von Betriebssystem zu Betriebssystem, aber du kannst bei Bedarf die vollständige Installationsanleitung für DevKinsta einsehen. Anschließend kannst du Docker Desktop installieren, um Container für das lokale WordPress zu erstellen.

Sobald du DevKinsta und Docker erfolgreich installiert hast, kannst du deine lokale Website erstellen. Du kannst entweder eine neue WordPress-Site erstellen, eine bestehende Site von

Kinsta importieren oder eine eigene Site erstellen:



Eine lokale Website mit DevKinsta erstellen
Wähle einfach deine bevorzugte Option. Wenn du eine Website von Kinsta importierst, musst du die richtige Website für den Import auswählen und deine Anmeldedaten eingeben. Dann wirst du zum Bildschirm mit **den Website-Informationen** weitergeleitet, der wie ein Dashboard für deine lokale Umgebung funktioniert.

Du kannst die Kinsta-API auch nutzen, um eine neue WordPress-Seite/Installation zu erstellen, ohne auf DevKinsta zuzugreifen.

So testest du die Funktionalität deiner WordPress-Website (5 Funktionen)

Sehen wir uns nun fünf Möglichkeiten an, wie du die Funktionalität deiner WordPress-Website testen kannst. Das Beste an den Funktionstests ist, dass du sie direkt in deiner lokalen Umgebung oder mit DevKinsta durchführen kannst (im Gegensatz zu anderen Testarten, bei denen deine Website live sein muss).

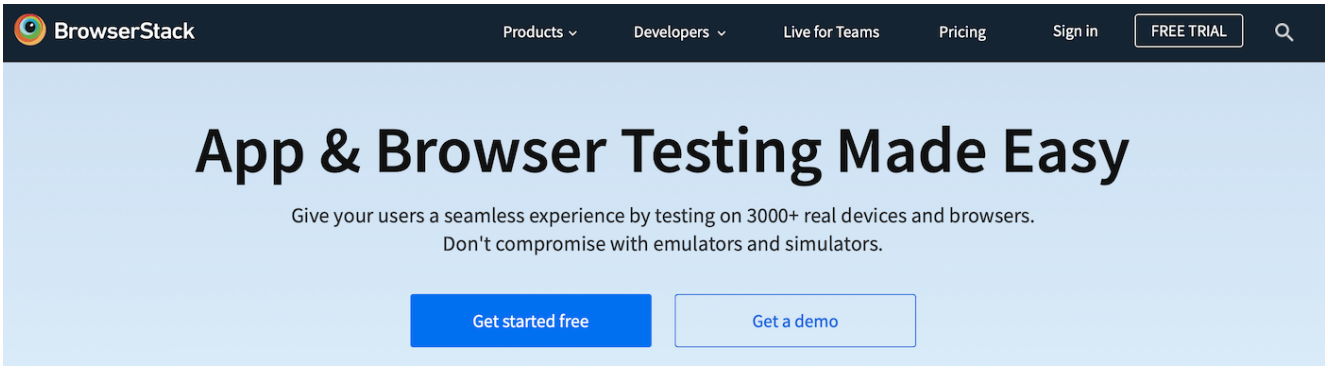
Cross-Browser-Unterstützung

Es ist wichtig, deine WordPress-Website in verschiedenen Browsern zu testen, um zu sehen, wie deine Website für alle Besucher aussieht. Das liegt daran, dass verschiedene Browser unterschiedlichen Code verwenden. Daher behandelt und zeigt jeder Browser Elemente auf seine eigene Weise an.

Ein Nutzer, der deine Website mit Chrome aufruft, sieht sie vielleicht anders als ein Nutzer, der deine Website mit Firefox besucht. Und obwohl 3,2 Milliarden Internetnutzer/innen im Jahr 2021 Chrome als Hauptbrowser bevorzugen, nutzen viele weiterhin Firefox, Edge, Opera und Safari.

Vielleicht möchtest du herausfinden, welche Browser bei deinen Besuchern beliebt sind, um deine Seite speziell für diese Browser zu optimieren. Wenn du Google Analytics verwendest, kannst du diese Informationen in deinen Besucherberichten finden.

Dann kannst du deine Website mit einem Tool wie BrowserStack auf Browserunterstützung testen:



Browserübergreifende Tests mit BrowserStack durchführen

Mit BrowserStack kannst du deine Website in 3000 verschiedenen Browsern testen, darunter die neuesten Versionen von Edge, Safari, Firefox und Chrome. Du kannst auch eine kostenlose Testversion nutzen, bevor du dich für einen kostenpflichtigen Plan entscheidest.

Unit-Tests

Beim Unit Testing wird die kleinste Einheit einer Anwendung isoliert getestet. Das kann eine Funktion, eine Eigenschaft oder eine Methode sein. Diese Einheiten werden dann auf ihre Funktionstüchtigkeit untersucht, um sicherzustellen, dass sich die Anwendung wie erwartet verhält.

Du kannst Unit-Tests automatisch mit einem Drittanbieter-Tool wie Travis CI durchführen. Es ist jedoch schneller, die Tests lokal während der Entwicklung durchzuführen, als Änderungen vorzunehmen und darauf zu warten, dass Travis CI sie ausführt.

Du könntest zum Beispiel ein Theme oder ein Plugin einem Unit-Test unterziehen. Hierfür musst du Git, SVN, PHP und Apache installieren. Außerdem musst du dein Plugin fertig haben.

Um loszulegen, öffne DevKinsta, um deine lokale Entwicklungsumgebung zu starten. Installiere dann PHPUnit. Nun musst du die Testdateien für das Plugin mit folgendem Befehl erstellen:

bash
```
wp scaffold plugin-tests my-plugin
```

Jetzt kannst du die Testumgebung lokal initialisieren, indem du das Installationsskript ausführst:

bash
```
bash bin/install-wp-tests.sh wordpress_test root '' localhost latest
```

Dieses Skript installiert eine Kopie von WordPress auf /tmp directory und in den WordPress Unit Testing Tools.

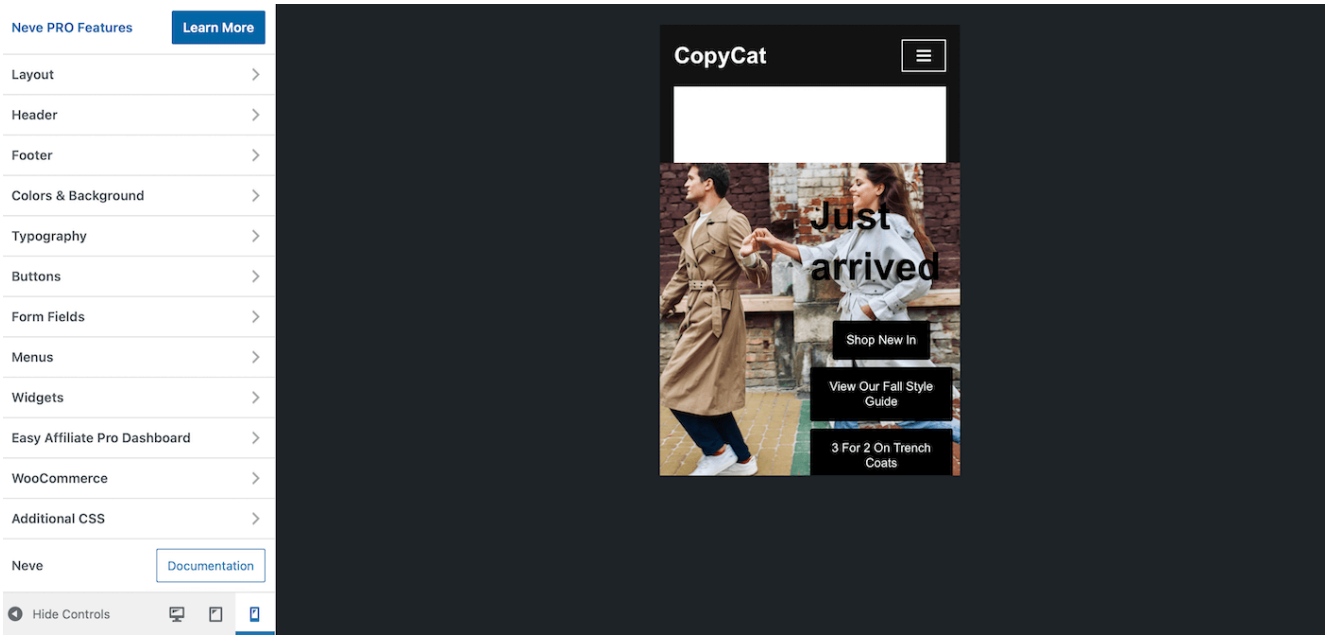
Im nächsten Schritt führst du die Plugin-Tests mit Hilfe von phpunit aus. Eine ausführliche Anleitung findest du in diesem Leitfaden zu Unit-Tests.

Responsivität für Mobilgeräte/Desktop

Da über 60 Prozent der Menschen mit einem mobilen Gerät online gehen, ist es wichtiger denn je, dass deine WordPress-Website responsive ist. Auf diese Weise kannst du sicherstellen, dass deine Seiten auf allen Bildschirmgrößen, einschließlich Desktop, Tablet und Handy, reibungslos angezeigt werden.

Am einfachsten kannst du die Reaktionsfähigkeit deiner Website testen, indem du die URL deiner Website auf deinem mobilen Gerät eingibst. Wenn du jedoch die Darstellung deiner Website von deinem Desktop aus testen möchtest, kannst du den WordPress Customizer verwenden.

Gehe einfach zu **Darstellung** > **Anpassen:**



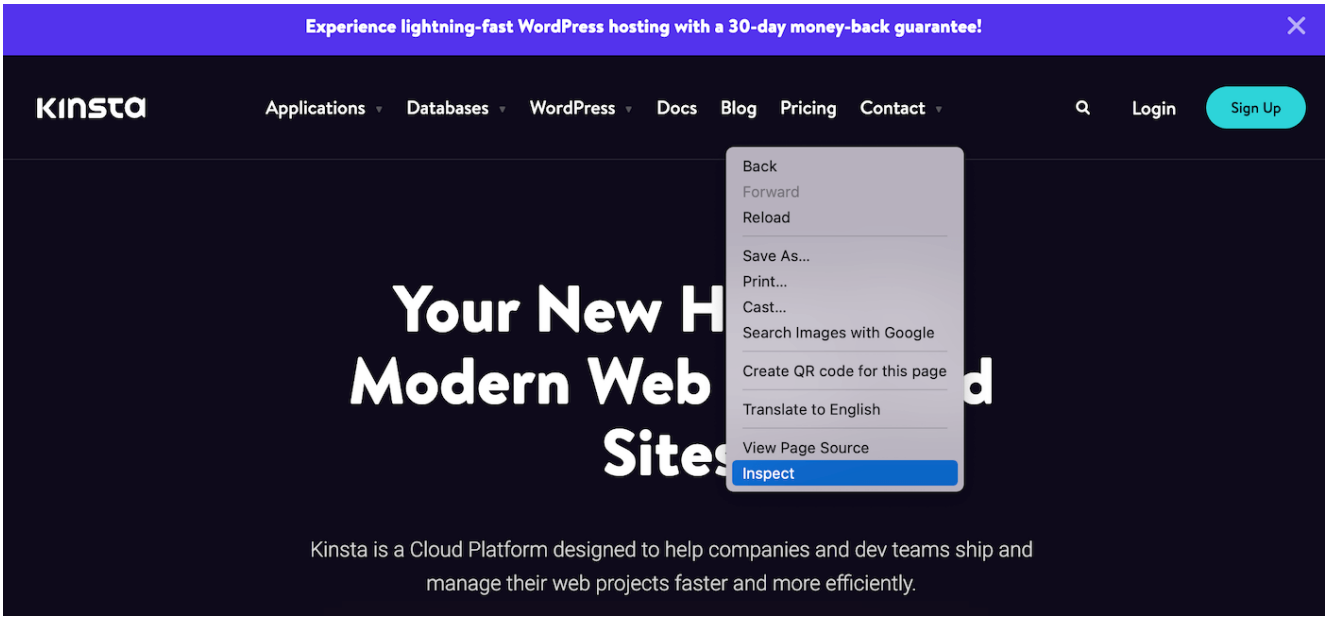
Teste die Reaktionsfähigkeit von WordPress mit dem WordPress Customizer

Je nach Theme siehst du unterschiedliche Panels. Unten auf deiner Seite kannst du auf das Symbol für Mobilgeräte oder Tablets klicken, um eine Vorschau deiner Website in der angegebenen Bildschirmgröße anzuzeigen.

Außerdem kannst du auf die Entwicklertools von Google Chrome zugreifen, um zu sehen, wie deine WordPress-Website auf mobilen Geräten aussieht. Dazu musst du nur eine Seite deiner

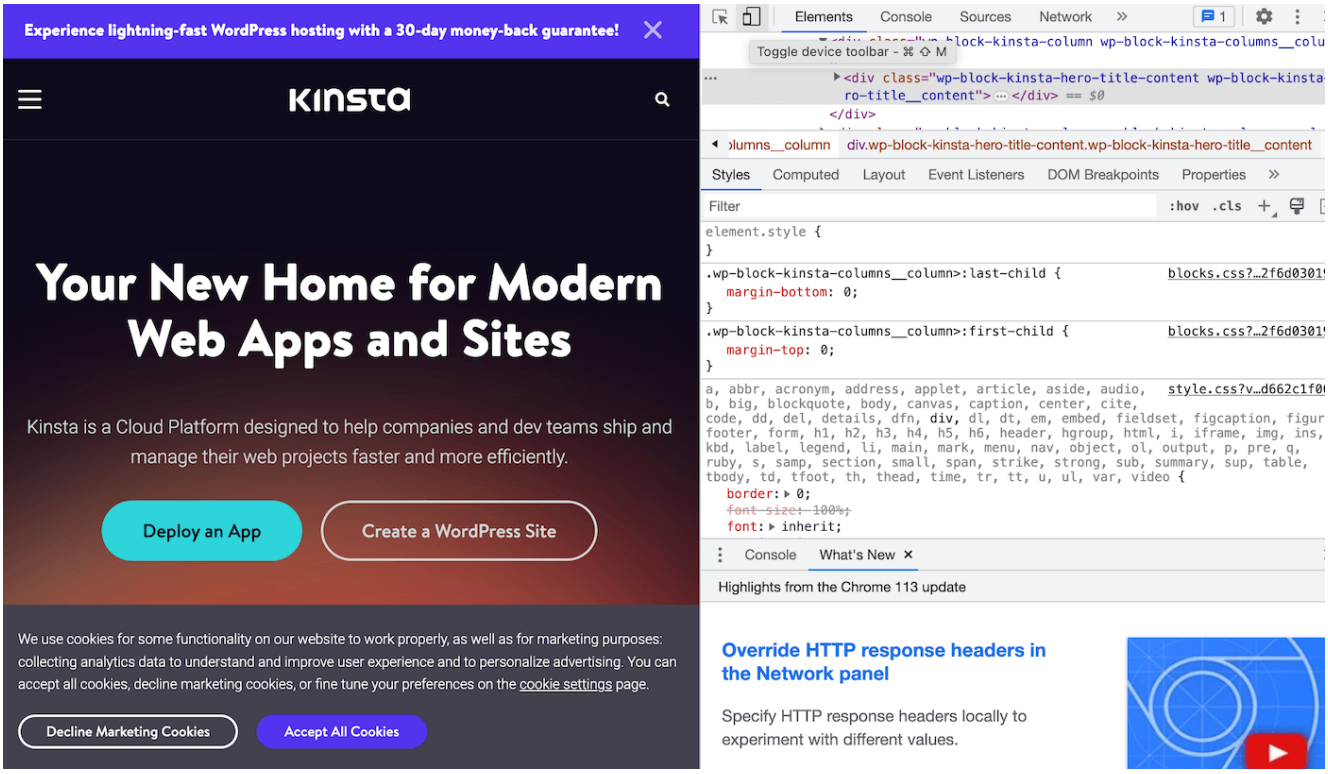
Website in Google Chrome öffnen.

Dann klickst du mit der rechten Maustaste auf die Seite und wählst **Inspizieren**:

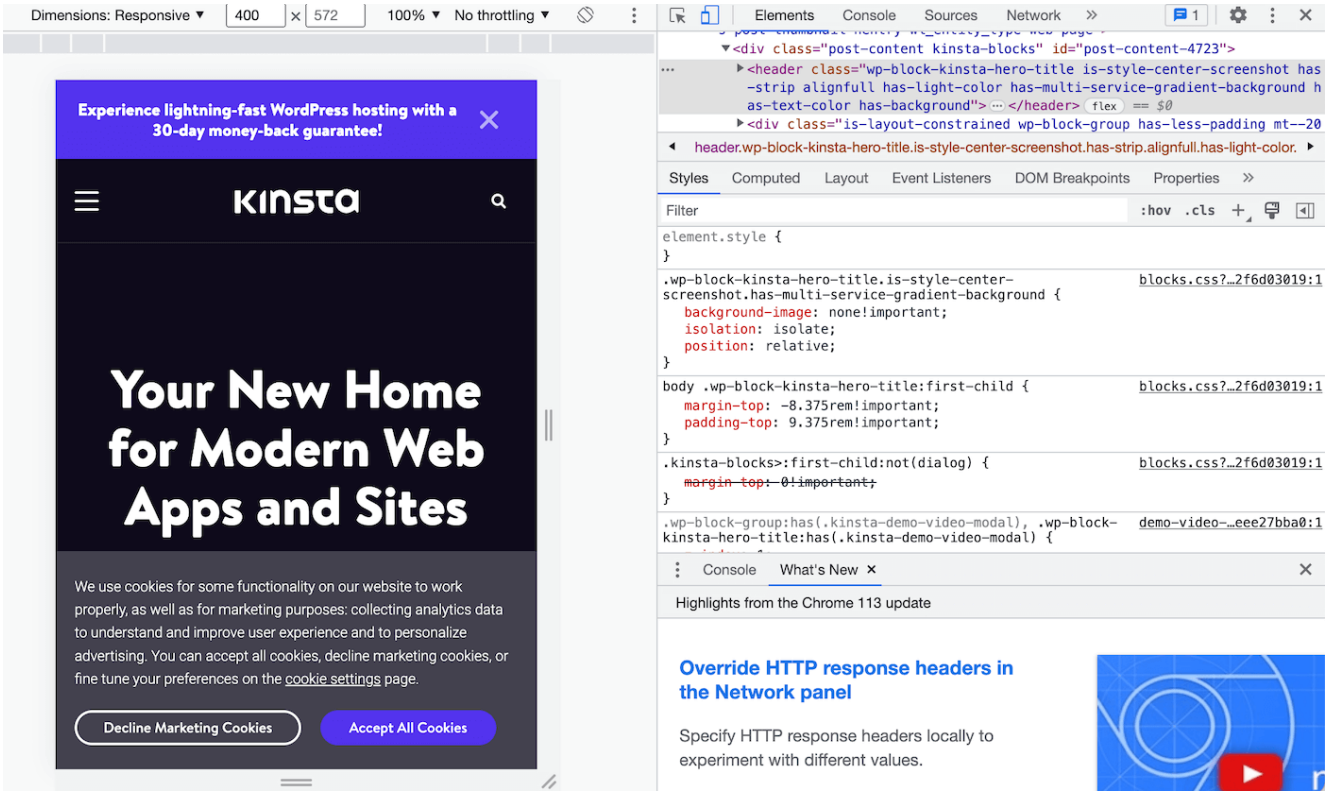


Teste die Reaktionsfähigkeit von WordPress mit Google Chrome Inspect

Jetzt suchst du die **Symbolleiste Gerät umschalten** oben im Popup (links neben dem Reiter **Elemente**):



Klicke auf die Symbolleiste Gerät umschalten in Chrome Inspect
Klicke darauf und dein Bildschirm wird sofort angepasst:



Betrachte deine Website in der mobilen Ansicht mit Google Chrome Inspect

Wie du siehst, kannst du jetzt testen, wie deine Website in **Responsive** Dimensionen angezeigt wird. Wenn du auf das Dropdown-Menü **Dimensionen** klickst, kannst du deine Seite auf weiteren Geräten testen, z. B. auf verschiedenen iPhone- und Samsung Galaxy-Modellen.

Testen der Benutzeroberfläche (UI)

Wenn wir von der Benutzeroberfläche (User Interface, UI) deiner Website sprechen, meinen wir damit alle Komponenten deiner Website, mit denen Besucher interagieren können. Die meisten Websites enthalten zum Beispiel Links, Schaltflächen, Menüs usw. Irgendwann müssen die Nutzer mit diesen Elementen interagieren.

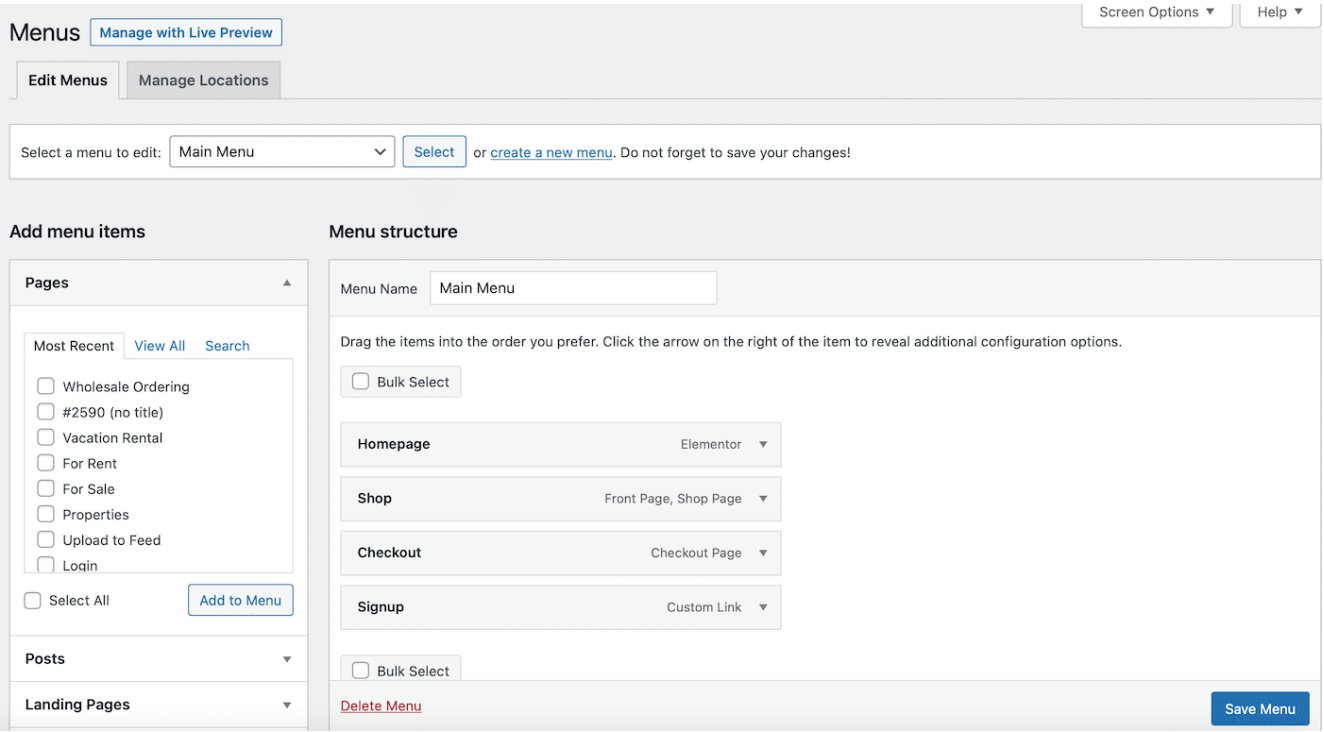
Deshalb ist es besonders wichtig, deine Benutzeroberfläche zu testen. Wenn etwas nicht richtig funktioniert, können Besucher/innen frustriert sein und deine Seite verlassen.

Du kannst eine lokale Umgebung einrichten, um deine UI-Elemente zu testen. Du könntest zum Beispiel ein neues

Navigationsmenü entwickeln und es ausprobieren.

In diesem Fall kannst du in deinem DevKinsta-Dashboard deinen lokalen Verwaltungsbereich öffnen. Dann navigierst du auf der lokalen Seite zu **Erscheinungsbild** > **Menüs** . Jetzt klickst du auf **Neues Menü erstellen**.

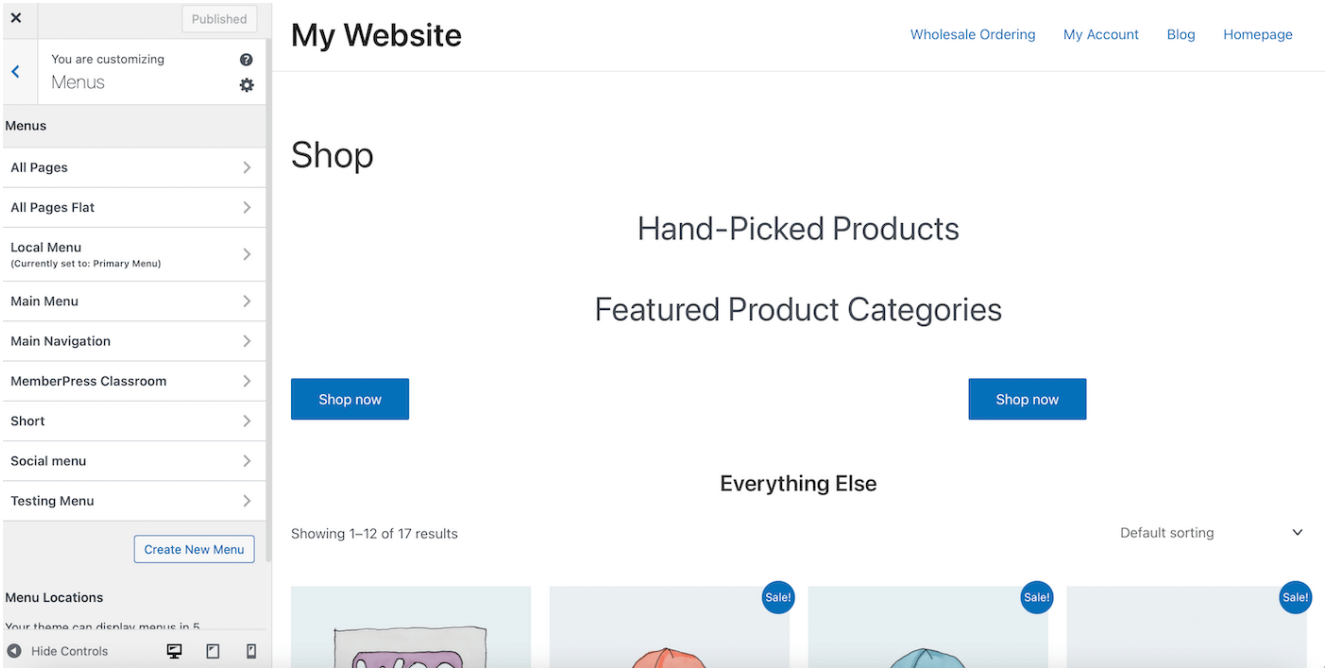
Gib deinem Menü einen Namen und klicke auf **Menü speichern**. Füge dann auf der linken Seite deines Bildschirms Menüpunkte hinzu und wähle **Zu Menü hinzufügen**:



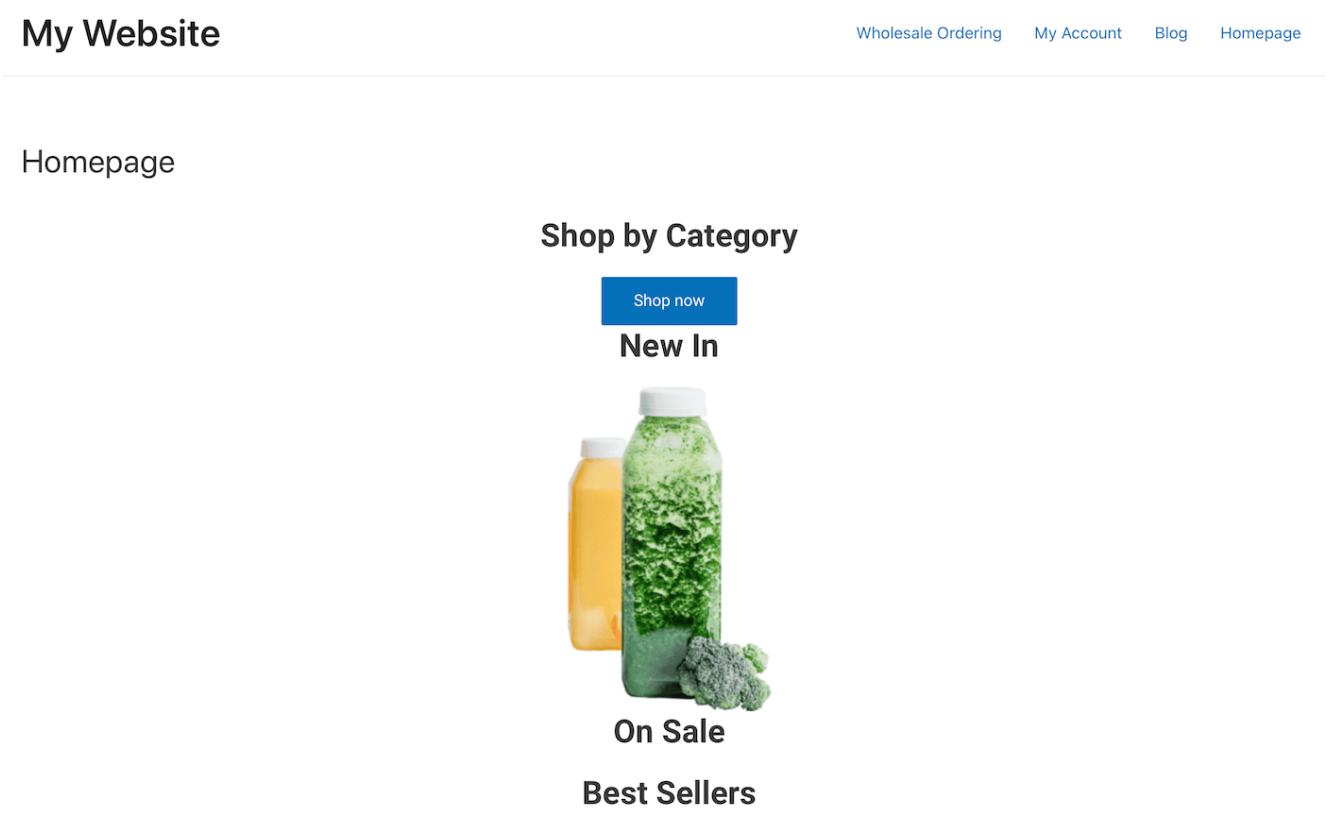
Lokales WordPress für UI-Tests

Aktiviere unter **Menüeinstellungen** das Kästchen **Primäres Menü**. Dann speicherst du deine Änderungen.

Du kannst auch auf **Verwalten mit Live-Vorschau** oben auf dem Bildschirm klicken, um zu sehen, wie sich dein Menü macht:

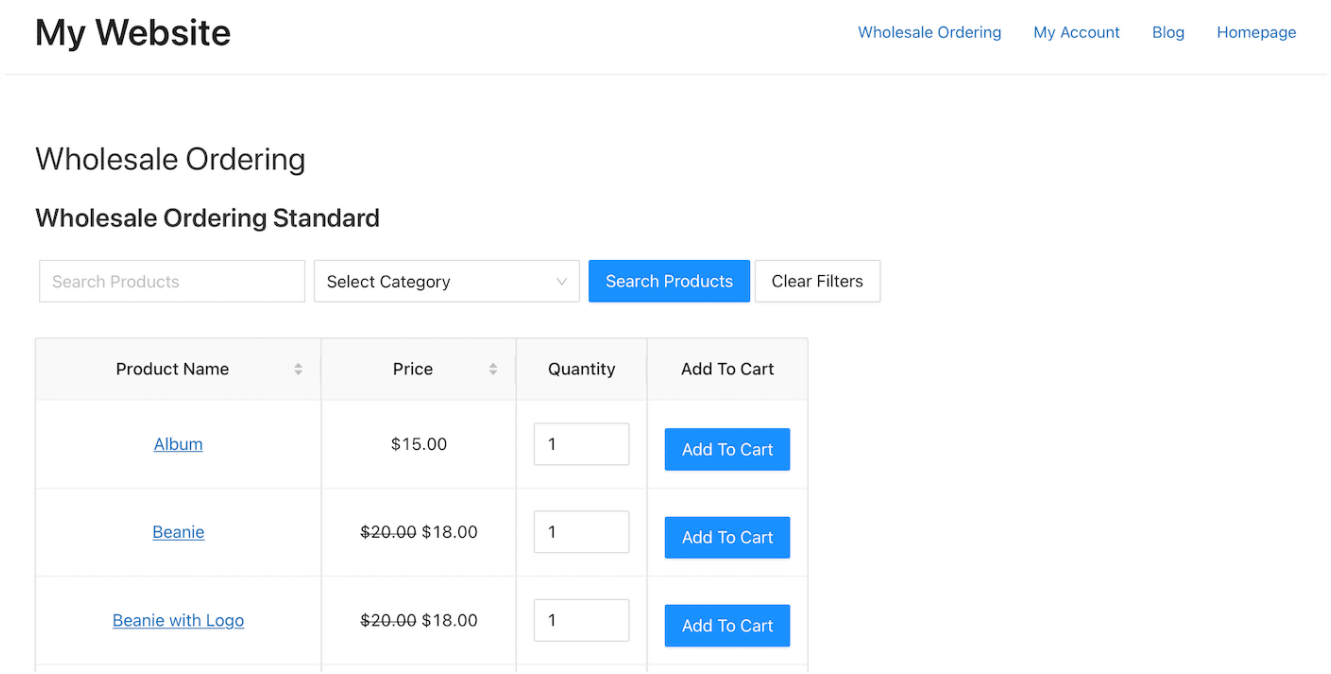


Dein lokales Menü mit Live-Vorschau anzeigen
Als Nächstes öffnest du deine lokale Website in einem neuen Browser, um dein neues Menü auf dem Frontend zu sehen:



Teste deine Benutzeroberfläche in deiner lokalen Umgebung
Du kannst auch die Navigationslinks testen, indem du auf jeden der Menüpunkte klickst. Wenn wir zum Beispiel auf den Link **Großhandelsbestellung** klicken, werden wir zu der entsprechenden Seite weitergeleitet, die wir unserem Menü

hinzugefügt haben:



Menülinktests in lokaler Umgebung
Auf diese Weise kannst du neue Designelemente testen und sicherstellen, dass deine Benutzeroberfläche richtig funktioniert.

Visuelle Tests

Visuelle Regressionstests (VRT) stellen sicher, dass alle deine Designelemente und Layouts so aussehen, wie sie sollen. Aus diesem Grund wird VRT oft nach Änderungen an der Website durchgeführt, z. B. wenn du das Theme wechselst oder ein Plugin aktualisierst.

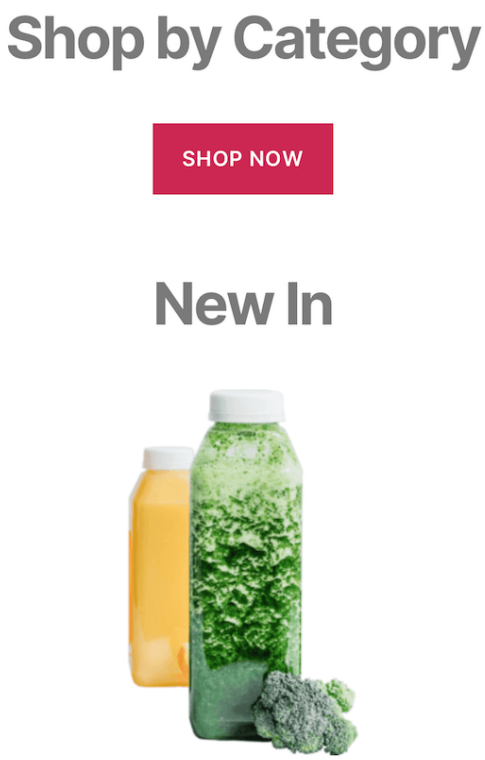
Auf diese Weise kannst du sicherstellen, dass die Änderungen deine visuellen Elemente nicht beeinträchtigen. So kann es zum Beispiel sein, dass dein Inhalt falsch ausgerichtet ist oder Schaltflächen verschwunden sind.

Wie bei den UI-Tests würdest du solche Probleme oft gar nicht bemerken, wenn du deine Website nicht am Frontend besuchst. Es gibt automatisierte VRT-Tools, die deine Website kontinuierlich auf visuelle Anomalien prüfen.

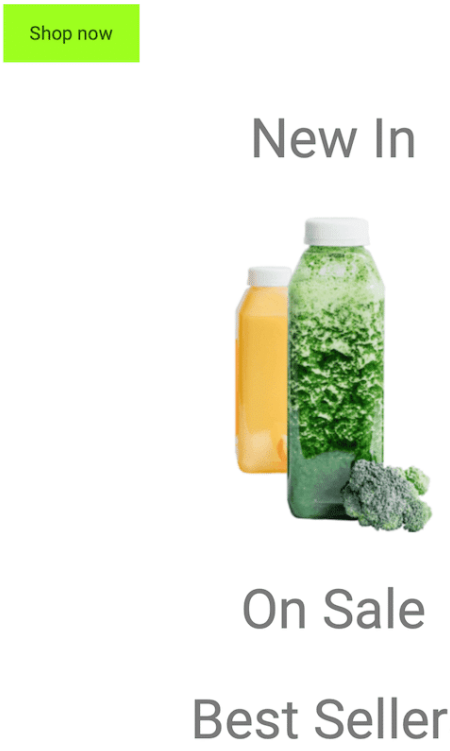
Oder du kannst deine Seiten einfach manuell vergleichen, bevor

und nachdem du deine Änderungen vorgenommen hast. Angenommen, du willst das Theme wechseln. Am sichersten ist es, dies in einer lokalen Umgebung wie DevKinsta zu tun, damit du visuelle Tests durchführen kannst, bevor du die Änderung auf deiner Live-Website anwendest.

Im Moment haben wir das Twenty Twenty-Theme auf unserer lokalen Website aktiviert. Wie du siehst, sind auf der Startseite alle Schaltflächen, Texte und Bilder mittig angeordnet:



Visuelle Tests in DevKinsta durchführen
Wenn wir jedoch zum Twenty Twenty-Three-Theme wechseln, kannst du sehen, dass die Schaltfläche **„Jetzt einkaufen“** falsch ausgerichtet ist:

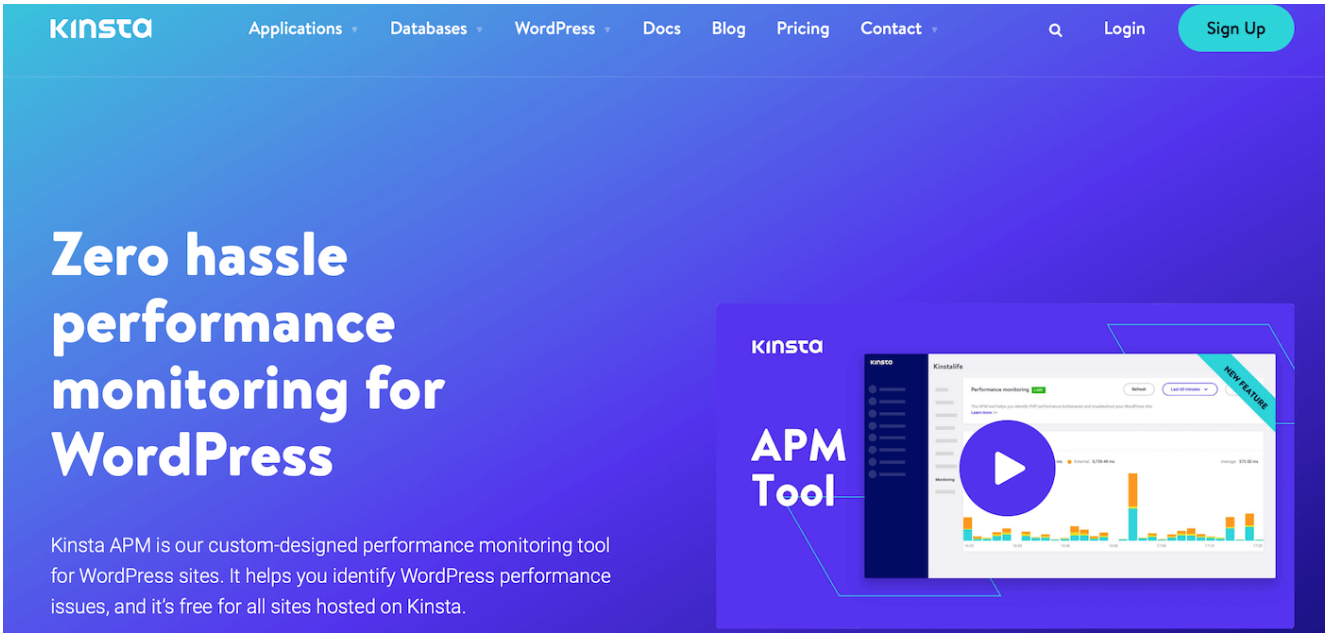


Erkenne visuelle Fehler mit visuellen WordPress-Tests
Wenn du eine lokale Umgebung für deinen Test einrichtest, kannst du visuelle Anomalien wie diese aufspüren.

Wie du die Geschwindigkeit deiner WordPress-Website testest (6 Überlegungen)

Eine weitere wichtige Methode, um deine WordPress-Website zu testen, ist die Überprüfung der aktuellen Geschwindigkeit deiner Website. In diesem Abschnitt gehen wir auf sechs Punkte ein, mit denen du die Leistung deiner Website testen kannst.

Vor diesem Hintergrund kann es hilfreich sein, mit Kinsta APM zu beginnen. Mit unserem Application Performance Monitoring Tool ist es ganz einfach, WordPress-Leistungsprobleme zu erkennen:



Kinsta APM-Tool

Du erhältst zum Beispiel Einblick in alle PHP-Prozesse, MySQL-Datenbankabfragen und externen HTTP-Aufrufe. Dadurch bist du in der Lage, lange API-Aufrufe, langsame Datenbankabfragen und nicht optimierten Plugin- und Theme-Code besser zu erkennen.

Das Beste daran ist, dass Kinsta APM in allen Kinsta-Tarifen kostenlos ist und du direkt von deinem MyKinsta-Dashboard aus auf das Tool zugreifen kannst. Insgesamt ist es eine einfach zu bedienende Lösung, die dir hilft, die Leistung und die Ladezeiten deiner Website zu verbessern.

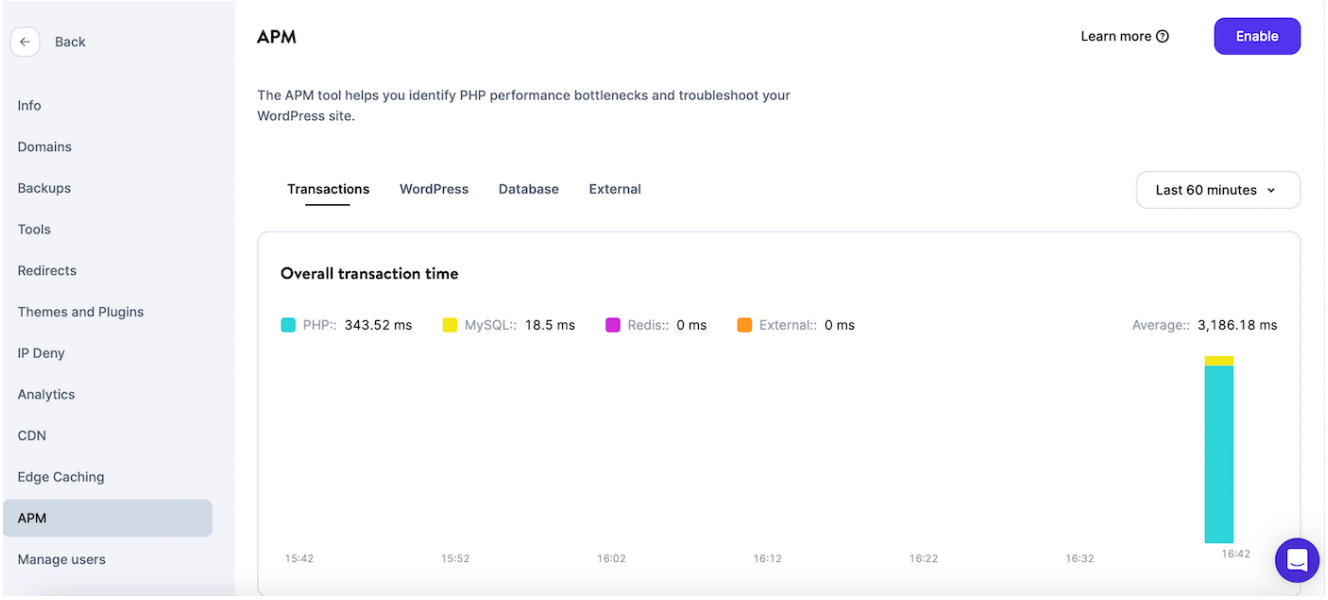
Langsame Abfragen oder Skripte

Um sicherzustellen, dass deine Website auf höchstem Niveau funktioniert, kannst du WordPress auf langsame Abfragen und Skripte testen. Langsame Abfragen und Skripte wirken sich auf die Gesamtgeschwindigkeit deiner Seite aus und machen deine Website weniger effizient.

Der einfachste Weg, langsame Abfragen und Skripte zu erkennen, ist die Aktivierung von Kinsta APM. Wenn du ein Kinsta-Kunde bist, kannst du das Tool kostenlos nutzen. Du musst es jedoch über dein MyKinsta-Dashboard aktivieren.

Logge dich dazu einfach in dein Konto ein und wähle die

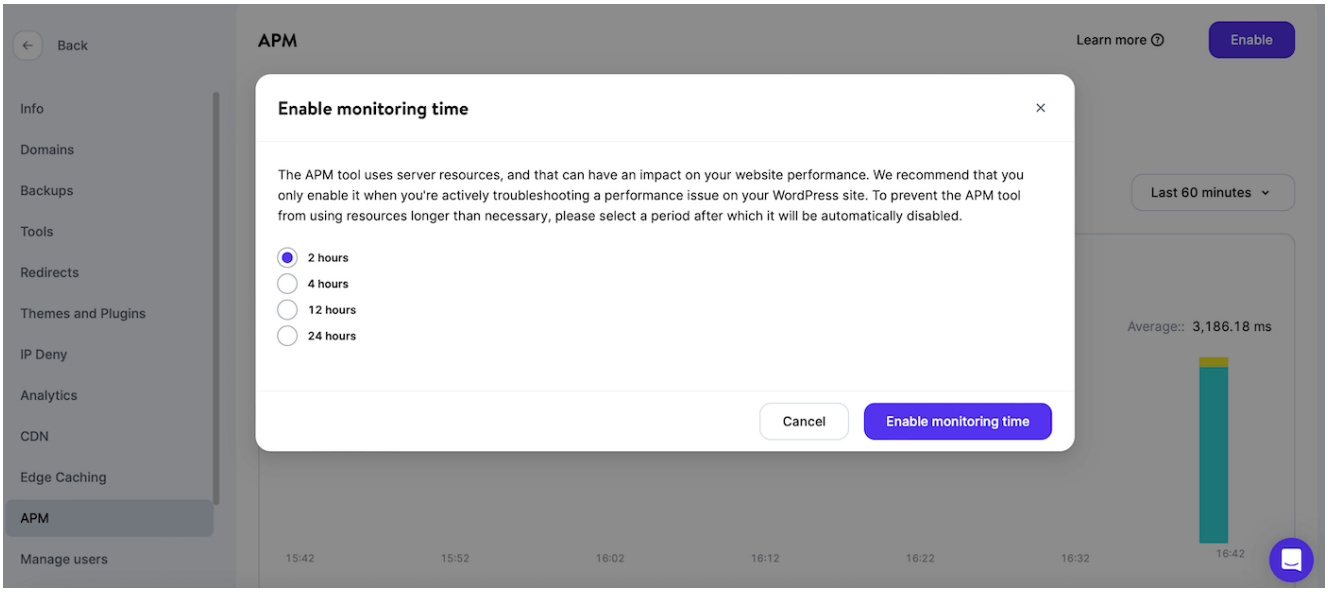
Website aus, auf der du das APM-Tool nutzen möchtest. Navigiere nun zum Reiter **APM** und klicke auf **Aktivieren**:



Aktiviere das Kinsta-APM-Tool über dein MyKinsta-Dashboard

Dann musst du die Dauer auswählen, für die du das Tool nutzen willst. Da das APM-Tool Serverressourcen verbraucht, kann es sich auf die Leistung deiner Website auswirken. Daher ist es am besten, das Tool nur für den Zeitraum zu aktivieren, in dem du aktiv an der Behebung eines Leistungsproblems arbeitest.

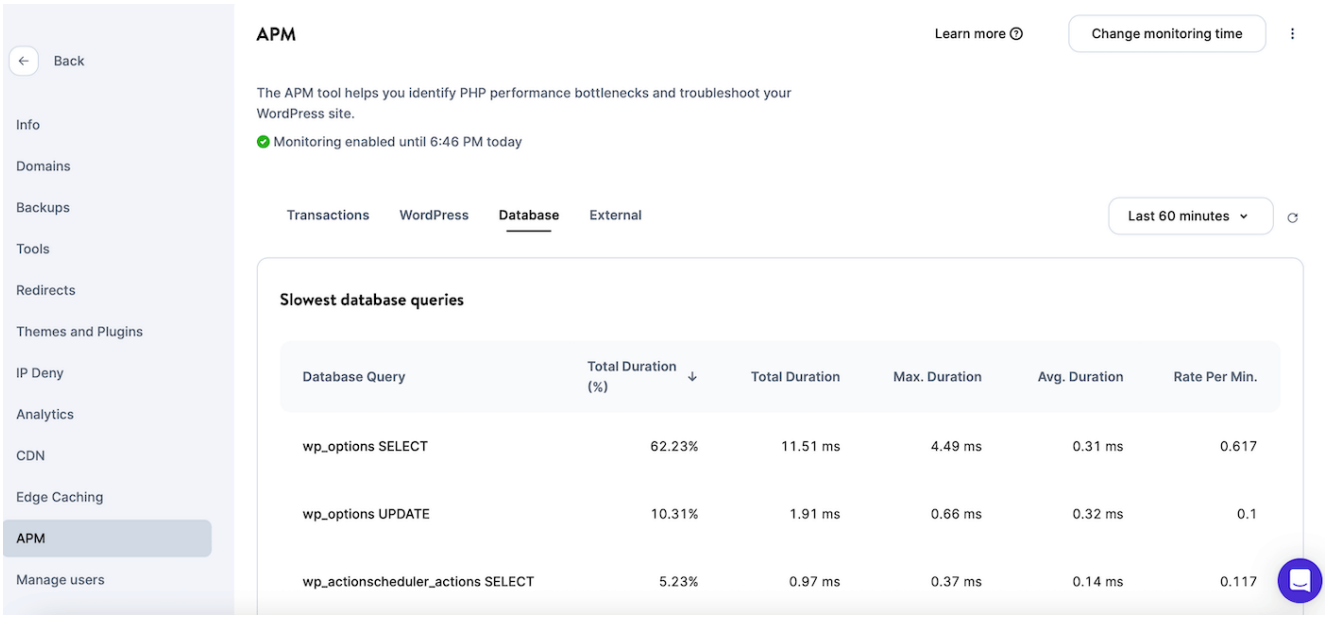
Triff deine Wahl und klicke auf **Überwachungszeit einschalten**:



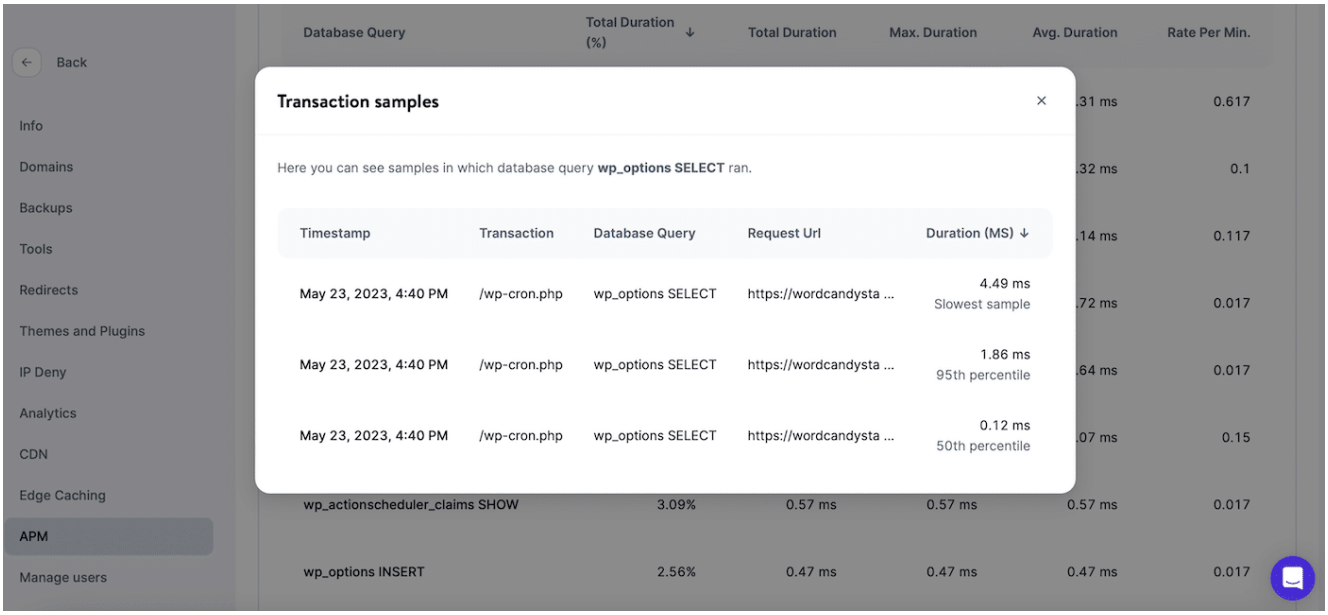
Aktiviere die Überwachungszeit für Kinsta APM

Es kann ein paar Minuten dauern, bis das Tool Daten über deine Website gesammelt hat. Wechsle danach auf die Registerkarte

Datenbank und suche den Abschnitt **Langsamste Datenbankabfragen** :



Langsamste Datenbankabfragen anzeigen
Hier findest du die zehn langsamsten Datenbankabfragen auf deiner Website. Wenn du auf eine Abfrage klickst, kannst du dir auch die Transaktionsmuster ansehen:

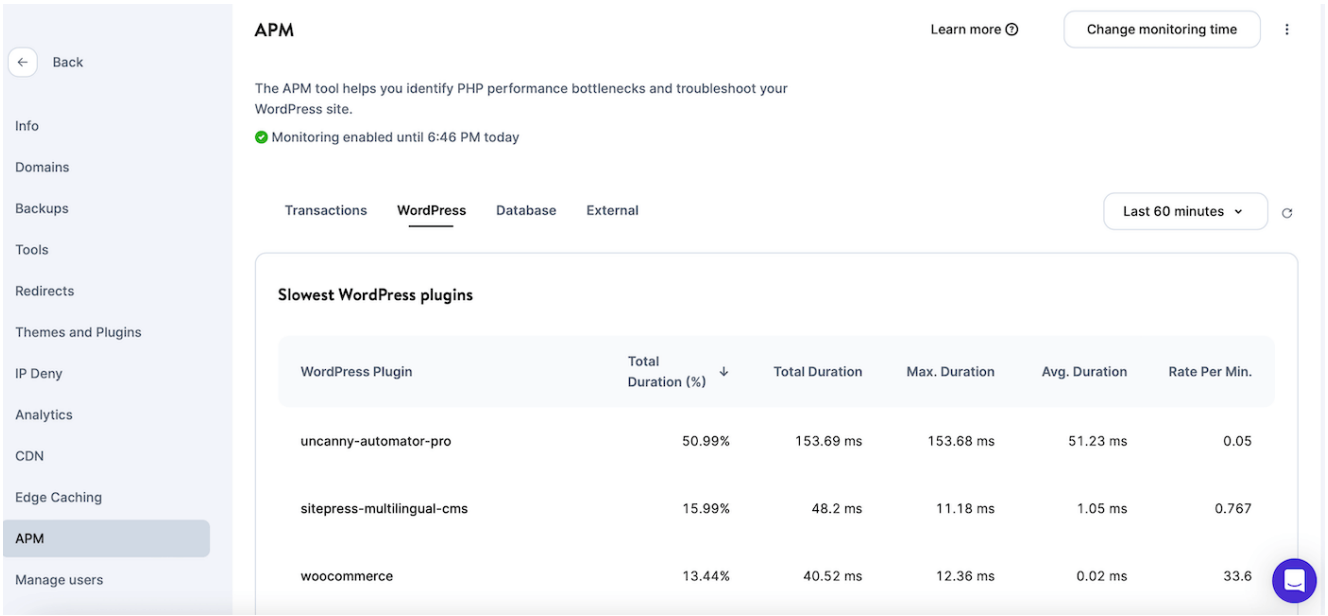


Transaktionsbeispiele anzeigen
Auf diese Weise kannst du mehr Informationen über die Probe, die Zeitleiste, die Spandetails und den Stacktrace herausfinden.

Langsame Plugins

Schlecht programmierte Plugins können nicht nur die Sicherheit deiner WordPress-Website beeinträchtigen, sondern auch die Leistung. Deshalb ist es wichtig, dieses Problem so schnell wie möglich zu erkennen.

Auch hier kannst du das Kinsta APM-Tool verwenden, um langsame Plugins zu identifizieren. Sobald du das Tool in deinem MyKinsta-Dashboard aktiviert hast, navigiere zum Reiter **APM** . Wechsle dann zu **WordPress**:



Testen auf langsame Plugins

Der erste Bereich, den du siehst, ist **Langsamste WordPress-Plugins**. Die langsamsten aufgezeichneten Plugins werden oben im Abschnitt aufgelistet.

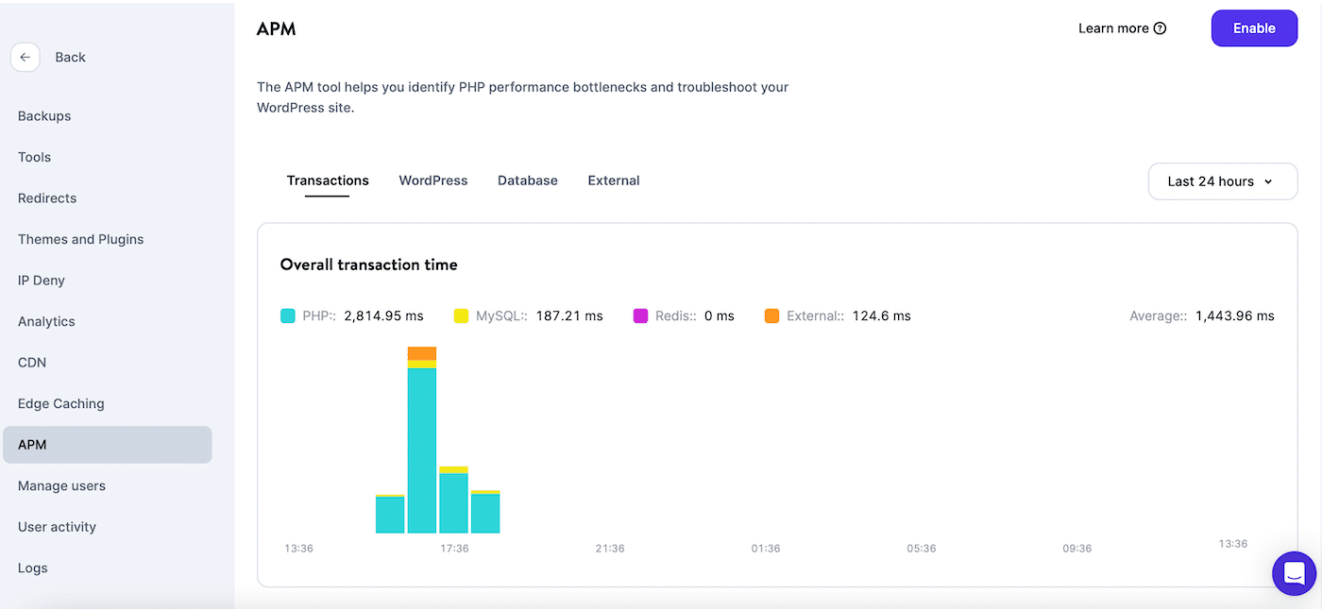
Um mehr Informationen über die Leistungsprobleme zu erhalten, klicke auf eines der aufgelisteten Plugins. Dadurch werden die Transaktionsbeispiele geladen, die das Plugin ausgeführt hat. Du kannst dir zum Beispiel den Zeitstempel, die Zeitleiste der Transaktionsverfolgung, die Details der Spanne, die Zeitleiste der Verfolgung und vieles mehr ansehen.

Langsame Seiten

Es ist auch wichtig, WordPress auf langsame Seiten zu testen, da dies zu einer schlechten UX führen kann. Außerdem ist die Seitengeschwindigkeit ein Rankingfaktor für Suchmaschinen wie Google.

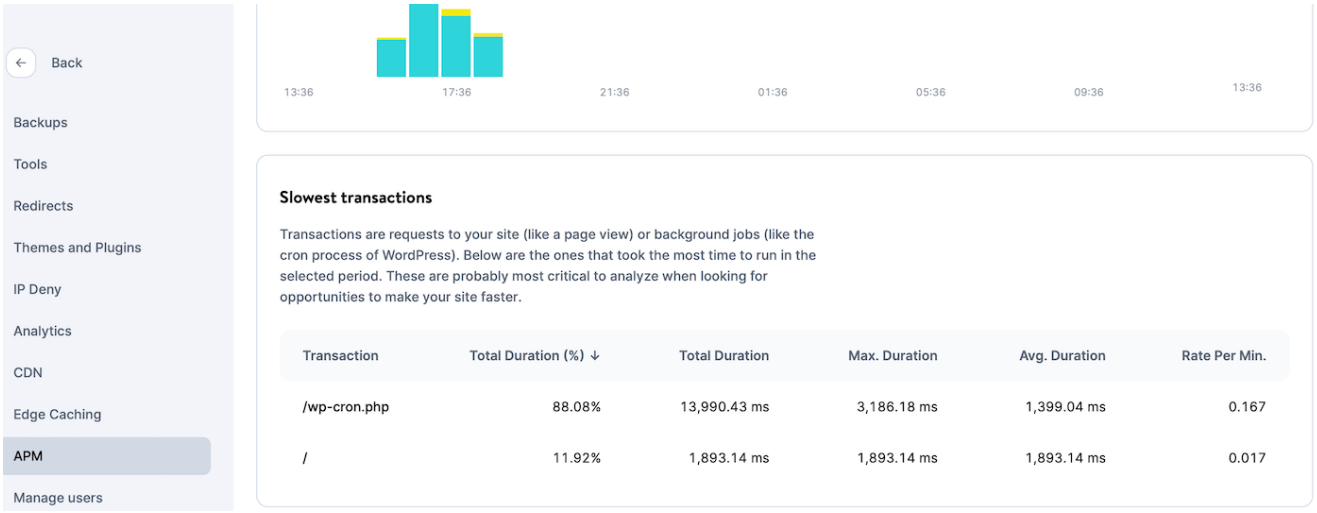
Du kannst ein kostenloses Website-Geschwindigkeitstest-Tool wie Pingdom oder PageSpeed Insights verwenden, um eine schnelle Bewertung der Seitengeschwindigkeit zu erhalten. Mit dem APM-Tool von Kinsta kannst du jedoch einen genaueren Einblick in die Geschwindigkeit deiner Seite gewinnen.

Sobald du Kinsta APM aktiviert hast, dauert es ein paar Sekunden, bis die Leistungskennzahlen deiner Website geladen sind. Gehe danach auf den Reiter **Transaktionen** :



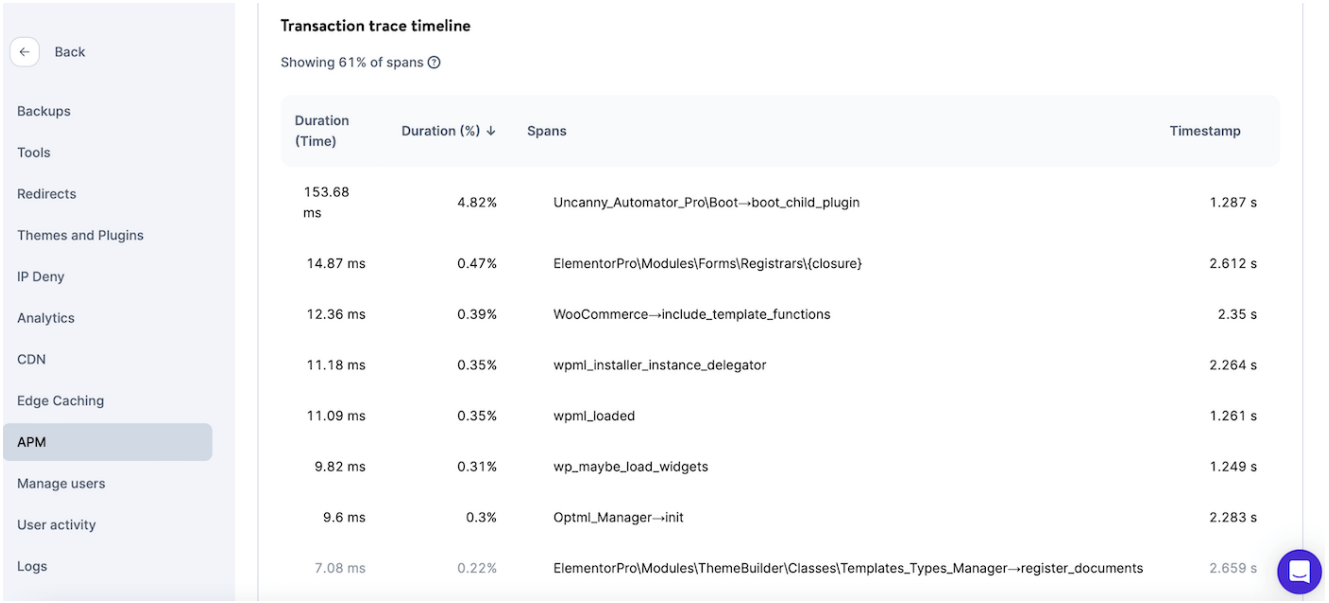
Teste langsame WordPress-Seiten mit Kinsta APM

Hier siehst du einige Daten über die gesamte Transaktionszeit deiner Website. Du kannst aber auch nach unten zu **Langsamste Transaktionen** scrollen, um die PHP-Prozesse zu sehen, die die meiste Transaktionszeit benötigen:



Langsamste Transaktionen anzeigen

Wenn du eine Transaktion auswählst, kannst du die URL herausfinden, die sie erzeugt. Klicke dann auf die URL, um die **Zeitleiste der Transaktionsverfolgung** anzuzeigen:



Zeitleiste für die langsamsten Transaktionen

Auf diese Weise kannst du die Zeitspanne finden, die am meisten Zeit in Anspruch nimmt. Wenn diese Zeitspannen als kritisch für deine Leistung eingestuft werden, werden sie in der Regel orange oder rot hervorgehoben.

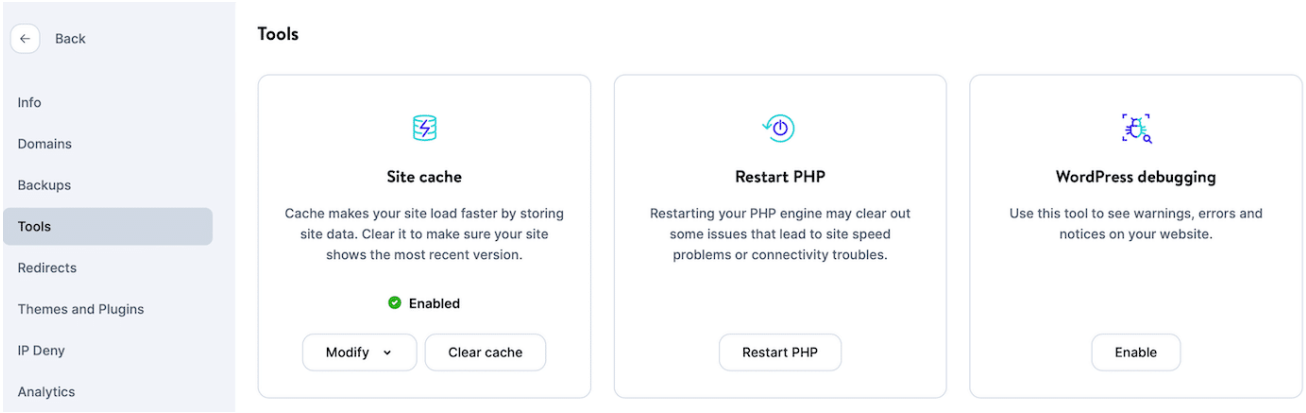
Caching

Caching ist eine einfache Methode, um deine Ladezeiten zu verbessern. Dabei werden Kopien deiner Website auf dem Server gespeichert. Wenn ein Nutzer deine Seite aufruft, kann dein

Server die im Cache gespeicherte Version anzeigen, so dass die Daten viel schneller übertragen werden können.

Bei Kinsta erhältst du Zugang zum Server-Level-Caching, das automatisch auf allen Live-Websites aktiviert ist. Wenn du jedoch eine Staging-Umgebung verwendest, musst du den Cache manuell aktivieren.

Klicke in deinem MyKinsta-Dashboard auf **WordPress-Sites** und wähle deine Website aus. Dann navigierst du zu **Tools** und klickst unter **Site Cache** auf **Enable**:



Aktiviere den Cache auf Serverebene in MyKinsta

Der einfachste Weg, dein Caching zu testen, ist, deine Website mit einem Web-Speed-Test-Tool wie Pingdom zu testen. Es ist jedoch wichtig, dass du den Test mehr als einmal durchführst. Denn wenn du ihn nur einmal durchführst, kann es sein, dass der Inhalt noch nicht auf dem Server des Hosts oder im CDN zwischengespeichert ist.

Gib deine URL in das **URL-Feld** bei Pingdom ein und wähle einen Ort aus. Suche nun unter **Response Headers** nach **x-kinsta-cache**. Wenn hier **MISS** steht, wird deine Website nicht aus dem Cache geladen.

Um das zu beheben, musst du deine Website noch ein paar Mal durch den Pingdom-Test laufen lassen. Dies sollte dazu führen, dass die **x-kinsta-cache** und **x-cache** Header einen **HIT** registrieren. Jetzt überprüfst du die Ergebnisse und schaust auf den großen gelben Balken, der die Wartezeit oder Time to

First Byte (TTFB) anzeigt.

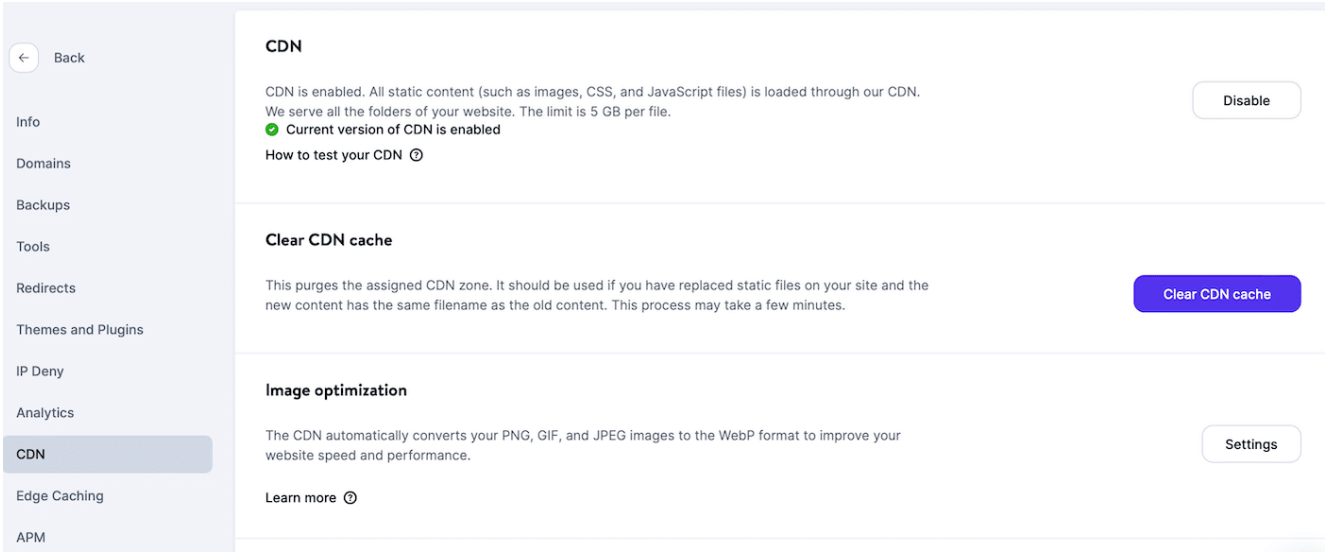
Diese Zahl ist in der Regel hoch, wenn eine Seite nicht aus dem Cache gekommen ist. Auch hier empfiehlt es sich, den Test einmal mit deaktiviertem und dann noch einmal mit aktiviertem Cache durchzuführen, um den Unterschied deutlich zu sehen.

Content Delivery Network (CDN)

Ein Content Delivery Network (CDN) ermöglicht es dir, deine Ladezeiten zu verbessern, indem es deine Webseiten über einen Server ausliefert, der physisch näher bei deinen Besuchern steht. Mit allen Kinsta-Tarifen erhältst du Zugang zu einem von Cloudflare betriebenen CDN.

Bei neuen Websites ist das CDN standardmäßig aktiviert. Du kannst aber überprüfen, ob dein CDN aktiviert ist, indem du dich in dein MyKinsta-Dashboard einloggst.

Gehe zu **WordPress Sites** und wähle den Namen deiner Website aus. Klicke auf den Reiter **CDN** und dann auf **Aktivieren**. Wenn du **Deaktivieren** siehst, weißt du, dass das CDN aktiv ist:

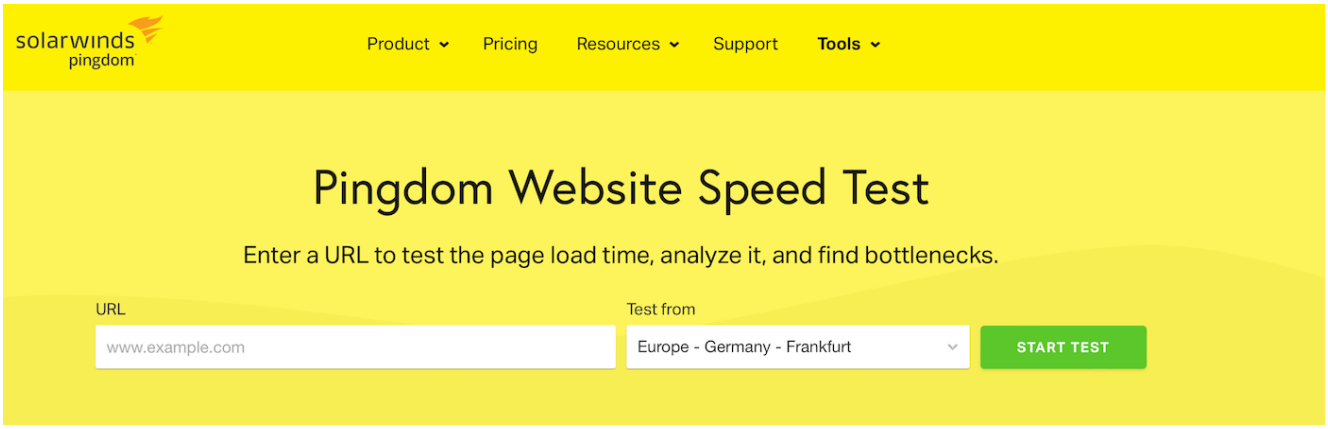


Aktiviere das Kinsta CDN

Um dein CDN zu testen, ist es am einfachsten, ein Tool zum Testen der Website-Geschwindigkeit zu verwenden. Aber zuerst ist es eine gute Idee, die HTTP-Header eines statischen Assets zu überprüfen, um sicherzustellen, dass es vom Kinsta CDN

geladen wird.

Du kannst dies mit dem Inspect Tool deines Browsers oder mit unserem kostenlosen HTTP-Status- und Redirect-Checker überprüfen. Jetzt musst du ein Tool zum Testen der Website-Geschwindigkeit auswählen, z. B. Pingdom:



Pingdom

Du kannst den ersten Test durchführen, nachdem du das CDN abgeschaltet hast. Dann kannst du deine Website mit aktiviertem CDN erneut testen, um den Unterschied zu sehen. Außerdem solltest du dein CDN von verschiedenen Standorten aus testen.

Wenn dein Test abgeschlossen ist, solltest du dir die Anfragen ansehen, die vom Kinsta CDN *(xxxxkinstacdn.com)* geladen werden. Ausführliche Informationen zu diesem Thema findest du in unserem Beitrag über die Durchführung eines CDN-Tests.

Lasttests

Entgegen der landläufigen Meinung gibt es einen wichtigen Unterschied zwischen Geschwindigkeitstests und Lasttests. Bei Geschwindigkeitstests wird im Wesentlichen die Ladezeit einer Seite gemessen, einschließlich der MySQL- und PHP-Antwortzeiten.

Andererseits bieten Lasttests eine feinere Granularität als Geschwindigkeitstests. Er kann zum Beispiel dazu verwendet werden, die Ladezeiten in bestimmten Situationen zu messen, z.

B. wenn deine Website von einem hohen Verkehrsaufkommen betroffen ist.

Das Einrichten eines Lasttests ist ziemlich komplex. Deshalb kann es eine gute Idee sein, einen Entwickler um Hilfe zu bitten. Wenn du einen Lasttest für deine Kinsta-Website durchführen möchtest, wende dich an einen Mitarbeiter unseres Support-Teams.

Wie du die Sicherheit deiner WordPress-Website testest

Wenn du WordPress testest, musst du sicherstellen, dass die gesamte Software auf deiner Website sicher ist. Das betrifft nicht nur die WordPress-Kernsoftware, die die Plattform nutzt, sondern auch die Sicherheit von Themes und Plugins.

Das Testen von Themes und Plugins kann sogar noch wichtiger sein, da sie nicht immer aus einer seriösen Quelle stammen. Wenn du Themes und Plugins von Drittanbieter-Websites installierst, gibt es keine Möglichkeit zu überprüfen, ob die Software alle erforderlichen Sicherheitsprüfungen durchlaufen hat.

Das heißt, das Plugin oder Theme könnte schlecht programmiert sein oder sogar bösartige Skripte oder Fehler enthalten, die deine Website beschädigen können. Außerdem ist es wichtig, dass du die Software auf deiner Website immer auf dem neuesten Stand hältst, denn veraltete Software kann als Hintertür für böswillige Akteure genutzt werden, um sich Zugang zu verschaffen.

Kernsicherheit

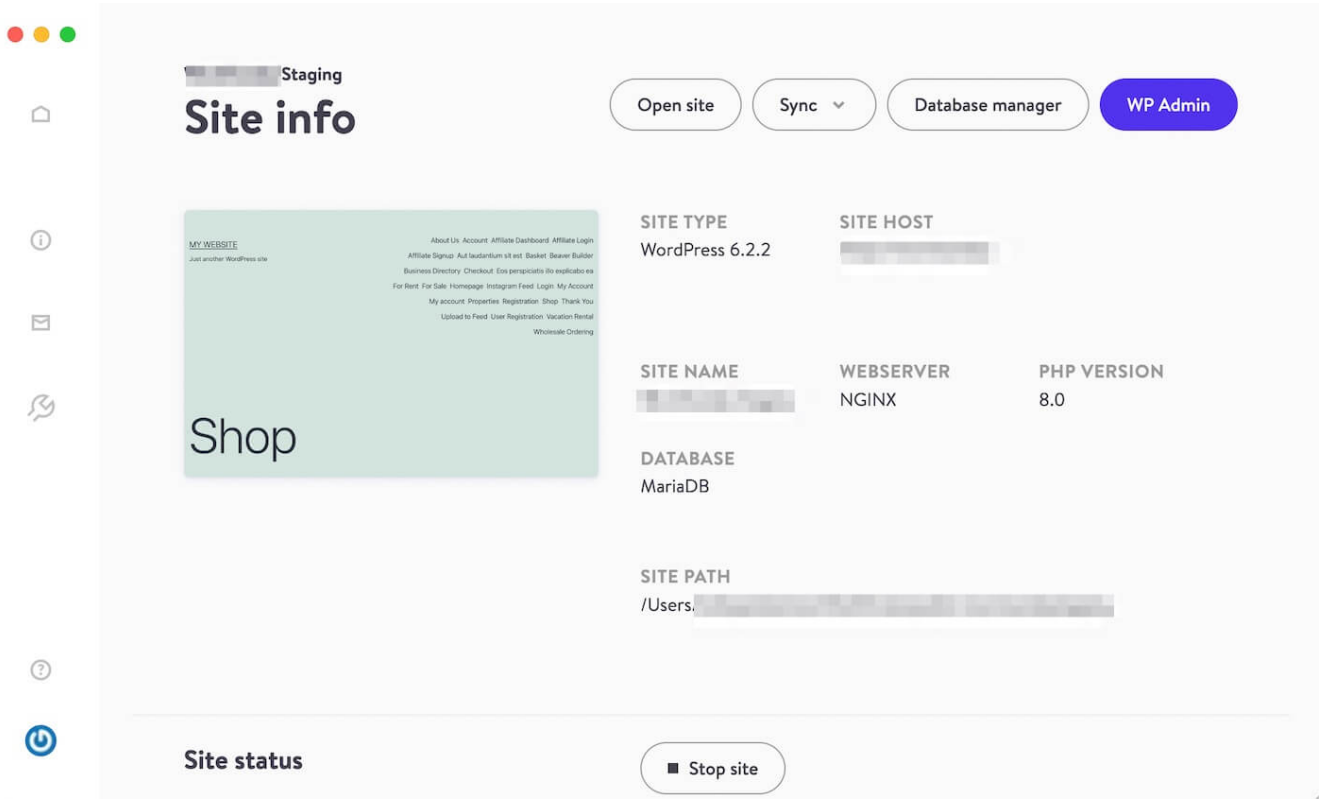
Obwohl WordPress eine sichere Plattform ist, ist sie nicht immun gegen Cyberangriffe. Deshalb ist es wichtig, dass du die Sicherheit deiner Kernsoftware regelmäßig überprüfst.

Eine der besten Möglichkeiten, deine Kernsoftware zu schützen, ist die Entscheidung für einen guten Webhoster. Bei Kinsta bekommst du zum Beispiel Zugang zu DDoS-Schutz, Firewalls und Malware-Scans. Außerdem haben wir ein spezielles Malware-Entfernungsteam vor Ort. Selbst wenn deine Website infiziert wird, können wir sie wieder in ihren ursprünglichen Zustand versetzen.

Wenn ein neues WordPress-Update veröffentlicht wird, kannst du es auf jeden Fall zuerst auf seine Sicherheit testen, indem du es auf einer Staging-Seite oder in einer lokalen Umgebung ausführst.

Bei Kinsta ist das ganz einfach. Du musst nur zu **WordPress Sites** navigieren und deine Website aus der Liste auswählen. Stelle dann sicher, dass deine Website auf **Staging** eingestellt ist, wenn du das Update ausführst.

Wenn du sicher bist, dass die neue WordPress-Version sicher ist, kehrst du zu diesem Bildschirm zurück und klickst auf **Push environment** > **Push to LIVE** , um die Änderung zu übernehmen:



Änderungen von der Staging-Website live schalten
Triff deine Wahl (zwischen Dateien oder Datenbank) und bestätige deine Entscheidung mit einem Klick auf **Push to live**.

Theme-Sicherheit

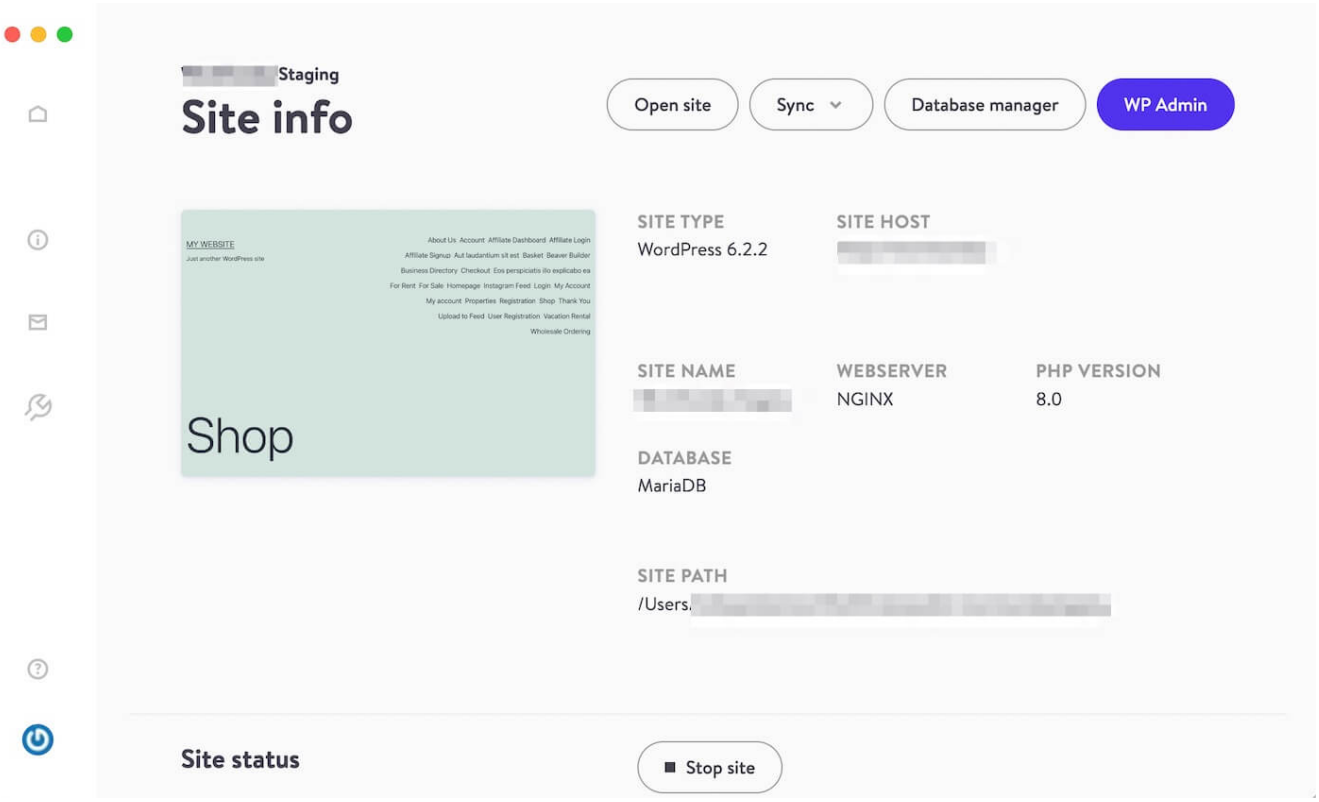
Wenn du ein neues Theme findest, das du installieren möchtest, aktivierst du es am besten in einer lokalen Entwicklungsumgebung oder auf deiner Staging-Site. Das Gleiche gilt, wenn ein bestehendes Theme auf deiner Seite ein Update veröffentlicht.

Die meisten Theme-Updates enthalten Patches für Sicherheitsprobleme. Es kann aber auch passieren, dass du ein schlechtes Update bekommst, das mit einer anderen Software auf deiner Website kollidiert.

Wenn es sich um ein Theme handelt, das du noch nie benutzt hast (und du die Entwickler nicht kennst), ist es viel sicherer, das Theme in einer lokalen Umgebung zu installieren. Das bedeutet, dass selbst wenn das Theme deine Website beschädigt, deine Live-Website davon nicht betroffen ist.

Wenn du Kinsta-Kunde bist, kannst du also eine Testseite einrichten. Wenn deine Website nicht bei Kinsta gehostet wird, kannst du auch kostenlos mit DevKinsta eine lokale Entwicklungsumgebung einrichten.

Wenn du DevKinsta auf deinem Computer geöffnet hast, rufe die Seite **Site Info** auf. Hier klickst du auf **WP Admin**:



Lokale Website von DevKinsta aus starten

Dann installierst und aktivierst du das Theme, wie du es normalerweise in WordPress tun würdest. Normalerweise ist es eine gute Idee, mindestens eine Woche zu warten, bevor du das Theme auf deiner Live-Website installierst (das gilt auch für ein neues Theme-Update).

Wenn du jedoch die Sicherheit eines bestehenden Themes auf deiner Website überprüfen möchtest, ist es am einfachsten, einen Sicherheitsscanner zu verwenden. WPScan ist eine großartige Option, die alle Sicherheitslücken in deinen WordPress-Themes aufspürt.

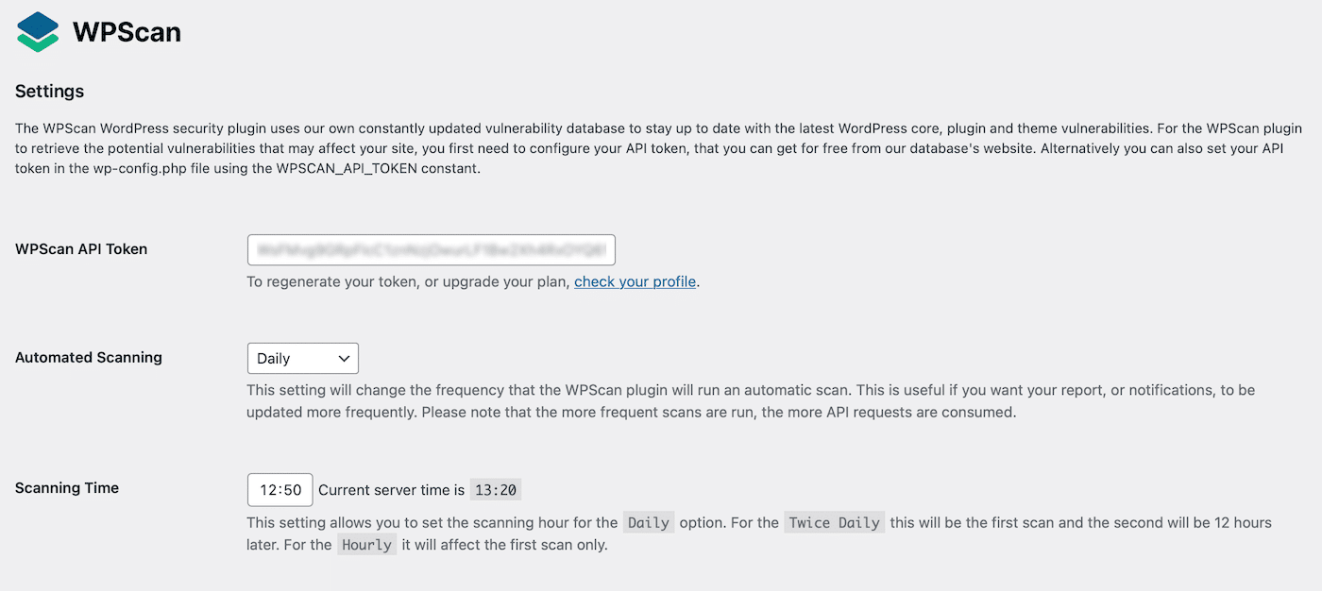
Plugin-Sicherheit

Auch Plugins können eine Gefahr für die Sicherheit deiner Website darstellen. Deshalb ist es eine gute Praxis, die Sicherheit deiner Plugins regelmäßig zu überprüfen.

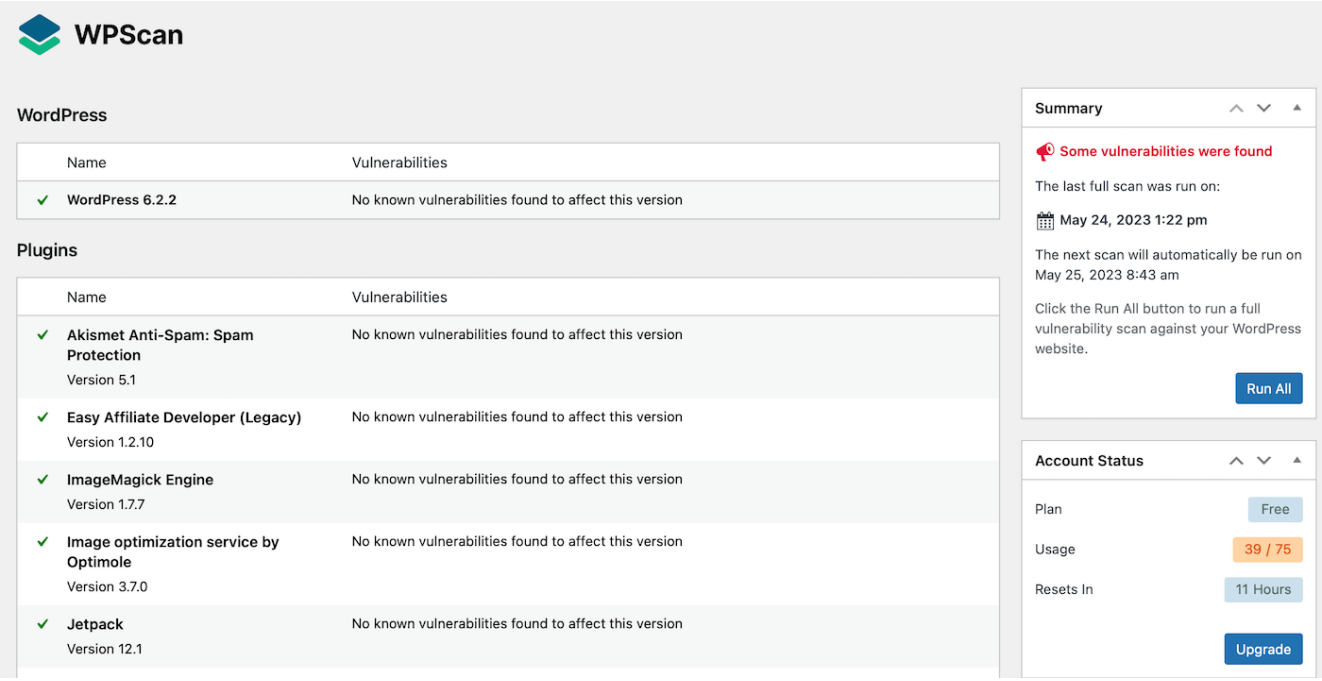
Wie bereits erwähnt, kannst du ein neues Plugin (oder ein Plugin-Update) in einer lokalen Umgebung oder auf einer Staging-Seite installieren. Auf diese Weise bleibt deine Live-Site intakt, falls etwas schief geht.

Wie bei Themes kann es aber auch nützlich sein, einen Schwachstellen-Scanner wie WPScan zu installieren. Die Nutzung dieses Tools ist völlig kostenlos. Alles, was du tun musst, ist, dich für ein Konto zu registrieren. Dann kannst du das API-Token zu deiner WordPress-Seite hinzufügen.

Sobald der Scanner mit deiner Website verknüpft ist, navigierst du zu **WPScan** > **Einstellungen** , wo du automatische tägliche oder stündliche Scans einrichten kannst:



Teste die Plugin-Sicherheit mit WPScan
Oder klicke auf die Registerkarte **Bericht** , um einen manuellen Test durchzuführen. Sobald der Test abgeschlossen ist, scrolle nach unten zum Abschnitt **Plugins** :



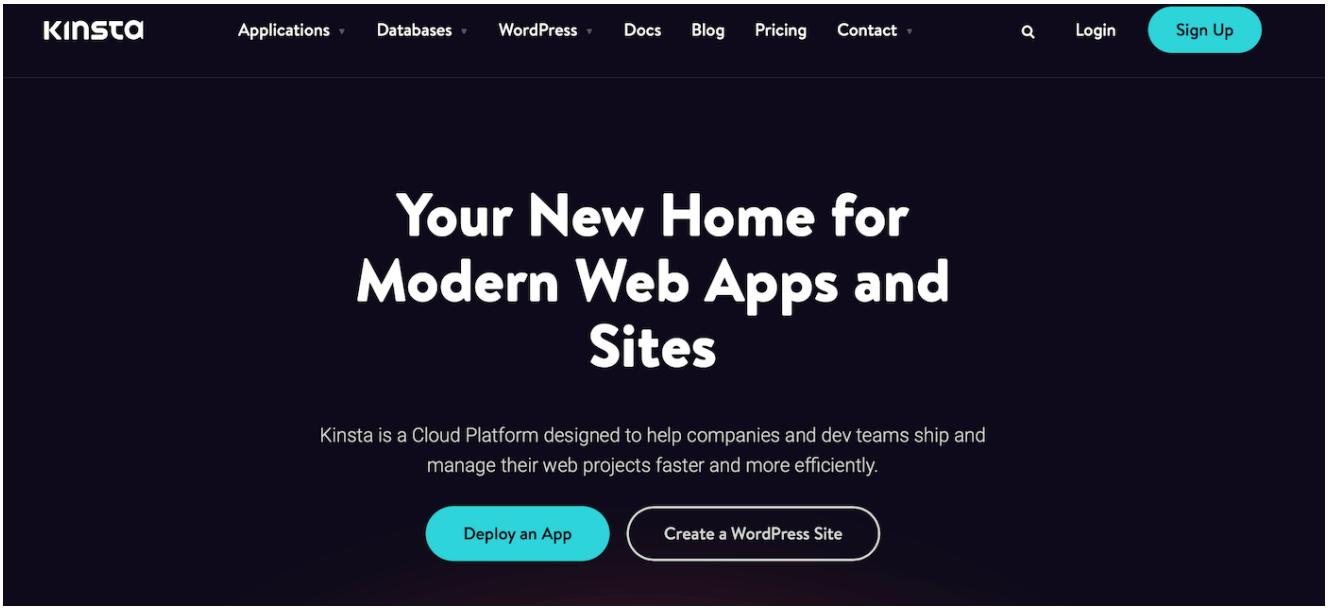
WPScan-Berichte

Hier kannst du eine vollständige Liste aller Plugins auf deiner Website sehen. Wenn deine Plugins sicher sind, siehst du ein Häkchen neben jedem Plugin-Namen. Andernfalls findest du einige Informationen in der Spalte **„Schwachstellen„**.

Geschwindigkeit und Sicherheit sind am besten, wenn du das richtige Hosting wählst

Natürlich kannst du deine Webseiten optimieren und alle notwendigen Sicherheitsmaßnahmen ergreifen, um eine erfolgreiche Website zu betreiben. Der beste Weg, um sicherzustellen, dass deine Website sicher und schnell ist, ist jedoch, einen guten Webhoster zu wählen.

Bei Kinsta legen wir großen Wert auf Geschwindigkeit und Sicherheit:



Kinsta
Alle unsere Angebote werden auf den besten CPUs mit globaler Verfügbarkeit gehostet. Außerdem erhältst du Zugang zu Kinstas Cloudflare-gestütztem CDN mit Servern an über 260+ Standorten.

Für alle, die sich um die Sicherheit im Internet sorgen, bietet Kinsta eine Vielzahl von Funktionen, um deine Website zu sichern. Du kannst tägliche Backups, Malware-Scans, DDoS-Schutz und Firewalls erwarten. Außerdem bieten wir einen sicheren SSH-Zugang und du kannst mit nur einem Klick ein kostenloses SSL-Zertifikat installieren.

Zusammenfassung

Ohne deine WordPress-Website zu testen, kannst du nicht richtig verstehen, wie die Nutzer deine Website erleben. Wer zum Beispiel bestimmte Browser benutzt, hat vielleicht Probleme mit deinem Menü. Mobile Besucher können mit langen Wartezeiten konfrontiert sein. Deshalb ist es wichtig, deine WordPress-Website zu testen.

Am besten testest du deine Website, indem du eine Staging-Site einrichtest oder mit DevKinsta eine lokale Umgebung erstellst. So erhältst du Einblicke in die Funktionalität, Leistung und Sicherheit deiner Website (ohne dein Live-Web-Erlebnis zu stören).

Ein bisschen zusätzliche Sicherheit kann aber nie schaden. Eine der einfachsten Möglichkeiten, um sicherzustellen, dass deine Website jederzeit reibungslos läuft, ist die Entscheidung für einen hochwertigen Webhoster wie Kinsta. Schau dir unsere Tarife an, um loszulegen!

SCA-Tools (Lieferkettensicherheits-Tools) in der Übersicht

Die Software Composition Analysis soll Risiken aufdecken, die Entwickler beim Einsatz von Open-Source-Komponenten eingehen, und die Softwarelieferkette absichern. Der Markt für passende Produkte ist riesig und in ständiger Bewegung.

-tract

- Software Composition Analysis (SCA) ist eine Form der

Codeanalyse, die ermittelt, welche Open-Source-Bibliotheken eine Software verwendet, welche bekannten Schwachstellen in ihnen enthalten sind und unter welcher Lizenz sie stehen.
- SCA-Werkzeuge unterstützen dabei und automatisieren diesen Prozess, indem sie sich in Code-Repositorys, CI/CD-Pipelines und oft auch IDEs integrieren.
- Der Markt ist geprägt von sehr vielen Anbietern und oft recht jungen Produkten. Eine Auswahl von Angeboten von etablierter Herstellern, die auf dem deutschen Markt aktiv sind, stellt diese Übersicht vor.

Sicherheit rückt nach links. Nicht politisch, sondern im Sinne des Left Shift der DevOps-Bewegung. Es bedeutet, dass immer mehr Kompetenzen am Anfang, also links im gesamten Prozess angesiedelt sind: bei den Entwicklern. Mit DevSecOps wird aus der Verantwortung für den Betrieb (DevOps) nun Verantwortung für den sicheren Betrieb. Das macht aber Entwickler nicht auf magische Weise zu Securityspezialisten. Deshalb ist jede Unterstützung in Form von Werkzeugen oder Frameworks gefragt, die helfen, möglichst viele Risiken so früh es geht zu entdecken und Sicherheitslücken zu stopfen.

Da nahezu jedes größere Softwareprojekt Open-Source-Komponenten enthält, betrifft dies nicht nur die vom eigenen Entwicklerteam zu verantwortenden Schwachstellen, sondern auch die in den eingebundenen Abhängigkeiten. Die Aufgabe der Software Composition Analysis besteht darin, herauszufinden, welche Komponenten in welchen Versionen in der eigenen Software stecken, und dann zu ermitteln, welche schon bekannten Schwachstellen diese haben. Über diese absolute Mindestanforderung an eine SCA-Software gehen aber alle am Markt vorhandenen Systeme hinaus und bieten Einbindung in CI/CD-Pipelines oder Entwicklertools, automatische Lösungsvorschläge für gefundene Schwachstellen (Remediation), diverse Dashboards, Frameworks zum Festlegen von Richtlinien und so weiter.

Entdecken, dokumentieren, beheben

In aller Regel erfüllt SCA zudem eine Doppelfunktion. Zusätzlich zu Sicherheitsrisiken soll sie auch Compliance-Risiken identifizieren, indem sie die Open-Source-Lizenzen findet, unter denen verwendete Komponenten veröffentlicht sind. Das macht auch Rechtsabteilungen und Management zu SCA-Anwendern, die Software darf also unter Umständen nicht ausschließlich auf die Bedürfnisse von Developern zugeschnitten sein. So gut wie immer kann ein SCA-Werkzeug SBOMs (Software Bills of Materials) erzeugen, also „Zutatenlisten“, die beispielsweise US-Behörden per Präsidentenerlass verlangen müssen [1].

Um die Komponenten zu ermitteln, lesen SCA-Tools die Abhängigkeiten aus den Manifestdateien verschiedener Paketmanager aus, etwa NPM, Maven oder NuGet; manche scannen darüber hinausgehend auch den Sourcecode selbst oder sogar Binärdateien. Für den Abgleich mit bekannten Sicherheitslücken nutzen kommerzielle Anbieter in der Regel eigene Datenbanken, Open-Source-Programme greifen oft auf frei verfügbare Quellen zurück, wie die National Vulnerability Database (NVD), die das US-amerikanische National Institute of Standards and Technology (NIST) pflegt, oder die ebenfalls recht umfassenden GitHub Security Advisories.

Der Markt für SCA-Software ist ausgesprochen vielfältig, neben ausgereiften und von großen Organisationen unterstützten Open-Source-Programmen tummeln sich Spezialhersteller und die etablierten Anbieter großer Sicherheitslösungen, die in den letzten zwei Jahren SCA entweder in ihre Suiten integriert oder separate Produkte lanciert haben. Zur großen Fülle an Herstellern und Produkten mag beitragen, dass es technisch eher eine Fleißarbeit ist, die Grundfunktionen zur Verfügung zu stellen: möglichst viele unterschiedliche Manifestformate der Paketmanager parsen und mit Datenquellen zu Sicherheitslücken abgleichen, Export in gängige SBOM-Formate,

dazu noch etwas Integration in bereits vorhandene Frameworks zu Datenaufbereitung, Nutzermanagement, Entwicklertools und DevOps-Pipelines – fertig ist die SCA-Lösung.

Deshalb grenzen sich die führenden Anbieter auf diesem Gebiet auch alle durch spezielle Alleinstellungsmerkmale von ihren Mitbewerbern ab. Häufig haben sie weitere Analyseverfahren im Angebot und gestatten das zusätzliche Scannen von Source- oder Binärcode. Oft pflegen sie erweiterte Schwachstellendatenbanken, können interne Projekte in die Analyse einbeziehen, oder sie positionieren sich gezielt als umfassende Enterprise-Lösung, die alle Anwendungsfälle abdeckt und sich an ein heterogenes Anwenderfeld richtet.

Viel Bewegung im Markt

Die OWASP listet auf ihrer Website zum SBOM-Format CycloneDX 170 Plattformen und Werkzeuge auf, die ganz oder teilweise SCA-Funktionen haben (siehe ix.de/zvbm). Beim Eingrenzen der Auswahl ist auf die jährlichen Analysen von Gartner, Forrester und Co. nur bedingt Verlass. Manche Hersteller, die laut dem einen Analysten seit Jahren eine stabile, besonders starke Marktposition haben, werden bei dem anderen nicht einmal erwähnt, andere rutschen von einem Jahr zum anderen zwischen Gartners magischen Quadranten hin und her.

Auch ist es fraglich, ob die Orientierung an den dort gelisteten Produkten immer sinnvoll ist, denn deren Schwerpunkt liegt auf großen Lösungen für den unternehmensweiten Einsatz. Nicht nur deren Implementierung kann aufwendig sein. Auch die Prozesse, an die sich alle Anwender gewöhnen müssen, sind nur mit großem Aufwand durchzusetzen. Mit etwas Pech ist das Produkt gekauft und eingerichtet, aber kaum einer nutzt seine elaborierten Features.

Für einzelne Projekte und kleinere Teams kann eine weniger umfangreiche, aber auch weniger komplexe Software die bessere

Entscheidung sein – vorausgesetzt, sie lässt sich gut mit den vorhandenen Tools und Abläufen verheiraten. Open-Source-Werkzeuge, aber auch manche auf Cloud-native gebürsteten Spezialhersteller mit ihren SaaS-Angeboten kommen da am ehesten infrage.

Die hier vorgestellten Werkzeuge zählen zu den eher etablierten Produkten dieses Segmentes und stammen hauptsächlich von SCA-Spezialisten oder zumindest von Herstellern, deren sonstige Expertise in der Codeanalyse liegt und die auch im deutschsprachigen Raum aktiv sind. Hinzu kommt eine kleine Auswahl Open-Source- oder anderer kostenloser Tools. Die Angaben in dieser Übersicht beruhen auf öffentlich zugänglichen Informationen und auf Nachfragen bei den Herstellern; soweit verfügbar wurden die aktuellen technischen Dokumentationen der Produkte herangezogen. Es sind sowohl Produkte dabei, die sich on Premises installieren lassen, als auch solche, die komplett als Service in der Cloud angeboten werden. Manche Anbieter lassen ihren Kunden die Wahl zwischen verschiedenen Bereitstellungsmethoden, andere haben hybride Modelle im Angebot.

Übersicht ausgewählter SCA-Anbieter									
Anbieter	Aqua		Anchore/Community	Synopsys	Checkmarx	FOSSA	Mend	OWASP/Community Dependency-Track	Snyk
Produkt	Aqua Supply Chain Security	Aqua Trivy	Syft/Grype	Black Duck	Checkmarx SCA	FOSSA	Mend SCA	OWASP Dependency-Track	Snyk Open Source
Bereitstellungsmodell	Public Cloud, Private Cloud, on Premises, AWS, GCP	lokal	lokal	on Premises	SaaS, Private Cloud, on Premises	SaaS, on Premises	SaaS, lokaler Scan möglich	on Premises	SaaS, lokaler Scan möglich
Export von SBOM-Formaten	SPDX, CycloneDX	SPDX, CycloneDX	SPDX, CycloneDX, eigenes Format	SPDX, CycloneDX, Protex	CycloneDX (über API auch SPDX)	SPDX, CycloneDX, weitere Formate	CycloneDX und SPDX mit separatem Tool	CycloneDX	SPDX und CycloneDX mit API und CLI (Beta)
Abgleich mit Schwachstellendatenbanken	eigene Datenbank	eigene Datenbank	durch Integration mit Grype	NIST NVD oder Black Duck Security Advisories (mit separater Lizenz)	eigene Schwachstellendatenbank, zusätzlich Datenbank bösartiger Pakete	eigene Datenbank	eigene Datenbank	NIST NVD und weitere	eigene Datenbank
Integration in DevOps-Tools	u. a. GitHub Actions, GitLab, CI CD, Jenkins, CircleCI, Terraform Cloud	GitHub Actions und Azure DevOps (offiziell), CircleCI und weitere (Community)	teilweise Community-Plug-ins	ca. 15 CI-Plattformen	Jenkins, Azure DevOps, TeamCity, Bamboo	ca. 15 CI-Plattformen	u. a. Azure DevOps, Jenkins, CircleCI, Travis	Jenkins, Maven, Gradle, GitHub Actions	CircelCI, GitHub Actions, Jenkins, Maven, TeamCity, Terraform
Code-Repositorys	GitHub, GitLab, Bitbucket, Azure	Git-basierte	n. a.	GitHub, GitLab, Bitbucket	GitHub, GitLab, Bitbucket, Perforce, Azure	GitHub, GitLab, Bitbucket, Azure, Custom Imports	Hosted Integration für GitHub, Bitbucket, Azure, Self-hosted GitHub Enterprise, BB Server, GitLab	n. a.	Git-basierte
Scan von Artefakt-Repositorys	JFrog Artifactory, Nexus	nein	n. a.	JFrog Artifactory, Nexus	JFrog Artifactory, Nexus	nein	JFrog Artifactory, GitHub Packages	nein	JFrog, Nexus und weitere

Übersicht ausgewählter SCA-Anbieter									
Anbieter	Aqua		Anchore/Community	Synopsys	Checkmarx	FOSSA	Mend	OWASP/Community Dependency-Track	Snyk
Produkt	Aqua Supply Chain Security	Aqua Trivy	Syft/Grype	Black Duck	Checkmarx SCA	FOSSA	Mend SCA	OWASP Dependency-Track	Snyk Open Source
Scan von Container-Images	Docker	Docker	Docker, OCI, Singularity	Docker (OpenShift, Kubernetes Package Manager, Pivotal Cloud Foundry)	Docker, AWS ECR (mittels Syft)	OCI-Container (apt, RPM und apk)	Docker, GCR, ACR, ECR	nein	mit Snyk Container
Compliance, Lizenzinformationen	ja	eingeschränkt	eingeschränkt	ja	ja	ja	ja	nein	mit Enterprise-Lizenz
IDE-Integration	(ja)	JetBrains IDEs, VS Code, (Vim mit Community-Plug-in)	VS Code für macOS und Linux	möglich mittels Code Sight	JetBrains IntelliJ, Visual Studio Code	nein	Visual Studio, VS Code, IntelliJ IDEA, GitHub Codespaces	nein	Eclipse, JetBrains-IDEs, VS, VS Code, Language Server (Beta)
CLI	ja	ja	ja	ja	ja	ja	ja	ja	ja
API	ja	nein	nein	ja	ja	ja	ja	ja	mit Enterprise-Lizenz
unterstützte Sprachen	Java, C/C++, .NET, Node.js, PHP, Python, Go, Ruby, Rust	Go, Java, .NET, PHP, Python, Ruby , Node.js	ca. 20	ca. 25	Java, C++, .NET, Python, PHP, Swift, Objective-C, Go, Ruby	ca. 20	über 200	Java, .NET, experimentell: Python, PHP, Node.js, Ruby, Swift	ca. 15
unterstützte Paketmanager		ca. 10	ca. 20	ca. 20	ca. 15	ca. 20	ca. 30	ca. 20, davon 2–3 experimentell	ca. 15
Scan von Binärdaten	Go	nein	nein	Java, .NET, Go	nein	nein	ja	nein	
Prüfung von Codeerreichbarkeit[1]	nein	nein	nein	für Java	ja, Exploitable Path	nein	ja, Reachability Path Analysis	nein	für Java, mit Snyk Code
automatisierte Remediation	nein	nein	nein	nein	Remediation Manifests für npm	automatisierte Pull Requests	automatisierte Pull Requests	nein	automatisierte Pull/Merge Requests
Definition von Richtlinien	ja	nein	nein	ja	ja	ja	ja	ja	mit Enterprise-LIzenz
Preis	auf Anfrage (Lizenzierung nach Repositorys)	kostenlos (Open Source)	kostenlos (Open Source)	auf Anfrage	auf Anfrage	ab 104 Dollar pro Entwickler und Monat, Enterprise	ab 16 000 Euro pro Jahr (für 20 Entwickler)	kostenlos (Open Source)	ab 23 Dollar pro Entwickler und Monat, limitierte Version kostenlos, Enterprise auf Anfr.
n. a. – nicht anwendbar, BB – Bitbucket; [1] Tests, ob die kompromittierte Funktion/Methode tatsächlich aufgerufen wird									

OWASP Dependency-Track

Eines der am längsten verfügbaren SCA-Tools kommt vom Open Worldwide Application Security Project: das Open-Source-Werkzeug OWASP Dependency-Track (ODT). Es gibt SBOMs im CycloneDX-Format aus und man kann sie in diesem Format auch importieren. Für den Abgleich mit bekannten Schwachstellen nutzt das Werkzeug die National Vulnerability Database, GitHub Advisories und den Sonatype OSS Index als Datenquellen. Weitere, zum Teil kostenpflichtige Quellen können Anwender über Plug-ins freischalten. Metadaten über Abhängigkeiten gewinnt ODT aus einer Reihe von verbreiteten Paketformaten, neben den üblichen NuGet, PyPi, Maven oder NPM sind auch Cargo für Rust-Projekte oder Hex für Elixir/Erlang darunter. ODT ist nicht auf die Analyse von Abhängigkeiten und Schwachstellen beschränkt, es ermöglicht auch, Richtlinien (Policies) festzulegen, die bestimmte Pakete, Softwarelizenzen oder Software mit Schwachstellen eines definierten Schweregrades

ausschließen.

ODT ist lokal installierbar. Ab Version 4 der Software sind Backend und Frontend voneinander getrennt. Das Backend – der API-Server – ist eine klassische Serverapplikation, die die API per Jetty zur Verfügung stellt und ihre Daten im lokalen Dateisystem und einer relationalen Datenbank speichert. Das Frontend ist eine Single-Page-Webapplikation. Sie stellt Dashboards und Reports dar und dient der Konfiguration. Am einfachsten ist die Installation als Docker-Container. Über ein offizielles Jenkins-Plug-in oder GitHub Actions wird ODT in die CI/CD-Pipeline integriert.

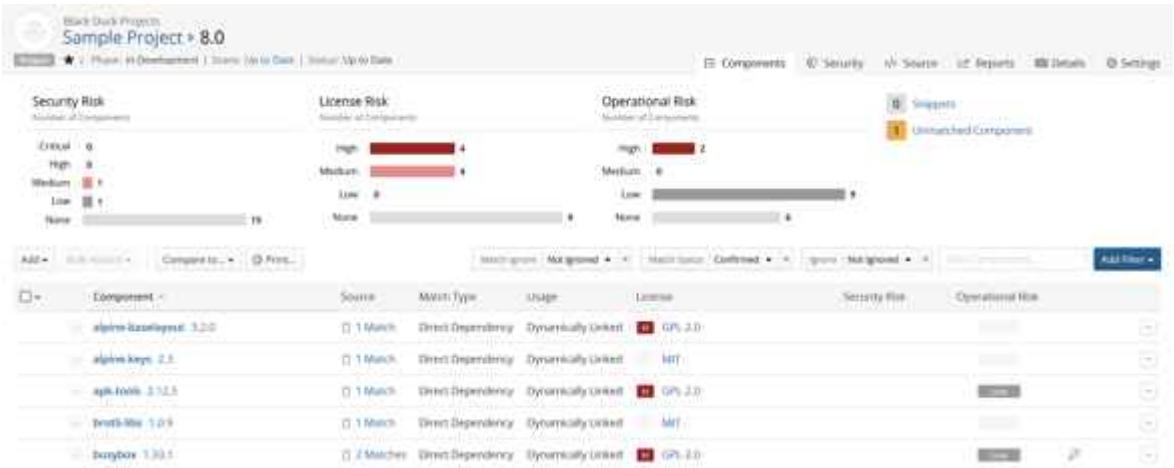
Syft und Grype

Das US-Unternehmen Anchore stellt mit Syft ein Open-Source-Tool zur Verfügung, das hauptsächlich der Erstellung von Software Bills of Materials (SBOMs) dient. Syft verfügt ausschließlich über eine Kommandozeilenschnittstelle, es stellt keine grafische Benutzeroberfläche bereit. Zusätzlich bietet Anchore das Tool Grype an, das in Verbindung mit Syft oder auch einzeln Vulnerability-Scans durchführt. Mit der Kombination von Syft und Grype lassen sich viele Anwendungsszenarien der großen kommerziellen Lösungen abdecken, wenn auch mit manuellem Konfigurationsaufwand. Für die Integration in CI/CD-Pipelines stellen Anchore und die Community Werkzeuge zur Verfügung, beispielsweise Jenkins-Plug-ins oder GitHub Actions, selbst ein IDE-Plug-in für VS Code gibt es.

Syft und Grype lassen sich lokal installieren; die Schwachstellendatenbank kommt im SQLite-Format und wird in der Standardkonfiguration automatisch über das Netz aktualisiert. Die beiden Open-Source-Werkzeuge von Anchore haben keine eigene API, als CLI-Tools mit wohldefinierten Ausgabeformaten lassen sie sich aber prinzipiell von anderen APIs benutzen. Eine der Stärken beider Anwendungen ist die Ausrichtung auf containerisierte Applikationen.

Synopsys Black Duck

Black Duck gehört zu den am längsten verfügbaren und am häufigsten eingesetzten SCA-Angeboten am Markt. Dazu kommt, dass es nach der Übernahme des Herstellers durch Synopsys mit dessen Codeanalysewerkzeugen verzahnbar ist: So lässt sich SCA mit statischen und dynamischen Codeanalysemethoden (DAST, SAST) und Fuzzing aus einer Hand kombinieren. Es ist auf den unternehmensweiten Einsatz ausgerichtet und soll dabei helfen, in großen Projekten zentrale Sicherheits- und Compliancerichtlinien zu definieren und durchzusetzen (siehe Abbildung 1).



Die BOM-Ansicht von Black Duck listet Lizenz-, Sicherheits- und Betriebsrisiken einer Komponente gemeinsam auf. Letztere ergeben sich zum Beispiel aus Paketen, die kaum noch gepflegt werden oder eine geringe Reputation besitzen (Abb. 1). *Synopsys*

Damit einher gehen ein umfassendes Rollen- und Berechtigungsmodell, komplexe Policies und Regelsätze, die definieren, wie mit bestimmten Risiken umzugehen ist, sowie Reportgeneratoren. Entsprechend langwierig kann die Einführung des Produkts sein. Synopsys gibt die Black Duck Security Advisories heraus und verspricht, dass seine SCA-Software viele Schwachstellen schon meldet, bevor sie in der National Vulnerability Datebase auftauchen.

Black Duck integriert sich via Plug-ins in alle verbreiteten CI/CD-Frameworks, Code- und Artefakt-Repositorys. Für die IDE-

Integration ist Synopsys Code Sight zuständig, ein separates Produkt, das Black-Duck-Anwender kostenlos nutzen können.

Neben Sourcecode analysiert Black Duck Java-, .NET- und Go-Binaries, binäre Repositorys im JFrog-Artifactory- und Nexus-Format und bestimmte Firmwareformate. Bei der Codeanalyse verlässt es sich nicht nur auf die Deklarationen in den Manifesten der Pakete. Der Hersteller wirbt mit einer Multi-Faktor-Open-Source-Erkennung und integriert eine proprietäre Methode namens Codeprint, um Open-Source- und Fremdanbieter-Komponenten zu identifizieren.

Aqua Supply Chain Security

Aqua Security gilt als Spezialist für die Absicherung von containerisierten Anwendungen. Nach der Übernahme von Argon Ende 2021 – eines auf Supply Chain Security spezialisierten Start-ups aus Israel – bietet das Unternehmen mit Aqua Supply Chain Security ein Produkt an, das die wesentlichen Aspekte der SCA abdeckt und darüber hinaus weitere Sicherheitsüberprüfungen durchführt. So scannt es per statischer Codeanalyse bei Abhängigkeiten auch den Quellcode selbst, sucht nach Fehlkonfigurationen in den Build-Tools und in Infrastructure as Code. Go-Code können die Aqua-Scanner auch in Binärform untersuchen.

Eine Besonderheit stellen die erweiterten SBOMs dar, die die Plattform erzeugen kann. Die als Next Generation SBOMs bezeichneten Dokumente sind mit zusätzlichen Informationen angereichert, etwa ob Peer-Reviews stattfanden oder ob das Code-Repository eine Zwei-Faktor-Authentifizierung verlangt. Zusätzlich soll Code Signing die Integrität sicherstellen.

Compliance- und Sicherheitsfunktionen sind integriert, Aqua Supply Chain Security eignet sich also auch zur Top-Level-Beurteilung der Risiken durch Open-Source-Einsatz im gesamten Unternehmen. Für die einzelnen Open-Source-Komponenten erstellt das Produkt einen Reputation Score, aus dem

Maintenance-Zustand, der Beliebtheit, der Zahl und Schwere von Sicherheitslücken und anderen Faktoren.

Aqua vermarktet Supply Chain Security innerhalb seiner Cloud-native Application Protection Platform (CNAPP), in dessen Variante Dev Security. Es wird dort von den Komponenten Risk &Vulnerability Scanning sowie Advanced Malware Protection ergänzt.

Aqua Trivy

Ein Kernbestandteil von Aqua Supply Chain Security ist der Security-Scanner Trivy, der als separates CLI-Tool vor allem in der Container-Welt häufig eingesetzt wird. Für sich genommen ist er zwar kein vollwertiges SCA-Produkt, aber er ist Open Source und deckt so viele SCA-Aspekte ab, dass er in Kombination mit ein paar Skripten und anderen Open-Source-Werkzeugen die Grundlage für eine kleine, flexible, selbst gebaute SCA-Lösung sein kann. Trivy ist kein reiner Container-Scanner, sondern kann auch Code in Git-Repositorys, auf dem lokalen Filesystem oder in Images virtueller Maschinen prüfen. Er identifiziert dort bekannte Schwachstellen, findet Abhängigkeiten, Konfigurationsfehler und sensible Informationen wie Zugangsdaten. Außerdem identifiziert er Open-Source-Lizenzen. Seit Kurzem kann Trivy auch SBOMs im SPDX- oder CycloneDX-Format erzeugen.

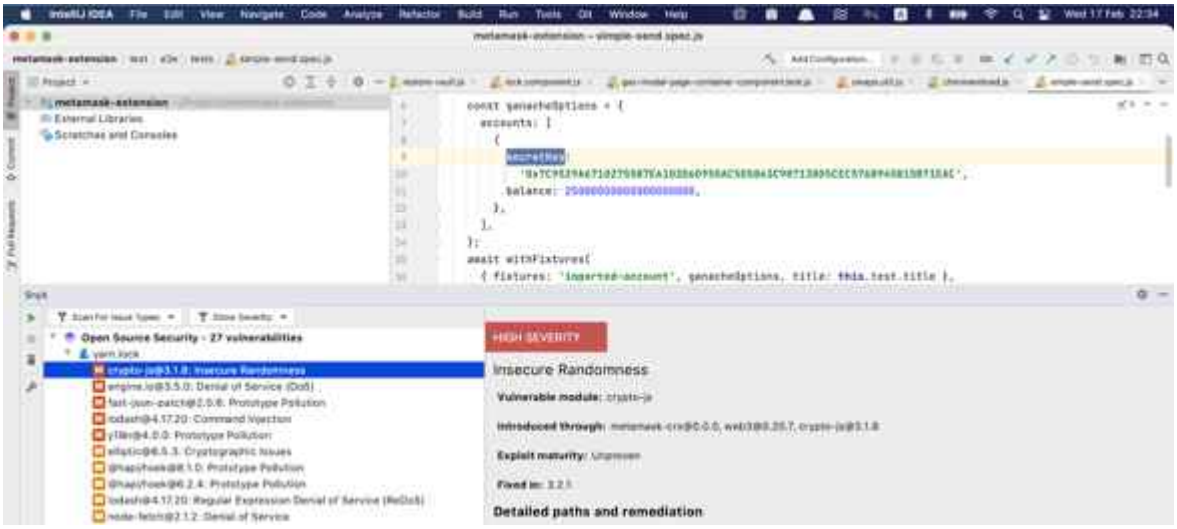
Trivy ist ein reines Kommandozeilenwerkzeug und somit automatisierungsfreundlich. Aqua Security stellt sogar selbst Integrationen für GitHub Actions und Azure DevOps zur Verfügung. Trivy bringt seine eigene kompakte Schwachstellendatenbank mit, bei gefundenen Lücken verlinkt er in der Ausgabe auf den entsprechenden Eintrag in der Aqua Vulnerability Database, die auch das kommerzielle Produkt Aqua Supply Chain Security nutzt.

FOSSA

Das Produkt FOSSA (Free Open Source Software Analysis) des gleichnamigen Anbieters bezeichnet dieser als Open Source Risk Management Platform. Sein Schwerpunkt liegt darauf, rechtliche und Sicherheitsrisiken gemeinsam zu betrachten und die Nutzung von Open Source unternehmensweit durch Richtlinien abzudecken. Eine zentrale Policy Engine soll Rechts- und Entwicklungsabteilungen bei der gemeinsamen Ausarbeitung dieser Richtlinien unterstützen und garantieren, dass sie im Softwarelebenszyklus durchgesetzt werden. FOSSA wirbt mit rechtssicheren, auditfähigen Berichten und automatisierten Risikobewertungen, die beispielsweise den Due-Diligence-Prozess bei Firmenübernahmen beschleunigen sollen. Für DevOps-Teams bietet FOSSA neben Integrationsmöglichkeiten in alle relevanten CI-Produkte auch eine generische CI-Schnittstelle für individuelle Pipelines an, es scannt Container nach OCI-Standard und unterstützt rund 20 verbreitete Programmiersprachen.

Snyk Open Source

Snyk vereint mehrere Produkte auf einer Plattform. Für SCA zuständig ist die Komponente mit dem Namen Snyk Open Source, daneben bietet Snyk Code eine statische Codeanalyse. Snyk Container und Snyk Infrastructure as Code sind weitere Komponenten. Snyk ist in erster Linie ein SaaS-Anbieter. In dieser Variante sind die Komponenten auch einzeln buchbar. Eine Enterprise-Lizenz umfasst immer alle Produkte; sie ist auch Voraussetzung, um Features nutzen zu können, die zu einem umfassenden SCA-Produkt gehören, wie Lizenzcompliance, Verwaltung von Richtlinien und Erstellung von Berichten sowie die Option, auf den Unternehmensservern gehostete Code-Repositorys einzubinden.



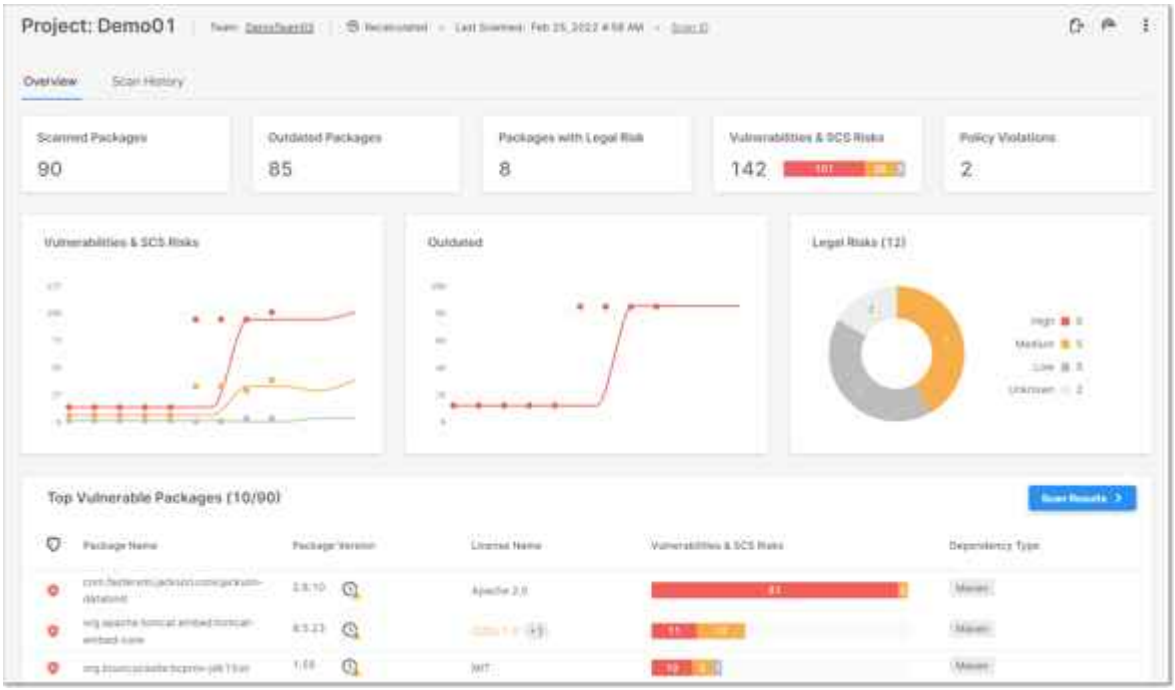
Mit einem Plug-in für JetBrains-IDEs informiert Snyk schon beim Schreiben des Codes über Sicherheitslücken in den eingebundenen Open-Source-Bibliotheken (Abb. 2). *Snyk*
Eine vollständige On-Premises-Installation bietet Snyk nicht an – die Enterprise-Variante erlaubt es aber, ein als Snyk Broker bezeichnetes Proxysystem einzurichten, das Codescans lokal ausführt und die Kommunikation mit den Snyk-Servern über einen Tunnel absichert. Mit einem normalen SaaS-Abo erfolgt der Scan auf den Servern von Snyk.

Snyk Open Source lässt sich mit IDEs, den gängigen CI/CD-Tools und Git-basierten Repositorys verknüpfen (siehe Abbildung 2). Im Vergleich zu anderen Produkten ist vor allem die IDE-Unterstützung gut ausgebaut. So schlägt zum Beispiel das JetBrains-Plug-in mit einer als Open Source Advisor bezeichneten Funktion geeignete Open-Source-Pakete vor und bezieht dabei Popularität, Maintenance-Zustand und Bewertungen der Community ein.

Der Umgang mit SBOMs zählte lange Zeit nicht zu den Stärken von Snyk. Kürzlich hat das Unternehmen aber angekündigt, dass die API und das Kommandozeilenwerkzeug künftig SBOMs in den CycloneDX- und SPDX-Formaten exportieren sollen. In der aktuellen Betaversion der API ist das Feature bereits zu finden.

Checkmarx SCA

Checkmarx ist ein 2006 in Israel gegründetes IT-Security-Unternehmen, dessen Sicherheitsforscher wiederholt wichtige Schwachstellen aufgedeckt haben und federführend an der Erstellung der OWASP API Top Ten beteiligt sind. Erstes Produkt der Firma war CxSAST, ein Werkzeug zur statischen Codeanalyse, Checkmarx SCA (CxSCA) kam erst 2020 hinzu. Wie alle der größeren Anbieter betreibt Checkmarx seine eigene Schwachstellendatenbank, zusätzlich dazu auch eine Datenbank bösartiger Pakete, die gezielt dafür entwickelt werden, Softwareprojekte zu infiltrieren.



Dashboards wie hier bei Checkmarx gehören zur Grundausstattung aller umfangreicheren SCA-Tools (Abb. 3). *Checkmarx*

Checkmarx SCA ist Teil von Checkmarx One, dem integrierten Hauptprodukt des Herstellers, das von diesem als Application Security Testing Platform bezeichnet wird. CxSCA kann aber auch separat lizenziert werden. Am günstigsten ist die Nutzung als Managed Service, optional ist der Betrieb in einer Private-Cloud-Umgebung oder vollständig on Premises möglich. Checkmarx SCA implementiert eine Methode namens Exploitable Path, die im Sourcecode des Projekts danach sucht, welche Funktionen in den Abhängigkeiten tatsächlich aufgerufen

werden. Laut Hersteller funktioniert das für jede Programmiersprache, die sich mit CxSAST untersuchen lässt. Bei Scans über die SCA-Website lädt das Tool auch den Sourcecode hoch und dort bleibt er für bis zu 24 Stunden gespeichert. Ein Resolver kann Abhängigkeiten aber auch on Premises ermitteln und schickt diese Daten dann an die Plattform zur Risikoanalyse.

Bei Verwendung von Agents oder des Resolvers gelangen nur Metadaten, Manifestdateien und Fingerprints des Sourcecodes auf die Checkmarx-Server. Zu den Metadaten zählt Checkmarx auch sämtliche Dateinamen. Daten landen in einem verschlüsselten S3-Bucket, Sourcecode wird höchstens 24 Stunden aufbewahrt.

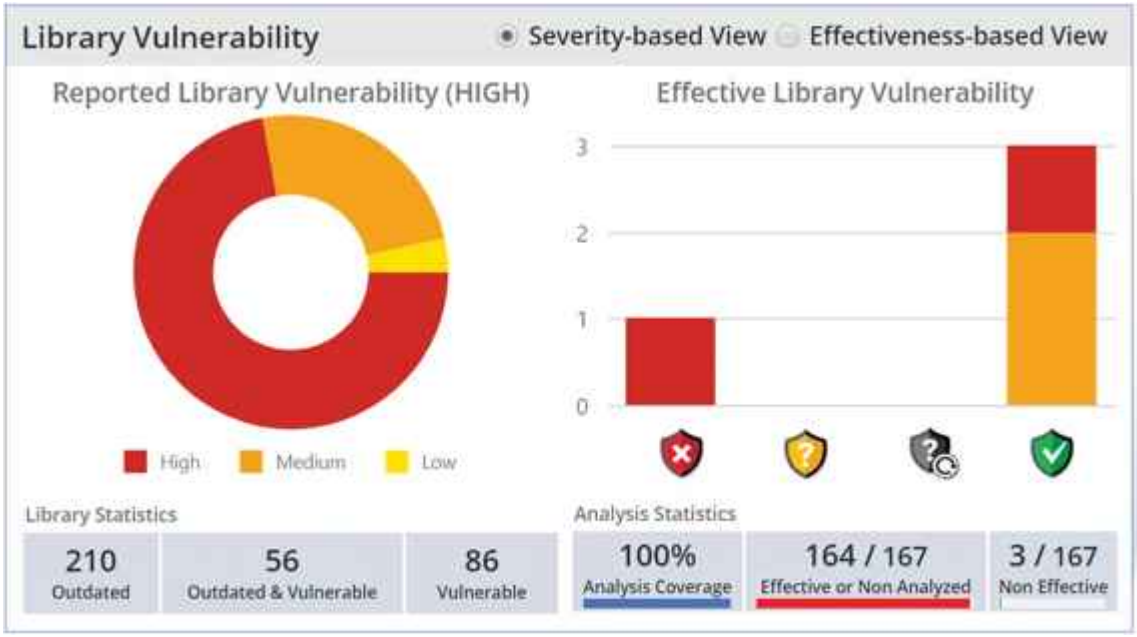
Mend SCA

Mend, vormals Whitesource, ist ein weiterer Hersteller im Umfeld der Anwendungssicherheit, der seine Wurzeln in Israel hat. Hier war das SCA-Produkt zuerst da, SAST kam später hinzu. Mend entwickelt auch den von Entwicklern viel gelobten Renovate Bot, ein Open-Source-Werkzeug zur automatischen Aktualisierung von Dependencies. Diesen wird iX in einer der kommenden Ausgaben vorstellen.

Mend sammelt Schwachstellen und Security Advisories aus zahlreichen Quellen in einer eigenen Datenbank und scannt auch Software, die in den Manifesten der Paketmanager nicht deklariert ist. Eine der Stärken des Produkts ist das Bewertungssystem von Schwachstellen (siehe Abbildung 4). Hier berücksichtigt Mend vor allem, ob der eigene Code verwundbare Funktionen aufruft (Reachable Path Analysis). Aber auch andere, nicht direkt die Schwachstelle selbst betreffende Faktoren, die insgesamt die Auswirkungen auf die Geschäftstätigkeit widerspiegeln sollen, gehen ein.

Damit gehen entwicklerfreundliche Benachrichtigungs- und Remediation-Möglichkeiten einher. Ist Mend SCA in ein

Repository integriert, kontrolliert es bei jedem Commit den Code auf vom Entwickler eingebaute Schwachstellen, Vulnerabilities in verwendetem Open-Source-Code und Lizenzverletzungen. Das Tool öffnet Pull Requests mit einem Upgrade des Pakets auf eine nicht verwundbare Version. Im einfachsten Fall ist somit die Schwachstelle mit einem Klick aus dem Abhängigkeitsbaum verschwunden.



Mend priorisiert Schwachstellen anhand verschiedener Metriken. Eine davon ist die Erreichbarkeit des Codes von der eigenen Anwendung aus (Abb. 4). *Mend*

Seine IDE-Pug-ins nennt der Anbieter Mend Advise, es gibt sie für IntelliJ Idea, WebStorm und PyCharm von JetBrains, für Visual Studio und VS Code sowie für Eclipse. Eine clevere Idee ist eine Browsererweiterung, die beim Stöbern auf Stack Overflow oder GitHub auf Sicherheitsrisiken in den gerade dargestellten oder erwähnten Komponenten hinweist.

Compliance- und Sicherheitsrichtlinien kann Mend SCA ebenfalls über entsprechende Regelwerke definieren und durchsetzen – insgesamt stehen bei diesem Produkt aber eher die Bedürfnisse der Developer als die der Rechtsabteilung im Vordergrund. In den letzten Monaten hat Mend seine API um einen SBOM-Export erweitert, vorher musste man SBOMs mit einem Tool aus dem internen Softwareinventarformat erzeugen. Jetzt lässt sich der Prozess automatisieren.

Weitere Anbieter

Contrast SCA ist Teil der vor allem im Java-Umfeld verbreiteten Secure Code Platform des Herstellers. Sie verfolgt den Ansatz, Agenten in den Code einer Anwendung zu integrieren, die im laufenden Betrieb Schwachstellen identifizieren. Diese Agenten liefern auch Informationen zu den verwendeten Open-Source-Komponenten, aus denen die Plattform Schwachstellen identifiziert und detaillierte SBOMs generiert. Neben Java unterstützt Contrast weitere Sprachen und Plattformen etwa .NET, Python, Ruby und Go.

Die kanadische Firma **MergeBase** bewirbt ihr SCA-Produkt mit niedriger Falsch-positiv-Rate und Laufzeitüberwachung des Produktivcodes. Als SaaS ist MergeBase relativ günstig (ab 38 US-Dollar pro Entwickler), Enterprise-Varianten lassen sich auch on Premises installieren. Der Funktionsumfang ist mit dem von Snyk vergleichbar.

Revenera FlexNet Code Insights lädt entweder die gesamte Codebasis eines Projekts zum Scannen auf den Server oder verbindet den Scanserver mit einem Software-Repository, das er dann automatisch nach Vorgaben scannt. Im Unterschied zu Werkzeugen, die auf die Cloud und DevOps-Prozesse ausgerichtet sind und sich an verschiedene andere Tools andocken, hat FlexNet Code Insight eine eher konservative Herangehensweise: Das System dient als „Single Source of Truth“ für den gesamten Code des Projekts, erstellt SBOMs und identifiziert Schwachstellen.

Unternehmen, die bei ihren Artefakt-Repositorys auf JFrog setzen, können mit **JFrog XRay** die dazu passende SCA-Lösung einsetzen, die eine native Artifactory-Anbindung bietet und Zugriff zu sämtlichen Metadaten im Repository hat und auch Binaries scannt. XFrog XRay identifiziert Lizenzen und Schwachstellen, erlaubt die Definition von Policies und exportiert SBOMs, JFrog pflegt eine Schwachstellendatenbank, die sich aus der VulnDB und eigenen Einträgen speist. Mit dem

FrogBot lässt sich JFrog XRay auch in GitHub-Repositorys einbinden.

Veracode kombiniert SCA mit statischer Codeanalyse. Bei Letzterer versteht es auch Cobol, PRG oder verschiedene SQL-Dialekte, ist also auch im traditionellen IT-Umfeld zu Hause. **Veracode SCA** kommt mit 13 verbreiteten moderneren Sprachen und den entsprechenden Paketformaten zurecht. Es ist ein umfangreiches, sowohl auf Security als auch auf Compliance ausgerichtetes SCA-Produkt, das alle entscheidenden Funktionen und Integrationsmöglichkeiten mitbringt.

Die Nexus-Plattform von Sonatype ist bei Cloud-Entwicklern vor allem für ihr Artefakt-Repository bekannt, das direkt mit JFrog Artifactory konkurriert. Sicherheitsforscher kennen Sonatype eher wegen seiner Schwachstellendatenbank. Mit **Nexus Lifecycle** hat das Unternehmen ein SCA-Produkt im Angebot, das zwar auf seine übrigen Securityprodukte abgestimmt, aber nicht auf Anwender der Nexus-Repositorys beschränkt ist. Nexus Lifecycle ist ein umfassendes Produkt für den Enterprise-Einsatz.

Fazit

Für die Auswahl einer der großen kommerziellen Lösungen ist auf jeden Fall eine genaue Anforderungsanalyse sowohl seitens der Entwickler und des Sicherheitsteams als auch – wenn Complianceaspekte wichtig sind – der Rechtsabteilung notwendig. Sehr empfehlenswert zur Vorbereitung ist der 13-seitige „Open Guide to Evaluating Software Composition Tools“ der Linux Foundation, der die wichtigsten Metriken identifiziert und dabei hilft, ihre Relevanz für das eigene Projekt oder Unternehmen einzuschätzen.

Eine längere, gut geplante Testphase vor der Lizenzierung des Produktes ist unabdingbar und bei allen seriösen Anbietern möglich. Bei Herstellern, die ihre komplette Nutzer- oder Administrationsdokumentation frei verfügbar machen, lassen

sich einige Anforderungen schon vorher klären, denn nicht selten zeigen die Dokumente, wie die in Fact Sheets beworbenen Features tatsächlich funktionieren, oder sie decken Einschränkungen auf.

Zu beachten ist auch, dass bei möglicherweise schnell eingekauften SaaS-Angeboten Sourcecode und Metadaten das Unternehmen verlassen können und unter Umständen auf US-Servern landen. Im Sinne der DSGVO dürfte das meist zwar unproblematisch sein, da es sich nicht um personenbezogene Daten handelt. Aber das eine oder andere Unternehmen hat vielleicht doch gute Gründe, den Sourcecode lokal zu halten – speziell, wenn es um Auftragsentwicklung geht. Zum Glück gehen die meisten Anbieter mit Informationen, wo und wie lange Kundendaten gespeichert werden, recht transparent um.

Aus technischer Sicht essenziell ist, dass sich das SCA-Produkt an möglichst viele der im Unternehmen eingesetzten Entwicklungs- und Deployment-Werkzeuge anbinden lässt – am besten auch an solche, die für später auf der Wunschliste stehen. Kleinere Integrationen lassen sich über die API nachrüsten.

Darüber hinaus ist eine niedrige Falsch-positiv-Rate bei den gemeldeten Schwachstellen wichtig, damit das Werkzeug den Entwicklern nicht im Weg steht. Idealerweise kommt eine Überprüfung dazu, ob der Code mit der Schwachstelle überhaupt aufgerufen wird. Dieses Feature ist unter verschiedenen Namen (Reachable Path, Exploitable Path etc.) bei Anbietern verfügbar, die auch SAST-Produkte im Portfolio haben, manchmal jedoch nur für ausgewählte Sprachen.

Eine gute Integration in IDEs ist ein großes Plus, denn so verhindert man, dass Schwachstellen überhaupt den Weg in den Code finden und nicht erst beim Einchecken in das Repository oder noch später auffallen. Automatisierung und permanente Überwachung der CI-Pipelines sollte möglich sein.

Schwieriger wird es, wenn das Werkzeug dazu benutzt werden soll, unternehmensweite Policies durchzusetzen und Complianceanforderungen zu überwachen. Dann bringt ein Test der Software innerhalb eines Entwicklerteams keinen nennenswerten Erkenntnisgewinn. Hier könnte ein abteilungsübergreifendes Projektteam die Anforderungen möglichst genau spezifizieren und nach einer sinnvollen Vorauswahl eine kleine Zahl von Anbietern genauer unter die Lupe nehmen.

Wenn es darum geht, überhaupt erstmalig werkzeuggestützte Software-Composition-Analyse zu betreiben, ließe sich alternativ in einem Developer-Team ein eher an den Bedürfnissen der Entwickler ausgerichtetes Produkt einführen. Es muss aber zumindest von seinen Spezifikationen her den Compliancebereich mit abdecken könnte und ginge erst nach positiven Erfahrungen der Developer in den unternehmensweiten Einsatz. Auch ein nicht ganz optimales Werkzeug zur Ermittlung von Risiken durch Open-Source-Software sichert die Softwarelieferkette besser ab als gar keines. (ulw@ix.de)

1. Quellen
2. Udo Schneider; SBOMs – Stücklisten für Software; iX 10/2022, S. 54
3. Weitere Infos zu Tools und Auswahlkriterien: ix.de/zvbm

QR-Codes – Sicherheitsprobleme

Gefahr im Bithaufen

QR-Codes: Sicherheitsproblem oder nicht?

QR-Codes können ähnlich wie Phishing-Mails Träger gefährlicher URLs sein. Wir erklären, welche Tricks sich Kriminelle ausgedacht haben und worauf Sie beim Scan von QR-Codes achten müssen.

Von Wilhelm Drehling

Die quadratischen Codes sind im Alltag nützliche Helfer: Mit einem Scan können Sie eine URL aufrufen, einen Kontakt hinzufügen oder dem Gast zu Hause das Abtippen des WLAN-Passworts ersparen. Weil sie praktisch sind und auch mal leichtfertig gescannt werden, haben auch Angreifer ihre Freude an QR-Codes gefunden. Denn das Aussehen des QR-Codes verrät nichts über dessen Inhalt, so kann sich in dem Pixelhaufen ein gefährlicher Link zu einer täuschend echten Anmeldeseite einer Fake-Bank oder zu einem Trojaner verbergen. In den vergangenen Jahren haben Kriminelle originelle Methoden erfunden – denen man aber zum Glück nicht schutzlos ausgeliefert ist.

Quishing

Das erste Angriffsszenario gehört in die Kategorie der Phishing-Angriffe: Vermutlich kommen Ihnen dubiose Mails wie „PayPal: Ihr Konto ist vorübergehend eingeschränkt“ bekannt vor. Mit solchen Mails versuchen die Angreifer häufig, an Ihre Anmeldedaten heranzukommen, indem sie Sie auf eine gefälschte Webseite mit gewohntem Anmeldefenster weiterleiten. Enthält die Mail einen QR-Code, der zur Phishing-Seite führt, spricht man von Quishing.

Der große Unterschied zu den üblichen Mail-Betrügereien: Es

hat sich bereits herumgesprochen, dass man nicht einfach so auf Links in Mails klicken sollte, die möglicherweise obendrein in schlechtem Deutsch verfasst sind. Bei QR-Codes ist das nicht der Fall. Ergo schenkt man QR-Codes mehr Vertrauen, scannt sie ein und landet dann womöglich auf einer Phishing-Seite oder Ärgerem.

Diese Masche tritt häufig in unterschiedlichen Varianten auf: Die Volksbank warnte im Dezember 2021 vor Mails und sogar Briefen mit QR-Codes, die Kunden dazu aufforderten, eine neue App herunterzuladen und sich dort zu registrieren. Ähnliche Angriffe mit QR-Codes häuften sich in letzter Zeit so sehr, dass die Polizei eine Warnung vor QR-Codes in Mails aussprach (sämtliche Warnungen haben wir Ihnen unter ct.de/yrf5 verlinkt).

Ob diese Warnungen wirklich etwas bringen, lässt sich diskutieren. Der c’t-Security-Experte Jürgen Schmidt geht in seinem Kommentar im Kasten rechts dieser Frage auf den Grund.

QR-Codes sind nicht das Problem

Ein Kommentar von Jürgen Schmidt (Leiter heise Security)

Die Krypto-Börse Coinbase platzierte in der Halbzeitpause des Superbowls einen Werbespot, der die Zuschauenden dazu verleiten sollte, einen über den Fernseher hüpfenden QR-Code mit der Handy-Kamera einzufangen. Auf der dann angezeigten Website erwartete sie nur eine Meldung, dass der Dienst nicht erreichbar ist – vermutlich wegen Überlastung. Aber das ist eine andere Geschichte.

Es folgte ein Aufschrei der um die Sicherheit besorgten

Experten, dass man den Anwendern unsichere Verhaltensweisen antrainiere und somit Phishing-Betrügern in die Karten spiele. Schließlich könne sich hinter dem QR-Code doch auch eine bösartige Phishing-Webseite verbergen, die es auf ihre Zugangsdaten abgesehen hat. Ich halte diesen Ansatz für falsch.

Das World Wide Web beruht darauf, dass Anwender Links öffnen. Auch solche, bei denen sie vorher nicht wissen, was genau sich dahinter verbirgt, schließlich will man ja Dinge entdecken. Es ist deshalb unsere (uns hier im Sinne von all denen, die im weitesten Sinne das Web mitgestalten) Aufgabe, den Anwendern Werkzeuge bereitzustellen, mit denen sie das tun können. Sprich: Anwender sollten einen Link ohne unmittelbare Gefahr öffnen können. Wenn allein durch das Öffnen eines Links etwas Böses passiert, dann ist das ein Fehler im Browser, den dessen Hersteller zu verantworten und zu beseitigen hat.

Die Verantwortung des Anwenders beginnt, wenn er mit der Seite interagiert. Bevor er dort persönliche Daten oder sogar ein Passwort eingibt, sollte er sich die Frage stellen, ob und wie weit er der Seite vertrauen kann. Da spielt primär der Kontext eine wichtige Rolle. Das ist in der analogen Welt nicht anders: Dem Hotel-Angestellten beim Check-in gibt man seine Kreditkarte; einem Unbekannten am Bahnhof eher nicht.

In der digitalen Welt zeigt sich da schon das erste Problem: Browser zeigen immer öfter gar nicht mehr an, wo sich der Anwender gerade befindet und machen es damit schwer, die Vertrauenswürdigkeit einer Passwortabfrage zu beurteilen oder gar zu überprüfen. Immerhin können sich Anwender fragen: Wie bin ich hierher gelangt? Über ein gespeichertes Lesezeichen oder einen QR-Code in einem eher zweifelhaften Zusammenhang? Der Vertrauens-Check ist nicht trivial – aber etwas, was man Anwendern beibringen kann und sollte. „Klicke nicht auf Links“ oder „Verwende keine QR-Codes“ hingegen sind keine sinnvollen Lernziele. Darüber hinaus kann man Anwender zu Multifaktor-Authentifizierung und insbesondere FIDO2 ermuntern, weil sie

konzeptionell vor Phishing schützen.

Eine Verteufelung von QR-Codes hingegen führt nur zu noch mehr angeblichen „Best Practices der Security“, die zwar gebetsmühlenartig wiederholt werden, an die sich niemand wirklich hält, weil sie praxisfern sind. Ich scanne den QR-Code im Restaurant, um mir die Speisekarte anzuschauen und ich würde mir wünschen, dass auch meine Bank Girocodes einführt [1], weil ich es satthabe, ständig gefühlt 100-stellige IBANs von Hand einzutippen. Ich werde also auch anderen Menschen, die sich von mir Sicherheitstipps erhoffen, nicht erzählen, dass sie keine QR-Codes benutzen dürfen, sondern lieber zur Zweifaktor-Authentifizierung raten.

Überklebt

Ein deutlich gefährlicherer und unscheinbarer Angriffsvektor geht von öffentlichen QR-Codes aus, die Sie in Broschüren, Werbeplakaten oder Speisekarten finden. Angreifer können die Codes überkleben und die Opfer somit auf gefälschte Webseiten locken. Die Idee hinter dem Angriff ist nicht neu, schon 2013 warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor überklebten QR-Codes.

Das passiert nicht unbedingt bei Speisekarten; vorsichtig müssen Sie bei QR-Codes sein, die „alternative Bezahlmöglichkeiten“ anpreisen. Das FBI warnt in den USA zum Beispiel davor, keine QR-Codes bei Parkplätzen zu scannen, die zu einem Bezahldienst weiterleiten: Anstatt zum Parkautomat zu laufen, könne man so bequem die Rechnung für die Parkdauer bezahlen. Doof nur, wenn das Geld dann nicht an den Parkplatzbetreiber fließt, sondern direkt in die Taschen der Betrüger.

Überklebte QR-Codes verheißen auch bei Außenwerbung Unheil, die dazu einlädt, eine App herunterzuladen oder Webseiten zu besuchen. In solchen Fällen greifen die Angreifer erneut nach Ihren Daten und im schlimmsten Falle versuchen sie, über eine

App einen Trojaner auf Ihr Smartphone herunterzuladen (zugegebenermaßen ist das leichter beim Google Play Store zu bewerkstelligen als über den App Store auf iOS).

Genauso kritisch sind leicht zugängliche QR-Codes in Zügen oder Einkaufszentren, die einen einfachen Zugang zum WLAN anbieten: Ein solcher QR-Code kann von Angreifern überklebt worden sein. Mit einem Klick verbinden Sie sich mit einem von Angreifern eingerichteten gleichnamigen Hotspot.

Gegenmaßnahmen

Hersteller von Smartphones haben schon früh reagiert: Kamera-Apps folgen nicht mehr direkt einer gescannten URL. Ein Großteil aller modernen Kamera-Apps zeigt den Link stattdessen auf dem Bildschirm an. Danach ist es an Ihnen, zu entscheiden, ob Sie darauf klicken oder nicht. Dabei ist der gesunde Menschenverstand gefragt: Sieht die URL merkwürdig aus, dann sollten Sie den QR-Code genauso wie eine Phishing-Mail in den Papierkorb befördern.

Wenn Sie zusätzlich auf Nummer sicher gehen wollen (oder Familienangehörigen einen Gefallen tun wollen), weichen Sie unter Android auf eine App wie zum Beispiel Trend Micro QR-Scanner aus (siehe ct.de/yrf5), die den Inhalt des QR-Codes prüft und Sie vor potenziell gefährlichen Links warnt. iOS-Nutzer nehmen die App Intercept X von Sophos (siehe ct.de/yrf5). Die sichere Scanfunktion für QR-Codes ist aber nur ein kleiner Teil der Antiviren-App: Mit der App laden Sie leider noch viele weitere Funktionen herunter, deren Sinn mindestens zweifelhaft ist.

Mit der App QR-Scanner von Trend Micro bekommen Sie eine Einschätzung, ob die URL hinter dem QR-Code potenziell gefährlich ist.
Tipp für ganz harte Tüftler: Alternativ können Sie Ihr Smartphone beiseitelegen und den QR-Code per Hand dekodieren [2]. Das ist zwar mühsam, aber Sie fangen sich auf diese Art und Weise definitiv kein Virus ein.

Fazit

Wie bei vielen der vorgestellten Szenarien spielt der Kontext

eine wichtige Rolle: Ein QR-Code mit WLAN-Daten bei Ihnen zu Hause genießt ein höheres Vertrauen als ein QR-Code auf einem Laternenmast, der für ein öffentliches WLAN wirbt. Im Zweifel sollten Sie die Entscheidung, eine fragwürdige URL anzuklicken, dem gesunden Menschenverstand überlassen oder bei noch größeren Zweifeln eine QR-Überprüfungs-App konsultieren. *(wid@ct.de)*

1. Literatur
2. Jan Mahn, Schöner zahlen, Rechnungen schneller überweisen mit QR-Codes, c't 7/2022, S. 138
3. Wilhelm Drehling, Bithaufen, QR-Codes verstehen und ohne technische Hilfsmittel per Hand dekodieren, c't 17/2022, S. 142

Warnungen und Scanner-App: ct.de/yrf5

BSI-Warnung vor Kaspersky: Die Chronologie

BSI-Warnung vor Kaspersky: Die Chronologie

Interne Unterlagen beweisen, wie das BSI zusammen mit dem Bundesinnenministerium drei Wochen brauchte, um eine Warnung vor Kaspersky-Produkten auszusprechen.

Erst am 15. März, rund drei Wochen nach dem Einmarsch Russlands in die Ukraine, veröffentlicht das BSI eine offizielle Empfehlung, keine weiteren Kaspersky-Produkte mehr zu benutzen.
Mitte März sprach das Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgrund des Angriffskrieges auf die Ukraine eine Warnung vor sämtlichen Kaspersky-Produkten aus. Grund: Kaspersky ist ein russischer Antivirenhersteller mit Sitz in Moskau. Daher besteht die realistische Gefahr, dass die russische Regierung die tiefreichenden Rechte ausnutzt, die Antivirenprogramme in Betriebssystemen haben, um beispielsweise an Informationen heranzukommen. 370 Seiten an Dokumenten zeigen nun die Chronologie dieser Entscheidung.

Der Bayerische Rundfunk forderte die Unterlagen durch eine Anfrage nach dem Informationsfreiheitsgesetz an und wertete sie zusammen mit dem Magazin Der Spiegel aus (siehe ct.de/yu6a). Daraus geht hervor, dass das BSI kurz nach Beginn des Krieges recht schnell die brisante Lage Kaspersky erkannte und nach technischen Gründen suchte, um eine Warnung auszusprechen.

In den internen Mails diskutierten die BSI-Angestellten rege Argumente wie: „Es ist nicht sicher, dass Kaspersky noch die vollständige Kontrolle über seine Software und IT-Systeme hat bzw. diese nicht in Kürze verlieren wird.“ Und man müsse mit „feindlichen Übergriffen auf deutsche Institutionen, Unternehmen und IT-Infrastrukturen“ rechnen. Aber nicht alle

waren dieser Meinung, ein Abteilungsleiter schrieb etwa, dass man nicht vorschnell handeln solle oder womöglich sogar rechtswidrig, denn immerhin habe Kaspersky schon vor längerer Zeit angefangen, Server in die Schweiz auszulagern.

Nach einer intensiven Debatte nickte der BSI-Chef Arne Schönbohm am 5. März intern eine mögliche Warnung ab. Es folgten mehrere Absprachen mit dem Bundesinnenministerium (BMI), dem das BSI unterstellt ist. Etwa zeitgleich wendete sich Kaspersky Hilfe suchend an das BSI und erhoffte sich Rückendeckung, was aber innerhalb der Behörde auf taube Ohren stieß.

Erst einen Tag vor dem Aussprechen der Warnung durch das BSI erfuhr Kaspersky per Mail von der Entscheidung, mit der Bitte zu Stellungnahme innerhalb von drei Stunden. Das Unternehmen fühlt sich nach eigener Aussage übergangen und diskreditiert, weswegen es rechtliche Schritte eingeleitet hat. In zwei Instanzen wurde dem BSI recht gegeben, eine abschließende Entscheidung fällt aber erst im langwierigen Hauptverfahren.

Nach dem Okay des BMI sollte die Warnung am 16. März veröffentlicht werden, doch die Presseabteilung grätschte dazwischen und wünschte sich die Erklärung einen Tag früher zu veröffentlichen: „Dann können wir damit in die nächste c’t und in Die Zeit hineinkommen und das BSI als Akteur positionieren.“ So ging die Warnung schließlich am 15. März raus.

Laut den Dokumenten sollte ursprünglich die Sicherheitsfirma G Data mit in der Erklärung auftauchen, da die ehemalige Frau des Kaspersky-Chefs Natalja Kaspersky 17 Prozent des Unternehmens hält. Diese stehen laut Spiegel aber offenbar zum Verkauf. Deswegen, und vermutlich, weil G Data in Bochum angesiedelt ist und vom BSI als besonders qualifizierter Dienstleister gehandelt wird, hat die Behörde den Namen wohl als „Gefallen“ aus der Warnung herausgehalten, schlussfolgert der Spiegel. (wid@ct.de)

BSI-Warnung und Recherche: ct.de/yu6a

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

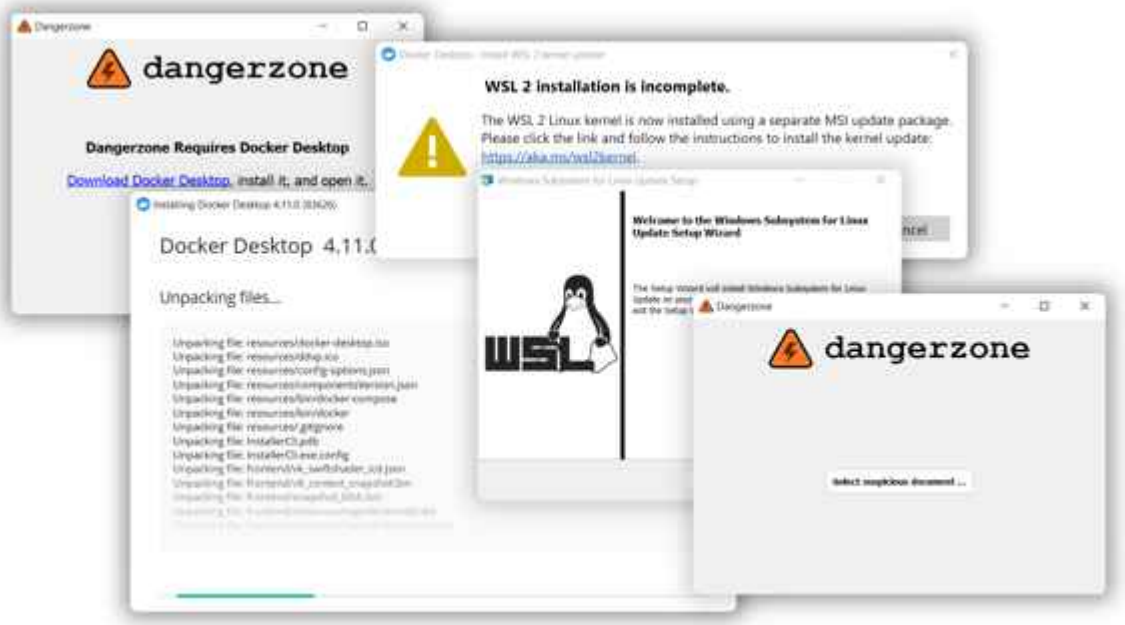
echte virtuelle Maschinen, stellen für Malware aber dennoch eine massive Hürde dar.

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).

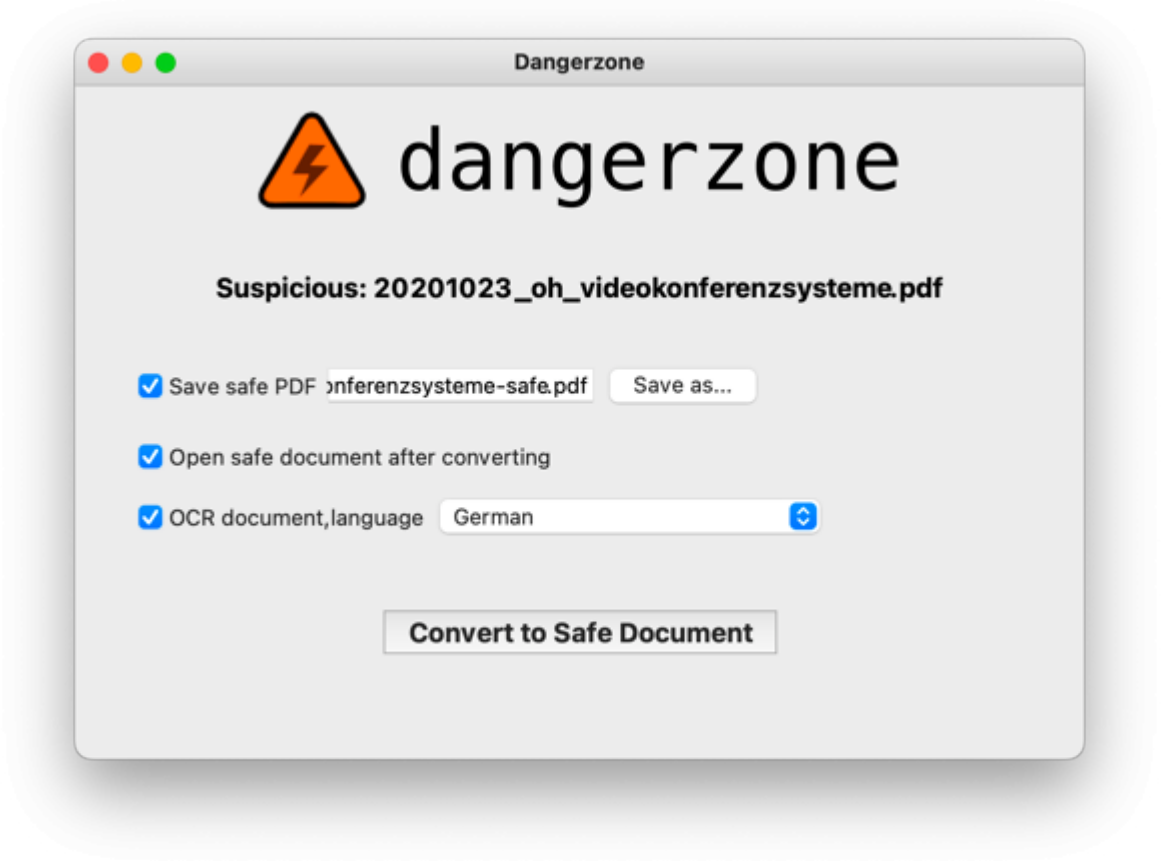
Leider unterstützt Dangerzone im Moment nur bei Debian aktuelle Versionen (11 und 12), bei Ubuntu und Fedora funktionieren von Haus aus nur etwas ältere Ausgaben (20.10, 21.04 und 21.10 beziehungsweise 33, 34 und 35). Auch bei anderen Distributionen sollten Sie sich nicht zu früh freuen: Beispielsweise 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

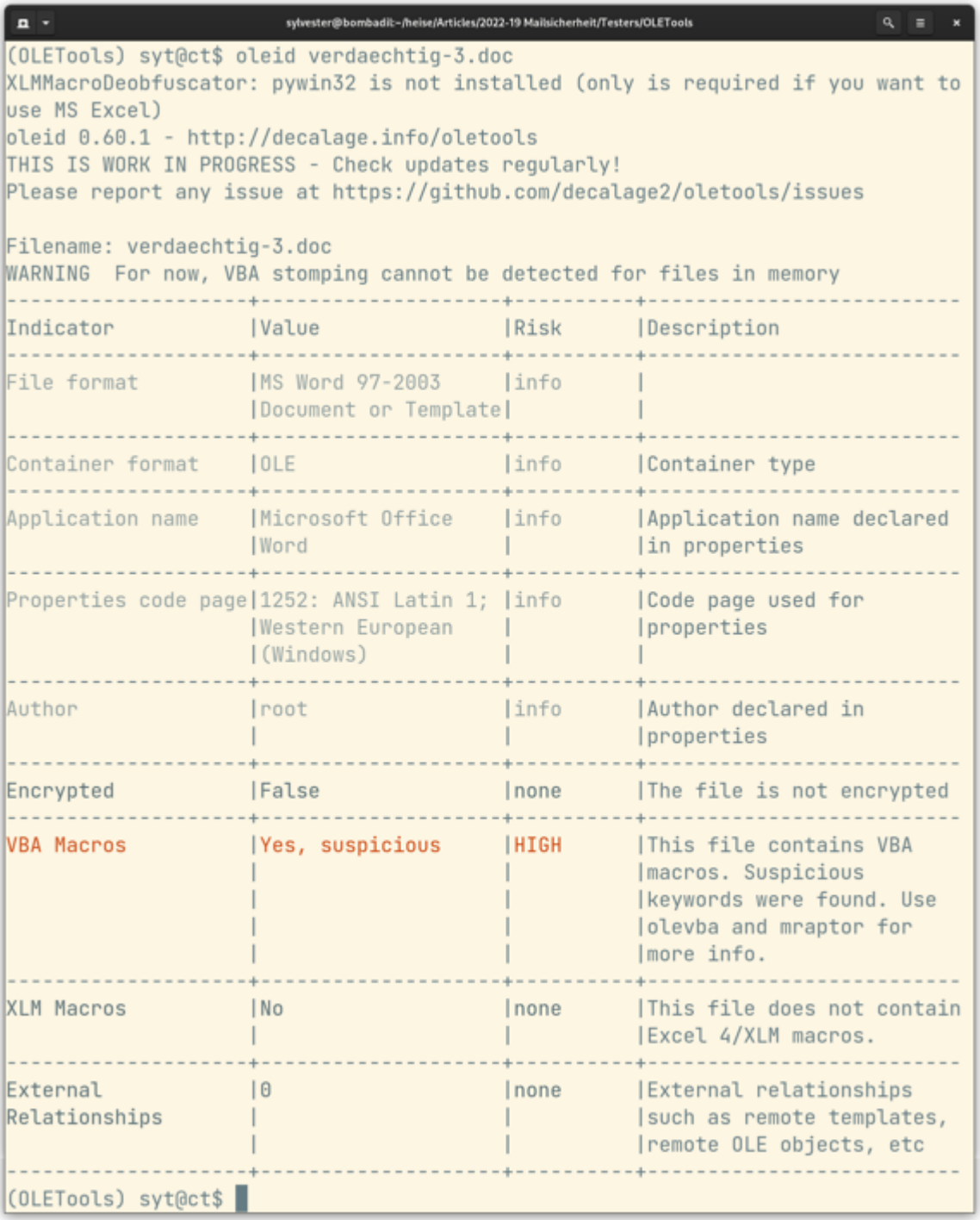
Werkzeuge in der Art von pdfid, aber nicht immer benötigen Sie dergleichen: Microsofts neuere Formate, die auf X enden (DOCX, XSLX, PPTX), sind im Grunde Zip-Archive, die lediglich einen speziellen Inhalt haben. Das hilft, falls Sie beispielsweise nur an den Bildern in einem Word-Dokument interessiert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

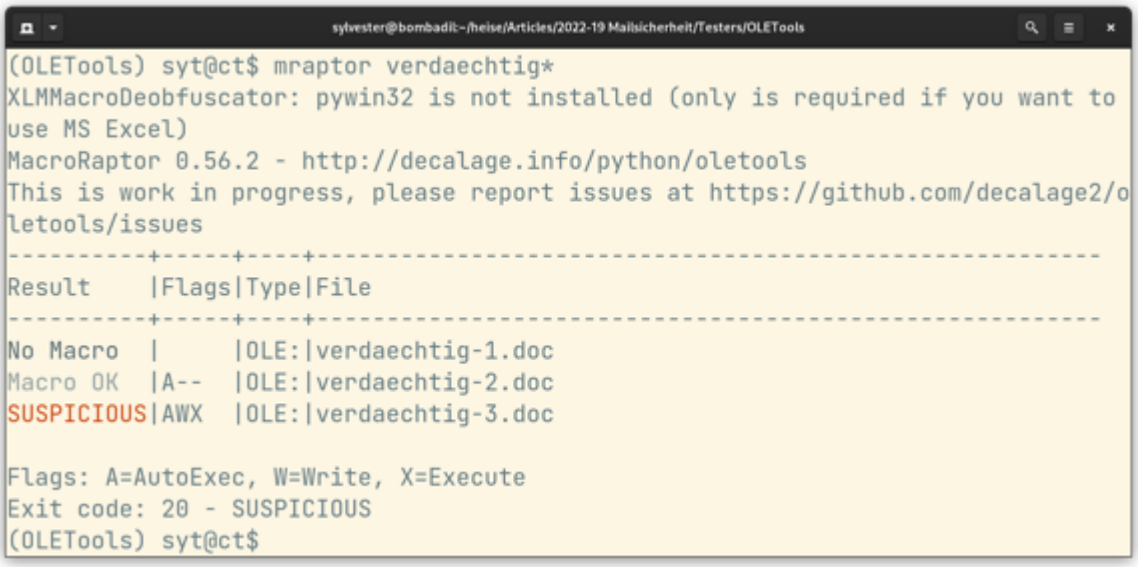


„VBA Macros: Yes, suspicious; Risk: HIGH“ meldet oleid und hat recht. Diese Datei ist tatsächlich höchst suspekt.
Ein Dokument mit einem höchst suspekten Makro, das versucht, eine Datei auf die Festplatte zu schreiben, bewertet oldid in Rot als „suspicious“ (verdächtig) und warnt in Großbuchstaben vor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

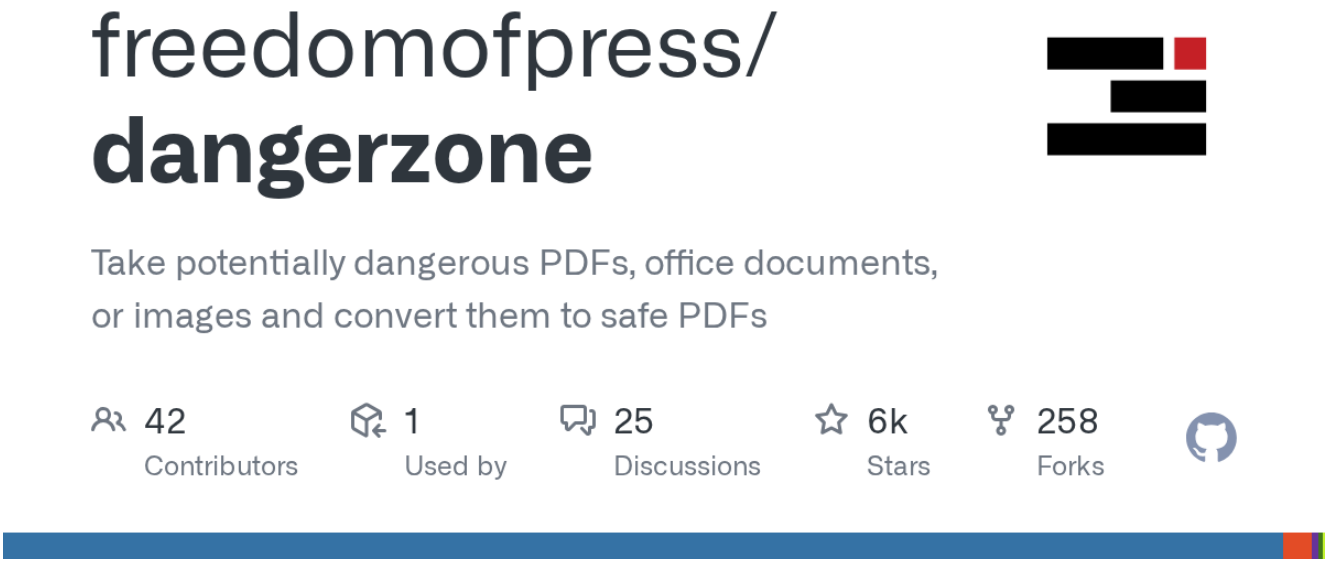
Auch ohne weitere Analyse müssen Sie keine Angst vor bösartigen Anhängen haben, wenn Sie die in diesem Artikel vorgestellten Werkzeuge einsetzen. Das Risiko, dass etwas den Filter von Dangerzone passiert, ist extrem gering. Übrigens sammeln sich unter Windows und macOS mit der Zeit immer mehr „Containers“ (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**

Phishing-E-Mails erkennen und abwehren

E-Mails durchleuchtet

Phishing-Mails erkennen und abwehren

Der gefährlichste Ort im Internet ist Ihr Posteingang: Hinter jeder Mail kann ein Angriff stecken. Und die Zeiten, in denen man Phishing auf den ersten Blick erkennen konnte, sind längst vorbei. Mit den folgenden Tipps sortieren Sie auch die kniffligen Fälle gekonnt aus.

Von Ronald Eikenberg

Die von Phishing-Mails ausgehende Gefahr wird gern unterschätzt, schließlich erkennt man die Fälschungen doch scheinbar schon aus zehn Meter Entfernung durch merkwürdige Absender wie „✩P.A.Y.P.A.L✩“, Betreffzeilen wie „Ihr Konto wurde begrenzt“ oder völlig schiefe Grammatik. Doch die Zeiten ändern sich: Solche tölpelhaften Mails gibt es zwar nach wie

vor, sie bleiben jedoch meist im Spamfilter hängen und die wahre Gefahr lauert woanders.

Was es in den Posteingang schafft, ist von höherer Qualität. Perfekte 1:1-Kopien von echten PayPal- oder Rechnungsmails sind dabei noch das geringere Übel. Richtig gefährlich wird es, wenn die Absender mit echten Daten arbeiten, die sie zum Beispiel aus Datenleaks ziehen oder bei Personen aus Ihrem Umfeld erbeuten. Letzteres ist besonders gefährlich, denn es ist durchaus möglich, dass Sie heute eine Phishing-Mail von einer Person erhalten, mit der Sie gestern tatsächlich kommuniziert haben.

Dieses sogenannte Dynamit-Phishing nahm durch Emotet Fahrt auf und ist weltweit etlichen Firmen, Behörden, Bildungseinrichtungen und vielen mehr zum Verhängnis geworden. Die Schäden gehen in die Milliarden. Die Einstellung „Bei mir gibt es eh nichts zu holen“ ist übrigens fatal, denn Online-Schurken haben es nicht nur auf DAX-Konzerne abgesehen, sondern auf jeden. Ihr Instagram-Account oder Ihr Netflix-Zugang bringt den Phishern im Darknet zwar nur ein paar Dollar ein, doch wer große Stückzahlen verkauft, macht trotzdem einen guten Schnitt.

Mit den folgenden Strategien und Tipps sind Sie dazu in der Lage, verdächtige Mails zu erkennen und die richtigen Entscheidungen zu treffen, um nicht in die Phishing-Falle zu tappen. Es geht mit den offensichtlichen Warnsignalen los, die jeder kennen sollte, und weiter damit, wie Sie anhand der Mail-Innereien den Versandweg rekonstruieren und mithilfe des Sender Policy Framework (SPF) gefälschte Absender aufdecken.

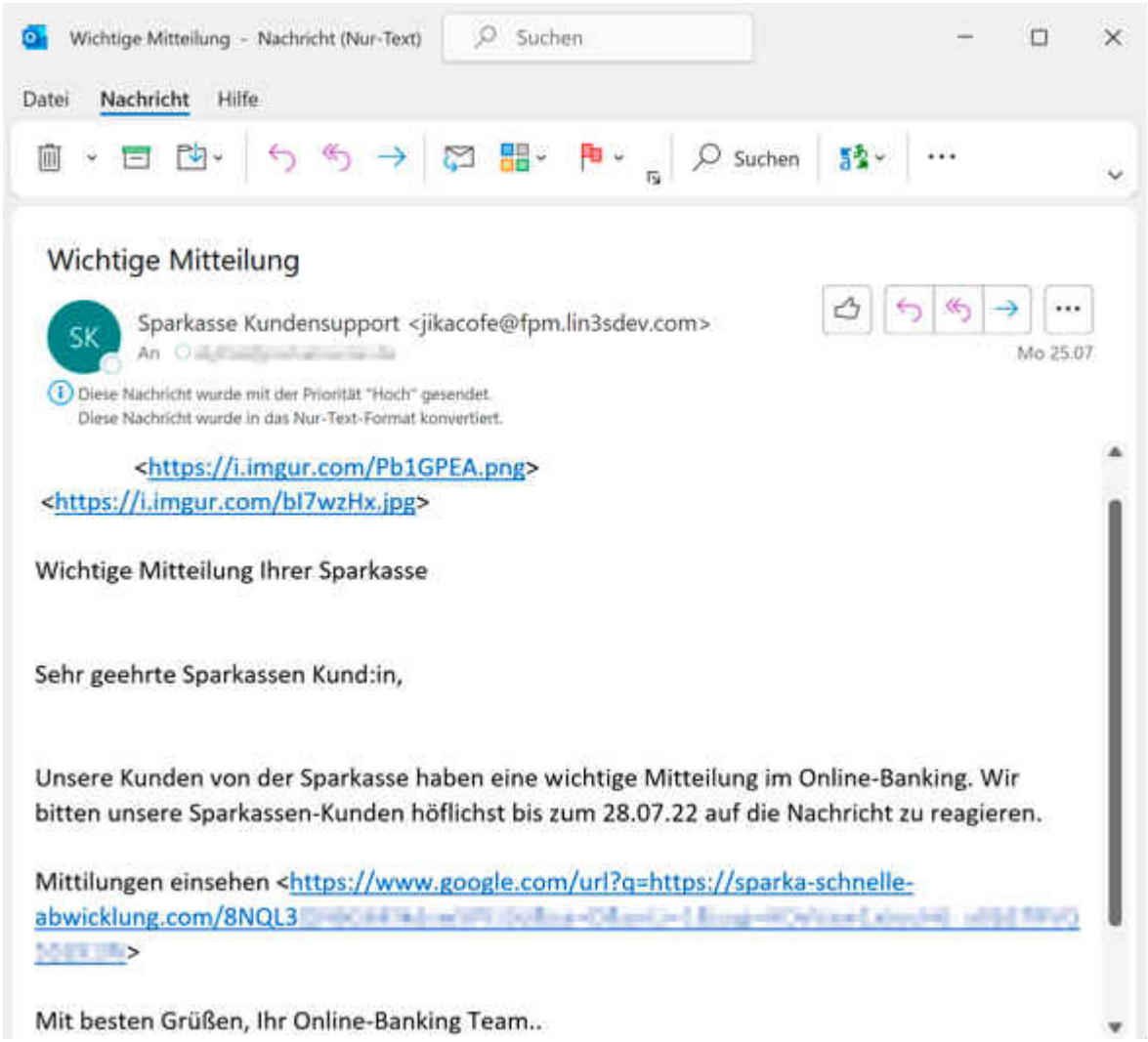
Gut vorbereitet

Um keine unnötigen Risiken einzugehen, sollten alle verfügbaren Software-Updates für Betriebssystem, Browser und Mailprogramm installiert sein, da Updates häufig Sicherheitslücken schließen. Das gilt auch für alle

Anwendungen, mit denen Sie Anhänge öffnen, allen voran Ihre Office-Suite und Ihr PDF-Viewer.

Stellen Sie Ihren Mailclient oder Webmail-Account am besten so ein, dass standardmäßig die Textversion einer Mail angezeigt wird, sofern möglich. Denn HTML-Mails können Sie leicht in die Irre führen, etwa durch ein offiziell anmutendes Äußeres oder gefälschte Links, die auf eine andere als die angezeigte URL verweisen. Im Textmodus sehen Sie das tatsächliche Linkziel auf den ersten Blick.

Seriöse HTML-Mails enthalten in der Regel eine Textversion mit demselben Inhalt, Ihnen entgeht also nichts. Falls Sie Thunderbird benutzen, klicken Sie für den Textmodus im Menü auf „Ansicht/Nachrichteninhalt/Reiner Text“, bei Outlook ist der Weg länger: „Datei/Optionen/Trust Center/Einstellungen für das Trust Center…/E-Mail-Sicherheit/Als Nur-Text lesen/Standardnachrichten im Nur-Text-Format lesen“.



Phishing entzaubert: Im Nur-Text-Modus wird sofort klar, dass an der angeblichen Sparkassen-Mail von Seite 17 etwas faul ist. Die Grafiken liegen beim Gratis-Bilderhoster Imgur, der Link „Mitteilungen einsehen“ nutzt eine Google-Umleitung auf sparka-schnelle-abwicklung.com.

Führt kein Weg an der HTML-Version vorbei, sollte Ihr Mailclient so eingestellt sein, dass er keine Inhalte aus externen Quellen lädt. Beim Abruf solcher Inhalte nimmt Ihr System direkten Kontakt mit dem Zielserver auf, wodurch der Absender erfährt, dass Sie die Mail geöffnet haben und Ihre Mailadresse tatsächlich existiert – es lohnt sich also, Sie mit weiteren Mails zu belästigen. Thunderbird und Gmail laden standardmäßig keine externen Inhalte, bei Outlook gibt es wenige Ausnahmen (etwa für bekannte Absender), die Sie im Trust Center unter „Automatischer Download“ konfigurieren können.

Plausibilitätscheck

Jetzt ist es Zeit für den obligatorischen Plausibilitätscheck: Kennen Sie den Absender? Erwarten Sie eine Mail von ihm? Ist sein Anliegen plausibel? Besteht auch nur der geringste Zweifel, sollten Sie weiter recherchieren, ehe Sie sich weiter auf die Mail einlassen und gar einen Link oder Anhang öffnen.

Stammt die Mail angeblich von einer Person, mit der Sie bereits in Kontakt standen – etwa Kollegen, Geschäftspartnern, Freunden oder Familie? Der einfachste Weg, für Klarheit zu sorgen, ist beim Absender nachzufragen, ob er die Mail tatsächlich verschickt hat. Nutzen Sie dazu keine Kontaktdaten aus der Mail (auch wenn sie auf den ersten Blick korrekt erscheinen), sondern eine Mailadresse oder Telefonnummer, über die Sie bereits in der Vergangenheit Kontakt hatten oder die von der legitimen Website des Absenders stammt.

Das Gleiche gilt für Zahlungsaufforderungen, Versandbestätigungen über nicht bestellte Ware, Anwaltsschreiben, Hinweise von Zahlungsdienstleistern und Banken sowie Mails, die Sie auffordern, sich auf einer Website einzuloggen. Recherchieren Sie die Kontaktdaten des angegebenen Absenders aus einer unabhängigen Quelle wie Google und fragen Sie nach. Wenn Sie einen Account beim angeblichen Absender haben, dann loggen Sie sich dort ein (wohlgemerkt nicht über einen Link aus der Mail) und sehen sie nach, ob sich auch dort die Mitteilung findet.

Es gehört zum guten Ton, dass Sie in Mails mit Ihrem Namen angesprochen werden, Unternehmen geben oft auch Ihre Kundennummer oder ähnliches mit an. Dies allein ist kein Beweis dafür, dass eine Mail unbedenklich ist, allerdings sollten Sie skeptisch werden, wenn ein an Sie gerichtete Mail keine persönliche Anrede enthält.

Auch der angegebene Absender kann eine Mail zwar be-, aber nicht entlasten: Bei E-Mails sind Absenderadresse und

Absendername frei wählbar, wie bei einer Postkarte. Sie können darüber also nicht zweifelsfrei feststellen, ob eine Mail echt ist. Nur die gegenteilige Feststellung ist möglich: Stammt die Mail von einer ungewöhnlichen Absenderadresse, dann ist ziemlich sicher etwas faul.

Bei Mails von Firmen und Behörden sollte die Absenderdomain zum Webauftritt passen, bei PayPal-Mails etwa paypal.de oder paypal.com. Offizielle Post werden Sie niemals von einer Freemail-Adresse (etwa @gmail.com oder @outlook.com) erhalten. Achten Sie bei der Absenderdomain penibel auf die Schreibweise, denn paypal.com ist eine andere Domain als paypa1.com oder paypal-kunden-support.com.

Wenn Sie sich unsicher sind, können Sie Absenderadresse zum Beispiel mit dem Reputationsdienst „Simple Email Reputation“ überprüfen (siehe ct.de/y2qp). Der Dienst liefert anhand zahlreicher Quellen wie Darknet-Leaks und Social-Media-Profilen eine Einschätzung, ob die Mailadresse vertrauenswürdig ist.

Der Webdienst „Simple Email Reputation“ schätzt ein, ob eine

Absenderadresse vertrauenswürdig ist. Dafür zapft er zahlreiche Datenquellen an.

Social Engineering

Phishing ist eine Social-Engineering-Attacke – die Angreifer versuchen Sie trickreich in die Falle zu locken. Bei Phishing-Mails werden Sie meist direkt oder indirekt aufgefordert, einen Anhang zu öffnen oder einen Link anzuklicken, doch die Fantasie der Online-Schurken kennt keine Grenzen. Bei der Chef-Masche (auch CEO-Fraud genannt), gibt sich der Absender als Ihr Chef aus und fordert Sie beispielsweise auf, eine dringende Überweisung auszuführen. Lassen Sie sich nicht davon einschüchtern.

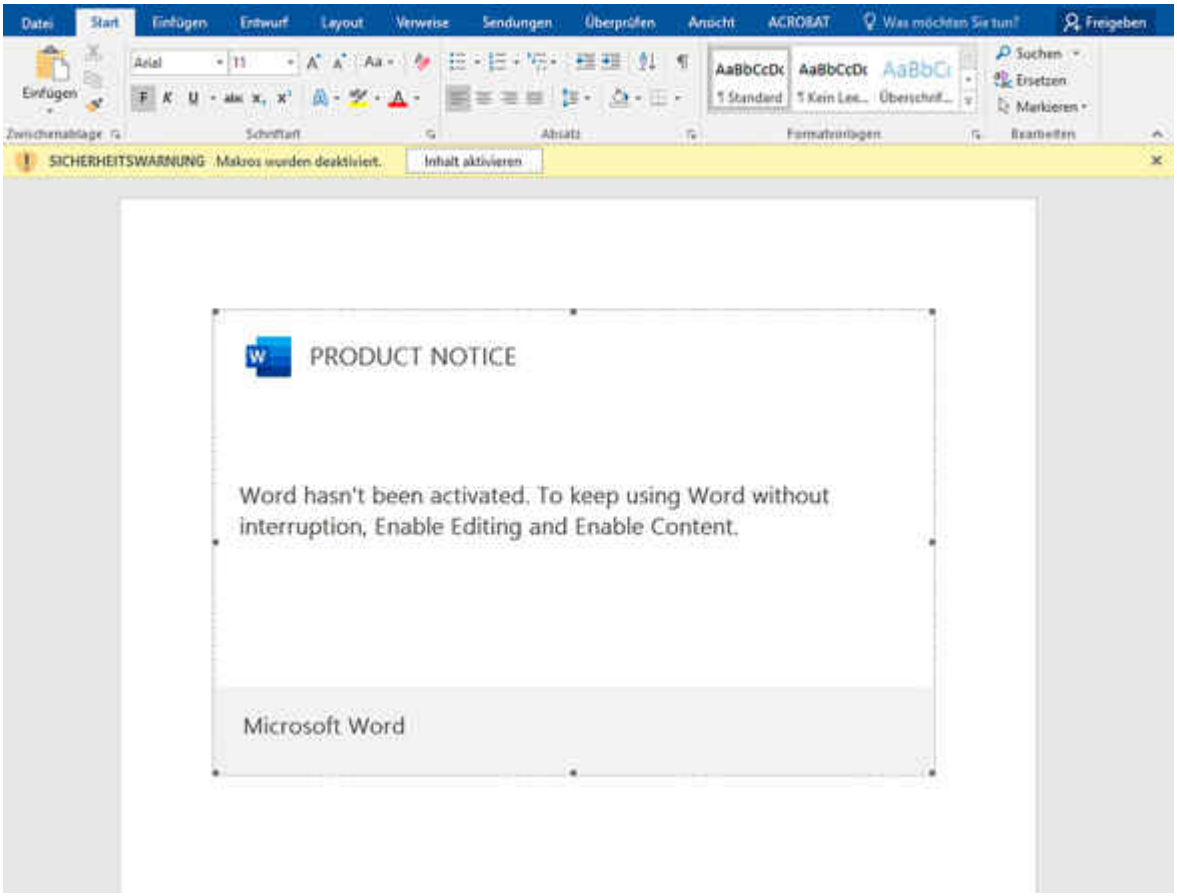
Gelegentlich verwickeln Sie die Betrüger auch in ein Gespräch, um zunächst eine Vertrauensbasis aufzubauen, ehe es ans Eingemachte geht. Geht es ums Geld, sollten den angegebenen Zahlungsempfänger genau überprüfen. Passen die angegebenen Bankdaten tatsächlich zu dem Unternehmen, das die Rechnung ausgestellt hat? Ist eine Bitcoin-Adresse oder eine ähnliche Krypto-Adresse im Spiel, handelt es sich mit hoher Wahrscheinlichkeit um einen Betrugsversuch.

Office ist Angreifers Liebling

E-Mail-Anhänge sind gefährlich – manche Dateiformate sind jedoch gefährlicher als andere. Angreifer haben es vor allem auf Microsoft Office abgesehen. Der Angriffscode steckt dann meist in Office-Makros, die den eigentlichen Schädling aus dem Internet nachladen und ausführen. Sie sollten bei Office-Dokumenten die gleiche Vorsicht walten lassen wie bei ausführbaren Dateien und sie erst mal nur mit der Kneifzange anfassen.

Sie erkennen Phishing-Dokumente zumeist daran, dass Sie nach dem Öffnen durch einen Text im Dokument aufgefordert werden, auf die gelbe Benachrichtigungsleiste oberhalb des Dokuments

zu klicken, um die Ausführung von Makros zu genehmigen. Achtung: Der Text und das Dokument selbst werden oft trickreich gestaltet, sodass der Inhalt nicht nach Word-Seite oder Excel-Tabelle aussieht, sondern wie ein offizieller Programmdialog. Konkret werden Sie gebeten, in der Leiste auf „Bearbeitung aktivieren“ und „Inhalt aktivieren“ zu klicken. Kommen Sie dieser Aufforderung auf keinen Fall nach.



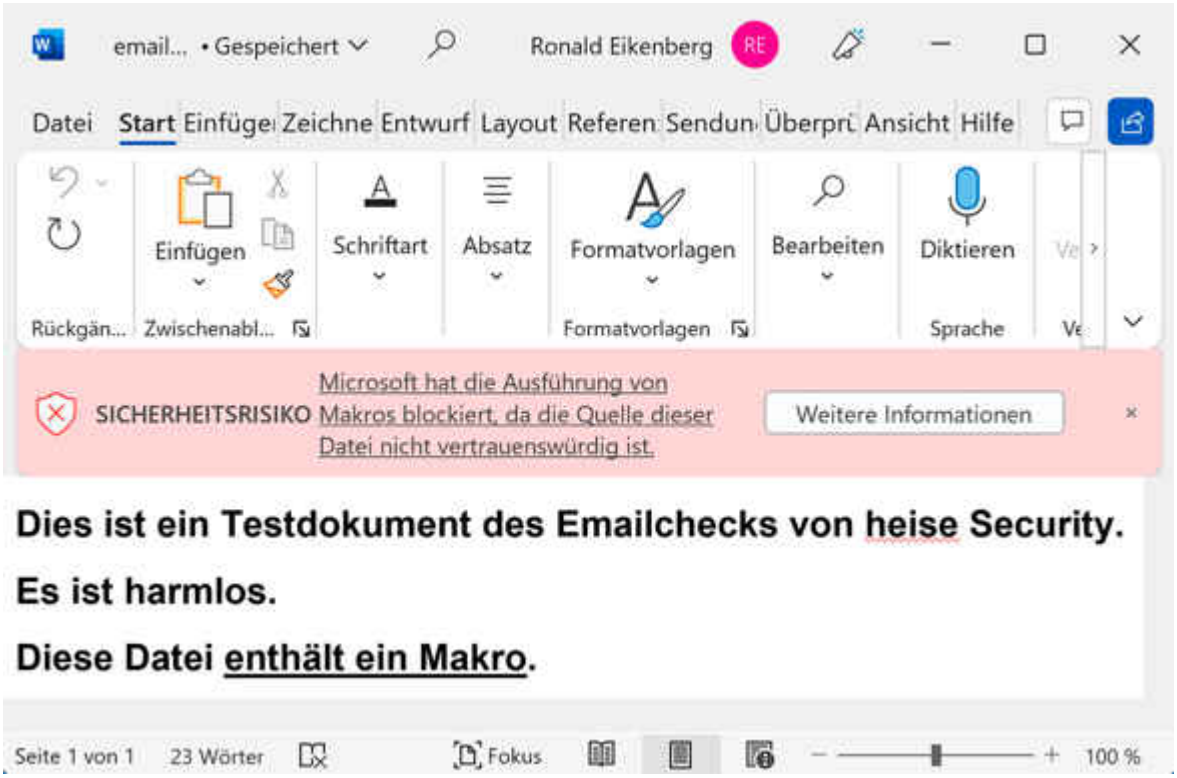
Phishing-Dokumente fordern häufig mit fadenscheinigen Argumenten dazu auf, auf die gelbe Leiste von Microsoft Office zu klicken. Dadurch wird das mitgelieferte Schadcode-Makro ausgeführt.
Kontrollieren Sie die Makro-Einstellungen in Ihrem Office, um sicherzustellen, dass Makros nicht automatisch ausgeführt werden. Klicken Sie hierzu auf „Datei/Optionen/Trust Center/Einstellungen für das Trust Center …“. Standardmäßig ist dort „Alle Makros mit Benachrichtigung deaktivieren“ eingestellt. Diese Einstellung begünstigt Phishing, weil man die Sperre über die gelbe Benachrichtigung umgehen kann.

Wenn Sie ohnehin nicht mit Makros arbeiten, schalten Sie diese

am besten mit „Alle Makros ohne Benachrichtigung deaktivieren“ aus. Falls Makros in Ihrer Firma eingesetzt werden, sollten diese digital signiert werden, damit Office die Echtheit überprüfen kann. Dann können Sie in Office „Alle Makros, außer digital signierte Makros deaktivieren“ einstellen.

Um zu überprüfen, wie Ihr Office auf Makros reagiert, können Sie sich über den Emailcheck von heise Security eine Testmail mit einer ungefährlichen Word-Datei zusenden lassen (siehe ct.de/y2qp). Wird der darin enthaltene Makro-Code ausgeführt, erscheint der Hinweis „Achtung! Makro wurde ausgeführt!“.

Aktuell ist Microsoft dabei, die Zügel weiter anzuziehen und Makros in Office-Dokumenten, die aus dem Internet stammen, standardmäßig zu blockieren. In solchen Fällen erscheint statt der gelben Leiste eine rote Warnung: „SICHERHEITSRISIKO: Microsoft hat die Ausführung von Makros blockiert, da die Quelle dieser Datei nicht vertrauenswürdig ist.“



Office blockiert neuerdings Makros in Dokumenten aus Online-Quellen mit rotem Alarm. Der Schutz ist allerdings lückenhaft. Ein echtes Hindernis ist dies jedoch nicht, man kann die Blockade leicht umgehen, indem man in den Dateieigenschaften

bei „Sicherheit:“ das Häkchen „Zulassen“ setzt. Es ist davon auszugehen, dass sich diese Handlungsanweisung in Kürze auch in den Phishing-Dokumenten wiederfinden wird. Zudem ist der Schutz keineswegs zuverlässig: Die Entscheidung, ob er aktiv wird, trifft Office anhand der Dateimarkierung Mark-of-the-Web (MOTW), die Dateien aus dem Internet kennzeichnet.

Das MOTW steckt in den Alternate Data Streams (ADS) einer Datei, die normalerweise unsichtbar sind. Wenn Sie einen Blick riskieren möchten, können Sie die ADS in der Windows-Eingabeaufforderung mit dir dokument.doc /R auflisten und das MOTW mit notepad dokument.doc:Zone.Identifier:$DATA anschauen. „ZoneId=3“ kennzeichnet Dateien aus dem Internet.

Die Markierung muss das Programm setzen, das die Datei heruntergeladen hat. Doch daran hält sich längst nicht jedes: Öffnet man ein Word-Dokument über Outlook, erscheint die oben zitierte Warnung. Öffnet man die gleiche Datei über Thunderbird, fehlt das MOTW und Word zeigt lediglich die übliche gelbe Leiste mit „Makros wurden deaktiviert“. Ein Klick auf „Inhalt aktivieren“ rechts daneben reicht aus, um den Code auszuführen.

Ist einer Mail ein Containerformat wie ZIP oder ISO angehängt, ist zwar der Container mit der MOTW markiert, häufig jedoch nicht die daraus geöffnete Office-Datei. Das wissen auch die Cyber-Banden: Laut der Security-Firma Proofpoint verschicken die Phisher verstärkt Container anstelle von bloßen Office-Dokumenten, um die Schutzvorkehrung zu umgehen.

Gute Formate, schlechte Formate

Die Liste der Dateiformate, die gefährlichen Schadcode ausführen können, ist sehr lang. Schon bei den Microsoft-Office-Formaten gibt es mindestens 17, die Makros mitschleppen können, darunter die alten Binärformate DOC, PPT und XLS. Microsoft Excel kann sogar das Textformat CSV zum Verhängnis werden.

Darüber hinaus gibt es unzählige weitere Dateiformate, die Schaden unter Windows anrichten können. Das weiß auch Microsoft, denn Outlook blockiert standardmäßig den Zugriff auf über einhundert Dateitypen von ADE bis XNK. Noch nie gehört? Wir auch nicht. Es gilt: Was man nicht kennt, öffnet man nicht.

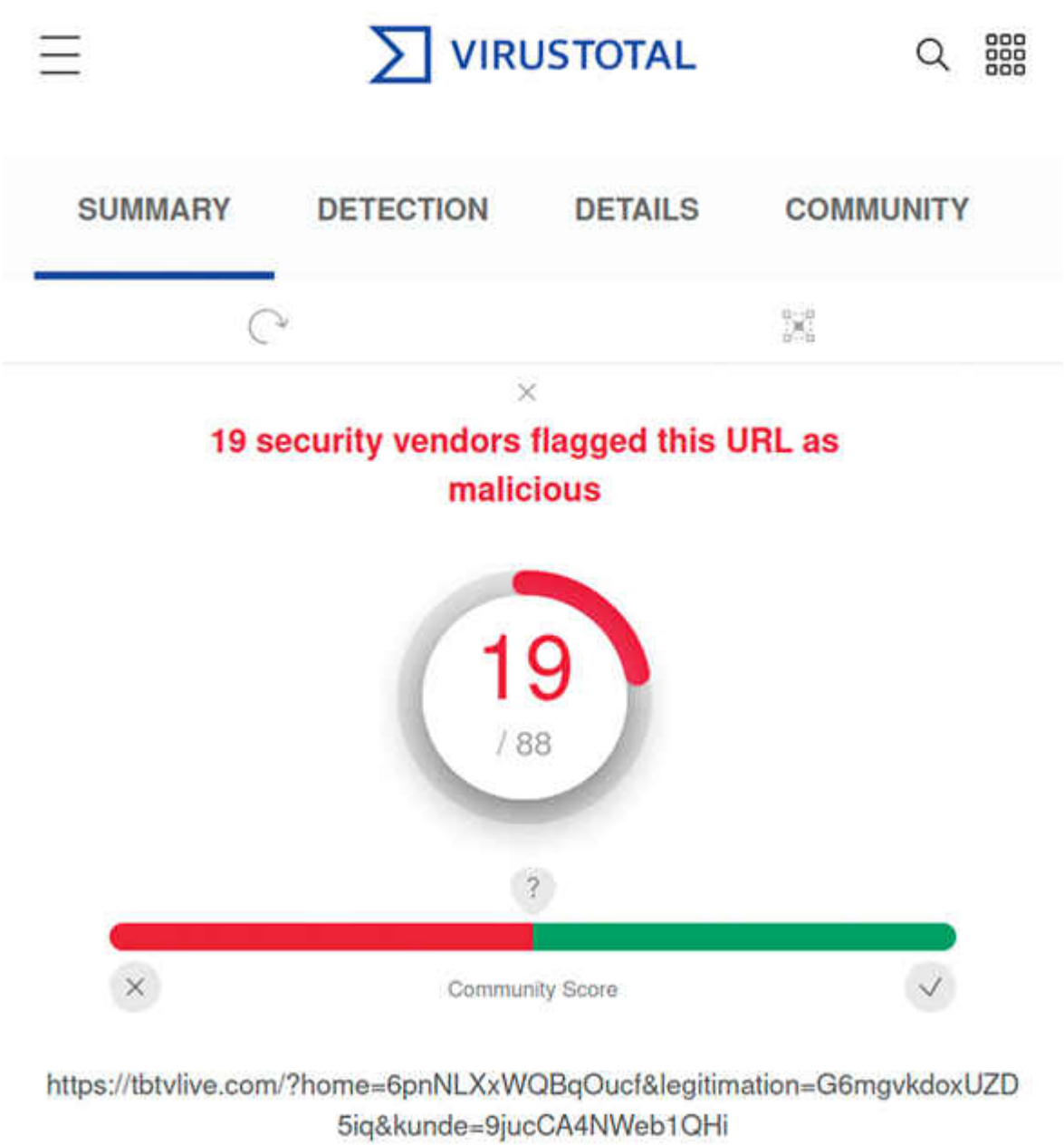
Höchst verdächtig sind verschlüsselte Dateien, wenn das dazugehörige Passwort in der Mail steht. Es handelt sich um einen alten Trick zur Verbreitung von Malware, denn Virenfilter können den Inhalt verschlüsselter Dateien nicht überprüfen. Selbst HTML-Dateien werden für Angriffe missbraucht, in solchen Fällen steckt die Phishing-Seite direkt im Anhang.

Wichtig zu wissen ist, dass die Office-Formate DOCX, PPTX und XLSX keine Makros enthalten können, von solchen Dokumenten geht also eine geringere Gefahr aus. Eine Unbedenklichkeitserklärung ist das jedoch nicht, denn selbst ohne Makros sind Angriffe möglich, zum Beispiel durch Sicherheitslücken in Office. Um das Risiko zu verringern, können Sie Office-Dokumente mit weniger verbreiteter Software wie LibreOffice öffnen. Die ist nicht per se sicherer, aber ein weniger wahrscheinliches Ziel für Angreifer.

PDF-Dateien sind ebenfalls nur mit Einschränkungen zu genießen, denn sie können JavaScript und eingebettete Dateien mit Schadcode enthalten. Öffnen Sie verdächtige PDFs besser nicht mit dem funktionsreichen Adobe Acrobat Reader, sondern mit dem Browser. Die PDF-Viewer der Browser unterstützen weniger PDF-Funktionen und bieten so eine geringere Angriffsfläche. Außerdem laufen sie eben im Browser und der ist darauf ausgelegt, mit nicht vertrauenswürdigen Inhalten aus dem Internet konfrontiert zu werden. Am besten untersuchen Sie die Office- und PDF-Dateien vor dem Öffnen, ob sie ausführbaren Code oder eingebettete Dateien enthalten. Wie das funktioniert, erfahren Sie ab Seite 28.

In seltenen Fällen, zum Beispiel im Rahmen staatlich initiierter Cyber-Angriffe, werden sogenannte Zero-Day-Lücken ausgenutzt, für die es noch keinen Patch gibt. Beispielsweise hat Microsoft im Mai eine hochgefährliche PDF-Datei entdeckt, die zunächst eine zum damaligen Zeitpunkt ungepatchte Lücke im Adobe Reader ausgenutzt haben soll, um anschließend über eine weitere Zero-Day-Lücke Windows zu attackieren. Die Datei soll zur Verbreitung der Spionagesoftware Subzero eines Wiener Herstellers gedient haben. Vor Zero-Day-Attacken können Sie sich kaum schützen, sie sind allerdings auch recht selten und richten sich eher gegen spezifische Ziele, nicht gegen die breite Masse der Anwender.

Insbesondere unter Windows sollte ein Virenschutz aktiv sein, der neue Dateien automatisch überprüft. Der vorinstallierte Windows Defender leistet gute Dienste. Ein Virenscanner erhöht die Chance, dass eine schädliche Datei frühzeitig auffliegt. Wird der Virenschutz nicht fündig, ist das jedoch keine Garantie dafür, dass eine Datei sauber ist. Sehen Sie davon ab, Dateianhänge, die persönliche oder vertrauliche Daten enthalten könnten, bei kostenlosen Online-Analysediensten wie VirusTotal oder Hybrid Analysis hochzuladen. Solche Dienste teilen die Dateien mit Dritten, etwa zu Forschungszwecken. Sie riskieren durch den Upload einen DSGVO-Verstoß.



Mailanhänge bei Online-Analysediensten wie VirusTotal hochzuladen ist keine gute Idee, da die Dienste die Dateien mit Dritten teilen. Verdächtige URLs können Sie den Diensten aber anvertrauen.

Lassen Sie sich nicht linken

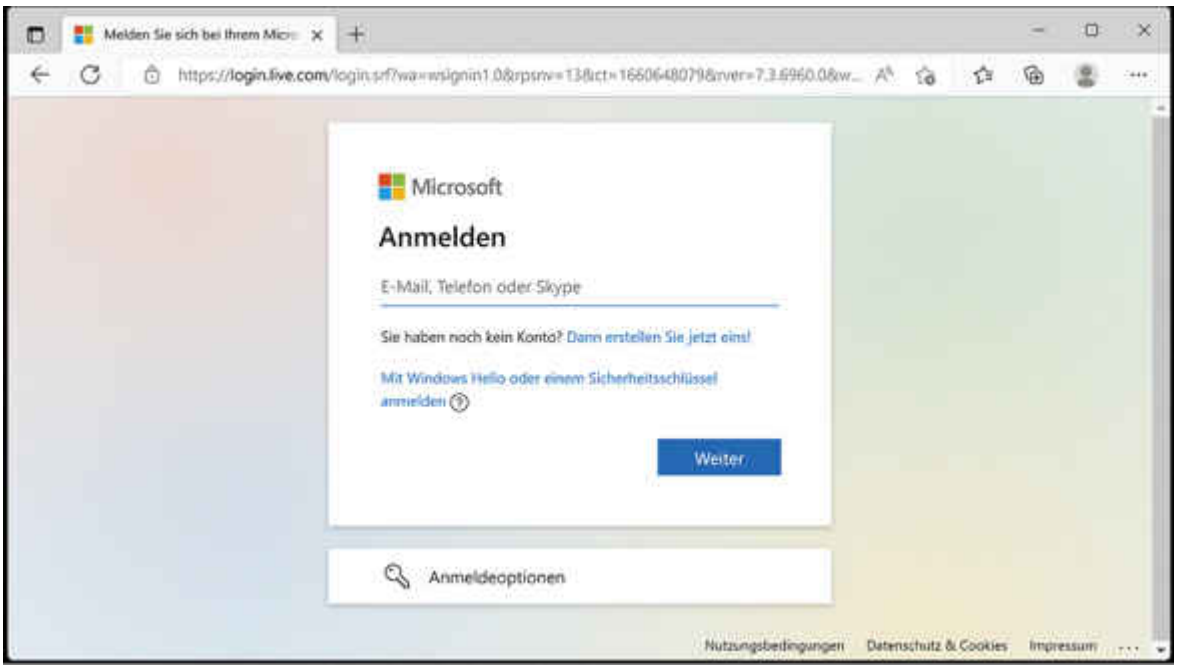
Nicht nur Dateianhänge können gefährlich sein, sondern auch Links. Stellen Sie wie oben beschrieben den Nur-Text-Modus im Mail-Client ein, damit man Ihnen keine manipulierten Links unterjubeln kann, deren Ziel von der angezeigten URL abweicht. Achten Sie außerdem darauf, dass die Zieladresse mit https:// beginnt. An diesem Präfix erkennen Sie Websites, die nach

Stand der Technik transportverschlüsselt (TLS/SSL) übertragen werden. Allerdings ist HTTPS kein Indikator dafür, dass sie der Website vertrauen können, da auch auch die meisten Phishing-Websites über HTTPS ausgeliefert werden.

Achten Sie penibel auf die Schreibweise der URL. Ein falscher Buchstabe, ein „I“ (großes „i“) anstelle eines „l“ (kleines „L“), reicht aus, um Sie auf eine völlig andere Website zu lotsen. Phisher verlängern legitime Domains auch gern durch unauffällige Zusätze, etwa „sparkasse-onlinebanking.de“ statt „sparkasse.de“. Steuern Sie im Zweifel immer die Ihnen bekannte, echte Adresse einer Website an, zum Beispiel über Ihre Booksmarks im Browser.

Falls Sie sich schon vor dem Besuch eines Links sicher sind, dass etwas faul ist, sollte Sie davon absehen, die verlinkte Website aus Neugier anzusteuern – nicht nur, weil dort etwa Malware auf Lücken in Ihrem Browser spitzen kann: Die Links sind häufig mit der Empfängeradresse verknüpft. Sie bestätigen Ihre Mailadresse durch das Aufrufen des Links. Meiden Sie auch demselben Grund auch Abmelden-Links (Unsubscribe) in Spam-Mails.

Zur Analyse verdächtiger Links können Sie verschiedene Online-Dienste nutzen: Browserling öffnet URLs in einer virtuellen Umgebung mit einem Browser Ihrer Wahl, VirusTotal befragt nach der Eingabe eines Links über 80 Security-Dienste und urlscan.io trägt diverse Informationen über eine Website zusammen, ehe ein Urteil darüber gefällt wird, ob sie Böses im Schilde führt (siehe ct.de/y2qp).



Die Single-Sign-on-Seite von Microsoft bauen Phisher besonders oft nach, weil sie die Türen vieler Unternehmen öffnet.

Zwei Faktoren, null Hacks

Zum Schutz vor Phishing zählt auch, auf den Ernstfall vorbereitet zu sein: Fällt man in der Hektik des Alltags doch mal auf eine gut gemachte Phishing-Mail rein, sollte der Schaden so gering wie nur irgendwie möglich sein. Aktivieren Sie bei allen wichtigen Diensten die Zwei-Faktor-Authentifizierung [1]. Dann ist zum Einloggen neben den Zugangsdaten ein weiterer Faktor nötig – beispielsweise ein Einmalpasswort in Form eines kurzzeitig gültigen Zahlencodes, den Sie mit einer Authenticator-App auf Ihrem Smartphone generieren.

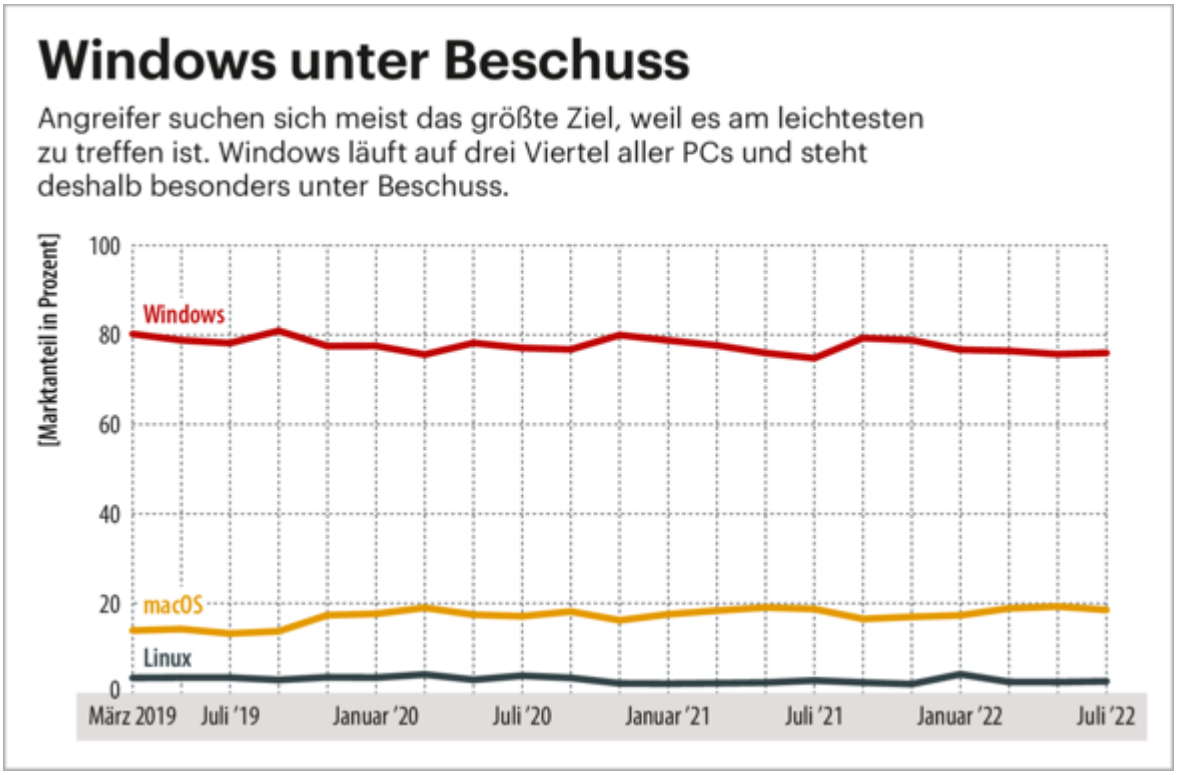
Haben Sie Ihre Zugangsdaten versehentlich einer Phishing-Website anvertraut, schauen die Cyber-Ganoven dann trotzdem in die Röhre, da sie sich ohne den zweiten Faktor nicht einloggen können. Gefährlich wird es allerdings, wenn Sie nicht nur Ihre Zugangsdaten, sondern auch das Einmalpasswort in die Phishingsite tippen. Für einen kurzen Moment ist dann ein Fremdzugriff möglich – Zeit genug, um automatisiert ein Session-Cookie vom Dienst abzurufen und Ihren Account damit dauerhaft zu übernehmen. Laut der Sicherheitsfirma Zscaler

richten sich solche Man-in-the-Middle-Angriffe auf den zweiten Faktor aktuell vor allem gegen Unternehmen, die Google- und Microsoft-Dienste einsetzen.

Davor schützt Sie der FIDO2-Standard, bei dem ein Sicherheitschip in Ihrem Rechner oder Smartphone den zweiten Faktor stellt. Alternativ können Sie auch einen USB-Sicherheitsschlüssel nutzen. Bei FIDO2 fließt automatisch die Domain der Website in die Berechnung des zweiten Faktors ein. Loggen Sie sich versehentlich auf der imaginären Phishing-Website paypa1.com mit FIDO2 ein, können die Online-Schurken die erbeuteten Daten deshalb nicht nutzen, um auf Ihr Konto bei paypal.com zuzugreifen.

Darüber hinaus gilt der alte, aber wichtige Tipp: Nutzen Sie möglichst für jeden Dienst ein anderes Passwort. So stellen Sie sicher, dass sich ein Angreifer mit erbeuteten Zugangsdaten nicht auch bei beliebig vielen weiteren Diensten einloggen kann. Die ganzen Passwörter müssen Sie sich weder merken noch ausdenken – ein Passwortmanager wie Bitwarden oder KeePass nimmt Ihnen die ganze Arbeit ab [2].

Auch das Thema Backups sollten Sie bei der Vorsorge für den Ernstfall nicht vernachlässigen. Cyber-Ganoven haben es auf Ihre Daten abgesehen und verschlüsseln diese, um von Ihnen anschließend ein Lösegeld zu erpressen. Damit sich in einem solchen Fall der Schaden in Grenzen hält, müssen Sie regelmäßig Backups Ihrer wichtigen Daten erstellen – insbesondere, wenn es um kritische Unternehmensdaten geht, ohne die der Geschäftsbetrieb nicht möglich ist.



Quelle: StatCounter

Risiko Windows

Wenn Sie mit Windows arbeiten, dann ist die von Phishing-Mails ausgehende Gefahr am größten: Angehängter Schadcode ist fast immer auf Windows abgestimmt. Das liegt nicht daran, dass Windows besonders unsicher ist, sondern vor allem an der enormen Verbreitung. Hierzulande läuft das Microsoft-Betriebssystem Statistiken zufolge auf rund 75 Prozent aller PCs, in Unternehmen dürfte der Anteil noch größer sein. Auf Platz 2 liegt macOS mit fast 20 Prozent.

Angreifer suchen sich meist das größte Ziel – also Windows, gefolgt von macOS. Je weniger verbreitet Ihr Betriebssystem ist, desto geringer ist die Wahrscheinlichkeit eines erfolgreichen Angriffs. Wenn Sie nicht auf Windows-Software angewiesen sind und ohnehin hauptsächlich im Browser arbeiten, lohnt es sich, einen Wechsel auf Linux oder Chrome OS in Betracht zu ziehen.

Bei den Mobilbetriebssystemen steht vor allem Android unter Beschuss, da man hier beliebige Apps als APK-Datei

installieren kann – ganz ohne den Store und die damit verbundenen Sicherheitsauflagen. Werden Sie unter fadenscheinigen Gründen aufgefordert, eine APK-Datei zu installieren, zum Beispiel ein vermeintliches Sicherheits-Update fürs Online-Banking, dann versucht ihnen jemand mit hoher Wahrscheinlichkeit einen Trojaner unterzujubeln. Bei iOS ist das Trojanerrisiko geringer, weil eine Infektion aufwendiger ist und etwa das Ausnutzen einer Sicherheitslücke erfordert.

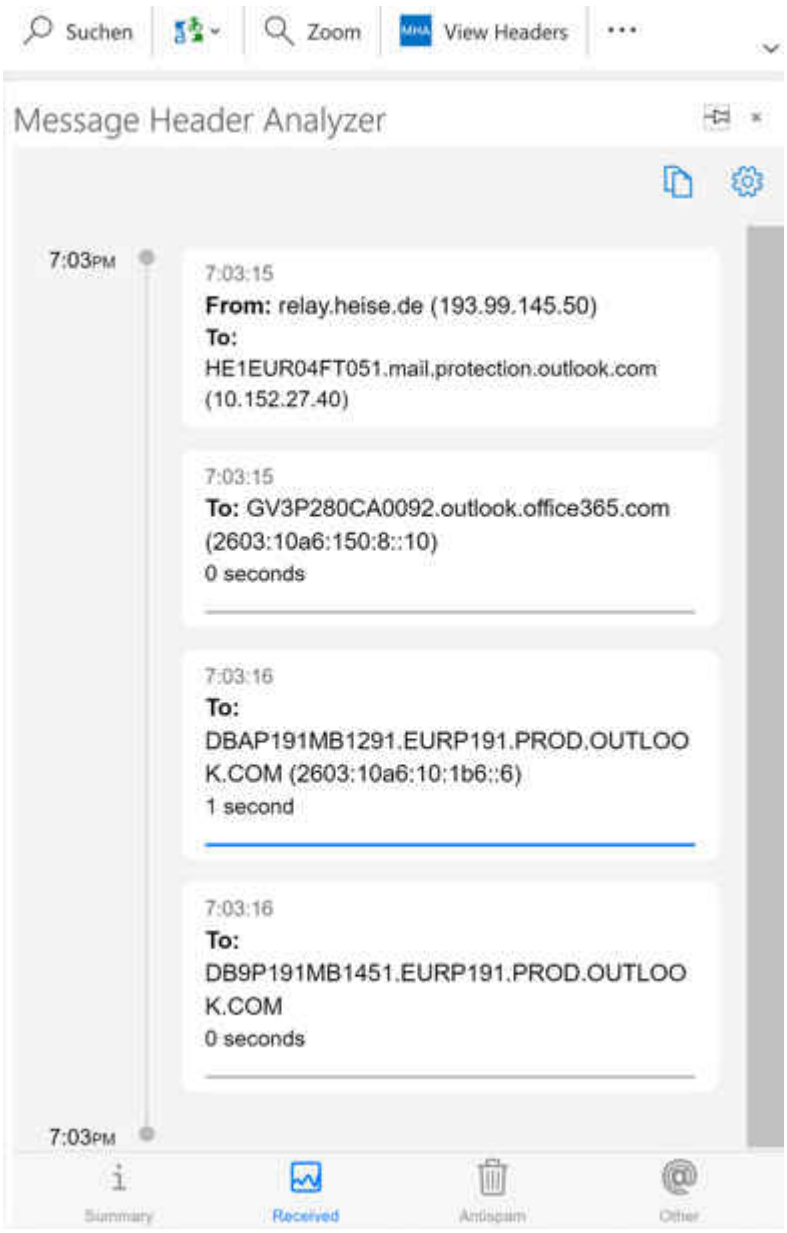
Achten Sie auch auf verdächtige Nachrichten aus sämtlichen Kanälen: Nicht nur Mails, auch WhatsApp-Nachrichten, SMS, Social Networks wie Facebook und Instagram, Anrufe und so weiter werden für Phishing missbraucht. Haben die Angreifer Kontaktdaten kopiert, kommt die Phishing-Nachricht womöglich sogar von einem Ihrer Freunde.

Herz und Nieren

Mit den oben beschrieben Maßnahmen sollten Sie die meisten Phishing-Fälle klären können, die größten Gefahren sind gebannt. Wenn Sie den Dingen gerne auf den Grund gehen, dann sollten Sie sich den Quelltext der verdächtigen Mail anzeigen lassen. Interessant ist vor allem der Header-Bereich oberhalb der eigentlichen Nachricht, denn hier gibt es viel zu entdecken; darunter der detaillierte Übertragungsbericht mit Informationen über das Mail-Relay, das die Mail eingeliefert hat.

Thunderbird-Nutzer finden den Quelltext einer gerade geöffneten Mail unter „Mehr/Quelltext anzeigen“. Wenn Sie Outlook nutzen, können Sie den Mail-Header wie folgt einsehen: Klicken Sie in der Nachrichtenliste doppelt auf eine Mail, um sie in einem eigenen Fenster zu öffnen, und anschließend auf „Datei/Eigenschaften“. Auch Webmailer bieten diese Funktion meist, bei Gmail klicken Sie nach dem Öffnen einer Mail unterhalb des Betreffs auf den Knopf mit den drei Punkten und „Original anzeigen“.

Welchen Weg die Mail genommen hat, verraten Ihnen die mit „Received:“ beginnenden Header-Zeilen von der untersten nach oben. Entscheidend ist der Übergabepunkt zum Eingangsserver Ihres Mail-Anbieters, bei einer Mail von rei@ct.de an eine Gmail-Adresse etwa: „Received: from relay.heise.de (relay.heise.de. [2a00:e68:14:800::19:19]) by mx.google.com […]“.



Der Mail Header Analyzer zeichnet den Versandweg einer Mail nach und zeigt nützliche Informationen aus dem Mail-Header an. Das Tool läuft im Browser und als Outlook-Add-In.

Um den Versandweg nachzuvollziehen, sind Analyse-Tools hilfreich, die automatisch die relevanten Zeilen im Mail-Code finden und in die richtige Reihenfolge stellen. Empfehlenswert

ist der „Message Header Analyzer“ des Microsoft-Mitarbeiters Stephen Griffin (siehe ct.de/y2qp), da das Tool Mails lokal im Browser auswertet. Outlook-Nutzer können es als Add-In ins Mailprogramm einklinken.

Die Mail wurde im obigen Beispiel vom Host relay.heise.de mit der IPv6-Adresse 2a00:e68:14:800::19:19 bei Google abgeliefert. Aber ist dieser Host tatsächlich für den angegebenen Absender rei@ct.de zuständig? Das können Sie im DNS-Eintrag der Absenderdomain nachschlagen. Die für die Domain zuständigen Mailserver sind dort in den sogenannten MX-Records vermerkt. Die MX-Records können Sie zum Beispiel über den Onlinedienst MXToolbox abfragen (siehe ct.de/y2qp).

Nach der Eingabe von ct.de listet der Dienst unter anderem auch relay.heise.de auf und ermittelt dazu die IP-Adresse, die der bereits bekannten aus dem Mail-Header entspricht – es passt also alles zusammen. Wenn Sie in der Zeile auf „Blacklist Check“ klicken, erfahren Sie auch gleich, ob der Mailserver auf Antispam-Blacklists steht.

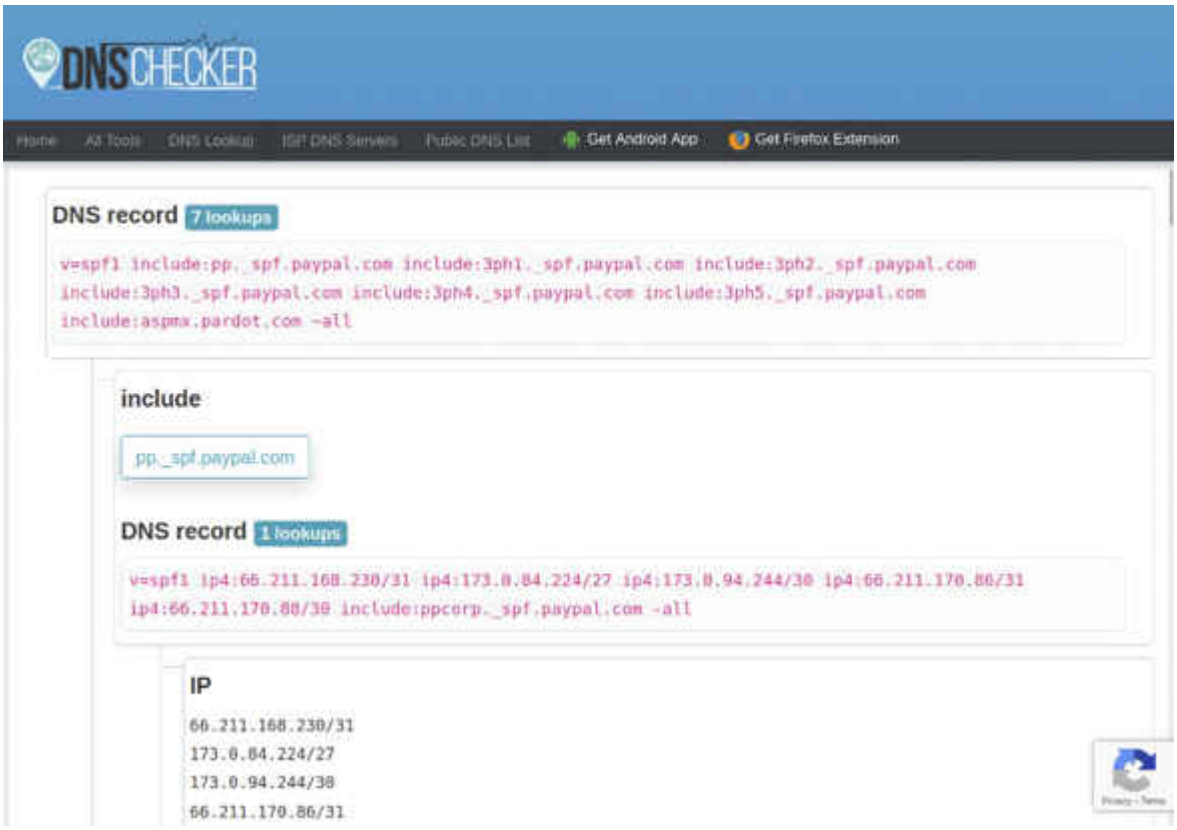
Anti-Spoofing-Check

Gespoofte Absender, also Absender mit gefälschter Mailadresse, stellen mittlerweile kein allzu großes Problem mehr dar. Das hat einen einfachen Grund: Solche Phishing-Mails kommen mit hoher Wahrscheinlichkeit nicht an. Das ist unter anderem dem Anti-Spoofing-Verfahren „Sender Policy Framework“ (SPF) zu verdanken. Damit können Admins im DNS-Eintrag ihrer Domains hinterlegen, von welchen IP-Adressen die Domains als Absender genutzt werden dürfen.

Der Empfangsserver kann beim Eintreffen einer Mail diese Informationen einfach per DNS-Abfrage abrufen und überprüfen, ob die IP-Adresse des einliefernden Mail-Relays auf der Whitelist steht. Im SPF-Eintrag kann vorgegeben sein, dass alle anderen IPs als „Fail“ zu behandeln sind, also als nicht autorisierte Absender. In diesem Fall wird ein moderner

Empfangsserver die Mail aussortieren, noch bevor sie den Posteingang erreicht.

Das Ergebnis der SPF-Überprüfung wird üblicherweise in den Header der Mail geschrieben, nachgelagerte Spamfilter und Mail-Clients können die Information also in die Risikobewertung einbeziehen. Mit dem oben erwähnten Add-on „Message Header Analyzer“ können Sie das Ergebnis auch in Outlook nachvollziehen, Gmail-Nutzer klicken im Menü der Nachricht auf „Original anzeigen“. Die SPF-Records eigener und fremder Domains können Sie zum Beispiel über den Webdienst „SPF Record Checker“ von DNS Checker (siehe ct.de/y2qp) herausfinden.



SPF macht es Phishern schwer, eine Domain als Absender zu missbrauchen. Mit dem SPF Record Checker überprüfen Sie, ob der Spoofing-Schutz für eigene und fremde Domains aktiv ist.
Wer selbst Mail-Accounts anbietet, ist gut damit beraten, nicht nur die SPF-Records eingehender Mails zu überprüfen, sondern auch für die eigenen Domains SPF-Einträge zu hinterlegen, damit die Domains nicht so leicht als Absender missbraucht werden können. Falls Sie externe Dienste mit der

Domain nutzen, etwa Newsletter-Dienstleister, müssen Sie auch diese in den SPF-Records hinterlegen.

Ein weiteres erwähnenswertes Schutzverfahren nennt sich „DomainKeys Identified Mail“ (DKIM). Damit lassen sich Mails digital signieren. Der Empfänger kann dann verifizieren, dass die Nachricht tatsächlich von einem Mailserver stammt, der für die Absenderdomain zuständig ist. Der Mailserver des Absenders nutzt zum Signieren einen geheimen Kryptoschlüssel, der dazu passende öffentliche Schlüssel muss im DNS-Eintrag der Domain hinterlegt sein.

Zum Anzeigen der DKIM-Daten aus dem Header können Outlook-Nutzer wieder das Add-on „Message Header Analyzer“ nutzen, Gmail-Nutzer klicken auf „Original anzeigen“. Für Thunderbird gibt es die Erweiterung „DKIM Verifier“ von Philippe Lieser (siehe ct.de/y2qp), die das Ergebnis der DKIM-Prüfung alltagstauglich im Kopfbereich jeder Mail anzeigt. Ausführliche Informationen über SPF, DKIM und DMARC, das beide Verfahren vereint, finden Sie in c’t 9/2019 [3].

PayPal-Phishing 2.0

Die Verfahren greifen allerdings nur, wenn die Phishing-Mail in irgendeiner Form technisch manipuliert und etwa mit einem gespooften Absender verschickt wurde. Nutzt der Absender ein eigenes oder kompromittiertes Mailkonto, schlagen SPF und DKIM nicht Alarm, weil die Mails über den legitimen Mailserver der Absenderadresse verschickt werden. Das Gleiche gilt, wenn es Online-Schurken gelingt, einen vertrauenswürdigen Dienstleister vor ihren Karren zu spannen.

Beispielsweise hat die Security-Firma Avanan beobachtet, dass Betrüger die PayPal-Funktion „Geld anfordern“ für Phishing missbrauchen. Darüber könnten PayPal-Nutzer Geldanforderungen an beliebige Mail-Adressen schicken. Der Empfänger bekommt auf diese Weise eine offizielle Mail von service@paypal.de mit gültiger DKIM-Signatur, die es mit hoher Wahrscheinlichkeit in

den Posteingang schafft. Der Absender kann einen bis zu 3500 Zeichen langen Text eingeben, der in der PayPal-Mail auftaucht. Vor solchen perfiden Phishing-Tricks können Sie sich nur selbst schützen: durch einen Plausibilitätscheck und eine gesunde Portion Skepsis.

Fazit

Die Tipps und Hintergründe in diesem Artikel helfen Ihnen dabei, Phishing-Mails zu erkennen, damit Sie nicht in die Falle tappen. Denn die wichtigste Verteidigung gegen solche Social-Engineering-Angriffe ist Wissen – insbesondere beim Bewerten von Dateianhängen und Links. Teilen Sie dieses Wissen mit anderen, damit auch Familie, Freunde und Kollegen nicht auf gefährliche Mails reinfallen. *(rei@ct.de)*

1. Literatur
2. Niklas Dierking und Ronald Eikenberg, Schlosskombination, Verfahren und Geräte für sichere Online-Zugänge, c't 9/2022, S. 18
3. Jan Schüßler und Marvin Strathmann, Ich kaufe ein ****, 25 Passwortmanager für PC und Smartphone, c't 5/2021, S. 16
4. Patrick Koetter, Wagenburg, Wie SPF, DKIM und DMARC gegen Phishing und Spoofing helfen, c't 9/2019, S. 174

Analysetools: ct.de/y2qp

Checkliste – E-Mail-Sicherheit

Checkliste: Mails so verschicken, dass man Ihnen vertraut

Damit Ihre Mails nicht aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie die folgenden Tipps beherzigen, gelingt das.

Lesezeit: 4 Min.

In Pocket speichern

vorlesen

Druckansicht Kommentare lesen 60 Beiträge

(Bild: Andreas Martini)
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.

E-Mail-Sicherheit

Gute Mails, böse Mails

Gefahrloser Umgang mit E-Mails

Gefährliche Mails sollte man nicht öffnen – aber ob eine Mail harmlos ist oder nicht, weiß man oft erst, nachdem man sie geöffnet hat. Und manchmal nicht mal dann. Damit Sie trotzdem nicht in die Phishing-Falle tappen, müssen Sie ein paar Sicherheitsvorkehrungen treffen, die wir Ihnen hier geben.

Von Ronald Eikenberg

EMails zu öffnen ist wie Russisch Roulette – man weiß nie, ob es knallt. Meist hat man keine Wahl, ob man mitspielen möchte. Versuchen Sie doch mal, Ihrem Chef zu erklären, dass Sie ab sofort keine E-Mails mehr öffnen. Schlagkräftige Argument hätten Sie zuhauf: E-Mails sind gefährlich und der wichtigste Verbreitungsweg für Schädlinge. Allein die berüchtigte, hauptsächlich per Phishing-Mail verbreitete Emotet-Malware hat weltweit unzählige Unternehmen, Behörden, Krankenhäuser & Co. lahmgelegt und dabei Schäden in Milliardenhöhe angerichtet.

Ein weiteres Argument ist, dass Sie Ihrem Chef nicht versprechen können, dass Sie alle Phishing-Mails aussortieren und nicht darauf reinfallen. Denn die Zeiten, in denen man solche Mails schon von Weitem erkennen konnte, sind längst vorbei. Angreifer nutzen immer häufiger echte – gestohlene – Daten, um Sie in die Falle zu locken, zum Beispiel plausible Absender, mit denen Sie bereits Kontakt hatten. Phishing-Mails zitieren mitunter sogar aus vorangegangenen Mailwechseln mit Kollegen, Partnerfirmen oder Kunden.

Zwickmühle E-Mail

Wer beruflich mit Mails arbeitet, muss nicht selten Dutzende oder gar Hunderte davon Tag für Tag bearbeiten – und genauso viele Entscheidungen treffen. Das ist ganz schön viel Verantwortung, denn jede Fehlentscheidung, jeder falsche Klick kann die ganze Firma über Wochen lahmlegen. Die Krux ist, dass man es sich aber auch nicht leisten kann, eine Kundenanfrage oder eine Auftragsmail zu übersehen. Jede Mail muss daher gecheckt werden.

Sie ahnen es vielleicht bereits: Auch mit den besten Argumenten kommen Sie aus der Nummer nicht raus. E-Mail ist

der kleinste gemeinsame Nenner bei der Online-Kommunikation und daher weiterhin unverzichtbar. Die interne Kommunikation kann man inzwischen gut über moderne Kollaborationssoftware wie Rocket.Chat, Slack oder Teams abwickeln, für die Kommunikation mit der Außenwelt gibt es jedoch keinen Ersatz mit breiter Akzeptanz.

Im Privatleben sieht es ähnlich aus: Freunde und Verwandte können Sie problemlos über Messenger-Apps wie WhatsApp oder Signal erreichen – Ende-zu-Ende-verschlüsselt nach Stand der Technik und mit überprüfbarem Absender. Für die Kontaktaufnahme mit Firmen, Behörden und vielen mehr müssen Sie jedoch oft noch eine Mail schreiben. Rechnungen, Versandbestätigungen, Benachrichtigungen über verdächtige Aktivitäten et cetera landen in Ihrem Posteingang, neben Phishing-Mails aller Art. Und es bleibt an Ihnen hängen, die guten Mails von den bösen zu unterscheiden.

Aber was tun? Phishing zählt zur Angriffskategorie „Social Engineering“ – die Angreifer zielen also nicht auf technische Sicherheitslücken ab, sondern auf die Schwachstelle Mensch. Genau hier setzen die folgenden Artikel an: Wir möchten Ihnen das nötige Wissen und einige praktische Tipps an die Hand geben, damit Sie leicht die Spreu vom Weizen trennen können und für Phishing-Mails nur noch ein müdes Lächeln übrig haben.

Phishing auf den zweiten Blick: Mittlerweile muss man genau hinsehen, um die Rechtschreibfehler von Online-Ganoven zu finden. In der Anrede wird hier sogar ein bisschen gegendert.

Mails entschärfen

Es geht nicht nur darum, wie Sie verdächtige Mails anhand offensichtlicher und versteckter Merkmale bewerten können (siehe S. 18), sondern auch um die kniffligen Fälle. Manchmal bleiben auch nach einer eingehenden Prüfung Restzweifel, ob es

sich um Spreu oder Weizen handelt und ob die angehängte Datei unentbehrlich ist oder ernstzunehmenden Schaden anrichtet.

In solchen Fällen können Sie den Anhang vor dem Öffnen mit einem Tool wie Dangerzone entschärfen, indem Sie ein harmloses PDF daraus machen – garantiert ohne Office-Makros. Oder Sie analysieren die Datei mit speziellen Tools, um vorab gefahrlos zu überprüfen, ob sich darin Makros oder eingebettete Dateien verstecken (siehe S. 28).

Wir möchten Sie dazu anregen, dieses Wissen auch mit Kollegen, Freunden, Familie und Geschäftspartnern zu teilen – in ihrem eigenen Interesse. Denn den größten Einfluss auf Ihren Posteingang haben nicht Sie, sondern die Absender der Mails. Wenn jeder die wichtigsten Dos & Don’ts kennt und beim Verschicken beherzigt, wird E-Mail für alle sicherer.

Wir haben die wichtigsten Tipps für den Mailversand daher als kompakte und leicht verdauliche Checkliste auf Seite 26 zusammengestellt. Die Checkliste ist online frei abrufbar, damit Sie sie leicht weitergeben können. Wenn Sie mögen, können Sie in Ihrer Mailsignatur darauf verweisen: **https://ct.de/sicher-mailen** (*rei@ct.de*)