ANLEITUNG

WordPress sicher machen in 9 Schritten

Für kleine Unternehmen, Kanzleien, Agenturen und Selbstständige, die ihre Website nutzen, sich aber nicht täglich mit IT-Sicherheit beschäftigen wollen.

1 Regelmäßige Updates durchführen

Warum? Veraltete WordPress-Versionen, Plugins oder Themes sind die häufigste Einfallstelle für Angreifer. Mit jedem Update werden Sicherheitslücken geschlossen.

So geht's

1. Melden Sie sich im WordPress-Dashboard an (www.IhreDomain.at/wp-admin).
2. Klicken Sie auf „Dashboard“ > „Aktualisierungen“.
3. Führen Sie alle angebotenen Updates durch (WordPress, Plugins, Themes).
4. Optional: Aktivieren Sie unter „Plugins“ beim jeweiligen Plugin „Automatische Aktualisierungen aktivieren“.

> **Tipp:** Vor Updates großer Plugins wie Ihres Pagebuilders (z. B. Elementor) sollten Sie ein Backup machen. Diese Updates lassen Sie deshalb besser nicht automatisch laufen.

2 Sichere Passwörter und Zwei-Faktor-Authentifizierung

Warum? Viele Angriffe laufen über leicht zu erratende Passwörter oder gestohlene Zugangsdaten. Die Zwei-Faktor-Authentifizierung (2FA) schützt auch dann, wenn das Passwort bekannt ist.

So geht's

1. Installieren Sie das kostenlose Plugin Wordfence Security.
2. Aktivieren Sie unter „Wordfence“ > „Login Security“ die Zwei-Faktor-Authentifizierung für Ihr Konto.
3. Laden Sie eine Authenticator-App auf Ihr Handy, z. B. Microsoft Authenticator oder Google Authenticator.
4. Scannen Sie den QR-Code und bewahren Sie die Wiederherstellungscodes sicher auf.

> **Tipp:** Ein Passwortmanager wie 1Password oder Bitwarden erzeugt starke Passwörter und speichert sie sicher.

3 Admin-Konto und Autoren-Konto trennen

Warum? Wenn das Admin-Konto auch Inhalte schreibt, ist sein Name für jeden im Internet sichtbar und damit ein leichtes Ziel für Angriffe.

So geht's

1. Legen Sie unter „Benutzer“ ein neues Konto mit der Rolle „Autor“ an.
2. Schreiben Sie alle Beiträge mit diesem Konto. Den Autor bestehender Inhalte ändern Sie unter „Seiten“ und „Beiträge“.
3. Verwenden Sie das Admin-Konto nur noch für technische Aufgaben wie Updates.

> **Tipp:** Verwenden Sie niemals „admin“ als Benutzernamen.

4 REST-API für anonyme Besucher sperren

Warum? Über die REST-API lassen sich Benutzernamen und andere Informationen auslesen, auch ohne Anmeldung. Das hilft Angreifern bei gezielten Angriffen.

So geht's

1. Installieren Sie das Plugin Disable REST API.
2. Aktivieren Sie es. Eine Grundkonfiguration ist nicht nötig.
3. Testen Sie die Sperre: Die Adresse IhreDomain.at/wp-json/wp/v2/users sollte ohne Anmeldung keine Daten mehr zeigen.

> **Tipp:** Das Plugin sperrt die REST-API nur für nicht angemeldete Besucher. Testen Sie danach Ihr Kontaktformular: Manche Formular-Plugins, etwa Contact Form 7, senden über die REST-API und müssen in den Einstellungen des Plugins freigegeben werden.

5 Spamschutz für Kontaktformulare

Warum? Kontaktformulare ohne Schutz sind ein beliebtes Ziel für Spam-Bots. Das Plugin WP Armour verhindert automatisierte Eingaben, ganz ohne Captcha.

So geht's

1. Installieren Sie das Plugin WP Armour – Honeypot Anti Spam.
2. Eine Konfiguration ist nicht nötig, es funktioniert sofort.
3. Testen Sie Ihr Kontaktformular. Echte Besucher merken keinen Unterschied.

> **Tipp:** Geeignet für Kontaktformulare mit Contact Form 7 oder Elementor Forms.

6 Firewall und Anmeldeversuche begrenzen

Warum? Angreifer probieren oft automatisch tausende Passwörter aus. Eine Firewall blockiert solche Versuche, bevor sie Erfolg haben.

So geht's

1. Installieren Sie Wordfence Security, falls noch nicht geschehen.
2. Aktivieren Sie die Firewall unter „Wordfence“ > „Firewall“.
3. Legen Sie unter „Wordfence“ > „All Options“ im Bereich „Brute Force Protection“ fest, nach wie vielen Fehlversuchen gesperrt wird, z. B. nach 3 bis 5.

> **Tipp:** Wordfence schickt Ihnen E-Mail-Warnungen bei auffälligem Verhalten. Lesen Sie diese aufmerksam.

7 Regelmäßige Backups einrichten

Warum? Ohne Backup verlieren Sie im Ernstfall alles: Inhalte, Kontaktanfragen und Ihre Platzierungen bei Google.

So geht's

1. Installieren Sie das Plugin UpdraftPlus.
2. Wählen Sie ein Speicherziel, z. B. Google Drive oder Dropbox.
3. Stellen Sie einen Zeitplan ein (täglich oder wöchentlich) oder sichern Sie bei Bedarf selbst.
4. Führen Sie sofort ein Backup durch und testen Sie, ob es sich wiederherstellen lässt.

> **Tipp:** Backups gehören nicht auf denselben Server wie die Website.

8 Nur notwendige Plugins verwenden

Warum? Jedes Plugin ist ein mögliches Sicherheitsrisiko. Weniger ist sicherer.

So geht's

1. Öffnen Sie im Dashboard „Plugins“.
2. Deaktivieren Sie Plugins, die Sie nicht mehr nutzen.
3. Löschen Sie deaktivierte Plugins.
4. Installieren Sie nur Plugins aus dem offiziellen WordPress-Verzeichnis oder von vertrauenswürdigen Anbietern, die regelmäßig aktualisiert werden.

> **Tipp:** Wenn Sie Ihre Seite nicht selbst eingerichtet haben und unsicher sind, ob ein Plugin gebraucht wird, fragen Sie lieber Ihren Anbieter.

9 Was tun im Ernstfall?

Warum? Wenn Ihre Website gehackt wurde, zählt jede Stunde. Gehen Sie in dieser Reihenfolge vor.

So geht's

1. Aktivieren Sie den Wartungsmodus (z. B. mit dem Plugin Maintenance), damit Besucher keine manipulierte Seite sehen und kein weiterer Schaden entsteht.
2. Spielen Sie das letzte saubere Backup ein.
3. Ändern Sie alle Passwörter.
4. Scannen Sie die Seite mit Wordfence auf Schadcode.
5. Informieren Sie Ihren Hosting-Anbieter. Er kann unterstützen und sollte die Sicherheit auf seiner Seite prüfen.
6. Holen Sie sich im Zweifel Unterstützung von einem IT-Dienstleister.

> **Tipp:** Dokumentieren Sie, was passiert ist. Das hilft bei der Wiederherstellung, bei Supportanfragen und in Haftungsfragen.

Und wie sieht es mit Ihrer IT insgesamt aus?

Ihre Website ist ein wichtiges Aushängeschild, aber nur ein kleiner Teil Ihrer IT-Sicherheit. Was passiert, wenn jemand E-Mails in Ihrem Namen verschickt? Oder wenn Ihre Microsoft-365-Daten plötzlich verschwunden sind?

Kostenloser Microsoft-365-Check, online und unverbindlich: **dantersec.com/kostenloser-microsoft-365-check**

Selbsteinschätzung in 10 Fragen: **dantersec.com/it-checkliste-fuer-kmus**

Lieber betreuen lassen?

Ich baue und betreue WordPress-Seiten für Unternehmen und übernehme Updates, Backups und Sicherheit.
+43 316 231589 · daniel.juch@dantersec.com · dantersec.com/kontakt