WWWEWERS

RATGEBER · WEBSITE-SICHERHEITSCHECK

WEBSITE-SICHERHEIT NACH DER PHP-WARNUNG.

Was hinter der BSI-Warnung vom 21. Oktober 2026 steckt. Und was du jetzt tun solltest.



Ein Ratgeber von WWWEWERS aus Dülmen · Stand: 22. Oktober 2026

KURZ & KLAR

DAS WICHTIGSTE IN 60 SEKUNDEN

- **Das BSI warnt vor zwei kritischen Lücken in PHP.** PHP ist die Technik, auf der fast alle Websites laufen.
- **Betroffen sind alle PHP-Versionen.** Mindestens zurück bis PHP 5.
- **Angreifer könnten aus der Ferne Schadcode auf dem Server ausführen.** Ohne Passwort und ohne dass jemand etwas anklickt.
- **Es gibt Updates.** Aber nur für neuere PHP-Versionen.
- **Ältere Websites trifft es am härtesten.** Für ihre Technik gibt es oft kein Update mehr.
- **Baukasten-Seiten sind fein raus.** Wix, Jimdo, Webflow und Squarespace aktualisieren selbst.
- **Nicht nur die Website zählt.** Auch E-Mail-Postfächer und Passwörter können betroffen sein.

Dein Weg durch diesen Ratgeber

Auf **Seite 5** machst du den Selbstcheck. Auf **Seite 6** siehst du, wie dringend es bei dir ist. Auf **Seite 9** findest du sieben Fragen für deinen Dienstleister. Kopieren, abschicken, fertig.

KAPITEL 1

WAS IST PASSIERT?

Am 21. Oktober 2026 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Warnung veröffentlicht. Stufe 3 von 4, „Orange“. Laut BSI heißt das: Maßnahmen müssen unverzüglich ergriffen werden.

Es geht um zwei Schwachstellen in PHP. Beide sind mit 9,2 von 10 Punkten bewertet. In Fachmedien heißen sie „PHP2Shell“.

Was ist PHP?

PHP ist eine Programmiersprache. Sie läuft auf dem Server deines Hosters. Dort baut sie jede Seite zusammen, sobald jemand sie aufruft. WordPress, TYPO3, Joomla und Shopware laufen alle mit PHP. Du siehst PHP nie. Aber fast jede Website braucht es.

Wie ernst ist es?

Zum Zeitpunkt der Warnung waren noch keine Angriffe bestätigt. Das BSI rechnet aber mit einer schnellen Ausnutzung. Der Grund: Mit KI-Werkzeugen lassen sich Angriffe heute in wenigen Stunden aus einem Update ableiten. Einige Betreiber haben ihre Server deshalb vorsorglich vom Netz genommen.

Was kann passieren?

Laut BSI könnten Angreifer eigenen Code auf dem Webserver ausführen. Aus der Ferne, ohne Passwort, ohne Klick. Wer das schafft, kann zum Beispiel:

- deine Website verändern oder Schadsoftware darüber verteilen,
- Daten aus Kontaktformularen abgreifen,
- über deinen Server Spam und Phishing-Mails verschicken,
- an E-Mail-Postfächer kommen, die auf demselben Server liegen.

> **Ehrlich gesagt:** Panik hilft niemandem. Aber abwarten ist hier die schlechteste Option.

KAPITEL 2

WARUM ES ÄLTERE WEBSITES BESONDERS TRIFFT

Die Lücke steckt in PHP, nicht in WordPress oder TYPO3. Dein Hoster muss also PHP aktualisieren. Bei aktuellen Versionen ist das meist schnell erledigt.

Updates gibt es für: PHP 8.2, 8.3, 8.4 und 8.5. Die sicheren Versionen sind 8.2.35, 8.3.36, 8.4.27 und 8.5.12.

Nachbesserungen gibt es für: PHP 7.4, 8.0 und 8.1. Ob dein Hoster sie einspielt, musst du bei ihm erfragen.

Kein Update gibt es für: PHP 7.3 und älter.

Das eigentliche Problem: Alte Website-Systeme laufen nur auf alten PHP-Versionen. Ein TYPO3 9 läuft zum Beispiel nicht auf PHP 8. Der Hoster kann PHP dann nicht einfach aktualisieren. Sonst ist die Website weg.

> **Ein Beispiel aus dieser Woche:** Wir haben die Website eines Handwerksbetriebs aus dem Münsterland geprüft. Sie läuft auf PHP 7.2. Diese Version bekommt seit November 2020 keine Sicherheitsupdates mehr. Die neue Lücke kommt also noch obendrauf.

Noch ein Datum für deinen Kalender: PHP 8.2 bekommt nur noch bis Ende 2026 Sicherheitsupdates. Wer heute auf 8.2 läuft, sollte das nächste Update jetzt schon einplanen.



KAPITEL 3

BIN ICH BETROFFEN?
DER SELBSTCHECK IN 3 SCHRITTEN

1 Welches System nutzt deine Website?

- Endet deine Login-Adresse auf **/wp-admin**? Dann ist es WordPress.
- Endet sie auf **/typo3**? Dann ist es TYPO3.
- Steht im Impressum oder in der Fußzeile „Umsetzung: Agentur X“? Dann frag dort nach.
- Hast du noch die Rechnung von damals? Dort steht das System oft drin.

2 Welche Version läuft?

- **WordPress:** Im Dashboard unter „Auf einen Blick“ steht die WordPress-Version. Die PHP-Version findest du unter „Werkzeuge → Website-Zustand → Bericht → Server“.
- **TYPO3:** Im Backend oben rechts über das Symbol für Systeminformationen. Dort stehen TYPO3- und PHP-Version.
- **Kein Zugang mehr?** Schau in den Kundenbereich deines Hosters. Die PHP-Version steht meist unter „Hosting“ oder „Webspace“.

3 Wer kümmert sich um Updates?

Eine Agentur, du selbst oder niemand? Die ehrliche Antwort ist wichtig. Gerade Websites ohne Betreuung sind oft seit Jahren nicht aktualisiert.

Du kommst bei einem Schritt nicht weiter? Das geht den meisten so. Genau dafür gibt es unseren kostenlosen Check auf Seite 10.

KAPITEL 4

DIE AMPEL: WIE DRINGEND IST ES BEI DIR?

Das ist eine Ersteinschätzung auf Basis deiner Angaben. Sie ersetzt keine technische Prüfung.

GRÜN: Kein Handlungsbedarf

Deine Website läuft auf einem Baukasten wie Wix, Jimdo, Webflow oder Squarespace. Der Anbieter schließt solche Lücken selbst. Nach unserer Einschätzung musst du nichts tun. Für diese Lücke brauchst du uns ehrlich gesagt nicht.

GELB: Lösbar, jetzt nachfragen

WordPress 6.x oder TYPO3 13 bzw. 14. Deine Version ist aktuell genug. Entscheidend ist, ob dein Hoster PHP schon aktualisiert hat. Frag nach (Fragen auf Seite 9). Meist ist das schnell erledigt.

ORANGE: Handlungsbedarf

WordPress 5.x oder TYPO3 11 bzw. 12. Deine Version läuft meist noch auf aktueller PHP-Technik, bekommt aber keine kostenlosen Sicherheitsupdates mehr. Plane ein Update ein. Orange gilt auch, wenn sich niemand um deine Website kümmert.

ROT: Dringend

WordPress 4.x oder älter, TYPO3 10 oder älter, ältere Shopsysteme wie Shopware 5. Deine Website braucht eine alte PHP-Version. Für die gibt es kein oder kaum noch ein Sicherheitsupdate. Hier solltest du diese Woche handeln.

GRAU: Noch offen

Du weißt nicht, welches System oder welche Version läuft. Damit bist du nicht allein. Viele ältere Websites sind betroffen. Lass es prüfen, bevor du dir Sorgen machst.

Zusätzlich wichtig: Hat deine Website einen Shop, eine Bezahlfunktion oder einen Kunden-Login? Dann ist das Risiko höher. Dort liegen Daten von Menschen, die dir vertrauen.

KAPITEL 5

WAS DU JETZT TUN KANNST

Bei Gelb

1. Frag deinen Hoster oder Dienstleister, ob das PHP-Update eingespielt ist.
2. Aktualisiere WordPress bzw. TYPO3 und alle Erweiterungen.
3. Prüfe, ob es ein aktuelles Backup gibt.

Bei Orange

Alles von Gelb. Dazu:

1. Plane das Update auf eine Version mit Sicherheitsupdates. Bei WordPress ist das oft ein Nachmittag. Bei TYPO3 kann es ein größeres Projekt sein.
2. Kläre, wer sich künftig kümmert. Schriftlich.

Bei Grau

Finde heraus, was läuft. Mit dem Selbstcheck auf Seite 5. Oder mit unserem Check auf Seite 10.

Bei Rot: drei ehrliche Optionen

1. Das System aktualisieren. Von einem alten TYPO3 auf ein aktuelles ist es fast ein Neubau. Das dauert eher Wochen als Tage. Langfristig richtig, kurzfristig zu langsam.

2. Eine Übergangslösung bauen. Wir legen eine reine HTML-Kopie deiner Website an. Sie sieht für Besucher genauso aus. Sie braucht aber kein PHP mehr und bietet damit diese Angriffsfläche nicht. Bei einfachen Websites dauert das wenige Stunden.

Was die Übergangslösung nicht kann: Formulare, Shop und Login funktionieren darin nicht oder nur eingeschränkt. Inhalte kannst du in der Zeit nicht selbst pflegen. **Wichtig:** Das alte System muss komplett vom Server. Sonst bleibt die Lücke offen.

3. Die Website vorübergehend offline nehmen. Das empfiehlt auch das BSI, wenn kein Update möglich ist. Unschön, aber besser als eine gekaperte Website.

KAPITEL 6

NICHT NUR DIE WEBSITE: E-MAIL, PASSWÖRTER, KONTEN

E-Mail-Postfächer

Liegen deine Postfächer auf demselben Server wie die Website? Dann sind sie im Ernstfall genauso gefährdet. Ein schneller Hinweis: Meldest du dich für deine Mails bei Microsoft 365 oder Google an, sind sie meist getrennt. Im Zweifel frag deinen Hoster.

Dein guter Name

Ein gekaperter Server kann Spam und Phishing-Mails in deinem Namen verschicken. Deine Kunden bekommen dann betrügerische Mails von deiner Adresse. Und deine echten Mails landen danach oft im Spam-Ordner.

Andere Konten

Viele nutzen dasselbe Passwort mehrfach. Für die Website, das Postfach, Instagram, Office und manchmal sogar das Online-Banking. Fließt ein Passwort ab, sind dann gleich mehrere Konten in Gefahr.

Datenschutz

Fließen personenbezogene Daten ab, etwa aus einem Kontaktformular, musst du das in der Regel innerhalb von 72 Stunden der Datenschutzbehörde melden (Art. 33 DSGVO). Das ist keine Rechtsberatung. Im Ernstfall hol dir fachlichen Rat.

Heute erledigt, in 15 Minuten

- [ ] Ändere die Passwörter deiner E-Mail-Postfächer und deines Website-Logins.
- [ ] Nutze für jedes Konto ein eigenes Passwort. Ein Passwort-Manager hilft.
- [ ] Schalte die Zwei-Faktor-Anmeldung ein. Mindestens für E-Mail, Social Media und Banking.
- [ ] Lösche alte Admin-Zugänge, zum Beispiel von früheren Mitarbeitenden oder Agenturen.

7 FRAGEN AN DEINEN DIENSTLEISTER

1. Welche PHP-Version läuft auf unserem Server?
2. Ist das Sicherheitsupdate vom 21.10.2026 eingespielt? (PHP 8.2.35, 8.3.36, 8.4.27, 8.5.12 oder eine Nachbesserung für ältere Versionen)
3. Welche Version unseres Website-Systems läuft? Bekommt sie noch Sicherheitsupdates?
4. Sind alle Erweiterungen und Plugins aktuell?
5. Liegen unsere E-Mail-Postfächer auf demselben Server wie die Website?
6. Gibt es ein aktuelles Backup außerhalb des Servers? Wann wurde die Wiederherstellung zuletzt getestet?
7. Wer ist zuständig, wenn etwas passiert? Und wie schnell reagiert ihr?

Bekommst du innerhalb von zwei Tagen klare Antworten? Gutes Zeichen. Dann bleib bei deinem Dienstleister. Für dieses Thema brauchst du uns dann nicht. **Keine Antwort oder nur Ausflüchte?** Dann melde dich bei uns.

SO BLEIBT DEINE WEBSITE DAUERHAFT SICHER

- [ ] PHP-Version mit Sicherheitsupdates. Heute heißt das: 8.3 oder neuer. 8.2 nur noch bis Ende 2026.
- [ ] Website-System und Erweiterungen jeden Monat aktualisieren.
- [ ] Automatische Backups außerhalb des Servers. Wiederherstellung einmal im Jahr testen.
- [ ] Nur die Admin-Zugänge, die wirklich gebraucht werden. Mit Zwei-Faktor-Anmeldung.
- [ ] Erweiterungen löschen, die niemand mehr nutzt.
- [ ] Zuständigkeit schriftlich festhalten. Wer kümmert sich, wer zahlt?
- [ ] E-Mail-Postfächer getrennt vom Webserver betreiben.
- [ ] Einmal im Jahr einen Blick von außen werfen lassen.

Das kannst du selbst machen. Oder du gibst es ab.

WWWEWERS

WEBSITE-SICHERHEITSCHECK

DER KOSTENLOSE SICHERHEITSCHECK.

Wir sind WWWEWERS, eine Agentur aus Dülmen. Zehn Leute, über 100 Unternehmen aus dem Münsterland, für die wir arbeiten. Wir bauen und betreuen Websites, zusammen mit unserem festen Entwicklungspartner. Seit der Warnung am 21. Oktober haben wir die Websites unserer Kunden geprüft und die ersten Übergangslösungen auf den Weg gebracht.

Was du bekommst

- Wir schauen von außen auf deine Website: welches System, welche PHP-Version, wo deine Mails liegen.
- Wir rufen dich an und sagen dir im Klartext, wie dringend es ist.
- Du bekommst deine Optionen mit ehrlicher Einschätzung von Aufwand und Kosten.

Was du nicht brauchst

Zugangsdaten. Passwörter fragen wir nie per Formular oder Mail ab.

Was der Check nicht ist

Keine vollständige Sicherheitsprüfung und keine Garantie. Aber ein klares Bild, was zu tun ist. Und wenn alles in Ordnung ist, sagen wir dir das auch.

DREHEN WIR EINE RUNDE?

Klartext: Fordere deinen kostenlosen Check an. Wir melden uns innerhalb von 2 Werktagen.

GO.WWWEWERS.DE/PHP-CHECK »

WWWEWERS GmbH · Coesfelder Str. 17 · 48249 Dülmen · hallo@wwwewers.de · wwwewers.de
Stand: 22. Oktober 2026. Alle Angaben nach bestem Wissen auf Basis öffentlicher Quellen. Ohne Gewähr, keine Rechtsberatung. Die Lage kann sich ändern.
Quellen: BSI-IT-Sicherheitshinweis „PHP: Kritische Schwachstellen bedrohen Webanwendungen weltweit“, Version 1.1 vom 21.10.2026 · php.net · Art. 33 DSGVO