Vorlage für Agenturen: Information an ihre Endkunden

Textvorlage, die mittwald betroffenen Agenturen und Resellern mitgibt. Die Agentur spricht in der Wir-Form, mittwald wird als Dienstleister in der dritten Person genannt. Die Anrede ist „Sie", weil die meisten Agenturen ihre Kunden so ansprechen. Wo es passt, auf „du" umstellen. Alles in eckigen Klammern füllt die Agentur selbst aus. Alle Fakten entsprechen Abschnitt 7. Ändert sich dort etwas, muss es hier nachgezogen werden.

Betreff: Sicherheitsvorfall bei unserem Hosting-Anbieter: Was das für Ihr Projekt bedeutet

Guten Tag [Name],

wir möchten Sie über einen Sicherheitsvorfall bei unserem Hosting-Anbieter mittwald informieren, der Ihr Projekt [Projektname / Website] betreffen kann. Wir legen Ihnen offen dar, was passiert ist, welche Daten betroffen sein können und was wir und Sie jetzt tun.

Was passiert ist
mittwald betreibt die Server, auf denen Ihr Projekt läuft. Am 27.10.2026 haben sich Unbekannte über eine Schwachstelle Zugriff auf eine Schnittstelle von mittwald verschafft. Es handelt sich um den sogenannten MCP-Server, über den Hosting-Kunden ihre Verwaltungsoberfläche mit KI-Assistenten verbinden konnten. Dabei wurden Zugangs-Token von Nutzern dieser Schnittstelle ausgelesen, darunter auch unseres. Mit diesem Token war ein Zugriff auf die Projekte möglich, die wir bei mittwald verwalten. Nach eigenen Angaben hat mittwald den Vorfall am 04.11.2026 erkannt und uns am [Datum] informiert. Passwörter wurden nicht ausgelesen.

Zeitraum
Der unbefugte Zugriff war vom 27.10.2026 bis zur Sperrung der Token am 04.11.2026 möglich.

Welche Daten betroffen sein können
Der entwendete Zugang hatte in der Verwaltungsoberfläche von mittwald dieselben Rechte wie wir. Deshalb können grundsätzlich alle Daten Ihres Projekts betroffen sein:

- Dateien und Programmcode der Website
- die Datenbank der Website mit den darin gespeicherten Daten [z. B. Kundenkonten, Bestellungen, Kontaktanfragen, Newsletter-Adressen; an das Projekt anpassen]
- im Projekt hinterlegte Zugangsdaten zu Drittdiensten [z. B. Zahlungsanbieter, Newsletter-Tool, Schnittstellen]. Ein Zugriff darauf war technisch möglich, Hinweise darauf gibt es bislang nicht. [zweiten Satz nur verwenden, wenn mittwald das bestätigt]
- E-Mail-Postfächer, die über das Projekt verwaltet werden [streichen, falls nicht zutreffend]

mittwald prüft derzeit für jedes Projekt einzeln, ob tatsächlich auf Daten zugegriffen wurde. Sobald uns das Ergebnis vorliegt, informieren wir Sie. Nach Angaben von mittwald gibt es bislang keine Hinweise darauf, dass Daten veröffentlicht wurden.

Was mittwald getan hat
mittwald hat die betroffene Schnittstelle abgeschaltet, die Schwachstelle geschlossen und alle ausgelesenen Zugangs-Token widerrufen. Seit dem 04.11.2026 prüft mittwald alle Projekte, die betroffen sein könnten. Findet mittwald in einem Projekt Spuren des Zugriffs, sperrt mittwald es vorsorglich und stellt es aus einer Sicherung mit Stand vor dem 27.10.2026 wieder her. Am 05.11.2026 hat mittwald außerdem die Verwaltungsoberfläche und den SSH-Zugang vorübergehend gesperrt. Ihre Website und Ihre E-Mails laufen davon unberührt weiter. Nach eigenen Angaben hat mittwald die zuständige Datenschutzbehörde [informiert / Formulierung aus der mittwald FAQ übernehmen].

Was wir getan haben

- Unsere Zugangsdaten bei mittwald ändern wir und aktivieren die Zwei-Faktor-Authentifizierung. [Anpassen, sobald die Verwaltungsoberfläche wieder erreichbar ist]
- Wir prüfen alle unsere Projekte auf Zugänge und Schlüssel, die wir nicht selbst angelegt haben.
- Wir erneuern vorsorglich die Zugangsdaten zu Drittdiensten, die in Ihrem Projekt hinterlegt sind. [Konkret benennen]
- Wir stehen in direktem Kontakt mit mittwald und erhalten das Prüfergebnis für Ihr Projekt.

Was Sie jetzt tun sollten
Nach aktuellem Stand wurden keine Passwörter ausgelesen. Die folgenden Schritte sind eine Vorsichtsmaßnahme, damit Ihr Projekt in jedem Fall abgesichert ist.

1. Wenn Ihre Website Nutzerkonten hat [Shop, Kundenlogin, CMS-Redakteure]: Ändern Sie vorsorglich Ihr eigenes Passwort und überlegen Sie, Ihre Nutzer ebenfalls darum zu bitten. Wir unterstützen Sie dabei.
2. Wenn Sie uns Zugangsdaten zu Drittdiensten gegeben haben [z. B. Zahlungsanbieter, Versand, Newsletter]: Erneuern Sie diese vorsorglich im jeweiligen Dienst. Geben Sie uns Bescheid, dann hinterlegen wir die neuen Daten.
3. Prüfen Sie, ob Sie als Verantwortlicher im Sinne der DSGVO den Vorfall Ihrer Datenschutzbehörde melden oder Ihre Nutzer informieren müssen. Für die Meldung an die Behörde gilt eine Frist von 72 Stunden ab Kenntnis. Falls Ihr Unternehmen unter NIS2 fällt, prüfen Sie zusätzlich, ob Sie den Vorfall dem BSI melden müssen. Dort gilt für die Erstmeldung eine Frist von 24 Stunden. Grundlage dafür sind die Angaben in dieser Mail und das Prüfergebnis von mittwald. Bei Bedarf stellen wir Ihnen alle Unterlagen zusammen.
4. Wenn Ihnen an Ihrer Website etwas Ungewöhnliches auffällt [fremde Inhalte, unbekannte Nutzer, Mails, die Sie nicht versendet haben], melden Sie sich bitte sofort bei uns.

Wie es weitergeht
Sobald mittwald uns das Prüfergebnis für Ihr Projekt mitteilt, sagen wir Ihnen, ob und welche Daten konkret betroffen sind und ob eine Wiederherstellung nötig war. Wir rechnen damit [Zeitraum / „in den nächsten Tagen"]. Bis dahin melden wir uns, sobald es Neues gibt.

Ihr Kontakt bei uns

[Name], [Telefon], [E-Mail]

Den aktuellen Stand veröffentlicht mittwald unter https://www.mittwald.de/lp/mcp-faq. Diese Seite ist die verbindliche Quelle von mittwald zu dem Vorfall.

Es tut uns leid, dass Ihr Projekt von diesem Vorfall bei unserem Dienstleister betroffen ist. Wir kümmern uns darum, dass es abgesichert wird.

Mit freundlichen Grüßen

[Name] [Agentur]

Hinweise für die Agentur beim Ausfüllen

Kürzt die Liste „Welche Daten betroffen sein können" auf das konkrete Projekt. Eine Visitenkarten-Website ohne Datenbank hat andere Risiken als ein Shop.

Versprecht nichts, was mittwald nicht bestätigt hat. Lasst „nach Angaben von mittwald" stehen.

Streicht Punkt 3 (DSGVO) nicht. Die Agentur ist Auftragsverarbeiter, der Endkunde ist Verantwortlicher. Die Meldepflicht liegt bei ihm.

Bei Fragen, die diese Vorlage nicht beantwortet:
support@mittwald.de, 05772 / 293 800, Stichwort „MCP-Vorfall".