

BEISPIEL - REPORT

Übernahme- Assessment

B2B-Bestellportal «Orderdesk» der Muster AG: technische Bestandsaufnahme, Risiken und ein Plan, wie die Anwendung sicher weiterbetrieben und weiterentwickelt werden kann.

AUFTRAGGEBERIN

Muster AG, Grosshandel Befestigungstechnik

ANWENDUNG

«Orderdesk», B2B-Bestellportal (PHP / Laravel)

ZUGANG VOLLSTÄNDIG · REPORT

11. September 2026 · 18. September 2026

VERFASST VON

Dimitri König, Unique-P GmbH

Beispiel: Firma, Anwendung, Befunde und Beträge in diesem Report sind frei erfunden. Aufbau, Tiefe und Tonalität entsprechen einem echten Übernahme-Assessment der Unique-P GmbH.

Die Anwendung ist übernehmbar. Kritisch ist nicht der Code, sondern ihr Umfeld.

«Orderdesk» wickelt rund 55 % des Umsatzes der Muster AG ab: 420 aktive Firmenkunden, rund 1'800 Bestellungen pro Monat. Entwickelt wurde die Anwendung ab 2014 von einem externen Freelancer, der seit 2025 nicht mehr erreichbar ist. Der Hoster hat angekündigt, PHP 7.4 per 31. März 2027 abzuschalten.

Der fachliche Kern ist solide gebaut und gut lesbar, ein Neubau ist nicht nötig. Die Risiken liegen im Betrieb: Die Plattform läuft auf Versionen ohne Sicherheitsupdates, es gibt keine Testumgebung und keine getesteten Backups, und ein Teil des produktiven Codes ist nicht versioniert. Mehrere Befunde sind sofort behebbar und sollten unabhängig von jeder weiteren Entscheidung angegangen werden.

GESAMTRISIKO

Hoch

4 kritische, 5 hohe Befunde

ÜBERNAHMEFÄHIGKEIT

6 / 10

Bedingt: mit Sofortmassnahmen
gut übernehmbar

HANDLUNGSFRIST

31.03.2027

Abschaltung PHP 7.4 durch den
Hoster

Die drei wichtigsten Risiken

- 1. Stillstand ab April 2027.** Ohne Upgrade läuft «Orderdesk» nach der Abschaltung von PHP 7.4 nicht mehr. Das Upgrade betrifft Framework, Pakete und Datenbank gleichzeitig.
- 2. Datenverlust bei einem Ausfall.** Es gibt nur die Datenbank-Backups des Hosters (7 Tage). Dateien werden nicht gesichert, eine Wiederherstellung wurde nie getestet.
- 3. Öffentlich abrufbare Kundendaten.** CSV-Exporte mit Kunden- und Bestelldaten liegen in einem öffentlich erreichbaren Verzeichnis. Das ist innert eines Tages behebbar.

Empfehlung: Option B, stabilisieren und schrittweise modernisieren. In drei Etappen bis Ende Februar 2027, zum Fixpreis von insgesamt CHF 31'800. Ein Neubau würde geschätzt CHF 180'000 bis 250'000 kosten und nicht vor der Abschaltung fertig.

Entscheidungsbedarf: Wahl der Option bis 15. Oktober 2026. Die Sofortmassnahmen (Kapitel 12) sollten sofort starten.

Kann das System sicher übernommen werden?

6 / 10

bedingt übernahmefähig

KRITERIUM	BEFUND	STATUS
Source Code	Vollständig vom Server gesichert und mit dem Git-Stand abgeglichen	● vorhanden
Versionshistorie	Git-Repository bis 2021; 31 Dateien wurden danach nur noch direkt auf dem Server geändert	● teilweise
Hosting & Domain	Zugriff vorhanden, aber Hosting-Konto und Domain laufen auf die private E-Mail-Adresse des Entwicklers	● teilweise
Datenbank & Backups	Zugriff vorhanden; nur Datenbank-Backups des Hosters, Wiederherstellung nie getestet	● teilweise
Test-/Staging-Umgebung	Keine. Änderungen gehen direkt in die Produktion	● fehlt
Dokumentation	README mit Installationshinweisen von 2016, sonst keine	● fehlt
Fachliches Wissen	Leiterin Innendienst kennt alle Abläufe und Sonderfälle	● vorhanden
Übergabe durch Vorgänger	Nicht möglich; Wissen wurde aus Code, Datenbank und Betrieb rekonstruiert	● fehlt

Was im Einsatz ist, und wie lange noch.

KOMPONENTE	VERSION	SUPPORT-ENDE	BEWERTUNG
PHP	7.4.33	November 2022	kritisch
Framework	Laravel 5.8	Februar 2020	kritisch
Datenbank	MySQL 5.7	Oktober 2023	hoch
Frontend	jQuery 1.12, Vue.js 2.6	Vue 2: Dezember 2023	hoch
PHP-Pakete	64 Pakete	23 ohne Sicherheitsupdates	hoch
PDF-Erzeugung	wkhtmltopdf 0.12	Projekt seit 2023 archiviert	mittel
Frontend-Build	Laravel Mix, 212 npm-Pakete	Build nicht reproduzierbar	mittel
Webserver	Apache 2.4 (Shared Hosting)	vom Hoster gepflegt	niedrig

Der Kalender entscheidet mit.

Laufzeitumgebung, Framework und Datenbank erhalten seit Jahren keine Sicherheitsupdates mehr. Bisher war das ein stilles Risiko. Mit der angekündigten Abschaltung von PHP 7.4 bekommt es ein Datum.



Wichtig: Ein Aufschub über ein «Legacy-PHP»-Angebot des Hosters verschiebt nur das Datum. Die Sicherheitslücken bleiben, und jedes weitere Jahr macht den Versionssprung grösser.

Wie die Anwendung heute betrieben wird.

Deployment

- Upload per FTP vom Laptop des Entwicklers, inklusive vendor/-Verzeichnis
- Kein Build-Prozess auf dem Server, keine Deployment-Dokumentation
- Kein Rollback: Eine fehlerhafte Änderung bleibt live, bis jemand sie findet

Betrieb

- 11 Cronjobs im Hosting-Panel, 3 davon ohne erkennbaren Zweck
- Kein Monitoring: Ausfälle bemerken zuerst die Kunden
- Logdateien ohne Rotation, aktuell 2,4 GB
- Bestellbestätigungen per PHP-mail(), teilweise im Spam

Stiller Fehler gefunden: Der Cronjob `prices:sync` bricht seit März 2026 wegen Zeitüberschreitungen ab, ohne Alarm. Rund 6 % der Artikel zeigen deshalb veraltete Preise.

Ein solider Kern mit ein paar gefährlichen Abkürzungen.

UMFANG

47'500

Zeilen PHP und JavaScript

AUTOMATISIERTE TESTS

0

kein Sicherheitsnetz für Änderungen

WARTBARKEIT

mittel

klar benannt, aber zentrale Logik gebündelt

- **Positiv:** konsequente Laravel-Struktur, verständliche Namen, Geschäftsregeln grösstenteils an einem Ort. Neue Fachpersonen finden sich schnell zurecht.
- **Preislogik gebündelt:** Die gesamte Preisberechnung inklusive Sonderkonditionen steckt in einer Klasse mit 2'100 Zeilen. Funktioniert, ist aber ohne Tests riskant zu ändern.
- **Änderungen im vendor/-Verzeichnis:** Zwei Drittanbieter-Pakete wurden direkt angepasst. Die Anpassungen gehen beim nächsten Paket-Update verloren.
- **Direkte SQL-Abfragen:** 14 Abfragen werden per Textverkettung gebaut, zwei davon mit Benutzereingaben (siehe Kapitel 08).

Woran die Anwendung hängt.

SCHNITTSTELLE	FUNKTIONSWEISE	BEFUND
ERP · Bestellungen	Nächtlicher CSV-Export per SFTP	Keine Prüfung, ob der Import im ERP gelingt. Fehlende Bestellungen fallen erst beim Kunden auf.
ERP · Artikel & Preise	Täglicher CSV-Import	Mapping nur im Code dokumentiert; bricht seit März 2026 teilweise ab (Kapitel 05).
Zahlungsanbieter	Kreditkarte und Rechnung	Veraltete API-Version; der Anbieter hat die Umstellung angekündigt.
E-Mail	PHP-mail() des Hosters	Absender nicht authentifiziert, Zustellung unzuverlässig.

Datenbank: 86 Tabellen, 4,2 GB; grösste Tabelle order_items mit 11 Mio. Einträgen. Keine Hinweise auf inkonsistente Daten.

Offensichtliche Risiken, die sofort auffallen.

Das Assessment ersetzt keinen Penetrationstest. Aufgeführt sind Warnsignale, die bei der Analyse von Code und Betrieb sichtbar wurden.

BEFUND	STUFE
CSV-Exporte mit Kunden- und Bestelldaten in einem öffentlich erreichbaren Verzeichnis	kritisch
Produktive Zugangsdaten (Datenbank, SFTP, E-Mail) in der Konfigurationsdatei im Git-Repository	kritisch
Zwei Abfragen mit Benutzereingaben anfällig für SQL-Injection (Suchfilter, Export)	kritisch
Admin-Login ohne Schutz gegen Passwort-Raten, ohne Zwei-Faktor-Authentifizierung	hoch
jQuery 1.12 mit bekannten XSS-Schwachstellen	mittel

09 · WISSENSRISIKO

Was nur der Vorgänger wusste.

- Deployment-Ablauf und Serverstruktur
- Zuordnung der ERP-Felder beim Export und Import
- Sonderkonditionen für 3 Kundengruppen, fest im Code hinterlegt
- Zweck der 11 Cronjobs
- Zugänge zu Hosting-Konto und Domain

Alles davon wurde im Assessment aus Code, Datenbank und Betrieb rekonstruiert und schriftlich festgehalten.

10 · BUSINESS CONTINUITY

Was bei einem Ausfall passiert.

SZENARIO	HEUTE	ZIEL
Server fällt aus	unklar, mehrere Tage	< 4 Std.
Fehlerhaftes Update	kein Rollback	< 15 Min.
ERP-Export bricht ab	unbemerkt	Alarm sofort
Entwickler fällt aus	Stillstand	jede Fachperson kann übernehmen

Alle Befunde auf einen Blick.

NR.	RISIKO	STUFE
R1	Abschaltung PHP 7.4 ab 31.03.2027	kritisch
R2	Öffentlich abrufbare Kundendaten	kritisch
R3	Zugangsdaten im Repository	kritisch
R4	SQL-Injection in Suchfilter und Export	kritisch
R5	Keine getesteten Backups	hoch
R6	Hosting und Domain auf Privatperson	hoch
R7	Kein Monitoring, stille Fehler	hoch
R8	Admin-Login ungeschützt	hoch
R9	Keine Testumgebung, keine Tests	hoch
R10	ERP-Schnittstelle ohne Kontrolle	mittel
R11	Unversionierte Änderungen auf dem Server und im vendor-/Verzeichnis	mittel
R12	Veraltetes Frontend (jQuery, Vue 2)	mittel
R13	PDF-Erzeugung ohne Wartung	mittel
R14	E-Mail-Zustellung unzuverlässig	niedrig
R15	Logdateien ohne Rotation	niedrig

	KLEIN	MITTEL	GROSS
WAHR-SCHEINLICH	R12	R7 R9	R1 R2 R3 R4
MÖGLICH	R14 R15	R10 R11 R13	R5 R6 R8
SELTEN			

Zeilen: Eintrittswahrscheinlichkeit · Spalten: Auswirkung

ZUSAMMENFASSUNG

4 kritisch 5 hoch 4 mittel 2 niedrig

Acht der neun kritischen und hohen Risiken lassen sich innert 30 Tagen beheben oder deutlich entschärfen.

12 · SOFORTMASSNAHMEN (0–30 TAGE)

Zuerst absichern. Das meiste davon dauert Stunden, nicht Wochen.

NR.	MASSNAHME	ENTSCHÄRFT	ZEITPUNKT
M1	Öffentliche Exporte sperren und ausserhalb des Web-Verzeichnisses ablegen	R2	Tag 1
M2	Alle Zugangsdaten wechseln, aus dem Repository entfernen und im gemeinsamen Passwort-Tresor ablegen	R3	Tag 1
M3	Die zwei SQL-Injection-Stellen schliessen	R4	Woche 1
M4	Tägliche Backups von Datenbank und Dateien an einen zweiten Standort in der Schweiz, Wiederherstellung testen und dokumentieren	R5	Woche 1
M5	Hosting-Konto und Domain auf die Muster AG übertragen	R6	Woche 1–2
M6	Vollständigen Produktionsstand in ein GitHub-Repository der Muster AG überführen, inklusive Dokumentation	R11	Woche 2
M7	Monitoring und Alarmierung für Verfügbarkeit, Fehler, Cronjobs und ERP-Export	R7 R10	Woche 2
M8	Admin-Login mit Zwei-Faktor-Authentifizierung und Schutz gegen Passwort-Raten	R8	Woche 3
M9	Testumgebung (Staging) mit anonymisierten Daten aufbauen	R9	Woche 3–4

13 · EMPFEHLUNGEN (3–12 MONATE)

Danach modernisieren, im laufenden Betrieb.

- **Sicherheitsnetz:** automatisierte Tests für die 12 geschäftskritischen Abläufe (Login, Preisberechnung, Bestellung, ERP-Export).
- **Upgrade:** PHP 8.4 und aktuelle Laravel-Version in mehreren Zwischenschritten, jeder einzeln getestet und ausgeliefert.
- **Datenbank:** Umzug auf MySQL 8.4 LTS mit Probelauf auf Staging.
- **Deployment:** automatisiert über GitHub, mit Staging-Freigabe und Rollback per Knopfdruck.
- **Schnittstellen:** ERP-Export mit Prüfung, Protokoll und Alarm; Zahlungsanbieter auf aktuelle API.
- **Altlasten:** wkhtmltopdf ersetzen, jQuery aktualisieren, Vue 2 schrittweise auf Vue 3.

Vier Wege. Einer passt.

A · Weiterbetreiben	Nur Sofortmassnahmen, PHP 7.4 über ein kostenpflichtiges Legacy-Angebot des Hosters verlängern. Günstig, aber die Sicherheitslücken bleiben und der Versionssprung wird jedes Jahr grösser.	NICHT EMPFOHLEN
B · Stabilisieren & modernisieren	Zuerst absichern, dann Upgrade in Etappen bei laufendem Betrieb. Die bewährte Fachlogik bleibt erhalten, das Risiko sinkt mit jeder Etappe. Abschluss vor der Abschaltung.	EMPFOHLEN
C · Teile ersetzen	Zum Beispiel das Frontend neu bauen und das Backend behalten. Sinnvoll erst, wenn nach Etappe 3 neue Anforderungen an die Bedienung dazukommen.	SPÄTER PRÜFEN
D · Komplette neu bauen	Geschätzt CHF 180'000 bis 250'000 und 9 bis 12 Monate. Nicht vor der Abschaltung fertig, und die über Jahre gewachsenen Sonderregeln müssten neu erfasst werden.	NICHT NÖTIG

15 · UMSETZUNGSVORSCHLAG

Option B in drei Etappen, jede zum Fixpreis.

ETAPPE	INHALT	ZEITRAUM	FIXPREIS
1 · Absichern	Sofortmassnahmen M1 bis M9	Oktober 2026	CHF 7'400
2 · Sicherheitsnetz	Tests für kritische Abläufe, automatisiertes Deployment, Laravel bis Version 8	Nov. 2026	CHF 9'800
3 · Modernisieren	PHP 8.4, aktuelle Laravel-Version, MySQL 8.4, Zahlungs-API	Dez. 2026 – Feb. 2027	CHF 14'600
Total Etappen 1 bis 3			CHF 31'800

Betreuung ab Etappe 1: CHF 1'100 pro Monat für Monitoring, Updates und Weiterentwicklung (4 Stunden inklusive), Reaktion am nächsten Arbeitstag, Notfälle priorisiert. Beträge exkl. MWST.

Was jetzt passiert.

1. **Besprechung des Reports** (60 Minuten) mit Geschäftsleitung und Innendienst, Fragen klären.
2. **Entscheid über die Option** bis 15. Oktober 2026.
3. **Start Etappe 1** in der Woche nach dem Entscheid, erste Massnahmen am ersten Tag.

Kein neuer Single Point of Failure

Die Übernahme soll die Abhängigkeit von einer einzelnen Person auflösen, nicht verschieben. Deshalb gilt ab dem ersten Tag:

CODE & DOKUMENTATION

Jede Zeile Code und die gesamte Dokumentation liegen im GitHub-Repository der Muster AG. Die Muster AG hat jederzeit vollen Zugriff.

ZUGANGSDATEN

Alle Zugänge (Hosting, Datenbank, Domain, Drittanbieter) liegen in einem gemeinsamen Passwort-Tresor, auf den die Muster AG jederzeit Zugriff hat. Nie im Code.

BETRIEB

Deployment, Backups und Wiederherstellung sind als Schritt-für-Schritt-Anleitungen dokumentiert. Eine andere Fachperson kann jederzeit übernehmen.

EIGENTUM

Hosting-Konto, Domain und alle Lizenzen laufen auf die Muster AG. Keine Lizenz-Miete, kein Lock-in.



Dimitri König

Unique-P GmbH · hallo@unique-p.ch · +41 76 231 32 71 · unique-p.ch

Beispiel-Report: Firma, Anwendung, Befunde und Beträge sind fiktiv. So sieht der Report aus, den du nach einem Übernahme-Assessment erhältst: für deine Anwendung, mit deinen Zahlen. Starte mit dem kostenlosen Fit-Check auf unique-p.ch/leistungen/webapplikation-uebernehmen.