



GAMBIO PRAXIS-HANDBUCH

Band 6

Wartung und Sicherheit

Backups, Updates, Diagnose und Schutz im laufenden Shopbetrieb

Zielgruppe	Shopbetreiber, Administratoren, Entwickler und technische Betreuer
Ausrichtung	Gambio 5.x; selbstgehostete und Cloud-basierte Shops
Stand	06.08.2026
Herausgeber	Gambio-Tuning - Torsten Lewe

Eigenständig formulierte Arbeitshilfe. Keine offizielle Veröffentlichung der Gambio GmbH.

0 So ist dieses Handbuch aufgebaut

Backups, Updates, Diagnose und Schutz im laufenden Shopbetrieb

Dieser Band orientiert sich an der öffentlich sichtbaren Gliederung und an ausgewählten Funktionsbeschreibungen des Gambio Entwickler-Handbuchs. Die Texte wurden für den praktischen Einsatz neu formuliert, zusammengefasst und um eigene Prüf-, Sicherheits- und Arbeitsabläufe ergänzt. Dieser Band behandelt schwerpunktmäßig: Toolbox, Cache, Datensicherung, Logs, Server Info, SQL, zeitgesteuerte Aufgaben sowie Sicherheits- und Updatepraxis.

VERSIONSHINWEIS: Menübezeichnungen und verfügbare Funktionen können je nach Shopversion, Theme, installierten Paketen sowie Cloud- oder Selbsthosting-Variante abweichen. Bei Unterschieden gilt die Bezeichnung in deinem aktuellen Gambio Admin.

Empfohlene Arbeitsweise

- | | |
|----------|---|
| 1 | Arbeitsschritt 1
Änderungen zuerst dokumentieren und bei kritischen Bereichen eine Sicherung anlegen. |
| 2 | Arbeitsschritt 2
Nur einen zusammengehörigen Bereich nach dem anderen bearbeiten. |
| 3 | Arbeitsschritt 3
Nach dem Speichern die Darstellung oder Funktion im Shopbereich prüfen. |
| 4 | Arbeitsschritt 4
Abhängigkeiten zu Modulen, Kundengruppen, Steuern, Versand und Cache beachten. |
| 5 | Arbeitsschritt 5
Die Abschlusscheckliste nutzen und offene Punkte schriftlich festhalten. |

PRAXIS: Bei produktiven Shops sollten Änderungen möglichst in einem ruhigen Zeitfenster oder zuerst in einer Testumgebung erfolgen.

Inhaltsübersicht

1. Verantwortung bei Cloud und Selbsthosting
2. Sicherungsstrategie
3. Wiederherstellung testen
4. Updates sicher vorbereiten
5. Update durchführen und nachprüfen
6. Cache richtig einsetzen
7. Logs und Serverinformationen
8. Konten, Passwörter und Zugänge
9. Dateien, Server und Schutzfunktionen
10. Monitoring und zeitgesteuerte Aufgaben
11. Sicherheitsvorfall und Notfallplan
12. **Abschlusscheckliste**
13. Schnellübersicht und Quellenhinweis

HINWEIS: Die Kapitel sind als eigenständige Arbeitsschritte aufgebaut. Bei umfangreichen Änderungen empfiehlt sich dennoch die Reihenfolge dieses Bandes.

1 Verantwortung bei Cloud und Selbsthosting

Wartungsaufgaben unterscheiden sich je nach Betriebsmodell. Im Cloud-Shop übernimmt Gambio Teile der technischen Plattformpflege; bei Selbsthosting liegen Server, Dateien, Datenbank und Wiederherstellung stärker beim Betreiber.

Verantwortungsbereiche

Bereich	Praxisregel
Cloud-Shop	Paketabhängige Updates und Plattformbetrieb durch Anbieter; Shopkonfiguration bleibt Betreiberaufgabe
Selbsthosting	Hosting, PHP, Dateien, Datenbank, Backups und Shopupdates koordinieren
Beide Varianten	Konten, Module, Inhalte, Zahlungen, Datenschutz und Funktionsprüfung

VERTRAG PRÜFEN: Maßgeblich sind dein Hosting- oder Cloud-Vertrag und die aktuell gebuchten Leistungen.

2 Sicherungsstrategie

MENÜPFAD

Toolbox > Datensicherung / Hosting-Backup

Eine Sicherung ist nur dann wertvoll, wenn sie vollständig, geschützt, aktuell und wiederherstellbar ist. Für einen selbstgehosteten Shop gehören Dateien und Datenbank zusammen.

3-2-1-Grundidee

- Mindestens drei Kopien wichtiger Daten
- Auf mindestens zwei unterschiedlichen Speichermedien oder Systemen
- Mindestens eine Kopie getrennt vom Produktivserver
- Automatische Sicherungen plus manuelle Sicherung vor Änderungen
- Aufbewahrungsfristen und Löschung dokumentieren

ZUGANGSDATEN: Sicherungen können Kundendaten und Zugangsinformationen enthalten. Speichere sie verschlüsselt und beschränke den Zugriff.

3 Wiederherstellung testen

Ein Backup ohne Wiederherstellungstest ist nur eine Annahme. Teste regelmäßig, ob Dateien und Datenbank zusammenpassen und der Shop in einer isolierten Umgebung startet.

Testablauf

1	Schritt 1 Geeignete Sicherung und Zeitpunkt auswählen.
2	Schritt 2 Isolierte Testumgebung vorbereiten.
3	Schritt 3 Dateien und Datenbank entsprechend dokumentiert einspielen.
4	Schritt 4 Konfiguration, URLs und Zugangsschutz anpassen.
5	Schritt 5 Login, Artikel, Suche, Warenkorb und Bestellung prüfen.
6	Schritt 6 Test und festgestellte Lücken dokumentieren.

PRODUKTIVDATEN: Beim Zurückspielen in den Live-Shop gehen alle seit dem Sicherungszeitpunkt entstandenen Bestellungen und Änderungen verloren. Vorher Shop offline stellen und aktuelle Daten gesondert sichern.

4 Updates sicher vorbereiten

MENÜPFAD

Gambio Store / Updatepaket des Herstellers

Updates beheben Fehler und Sicherheitslücken, können aber Anpassungen und Module beeinflussen. Verwende nur den für deine Version vorgesehenen Updatepfad.

Vor dem Update

- ☐ Ziel- und Ausgangsversion dokumentiert
- ☐ Systemvoraussetzungen erfüllt
- ☐ Changelog und Hinweise gelesen
- ☐ Module und Anpassungen auf Kompatibilität geprüft
- ☐ Vollständige Dateien- und Datenbanksicherung erstellt
- ☐ Wartungsfenster und Verantwortlicher festgelegt
- ☐ Rückfallplan vorhanden

SPRUNGVERSIONEN: Überspringe keine vorgeschriebenen Zwischenupdates. Beachte die Reihenfolge und Hinweise des jeweiligen Updatepakets.

5 Update durchführen und nachprüfen

Während eines Updates dürfen keine parallelen Änderungen stattfinden. Nach Abschluss ist eine strukturierte Funktionsprüfung wichtiger als die bloße Erfolgsmeldung des Updaters.

Ablauf

1	Schritt 1 Shop in den vorgesehenen Wartungs- oder Offlinezustand versetzen.
2	Schritt 2 Update exakt nach Herstelleranleitung durchführen.
3	Schritt 3 Fehlermeldungen und Protokolle sichern.
4	Schritt 4 Caches nach Vorgabe leeren oder neu erzeugen.
5	Schritt 5 Admin, Shop, Login, Suche, Warenkorb und Checkout testen.
6	Schritt 6 Zahlung, Versand, E-Mail und wichtige Module prüfen.
7	Schritt 7 Shop freigeben und erste Stunden überwachen.

KEINE LIVE-EXPERIMENTE: Bei einem Fehler nicht wahllos Dateien austauschen oder Datenbankbefehle ausführen. Erst Status sichern, Ursache eingrenzen und Rückfallentscheidung treffen.

6 Cache richtig einsetzen

MENÜPFAD Toolbox > Cache

Caches beschleunigen den Shop, können nach Änderungen aber veraltete Inhalte anzeigen. Leere nur die zur Änderung passenden Cachebereiche und prüfe anschließend mehrere Seitentypen.

Typische Anlässe

Bereich	Praxisregel
Artikel / Kategorien	Zuordnungs- und Seitencache nach umfangreichen Änderungen
Module	Modulinformationen nach Installation oder Konfiguration
Theme / Inhalte	Seitenausgabe und Template-bezogene Caches
Texte	Text- oder Sprachcache nach Textänderungen
Fehlersuche	Kontrolliert leeren, nicht als dauerhafte Problemlösung

PERFORMANCE: Permanentes Deaktivieren von Caches kann die Last erhöhen und verdeckt die eigentliche Ursache nicht.

7 Logs und Serverinformationen

MENÜPFAD

Toolbox > Logs anzeigen / Server Info

Logs liefern Zeit, Datei, Fehlertyp und Kontext. Sie sollten vor Änderungen gesichert werden, weil Rotation oder Cachebereinigung wichtige Hinweise entfernen kann.

Fehler eingrenzen

1	Schritt 1 Genaue Uhrzeit und reproduzierbaren Ablauf notieren.
2	Schritt 2 Passendes Shop-, PHP- oder Serverlog öffnen.
3	Schritt 3 Erste relevante Fehlermeldung statt Folgefehler identifizieren.
4	Schritt 4 Zuletzt geänderte Module, Dateien oder Einstellungen vergleichen.
5	Schritt 5 Fehler in Testumgebung reproduzieren.
6	Schritt 6 Lösung und betroffene Version dokumentieren.

DATENSCHUTZ: Logs können IP-Adressen, Pfade, Bestell- oder Kundendaten enthalten. Teile nur notwendige und geschützte Auszüge.

8 Konten, Passwörter und Zugänge

Admin-, Hosting-, FTP-, SSH-, Datenbank- und Zahlungszugänge gehören zu den kritischsten Schutzobjekten. Ein kompromittierter Zugang kann den gesamten Shop betreffen.

Schutzmaßnahmen

- [] Einzigartige, lange Passwörter und Passwortmanager
- [] Zwei-Faktor-Authentifizierung, wo verfügbar
- [] Persönliche statt gemeinsam genutzter Konten
- [] Nur erforderliche FTP-, SSH- und Datenbankrechte
- [] Zugänge nach Projekt- oder Personalende widerrufen
- [] Notfallkontakte und Wiederherstellungscodes geschützt ablegen

E-MAIL-KONTO: Schütze besonders die Administrator-E-Mail-Adresse. Wer das Postfach kontrolliert, kann häufig Passwörter zurücksetzen.

9 Dateien, Server und Schutzfunktionen

MENÜPFAD

Hosting-Verwaltung / Konfiguration > G-Protector

Selbstgehostete Shops benötigen ein gepflegtes Betriebssystem, unterstützte PHP-Version, sichere Dateirechte und eine saubere Webserverkonfiguration. Schutzfunktionen dürfen Updates und Checkout nicht blockieren.

Technische Basis

Bereich	Praxisregel
PHP / Datenbank	Unterstützte Versionen, aktuelle Sicherheitsupdates
HTTPS	Gültiges Zertifikat und sichere Weiterleitung
Dateirechte	So restriktiv wie funktionsfähig, keine unnötige Schreibbarkeit
G-Protector / WAF	Aktivieren, testen und Ausnahmen dokumentieren
Verzeichnisse	Backups, Exporte und Logs nicht öffentlich erreichbar

HOSTING: Serveränderungen nur durchführen, wenn Wiederherstellung, Konfiguration und Auswirkungen bekannt sind.

10 Monitoring und zeitgesteuerte Aufgaben

MENÜPFAD

Toolbox > Zeitgesteuerte Aufgaben / Hosting-Cronjobs

Automatische Aufgaben müssen regelmäßig ausgeführt und überwacht werden. Fehlerhafte Cronjobs können Exporte, Newsletter, Schnittstellen oder Wartungsprozesse unbemerkt stoppen.

Überwachung

- Erreichbarkeit und HTTPS-Zertifikat
- Fehlerrate und Serverressourcen
- Cronjob-Ausführung und letzte erfolgreiche Laufzeit
- Freier Speicherplatz und Backupstatus
- Zahlungs- und Versandrückmeldungen
- Ungewöhnliche Anmelde- oder Bestellmuster

ALARMIERUNG: Ein Monitoring ohne erreichbaren Empfänger hilft nicht. Teste regelmäßig, ob Warnungen zugestellt und bearbeitet werden.

11 Sicherheitsvorfall und Notfallplan

Bei einem vermuteten Angriff zählt ein geordneter Ablauf. Spuren dürfen nicht durch hektische Bereinigung vernichtet werden, gleichzeitig muss weiterer Schaden begrenzt werden.

Erste Reaktion

1	Schritt 1 Vorfalzeit, Symptome und betroffene Systeme dokumentieren.
2	Schritt 2 Zugriff kontrolliert begrenzen und verantwortliche Personen informieren.
3	Schritt 3 Logs, verdächtige Dateien und Systemzustand sichern.
4	Schritt 4 Zugangsdaten über ein sauberes System ändern.
5	Schritt 5 Ursache und Umfang fachgerecht untersuchen.
6	Schritt 6 Saubere Wiederherstellung und vollständige Tests durchführen.
7	Schritt 7 Melde- und Informationspflichten prüfen.
BEWEISSICHERUNG: Lösche verdächtige Dateien nicht sofort ohne Kopie und Dokumentation. Für Analyse und mögliche rechtliche Schritte können sie wichtig sein.	

12 Abschlusscheckliste

Nutze die folgende Liste nach der Bearbeitung dieses Bandes. Ergänze in der rechten Spalte Ergebnisse, Abweichungen oder notwendige Nacharbeiten.

Nr.	Prüfpunkt	Ergebnis / Notiz
1	Betriebsmodell und Verantwortlichkeiten sind dokumentiert	
2	Automatische und manuelle Sicherungen sind eingerichtet	
3	Dateien und Datenbank werden gemeinsam gesichert	
4	Backups sind verschlüsselt und getrennt gespeichert	
5	Wiederherstellung wurde erfolgreich getestet	
6	Updateweg und unterstützte Versionen sind bekannt	
7	Vor Updates wird vollständige Sicherung erstellt	
8	Module und Anpassungen werden auf Kompatibilität geprüft	
9	Update-Nachtest umfasst Checkout und E-Mail	
10	Cachebereiche werden gezielt behandelt	
11	Logs werden bei Fehlern vor Änderungen gesichert	
12	Serverinformationen und Ressourcen werden überwacht	
13	Admin- und Hostingkonten sind persönlich	
14	Zwei-Faktor-Authentifizierung ist eingesetzt	
15	FTP-, SSH- und Datenbankrechte sind begrenzt	
16	HTTPS-Zertifikat ist gültig	
17	PHP und Serverkomponenten werden unterstützt	
18	Backups und Exporte sind nicht öffentlich erreichbar	
19	Cronjobs und automatische Aufgaben werden überwacht	
20	Notfall- und Sicherheitsvorfallplan ist vorhanden	

13 Schnellübersicht und Quellenhinweis

Wichtige Menüpfade

Aufgabe	Menüpfad / Bereich
Datensicherung	Toolbox > Datensicherung / Hosting-Backup
Cache	Toolbox > Cache
Logs	Toolbox > Logs anzeigen
Server Info	Toolbox > Server Info
SQL	Toolbox > SQL - nur für Fachkundige
Zeitgesteuerte Aufgaben	Toolbox > Zeitgesteuerte Aufgaben
Shop online/offline	Inhalte > Shop online/offline
G-Protector	Konfiguration > G-Protector
Updates	Gambio Store / offizielles Updatepaket
Admin-Konten	Kunden > Administratoren / Berechtigungen

Bearbeitungsgrundlage

Dieses Praxis-Handbuch orientiert sich an der öffentlich zugänglichen Struktur des Gambio Entwickler-Handbuchs, insbesondere an den Bereichen Toolbox, Cache, Datensicherung, Logs, Server Info, SQL, zeitgesteuerte Aufgaben sowie Sicherheits- und Updatepraxis. Abrufdatum: 06.08.2026.

Quelle: developers.gambio.de/manual.html

URHEBERRECHT: Die Inhalte dieses Praxis-Handbuchs wurden eigenständig formuliert. Original-Screenshots und längere Originalpassagen des offiziellen Gambio-Handbuchs wurden nicht übernommen. Das offizielle Handbuch ist urheberrechtlich geschützt.

Kontakt Gambio-Tuning

Gambio-Tuning

Telefon: 02954 - 977 90 40
E-Mail: bestellung@gambio-tuning.de
Web: www.gambio-tuning.de

Ende Band 6 - Wartung und Sicherheit