

Generelles

Fachpersonal einbeziehen

Für ein sicheres und fachgerechtes Update ist der Einsatz und die Einbeziehung von erfahrenem Fachpersonal unerlässlich, um einen störungsfreien und regelkonformen Ablauf sicherzustellen.

Zu jeder neuen Version stellen wir auch sogenannte Release Notes zur Verfügung, in denen alle relevanten Änderungen, neue Funktionen sowie potenzielle Auswirkungen dokumentiert sind.

Diese Informationen sollten an das zuständige Fachpersonal weitergeleitet werden. Zudem ist es empfehlenswert, das Fachpersonal als technische Ansprechpersonen in der Plattform zu hinterlegen, um einen reibungslosen Informationsfluss sicherzustellen.

Versionsverwaltung sicherstellen

Verwenden Sie eine Versionierungssoftware – insbesondere bei Updates ist es entscheidend, Änderungen im Problemfall schnell rückgängig machen zu können.

Eine Versionierungssoftware wie Git ermöglicht es, Änderungen am Code oder an Dateien lückenlos nachzuvollziehen und verschiedene Versionen gezielt zu verwalten. So kann jederzeit ein früherer, stabiler Zustand wiederhergestellt werden.

Vor dem Einspielen in das Produktivsystem

Führen Sie Sicherheitsupdates zunächst in einer lokalen Entwicklungsumgebung durch. So lassen sich erste Probleme frühzeitig erkennen, bevor sie auf ein Test- oder Live-System treffen.

In den Release Notes auf der Kundenplattform wird auf besondere Änderungen hingewiesen, beispielsweise neue Einstellungsmöglichkeiten sowie deren potenzielle Auswirkungen.

Web <https://kunden.safefive.de/downloads>

Bei komplexeren Anpassungen kann zudem eine kurze Bedienungsanleitung enthalten sein. Es wird empfohlen, die Release Notes sorgfältig zu prüfen.

Tests im Testsystem durchführen

Nutzen Sie eine Testumgebung (Staging) – das ist eine möglichst exakte Kopie Ihres Live-Systems, in der reale Bedingungen simuliert werden können.

Ziel ist es, potenzielle Fehler zu identifizieren, bevor sie sich auf den laufenden Betrieb auswirken.

Standardprozesse testen

Stellen Sie sicher, dass zentrale Abläufe im Shop nach dem Update weiterhin reibungslos funktionieren.

Prüfen Sie insbesondere:

- **Bestellvorgang**
- **Kontaktformular**
- **Registrierung und Login**
- **Produktsuche**
- **Zahlungsarten und Versandoptionen**
- **sowie alle weiteren Prozesse, die für den Betrieb Ihres Shops relevant sind**

Einspielen in das Produktivsystem

Backups erstellen

Sichern Sie sowohl Ihre Dateien als auch die Datenbank, um im Notfall auf eine funktionierende Version zurückgreifen zu können. Testen Sie Ihre Backups regelmäßig – besonders bei Datenbanken –, um sicherzustellen, dass eine Wiederherstellung im Ernstfall reibungslos funktioniert

Bitte aktualisieren Sie das Plugin wie gewohnt auf sicherem Weg – etwa per ZIP im Admin, über den Plugin-Update-Prozess oder mit Ihren üblichen sicheren Deployment-Methoden.

Nach dem Einspielen in das Produktivsystem

Standardprozesse erneut prüfen

Testen Sie die oben genannten Kernfunktionen nochmals im Live-System – auch wenn sie im Testsystem funktioniert haben.

Drittanbieter besonders beobachten

Beachten Sie, dass Zahlungsanbieter und andere Drittanbieter-Dienste sich im Live-System anders verhalten können als in Testumgebungen – oder dort überhaupt erst aktiv sind.

E-Mails und Cronjobs prüfen

Stellen Sie sicher, dass automatische Prozesse wie E-Mail-Benachrichtigungen und Cronjobs wie erwartet laufen. Kontrollieren Sie z. B. Bestellbestätigungen und Versandbenachrichtigungen.

Maßnahmen bei Problemen

Nach einem Sicherheitsupdate kann es in bestimmten Konstellationen vorkommen, dass einzelne Funktionen nicht wie gewohnt mit bestimmten Plugins oder Drittanbieterdiensten zusammenarbeiten. Deshalb sollten Sie nach einem Update unbedingt prüfen, ob alle wichtigen Bereiche Ihres Shops weiterhin einwandfrei funktionieren. Falls es zu Problemen kommt, gehen Sie wie folgt vor:

1. Feature gezielt deaktivieren

In der Plugin-Konfiguration können Sie einzelne Funktionen mithilfe von Feature-Flags flexibel steuern.

Pfad: **Plugin** > **Safefive-Sicherheitsplugin** > **Konfiguration** > **Sicherheitseinstellungen**

Über die jeweiligen Schieberegler lassen sich Sicherheitsfeatures aktivieren oder deaktivieren – je nach Bedarf und Kompatibilität Ihrer Systemumgebung.

2. Sicherheits-Einstellung anpassen

Unter **Plugin** > **Safefive-Sicherheitsplugin** > **Konfiguration** > **Sicherheitseinstellungen**

haben Sie die Möglichkeit, weiterführende Sicherheitseinstellungen vorzunehmen, die je nach Update zur Verfügung stehen. Relevante Informationen zu den Inhalten und Konfigurationsmöglichkeiten der einzelnen Updates finden Sie auf der safefive-Kundenplattform unter dem Menüpunkt „Sicherheitsplugin und Patches“:

Web <https://kunden.safefive.de/downloads>

Wählen Sie dort die entsprechende Version aus und klicken Sie auf „**Dokumentation anzeigen**“, um weitere Details zu erhalten.

Ob eine Konfiguration für eine bestimmte Version erforderlich ist, erkennen Sie am jeweiligen Tag mit dem Hinweis „**needs-configuration**“.

3. Cookie-Sicherheit: Umstellung von “Lax” auf “Strict”

Ab Version 1.4.1 können Sie in den Sicherheitseinstellungen beispielsweise strengere Cookie-Einstellungen aktivieren. Diese erhöhen das Sicherheitsniveau, können jedoch die Funktionsweise bestimmter Dienste einschränken – insbesondere bei:

- **Zahlungsanbietern**
- **Single Sign-On-Diensten (Facebook, Google, Amazon)**
- **Eigenen SSO-Lösungen**

Hinweis

Sollten z. B. Zahlungsfunktionen oder Logins nicht wie erwartet funktionieren, ändern Sie die Einstellung von **SameSite=Strict** auf **SameSite=Lax**

4. Kontaktieren Sie uns bei anhaltenden Problemen

Wenn sich Probleme nicht durch die oben genannten Maßnahmen lösen lassen, senden Sie uns bitte folgende Informationen per E-Mail:

- **Welche genauen einzelnen Schritte sind nötig, um den Fehler auszulösen?**
- **Welches Verhalten hatten Sie erwartet?**
- **Welches Verhalten hat sich stattdessen gezeigt?**
- **Welche Shopware-Version verwenden Sie?**

Über Shopware - Wie wurde Shopware installiert?

- **Es gibt mindestens drei Arten um Shopware zu installieren:**
 - ZIP Datei heruntergeladen und damit installiert
 - composer als create-project, d.h. Shopware ist eine Abhängigkeit
 - composer, aber als Kopie des Shopware 5 Repositories
- **Welche Plugins sind aktiv? (gern mit Screenshot aus dem Plugin-Manager)**
- **Welche Version unseres Plugins ist installiert?**
Die Version finden Sie im Plugin Manager in der Spalte Version.
- **Wurden manuelle Änderungen am Shopware-System vorgenommen?**

Zusätzliche Hinweise und Hilfestellungen finden Sie auch auf der Kunden-Troubleshooting-Seite unter:

Web <https://safefive.de/kunden-troubleshooting/>

Je vollständiger Ihre Angaben sind, desto besser können wir Sie bei der Lösung unterstützen.

Bei weiteren Fragen stehen wir Ihnen jederzeit gerne unter info@safefive.de zur Verfügung.