Wichtige Sicherheitsempfehlungen für Zen Cart

Nach erfolgreicher Installation des Shops sind folgende Maßnahmen empfohlen, um die Sicherheit des Shops zu erhöhen.

Generell

Betreiben Sie Ihren Onlineshop NICHT OHNE SSL!

Ihre Kunden können erwarten, dass ihre Daten beim Konto erstellen, Login, Daten ändern und im Bestellablauf nicht völlig unverschlüsselt übertragen werden. Empfohlen ist ein „echtes“ auf Ihre Domain ausgestelltes SSL Zertifikat, kein Shared SSL!
In Zeiten von Lets Encrypt sollte keine Website mehr ohne SSL betrieben werden.
Auch für Ihre Zen Cart Administration ist SSL eine ganz wesentliche Absicherung.
Empfohlen ist, https nicht nur für Login und Checkout zu verwenden, sondern den gesamten Shop durchgehend per https erreichbar zu machen, siehe dazu:
https://www.zen-cart-pro.at/knowledgebase/wie-stelle-ich-zen-cart-deutsch-komplett-auf-ssl-um/

Übertragen Sie Daten per FTP nur per SFTP oder FTPS

Per normalem FTP werden die Daten unverschlüsselt übertragen. Sollte Ihr Provider keine SFTP oder FTPS Übertragung unterstützen, stellt sich die Frage, ob der Provider für Ihren Onlineshop wirklich geeignet ist.

Legen Sie die Ordner pdf und logs auf eine Ebene oberhalb des www

Damit Logfiles mit sensiblen Informationen oder pdf Rechnungen keinesfalls überhaupt per Browser aufrufbar sind, legen Sie die Ordner auf eine Ebene oberhalb des www und geben den Pfad zum logs Ordner in den beiden configure.php entsprechend an. Den Pfad zu den pdf Rechnungen geben Sie in der Konfiguration der pdf Rechnung entsprechend an.
Sollte Ihr Provider das Anlegen von Ordner unterhalb des www nicht unterstützen, stellt sich die Frage, ob der Provider für Ihren Onlineshop wirklich geeignet ist.

Wichtige Sicherheitsempfehlungen

1. Löschen Sie das Installationsverzeichnis zc_install und

andere nicht benötigte Dateien und Ordner

Der Ordner zc_install wird am Server nicht mehr benötigt und sollte komplett gelöscht werden. Falls Sie ihn nach der Installation nur umbenannt und nicht gelöscht haben: Nicht umbenennen und am Server lassen, sondern komplett löschen!

Löschen Sie auch folgende Datei, falls Sie die hochgeladen haben:
– install.txt

Falls Sie in Ihrem Shop keine Downloads oder Musikdateien anbieten werden, können Sie nun auch die folgenden Ordner löschen:
– download
– media
– pub
Damit Sie keine Warnmeldung über den fehlenden Downloadordner bekommen, müssen Sie danach in der Administration unter Konfiguration > Attributeinstellungen „Downloads aktivieren“ auf false stellen.
Sollten Sie später einmal Downloads anbieten wollen, müssen Sie diese Ordner wieder hochladen und ihnen die entsprechenden Berechtigungen geben.

Hinweis:
In älteren Zen Cart Versionen konnte der Ordner extras gelöscht werden. Seit Zen Cart 1.5.3 deutsch diesen Ordner keinesfalls löschen, da er für die Funktionalität benötigt wird!

2. Setzen Sie einen Schreibschutz für die beiden configure.php

Die beiden Zen Cart Konfigurationsdateien sollten nachdem Sie darin alle gewünschten Änderungen vorgenommen haben, nicht mehr am Server änderbar sein.
Daher müssen sie mit einem Schreibschutz versehen werden. Normalerweise wird das vom Installationsprogramm automatisch gemacht.
Wenn sich Ihr Shop auf einem Linux-Server befindet, setzen Sie den Schreibschutz mit Ihrem FTP Programm und geben folgenden Dateien den Befehl chmod 444
includes/configure.php
DEINADMIN/includes/configure.php

3. Verwenden Sie als Emailtransportmethode smtpauth oder smtp

Unter Konfiguration > Emailoptionen können Sie einstellen, wie Ihr Shop Emails versenden soll. Standardmäßig ist hier meist PHP eingestellt, damit der Shop direkt einsatzbereit ist.
Es ist wesentlich besser, die Emails über einen SMTP Server versenden zu lassen. Zum einen reduziert das die Wahrscheinlichkeit, dass Emails bei Ihren Kunden im Spamordner landen. Zum anderen ist es bei Versand über PHP je nach Serverkonfiguration möglich, dass bei Mails aus dem Adminbereich (z.B. Bestellstatusupdates) der Name Ihres admin Verzeichnisses im Mail auslesbar ist.
Daher stellen Sie um auf smtpauth und geben weiter unten in

der Konfiguration den Namen Ihres SMTP Servers und eine gültigen Usernamen/Passwort dazu ein.

4. Löschen Sie alle nicht benötigten Admin Accounts

Haben Sie mehrere Administratoren angelegt? Werden wirklich mehrere Admin Accounts verwendet? Sind die zusätzlichen Admin Accounts wirklich nötig? Gibt es noch einen Adminaccount namens Demo?
Überprüfen Sie, ob mehrere Admins angelegt sind und löschen Sie nicht unbedingt benötigte Administratoren.
Seit Zen Cart 1.5 finden Sie das unter Admin > Admin Benutzerechte > Adminbenutzer

5. Verwenden Sie sichere Passwörter

Das Passwort für Ihren Admin Account sollte mindestens 8 Zeichen lang sein und am besten aus einer Ziffern-, Buchstaben-Kombination bestehen. Verwenden Sie auch Groß- und Kleinschreibung. Verwenden Sie keine „normalen“ Wörter, die einen Sinn ergeben.
In Zen Cart 1.5.x und höher werden Sie alle 90 Tage automatisch aufgefordert, Ihr Passwort zu änden.
Passwortänderung in Zen Cart 1.5.6 und höher unter Admin > Administratoren > Admin User > Passwort zurücksetzen
Diese Passwortempfehlungen gelten genauso für Ihren FTP User oder das Passwort zum Zugang zu phpMyAdmin. Verwenden Sie auch hier sichere Passwörter!

6. Versehen Sie Ihre define pages mit einem Schreibschutz

Damit Sie unter Admin > Tools > Seiteneditor Ihre Define Pages online bearbeiten können, mussten Sie diesen Dateien Schreibrechte geben.
Die Dateien befinden sich im Ordner includes/languages/german/html_includes
Falls Sie weitere Sprachen einsetzen im entsprechenden Sprachverzeichnis, z.B. includes/languages/english/html_includes
Wenn Sie mit dem Editieren Ihrer Seiten fertig sind, setzen Sie auf all diese Dateien wieder einen Scheibschutz mit chmod 644.
Wenn Sie später wieder über den Seiteneditor im Adminbereich Änderungen an diesen Seiten vornehmen wollen, müssen Sie natürlich wieder per FTP den entsprechenden Dateien Schreibrechte geben (z.B. chmod 666)

7. Verwenden Sie die mitgelieferten .htaccess und index.html Dateien

In verschiedenen Verzeichnissen der Zen Cart Installation befinden sich .htaccess Dateien und index.html Dateien.
Löschen Sie diese Dateien nicht! V.a. die verschiedenen .htaccess Dateien z.B. im admin Verzeichnis oder im includes Verzeichnis sind für die Sicherheit Ihres Shops sehr wichtig!
Die leeren index.html Dateien dienen dazu, dass beim Aufruf des Verzeichnisses nicht der Inhalt angezeigt wird.

Noch sicherer ist es, dazu zusätzlich eine .htaccess Datei zu erstellen und sie in Verzeichnisse mit einer index.html zu legen.

Diese .htaccess könnte folgenden Inhalt haben:

```
#.htaccess to prevent unauthorized directory browsing or access to .php files
IndexIgnore */*
<Files *.php>
Order Deny,Allow
Deny from all
</Files>
```

Manche Provider erlauben das manuelle Erstellen von .htaccess Dateien nicht oder benötigen andere Settings als die in obigem Beispiel.
Nehmen Sie bei Unklarheiten oder Schwierigkeiten mit Ihrem Provider Kontakt auf, um die besten Einstellungen für Ihr System zu ermitteln.

8. Schützen Sie das images Verzeichnis

Während der Zen Cart Installation wurde empfohlen, dem images Verzeichnis Schreibrechte zu geben (chmod 777).
Das dient dazu, dass Sie in der Lage sind, über das Adminmenü Bilder hochzuladen.
Wenn Sie Ihren Shop fertig eingerichtet haben, ist es besser, das images Verzeichnis wieder auf chmod 755 zurückzustellen.

Dadurch haben Hacker nicht die Möglichkeit, zu versuchen, schadhaften Code in Ihr images Verzeichnis einzuschleusen.
Stellen Sie daher die Rechte des images Verzeichnisses und der Unterordner darin von chmod 777 auf chmod 755.
Ähnlich wie bei Empfehlung 6 (Versehen Sie Ihre define pages mit einem Schreibschutz) müssen Sie dann später möglicherweise wieder auf 777 stellen, bevor Sie über das Adminmenü weitere Bilder hochladen können.

Sollte bei Ihrem Provider PHP als CGI-Modul laufen, ist folgende .htaccess Datei für das images Verzeichnis empfehlenswert:

```
# Prevent directory viewing and the ability of any scripts to run.
# No script, be it PHP, PERL or whatever, can normally be executed if ExecCGI is disabled.
OPTIONS -Indexes -ExecCGI
```


9. Hinweise zu Schreibrechten für verschiedene Ordner

Während der Zen Cart Installation wurde empfohlen, bestimmten weiteren Verzeichnissen Schreibrechte (chmod 777) zu geben.
Nachdem der Shop fertig eingerichtet ist, sind diese Rechte meist nicht mehr nötig.
Faustregel: Je weniger chmod 777 desto besser!

Hier einige Informationen zu diesen Verzeichnissen. Bitte

wenden Sie sich bei Unklarheiten an Ihren Provider, nicht alle hier beschriebenen Enpfehlungen sind bei allen Providern so möglich.

logs
Dieser Ordner wird seit Zen Cart 1.5.3 deutsch nur für das Schreiben von Errorlogs verwendet (ältere Zen Cart Versionen haben dafür den Ordner cache verwendet).
Statt diesem Ordner chmod 777 zu geben ist es besser, den Ordner eine Ebene über das public_html/htdocs/www Verzeichnis zu legen.
Verzeichnisse auf dieser Ebene sind im Browser nicht aufrufbar.
Wenn Sie das tun, müssen sie auch in beiden configure.php den Pfad zum logs Verzeichnis entsprechend anpassen.

cache
Dieser Ordner wird seit Zen Cart 1.5.3 deutsch nur noch für echtes Caching verwendet. Unter cache/images werden die vom Image Handler generierten Bildercaches abgelegt und unter cache/minify werden die komprimierten Stylesheets und Javascripts gecached. Auch RSS Feeds werden falls aktiviert im Ordner cache/rss gecached.
Dieser Ordner muss daher samt Unterverzeichnissen vom Webserver beschreibbar sein und der Inhalt muss per Browser aufrufbar sein.
Der Ort dieses Ordners sollte seit Zen Cart 1.5.3 deutsch am besten nicht geändert werden.

images

siehe Empfehlungen unter 7.

includes/languages/german/html_includes
siehe Empfehlungen unter 6.

media
Dieses Verzeichnis muss nur Schreibrechte haben, wenn Mediendateien zum Artikeltyp Musik per Admin hochgeladen werden sollen.
Wenn Sie in Ihrem Shop nichts Derartiges anbieten, setzen Sie das Verzeichnis auf chmod 755

pub
Dieses Verzeichnis wird nur verwendet, wenn Sie in Ihrem Shop Downloads anbieten.
Wenn Sie in ihrem Shop keine Downloads anbieten, setzen Sie das Verzeichnis auf chmod 755

DEINADMIN/backups
Dieses Verzeichnis benötigt chmod 777, falls Sie via Admin Sicherungen Ihrer Datenbank durchführen.
Wenn Sie das nicht verwenden, setzen Sie das Verzeichnis auf chmod 755

DEINADMIN/images/graphs
Dieses Verzeichnis benötigt nur chmod 777, um die Statistiken und Grafiken unter Admin > Tools > Banner Manager aktualisieren zu können.
Wenn Sie dieses Feature nicht brauchen, setzen Sie das Verzeichnis auf chmod 755

Generelle Empfehlung für alle übrigen Verzeichnisse und Dateien:
Verzeichnisse: chmod 755
Dateien: chmod 644

10. Drucken Sie nicht die Admin URL mit

Falls Sie Rechnungen über den Adminbereich ausdrucken („in Rechnung stellen“), achten Sie darauf, dass im Ausdruck nicht die URL mitgedruckt wird:
In Firefox:
Datei > Seite einrichten > Ränder & Kopf- und Fusszeilen
Stellen Sie in allen Dropdownmenüs auf „leer“ oder entfernen Sie zumindest „URL“ oder „Titel“
In Internet Explorer:
Datei > Seite einrichten
Entfernen Sie bei Kopfzeile und Fusszeile die Werte Titel und URL

11. Achten Sie auf Sicherheitswarnungen und Updateankündigungen

Im Thema „Aktuell“ dieser Knowledgebase veröffentlichen wir Hinweise auf Sicherheitslücken, Patches und neue Zen Cart Versionen.
Abonnieren Sie den **Newsletter der deutschen Zen Cart Version**, um über Sicherheitslücken, Patches und neue Zen Cart Versionen informiert zu werden.

12. Was Sie regelmäßig tun sollten

1. Stellen Sie sicher, dass Sie alle Empfehlungen aus dieser Anleitung beachtet haben.
2. Machen Sie regelmäßig Sicherungen Ihrer Shopdateien und Ihrer Datenbank. Für die Übertragung per FTP verwenden Sie wenn möglich (und wenn von Ihrem Provider unterstützt) FTP via SSL/TLS
   Für die Datenbanksicherung (z.B. via phpMyAdmin) sollten Sie falls möglich SSL aktiv haben.
3. Überprüfen Sie regelmäßig die Logfiles am Server auf Seltsamkeiten. Achten Sie dabei auf Seitenaufrufe von URLs, zu denen nirgendwo auf Ihrer Seite gelinkt wird. Und achten Sie auf Links, die nach index.php ein http enthalten.
4. Überprüfen Sie regelmäßig die Dateien am Server. Wurden neue Dateien hinzugefügt? Wurden bestehende Dateien geändert?