8 Schutz des eigenen Internetauftritts

[1. Die technisch notwendigen Schritte für einen nachhaltigen und sicheren Webauftritt mit einem CMS (Content Management Systems) können auf einige wesentliche Punkte zusammengefasst werden: 1](#_heading=h.gjdgxs)

[2. die Wahl des passenden Hosting-Produkts 2](#_heading=h.30j0zll)

[3. Benutzerrechte und Passwortsicherheit 3](#_heading=h.1fob9te)

[4. Ausführung automatischer Back-ups 3](#_heading=h.3znysh7)

[5. Anzahl und Qualität der installierten Themes und Plug-ins 4](#_heading=h.2et92p0)

[5.1. Folgende Kriterien sollten bei Bewertungen beachtet werden: 4](#_heading=h.tyjcwt)

[5.2. Folgende Informationen zum/zur Entwickler:in können hilfreich sein: 4](#_heading=h.3dy6vkm)

[5.3. Code-Qualität überprüfen: 4](#_heading=h.1t3h5sf)

[5.4. Zusätzliche Informationen für bezahlte Plug-ins: 5](#_heading=h.4d34og8)

[6. Durchführung regelmäßiger Updates 5](#_heading=h.2s8eyo1)

[7. automatisierte Scans auf Malware und Dateiänderungen 6](#_heading=h.17dp8vu)

# Die technisch notwendigen Schritte für einen nachhaltigen und sicheren Webauftritt mit einem CMS können auf einige wesentliche Punkte zusammengefasst werden:

* die Wahl des passenden Hosting-Produkts
* Benutzerrechte und Passwortsicherheit
* Ausführung automatischer Back-ups
* Anzahl und Qualität der installierten Themes und Plug-ins
* Durchführung regelmäßiger Updates
* automatisierte Scans auf Malware und Dateiänderungen

# die Wahl des passenden Hosting-Produkts

Hosting-Provider und Hosting-Produkte gibt es viele. Dabei variieren die Preise und zugesicherten Leistung stark. Für Laien ist es meist nicht einfach, das passende Hosting-Produkt zu finden, da die prominent platzierten Kennzahlen oftmals wenig über die tatsächlichen Leistungen aussagen. Die folgende Punkte sollten bei der Wahl des Hosting-Produkts berücksichtigt werden:

* Wie viele Nutzer:innen pro Tag/Stunde werden erwartet und welche Datenmengen sind geplant (Download großer Dateien)?
* Um welche Art von Anwendung handelt es sich (kleine Webseite, Onlineshop, Plattform etc.)?
* Wieviel Speicherplatz wird benötigt (auch bei SSD gibt es Unterschiede in der Performance)?
* Serverstandort (DSGVO)
* Support: Achtung, hier gibt es enorme Unterschiede bei Erreichbarkeiten und Reaktionszeiten.
* zugesicherte Ressourcen (Traffic, CPU, RAM etc.), DDoS-Schutz und Virenscan
* SSL-Zertifikate
* aktuelle PHP-Versionen (PHP 8.n) inkl. regelmäßiger Updates, Datenbanken inkl. regelmäßiger Updates
* Verträge: Auftragsdatenverarbeitung, Service Level Agreement (SLA)

# Benutzerrechte und Passwortsicherheit

Häufig verschaffen sich kriminelle Personen Zugang aufgrund schwacher Passwörter. Die folgende Checkliste sollte beim Absichern von Benutzerkonten in CMS-Websites unterstützen:

* starke Passwörter verwenden, die einer Kennwortrichtlinie entsprechen (Mindestlänge, Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen, etc.)
* für jedes Benutzerkonto ein anderes Passwort verwenden,   
  Zwei-Faktor-Authentifizierung aktivieren
* maximal notwendige Benutzerrechte vergeben
* Liste der Benutzerkonten regelmäßig kontrollieren und Benutzerrechte ggf. anpassen bzw. Benutzerkonten löschen, wenn diese nicht mehr benötigt werden
* Passwörter in Passwort-Managern verwalten oder aufschreiben und sicher verwahren

# Ausführung automatischer Back-ups

Back-ups sind ein wesentlicher Bestandteil, um bei möglichen Vorfällen den Schaden möglichst gering zu halten. Die folgenden Punkte sind für Back-ups wichtig:

* Back-ups sollten automatisiert durchgeführt werden.
* Die Häufigkeit der Durchführung kann je Webprojekt variieren. Empfohlen wird ein tägliches Back-up in der Nacht.
* Back-ups sollten mehrfach gesichert sein (z.B. beim Hoster und in einem Cloudspeicher).
* Automatisierte Back-ups sollten überprüft werden (Logfiles, Fehlermeldungen), vor jedem Update wird ein Back-up empfohlen.

# Anzahl und Qualität der installierten Themes und Plug-ins

Plug-ins sind das größte Sicherheitsrisiko bei CMS-Websites. Personen, die mit CMS-Websites wenig Erfahrung haben, sind oftmals überfordert mit den unzähligen Plug-ins und Themes, die zur Auswahl stehen. Die folgende Checkliste sollte bei der Wahl und Qualitätsprüfung unterstützen:

* In erster Linie sollte die benötigte Funktionalität gegeben sein.
* Beschreibungen liefern in der Regel Informationen über den Funktionsumfang.
* Ist eine Dokumentation vorhanden und wie detailliert ist diese?
* Wird Support angeboten?
* So wenig wie möglich, so viel wie unbedingt notwendig installieren, nicht Benötigtes deaktivieren und löschen.
* Plugins zuvor in einem Testsystem ausprobieren (falls möglich), Lizenzbestimmungen beachten.

## Folgende Kriterien sollten bei Bewertungen beachtet werden:

* Wie gut ist die Gesamtbewertung (je höher, desto besser)?
* Wie viele Bewertungen gibt es (je mehr, desto aussagekräftiger)?
* Aus welchem Zeitraum stammen diese Bewertungen (je aktueller, desto besser), wie wird mit Kritik und Fehlermeldungen umgegangen?

## Folgende Informationen zum/zur Entwickler:in können hilfreich sein:

* Steht ein Unternehmen hinter der Entwicklung?
* Gibt es Bewertungen zu diesem/dieser Autor:in bzw. Unternehmen?
* Haben diese auch andere Plug-ins und/oder Themes entwickelt?

## Code-Qualität überprüfen:

* Ein Pagespeed-Test kann auf schlecht programmierten oder unnötig geladenen Code hinweisen (Installation sollte nicht zu längeren Ladezeiten führen).
* Personen mit Programmierkenntnissen können den Code überprüfen oder zumindest rasch erkennen, ob der Code strukturiert aufgebaut ist.

## Zusätzliche Informationen für bezahlte Plug-ins:

* Bezahlte Plug-ins und Themes können in der Regel nicht ausprobiert werden, daher sind die zuvor genannten Punkte gründlich zu prüfen.
* Oftmals sind (nur) 12 Monate Updates und Support inkludiert.
* Anbieter sind grundsätzlich verpflichtet, am aktuellen Stand der Technik zu arbeiten und eine funktionierende Software bereitzustellen.
* Wenn Plug-ins und Themes bei IT-Unternehmen oder Agenturen in Auftrag gegeben werden, sollte genauso darauf geachtet werden, dass eine regelmäßige Wartung möglich ist.

# Durchführung regelmäßiger Updates

In der Regel werden CMS-Websites gehackt, weil sie schlecht oder gar nicht gewartet werden. Die folgende Checkliste unterstützt bei den regelmäßigen Updates:

* CMS-Websites Core-Sicherheitsupdates werden bei vielen Systemen automatisch installiert, sofern diese nicht deaktiviert sind.
* Die Überprüfung auf bereitgestellte Updates sollte täglich durchgeführt werden. Folgendes ist zu beachten bzw. kann unterstützen:
* Nicht alle Plug-ins und Themes können über das CMS-Website-Backend aktualisiert werden (einige Entwickler:innen bieten Updates bspw. nur über ihre Webseite oder über GitHub an).
* Plug-ins und Themes, bei denen die Lizenz abgelaufen ist, bekommen in der Regel keine Updates bereitgestellt und oftmals auch keine Hinweise auf Updates.
* Manche Hosting-Produkte stellen ein serverseitiges Monitoring bzw. E-Mail-Benachrichtigungen für offene Updates bereit.
* Plug-ins und Themes erhalten nur Updates, wenn diese auch von dem/von der Entwickler:in gewartet werden. Daher sollten Plug-ins und Themes, wie im Punkt zuvor beschrieben, regelmäßig geprüft werden (nicht nur vor der Installation).

**Sicherheitsupdates sollten grundsätzlich immer so rasch wie möglich durchgeführt werden. Vor allen anderen Updates ist folgendes zu beachten:**

* Änderungsverlauf prüfen (was ändert sich bei dem Update)
* Kompatibilitätshinweise prüfen
* Updates zuvor in einem Testsystem durchführen (falls möglich)
* vor dem Update ein Back-up erstellen
* Updates einzeln durchführen und die Funktion der Webseite sofort prüfen
* Updates in einer Zeit durchführen, zu der nur wenige Nutzer die Webseite besuchen
* Webseiten-Überprüfung in einem Gast- bzw. privaten Modus des Browsers ausführen (Caching)
* Von automatischen Updates wird abgeraten, da diese im Vorfeld geprüft werden sollten. Falls ein Fehler durch ein Update verursacht wird, wird dieser bei automatischen Updates meist erst nach längerem Zeitraum bekannt.
* Bei Funktionsupdates ist es manchmal sogar vorteilhaft ein paar Tage zu warten, da inzwischen mögliche Fehler bekannt werden und dann eventuell bereits behoben sind.

# automatisierte Scans auf Malware und Dateiänderungen

Es wird empfohlen, regelmäßige Scans nach Malware und Dateiänderungen durchzuführen, um kompromittierte Systeme rasch zu erkennen und handeln zu können. Sollten diese Leistungen nicht vom Hosting-Provider durchgeführt werden, können folgende Maßnahmen gesetzt werden:

* serverseitige Skripte (falls möglich)
* externe Scans (bspw. managewp-com, wpsec.com u.ä.)
* externe Security Tools (bspw. Sucuri u.ä.)
* Security-Plug-ins (bspw. Wordfence, Sucuri u.ä.)   
  Achtung: Die Funktionsweise bei derartigen Plug-ins ist daran gebunden, dass die CMS-Website technisch „läuft“.

*Dieser Handlungsleitfaden wurde auf Basis der Resultate der Masterarbeit von Christian Hörzer mit dem Titel „Handlungsleitfaden in Form einer Checkliste für nachhaltig sichere CMS-basierende Webseiten am Beispiel WordPress” erstellt und stützt sich auf die Expertise der für diese wissenschaftliche Untersuchung interviewten Personen. Mit diesem Leitfaden ist es Betreiber:innen von CMS-basierten Webseiten möglich, einen Mindeststandard an Sicherheit zu erlangen und eine CMS-basierende Webseite selbstständig zu warten.*

Dieses Dokument wurden von einer Expertengruppe der Cybersicherheit-Plattform (CSP) erstellt.

Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr. Eine Haftung der Wirtschaftskammern Österreichs, der CSP oder der Mitglieder der Expertengruppe ist ausgeschlossen.

Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für alle Geschlechter!

Stand: März 2024