

# Checkliste Webseite

## System

- Welches **System** / **CMS** wird verwendet?
- Falls CMS; wird die **aktuellste Version** verwendet?<sup>1)</sup>
- Gibt es **regelmässige Updates** <sup>2)</sup>
- Werden auch **Erweiterungen** / **Plugins** regelmässig aktualisiert? <sup>3)</sup>
- Sind **automatische Updates** aktiviert?
- Gibt es eine **Backupfunktion** oder ein **Backup-Plugin**? <sup>4)</sup>

## Sicherheit

- Wird die Webseite auf **Schadcode** überwacht?<sup>5)</sup>
- Verfügen Sie über **sämtliche Zugangsdaten** oder gibt es noch einen „versteckten Adminzugang“?<sup>6)</sup>
- **Wer** kann die Webseite alles bearbeiten?
- Verfügen Sie über einen **zuverlässigen Host**?<sup>7)</sup>

## Domain (Branding)

- Ist Ihre Domain (z.B. pitw.ch) auf **Ihren Namen / Firmennamen eingetragen**? <sup>8)</sup>
- **Verlängert** sich Ihr Domainname automatisch? Werden Sie informiert, wenn dieser **abläuft**?
- Kennen Sie Ihre **Nameserver**? Wer kontrolliert diese?<sup>9)</sup>
- Sind mehrere **Nameserver** eingetragen (Redundanz, Geschwindigkeit)?
- Wissen Sie, wer alles auf Sie **verlinkt**? Wer **erwähnt** Sie? <sup>10)</sup>

## Passwörter

- Verwenden Sie **sichere Passwörter**?
- Verwenden Sie für **verschiedene Zugänge verschieden Passwörter**?
- Verwenden Sie eine **zweistufige Authentifizierung**?
- Welche E-Mailadresse ist für eine **Passwortrücksetzung** hinterlegt?

## Erweiterte Möglichkeiten

Diese Checkpunkte **lohnen sich nur bei einer Firmenwebseite** bzw. einer Seite mit vielen Besuchern. Für private Webseiten können diese Punkte vernachlässigt werden.

- Ist Ihre Webseite vor **DDos-Angriffen** sicher?
- Verwenden Sie einen zuverlässigen **CDN**?<sup>11)</sup>
- Haben Sie den Überblick über Ihre **SSL-Zertifikate**?

1)

Ein „Schnelltest“ kann z.B. mit [Sucuri](#) durchgeführt werden

2)

Wichtig! Insbesondere wenn eine Datenbank verwendet wird

3)

Erst kürzlich wurden eine [Reihe von schweren XSS Vulnerabilitys](#) in bekannten Plugins gefunden

4)

Auch wenn der Hoster ein Backup erstellt, lohnt sich ein zusätzliches, eigenes Backup

5)

z.B. mit [Google Webmaster Tools](#) oder [Quttera](#)

6)

Verlangen Sie sämtliche Passwörter!!!

7)

Ein professioneller Hoster wird empfohlen! „Eigenes Hosting“ ist aufwändig und braucht Fachwissen

8)

Der entsprechende Eintrag kann mit [Who.is](#) geprüft werden

9)

Die Nameserver einer Domain können z.B. mit [Who.is](#) in Erfahrung gebracht werden

10)

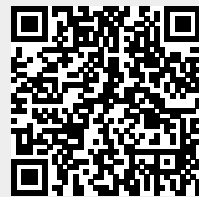
Mit dem Artikel [1-2-3 Überwachung für KMU's](#) kann man diesen Schritt automatisieren

11)

z.B. [Cloudflare](#)



Dieses Dokument stammt aus dem Wiki der Pedrett IT+Web AG. Unter Berücksichtigung der [Nutzungsbedingungen](#) ist eine Weiterverbreitung des Inhalts erlaubt, solange die [Pedrett IT+Web AG](#) als Autor genannt wird.



[Zum Eintrag](#)