So beugst du einem Hack vor: Sicherheits-Checkliste für Websites kleiner Unternehmen

- [ ] **Regelmäßige Updates** Das kannst du selbst erledigen
  Die Aktualisierung von WordPress-Kern, Theme und Plugins ist der wichtigste Schutz.
- [ ] **Backups unabhängig vom Hosting** Das solltest du einem Fachmann überlassen
  Wird dein Hosting-Konto gehackt oder vom Hoster gesperrt, sind die dort gespeicherten Backups womöglich ebenfalls unerreichbar.
- [ ] **Zwei-Faktor-Anmeldung** Das kannst du selbst erledigen
  Aktiviere sie für WordPress-Administratorkonten, das Hosting, die Domainverwaltung und alle verbundenen Dienste (zum Beispiel Google Tag Manager, Shopify-Mitarbeiterkonten).
- [ ] **Einzigartige, starke Passwörter** Das kannst du selbst erledigen
  Jeder Dienst braucht ein eigenes Passwort, gespeichert in einem Passwort-Manager.
- [ ] **Regelmäßige Überprüfung der Zugänge** Das kannst du selbst erledigen
  Prüf vierteljährlich, wer Zugang zur Website, zum Hosting und zu den verbundenen Konten hat.
- [ ] **Nur lizenzierte Plugins und Themes** Die Prüfung überlässt du einem Fachmann
  Verwende nie ein gecracktes („nulled“), kostenlos heruntergeladenes Premium-Theme oder -Plugin: Sie enthalten fast ausnahmslos eine versteckte Hintertür.
- [ ] **Unnötige Plugins und Themes löschen** Das kannst du selbst erledigen
  Auch ein deaktiviertes Plugin bleibt auf dem Server und ist, wenn es eine Lücke hat, genauso angreifbar.
- [ ] **Firewall und Härtung** Das solltest du einem Fachmann überlassen
  Eine Web Application Firewall (WAF) filtert bekannte Angriffsmuster heraus, und korrekte Dateiberechtigungen sowie einige WordPress-Einstellungen (zum Beispiel das Abschalten des Datei-Editors im Admin) erschweren dem Angreifer die Arbeit.
- [ ] **Eine aktuelle PHP-Version** Das solltest du einem Fachmann überlassen
  Auch die PHP-Version deines Hostings hat einen Support-Zeitraum.
- [ ] **Eine Website, ein Hosting-Konto** Besprich das mit deinem Hoster oder Entwickler
  Laufen mehrere Websites in einem Hosting-Konto, kann eine gehackte Website die anderen anstecken.
- [ ] **Google Search Console** Das kannst du selbst erledigen
  Registriere deine Website und prüf, ob die Benachrichtigungen an deine E-Mail-Adresse gehen.
- [ ] **Verfügbarkeitsüberwachung** Das kannst du selbst einrichten
  Ein Überwachungsdienst prüft deine Website minütlich und benachrichtigt dich, wenn sie ausfällt.

EINE 15-MINÜTIGE MONATSROUTINE

- [ ] Prüf, ob Updates ausstehen.
- [ ] Prüf, ob das letzte Backup erstellt wurde.
- [ ] Geh die Benutzerliste durch.
- [ ] Gib in Google site:deinedomain.de ein und achte auf fremde Ergebnisse.
- [ ] Sieh dir die Benachrichtigungen der Search Console an.

Der vollständige Artikel mit Erklärungen: https://redwebdesign.hu/de/wissen/website-sicherheit-checkliste/
Ferenc Kulcsár · hello@redwebdesign.hu · +36 30 501 9090