WEBSITE-SICHERHEIT: 10 MASSNAHMEN

Gute Absicherung braucht keine IT-Abteilung. Haken Sie ab, was bei Ihnen schon steht, und planen Sie den Rest.

GRUNDSCHUTZ

- [ ] **Software aktuell halten:** CMS, Plugins, Themes und PHP-Version.
- [ ] **Starke, einmalige Passwörter,** am besten aus einem Passwortmanager.
- [ ] **Zwei-Faktor-Anmeldung** für Administratoren, Hosting und E-Mail.
- [ ] **Backups, die helfen:** regelmäßig, getrennt vom Server, mit Test.
- [ ] **Zugänge begrenzen:** eigene Konten mit nötigen Rechten, Ehemalige löschen.

TECHNIK UND BETRIEB

- [ ] **Verschlüsselt arbeiten:** HTTPS für die Seite, SFTP statt FTP.
- [ ] **Nur Nötiges installieren:** ungenutzte Plugins, Themes, Testseiten löschen.
- [ ] **E-Mail absichern:** SPF, DKIM und DMARC einrichten, Phishing erkennen.
- [ ] **Formulare und Logins schützen:** Spam-Schutz, Begrenzung falscher Anmeldeversuche.
- [ ] **Überwachen und prüfen:** Erreichbarkeit, Zertifikatsablauf, Schadcode, veraltete Komponenten.

NOTFALLPLAN AUF EINER SEITE

Ansprechpartner Website / Vertretung

Wo liegen Zugangsdaten und Backups?

Hoster, Domain, E-Mail: Kontakt

Wen informieren, wenn die Seite ausfällt?

GUT ZU WISSEN

- Angriffe laufen automatisiert und treffen jede erreichbare Seite.
- Der Hoster sichert den Server, nicht Ihre Website und Ihre Passwörter.
- Nach einem Vorfall: Checkliste »Website gehackt«.

Jens Dartsch · Webentwickler · work@dualbytes.de

Mehr dazu: dualbytes.de/ratgeber/website-sicherheit-kleine-firmen/