KUNDE

Website Sicherheit
Checkliste

Online-Sicherheit ist ein kritischer Aspekt jeder Website. Wenn du Betreiber einer Website bist, ist es essenziell sicherzustellen, dass deine Besucher und ihre Daten sicher sind. Mit dieser Checkliste kannst du prüfen, ob du die Schlüsselfaktoren für eine sichere Webseite beachtet hast.

FIRMA	DATUM	PROJEKT

SSL-Zertifikat und HTTPS-Nutzung:

Das SSL-Zertifikat sorgt dafür, dass Daten sicher zwischen dem Server und dem Browser des Nutzers übertragen werden.

- [ ] Nutzt meine Website HTTPS anstelle von HTTP?
- [ ] Ist mein SSL-Zertifikat gültig und aktuell?
- [ ] Habe ich alle HTTP-Inhalte zu HTTPS umgeleitet?
- [ ] Erzwinge ich eine Verbindung über HTTPS auf dem Server?

Tipp: Die Verwendung von HTTPS nicht nur sichert die Daten, sondern kann auch zu einem besseren Ranking in Suchmaschinen führen.

Regelmäßige Software-Updates:

Software-Updates sind ein essenzieller Bestandteil der Website-Sicherheit. Sie schließen bekannte Sicherheitslücken und verbessern die Stabilität und Leistung der Seite.

- [ ] Sind mein CMS (z. B. WordPress, TYPO3), alle installierten Plugins und verwendeten Themes auf dem neuesten Stand?
- [ ] Nutze ich Tools oder Services, die regelmäßig auf bekannte Schwachstellen in der Software hinweisen?
- [ ] Führe ich ein vollständiges Backup meiner Website und Datenbank durch, bevor ich größere Updates installiere?
- [ ] Folge ich einem festen Zeitplan für nicht sicherheitskritische Updates, um Stabilität und Sicherheit laufend zu verbessern?
- [ ] Habe ich alle inaktiven oder veralteten Plugins deinstalliert?

Tipp: Regelmäßige Software-Updates sind entscheidend, um Sicherheitslücken zu schließen und die Zuverlässigkeit deiner Website zu gewährleisten. Durch ein systematisches Update-Management schützt du deine Seite effektiv vor potenziellen Angriffen.

Sicherheit von Formularen und Datenübertragungen:

Formulare sind häufig das Tor für Cyberangriffe, da sie Daten sammeln und übertragen.

- [ ] Habe ich alle meine Formulare gegen SQL-Injection geschützt?
- [ ] Nutzen meine Formulare CAPTCHA oder ähnliche Mechanismen, um Bots abzuwehren?
- [ ] Werden sensible Daten, die über Formulare übermittelt werden, verschlüsselt?

Hashing und Salting (Hash & Salt):

Das Hashing und Salting von Passwörtern (oder andere äußerst sensiblen Daten) ist eine bewährte Methode, um sicherzustellen, dass Passwörter auch bei einem Datenleck nicht im Klartext gespeichert oder gestohlen werden können.

- [ ] Anstatt Passwörter im Klartext zu speichern, wende ich Hashing-Algorithmen an?
- [ ] Verwende ich bewährte Hashing-Algorithmen wie bcrypt, Argon2 oder PBKDF2, die speziell für die sichere Speicherung von Passwörtern entwickelt wurden?
- [ ] Füge für jedes Passwort ein sogenanntes “Salt” hinzu – eine zufällige Zeichenfolge, die dem Passwort vor dem Hashing-Prozess angehängt wird?
- [ ] Sind meine Formulare möglichst kurz und enthalten nur die wichtigsten Felder?
- [ ] Verwende ich eine klare, unterstützende Beschriftung für jedes Formular-Feld?

Tipp: Hashing und Salting erhöhen die Sicherheit deiner Website erheblich, da sie Passwörter auch dann schützen, wenn die Datenbank kompromittiert wird.

Zugangskontrolle und Berechtigungen:

Ein restriktiver Zugang zu sensiblen Bereichen kann Sicherheitsrisiken erheblich reduzieren.

- [ ] Haben alle Benutzer nur die notwendigen Zugriffsrechte, die sie für ihre Aufgaben benötigen?
- [ ] Nutze ich Zwei-Faktor-Authentifizierung (2FA) für administrative Konten?
- [ ] Werden Benutzerkonten regelmäßig überprüft und inaktive oder nicht mehr benötigte Konten entfernt?

Tipp: Die Zwei-Faktor-Authentifizierung erhöht die Sicherheit erheblich, besonders für Administratoren.

Schutz vor Brute-Force-Angriffen:

Brute-Force-Angriffe versuchen, Passwörter durch systematisches Ausprobieren zu erraten.

- [ ] Habe ich eine Sperrung nach mehreren fehlgeschlagenen Login-Versuchen eingerichtet?
- [ ] Verwende ich Plugins oder Tools, die Brute-Force-Angriffe erkennen und blockieren?

Tipp: Limitiere die Anzahl der möglichen Login-Versuche, um Brute-Force-Angriffe zu verhindern.

Sicherheit beim Datentransport und in API-Integrationen:

Stelle sicher, dass auch alle externen Verbindungen und Datenflüsse sicher sind.

- [ ] Verwende ich HTTPS für alle API-Verbindungen?
- [ ] Sind API-Schlüssel und Zugangsdaten sicher gespeichert und nicht im Code eingebettet?
- [ ] Nutze ich Token-basierte Authentifizierung oder andere Mechanismen, um die API-Sicherheit zu gewährleisten?

Content Security Policy (CSP) und Schutz vor Cross-Site Scripting (XSS):

CSP kann helfen, die Ausführung ungewollten Codes zu verhindern und XSS-Risiken zu minimieren.

- [ ] Habe ich eine Content Security Policy eingerichtet, um die Herkunft von Inhalten zu kontrollieren?
- [ ] Sind meine Eingabefelder und dynamischen Inhalte gegen XSS-Angriffe abgesichert?

Tipp: Mit einer korrekt konfigurierten CSP kannst du die Ausführung von bösartigem JavaScript einschränken.

Schutz vor missbräuchlicher Verwendung von Domain und E-Mail:

Diese Mechanismen verhindern E-Mail-Spoofing und schützen die Domain vor Missbrauch.

- [ ] Habe ich eine DMARC-Richtlinie eingerichtet, die festlegt, wie E-Mail-Provider ungültige E-Mails handhaben sollen?
- [ ] Ist ein SPF-Eintrag konfiguriert, der festlegt, welche Server berechtigt sind, E-Mails von meiner Domain zu versenden?
- [ ] Verwende ich DKIM, um E-Mails mit einer digitalen Signatur zu versehen, die die Authentizität des Absenders bestätigt?
- [ ] Habe ich DNSSEC aktiviert, um die DNS-Authentizität sicherzustellen und sicherzustellen, dass Besucher tatsächlich die richtige IP-Adresse der Domain erreichen?
- [ ] Zonen-Signaturen: Sind meine DNS-Zonen mit kryptografischen Schlüsseln signiert?

Schutz vor Malware und Hackerangriffen:

Ein proaktiver Ansatz ist der beste Weg, um Malware und Hackerangriffe zu verhindern.

- [ ] Verwende ich eine vertrauenswürdige Sicherheitssoftware oder einen Service, um meine Website auf Malware zu überprüfen?
- [ ] Habe ich Firewall-Schutz aktiviert?
- [ ] Nutze ich starke und einzigartige Passwörter für alle meine Konten?

Datensicherung:

Ein Backup deiner Daten ist wie ein Sicherheitsnetz für deine Website.

- [ ] Führe ich regelmäßig Backups meiner Website durch?
- [ ] Bewahre ich mehrere Backup-Kopien an unterschiedlichen Orten auf?
- [ ] Habe ich bereits einmal ein Backup wiederhergestellt, um sicherzustellen, dass es funktioniert?

Online-Sicherheit ist kein einmaliges Unterfangen, sondern erfordert ständige Aufmerksamkeit und Aktualisierung. Mit dieser Checkliste kannst du sicherstellen, dass du den Großteil der Sicherheitsaspekte berücksichtigst und stets auf dem neuesten Stand bleibst.

Benötigst du Hilfe bei der Sicherung deiner Website? Kontaktiere uns, um zu erfahren, wie wir dir helfen können!

Beratungsgespräch vereinbaren

https://www.homepage-helden.de/kontakt/

Eigene Prüfpunkte:

- [ ] Check #1:
- [ ] Check #2:
- [ ] Check #3:
- [ ] Check #4:
- [ ] Check #5:
- [ ] Check #6:
- [ ] Check #7:
- [ ] Check #8:

Notizen:

Diese einfache Checkliste ist für die Anwendung durch dich als Kunde/Auftraggeber gedacht. Du kannst damit eine grundlegende Bedarfsermittlung durchführen oder erste Optimierungspotenziale aufdecken. Darüber hinaus beachten und prüfen unsere Webdesign-Experten bei einer professionellen Analyse, Gestaltung und Realisierung einer Website eine Vielzahl weiterer Aspekte.