

Domain & Hosting- Checkliste

Praktische Checkliste für Eigentum, Sicherheit und zuverlässigen Betrieb



Domain & Hosting-Checkliste

Domain und Hosting sind die technische Grundlage einer Website. Mit dieser Checkliste stellen Sie sicher, dass Eigentum, Zugänge, DNS, E-Mail, Backups und ein späterer Anbieterwechsel sauber geregelt sind.

So nutzen Sie die Checkliste

Prüfen Sie jeden Punkt aus Sicht Ihrer Kunden. Markieren Sie offene Punkte und priorisieren Sie anschließend die Maßnahmen, die Verständlichkeit, Vertrauen, Sichtbarkeit oder Anfragen am stärksten beeinflussen.

01 Eigentum und Verträge

- ☐ Domain und Hostingvertrag laufen auf das Unternehmen oder eine eindeutig berechnigte Person.
- ☐ Rechnungsadresse, Vertragspartner und hinterlegte Kontaktdaten sind aktuell.
- ☐ Laufzeiten, Kündigungsfristen und automatische Verlängerungen sind dokumentiert.
- ☐ Leistungsumfang, Speicher, Datenbanken und Supportbedingungen sind bekannt.
- ☐ Zugriff hängt nicht ausschließlich von einem externen Dienstleister oder ehemaligen Mitarbeiter ab.
- ☐ Ein späterer Umzug oder Export ist vertraglich und technisch möglich.

02 Zugänge und Berechtigungen

- ☐ Kundenkonto, Domainverwaltung, Hosting, SFTP und Datenbanken sind getrennt dokumentiert.
- ☐ Starke, einzigartige Passwörter werden in einem Passwortmanager gespeichert.
- ☐ Mehrfaktor-Authentifizierung ist für zentrale Konten aktiviert.
- ☐ Externe Dienstleister erhalten nur notwendige und zeitlich passende Rechte.
- ☐ Ehemalige Mitarbeitende und nicht mehr benötigte Konten wurden entfernt.
- ☐ Wiederherstellungs-E-Mail, Telefonnummer und Notfallzugriff sind aktuell.

03 Domain und DNS

- ☐ Hauptdomain, zusätzliche Domains und Weiterleitungen sind vollständig erfasst.
- ☐ DNS-Einträge besitzen verständliche Dokumentation und einen verantwortlichen Ansprechpartner.
- ☐ A-, AAAA-, CNAME-, MX- und TXT-Einträge zeigen nur auf tatsächlich genutzte Dienste.
- ☐ Subdomains für Staging, Mail oder externe Anwendungen sind bekannt und abgesichert.
- ☐ DNS-Änderungen werden mit Backup, Zeitplan und Rückfalloption durchgeführt.
- ☐ Nicht mehr benötigte Domains und Einträge werden kontrolliert stillgelegt.

04 E-Mail und Zustellbarkeit

- ☐ Postfächer, Aliase, Weiterleitungen und Verteiler sind vollständig dokumentiert.
- ☐ MX-, SPF-, DKIM- und DMARC-Konfiguration passen zum eingesetzten Maildienst.
- ☐ Formularversand verwendet eine verlässliche und authentifizierte Absenderlösung.
- ☐ Catch-all-Adressen und unnötige Weiterleitungen werden vermieden.

- ☐ Speichergrenzen, Archivierung und Backup der E-Mail-Kommunikation sind geklärt.
- ☐ Ein Anbieterwechsel berücksichtigt Postfächer, Kalender, Kontakte und Geräte.

05 Leistung und Skalierung

- ☐ Hostingstandort, Serverressourcen und Tarif passen zur Zielgruppe und Nutzung.
- ☐ PHP-, Datenbank- und Softwareversionen werden aktuell und unterstützt gehalten.
- ☐ Caching, Komprimierung und HTTP-Konfiguration sind sinnvoll eingerichtet.
- ☐ Traffic-Spitzen, Kampagnen und wachsende Datenmengen können abgefangen werden.
- ☐ Verfügbarkeit und Antwortzeiten werden mit einem unabhängigen Monitoring geprüft.
- ☐ Supportqualität und Reaktionszeiten passen zur geschäftlichen Bedeutung der Website.

06 Backups und Wiederherstellung

- ☐ Dateien, Datenbank und wichtige Konfigurationen werden regelmäßig gesichert.
- ☐ Mindestens eine Sicherung liegt getrennt vom Produktivsystem.
- ☐ Aufbewahrungsdauer und Häufigkeit passen zu Änderungsrate und Risiko.
- ☐ Backups sind verschlüsselt oder angemessen vor unbefugtem Zugriff geschützt.
- ☐ Die Wiederherstellung wurde praktisch getestet oder klar dokumentiert.
- ☐ Zuständigkeit und Reaktionsweg für einen Notfall sind bekannt.

07 Sicherheit und Zertifikate

- ☐ SSL-Zertifikat ist aktiv, automatisch erneuerbar und für alle relevanten Domains gültig.
- ☐ Unsichere Protokolle und nicht benötigte Dienste sind deaktiviert.
- ☐ Firewall, Malware-Schutz und Login-Schutz sind risikogerecht eingerichtet.
- ☐ Sicherheitsupdates werden zeitnah und kontrolliert eingespielt.
- ☐ Dateirechte, Verzeichnisschutz und öffentliche Backups wurden geprüft.
- ☐ Sicherheitsvorfälle werden protokolliert und besitzen einen klaren Eskalationsweg.

08 Staging und Änderungen

- ☐ Es existiert eine geschützte Testumgebung für größere Änderungen.
- ☐ Staging-Seiten sind nicht öffentlich indexierbar und enthalten keine unnötigen Echtdaten.
- ☐ Deployments besitzen Backup, Testplan und Möglichkeit zur Rückkehr.
- ☐ Produktivzugänge werden nicht für spontane Experimente verwendet.
- ☐ Änderungen an DNS, Server und Software werden nachvollziehbar dokumentiert.
- ☐ Wartungsfenster und mögliche Ausfälle werden intern oder gegenüber Kunden kommuniziert.

09 Dokumentation und Anbieterwechsel

- ☐ Eine aktuelle Übersicht enthält Verträge, Zugänge, Domains, Dienste und Ansprechpartner.
- ☐ Exportwege für Dateien, Datenbanken, E-Mails und DNS sind bekannt.
- ☐ Technische Abhängigkeiten zu CDN, Mail, Schriften oder Drittanbietern sind erfasst.
- ☐ Kündigung erfolgt erst, wenn Datenübernahme und Funktion vollständig geprüft sind.
- ☐ Transfercodes und Freigaben werden sicher und zeitlich koordiniert verwendet.

- ☐ Nach dem Wechsel werden alte Zugänge, Daten und Verträge kontrolliert beendet.

Ihre Auswertung

Wählen Sie die drei Maßnahmen mit dem größten Hebel. Formulieren Sie jeweils eine konkrete Aufgabe, eine verantwortliche Person und einen realistischen Termin.

1. Priorität

2. Priorität

3. Priorität

Technische Kontrolle schützt das Unternehmen

Gutes Hosting zeigt sich nicht nur an Geschwindigkeit. Entscheidend sind klare Eigentumsverhältnisse, sichere Zugänge, funktionierende Backups und die Freiheit, bei Bedarf den Anbieter zu wechseln.

Die passende Konfiguration hängt von Anbieter, Website, E-Mail-System und Schutzbedarf ab. Kritische Änderungen sollten durch qualifizierte Fachleute erfolgen.