



Handbuch Website-Administration

Aufgaben und Pflichten für Website-Verantwortliche



Site-Management

Monitoring	_____	0.1
Sicherheit	_____	0.2
Server-Wartung	_____	0.3
Backups	_____	0.4
Updates	_____	0.5
Datenschutz	_____	0.6
Neukunden-Angebot	_____	0.7

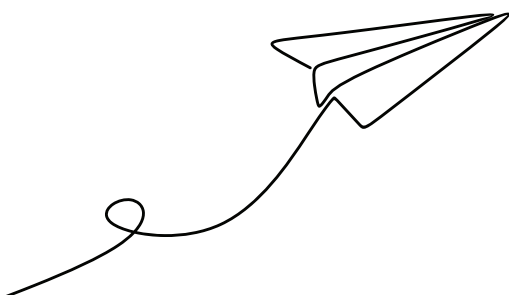
Herzlichen Glückwunsch zu Ihrer Internetseite!

Eine Internetseite ist eine großartige Chance aber auch eine nicht zu unterschätzende Verantwortung. Jetzt, da Ihre Seite online, ist es an der Zeit, zu entscheiden, wer diese Verantwortung für die Sicherheit und Erreichbarkeit in der Zukunft übernehmen soll.

Eine Internetseite benötigt, wie jedes technische System, regelmäßige Wartung, Sicherung und Aktualisierung. Für den Fall, dass Sie sich dafür entscheiden, Ihre Internetseite eigenverantwortlich zu administrieren, erhalten Sie auf den folgenden Seiten einen umfassenden Überblick über Ihre Sorgfaltspflichten als Administrator.

Wir möchten, dass Sie lange Freude an Ihrer Website haben - und so wenig Arbeit wie möglich. Mit unseren Site-Management-Paketen ab 39 € pro Monat* sparen Sie regelmäßig mindestens 10 Arbeitsstunden pro Monat.

Erfahren Sie mehr unter www.enym.com/site-management



*Unsere Sonderangebote für Neukunden finden Sie am Ende dieses Dokuments in Kapitel 7

0.1 Monitoring

Alles im Blick behalten

Sobald Sie als Administrator der Internetseite eingetragen wurden, wird die gesamte Verantwortung für den reibungslosen Betrieb der Seite auf Sie übertragen. Das bedeutet, dass eine Reihe von Pflichten und regelmäßigen Aufgaben auf Sie zukommen.

Richten Sie ein Monitoring ein

Auch der aktivste Administrator kann nicht zu jedem Moment prüfen, ob alle technischen Systeme fehlerfrei laufen. Dafür gibt es eine Reihe von praktischen Tools, mit denen Sie sich beschäftigen sollten. Ein gut eingerichtetes Monitoring informiert sie rechtzeitig über etwaige Probleme bevor diese Schaden anrichten können.

Vermeiden Sie unbedingt, dass Sie erst durch Ihre Besucher oder Kunden von einem Problem auf Ihrer Seite erfahren. Das könnte peinlich werden.

- **Software-Monitoring: Überwachen Sie mit Hilfe geeigneter Plug-ins den funktionalen Betrieb der Internetseite.**
- **Technisches-Monitoring: Geeignete externe Monitoring-Services helfen Ihnen dabei, zu erkennen wann Ihre Internetseite offline oder ein SSL-Zertifikat abgelaufen ist.**

Monitoring der Software

Ein gut eingerichtetes Software-Monitoring überprüft die Funktionsfähigkeit seiteninterner Abläufe und ist der Grundstein für rasche Fehleranalysen und schnelle Korrekturen.

- **Richten Sie ein System ein, das Sie über anstehende Plug-in-Updates informiert**
- **Installieren Sie ein System, das Sie über illegitime Login-Versuche informiert und diese unterbindet.**
- **Installieren Sie ein System, dass Sie über Änderungen und Auffälligkeiten im Dateisystem informiert.**

Empfehlung: Nutzen Sie bspw. die kostenlosen Versionen von WordFence oder iThemes Security. Die Einrichtung ist komplex aber den Aufwand wert.

Monitoring der Technik

Ihre Internetseite besteht nicht nur aus der WordPress-Software und den Plug-ins. Auch der Server muss erreichbar und die Domain sowie das SSL-Zertifikat müssen korrekt konfiguriert sein. Kommt es hier zu einem Problem ist schnelles Handeln gefragt, denn meist bedeutet es, dass Ihre Seite gar nicht mehr erreichbar ist, das schafft große Probleme - nicht nur bei Google.

- **Richten Sie ein System ein, das regelmäßig prüft, ob Ihr Server einen korrekten Statuscode auf den relevanten Ports sendet.**
- **Nutzen Sie einen Dienst, der Sie informiert sobald Ihr SSL-Zertifikat nicht mehr gültig ist.**

Empfehlung: Nutzen Sie bspw. die kostenpflichtigen externen Dienstleister Uptime Robot oder BetterUptime. und erhalten Sie Meldungen per E-Mail.

Als Kunde unseres Site-Managements werden alle Monitoring-Varianten von uns eingerichtet, lizenziert und laufend überwacht.

0.2 Sicherheit

Auf der sicheren Seite sein

Jedes komplexe System ist nur so sicher wie sein schwächste Element. WordPress-Seiten sind sehr verbreitet und deshalb im Durchschnitt bis zu 20x Mal am Tag Angriffen ausgesetzt. Damit Ihre Seite gegen Hacker optimal geschützt ist, müssen Sie eine Reihe von Vorbereitungen treffen.

Halten Sie das System aktuell

Der elementarste Schutz eines jeden Web-Systems sind aktuelle Komponenten. Achten Sie daher darauf, dass Sie Ihre WordPress-Seite stets auf dem aktuellen Stand halten. Wenn Sie ein geeignetes Monitoring eingerichtet haben, erfahren Sie, wann es ausstehende Updates gibt. Üblicherweise gibt es mehrere Updates pro Woche. Verzichten Sie auf automatische Updates damit Sie die Übersicht über Änderungen behalten.

- **Halten Sie die Seite schlank und löschen Sie ungenutzte Plug-ins.**
- **Aktualisieren Sie regelmäßig die Serverkomponenten und PHP.**
- **Aktualisieren Sie regelmäßig alle installierten Plug-ins und das WordPress-Kernsystem. Wie Sie dabei am besten vorgehen erfahren Sie im Abschnitt zu den Updates.**

Sicherheits-Scans Ihres Systems

Auch das aktuellste System ist niemals vollständig vor Angriffen geschützt. Um dieser Unsicherheit bestmöglich begegnen zu können, sollten Sie Ihre Internetseite mehrmals wöchentlich scannen, um auffällige Veränderungen oder Sicherheitslücken rechtzeitig zu erkennen.

- **Nutzen Sie die kostenlosen Dienste des Security Content Automation Protocol (SCAP), um zu prüfen, ob es bekannte Sicherheitslücken zu den von Ihnen verwendeten Plug-ins gibt.**
- **Verwenden sie die WPScan Vulnerability Database, um tagesaktuelle Bedrohungslagen von Themes zu erkennen.**
- **Nutzen Sie hin und wieder externe Dienste wie Sucuri, um umfassende Malware-Scans auszuführen.**
- **Konfigurieren Sie eine Sicherheitssoftware, die regelmäßig das Dateisystem und die Datenbank auf Auffälligkeiten und Schadcode überprüft.**

Vorsicht: Manchmal sind es gerade Updates, die Probleme erst schaffen. Nicht selten haben neue Versionen noch Fehler. behalten Sie die daher die Changelogs nach größeren Versionssprüngen besonders im Blick.

Informieren Sie sich

Ein gutes Sicherheitskonzept erfordert, dass auch Sie sich auf dem Laufenden halten. Informieren Sie sich in den einschlägigen Kanälen wie bspw. dem Bundesamt für Informationssicherheit (BSI). Abonnieren Sie spezialisierte Anbieter, die Sicherheitslücken veröffentlichen und behalten Sie die Changelogs Ihrer Plug-ins im Auge. Möglicherweise wurde gerade eine Sicherheitslücke gestopft von der Sie noch gar nichts bemerkt hatten.

Als Kunde unseres Site-Managements ergreifen und betreuen wir für Sie all diese und noch einige weitere Sicherheits-Maßnahmen.

0.3 Server-Wartung

Ein solides Fundament

Ein gut administrierter Server ist das wichtigste Fundament eines stabilen Seiten-Betriebs. Dieser Abschnitt gibt Ihnen einen Überblick darüber, wie Sie ihr Webhosting pflegen und welche Prozesse Sie regelmäßig ausführen müssen, um maximale Sicherheit zu gewährleisten.

Konfiguration externer Webhostings

Wenn Sie ein externes, nicht von enym administriertes, Webhosting verwenden, achten Sie darauf, dass Sie stets die optimalen Sicherheitseinstellungen aktiviert haben. Zudem ist es wichtig, dass Sie regelmäßig prüfen, ob die aktuelle PHP-Version eingesetzt wird.

- **Vorsicht: Wenn Sie eine veraltete PHP-Version im Einsatz haben wird dies bei Ihrem Webhosting-Anbieter zusätzliche Kosten verursachen, da Sie automatisch in den kostenpflichtigen sog. "Extended Support" für veraltete PHP-Versionen geraten.**
- **Vorsicht: Häufig werden Ihnen auch vermeintlich performantere Beta-Versionen vorgeschlagen. Wir empfehlen ausschließlich die Nutzung stabiler PHP-Versionen.**

Webhosting und PHP-Version

PHP ist das Betriebssystem auf dem Ihre Internetseite läuft. Jeder Webhoster bietet Ihnen an, regelmäßig auf eine neuere PHP-Version zu aktualisieren. Ein Update erfolgt nicht automatisch. Sie sollten monatlich schauen, ob eine neue Version zur Verfügung steht.

Steht ein Update auf eine höhere stabile Version (keine Beta-Version) zur Verfügung, dann prüfen Sie als nächstes ob alle Komponenten bereits zur Nutzung mit der neuen Version kompatibel sind. Die Informationen dazu finden Sie in den Beschreibungen der Plug-ins.

- **Prüfen Sie regelmäßig, ob neue stabile PHP-Versionen in Ihrem Webhosting zur Verfügung stehen (keine Beta-Versionen).**
- **Prüfen Sie, ob die eingesetzten Plug-ins mit der neuen PHP-Version kompatibel sind. Lesen Sie dazu die Hinweise auf den Herstellerseiten. Meist finden Sie diese in den Changelogs.**
- **Sichern Sie die gesamte Internetseite: Datenbank und Dateisystem bevor Sie das PHP-Update ausführen.**
- **Prüfen Sie die Seite nach dem erfolgten Update auf Funktionsfähigkeit. Testen Sie v.a. interaktive Funktionen.**

Tipp: Achten Sie auch darauf, den MySQL-Datenbank-Server aktuell zu halten, denn v.a. dieser bestimmt die Lade-Geschwindigkeit der Seite.

Virtuelle-Server

Wenn Sie ein selbstadministriertes externes Webhosting wie bspw. einen V-Server verwenden achten Sie bitte darauf, dass Sie zusätzlich regelmäßig weitere Updates zur Serversicherheit einpflegen müssen. Nutzen Sie als Serververwaltung Plesk, empfiehlt es sich, wöchentlich die aufgelaufenen Updates zu den einzelnen Serverkomponenten zu prüfen und auszuführen.

Wenn Sie einen Managed Server über enym beziehen, übernehmen wir für Sie die gesamte Server-Administration für maximale Leistung.

0.4 Backups

Lieber doppelt und dreifach

Auch das sicherste System kann mal ein Problem bekommen, dessen Korrektur ein Restore erfordert. Sei es, dass Sie ein Plug-in auf eine vorige Version zurücksetzen oder ein versehentlich gelöscht Dokument wiederherstellen möchten. Backups sind Ihre digitale Lebensversicherung.

Entwickeln Sie eine Backup-Strategie

Verlassen Sie sich nicht auf vermeintliche automatische Backups eines externen Hosting-Anbieters. Daten von dort im Notfall wiederherzustellen ist meist teuer, kompliziert und nicht zuletzt sehr zeitaufwändig. Eine eigene Backup-Strategie schafft die Ruhe, die Sie nachts gut schlafen lässt. Dazu gehören unbedingt zwei meist kostenpflichtige Komponenten:

- **Nutzen Sie ein bewährtes Backup-Plug-in. Vergessen Sie vermeintlich kostenlose Lösungen. Es lohnt wahrlich nicht, bei etwas systemkritischem wie einem Backup-System zu sparen.**
- **Buchen Sie externen Speicherplatz bei einem verlässlichen Cloud-Speicher Anbieter wie Microsoft OneDrive, Google Drive, DropBox oder Wasabi.**

Konfigurieren Sie Ihr Backup-Tool

Es nützt nichts, wenn Sie ihr tägliches Datenbankbackup in der Seite lagern in der es erstellt wurde. Wenn der Server einmal offline ist, kommen Sie auch nicht mehr an das Backup, um es bspw. schnell auf einem Ersatz-Server einzurichten. Verwenden Sie daher einen der großen Cloud-Speicher Anbieter und archivieren Sie Ihre Backups extern. Achten Sie bei der Konfiguration Ihrer Backup-Lösung auf folgende Anforderungen:

- **Integrieren Sie eine performante Backup-Lösung und prüfen Sie ob sie auch große Dateimengen problemlos sichern kann.**
- **Konfigurieren Sie Ihr Backup-Plug-in so, dass mindestens täglich Datenbank-Backups angefertigt werden.**
- **Dateisystembackups sollten mindestens wöchentlich erfolgen.**
- **Stellen Sie Ihre Backup-Lösung so ein, dass sie idealerweise immer für 30 Tage rückwirkend Backups vorhält und ältere Versionen automatisch überschrieben werden.**
- **Erstellen Sie von Zeit zu Zeit Snapshots des Gesamtsystems.**
- **Auf sehr großen Seiten nutzen Sie die Backup-Lösung von Plesk.**

Vorsicht: Vermeiden Sie funktionsreduzierte kostenlose Backup-Plug-ins.

Proben Sie den Ernstfall

Ein Backup zu haben ist wichtig. - im Bedarfsfall damit auch umgehen zu können noch wichtiger. Probieren Sie die Wiederherstellung ruhig einmal in einer Testumgebung aus damit Sie im Ernstfall wissen wie Sie vorgehen müssen. Sollten Sie bei einem Servertotalausfall auf ein Ersatzsystem wechseln wollen beachten Sie bitte, dass die Umstellung der DNS-Daten in der Domain einige Stunden in Anspruch nehmen kann.

Als Kunde unserer Site-Managements profitieren Sie von einer professionellen externen Backup-Lösung und redundanten Servern.

0.5 Updates

Auf dem Laufenden bleiben

Die häufigste Aufgabe der Administration ist das Ausführen von Updates. Kaum etwas ist so schnelllebig wie digitale Systeme. Selbst kleine Seiten erfahren wöchentlich mehrere Aktualisierungen. Das lohnt sich, denn Updates bringen meist mehr Sicherheit, Leistung und neue Funktionen.

Folgen Sie dem Update-Prozess

Ausstehende Updates werden Ihnen im WordPress-Backend als Zahl in der Administrations-Leiste angezeigt. Wir setzen in den von uns entwickelten Systemen nur professionell und gut gewartete Plug-ins externer Autoren ein. Das erkennen Sie u.a. an der hohen Update-Frequenz. Außerdem achten wir darauf, dass so wenig Plug-ins wie möglich im Einsatz sind.

Gehen Sie bei der Ausführung von Updates immer nach dem folgenden gleichen Muster vor. Dieses Prinzip gilt immer, egal um was für eine Art von Aktualisierung es sich handelt.

- **Kompatibilitätsprüfung**
- **Backup**
- **Update**
- **Funktionsprüfung**

Die Prüfung vor dem Update

Grundsätzlich empfehlen wir, automatische Updates nicht zu aktivieren. Der Grund dafür ist einfach: Nicht alle Aktualisierungen sind gewünscht, passend oder kompatibel. Manchmal kann es dazu kommen, dass Sie zunächst die Serverumgebung anpassen müssen, oder dass neue Versionen bestimmte Funktionen, die Sie dringend benötigen, nicht mehr unterstützen.

Auch ist bei manchen Aktualisierungen Geduld eine gute Tugend. Es lohnt sich daher immer zunächst in die Changelogs der Aktualisierung zu schauen und zu prüfen, um was für eine Art von Update es sich handelt. Ein gutes Beispiel ist die Umstellung des Standard-Editors on WordPress vor einigen Jahren. Wer schon die frühen Versionen genutzt hat hatte mitunter einiges auszustehen und musste danach alle Inhalte aufwändig anpassen.

- **Man kann es nicht oft genug sagen: Bevor sie irgendetwas aktualisieren erstellen sie ein Backup!**
- **Verschaffen Sie sich einen Überblick darüber, welche Bestandteile eines Plug-ins vom Update betroffen sind. Lesen Sie die Changelogs oder die Kommentare im Support-Bereich.**
- **Handelt es sich um geschlossene Sicherheitslücken aktualisieren Sie die betroffene Komponente sofort.**
- **Prüfen Sie nach einem Update immer die Funktionen der Seite!**

Tipp: Wenn Sie unsicher sind warten Sie noch mit dem Update.

Die Prüfung nach dem Update

Der wichtigste Prozess nach einem erfolgten Update ist die ausführliche Prüfung der Seite danach. Testen Sie in einem Inkognito-Fenster, ob es getalterische Probleme gibt und prüfen Sie die interaktiven Elemente, insbesondere die Kontaktformulare, auf Ihre Funktionsfähigkeit.

Als Kunde unserer Site-Managements übernehmen wir den gesamten Update-Prozess und prüfen Ihre Seite hinterher exakt.

0.6 Datenschutz

Cookies und Co.

Als Webseiten-verantwortliche Person müssen Sie auch eine Reihe rechtlicher Anforderungen beachten. Es ist erforderlich, dass Sie sich regelmäßig informieren und die Seite technisch sowie redaktionell, insbesondere die Rechtstexte, an die aktuellen Bedingungen anpassen.

Die Anforderungen im Blick behalten

Die rechtlichen Rahmenbedingungen ändern sich zwar nicht allzu oft, aber regelmäßig, und wenn sie es tun sind die Konsequenzen meist weitreichend. Beispiele gibt es viele: Die Button-Lösung für Shop-Betreiber, Die Cookie-Richtlinien der DSGVO und viele andere.

Für alle, die nicht aufpassen, kann eine Abmahnung teuer werden. Passen Sie Ihre Seite daher regelmäßig an die geltenden Rechtspflichten an:

- **Berücksichtigen Sie die Anforderungen der Impressumspflicht.**
- **Pflegen Sie das Auftragsdatenverarbeitungsverzeichnis und Ihre Datenschutzhinweise sobald Sie Plug-ins aktualisieren.**
- **Passen Sie die Cookie-Richtlinie regelmäßig an die aktuelle Technik Ihrer Seite an. Wiederholen Sie die Scans regelmäßig.**
- **Installieren Sie einen Cookie-Banner der Cookies wirklich blockt.**

Cookie-Banner

Cookie-Banner sind lästig und sicherlich technisch nicht der Weisheit letzter Schluss. Aber sie sensibilisieren für ein sehr wichtiges Thema und wer sich die langen Listen so mancher Cookie-Hinweise einmal genauer anschaut, der weiß, dass es sinnvoll ist, an diesem Punkt, Transparenz zu schaffen.

Es ist meist technisch aufwändiger, gänzlich auf Cookies zu verzichten als einen guten Cookie-Banner einzubauen. Aber auch hier gibt es einiges zu berücksichtigen und leider gibt auch es keine "One-size-fits-all" -Lösungen:

- **Lizensieren Sie ein professionelles Cookie-Banner-System.**
- **Achten Sie bei der Konfiguration darauf, dass das Plug-in Cookies wirklich unterbindet. Vor dem Setzen von Cookies ist eine "informierte Einwilligung" zwingend erforderlich.**
- **Tracking fällt nicht unter Absatz 6 "berechtigtes Interesse" und erfordert die ausdrückliche Einwilligung des Besuchers.**
- **Implementieren Sie eine Steuerungsfunktion im Datenschutz.**

Vorsicht: Vermeiden Sie funktionsreduzierte kostenlose Cookie-Banner.

Auftragsdatenverarbeitungsverzeichnis

Sobald Sie eine Webseite haben, sind Sie ein datenverarbeitendes Unternehmen. Das bedeutet auch, dass Sie ein Verzeichnis der Datenverarbeitungstätigkeiten führen und bei Ihren Dienstleistern (Webhosting etc.) eine Datenverarbeitungsvereinbarung einholen müssen. Das Auftragsdatenverarbeitungsverzeichnis muss im Falle einer Prüfung vorgelegt werden. Beachten Sie, dass Sie das Verzeichnis nach wesentlichen technischen Änderungen an Ihrer Seite aktualisieren müssen.

Hinweis: Die hier beschriebenen Hinweise sind keine Rechtsberatung!

Als Kunde unserer Site-Managements übernehmen wir die Erstellung und Pflege aller Rechtsdokumente und Cookie-Systeme.



Site-Management von enym - medienkompetenz

Die in diesem Dokument gezeigten Anforderungen sind nur ein Auszug dessen, was Sie als verantwortlicher Administrator bei der Pflege und Wartung Ihrer Internetseite berücksichtigen müssen. Wenn Sie diese wichtige Aufgabe lieber einem vertrauensvollen Partner übergeben möchten, dann ist unser Site-Management genau das Richtige für Sie.

Site-Management von enym erhalten Sie bereits ab 39 € pro Monat. Erfahren Sie mehr darüber unter: www.enym.com/site-management



Unsere Site-Management-Angebote für Neukunden

Mit unseren Site-Management Paketen sparen Sie durchschnittlich ca. 10 Stunden administrative Arbeitszeit pro Monat. Neu: Inkl. Cookie-Banner!

99 €*
pro Monat, inkl.
Cookie-Banner



Updates & Backups

~~149 €~~
p. Monat statt 199 €*
*für die ersten 12 Monate, danach 199 €.

Administration & Wartung

Server & Domain Management
Monitoring
Reputationsschutz
Backups
Updates
Compliance

+1 Service-Stunde p. M. für die funktionelle/ inhaltliche Betreuung

39 €
pro Monat, inkl.
Cookie-Banner

Mini-Websites

Dieses Paket kostet für Solo-Selbstständige mit Internetseiten, die weniger als 8 Einzelseiten haben, sowie für die Wartung einzelner Landingpages nur:

39 € p. Monat*
* Für die ersten 6 Monate danach 49,90 €*

199 €*
pro Monat, inkl.
Cookie-Banner



Entwicklung & Performance

~~299 €~~
p. Monat statt 399 €*
*für die ersten 12 Monate, danach 399 €.

Administration & Wartung

Server & Domain Management
Monitoring
Reputationsschutz
Backups
Updates
Compliance

Sicherheit & Performance

Caching & Performance-Boost
Firewall
Sicherheits-Scans

+3 Service-Stunden p. M. für inhaltliche Betreuung und die weitere Entwicklung der Seite

JETZT STARTEN →

349 €*
pro Monat, inkl.
Cookie-Banner



SEO & Reichweite

~~499 €~~
p. Monat statt 599 €*
*für die ersten 12 Monate, danach 599 €.

Administration & Wartung

Server & Domain Management
Monitoring
Reputationsschutz
Backups
Updates
Compliance

Sicherheit & Performance

Caching & Performance-Boost
Firewall
Sicherheits-Scans

SEO & Marketing

Publishing für Onsite- & Offsite SEO
SEO & Analytics-Dashboard
E-Mail-Berichte zur Seitenleistung

+6 Service-Stunden p. M. für inhaltliche Betreuung und die weitere Entwicklung der Seite

JETZT STARTEN →

* Die Angebote umfassen zusätzlich die Lizenz für ein Cookie-Banner im Wert von 9,99 € pro Monat und gelten ausschließlich für Neukunden, die sich innerhalb von 8 Wochen nach Fertigstellung des Projekts für eines der Site-Management-Pakete entscheiden. Die Angebotspreise gelten jeweils zunächst für 12 Monate.

Mit unserem Site-Management sparen Sie Arbeitszeit, Lizenzkosten und eine ganze Menge Aufwand. Fragen? Melden Sie sich: info@enym.com

Handbuch Website-Administration

17