CYBERDAY®

Whitepaper

# SHOPHOSTING

CYBERDAY®

Hrgs.: CYBERDAY GmbH
Autor: Simon Huck

Whitepaper

# Shophosting

# Inhalt

## Einleitung

Es gibt sehr viele günstige Standard-Hostingangebote am Markt, die prinzipiell den Betrieb eines Onlineshops erlauben. Allerdings ist es ein Fehler, ausgerechnet an den Hostingkosten sparen zu wollen.

Denn ein reibungsloser und ausfallsicherer Betrieb des Shops ist praktisch die Geschäftsgrundlage im E-Commerce: Gibt es Aussetzer, sogar wenn diese nur kurz auftreten sollten, untergräbt dies das Vertrauen bei den Kunden. Ist ein Shop nicht zuverlässig und nicht stets schnell erreichbar, wird dies unter Umständen auch zusätzlich von Google mit schlechterem Ranking und höheren AdWords-Preisen bestraft.

Noch fataler jedoch, wenn aufgrund einer falschen Entscheidung alle Daten weg sind und der Hoster über keine oder keine ausreichende Backup-Strategie verfügt. Die Annahme, dass der Provider im Notfall sowieso über eine aktuelle Datensicherung verfügt, ist einer der größten Hosting-Irrtümer, nicht nur unter Shopbetreibern.

Auch Datendiebstahl und DDos-Angriffe sind keine Gefahr, die nur andere betrifft. Da auch Hacker immer dazulernen, werden Attacken alltäglicher und die Notwendigkeit seinen Onlineshop zu schützen größer.

Sein Einzelhandelsgeschäft und Warenlager wird man schließlich auch ausreichend sichern und sich nicht darauf verlassen, dass schon niemand die offene Eingangstür bemerken wird. Nicht anders verhält es sich letztlich mit dem Server für sein Onlinegeschäft.

Die Frage, die man sich stellen sollte, lautet: „Welchen Umfang haben die Hostingkosten auf das Gesamtbudget und wie wichtig ist der Schutz und eine schnelle und zugleich zuverlässige Auslieferung meiner Daten?“

### Häufige Fehler - zu geringe Ressourcen gewählt

Aus Sparsamkeit werden beim Shophosting oft Kompromisse gemacht. Dabei ist ein schneller, zuverlässiger und reibungsloser Betrieb zu jeder Zeit (auch in Zeiten vieler Zugriffe) die geschäftsentscheidende Grundlage im E-Commerce.

Die erste Grundsatzfrage ist, ob der Shop intern auf eigenen Servern oder extern in einem Rechenzentrum betrieben werden soll. Es sprechen nur sehr wenige Argumente für einen Eigenbetrieb, beispielsweise wenn zwingend und laufend auf andere interne Systeme (z.B. komplexe ERP- oder CRM-Systeme, wie SAP und Siebel) zugegriffen wird, und dabei aus Sicherheitsgründen keine externen Komponenten zwischengeschaltet werden dürfen. Denn es ist extrem teuer, ein eigenes Rechenzentrum zu betreiben, das die benötigten Dimensionen an Netzwerkanbindung, Leistungsstärke, Ausfallsicherheit (Redundanz) und auch administrativer Expertise für alle Eventualitäten vorhalten kann.

E-Commerce-Experte Eric Jankowfsky rät in diesem Zusammenhang: *„Kleinere Shop-Projekte, die nicht geschäftskritisch sind, könnten auf einem Shared Server gehostet werden. Ab einem Bestellaufkommen von zwanzig Bestellungen am Tag sollte es auf jeden Fall ein eigener Server sein. Dabei summieren sich die verschiedenen Kostenblöcke schnell auf 150 – 300 Euro im Monat, beispielsweise für:*

- *Rechnermiete*
- *Servermanagement /SLA (Service-Level-Agreement)*
- *Backup-Strategie*
- *SSL-Zertifikat*

*Für den Betrieb in einem Servercluster bestünde der kleinste Cluster aus zwei Rechnern, auf denen jeweils die Datenbank und der Shop läuft. Die Kosten würden sich also verdoppeln. Für eine 99,9%-ige Verfügbarkeit würde ich zwei Datenbank- und zwei Shop-Server empfehlen, was die Kosten entsprechend vervierfachen würde.“*

## Ladezeiten

Bekanntermaßen steigert ein performanter Onlineshop, mit entsprechend schnellen Ladezeiten, maßgeblich die Kundenzufriedenheit und kann daher deutliche Auswirkungen auf die Konversionsrate haben. Gleichzeitig ist mittlerweile eine schnelle Ladezeit des Onlineshops auch für Suchmaschinen wie Google ein wichtiges Qualitätsmerkmal und fließt dementsprechend in deren Rankingkriterien ein. Ein schneller Webserver sorgt daher im besten Fall auch für mehr Besucher im Onlineshop. Besucher, die sonst möglicherweise teuer über das Online-Marketing eingekauft werden müssten.

Als eine der Herausforderungen für jeden Shop-Betreiber bei diesem Thema gilt, herauszufinden, an welchen Stellschrauben gedreht werden kann beziehungsweise muss, um die Ladezeit zu verringern. Neben den in den folgenden Kapiteln vorgestellten Punkten wie Leistungsfähigkeit der Hardware und der Netzwerkinfrastruktur, gibt es weitere Einflüsse, welche die Geschwindigkeit von Webseiten beeinflussen.

Eine sehr gute Möglichkeit Optimierungspotential festzustellen, bieten beispielsweise die kostenlosen Tools Firebug (https://addons.mozilla.org/de/firefox/addon/1843) und die Google Webmastertools (https://www.google.com/webmasters/tools) sowie externe Monitoringtools wie Nagios, Sitewert oder uptrends. So erlaubt Firebug, eine Erweiterung des Browsers Mozilla Firefox, die Fehlersuche und das Monitoring von Webseiten. Firebug zeigt für alle Elemente einer Webseite deren benötigte Ladezeit auf einer Zeitleiste an und gibt konkrete Empfehlungen für die Optimierung, wie beispielsweise der Auslagerung von CSS-Elementen oder Komprimierung der eingebetteten Bilder.

Im Google Webmastertool wiederum kann man sich die Crawlergeschwindigkeit anzeigen lassen, wird bei Problemen gewarnt und erhält ebenfalls Tipps für die schnellere Auslieferung der Webseite.

Meist muss erst etwas passieren, bevor sich Shop-Betreiber um ein geeignetes und skalierbares Hosting kümmern. Doch wenn die Seite „gehackt“ wurde, der Server ohne Backup-Strategie ausfällt oder die Kapazitäten nicht mehr genügen, ist es zu spät. Beim Hosting ist Prävention statt Intervention gefragt.

# 1. Hardware

Sowohl Prozessor als auch Arbeitsspeicher sind für den Nutzer am stärksten spürbar. Sie bestimmen, wie schnell der Rechner das geforderte Programm ausführt – die Hauptaufgabe eines Webservers. Bei den Angaben der Hoster ist hier jedoch etwas Fingerspitzengefühl gefordert: Ein virtueller Server mit acht Kernen etwa entspricht keineswegs einem physikalischen Acht-Kern-Server. Werden beispielsweise vier Kunden auf einem Rechner untergebracht, bleiben dem einzelnen gerade einmal zwei dedizierte CPU-Kerne. Die einzelnen Kerne müssen hoch getaktet sein, da viele Applikationen Probleme haben, mehrere Kerne zu nutzen (Multi-Threading). Dasselbe gilt für den verbauten Arbeitsspeicher. Hier sind nur „garantierte“ oder „zugesicherte“ Angaben aussagekräftig.

Erfährt der eigene Shop starke Zuwachsraten, ist ein Aufrüsten der Hardware unvermeidbar. Doch nicht jeder Anbieter reagiert so flexibel darauf, wie dies notwendig ist. Das kann auch daran liegen, dass alle im Server verfügbaren RAM-Steckplätze belegt sind. Hier hilft es, wenn der Hoster den Einsatz von 19-Zoll-Servern bekannter Qualitätshersteller garantiert. Solche „Markenrechner“ sind darauf ausgelegt, schnell und einfach erweitert zu werden.

Ein Vorteil, der sich auch beim Thema Redundanz bemerkbar macht. Denn um für den Ernstfall hinsichtlich Wachstum und Ausfallsicherheit gerüstet zu sein, sollte jede „lebenswichtige“ Komponente doppelt vorhanden sein: zwei Netzteile, zwei Festplatten, im Idealfall auch zwei Netzwerkkarten, die über unterschiedliche Switche in das Netz eingebunden sind.

## 1.1 Server

Stark frequentierte und technisch komplexe Onlineshops benötigen eine solide Hosting-Basis. Auch wenn dafür theoretisch auch ein Shared Server vorstellbar ist, sollte der Shop - der ja immerhin die Geschäftsgrundlage darstellt – auf einem Managed Server, wenn nicht sogar einem Root Server laufen. Der Hosting-Kunde erhält die volle Kontrolle über die Server-Hardware und kann diese nach seinen individuellen Bedürfnissen selbst einrichten. Diese Flexibilität hat jedoch auch ihren Preis: Notwendiges Know-how und der Zeitaufwand für die Administration sind nicht zu unterschätzen und der Shop-Betreiber muss sich um alle auftretenden Probleme selbst kümmern.

Beim Shared Hosting dagegen teilen sich viele Websites oder Onlineshops den Speicherplatz und die Ressourcen eines Servers. Für professionelle Auftritte genügt dies selten. Neben geringeren Server-Ressourcen fehlt der Freiraum, den Server auf die Bedürfnisse der Shop-Software und anderen benötigten Applikationen anzupassen.

Die Leistungsfähigkeit eines Root Servers unterscheidet sich grundsätzlich nicht oder kaum von einem Managed Server, bei dem sich der Hosting-Provider um Administration und Wartung kümmert. Den Unterschied macht hier die zeitliche und technische Flexibilität, da man den Server selbst konfiguriert.

Diese Freiheit setzt jedoch geschultes Personal voraus und kostet Zeit. Der Hoster stellt lediglich die gewählte Infrastruktur im Rechenzentrum sowie die Netzanbindung zur Verfügung.

Datenbankserver sollten über ausreichend RAM verfügen, damit möglichst viele Abfragen nicht erst an eine Festplatte geleitet werden müssen. Um aber auch die Zugriffe auf die Festplatten schnell zu halten, empfiehlt sich der Einsatz von SSD Platten, die wesentlich schneller als herkömmliche Festplatten sind und aktuell sogar auch günstiger zu kaufen sind wie SAS Platten.

Damit aufwendige Abfragen schnell abgearbeitet werden, sollte auf aktuelle CPU gesetzt werden. Eine hohe Taktrate ist hier Pflicht.

Um Ausfälle zu vermeiden, kann die Datenbank mittels Replikation auf einen zweiten Server gespiegelt werden. Dieser Server kann dann bei Problemen den Hauptserver ersetzen oder für die Datensicherung verwendet werden.

Eine Trennung von Webservern und Datenbankservern ist Pflicht, einfach um die Last der Website auf zwei Maschinen zu verteilen. Somit lassen sich die Konfigurationen ideal auf die entsprechende Hardware einstellen.

## 1.2 Storage

Eine nur scheinbar untergeordnete Rolle spielt der verfügbare Speicherplatz. So benötigt eine Standard Shopsoftware mitunter nicht einmal 100 MByte, inklusive der Datenbank. Den Großteil des benötigten Fest-plattenspeichers machen sicherlich Produktbilder aus. Rechnet man je Produktbild mit nur 70 KByte, bei drei bis vier Bildern je Produkt, käme man bei 5.000 Artikeln bereits auf einen zusätzlichen Speicher-bedarf von mehr als 1,2 GByte.

Für umfangreiche Datenbanken sind herkömmliche IDE-, SATA- oder SAS-Festplatten möglicherweise zu langsam. In solchen Fällen ist die Aufrüstung mit Solid State Discs (SSD) interessant. Bei besonders großen Anforderungen lohnt zudem ein Blick auf eine Cluster-Lösung: Die Redundanz wird hierbei durch mehrere Rechner sichergestellt; auch die Datenbank findet mitunter auf einem dedizierten Rechner Platz.

### RAID

Festplattenausfälle gehören zu den häufigsten Ursachen für Server-Probleme. Um dem dadurch bedingten Datenverlust vorzubeugen, gehört die Serverausrüstung mit mindestens zwei Festplatten für ambitionierte Shop-Betreiber zum Mindeststandard. Die Festplatten werden in einem RAID-Verbund parallel betrieben und alle Daten auf beiden Festplatten gleichermaßen gespeichert. Diese Spiegelung erhöht die Sicher-heit, weshalb jedoch immer nur der Platz einer Festplatte zur Verfügung steht. Idealerweise wird RAID10 eingesetzt, wobei mindestens vier Platten notwendig sind, jedoch nur die Hälfte der möglichen Kapazität nutzbar ist.

## 1.3 Internetanbindung

Ist das System fürs Erste ausreichend leistungsfähig, bleibt die Leitung als möglicher Flaschenhals. Eine entsprechend starke Internetanbindung des Rechenzentrums ist deshalb Grundvoraussetzung, wobei die Angaben hier immer relativ zur Anzahl der gehosteten Projekte sind.

Als Faustregel gilt, dass die Anbindung der Server an das Internet mindestens mit einer 1 Gbit/s-Leitung erfolgen sollte. Somit steht genügend Bandbreite zur Verfügung, um eine gleichbleibend hohe Zugriffsge-schwindigkeit für den Onlineshop zu gewährleisten. Hier ist sicherzustellen, dass der Server eine 1 Gbit/s-Anbindung hat und nicht nur das Rechenzentrum oder das Rack diese Leistung aufweist.

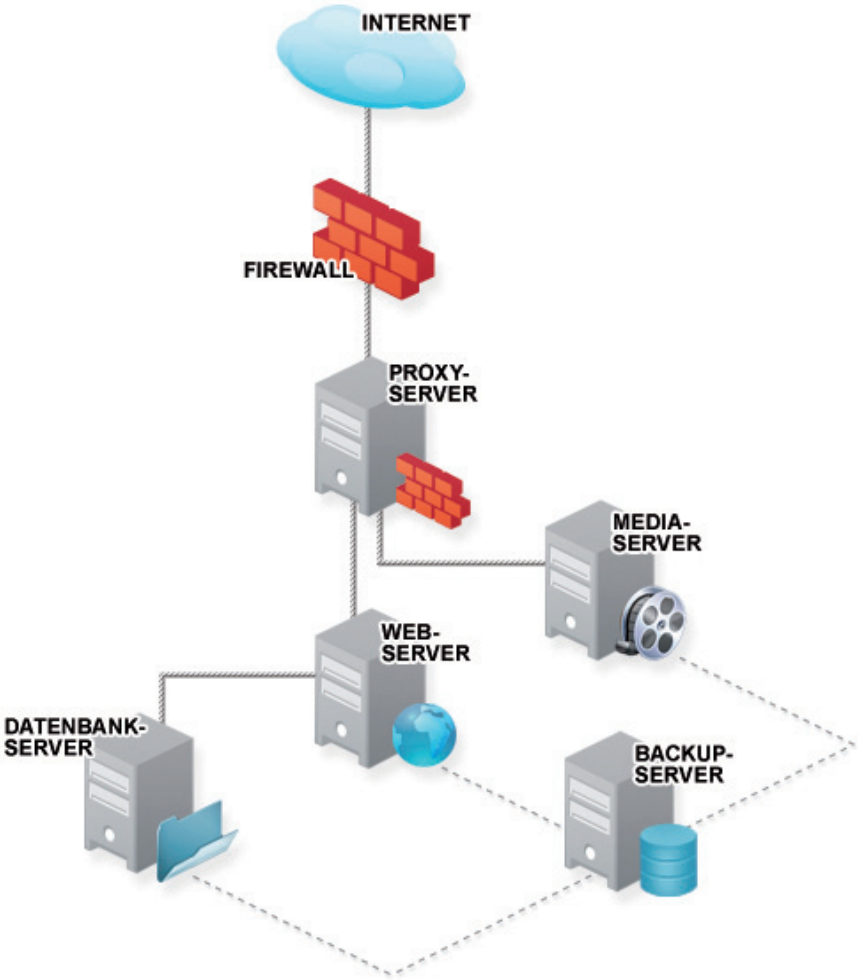
Leider sind viele Hoster mit diesbezüglichen Zahlen sehr sparsam. Ratsam ist es in diesen Fällen, sich an den großen Knotenpunkten des Internets zu orientieren: Wirbt ein Anbieter damit, an einen zentralen „Internet Exchange Point“ (IXP) angebunden zu sein, ist auch mit einer stärkeren Leitung zu rechnen. Der stärkste IXP Deutschlands steht in Frankfurt, weitere Knoten befinden sich in Berlin und Düsseldorf.

## 1.4 Best Practice

Beim Hosting-Anbieter CYBERDAY bewährt sich in aller Regel eine Kombination aus vier Systemen, einem Proxy- und Webserver sowie einem Media- und Datenbankserver.

Den Proxy- und Mediaserver könnte man aus Kostengründen auf dem Webserver mitlaufen lassen und so das System auf zwei Server reduzieren. Performanter und daher grundsätzlich empfehlenswerter ist jedoch die vorgeschlagene Lösung mit vier Systemen.

Zur Steigerung der Redundanz und Ausfallsicherheit kann man noch alle Server im Standby als Failover oder im Cluster verdoppeln.



# 2. Netzwerke und Dienste

## 2.1 Proxys

Der Betrieb des Proxy- (oder genauer: Caching-Proxy-)Servers gehört - gemessen an den Server-Ressourcen bzgl. Rechenzeit, Plattenbedarf und Netzbandbreite - zu den wichtigsten Komponenten eines Webservers.

Ein Proxy-Server kann mehrere Aufgaben übernehmen. Allgemein kann er dazu verwendet werden, den eigentlichen Server in ein geschütztes Netz zu stellen, wodurch er von außen aus nur durch den Proxy erreichbar ist. Auf diese Weise wird der Server vor Angriffen geschützt, da nur der Proxy mit seiner IP-Adresse Zugriff auf die Webserver hinter einer Firewall hat.

Gleichzeitig kann er verschiedenen Benutzern und Gruppen je nach Auslastung unterschiedliche Ressourcen zuteilen und so mit relativ geringem Aufwand eine Lastverteilung und hohe Verfügbarkeit erreichen.

Ein Caching-Proxy-Server beschleunigt Serviceanfragen durch Abrufen gespeicherter Inhalte aus einer früheren Anfrage, die vom gleichen Client oder auch von anderen Kunden gemacht wurde. Caching-Proxys halten lokale Kopien von häufig angeforderten Ressourcen und helfen somit Kosten zu reduzieren und die Performance deutlich zu erhöhen. Der Einsatz eines Proxy-Servers sollte für jeden professionellen Onlineshop „State-of-the-Art“ sein, um statische Seiten direkt ausliefern zu können, ohne die empfindlicheren Systeme (Shop-Engine, Datenbanken etc.) zu belasten.

Dynamischer Inhalt, so zum Beispiel die Abwicklung der Bestellung, wird weiterhin vom Webserver verarbeitet.

Ein Proxy-Server erhöht insgesamt die Performanz des Webshops deutlich, was unmittelbar die Nutzererfahrung verbessert und sich seit einiger Zeit auch positiv auf das Ranking in Suchmaschinen auswirkt.

## 2.2 Load Balancing/Clustering

Load Balancing/Clustering wird entweder als Ausfallschutz eingesetzt, da im Notfall einfach auf einen anderen (redundanten) Server umgeschaltet wird („failover“), oder zur Lastverteilung auf alle verfügbaren Server („load balancing“) genutzt.

Die zunehmende Komplexität moderner Web-Anwendungen erfordert in den meisten Fällen den Betrieb von mehreren Applikationsservern. Die Gründe hierfür sind vielfältig und reichen von steigenden Besucherzahlen über die Sicherstellung der Verfügbarkeit bis hin zu den stetig wachsenden Anforderungen der Web-Anwendungen selbst.

So wird es häufig sogar notwendig selbst statische Web-Seiten über mehrere Server zu verteilen, um somit deren zeitige Auslieferung sicherzustellen.

Die Bereitstellung von parallelen Webservern ermöglicht in Spitzenzeiten die Verteilung der Anfragen auf mehrere Schultern (Datenbanken/Webserver). Das Ziel ist, die Last der Anfragen auf den Onlineshop auf mehrere Server aufzuteilen und so den Shop bei einer Überlastung oder bei einem Hardware-Ausfall vor dem Totalausfall zu schützen.

Im Unterschied zu verteilten Rechnersystemen muss beim Load Balancing gewährleistet sein, dass der Anwender immer mit demselben Server in Verbindung bleibt, wie beispielsweise bei SSL-gesicherten Verbindungen oder mit Session-ID protokollierten Transaktionen, wie beim Online-Shopping üblich.

Load Balancing-Systeme gibt es als Hardware „out of the box“, aber auch als reine Software-Lösung, die man auf einer eigenen Maschine installiert. Welches Produkt am besten geeignet ist, kommt auf die Situation und die Anforderungen an.

## 2.3 Dedizierte Firewall

Eine Firewall ist ein Sicherungssystem, das ein Netzwerk vor unerwünschten Netzwerkzugriffen schützt. Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente. Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie unerlaubte Netzwerkzugriffe zu unterbinden.

Mit einer dedizierten Firewall lassen sich im Schadensfall einerseits IP-Adressen aussperren (Blackholing) und andererseits einzelne Zieladressen, beispielsweise eigene IPs oder URL, deaktivieren (Sinkholing).

Da alle Anfragen für den Onlineshop erst einmal zur Firewall gehen und dann erst zum Webserver, kann eine Firewall Angriffe, wie beispielsweise DDoS-Attacken abfangen und behandeln. Gleiches gilt auch, wenn der Datenverkehr des eigenen Onlineshops durch übermäßiges Crawlen Dritter empfindlich gestört wird.

## 2.4 Servervirtualisierung

Eine Servervirtualisierung ermöglicht es, mehrere Betriebssysteme gleichzeitig auf einem physischen Rechner auszuführen. Dies können mehrere Instanzen desselben Betriebssystems sein oder auch unterschiedliche Betriebssysteme zum Beispiel Windows und Linux-Systeme. Dabei läuft jedes System in einer isolierten Umgebung, die als „virtuelle Maschine“ bezeichnet wird. Virtuelle Maschinen verhalten sich für den Anwender und auch gegenüber anderen Systemen im Netzwerk wie eigenständige Rechner.

Teilweise werden für bestimmte Aufgaben eigene Server betrieben, beispielsweise dedizierte Mail-, Datenbank-, Bilder- und Webserver. Damit soll ein möglichst stabiler Betrieb der Anwendungen sichergestellt werden. Nachteil ist jedoch, dass die Rechenkapazitäten dieser einzelnen Server meist nicht annähernd ausgenutzt werden.

Gleichzeitig entstehen durch immer komplexere Serverlandschaften hohe Infrastrukturkosten. Die Servervirtualisierung ermöglicht es, die dedizierten Server auf virtuelle Maschinen zu verlagern. So kann die Anzahl der benötigten physischen Rechner reduziert und die Hardware-Auslastung deutlich verbessert werden.

## 2.5 Hochverfügbarkeit sicherstellen

Servervirtualisierung unterstützt auch bei der Sicherstellung einer Hochverfügbarkeit. Der Ausfall einer virtuellen Maschine beeinträchtigt die übrigen Gastsysteme auf demselben Server nicht und ein anderes System kann sofort die Aufgaben der ausgefallenen Maschine übernehmen.

Für den Fall, dass der gesamte Server ausfällt, werden üblicherweise Backup-Kopien der virtuellen Maschinen vorgehalten. Diese können dann innerhalb kürzester Zeit auf einer anderen Hardware-Plattform gestartet werden.

Im Enterprise Umfeld gibt es ausgeklügelte HA- (Hochverfügbarkeits-)Lösungen, welche entweder auf Virtualisierungs- oder Systemebene realisiert werden.

Die Kosten werden hierfür jedoch schnell sehr hoch, da man bei HA-Lösungen alle Systeme redundant bereitstellen muss. Dies fängt bei den Stromkosten an, geht über die notwendige Internetanbindung bis hin zu den einzelnen Netzwerkswitches und Servern. Eine 100%-ige Verfügbarkeit kann dennoch auch dann nicht garantiert werden.

Die „Deluxe"-Variante ist sicherlich mit zwei Rechenzentren zu arbeiten, welche allerdings einen ausreichenden Abstand voneinander haben sollten.

Wenn eine technische Hochverfügbarkeit erwünscht oder benötigt wird, ist es zudem notwendig, die Prozesse für die Software-Entwicklung entsprechend anzupassen. Nur so kann sichergestellt werden, dass in diesem Fall die Software die Systeme nicht beeinträchtigt.

## 2.6 Content Delivery Network (CDN)

Ein Content Delivery Network ist ein Netzwerk verteilter Server, bestehend aus einem Ursprungsserver und mehreren Cache-Servern. Es dient dazu, dynamische und statische Objekte performant und mit lediglich geringen Verzögerungen zu verteilen.

Fordert der Besucher eines Onlineshops eine Seite oder ein Bild an, prüft der Cache-Server, ob er es bereits besitzt. Falls ja, überträgt er die Daten unverschlüsselt oder SSL-verschlüsselt an den Nutzer. Liegt das Objekt noch nicht auf dem Cache-Server, leitet dieser die Anfrage an den Webserver weiter und lädt sich gleichzeitig den neuen Inhalt in den Cache.

### Ladezeiten verkürzen

Ein Browser verbraucht etwa 80 bis 90 Prozent der Ladezeit, um Inhalte zu laden, die kleiner als ein MByte sind. Dies betrifft beispielsweise Bilder, Texte und Produktvideos. Befindet sich der Internetsurfer in der Nähe des Servers, kann der Browser die angefragten Inhalte innerhalb von 30 Millisekunden mit dem Server verbinden und beginnen zu laden. Bekommt der Server in Frankfurt jedoch eine Anfrage aus dem 2.000 Kilometer entfernten Moskau, verzögert sich die Wartezeit auf bis zu 200 Millisekunden. Muss die Information einmal um die Welt, kann die Latenz sogar bis zu einer halben Sekunde betragen.

Content Delivery Networks verkürzen die Ladezeit und sorgen dafür, dass statische Objekte weltweit mit nahezu der gleichen geringen Latenz auf die Rechner der Internetsurfer ausgeliefert werden.

## 2.7 Backup

Für zusätzliche Sicherheit sorgen Backups auf andere Server, die mittels Backup Software und per (S)FTP oder Synchronisationsmechanismen wie „rsync" auf andere Server oder Rechenzentren übertragen werden. Interessanterweise bieten viele Provider ihren Kunden kein ausreichendes Sicherheitsnetz über Backups an. Dabei besteht der Aufwand weniger in der Erstellung eines Backups, sondern beim Wiedereinspielen im Ernstfall. Eine ausreichende Strategie für Sicherungen sollte den mindestens täglichen Abzug des Servers beinhalten, der bis zu zehn Tage vorgehalten wird und den der Kunde bei Bedarf entweder selbst wieder einspielen kann oder mittels dessen der Provider das System zeitnah zurücksetzt.

Die Sicherungen sollten zusätzlich an einem zweiten Ort aufbewahrt werden.

## 2.8 Konfigurationsmanagement

Der Betrieb von Server-Farmen erfordert ein durchdachtes Konfigurationsmanagement, damit von zentraler Stelle sämtliche Server und Dienste sicher und effizient verwaltet werden können. Die Verwaltung einer Vielzahl von Servern bringt die Herausforderung mit sich, über jeden einzelnen Server jederzeit die Kontrolle zu haben.

Softwareupdates, Konfigurationen und Dienste müssen überwacht und gesteuert werden. Diese Aufgaben werden beim Betrieb von komplexen IT-Strukturen nur durch die Anwendung automatisierter Konfigurationsmethoden kosteneffizient und verlässlich bewältigt.

Mit einem guten Konfigurationsmanagement wird die IT entlastet und die Gefahr, dass „etwas vergessen wurde“, also menschliches Versagen, kann quasi ausgeschlossen werden. Da allerdings der initiale Aufwand nicht zu unterschätzen ist, gilt es abzuwägen, ab wann sich ein Konfigurationsmanagement lohnt.

# 3. Monitoring

Eine permanente Analyse des laufenden Netztraffics führt zu einer frühzeitigen Erkennung von Auffälligkeiten bei den Lasten und der Hardware. So kann rechtzeitig entgegengewirkt und Schaden vermieden werden.

Selbstverständlich nutzen die besten Monitoring-Tools nichts, wenn diese nicht ständig überwacht werden. Da es jedoch kaum zumutbar (und bezahlbar) ist, einen Mitarbeiter abzustellen, der rund um die Uhr die Last des Webservers abliest, müssen diese Analyse- und Monitoringwerkzeuge so konfiguriert sein, dass bei Auffälligkeiten ein automatischer Alarmhinweis per SMS und E-Mail verschickt wird. Dieser Alarm darf allerdings auch nicht so feinkörnig eingestellt sein, dass er bei den geringsten Norm-Abweichungen ausschlägt. Es ist offensichtlich, dass Ausfälle und Engpässe zu den Geschäftszeiten völlig anders behandelt werden müssen, als beispielsweise nachts oder zu betriebsfreien Zeiten. Entscheidend sind auch der Grad der Verzögerung und die Dauer eines Ausfalls. Das bedeutet, dass jegliche Engpässe immer mit Rücksicht auf die Benutzer, die Zeit, die geschäftliche Relevanz, den Grad der Verzögerung usw. gewertet werden müssen.

Bei einem umfassenden Monitoring werden unter anderem folgende Hardware- und Netzwerkkomponenten, sowie Anwendungen und Dienste laufend überwacht:

## Hardware

- Systemlast
- Hardwarestatus der Festplatten, Lüfter und Netzteile
- Rechnertemperatur
- RAID Status
- Festplattenplatz

## Rechenzentrum

- Klima
- Temperatur
- Strom

### Netzwerk

- Traffic, Bandbreiten
- Router
- Switche
- Portstatus

### Backbone

- Latenz, Durchsatz
- Paket Delivery
- Gesamtverfügbarkeit

### Anwendungen und Dienste

- Datenbank
- Failover Status
- Backup
- Replikation und Cluster

## 4. Sicherheit geht über alles

Cyberangriffe auf Onlineshops haben Hochkonjunktur und ziehen stets einen wirtschaftlichen Schaden nach sich. So finden Attacken gerne ab Oktober statt, wenn für die Shop-Betreiber das wichtige, da umsatzträchtige Weihnachtsgeschäft beginnt. In dieser Zeit berichten Onlinehändler immer häufiger von Angriffen und auch Erpressungsversuchen.

Simon Huck, Geschäftsführer und Security-Experte des Enterprise-Hosters Cyberday GmbH, rät daher: „*Sinnvollerweise sollte sich jeder professionell ausgerichtete Shopbetreiber bereits beim Start seines Onlinegeschäfts mit seinem Provider darüber unterhalten, inwiefern sein Server wirkungsvoll geschützt werden kann. Angriffe wie DDoS-Attacken zählen ja in Wirklichkeit noch zu einer der harmloseren Angriffsarten. Weitaus schlimmer ist es, wenn beispielsweise sensible Daten vom Webserver gestohlen werden*.“

•

Nach Beobachtung von Cyberday scheuen jedoch leider nach wie vor die meisten Webseiten-Betreiber davor zurück, sich mit Sicherheitsthemen auseinanderzusetzen. Viele vertrauen nach dem „Prinzip Hoffnung“ lieber darauf, dass ausgerechnet ihnen schon nichts passieren würde – eine Vorgehensweise, die nicht nur fahrlässig ist, sondern auch nachteilig: Denn die wirkungsvollen Präventivmaßnahmen zum Schutz der Webseite gehören nicht nur zu den MUST DO’s eines professionell ausgerichteten Onlinehändlers, sie haben zugleich eine ganze Reihe weiterer – auch direkt wirtschaftlicher – Vorteile.

Nach Beobachtung von Cyberday scheuen jedoch leider nach wie vor die meisten Webseiten-Betreiber davor zurück, sich mit Sicherheitsthemen auseinanderzusetzen. Viele vertrauen nach dem „Prinzip Hoffnung“ lieber darauf, dass ausgerechnet ihnen schon nichts passieren würde – eine Vorgehensweise, die nicht nur fahrlässig ist, sondern auch nachteilig: Denn die wirkungsvollen Präventivmaßnahmen zum Schutz der Webseite gehören nicht nur zu den MUST DO’s eines professionell ausgerichteten Onlinehändlers, sie haben zugleich eine ganze Reihe weiterer – auch direkt wirtschaftlicher – Vorteile.

Folgende Punkte sollten bei der Auswahl des Shop-Providers beachtet werden:

- Ist das Betriebssystem auf einem aktuellen Stand und wurden alle Sicherheitsupdates installiert?
- Sind die relevanten Programme, wie beispielsweise PHP, Apache und MySQL auf einem aktuellen Sicherheitsstand?
- Sind die Server durch eine dedizierte Firewall gesichert?
- Sind nicht benötigte Ports auf dem Server geschlossen und nicht erreichbar? Im Normalfall werden nur die Ports 80 und 443 öffentlich benötigt, andere Ports sollten über VPN bereit gestellt werden.
- Werden die Zugangsdaten regelmäßig gewechselt?
- Gibt es einen Prozess, welcher die Logfiles analysiert, um Attacken frühzeitig zu erkennen?
- Werden die Backups regelmäßig geprüft und sichergestellt, dass diese im Notfall auch korrekte Daten beinhalten?
- Ist bekannt, wo die Server stehen und wer Zugang zu den Daten hat?

Im kostenlosen Ratgeber *So schützen Sie Ihren Onlineshop vor Hackerangriffen* wird detailliert aufgezeigt, wie man sich vor Hackerangriffen schützen und effizient vorbeugen kann: (http://www.cyberday-gmbh.de/Sicherheit_Whitepaper.php).

## 5. IT-Aufgaben beim Shophosting

Der Betrieb des Servers, der Webserver oder eines ganzen Serverclusters ist mit verschiedenen administrativen Aufgaben verbunden. Dabei genügt es nicht, das System einmalig aufzusetzen. Man muss es als tägliche Aufgabe ständig „im Auge behalten“, Updates sind zu installieren und Logfiles müssen ausgewertet werden, um aktuelle und sichere Systeme zu haben. Sollte dies nicht erfolgen, kann man sich quasi darauf verlassen, dass sich daraus ergebende Sicherheitslücken erkannt und ausgenutzt werden oder der Server mit der Zeit „voll läuft“ und langsamer wird.

### 5.1 Hardware

Gerade bei einem 24/7-Betrieb unterliegen Hardware-Komponenten einer hohen Belastung. Vor allem Festplatten, Lüfter und Netzteile müssen für einen Dauerbetrieb ausgelegt sein.

Ein zuverlässiges Monitoring gibt Aufschluss über den Zustand der Systeme und erlaubt dem Administrator rechtzeitig zu erkennen, wann etwas optimiert oder ausgetauscht werden muss. Empfehlenswert ist hier der Erwerb einer Herstellergarantie zur Lieferung oder im Idealfall sogar direktem Austausch von benötigten Ersatzteilen innerhalb eines Arbeitstages.

Nach Ablauf der Garantie empfiehlt es sich, systemkritische Komponenten auszutauschen und durch neue zu ersetzen. Hierzu gilt es, das Ende der Garantiezeit im Fokus zu behalten und idealerweise vor Ablauf dieser automatisch informiert zu werden.

## 5.2 Netzwerke und Dienste

Netzwerkauslastung und -verfügbarkeit der Services müssen mit entsprechenden Tools permanent überprüft werden, um Auffälligkeiten zu erkennen. Im Zweifelsfall muss hier sofort agiert werden, falls Unregelmäßigkeiten auftauchen. Tools wie CACTI oder Nagios stellen hier gute Open Source-Lösungen dar.

Da Software-Komponenten permanent weiterentwickelt werden, müssen diese periodisch eingespielt werden. Dies geschieht entweder automatisiert oder manuell. Nur so kann man von diesen Erweiterungen, Performanceverbesserungen oder auch mit dem Update geschlossenen Sicherheitslücken profitieren.

Sollten Updates nicht mehr möglich sein oder üblicherweise bei Release-Wechsel, werden neue Server benötigt. Wichtig ist hierbei, dass dem Administrator bekannt ist, was die Software-Entwicklung im Einsatz hat. Es wäre nicht das erste Mal, dass eine Software mit der neuesten Version von beispielsweise PHP nicht lauffähig ist. Von Vorteil ist es auch, wenn die Administratoren die Systeme sehr gut kennen oder auch bereits damit gearbeitet haben.

## 5.3 Vergleich interne vs. externe IT

Der Betrieb von ein bis zwei Servern ist keine extrem zeitintensive Aufgabe, aber die Tätigkeiten müssen regelmäßig ausgeführt werden. Gerade bei Problemfällen oder schnellen Problembehebungen muss eine sofortige Reaktion gewährleistet sein. Um dies sicherzustellen sind mindestens zwei fachlich kompetente Administratoren notwendig, was sich bei einer kleinen IT-Infrastruktur jedoch nicht lohnt.

Auch wenn Webseiten und Onlineshops meist während des Tages und in den Abendstunden besucht werden, müssen diese rund um die Uhr verfügbar sein.

Dies wiederum bedeutet, dass Updates und der Neustart von Servern, sowie der Austausch von Komponenten nachts zu erfolgen hat. Dies führt zu besonderen Anforderungen an das Personalmanagement und auch die Bereitschaft der Mitarbeiter Nachtschichten zu übernehmen.

Ein nicht zu unterschätzender Aufwand ist es, die jeweils aktuellen Versionen im Fokus zu behalten. Weiterhin ist wichtig zu wissen, welche Updates dringend notwendig sind und welche Komponenten man möglichst nicht auf die aktuelle Version portieren sollte.

Ein Administrator, der nur nebenbei das Webhosting betreut und sich auch noch bzw. vor allem um die interne IT zu kümmern hat, wird hier Schwierigkeiten haben, auf dem stets und notwendigerweise aktuellsten Informationsstand zu sein.

Zumindest bei ambitionierten Online-Projekten sollte sich ein Administrator nahezu ausschließlich um das Webhosting und die damit verbundenen Systeme kümmern können. Auch regelmäßige Weiterbildungen und Messebesuche sind von Vorteil, bspw. um im Gespräch mit anderen Administratoren verschiedene Hostingsituationen besprechen und lösen zu können.

Sollte jedoch die Serverfarm größer sein und sich die Software-Entwicklung im Hause befinden, empfiehlt es sich auf jeden Fall zu prüfen, ob auch das Hosting - der besseren Abstimmungsmöglichkeiten und des vorhandenen Arbeitsaufwands wegen - intern betrieben werden kann.

## 6. Auf den Provider kommt es an

Neben der Hardwareausstattung und der Netzwerk-Infrastruktur kommt es bei der Providerwahl vor allem auch auf den Service an. Wie stark der (fachkundige) Support beworben wird, lässt zudem darauf schließen, wie viel Entgegenkommen man bei anstehenden Systemaktualisierungen erwarten kann: Eine „proaktive Upgradesicherung“ heißt nämlich nichts anderes, als dass der Hoster den Kunden via E-Mail über vorliegende Upgrades auf dem Laufenden hält. Aktualisieren muss man aber selbst. Hier teilt sich dann auch das Feld der Managed-Server-Anbieter auf: Einerseits in Hoster, die unter „managed“ lediglich das Beherbergen von (virtueller) Hardware verstehen und andererseits in Anbieter, die zusätzlich die komplette Wartung der einzelnen Komponenten übernehmen.

### Starke und sichere Netzwerkanbindung

Die meisten professionellen Webhoster können eine schnelle und stabile Netzwerkanbindung vorweisen. Angesichts immer mal wieder vorkommender Störungen an einzelnen Netzknotenpunkten ist es aber von Vorteil, wenn der Hoster an mehr als einen zentralen Netzknoten angebunden ist. Das kann insbesondere dann wichtig sein, wenn auch international, und dabei insbesondere auch in Übersee, verkauft werden soll. Die beste Netzanbindung des Webhosters hilft allerdings nichts, wenn im gebuchten Hosting-Paket aus Kostengründen nur geringere Übertragungsdurchsätze enthalten sind oder bei zu viel Besuchern/Traffic der Durchsatz beispielsweise einfach auf 10 Mbit/s gedrosselt wird.

### Leistungsstarke Hard- und Software

Während für den Betrieb einer statischen Website günstigstenfalls auf der Hardware des Providers nur ein einfacher Webserver laufen muss, spielen bei einem Onlineshopsystem verschiedene Softwares ineinander, um die Shopseiten in das Internet auszuliefern und die benötigten Funktionen zu realisieren. So laufen bereits beim einfachen Ausliefern von Shopseiten diverse Datenbankaktionen ab und zu jedem Besucher muss eine eigene Verbindung („Session“) gehalten werden. Es liegt nicht am Shopsystem allein, ob diese Vorgänge im Hintergrund schnell (und zuverlässig) genug ablaufen können: Auch die Hardware, aber ebenso die Softwareelemente beim Hoster müssen entsprechend ausgelegt und optimal konfiguriert und gewartet sein.

### Gut geschulte, engagierte und ansprechbare Administratoren

Damit wird klar, dass beim Provider auch entsprechende Expertise und Engagement vorhanden sein sollte: Administratoren bei „Billighostern“, die rein auf Standardkomponenten vorbereitet sind und mit denen im Bedarfsfall womöglich nur über Kontaktformulare kommuniziert werden kann, sind auf individuelle Konfigurationen oder Anfragen oft gar nicht vorbereitet.

Dabei entstehen beim Betrieb eines Onlineshops regelmäßig Situationen, bei denen eine gute Kommunikation mit dem Hoster entscheidend ist. Zum einen greifen hier ständig viele Prozesse ineinander – auch zwischen dem eigenen Shop¬system und den Systemen Dritter (von Payment bis Logistik). Bei vielen beteiligten Systemen erhöht sich zwangsläufig auch die Anzahl von anfallenden Systemupdates, ob des eigenen oder der Dritter, wobei jedes Mal sichergestellt sein muss, dass der laufende Betrieb davon unbeeinträchtigt bleibt und auch im Anschluss alles wieder reibungslos miteinander läuft. Ein Hostingunternehmen, das über den reinen Webserver-Betrieb auch Erfahrungen im Hosting von Shopsystemen hat, kann wertvolle Hilfestellungen geben.

Zum anderen stehen Onlineshops heutzutage praktisch ständig unter „Beschuss“ von Kriminellen, die routinemäßig alle Systeme auf Schwachstellen abtasten und, wenn sie fündig werden, auch kompromittieren. Ebenfalls zugenommen hat das „Geschäftsmodell“ DDoS-Erpressung, bei der Shops kurzzeitig lahmgelegt werden, um Schutzgeld zu erpressen. Händler, die nicht zahlen, erleben in der Folge oft massive DDoS-Angriffe, die angesichts der Professionalität heute oft nicht so einfach abzuwehren sind. Liegt der Shopserver dabei auf einem Shared Server, so ist der Hoster oft gezwungen, ihn vorübergehend ganz vom Netz zu nehmen, um die anderen auf demselben Server liegenden Webangebote zu schützen.

Wenn ein direkt ansprechbarer technischer Kontakt beim Provider geboten wird, ist dies erfahrungsgemäß ein Vorteil, der durchaus einige Zusatzkosten wert ist.

## Ausfallsicherheit

Ist der Onlineshop für das Unternehmen strategisch bzw. für den Händler existenziell wichtig und ein Ausfall von einem Tag aus wirtschaftlichen Gründen nicht tragbar, wird eine Ausfallsicherheit von über 99% benötigt. Für eine 99,9%ige Ausfallsicherheit aber (was einer tolerierten Ausfallzeit von guten acht Stunden pro Jahr entspricht) ist ein Betrieb im Servercluster notwendig, was deutlich aufwendiger und entsprechend deutlich teurer ist. Andererseits skalieren solche Cluster auch besser – nicht nur bei Angriffen, sondern auch bei erwünschten Steigerungen der Zugriffe, beispielsweise im Weihnachtsgeschäft, bei erfolgreicher Viralwerbung oder bei Kampfangeboten. Immer wieder scheitern tolle Marketingkampagnen daran, dass die Shopserver mit dem plötzlichen Andrang nicht Schritt halten können. Als Beispiel ein Notebookangebot von Notebooks-billiger.de zum Kampfpreis: Binnen weniger Stunden fiel der eigentlich vorgesehene Facebook-Shop in sich zusammen und in der Folge ging zeitweise auch im normalen Webshop kaum mehr was bzw. war auch dieser fast lahmgelegt.

Zur Ausfallsicherheit gehört auch die Backup-Strategie. Nur eine Strategie, die dafür sorgt, dass alle Systembestandteile laufend und sinnvoll gesichert werden, und dass diese Sicherungen auch geeignet sind, aus ihnen im Notfall sehr schnell wieder ein laufendes System zu erstellen, bietet die Garantie, dass im Schadensfall der Webshop in erträglicher Frist wieder in Gang gesetzt werden kann.

Betrachtet man alle genannten Punkte, zeigt sich schnell, dass sich bei professionellen Onlineshop-Projekten ein ‘Billighosting’ eigentlich verbietet. Sinnvoll ist es, für die Wahl des eigenen Hostings andere Kunden nach ihren Erfahrungen mit dem jeweiligen Hosting-Provider zu befragen: Wie gut ist der Support tatsächlich? Bekommt man auf Fragen sachkundige Antwort oder nur Mails mit zusammengesetzten Standard-Textbausteinen? Und schließlich sollte man auch das Gespräch mit dem Anbieter direkt suchen. Denn die Providerwahl ist auch Vertrauenssache, weswegen es sehr wichtig ist, dass man am Ende vor allem auch ein gutes Gefühl mit der Wahl des Hosting-Partners hat.

## Dediziert ist nicht gleich dediziert

Webhosting-Provider werben gerne mit „virtuellen dedizierten Servern“, bei denen es sich in Wahrheit um Software-Lösungen handelt. Auf besonders leistungsfähiger Server-Hardware werden mehrere Software-Server betrieben, die sich wie dedizierte Server verhalten. Dies ist zwar eine kostengünstige Alternative zu einem Root Server, technisch betrachtet jedoch ein ungleichwertiges Angebot. Provider sollten zumindest klar erkenntlich darauf hinweisen. In diesem Fall gilt auch auf die verschiedenen Formen der Virtualisierung hingewiesen zu werden. So macht es einen deutlichen Unterschied, ob eine Komplett-, Para- oder Betriebssystem-Virtualisierung genutzt wird.

## 6.1 Provider Checkliste

- Wie häufig werden Backups erstellt und wie lange ist die Aufbewahrungsfrist?

  _____
  _____
  _____

- Was wird gesichert und wie ist der Prozess für die Wiederherstellung?

  _____
  _____
  _____

- Handelt es sich bei den eingesetzten Servern um Markenprodukte, so dass Speicherplätze problemlos erweitert werden können?

  _____
  _____
  _____

- Ist eine schnelle Skalierbarkeit der Systeme gewährleistet, um auf kurze Spitzen in der Belastung reagieren zu können?

  _____
  _____
  _____

- Ist die Skalierbarkeit bzw. Erweiterbarkeit des Hostings, beispielsweise bei erwarteten hohen Zugriffen durch einen TV-Beitrag oder reichweitenstarken Marketingkampagnen „on the fly“ und ohne Betriebsunterbrechung, zumindest nachts, möglich?

  _____
  _____
  _____

- Was sind die garantierten Verfügbarkeiten des Servers (nicht des Internetzugangs)?

  _____
  _____
  _____

- Gibt es eine Erstattung wenn das SLA nicht eingehalten wird?

  _____
  _____
  _____

- Wie sind die Server am Internet angeschlossen, wie gut ist die Anbindung, gibt es eine Drosselungsklausel?

  _____
  _____
  _____

## 6.1 Provider Checkliste Fortsetzung

- Ist der Server durch eine dedizierte Firewall gesichert?

  _____
  _____
  _____

- Wie sind die Reaktionszeiten bei Problemen und wie und zu welchen Uhrzeiten ist die Erreichbarkeit in Supportfällen?

  _____
  _____
  _____

- Gibt es versteckte Kosten wie beispielsweise eine kostenpflichtige Hotline oder hohe Stundensätze bei außerordentlichen Tätigkeiten?

  _____
  _____
  _____

- Wie ist die Qualität der Supportmitarbeiter einzuschätzen?

  _____
  _____
  _____

- Ist der Provider mit der Problemstellung vertraut?

  _____
  _____
  _____

- Ist dem Provider die verwendete Software bekannt?

  _____
  _____
  _____

## Autoreninformation

CYBERDAY®

Seit Bestehen der Agentur 1999 bietet die CYBERDAY GmbH Hosting auf Enterprise-Niveau für ihre Kunden an. CYBERDAY hat sich auf Individuallösungen spezialisiert und bietet eine Produktpalette von einzelnen Servern bis hin zu Clustern über mehrere Standorte.

Neben dem Hosting bietet CYBERDAY Software-Entwicklung von Internetapplikationen mit Schwerpunkt Shoplösungen an. Die mannigfaltigen Erfahrungen aus Projekten jeder Größe, ermöglichen eine 360-Grad-Betrachtung auf die Anforderungen an ein individuelles Hosting.

Als Ergebnis steht ein optimales und perfekt auf das Projekt abgestimmtes Produkt.

CYBERDAY betreibt ihre Server in verschiedenen Rechenzentren in Deutschland. Seit mehreren Jahren richtet sich CYBERDAY nach den PCI DSS Standards. Dadurch profitieren Kunden, die Kreditkartendaten speichern, da die Anforderungen bekannt sind und umgesetzt werden können.

## Und das ist der Autor

Simon Huck gründete 1999 die CYBERDAY KG, welche als erstes Kunstportal im Internet ein renommiertes Ansehen genießt. 2003 wurden die Internettätigkeiten in die neu gegründete CYBERDAY GmbH ausgelagert, welcher er heute als Geschäftsführer vorsteht.
In den vergangenen Jahren betreute Huck zahlreiche Kunden im Enterprise Umfeld sowie eine Vielzahl an KMUs. Heute leitet er hauptsächlich das Projektmanagement der Agentur und unterstützt Kunden in allen Aspekten des Hosting und in Sicherheitsthemen mit seiner langjährigen Erfahrung.

# Impressum

Der vorliegende Ratgeber ist eine kostenlose Publikation von:

Cyberday GmbH | Schwanthalerstraße 91 | 80336 München
Tel. +49 89 23 23 92 94 - 0
E-Mail: info@cyberday-gmbh.de
Web: www.cyberday-gmbh.de

Chefredakteur (für den Inhalt verantwortlich):
Simon Huck (info@cyberday-gmbh.de)

**Autor:**
Simon Huck

**Grafik, Layout & Satz:**
Uta Kroder (internetgarden®, Schwelm)

**Titelfoto:**
sturti/stuart rayner photographer limited - istockphoto.com

**Zuschriften unter:** info@cyberday-gmbh.de
Weitere Informationen erhalten Sie auf dem Webauftritt unter http://www.cyberday-gmbh.de



**Haftung:**
Das Autorenteam hat die in diesem Werk genannten Fakten sorgfältig und nach bestem Wissen gesammelt und aufbereitet. Das schließt jedoch nicht aus, dass sich trotz aufwändiger Kontrolle Fehler eingeschlichen haben. Insbesondere die Textteile, die sich auf juristische Sachverhalte beziehen, können kein Ersatz für eine anwaltliche Beratung sein. Außerdem ist zu bedenken, dass sich sowohl die Gesetzgebung als auch die Rechtsprechung im Fluss befinden. Der Herausgeber wird Sorge tragen, diesbezügliche wesentliche Änderungen zeitnah in das Werk einzuarbeiten.
Er kann jedoch keine Gewähr dafür übernehmen, dass alle Teile des Textes jederzeit auf dem aktuellsten Stand sind. Es obliegt der Sorgfaltspflicht der Nutzer, die genannten Fakten zu verifizieren. Der Herausgeber und das Team der Autoren freuen sich über konstruktive Kritik – sie ist ein Weg, die Qualität des Werkes fortlaufend zu verbessern.

Cyberday GmbH
Schwanthalerstraße 91
80336 München
Tel. +49 89 23 23 92 94 - 0
E-Mail: info@cyberday-gmbh.de
Web: www.cyberday-gmbh.de