shopanbieter.de
Das Portal für den Internethandel

CYBERDAY®

Whitepaper

DDoS-Attacken – keine Panik, schnell reagieren

Sofortmaßnahmen bei einem Angriff und deren Prävention

Herausgeber:
shopanbieter.de
in Zusammenarbeit mit
CYBERDAY GmbH

Whitepaper

CYBERDAY®

shopanbieter.de
Das Portal für den Internethandel

Hrsg.: shopanbieter.de
in Zusammenarbeit mit
CYBERDAY GmbH

Whitepaper

DDoS-Attacken – keine Panik, schnell reagieren

Sofortmaßnahmen bei einem Angriff und deren Prävention

Inhalt

Einleitung 04

Kapitel 1 Sofortmaßnahmen bei einer DDos-Attacke 05
1.1 Analyse des Netzwerkverkehrs 05
1.2 Anfragen ins Leere laufen lassen (Sinkholing) 05
1.3 Bestimmte IP-Adressen aussperren (Blackholing) 06
1.4 Sizing 06

Kapitel 2 Präventivmaßnahmen 07
2.1 Kommunikation und Verantwortlichkeiten mit dem Provider (ISP) klären 07
2.2 Einsatz von Analysemitteln und Monitoringtools 08
2.3 Absicherung der Netzwerkinfrastruktur 08

Fazit 10

Autoreninfo 11

Impressum 12

Einleitung

Distributed Denial-of-Service-Attacken (DDoS-Attacken) auf Onlineshops finden gerne ab Oktober statt, wenn für die Shop-Betreiber das wichtige, da umsatzträchtige, Weihnachtsgeschäft beginnt. In dieser Zeit berichten Onlinehändler immer öfter von Angriffen und, wie wir bei ▶ shopanbieter.de bereits Anfang 2011 ausführlich berichteten, auch Erpressungsversuchen.

Leider informieren noch viel zu wenige Onlinehändler die Öffentlichkeit, wenn Sie Opfer einer solchen Attacke wurden. Die beiden kürzlich bekannt gewordenen Fälle von ▶ Dawanda und ▶ Noblego führen jedoch wieder nur zu deutlich vor Augen, dass DDoS-Attacken nach wie vor eine aktuelle Bedrohung darstellen, die hohen Schaden bei den betroffenen Onlineshops verursachen können.

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, wie sein Server wirkungsvoll geschützt werden kann. 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 der CYBERDAY GmbH 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, wie im Folgenden aufgezeigt wird.

Distributed Denial-of-Service-Attacke (DDoS-Attacke)

Die Methode einer DDoS-Attacke ist vergleichsweise simpel: Ein Webserver (oder auch andere Services, wie FTP bzw. Mailserver) und das Netzwerk werden mit Anfragen schlicht überlastet.

Im Groben geschieht dies so: Normalerweise erhalten Webserver von dem Rechner eines Websitebesuchers aus eine Seitenanfrage, diese wird mit dem Ausliefern der angefragten Seite beantwortet. Bei einer DoS/DDoS-Attacke werden nun sehr viele Anfragen (beispielsweise über Botnetze) erzeugt, um so die technische Infrastruktur des Opfersystems zu überlasten. Die Systeme der Zielwebsite werden zunächst verlangsamt und können schließlich gar nicht mehr antworten (Denial of Service = den Dienst verweigern). Dies hat zur Folge, dass die Webseite nicht mehr ausgeliefert wird – Besucher sehen schlicht keine Inhalte mehr.

Solche Angriffe werden dadurch erleichtert, dass bei heutigen Webarchitekturen nicht nur einfache Webseiten vorliegen und ausgeliefert werden: Seiten von Onlineshops werden heute meist „on the fly“, also während der Ausgabe, mittels Datenbankabfragen zusammengesetzt. Gleichzeitig werden Benutzer-Sessions angelegt und gehalten etc. pp. Somit sind bei der Beantwortung von Website-Anfragen nicht nur die reinen Webserver-Dienste als mögliche Schwachstellen angreifbar, sondern auch die Datenbankschnittstellen, die Abfragen etc.

Dynamische Websites, wie es Onlineshops i.d.R. darstellen sind somit noch leichter angreifbar als rein statische Infoseiten.

Anmerkung: Bei den von Angreifern genutzten Botnetzen handelt es sich zumeist um Tausende von gehackten oder trojanerifizierten Rechnern von Privatnutzern in der ganzen Welt, deren Besitzer nichts davon ahnen, was ihre Computer „nebenbei“ so treiben.

Kapitel 1 Sofortmaßnahmen bei einer DDos-Attacke

Wurde der eigene Onlineshop Opfer einer DDoS-Attacke, gilt es sofortige Gegenmaßnahmen einzuleiten, um den Schaden so gering wie möglich zu halten.

Vorweg sei gesagt, dass sich die Ursachen einer DDoS-Attacke naturgemäß nicht abschalten lassen. Man hat keinen Zugriff auf die Botnetze. In dieser Situation helfen nur konsequente Abwehr-Maßnahmen. Die dann erfahrungsgemäß, jedoch schnell zum Erfolg führen werden.

1.1 Analyse des Netzwerkverkehrs

Die Analyse des eingehenden Netzwerkverkehrs ermöglicht es, die Angriffsmethode zu erkennen und bildet damit die Grundlage abgestimmter Gegenmaßnahmen.

Quell-Adressen

Zu klären ist woher die Angriffe kommen: Welche IP-Adressen bzw. welche IP-Netze werden genutzt und aus welchen Ländern kommen diese IP-Adressen? Nach wie vor kommen vor allem die „einfacher gestrickten“ Angriffe vor allem oder ausschließlich aus bestimmten Ländern.

Ziel-Adressen

Es ist zu prüfen, ob nur bestimmte IP-Adressen oder URLs des Webservers angegriffen werden.

1.2 Anfragen ins Leere laufen lassen (Sinkholing)

Falls bei der Analyse festgestellt wurde, dass nur eine spezielle IP-Adresse oder URL angegriffen wird, kann diese einzelne Zieladresse deaktiviert werden. Dadurch erreicht der Angreifer zwar sein Ziel, die Adresse nicht erreichbar zu machen, aber es werden unter Umständen Kollateralschäden auf dem Server vermieden.

Sind die Angriffe nicht auf wenige Zieladressen eingrenzbar, muss der wahrscheinlich schmerzlichste Eingriff bei der Abwehr einer DDoS-Attacke erfolgen.

Webserver abschalten

Bei einem Angriff geht in der Regel nicht nur der Shop an sich, sondern der gesamte Server in die Knie. Daher hat man in dieser Situation meist auch keinerlei Zugriff mehr auf das Shop-Backend und die Serveradministration.

Um überhaupt die notwendigen Maßnahmen ergreifen zu können, muss der Onlineshop daher meist für ein paar Stunden vom Betrieb genommen werden.

Ausnahme: Eine sog. „Backdoor“ ist eingerichtet. Diese Präventivmaßnahme ist jedoch aufwendig und deshalb selten vorhanden.

1.3 Bestimmte IP-Adressen aussperren (Blackholing)

Üblicherweise können bei der Analyse der Quell-Adressen eindeutige Muster abgeleitet werden. So stellt die CYBERDAY GmbH auf den von ihnen gehosteten Webseiten quasi täglich nicht nur gezielte DDoS-Angriffe sondern auch massive Crawling-Versuche vor allem aus China und Russland fest.

„Für den Seitenbetreiber spielt es letztlich ja keine Rolle aus welchen Gründen seine Webseite einer starken Belastung ausgesetzt ist. Wichtig ist, dass sein Provider dies rechtzeitig erkennt und rechtzeitig reagiert, also bereits bevor der Server unter der Last zusammenbricht. So können wir beispielsweise einen Teil der DDoS-Attacken mit unseren Maßnahmen abwehren, ohne dass der Seitenbetreiber überhaupt etwas von dem Angriff mitbekommt.“ beschreibt Simon Huck die Anforderungen an einen verantwortungsvollen Provider.

IP-Datenbanken

Können also mittels GEO-Datenbanken im Angriffsmuster bestimmte Angreifer-Länder klar lokalisiert werden, können länderbasierend IP-Adress-Bereiche ggf. komplett gesperrt werden. Dies ist jedoch nur möglich, wenn aus diesen Ländern keine (nennenswerten) Kundenströme kommen.

Früher reichte es oft sogar, einzelne angreifende IP-Adressen oder IP-Netze auszusperren. Diese Möglichkeit greift heute jedoch leider nur in ganz seltenen Fällen, weil die heutigen Botnetze meist aus Rechnern mit Standorten in der ganzen Welt bestehen – und oft auch viele Computer mit dynamischer Internetanbindung enthalten, die ihre IP-Adresse laufend wechseln.

Ist daher eine flächendeckende Sperre von IP-Adressen nicht möglich, sollte man die den Serversystemen vorgeschalteten Firewalls so konfigurieren, dass mehr als eine bestimmte Anzahl von Zugriffen von ein und derselben IP innerhalb eines zu definierenden Zeitraums blockiert wird. Diese Maßnahme trifft „böswillig“ anfragende Computer, weil diese enorm viele Anfragen senden, während echte Besucher bei normalem Surfverhalten deutlich weniger Anfragen auslösen und daher von solchen Blockierungen nur selten getroffen werden.

In der Folge der IP-Maßnahmen kann das Sinkholing dann in der Regel bereits wieder aufgehoben werden.

Der Vollständigkeit wegen sei noch erwähnt, dass die Angreifer auch inländische Botnetze nutzen oder die IP-Adressen fälschen könnten. Jedoch ist die Fälschung von IP-Adressen nicht trivial und auch eher selten. Auch inländische Botnetze kommen noch eher selten vor und machen wenn überhaupt in der Regel lediglich einen Teil, aber nicht das gesamte Botnetz aus.

1.4 Sizing

Oftmals ist der Abwehr einer DDoS-Attacke mit dem sogenannten Blackholing bereits Genüge getan und die Angreifer sind ausgesperrt. Waren diese Maßnahmen jedoch noch nicht ausreichend, sind umgehend die Kapazitäten des Webservers zu erweitern und zu prüfen inwiefern eine statische Seitenauslieferung möglich ist, um den Ansturm der Anfragen bewältigen zu können.

Dies war auch eine der beiden zielführenden Gegenmaßnahmen des kürzlich attackierten Onlineshops Noblego.de. So führt Benjamin Patock, Geschäftsführer des Betreibers Solid Taste GmbH aus: „*Wir haben im wesentlichen zwei Dinge getan, um die DDoS-Attacken dauerhaft abzuwehren. Zum einen sind wir zu einem Provider gewechselt, der bei großer Nachfrage mehr Skalierbarkeit ermöglicht. Und zum anderen haben wir einen Dienstleister dazwischengeschaltet, der uns zuverlässig vor DDoS-Attacken schützt.*“

Statische Seitenauslieferung sicherstellen

Bei dynamischen Shopsystemen ist oftmals nicht die Netzwerkverbindung oder der Webserver das schwächste Glied, sondern die notwendigen Datenbankabfragen in der Shop Software. Daher ist es wichtig, zumindest während eines Angriffes die Seiten über einen Proxy statisch ausliefern zu lassen. Wo Shopsysteme selbst die Möglichkeit bieten, auf statische Seiten (maximales Seitencaching) umzuswitchen, ist dies ein sehr schneller und einfacher Weg, angegriffene Systeme zu entlasten.

Traffic-Anbindung erweitern

Als Faustregel gilt, dass die Anbindung an das Internet mindestens mit einer 1 Gbit/s-Leitung erfolgen sollte.

Loadbalancing/Clustering

Die Bereitstellung von parallelen Webservern ermöglicht in Spitzenzeiten, wie es bei DDoS-Attacken der Fall ist, die Verteilung der Anfragen auf mehrere Schultern (Datenbanken/Webserver) und verhindert so ein Überlaufen der Speicher.

Diese geschilderten Maßnahmen des „Sizings“ sind nicht nur im Angriffsfall wichtig – sie stellen bereits einen Teil der sinnvollen Präventivmaßnahmen dar.

Kapitel 2 Präventivmaßnahmen

2.1 Kommunikation und Verantwortlichkeiten mit dem Provider (ISP) klären

Da es im Notfall insbesondere auf eine schnelle Reaktion ankommt, sollten Websitebestreiber bereits „in friedlichen Zeiten“ bestimmte Absprachen mit ihrem Provider treffen: So sollte der richtige Ansprechpartner mit Notfallnummer und den Erreichbarkeiten bekannt sein. Zudem muss klar sein, welche Leistungen seitens des Providers im Servicevertrag abgedeckt sind. Die Frage dabei ist, ob bzw. welche Maßnahmen im Ernstfall vom Provider ergriffen werden (dürfen) oder ob er den Webserver nur einfach abschaltet, bis der Shop-Betreiber selbst das Problem gelöst hat.

Auch Simon Huck von der CYBERDAY GmbH rät dringend: „*Man sollte sich stets bewusst halten, dass die genannten Sofortmaßnahmen in der Regel nicht zur Standardleistung eines Providers gehören und somit separat zu bezahlen sind bzw. höhere monatliche Hostingkosten bedingen.*“

Shopbesitzern muss auch klar sein, dass beispielsweise bei kostengünstigen Shared Hosting-Verträgen – auf denen durchaus sogar Onlineshops manchmal laufen – der Provider unter dem Zwang steht, im Angriffsfall auch die weiteren auf dem selben System laufende Anwendungen seiner anderen Kunden schützen zu müssen. Dies minimiert den Spielraum für Gegenmaßnahmen und führt oft dazu, dass das angegriffene System zugunsten der anderen „Mieter“ auf dem Webserver weichen muss.

2.2 Einsatz von Analysemitteln und Monitoringtools

Es sollten bereits im Vorfeld Anwendungen zur Verkehrs- und Dienstanalyse auf den Servern bereitgestellt werden, damit diese im Angriffsfall direkt zur Verfügung stehen und nicht erst nachinstalliert werden müssen. Gleiches gilt für die weiteren betroffenen Netzwerkkomponenten.

Eine permanente Analyse des laufenden Netztraffics führt zu einer frühzeitigen Erkennung von Auffälligkeiten. In den meisten Fällen von DDoS-Attacken wird nicht das gesamte Botnetz gleichzeitig aktiviert, sondern peu-a-peu zugeschaltet. Da sich Botnetze also quasi vorankündigen, können durch konsequentes Monitoring ggf. rechtzeitig wirksame Gegenmaßnahmen ergriffen 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.

2.3 Absicherung der Netzwerkinfrastruktur

Auch auf der Netzwerkebene können vorbeugende Maßnahmen für den DDoS-Fall getroffen werden.

Dedizierte Firewall

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 DDoS-Attacken abfangen und behandeln.

Proxy-Server

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.

Loadbalancer/Cluster

Wie bereits in den Sofortmaßnahmen geschildert, ermöglichen Loadbalancer und Clustering den Betrieb von mehreren parallelen Webservern, um so in Spitzenzeiten die Last zu verteilen.

Genauso wie ein Proxy-Server, erhöht auch das Loadbalancing insgesamt die Performanz des Webshops deutlich, was unmittelbar die Nutzererfahrung verbessert und seit einiger Zeit auch positiv auf das Ranking in Suchmaschinen wirkt.

Server härten – Hardening

„Härtung“ bedeutet, dass stetst wirklich nur die Dienste laufen, welche für das Ausliefern der Webseite notwendig sind. Abweichend von den üblichen Werten in den Voreinstellungen sollte der Server hierfür so konfiguriert werden, dass eine höhere Anzahl an zugelassenen Verbindungen auf der jeweiligen Hardware zugelassen wird. Dies stellt sicher, dass die Performance-Möglichkeiten der Hardware auch real zur Verfügung stehen.

Ports schließen

Auf dem Server sollten wirklich nur die Ports nach außen geöffnet werden, welche für den Betrieb der Seite unerlässlich sind. Die Konfiguration des Servers sollte darum so geändert werden, dass der Server möglichst wenig Angriffsfläche bietet.

Ein Webserver sollte beispielsweise nur TCP-Pakete auf Port 80 und 443 (für TLS/SSL) annehmen und den Rest aus dem Internet verwerfen.

Hinweis: Dies kann auch bereits als Filterung an der Firewall durchgeführt werden.

Die Dienste FTP, SSH und SCP sind Ports, die blockiert werden sollten oder der Zugang mittels IP-Restriction (Firewall) beschränkt sein sollte. Denn am Internet angebundene Systeme unterliegen laufend Port-Scans; für Angreifer ist dies eine Basis-Routine, offene Ports werden daher unmittelbar gefunden und können dann als Angriffsziel dienen.

Lasttests

Im Angriffsfall muss entschieden werden, ab welcher Last, also ab welcher Bandbreite, Anfrageanzahl pro Sekunde oder ab welcher Paketrate, ein Angriff als ernstzunehmend betrachten wird und eine Reaktion notwendig wird. Häufig genügt es, das Ausmaß des Angriffs erst einmal intensiv zu beobachten.

Vor diesem Hintergrund ist es wichtig, die Leistungsgrenzen der Systeme zu kennen. Zu beachten ist dabei, dass nicht alleine die Parameter des Webservers entscheidend sind. Vielmehr sind bei der Identifikation der Leistungsgrenzen insbesondere auch die Netzwerkkomponenten mit einzubeziehen, die sich auf den wahrscheinlichen Angriffswegen befinden (Paketfilter, Switche, Router, etc.).

Traffic-Anbindung sicherstellen

Abhängig von den Lasttests sind die Kapazitäten der Traffic-Anbindung zu erweitern. Wie bereits geschildert gilt als Faustregel, dass die Anbindung an das Internet mindestens mit einer 1 Gbit/s-Leitung erfolgen sollte.

Dedizierte Appliance zur Abwehr von DDoS Attacken [DDoS-Mitigation Appliances]

Es gibt eine ganze Anzahl von Hardware- ("Hardware DDoS Firewall") und Software-Lösungen (z.B. zum "Traffic Scrubbing"), die DoS-, und auch DDoS-Angriffe abwehren bzw. die eigenen Systeme vor Überlastungen schützen sollen. Ob damit im Ernstfall tatsächlich eine Abwehr gelingt, hängt jedoch immer auch davon ab, wie „gut" (technisch versiert und aufwendig gestaltet) die Angreifer vorgehen. Denn so wie die Verteidiger entwickeln natürlich auch die Angreifer ihre Werkzeuge wie im Hase-und-Igel-Spiel ständig weiter. Zudem sind solche speziellen Schutz-Komponenten teuer.

Daneben gibt es auch spezialisierte Dienstleister, die die IP-Adresse des Shops verschleiern. Hierzu wird nach außen die Shop-IP auf eine eigene IP-Adresse geändert und der Datenverkehr erst von dieser aus wieder auf das Shopsystem umgeleitet. Die Antworten des Shopsystems werden dann vom Dienstleister sozusagen „im Namen des eigentlichen Shopsystems" ausgeliefert. Dabei wird der Datenverkehr ständig überwacht und notfalls „gesäubert" („Traffic Scrubbing").

Manche dieser Anbieter geben sogar Garantien, dass dieser Mechanismus gegen DDoS Attacken wirksam sei, nehmen allerdings keine Kunden an, welche aktuell attackiert werden.

Neben den Kosten, die für solche Dienstleistungen entstehen – und die z.B. bei einer Berechnung auf Basis des durchgeleiteten Traffics im Angriffsfall explodieren können – muss generell bedacht werden, dass man bei solchen Diensten praktisch die Hoheitsgewalt über den eigenen Datenverkehr aus der Hand gibt. Zudem entstehen durch die Zwischenfilterung und Umleitung Geschwindigkeitsverluste.

Patch- und Sicherheitsmanagement

Auch wegen der schnellen Weiterentwicklung der Angriffsmöglichkeiten sollten Websitebetreiber ihre Systeme und Shop Software standig auf dem aktuellsten Stand halten, um bekannte Schwachstellen zu identifizieren und zu schließen. Dies gilt jedoch auch für die Mitarbeiter der verantwortlichen IT-Abteilung bzw. des Providers seines Vertrauens.

Fazit

Gegen DDoS-Attacken kann man sich letztlich nur auf Netzwerkebene schützen bzw. im Notfall agieren, indem man das Netzwerk „dicht“ macht. Maßnahmen auf Serverebene, wie das Sizing, sind als flankierende Maßnahmen zu verstehen, da diese dazu beitragen, DDoS-Attacken unwirksam zu machen.

Auch wenn man im Falle einer DDoS-Attacke sofort reagieren muss, besteht kein Grund für Panik. Mit den richtigen Gegenmaßnahmen bekommt man diese meist in relativ kurzer Zeit in den Griff.

Die erste Handlung sollte stets das Gespräch mit dem Provider sein. Dieser kann prüfen, ob es sich tatsächlich um eine DDoS-Attacke handelt und woher diese kommt. Bei einem klar erkennbaren Muster sollte man umgehend die entsprechenden Sofortmaßnahmen einleiten.

Es sollte nicht versäumt werden, eine Strafanzeige zu stellen. Denn DDoS-Attacken benötigen ein hohes Maß an krimineller Energie mit der Absicht, jemand anderem einen Schaden zuzufügen. Schließlich ist es auch nicht so einfach ein Botnetz aufzubauen. Verfolgt man die einschlägigen Foren, findet man eine Vielzahl an günstigen Angeboten zur Miete von ausländischen Botnetzen. Wobei auch die Anmietung eines inländischen Botnetzes, nach Aussage eines Providers, nicht erheblich teurer sein soll.

Simon Huck von der CYBERDAY GmbH empfiehlt abschließend: *„Als wichtigste Präventivmaßnahmen gilt es, den Shop mittels einer dedizierten Firewall zu schützen und beim Hosting auf eine gute Skalierbarkeit des Systems zu achten, um im Notfall ggf. umgehend reagieren zu können. Skalierbarkeit ist dabei nicht nur für DDoS-Attacken wichtig, sondern auch wenn der Onlineshop unvorhergesehen einen plötzlichen Ansturm an Besuchern erhält. Sei es, dass man überraschend von einer reichweitenstarken Webseite verlinkt wird oder ein Bericht in einer auflagenstarken Publikation erscheint.“*

Autoreninformation

shopanbieter.de ist ein Info-Portal, dass ganz auf den Bedarf von Betreibern Online-Shops jeder Unternehmensgröße zugeschnitten ist. Neben dem größten deutschsprachigen Anbieterverzeichnis, ist shopanbieter.de insbesondere für seine meinungsbildenden Fachartikel und den praxisnahen Whitepaper bekannt. Deren Publikationen gelten in der Branche regelmäßig als Leitmedium in der Branche für das jeweils behandelte Thema.

shopanbieter.de ging 2004 als Bookmarksammlung zum Thema Shopsysteme online. Im Februar des darauffolgenden Jahres wurde der erste Artikel im Blog veröffentlicht. Dieses hat sich schon in kürzester Zeit sehr erfolgreich entwickelt und gilt heute als eines der bekanntesten deutschsprachigen E-Commerce-Portale.

Seit Bestehen der Agentur 1999 bietet die CYBERDAY GmbH Hosting auf Enterprise-Niveau für seine Kunden an. Die CYBERDAY GmbH hat sich auf Individuallösungen spezialisiert und bietet eine Produktpalette von einzelnen Servern bis hin zu Clustern über mehrere Standorte. Die CYBERDAY GmbH betreibt seine Server in verschiedenen Rechenzentren in Deutschland.

Und das sind die Autoren

Peter Höschl bewegt sich seit 1997 beruflich im Internethandel, gilt als E-Commerce Experte und verfügt über große gelebte Praxiserfahrung. Er ist Autor mehrerer Fachbücher und einer Vielzahl von Fachartikeln zu allen Aspekten des Onlinegeschäfts, für verschiedene Wirtschafts- und E-Commerce-Publikationen. Heute berät und begleitet er vor allem mittelständische Unternehmen im E-Commerce. Schwerpunkte hierbei sind: Strategieentwicklung, Daten Management, Shop- / Marktplatz Management, Steuerung / Controlling E-Commerce, Online-Marketing und die Lieferantenbeziehung zu Online-Händlern.

Simon Huck gründete 1999 die CYBERDAY KG, welches 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 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.

CYBERDAY®

shopanbieter.de
Das Portal für den Internethandel

Impressum

Der vorliegende Ratgeber ist eine kostenlose Publikation von:
shopanbieter.de | Haydnstr. 21 |
85521 Ottobrunn bei München
Tel. +49 89 470 77 941 | Fax +49 89 665 93 747
E-Mail: info@shopanbieter.de
Web: www.shopanbieter.de
Chefredakteur (für den Inhalt verantwortlich): Peter Höschl (info@shopanbieter.de)

Autoren
Peter Höschl | Simon Huck - CYBERDAY GmbH

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

Titelgrafikelement:
tiero / fotolia.com

Zuschriften unter: info@shopanbieter.de
Weitere Informationen erhalten Sie auf dem Webauftritt unter http://www.shopanbieter.de

Urheberrecht
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechts ist ohne Zustimmung des Herausgebers unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung sowie die Verarbeitung in elektronischen Systemen.

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 Recht-sprechung 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.