shopanbieter.de
Das Portal für den Internethandel

ratgeber.

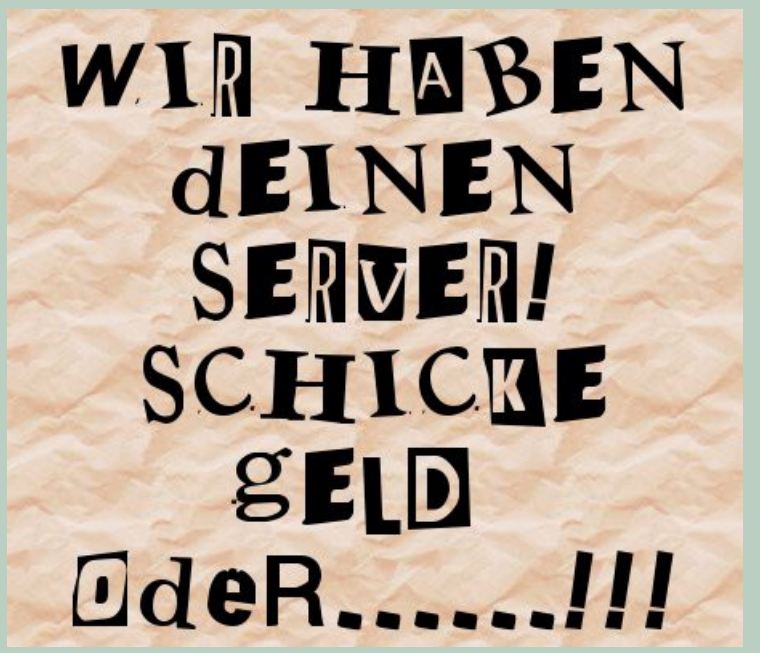
Fachartikel
Nicola Straub, Shopanbieter.de

Nachgefragt
DDoS-Schutzgelderpressung – was tun?

ratgeber.

Inhaltsverzeichnis

Das Phänomen



Die Androhung von DDoS-Attacken als Druckmittel bei Erpressungen zu benutzen tauchte in der Öffentlichkeit erstmals mit der Fußball-Europameisterschaft 2004 auf: Mehrere Online-Wettbüros, darunter auch mybet.com wurden zur Zahlung von 15.000 Dollar aufgefordert, *„andernfalls würden sie die Internet-Präsenz des Unternehmens mit einem gezielten DDoS-Angriff (Distributed Denial of Service) abschießen“* (heise.de-News). Nachdem die Drohmails zunächst ignoriert worden waren, folgte ein Angriff, der mybet.com für 16 Stunden lahmlegte.

Mittlerweile sind DDoS-Angriffe zu einer Standardwaffe bei Auseinandersetzungen im Internet geworden, die nicht nur von Wirtschaftskriminellen genutzt wird, sondern auch von politischen Aktivisten (siehe Wikileaks-Auseinandersetzung).

Die Methode

Die Methode einer Distributed Denial-of-Service-Attacke (DDoS-Attacke) ist vergleichsweise simpel: Ein Webserver (oder auch andere Services, wie FTP, Mailserver...) wird 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/DDdoS-Attacke werden nun sehr viele Anfragen erzeugt, um so die technische Infrastruktur des Opfersystems überlasten. Dieses wird zunächst verlangsamt und kann schließlich gar nicht mehr antworten (Denial of Service = den Dienst verweigern). Dabei kommt erschwerend hinzu, 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.

Die Erpressungen verlaufen i.d.R. so: Ein Händler erhält eine Erpressermail, in der eine (meist überschaubare) Geldsumme per Zahlung via Ukash oder PaySafeCard verlangt wird. Dabei wird entweder auf eine zeitnah zurückliegende Downtime des Shops von wenigen Minuten verwiesen oder eine solche für in Kürze angekündigt. Mit diesem Kurz-Angriff soll die Forderung untermauert werden. Bei Nichtzahlung bis zu dem gesetzten Termin wird mit einer längerfristigen Störung des Shopbetriebes gedroht.

Dass diese Drohungen durchaus ernst zu nehmen sind, bestätigt Hostingprovider **1&1**:

> *„In der Regel sind es professionell organisierte Banden, die hinter den Erpressungsversuchen stecken. Diese sind rund um den Erdball verstreut und verfolgen ihre Interessen knallhart. Es gibt immer häufiger aber auch wenig ernstzunehmende Trittbrettfahrer, die das schnelle Geschäft wittern.“*

Ausmaß des Problems

Bereits 2005 berichteten Medien, dass sich Unternehmen zunehmend DDoS-Erpressungsversuchen ausgesetzt sähen. Heute verfügen Kriminelle über eine gut ausgerüstete Infrastruktur an Botnetzen, in denen Millionen Computer mit Internetzugang auf Knopfdruck zusammengeschlossen und ferngesteuert werden können. Diese Netzwerke können zu erstaunlich billigen Preisen minuten-, stunden- oder tageweise gemietet werden, so lag nach Untersuchungen der Analysten von VeriSign iDefense Mitte 2010 die Preise für 24 h bei unter 55,- Euro (Quelle), nach eigenen Recherchen sind DDoS-Dienste jedoch mittlerweile auch erheblich günstiger buchbar (s. Abb.).

Hinzu kommt, dass dank „Out-of-the-Box“-Lösungen auch eigene Netze ohne vertiefende Kenntnisse sehr schnell aufsetzbar sind, wie die Rache-Aktionen gegen Paymentunternehmen im Zuge der Wikileaks-Verfolgung zeigten.

[redacted] > Marketplace > Service Offerings > High-Grade 300gb/s+ DDoS for Hire/Rent

Full Version: High-Grade 300gb/s+ DDoS for Hire/Rent

You're currently viewing a stripped down version of our content. View the full version with proper formatting.

Pages: 1 2 3 4 5 6 7 8 9

[redacted] 02-08-2010, 11:44 PM

Services:

Linux based DoSnet, pushes over 300gb's upstream. People, Servers, Clusters, Corporations, Small ISP's, if you want it knocked offline we can do it. These bots are also for Sale/Rent/Hire.

Prices:

DDoS Pricing depends on bandwith required/length desired, anywhere from $1 for host booting/single machines to $1000+ for Corps and ISP's.
Renting is $10 for 7 days per Bot, renters must come into our IRC Channel.
Buying is $25 per bot, IRC server and Channel provided if needed

Contact us for pricing/details

Mietbare Botnetze bestehen nicht nur aus Serverfarmen in „Schurkenländern“, sondern auch aus Computern ahnungsloser Nutzer, die dank unzureichender Schutzmaßnahmen „gekapert“ wurden. Wer heute Botnetze mieten möchte, findet daher Angebote mit Rechnerstandorten in allen Ländern – einschließlich Deutschland.

Weil die Mittel für DDoS-Angriffe mittlerweile so verbreitet und gut steuerbar sind, sind Erpressungen mit DDoS-Drohungen zu einer gängigen kriminellen Methode geworden. So erleben Provider regelmäßig DDoS-Angriffe auf Websites ihrer Kunden, wobei aber nicht immer auch ein konkreter Erpressungsversuch hinter den Angriffen stehen muss, wie **1&1** betont:

> *„DDoS-Attacken können sehr unterschiedliche Ziele verfolgen und gehen nicht zwangsläufig mit einer Erpressung einher. Konkrete Zahlen zu nennen, ist daher schwer. Generell, also nicht nur im Weihnachtsgeschäft, ist hier aber eine deutliche Zunahme zu verzeichnen.“*

Auch Provider **Strato** berichtet, regelmäßig mit dem Problem konfrontiert zu sein:

> *"Denial of Service Attacken" (DDoS) versuchen Hacker regelmäßig, Server durch eine große Zahl von Anfragen von unterschiedlichen Adressen arbeits-*

> *unfähig zu machen. Davon ist STRATO, wie andere Provider auch, ebenfalls häufig betroffen.“*

Provider **Host Europe** widmet sich diesem Problem mit besonderen Anstrengungen:

> *„Das Thema ist definitiv eine Herausforderung für die gesamte Hosting-Branche und wir sind der Auffassung, dass unser bereits aufgebautes Know-How, das Engagement und die weiteren Planungen der Weg in die richtige Richtung sind.“*

Obwohl Onlineshops in der Vorweihnachtszeit besonders erpressbar scheinen, konnte Host Europe trotz besonderer Aufmerksamkeit keinen Anstieg in dieser Zeit feststellen:

> *„Entgegen unserer Erwartung kam es jedoch in der Weihnachtszeit nicht zu einem Anstieg, im Gegenteil die uns gemeldete bzw. festgestellte Anzahl von solchen Fällen ist rückläufig.“*

Host Europe berichtet zudem von einer internen Befragung des Providerverband eco.de. Auch diese habe ergeben, dass *„das Problem sich jedoch nicht zu einer "globalen" Bedrohung entwickelt sondern im Vergleich zu der Anzahl der nicht betroffenen Kunden überschaubar ist.“*

Alle befragten Provider betonen, dass sie gut gerüstet und durch die laufenden Angriffe auch routiniert darin sind, solche abzuwehren. So verfügt 1&1 über mehr als 40 Mitarbeiter, die sich gezielt mit Internet-Kriminalität beschäftigen. STRATO schreibt auf Nachfrage, dass es „im Rahmen einer Forschungskooperation mit dem Max-Planck-Institut für Informatik intelligente Filtermechanismen für die eigene Plattform entwickelt [hat], die gezielt Rechner ermitteln, die Teil eines Botnetzes und häufig Quelle von DDoS-Attacken sind. Damit sind wir in der Lage, schädlichen Traffic aus Botnetzen von vorn herein abzulehnen. So sind 99,99 Prozent aller Angriffe für unsere Kunden nicht sichtbar, weil sie automatisch abgewehrt werden. Auch Host Europe beschäftigt sich eingehend mit der Problematik von DdoS-Angriffen und bietet ausführliche Anleitungen und technische Hintergrund-Infos an (s. u.).

Reaktionsmöglichkeiten

Wenn eine Erpresermail eingeht (oder eine unerklärliche Downtime des Webshops/der Website auftritt) sollte die erste Reaktion stets sein, **den Provider zu benachrichtigen**. Denn es gibt einiges, was der (bzw. bei eigenen Servern man selbst) tun kann, um den Angriffen zu begegnen. Läuft die Website auf einem shared Hosting Paket, ist die umgehende Benachrichtigung des Providers schlicht auch eine Frage der Fairness: Denn hier liegen auf demselben Server ja auch Webseiten Dritter, die bei Angriffen automatisch in Mitleidenschaft gezogen werden. Für Shops auf Shared Hosting-Paketen sollte bei angedrohten DDoS-Angriffen daher — wenn möglich — auch ein schneller Umzug auf einen dedizierten Server erfolgen.

Die zweite Reaktion sollte **eine Anzeige bei der Polizei** sein. Leider scheinen nicht allzu viele Erpressungsopfer diesen Weg zu gehen. So weisen die Statistiken des LKA NRW für das vergangene Jahr nur 102 Anzeigen wegen „Erpressung/Datendiebstahls“ auf, davon waren 14 reine „Versuche“. Die Pressestelle des LKA NRW betont, dass die Anzeige auf jeder örtlichen Polizeidienststelle aufgegeben werden kann. Die Polizei verfügt mittlerweile über geschultes Personal zur IuK-Kriminalität, die die Beweismittel (das ist zunächst einmal die Erpressermail) auswerten können.

Um einem DDoS-Angriff **auf technischer Ebene zu begegnen**, gibt es veschiedenste Möglichkeiten. Zunächst geht es darum, den Angriff festzustellen und zu analysieren. Host Europe, das seine Erfahrungen mit und die Vorgehensweise bei DDoS-Angriffen sehr offen mitteilt, gibt eine Empfehlung zur Vorgehensweise zur Detektion und Analyse von DDoS-Angriffen. Diese bezieht sich naturgemäß auf die Gegebenheiten bei Host Europe, andere Hoster bieten jedoch ggf. vergleichbare Services, so dass auch dort ein analoges Vorgehen möglich sein kann:

> *1. Im Kundenportal KIS einen Blick auf die Auslastung des Switch Ports werfen um grob zu erkennen mit was man es zu tun hat:*

-> Massiver Anstieg der eingehenden Pakete?
-> Massiver Anstieg des eingehenden Traffics?
-> In welchem Umfang kann das eigene System noch gen Internet ausliefern?

2. Serverseitig eine IST-Aufnahme der TCP/IP Kernelparamter (Linux) erstellen sowie die Connection Table auswerten um das Ziel zu lokalisieren

3. Serverseitige Gegenmaßnahmen einleiten (TCP/IP Kernelparameter via /proc/sys/net/ipv4/ tunen, GEO-IP Firewalling in Erwägung ziehen)
-> Sollte eine Cisco Hardware Firewall gebucht sein folgenden Artikel im Hinterkopf halten: Netwerksicherheit/DDoS
http://faq.hosteurope.de/index.php?cpid=16056

4. Nach Ziel-Lokalisierung (sofern dies eindeutig möglich gewesen ist) in Erwägung ziehen, selbiges zu deaktivieren um die Auswirkung auf andere Web/Services auf dem System zu minimieren

Als erste Reaktion reicht laut Host Europe oft das **Aussperren der ausländischen IPs** bereits aus, die Angriffe abzuwehren:

In nahezu alle Fällen (Wir sprechen hier wirklich nur von den Fällen wo die Erpresser Geld via Ukash oder PaySafeCard verlangten und nicht von Bandbreiten Floods die Server oder gar Switch Uplinks überlasten) reichte es aus auf dem Kundensystem eine Länderbasierende Software Firewall zu installieren die den Zugriff nur von den Ländern aus erlaubte die der Kunde als essentiel für das Tagesgeschäft angab.

Im Detail sorgte ein Script dafür dass nur die IP Allokation die mit einem gewünschten Ländercode verknüpft sind (ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest) zugreifen durften.

Solange die Angriffe aus „exotischen“ Ländern laufen, in die nicht verkauft wird – und die Absender-IPs entsprechend zuordenbar (also nicht gefälscht) sind, ist dies sicherlich die einfachste Möglichkeit der Abwehr.

Professionelle Angreifer gehen heute allerdings mitunter auch geschickter vor, so fälschen sie beispielsweise die IPs oder greifen direkt mit inländischen Botnetzen an. Ein

Ausperren der IP-Adressen würde dann dazu führen, dass auch diverse echte Kunden abgewiesen werden: Nämlich die, deren IP-Adresen für die Fälschung hergenommen wurden und/oder solche, die dynamisch eben erst gesperrte IPs von ihren Providern zugewiesen bekommen.Eine weitere schnelle und einfache Maßnahme ist es, die Zeiten herunterzusetzen, in denen Verbindungen vom Webserver gehalten werden. Denn so werden die Serverressourcen geschont. Host Europe hierzu:

> *Wenn dann weiterhin gespoofte Anfragen (TCP SYN) oder HTTP GET / Requests angekommen sind die zu einer Überlastsituation geführt haben wurden die Kernelparameter des TCP/IP Stack erweitert um allokierte Ressourcen schneller freizugeben.*

Da bei dynamischen Shopsystemen oft gar nicht die Netzwerkverbindung oder der Webserver, das schwächste Glied bei DDoS-Angriffen darstellen, sondern die notwendigen Datenbankabfragen im Shopsystem, ist es vorteilhaft, während eines Angriffes **das System auf eine statische Shopversion** umschalten zu können. Diese Option bieten jedoch leider nicht alle Shopsysteme.

Besondere Schutzmaßnahmen

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, so kosten beispielsweise die spezialisierten Produkte von RioRey je nach Dimensionierung zwischen 14.000-50.000 Euro.

Natürlich bieten auch Hosting-Provider spezielle DDoS-Schutz-Service-Pakete an, Beispiele sind AT&T oder Swisscom. Auch Host Europe arbeitet nach eigenen Angaben an einem entsprechenden Servicepaket.

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 sowie die Antworten des Shopsystems vom Dienstleister sozusagen „im Namen des eigentlichen Shopsystems“ ausgeliefert. Dabei wird der Datenverkehr ständig überwacht und notfalls „gesäubert“ („Traffic Scrubbing“). Folgende Anbieter bieten derartige Lösungen an:

http://www.serverorigin.com/ethproxy-ddos-mitigation
http://www.blockdos.net/process.html
http://www.prolexic.com/
http://www.gigenet.com/ddos-protection.html
http://www.ddosprotection.com/
http://ultradns.com/technology/dnsshield.html

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 nach Traffic 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.

Ein Erfahrungsbericht

Shopbetreiber sind meist Verkaufsprofis, aber keine Netzwerk-Experten. So treffen Schutzgelderpresser nicht selten zunächst einmal auf ratlose Opfer — tatsächlich setzt das „Geschäftsmodell“ der DDoS-Erpressung genau hierauf, wie der Erfahrungsbericht des Spirituosenshops www.bottleworld.de zeigt. So wurde für die erste Mail sicherlich nicht zufällig das Wochenende gewählt:

> *Wir erhielten die 1. Mail in einer Nacht von Freitag auf Samstag, was ein denkbar schlechter Zeitpunkt ist wenn es um Reaktionszeiten geht, schließlich haben auch Shopanbieter ein Wochenende. Uns wurde mit einem 1. Testlauf gedroht, der der Veranschaulichung dienen sollte.*
>
> *Tatsächlich hatten wir Samstags einen Ausfall von 5 Minuten. In der Nacht von Samstag auf Sonntag wurde uns dies berichtet und mit weiteren ausgedehnten*

ratgeber.

Angriffen gedroht, die sich bereits Sonntag fortsetzen sollten. Diese Mail im exakt gleichen Wortlaut haben wir dann jede Nacht zw. 1 und 2 Uhr erhalten über einen Zeitraum von etwa 1 Woche.

Zum Vorgehen und unseren Gegenmaßnahmen. Montags haben wir erst mit dem Hoster gesprochen, der bereits Gegenmaßnahmen ergriff. Wir lagen zu der Zeit auf einem kleinen Paket im Sharedhosting. Uns wurde nahegelegt auf einen dedizierten Server zu wechseln, andernfalls müsse man uns von Seiten des Hosters offline schalten um die weiteren Seiten die mit auf unserem Sharedhosting liegen zu schützen. Diese Maßnahme ist zwar hart, aber verständlich und auch fair. Insgesamt wurden wir von unserem Hoster HostEurope sehr gut unterstützt und als man sich dort der Angriffe gewahr wurde, waren auch keine Probleme mehr zu erkennen. Am gleichen Tag noch haben wir Anzeige erstattet und der Polizei alle erhaltenen Mails sowie die Logfiles übermittelt.

Nun hatten wir bereits einen dedizierten Server in der Hinterhand, da wir eigentlich in der Woche das Shopsystem wechseln wollten. Auf diesen sind wir dann mit dem alten System gewechselt. Allein der Wechsel von einem Web-paket auf einen eigenen Server brachte eine Besserung, da offensichtlich unsere Ressourcen die der Angreifer erst einmal überstiegen. Allerdings besserten die nach 2 Tagen (Mittwoch) nach. Zu diesem Zeitpunkt haben wir dann erstmals eine Firewall implementiert die 1. mehr als x Zugriffe von einer IP blockierte und 2. Zugriffe aus dem ausländischen IP Raum ganz blockierte.

Für unser Geschäft ergibt sich daraus kaum negatives, da wir vor allemTraffic aus Deutschland haben.

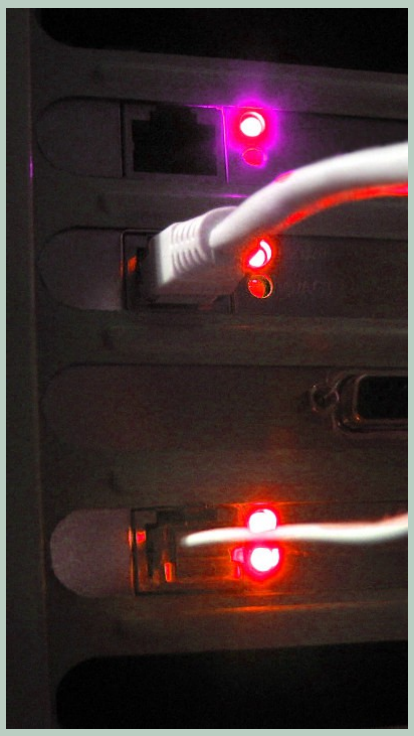
Rückblickend muss man sagen dass es gut war auf einem statischen Shop-system zu sein, da dieses weniger Angriffsfläche zu bieten scheint. Den angedachten Wechsel auf ein dynamisches System haben wir daher von Anfang November auf Januar verschoben.

Ausserdem ist natürlich die „Gegenwehr“ bei einem Sharedhosting nur schwer möglich, auch wenn HostEurope hier nach eigener Aussage in Zukunft vielleicht einen Zusatzservice anbieten will. Zudem ist natürlich ein kleines Webpack sehr viel schneller an den Grenzen seiner Ressourcen.

Die wenigen Gegenmaßnahmen die wir ergriffen haben sind erstaunlich einfach und vom Aufwand gering. Ein eigener Server mit Firewall hat vollkommen gereicht.

Fazit

Das „Geschäftsmodell“ der Schutzgelderpresssung via DDoS ist einfach, profitabel und (noch) relativ risikoarm. Shophändler dürften sich daher noch längere Zeit mit kriminellen Machenschaften dieser Art konfrontiert sehen.



Als langfristige Strategie kann daher nur versucht werden, für die Täter die Einträglichkeit herunter- und das Risiko heraufzufahren. Das bedeutet: Händler sollten im Erpressungsfall **NIEMALS Geld bezahlen**, selbst wenn die geforderten Summen im Vergleich zum durch einen Angriff entstehenden Aufwand gering erscheinen.

Gleichzeitig sollten **IMMER die Strafverfolgungsbehörden eingeschaltet** werden. Viele Täter rechnen nicht mit einer Strafverfolgung, außerdem ist die Polizei mittlerweile durchaus besser auf IT-Kriminalität vorbereitet – beide Faktoren zusammen sorgen dafür, dass der eine oder andere Erpresser ermittelt wird, mit hoffentlich abschreckender Wirkung auf Nachahmer.

Auf technischer Ebene gibt es **ein ganzes Arsenal von Strategien, Tools und Geräten**, die DDoS-Attacken ausbremsen können. Während sich spezialisierte Dienste für „normale“ Onlineshops (noch) kaum rechnen dürften, können sie für besonders exponierte E-Commerce-Unternehmen, beispielsweise aus dem Sportwetten-Bereich, durchaus eine gute Wahl sein.

ratgeber.

Hostingprovider beschäftigen sich schon aus Eigenschutz seit einiger Zeit verstärkt mit der Erkennung und Abwehr von DoS-/DDoS-Angriffen. Der technische Support sollte im Fall der Fälle daher schnell und kompetent helfen können, die nötigen Maßnahmen zu ergreifen, um das eigene System zu entlasten. Bei Shared Hosting Lösungen gebietet es schon die Fairness, beim Eingehen von Erpressungsschreiben nicht abzuwarten, sondern **sofort den Provider zu informieren**, damit im Angriffsfall nicht auch noch andere auf demselben Server liegende Webangebote getroffen werden.

Während professionelle Angreifer heute technisch deutlich ausgefeilter vorzugehen in der Lage sind, als es bei einfachen DoS-Attacken früher der Fall war, zeigt eine Anzahl aktueller DdoS-Erpressungen, dass das Gros der Angriffe noch immer relativ simpel gestrickt ist. Solche einfachen Attacken sind von technischer Seite aus relativ einfach beherrschbar, wenn Shophändler und Hostingprovider engagiert zusammenarbeiten.

ratgeber.

Über Shopanbieter.de

Shopanbieter.de ist ein Info-Portal, dass ganz auf den Bedarf von Betreibern kleinerer und mittlerer Online-Shops zugeschnitten ist. Sie finden hier alle relevanten Informationen an einer Stelle konzentriert vor:

- Ein umfassendes Linkverzeichnis,
- einen aktuellen Newsservice,
- Hintergrund- und Fachartikel,
- Whitepaper sowie
- dem Standardwerk "Leitfaden für Shop-Einsteiger" zum kostenlosen Download

Über Nicola Straub

Nicola Straub ist als Autorin für E-Commerce-Themen seit 2005 Redakteurin des Infoportales Shopanbieter.de. Daneben erstellt, realisiert und coacht sie Webprojekte und konzipiert Onlinemarketing-Kampagnen. Zu diesem Thema bietet sie zudem auch E-Learning-Workshops an.

Herausgeber, Bildnachweis und Nutzungsrechte

Herausgeber

Shopanbieter.de
Peter Höschl
Haydnstr. 21
85521 Ottobrunn bei München

Telefon Nr. ++49 89 470 77 941
Telefax Nr. ++49 89 665 93 747
E-Mail info@shopanbieter.de

USt.Id Nr. DE 187 688 555

Nutzungsbedingungen

Bildnachweis

Alle Bilder außer des Erpresserschreibens von stock.xchng.