

## Mailwechsel mit Hosteurope aufgrund einer Webpack-Sperre

An den weiter unten wiedergegebenen Mails wurden einige Veränderungen durchgeführt:

- a) Signaturen (Werbung) entfernt
- b) Hervorhebungen (fett) zur Verdeutlichung
- c) Hosteurope-Ticketnummer durch XYZ ersetzt
- d) Webpack-Hostname durch wpXYZ ersetzt
- e) Webpack-Nummer durch XXX ersetzt
- f) Vor- und Zunamen der Sachbearbeiter durch eine Sachbearbeiter-Nummer ersetzt

**From:** Host Europe ServiceCenter <support@hosteurope.de>  
**To:** ronald.woelfel@rhoen.de  
**Reply-To:** support@hosteurope.de  
**Subject:** WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#  
**Date:** Thu, 16 Nov 2006 15:23:18 +0100

```
*****  
**   Achtung! Bei Antwort/Reply auf diese E-Mail bitte   **  
** NICHT das Subject/Betreff verändern, da eine weitere **  
** Bearbeitung sonst nicht möglich ist. Vielen Dank! **  
*****
```

Sehr geehrter Herr Wölfel,

leider mussten wir feststellen, daß der Server durch Ihre Domain übermaeßig stark ausgelastet wird. Dies koennen wir in einer Shared Hosting Umgebung - auch im Interesse der anderen Kunden, die auf diesem Webserver liegen - nicht akzeptieren.

Wir haben daher Ihr Webpack gesperrt.  
Setzen Sie sich mit uns in Verbindung, wenn Sie die Scripte ueberarbeitet und externe Links entfernt haben.  
Vielleicht wechseln Sie auch auf einen VPS.

Mit freundlichen Grüßen

Sachbearbeiter Nr. 1

Kundenservice Webhosting  
- Privat- und Geschäftskunden -

=====  
**Date:** Thu, 16 Nov 2006 15:53:49 +0100 (CET)  
**From:** Ronald Woelfel <ronald.woelfel@rhoen.de>  
**To:** Host Europe ServiceCenter <support@hosteurope.de>  
**Subject:** Re: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#

Sehr geehrter Herr Sachbearbeiter 1,

vielen Dank für ihren Hinweis. Leider kann ich nicht verstehen, dass das Sperren der Webseite nicht angekündigt wurde. Seit Wochen, eher aber schon seit einigen Monaten habe ich keine neuen Anwendung auf dem Webpack installiert.

Warum musste das Sperren ohne Vorankündigung erfolgen?

Was mir aber weitaus wichtiger ist: Zum Webpack gehören 7 (in Worten sieben) Domains mit hunderten von PHP-Skripten. Wie soll ich denn "problematische" Skripte finden, wenn Sie noch nicht einmal eine Domain angeben, geschweige denn das Problem näher benennen?

Mit freundlichen Grüßen  
Ronald Wölfel

=====  
**From:** Host Europe ServiceCenter <support@hosteurope.de>  
**To:** ronald.woelfel@rhoen.de  
**Reply-To:** support@hosteurope.de  
**Subject:** WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#  
**Date:** Thu, 16 Nov 2006 17:06:53 +0100

\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*  
\*\*\*\*\*

Sehr geehrter Herr Woelfel,

> vielen Dank für ihren Hinweis. Leider kann ich nicht  
> verstehen, dass das Sperren der Webseite nicht angekündigt  
> wurde. Seit Wochen, eher aber schon seit einigen Monaten  
> habe ich keine neuen Anwendung auf dem Webpack installiert.  
>  
> Warum musste das Sperren ohne Vorankündigung erfolgen?  
>  
> Was mir aber weitaus wichtiger ist: Zum Webpack gehören  
> 7 (in Worten sieben) Domains mit hunderten von PHP-Skripten.  
> Wie soll ich denn "problematische" Skripte finden, wenn  
> Sie noch nicht einmal eine Domain angeben, geschweige denn  
> das Problem näher benennen?

Wir berufen uns bei der Sperrung Ihres Webpack auf den §5 Abs. 5 unserer AGB.

§5 Pflichten des Kunden

5) Der Kunde verpflichtet sich, bei Gestaltung seiner Internet-Präsenz auf Techniken zu verzichten, die eine übermäßige Inanspruchnahme der Einrichtungen des Providers verursachen, insbesondere CGI- und PHP-Skripte. Der Provider kann Internet-Präsenzen mit diesen Techniken vom Zugriff durch Dritte ausschließen, bis der Kunde die Techniken beseitigt/deaktiviert hat. Dies gilt nicht für Server, die dem Kunden zur alleinigen Nutzung zur Verfügung stehen (dedicated bzw. co-located Server).

Folgende Einträge in unseren Logs haben zur Sperrung Ihres Webpack geführt:

```
12-27 22837 0/28/14932 W 0.69 13 0 0.0 0.07 176.82 69.16.207.46 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
13-27 22635 0/32/14512 W 1.63 10 0 0.0 0.09 181.74 85.214.27.68 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
14-27 22843 0/21/15119 W 0.78 15 0 0.0 0.09 171.32 195.128.127.67 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
15-27 22854 0/24/15217 W 0.36 0 0 0.0 0.22 199.82 208.101.51.106 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
16-27 22636 0/14/14854 W 0.52 14 0 0.0 0.01 170.09 69.16.207.46 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f

18-27 22883 0/20/15009 W 1.04 4 0 0.0 0.25 175.56 82.98.225.171 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
19-27 22638 0/39/14892 W 1.06 12 0 0.0 0.09 165.49 210.193.49.174 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/includes/
20-27 22884 0/19/14528 W 0.95 5 0 0.0 0.07 214.78 200.137.197.6 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
21-27 22646 0/16/14848 W 0.19 14 0 0.0 0.01 171.25 65.18.185.89 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/includes/
22-27 23452 0/3/14849 W 0.01 2 0 0.0 0.00 146.51 70.85.88.196 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/includes/
23-27 22891 0/17/14489 W 0.09 14 0 0.0 0.01 147.49 69.16.207.46 www.beautifulda.de GET
```

```
+/bf/component/option,com_zoom/components/com_zoom/classes/f
24-27 22659 0/18/13723 W 0.48 14 0 0.0 0.05 175.06 69.16.207.46 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
25-27 23454 0/1/14405 W 0.22 3 0 0.0 0.00 159.75 82.98.225.171 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
26-27 22892 0/10/14818 W 0.02 23 0 0.0 0.07 166.64 200.137.197.6 www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
```

Mit freundlichen Grüßen

Sachbearbeiter Nr. 2  
Kundenservice Webhosting  
- Privat- und Geschäftskunden -

---

**Date:** Thu, 16 Nov 2006 18:16:34 +0100 (CET)  
**From:** Ronald Woelfel <ronald.woelfel@rhoen.de>  
**To:** Host Europe ServiceCenter <support@hosteurope.de>  
**Subject:** Re: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#

Hallo,

> Folgende Einträge in unseren Logs haben zur Sperrung Ihres Webpack geführt:

Ok, dann ist es tatsächlich meine Schuld. Anhand der access-Logs konnte ich die Schwachstelle in der Zoom-Komponente von Joomla leicht finden. Ich bedanke mich für die schnelle Sperrung und würde mich darüber freuen, wenn Sie mich beim nächsten Mal (das es hoffentlich nicht geben wird), schneller informieren.

Die zwei betroffenen Joomla-Domains habe ich deaktiviert. Theoretisch könnte der Angreifer natürlich in jedem einzelnen PHP-Skript eine Backdoor hinterlassen haben. Deshalb habe ich im KIS ein Restore beantragt. Ich würde mich freuen, wenn Sie das Paket baldmöglichst wieder freischalten könnten.

Mfg  
Ronald Wölfel

**From:** Host Europe ServiceCenter <support@hosteurope.de>  
**To:** ronald.woelfel@rhoen.de  
**Reply-To:** support@hosteurope.de  
**Subject:** WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#  
**Date:** Sat, 18 Nov 2006 05:04:05 +0100

\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*  
\*\*\*\*\*

Ihr Paket wurde inzwischen wieder freigeschaltet.

In Ihrem Rootverzeichnis hat unsere Technik folgende Datei gefunden

nobody-dateien.17.11.06.txt

Anhand dieser Logfiles können sie evtl. potenzielle unsichere Dateien auffinden.

Mit freundlichen Grüßen

Sachbearbeiter Nr. 3  
Kundenservice Webhosting  
- Privat- und Geschäftskunden -

**Date:** Sat, 18 Nov 2006 09:12:13 +0100 (CET)  
**From:** Ronald Woelfel <ronald.woelfel@rhoen.de>  
**To:** Host Europe ServiceCenter <support@hosteurope.de>  
**Subject:** Re: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#

>  
> In Ihrem Rootverzeichnis hat unsere Technik folgende Datei gefunden  
>  
> nobody-dateien.17.11.06.txt  
>  
> Anhand dieser Logfiles können sie evtl. potenzielle unsichere Dateien auffinden.

Danke für das Bereitstellen der Datei. Damit ich auf die Datei Zugriff habe, müsste der Administrator noch das Leserecht für "others" setzen. Die Datei hat nämlich als Eigentümer/Gruppe "root".

Danke  
Ronald Wölfel

---

**Date:** Mon, 20 Nov 2006 20:03:38 +0100 (CET)  
**From:** Ronald Woelfel <ronald.woelfel@rhoen.de>  
**To:** Host Europe ServiceCenter <support@hosteurope.de>  
**Subject:** Re: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#

Hallo,

ich möchte nochmal drauf hinweisen, dass ich auf die von Ihnen zur Verfügung gestellte Datei (s.u.) nicht zugreifen kann, da die Zugriffsrechte von Ihnen falsch gesetzt (bzw. nicht korrigiert) wurden.

Ihren Hinweis bezüglich der Überlastung nahm ich sehr ernst, schließlich erfolgte von den im Logfile angegebenen IP-Adressen aus ein automatisierter Angriff.

Zum Zwecke der Klärung, habe ich mich mit den Autoren der Joomla\_zoom-Komponente ausgetauscht. Der versuchte Angriff beanspruchte den Server nicht im Mindesten. 50% der Zugriffe waren 404-Fehler, der Rest gewöhnliche Seitenabrufe.

Die von Ihnen übermittelten Logfiles erlaubten keine zeitliche Zuordnung und waren daher für mich nur durch sehr großen Aufwand zuzuordnen. Eine Spaltenbeschreibung der Logfiles lag und liegt mir ebenfalls nicht vor.

Daher würde ich Sie bitten, mir noch einmal mitzuteilen, warum mein Webpack gesperrt wurde.

Welche Art von Überlastung lag wann vor. Denkbar sind hierbei z.B. Hauptspeicher und/oder CPU-Verbrauch.

Mfg  
Ronald Wölfel

---

**From:** Host Europe ServiceCenter <support@hosteurope.de>  
**To:** ronald.woelfel@rhoen.de  
**Reply-To:** support@hosteurope.de  
**Subject:** WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#  
**Date:** Wed, 22 Nov 2006 02:18:34 +0100

\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*

\*\*\*\*\*

Sehr geehrter Herr Wölfel,

> ich möchte nochmal drauf hinweisen, dass ich auf die  
> von Ihnen zur Verfügung gestellte Datei (s.u.) nicht  
> zugreifen kann, da die Zugriffsrechte von Ihnen  
> falsch gesetzt (bzw. nicht korrigiert) wurden.

die Rechte wurden nun angepaßt.

> Daher würde ich Sie bitten, mir noch einmal mitzuteilen,  
> warum mein Webpack gesperrt wurde.  
> Welche Art von Überlastung lag wann vor. Denkbar sind  
> hierbei z.B. Hauptspeicher und/oder CPU-Verbrauch.

Zum Zeitpunkt der Überlastung war Speicher und CPU überlastet  
genauer lässt sich aber nicht sagen denn dies wird nicht geloggt.

Mit freundlichen Grüßen

Sachbearbeiter Nr. 4  
Kundenservice Webhosting  
- Privat- und Geschäftskunden -

=====  
**Date:** Wed, 22 Nov 2006 13:31:51 +0100 (CET)  
**From:** Ronald Woelfel <ronald.woelfel@rhoen.de>  
**To:** Host Europe ServiceCenter <support@hosteurope.de>  
**Subject:** Re: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#

> > Daher würde ich Sie bitten, mir noch einmal mitzuteilen,  
> > warum mein Webpack gesperrt wurde.  
> > Welche Art von Überlastung lag wann vor. Denkbar sind  
> > hierbei z.B. Hauptspeicher und/oder CPU-Verbrauch.  
>  
> Zum Zeitpunkt der Überlastung war Speicher und CPU überlastet  
> genaueres lässt sich aber nicht sagen denn dies wird nicht geloggt.

Sie sprechen von einem "Zeitpunkt". Dieser Zeitpunkt würde mich  
interessieren, denn in den von Ihnen zur Verfügung gestellten  
Logdateien (s.u.) ist kein Zeitstempel vorhanden.  
Würden Sie mir bitte auch noch kurz über die Spalten der  
mitgeschickten Logdatei Auskunft geben?  
Welche Spalte gibt den Hauptspeicherbedarf meines Webpacks an?  
Welche Spalte steht für die CPU-Last, die durch mein Webpack  
verursacht wird?

```
12-27 22837 0/28/14932 W 0.69 13 0 0.0 0.07 176.82 69.16.207.46
www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
13-27 22635 0/32/14512 W 1.63 10 0 0.0 0.09 181.74 85.214.27.68
www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
14-27 22843 0/21/15119 W 0.78 15 0 0.0 0.09 171.32 195.128.127.67
www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
15-27 22854 0/24/15217 W 0.36 0 0 0.0 0.22 199.82 208.101.51.106
www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
16-27 22636 0/14/14854 W 0.52 14 0 0.0 0.01 170.09 69.16.207.46
www.beautifulda.de GET
+/bf/component/option,com_zoom/components/com_zoom/classes/f
```

Vielen Dank im voraus.  
Mfg  
Ronald Wölfel

=====  
**From: Host Europe ServiceCenter <support@hosteurope.de>**  
**To: ronald.woelfel@rhoen.de**  
Reply-To: support@hosteurope.de  
Subject: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#  
**Date: Wed, 22 Nov 2006 20:37:03 +0100**

\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*  
\*\*\*\*\*

Sehr geehrter Herr Woelfel,

die Angabe der CPU-Auslastung ist für Sie wahrscheinlich wenig hilfreich, da Ihnen die Gesamtauslastung der Server-CPU nicht bekannt ist.

Zum Zeitpunkt der Überlastung haben unsere Techniker die Logs erstellt, welche wir Ihnen zur Verfügung gestellt haben.

Eine exakte Zeitangabe ist demnach nicht mehr notwendig, da die betreffenden Aufrufe Ihres Webpack Ihnen bereits mitgeteilt wurden.

Mit freundlichen Grüßen

Sachbearbeiter Nr. 5

=====  
**From: Host Europe ServiceCenter <support@hosteurope.de>**  
**To: ronald.woelfel@rhoen.de**  
Reply-To: support@hosteurope.de  
Subject: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#  
**Date: Fri, 24 Nov 2006 21:57:58 +0100**

\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*  
\*\*\*\*\*

Sehr geehrte Kundin,  
sehr geehrter Kunde,

leider haben wir bisher keine Antwort von Ihnen auf unsere letzte E-Mail erhalten.

Zur Sicherheit senden wir Ihnen deshalb diese Nachricht erneut per E-Mail zu. Bitte teilen Sie uns Ihre Antwort so bald wie möglich mit, damit der Fall schnell gelöst werden kann.

Hier noch einmal die betreffende Nachricht:

Subject: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ)

\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*  
\*\*\*\*\*

Sehr geehrter Herr Woelfel,

die Angabe der CPU-Auslastung ist für Sie wahrscheinlich wenig hilfreich, da Ihnen die Gesamtauslastung der Server-CPU nicht bekannt ist.

Zum Zeitpunkt der Überlastung haben unsere Techniker die Logs erstellt, welche wir Ihnen zur Verfügung gestellt haben.

Eine exakte Zeitangabe ist demnach nicht mehr notwendig, da die betreffenden Aufrufe

Ihres Webpack Ihnen bereits mitgeteilt wurden.

Mit freundlichen Grüßen

Sachbearbeiter Nr. 5  
Kundenservice Webhosting  
- Privat- und Geschäftskunden -

=====  
**From: Host Europe ServiceCenter <support@hosteurope.de>**  
**To: ronald.woelfel@rhoen.de**  
Reply-To: support@hosteurope.de  
Subject: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#  
**Date: Mon, 27 Nov 2006 10:26:44 +0100**

\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*  
\*\*\*\*\*

Sehr geehrte Kundin,  
sehr geehrter Kunde,

leider haben wir bisher keine Antwort von Ihnen auf unsere letzte E-Mail erhalten. Daher leiten wir Ihnen diese nun noch ein letztes Mal weiter.

**Sollten wir auch auf dieses Schreiben bis zum 04.12.06 um 12 Uhr keine Reaktion von Ihnen erhalten, wird Ihr Paket gesperrt werden - es erfolgt keine weitere Erinnerung unsererseits.**

Vielen Dank.

-----

Subject: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ)  
\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*  
\*\*\*\*\*

Sehr geehrter Herr Woelfel,

die Angabe der CPU-Auslastung ist für Sie wahrscheinlich wenig hilfreich, da Ihnen die Gesamtauslastung der Server-CPU nicht bekannt ist.

Zum Zeitpunkt der Überlastung haben unsere Techniker die Logs erstellt, welche wir Ihnen zur Verfügung gestellt haben.

Eine exakte Zeitangabe ist demnach nicht mehr notwendig, da die betreffenden Aufrufe Ihres Webpack Ihnen bereits mitgeteilt wurden.

Mit freundlichen Grüßen

Sachbearbeiter Nr. 5  
Kundenservice Webhosting  
- Privat- und Geschäftskunden -

=====  
**Date: Mon, 27 Nov 2006 15:11:51 +0100 (CET)**  
**From: Ronald Woelfel <ronald.woelfel@rhoen.de>**  
**To: Host Europe ServiceCenter <support@hosteurope.de>**  
Subject: Re: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#

> leider haben wir bisher keine Antwort von Ihnen auf  
> unsere letzte E-Mail erhalten. Daher leiten wir  
> Ihnen diese nun noch ein letztes Mal weiter.

>  
> Sollten wir auch auf dieses Schreiben bis zum 04.12.06  
> um 12 Uhr keine Reaktion von Ihnen erhalten, wird Ihr  
> Paket gesperrt werden - es erfolgt keine weitere  
> Erinnerung unsererseits.

Für mich stellt sich die Sachlage folgt dar.

###

1. Tag: Donnerstag, 16. November

Am Donnerstag, 16. November ca. gegen 13.00 Uhr bemerke ich, dass keine meiner Domains in meinem Webpack bei Hosteurope funktionieren. Auf telefonisches Nachfragen, ca. gegen 14.00 Uhr erhalte ich die Auskunft, dass auf dem Server wohl "nur der Apache einmal neu gestartet werden müsse"

Um 15.23 Uhr erhalte ich eine Mail, die mich darauf hinweist, dass eine "Überlastung" vorliegt und das Webpack deshalb gesperrt wurde. Der enthaltene Hinweis "vielleicht wechseln Sie auch auf einen VPS" klingt wie Erpressung, wenn gerade alle sieben Domains, die ich in diesem Paket habe, ohne Vorwarnung abgeschaltet wurden.

In meiner sehr freundlichen Antwort (kurz vor 16.00 Uhr) zeige ich mich verwundert, dass keine Ankündigung erfolgte. Ich verweise auch auf das Problem, dass ich keinerlei Ansatzpunkt besitze, wie ich die Last reduzieren könnte.

Das freundliche Nachfragen meinerseits wird gegen 17.00 Uhr mit einem harschen Hinweis auf §5 der von mir akzeptierten AGBs beantwortet. Der Sachbearbeiter zitiert sogar den passenden Gummiparagraphen, nachdem der Webhoster eine Sperrung immer vornehmen darf, sofern "eine übermäßige Inanspruchnahme der Einrichtungen des Providers" vorliegt. Mit dem Hinweis "folgende Einträge in unseren Logs haben zur Sperrung Ihres Webpack geführt" erhalte ich einen unkommentierten Logfile-Auszug, ohne jeden zeitlichen Bezug und ohne irgendeinen Hinweis auf die Bedeutung der Spalten.

Immerhin sind IP-Adressen in der Logdatei enthalten. Das Webfrontend zum Abrufen der Logfiles funktioniert trotz der Sperrung. So kann ich sehen, dass am gleichen Tag tatsächlich ein Angriff auf eine Komponente des CMS Joomla erfolgte.

Ich ging daher davon aus, dass der Hosteurope-Support recht hätte, schrieb in meiner Antwort um 18.00 Uhr sogar, dass es in diesem Fall meine Schuld sei und bedankte mich. Ich bat um eine schnelle Freischaltung und gab an, dass ich die betreffenden Domains deaktivieren würde.

Was ich zu diesem Zeitpunkt noch nicht wusste: Es hatte zwar einige hundert Zugriffe auf das Verzeichnis der Joomla-Komponente gegeben, doch liefen fast alle Zugriffe ins Leere (404-Fehler). Die restlichen Zugriffe waren überschaubar. Zusammen mit dem Autor der Komponente überprüfte ich die vermutete Sicherheitslücke. Ergebnis nach 4-5 Stunden intensiven Suchens: es gab keine Sicherheitslücke!

Immerhin wurde das Paket gegen 18.30 Uhr freigeschaltet.

3. Tag: Samstag, 18. November

Frühmorgens wurde mir per Mail mitgeteilt, dass das Paket nun wieder freigeschaltet wäre. Außerdem wurde mir mitgeteilt, dass mir eine Textdatei bereitgestellt wurde, die potenziell "unsichere Dateien" enthielte. Leider konnte ich die Datei aufgrund falsch gesetzter Zugriffsrechte (Eigentümer "root") nicht lesen.

Um 9.00 Uhr teilte ich dies dem Support mit.

5. Tag: Montag, 20. November

Nun war ich mir sicher, dass keine Joomla-Sicherheitslücke bestand. Dies teilte ich dem Support gegen 20.00 Uhr per Mail mit und fragte nach dem Grund des gesperrten Webpacks (z.B. zuviel Hauptspeicher und/oder CPU-Verbrauch).

7. Tag: Mittwoch, 22. November

Der Support teilte mir nun mit, dass die Zugriffsrechte der Datei angepasst wurden, so dass ich nun endlich einen Blick darauf werfen konnte. Der Inhalt war eine Liste der Dateien, die nicht per FTP hochgeladen wurden, sondern direkt auf der Webpräsenz, z.B. via PHP oder CGI Skripte erzeugt wurden. Da ich via PHP-Shell auf dem Webpräsenz arbeite, besitzen fast alle Dateien (22000 an der Zahl) den Eigentümer nobody.

Wie Hohn klang der folgende Satz in der gleichen Mail in meinen Ohren: "Zum Zeitpunkt der Überlastung war Speicher und CPU überlastet genaueres lässt sich aber nicht sagen denn dies wird nicht geloggt". Mehr als eine pauschale Aussage war also nicht drin. Vor allem der Zeitpunkt wurde immer noch nicht genannt. Dies monierte ich in meiner Mail um 13.30 Uhr am gleichen Tag: Der Support antwortete:

"die Angabe der CPU-Auslastung ist für Sie wahrscheinlich wenig hilfreich, da Ihnen die Gesamtauslastung der Server-CPU nicht bekannt ist. Zum Zeitpunkt der Überlastung haben unsere Techniker die Logs erstellt, welche wir Ihnen zur Verfügung gestellt haben. Eine exakte Zeitangabe ist demnach nicht mehr notwendig, da die betreffenden Aufrufe Ihres Webpack Ihnen bereits mitgeteilt wurden."

Die genaue zeitliche Zuordnung, nämlich in Form einer Uhrzeit, wird mir erneut verweigert. Eine Handlungsaufforderung oder ein Hinweis auf eine neuerliche starke Beanspruchung des Webpacks gab es nicht.

9. Tag: Freitag, 24. November  
Ich erhalte eine Erinnerung der Mail vom Mittwoch.

12. Tag: Montag, 27. November  
Ich werde erneut auf die nichtssagende Mail vom Mittwoch hingewiesen. Gleichzeitig werde ich darauf aufmerksam gemacht, dass mein Paket erneut gesperrt werden würde, wenn ich bis zum 04.12.2006 nicht auf diese Mail reagieren würde.  
###

Worauf erwarten Sie eine Antwort von mir?  
Mfg  
Ronald Wölfel

=====  
Date: Mon, 27 Nov 2006 16:35:10 +0100  
From: Host Europe ServiceCenter <support@hosteurope.de>  
To: ronald.woelfel@rhoen.de  
Subject: WebPack XXX wegen Überlastung des Server gesperrt (wpXYZ) #Ticket:XYZ#

\*\*\*\*\*  
\*\* Achtung! Bei Antwort/Reply auf diese E-Mail bitte \*\*  
\*\* NICHT das Subject/Betreff verändern, da eine weitere \*\*  
\*\* Bearbeitung sonst nicht möglich ist. Vielen Dank! \*\*  
\*\*\*\*\*

Sehr geehrter Herr Wölfel,

> Worauf erwarten Sie eine Antwort von mir?

**Teilen Sie uns bitte mit, wie Sie solche Überlastungen in Zukunft verhindern werden.**

**Unsere Empfehlung wäre ein regelmäßiges Update Ihres CMS.**

Mit freundlichen Grüßen

Sachbearbeiter Nr. 5  
Kundenservice Webhosting  
- Privat- und Geschäftskunden -  
=====