

Suche

[Aktuell](#) | [Lokale Wirtschaft](#) | [Bizz Tipps](#) | [Lifestyle](#) | [Marketing](#) | [Finanzen](#) | [Fachwissen](#) | [Golf-on](#)
[Termine](#) | [News](#) | [IT & Telekommunikation](#) | [Recht & Steuern](#) | [Jobbörse](#) | [Messen](#) | ["München meint..."](#)

29.08.2011 13:04 Uhr

[Drucken](#) | [Versenden](#) | [Kommentare](#)

## IT-TIPP

## Hilfe – meine Website wurde gehackt !

**München.** Sollten Sie eines Morgens einen Anruf Ihres Kunden erreichen, dass Ihre Website nicht mehr erreichbar ist, auf dubiose Webseiten verweist oder nicht mehr einwandfrei funktioniert, so muss es nicht daran liegen, dass Ihr Hosting-Unternehmen einen Fehler gemacht hat oder dass der Server in Ihrem Hause einfach nur neu gestartet werden muss. Vielleicht hat Sie ein Hacker erwischt!








Anonyme Gäste auf ihrem Computer? Wenn Sie den Verdacht haben, Sie wurden gehackt, gilt es schnell zu handeln. Ein Erfahrungsbericht. © [pixelio.de](http://pixelio.de) /Klicker

In letzter Zeit nehmen die Vorwürfe – insbesondere gegen Hacker aus der Volksrepublik China zu. Den Chinesen wird häufig vorgeworfen – ob berechtigt oder nicht – dass Sie von der Regierung organisierte Wirtschaftsspionage betreiben – der Online-Krieg hätte demgemäß bereits längst begonnen. Lesen Sie den Erfahrungsbericht eines Bonner Unternehmens, dessen Website angegriffen wurde.

### Kürzlich in Bonn...

Als ich morgens kurz nach 8 Uhr auf unsere Website ging, war diese nicht erreichbar. „Ups“ dachte ich, da hat unsere Hostingfirma wohl ein Problem mit dem Server. Als nach dem Anruf beim Support aber klar war, daß das

## ARTIKEL ZUM THEMA

- » **Hacker-Angriff:**  
Erpresser-Trojaner fordert „Lösegeld“ oder sperrt den Computer 
- » **Atomkraftwerk Fukushima:**  
Aktuelle Lage in Japan - Jetzt sollen Planenabdeckungen helfen 
- » **iPad 2 und iPhone 4:**  
Zwei Geräte, ein Hotspot - aber zu welchen Kosten? 
- » **Darmerreger:**  
Zahl der EHEC-Infektionen in Bayern auf 26 gestiegen 
- » **Google-Indoor:**  
Google View bald auch in deutschen Wohnungen 

ANZEIGE

## BUSINESS-ON.DE IPHONE APP

Problem nicht technischer Herkunft war ging die große Fehlersuche los – aber der Reihe nach.

## Den Hack bemerken/ Präventionsmaßnahmen

Wenn ein Problem mit der Website auffällt, sollte man zunächst einmal klären, ob der Fehler selbst oder – im Falle dessen, dass das Hosting outgesourced wurde – vom Hoster kommt. Falls dies nicht der Fall ist, sollte man sich eine Checkliste erstellen, die man im Fall der Fälle schnell durchgehen und abhaken kann. Wenn mit der eigenen Website nämlich Umsätze durch Online-Verkäufe erzeugt werden oder sensible Daten online Partnern und Kunden bereitgestellt werden, dann kann ein Hack „business critical“ sein.

Zum Glück war das bei uns nicht der Fall – unsere Website enthielt ausschliesslich öffentliche und unkritische Daten und über unsere Website machen wir auch keinerlei Umsätze. Präventivmaßnahmen wie das regelmäßige Überwachen von Seitenzugriffen und Traffic sind in solchen Fällen absolute Pflicht. Auch ein sensibler Umgang mit sicheren Passwörtern sollte Teil des IT-Sicherheitskonzepts für Ihre Website sein – denn wer will schon dass beispielsweise ein ehemaliger Mitarbeiter auf diesem Wege Rache nimmt...

**Lassen sich alle internen Fehlerquellen ausschließen und wenn vieles auf einen Hack von außen hindeutet, sollten Sie die Website unverzüglich vom Netz nehmen, um Schaden insbesondere für Dritte zu vermeiden.**

## Der Notfallplan

Als uns gegen 8:30 Uhr klar war, dass es sich um ein Hack handelte, bedienten wir uns der Checkliste, die wir für solche Fälle erstellt hatten:

### ZUGEHÖRIGE ARTIKEL:

- ▶ Erpresser-Trojaner fordert „Lösegeld“ oder sperrt den Computer

- » Test, ob die Seite nur aus dem eigenen Netzwerk oder auch von außen nicht zu erreichen ist beziehungsweise fehlerhaft ist.
- » Ausschluss von Hostingproblemen beziehungsweise Problemen der Serververfügbarkeit durch eine (telefonische) Abstimmung mit dem Hosting-Verantwortlichen.
- » Prüfung des SSH/FTP-Servers um den Zeitpunkt der letzten Änderungen zu bestimmen.
- » Prüfung welche Dateien verändert wurden beziehungsweise ob neue Dateien hinzugefügt wurden.
- » Prüfung der Seitenzugriffe und Trafficzahlen sowie Analyse der Zugriffslogfiles.
- » Prüfung, ob redaktionelle Änderungen durch einen Mitarbeiter, beispielsweise die Änderung von Textbausteinen oder sonstigen Websiteelementen in einem Content Management System (CMS) die Fehlerursache war.

Wenn tatsächlich ein Hack vorliegt, sollten Sie eine temporäre Fehlermeldung auf der Website einspielen, in der Sie beispielsweise angeben, dass Ihre Website leider temporär aufgrund von Wartungsarbeiten nicht verfügbar ist. Hier reicht eine einfach Deaktivierung des CMS oft nicht – und auch das Austauschen der index-Datei wie zum Beispiel index.php bei einer mit PHP



## EMPFEHLUNG

[Handytarife Business](#)

Anmelden zum NEWSLETTER	Abonnieren Sie das RSS-FEED
Alle Top-News mit TWITTER	CONTENT für Ihre Webseite

## NEUESTE ARTIKEL

16.09.09:42	<b>Oktoberfest:</b> Letzte Aufbauarbeiten im Gange	
16.09.09:29	<b>Oktoberfest:</b> Hochkonjunktur zur Wiesn-Zeit	
16.09.09:03	<b>Surfen:</b> Die perfekte Welle	
16.09.08:26	<b>„O`zapft werd`“ bei Ammer:</b> Schauspieler Peter Landstorfer sorgt für die erste Maß in der Hühner- und Entenbraterei	
15.09.16:03	<b>Bauzeit beendet:</b> Neubau der Hochschule für Film und Fernsehen in München eröffnet	
15.09.15:46	<b>Oktoberfest:</b> Hotelpreis zur Wiesn verdreifacht	
15.09.14:24	<b>Mit Genuss zum Weltrekord!:</b> Münchens erster Fair Trade Shop lädt zur „fairen“ Kaffeepause	

## MEISTGELESENE ARTIKEL

- Von Apple offiziell bestätigt**  
iPhone 5: Großer Auftritt im September
- Apple**

programmierten Website ist nicht hinreichend. Das hat sich auch in unserem Fall bestätigt, da sich die Ursache auf die .htaccess Datei im Root-Verzeichnis zurückführen ließ, welche bei jedem Seitenaufruf eine weitere Datei geladen hat. Möglich ist dies, da mit der .htaccess Datei der Apache-Server gesteuert werden kann.

## Schadensbegrenzung und Fehlerbehebung

Nachdem Sie den Hack bemerkt haben, gilt es zunächst herauszufinden, welche Sicherheitslücke der Angreifer ausgenutzt hat. Dabei hilft eine Analyse des Logfiles, welche jeden Seitenaufruf gespeichert hat. Unabhängig davon, dass die Lücke gepatched werden sollte, muss vor dem Patchen der Lücke unbedingt das (regelmäßig erstellte) Backup einspielt werden. Falls das letzte Backup zu lange zurückliegt, müssen hier in den sauren Apfel beißen und Änderungen, die Sie seither erstellt haben nochmals durchführen – denn man kann nicht ausschließen, dass eventuell weitere Dateien oder Datenbankeinträge manipuliert wurden. Sie sollten dabei darauf achten, bereits vor dem Einspielen des Backups die Hauptzugangspasswörter geändert zu haben, damit ein möglicher Angreifer Ihnen nicht „dazwischenfunken“ kann. Zur Schließung der Sicherheitslücke empfiehlt sich einen Upgrade auf die aktuellste Version Ihres CMS – egal ob Adobe CQ5 (ehemals Day CQ5), Core Media, Tibco, Typo3 – durchzuführen. Gegebenenfalls funktionieren dadurch einige Inhalte nicht mehr, dies sollten Sie im Anschluss überprüfen. Um den Schaden schnell begrenzen zu können, ist ein Stand-By Support natürlich essenziell wichtig.

## Bei aller Technik nicht die Kommunikation mit Mitarbeitern und Kunden vergessen!

Außerdem vergessen Sie in einem solchen Fall bitte nicht die Kommunikation zu Kunden und Mitarbeitern. Es ist nichts schlimmer, als wenn diese von dem Vorfall aus der Presse beziehungsweise aus Internetportalen erfahren.

**Haben Sie keine Angst vor einem Imageschaden für Ihr Unternehmen, sondern gehen Sie den Vorfall proaktiv und offensiv mit Ihrer Kommunikation an. Außerdem helfen Sie anderen Unternehmen dabei, nicht auch noch demselben Hack zum Opfer zu fallen.**

In unserem Fall konnten wir uns glücklich schätzen einen IT-Administrator als Stand-By Support zu haben, der durch seine fundierte Ausbildung in Sachen IT-Sicherheit an der Ruhr-Universität Bochum das Problem äußerst schnell und effizient eingrenzen und beheben konnte. Die Sicherheitslücke in unseren Systemen war allerdings an ganz anderer Stelle zu finden. Eine Setup-Datei ist nach der Installation vor Jahren in Vergessenheit geraten und nie gelöscht worden. Diese enthielt eine Cross-Site Scripting-Lücke (XSS), über die der Angreifer weitere Dateien nachladen und schreiben konnte. Eine Analyse des Hacks hat ergeben, dass es sich um einen weniger schwerwiegenden automatisierten Angriff handelte, der unseren Webserver so manipuliert hat, dass wer immer uns gegoogelt hat auf eine pseudo-Suchmaschine weitergeleitet wurde.

**Simon Schoop** ist Geschäftsführer der [4-advice GmbH](#) | Change & Innovation Consulting und berät Kunden u.a. bei der Strategieerarbeitung und Umsetzung von technologischen Innovationen, wobei er auf weitreichende Erfahrungen aus Beratungsprojekten in der IT-Branche verweisen kann.

iPad 3 mit Retina-Display ausgestattet? Und wann kommt es?

### 3 Apple

Kommen iPhone 5 und iPhone 4S im September auf den Markt?

### 4 Samsung Galaxy S2 Testbericht

Der iPhone-Killer im Praxistest



### 5 Twitter-Test

Testen Sie Ihr Twitter-Wissen auf business-on.de



### 6 Entwicklerkonferenz

Steve Jobs präsentiert Updates für iOS und Mac OS und stellt die iCloud vor



### 7 Social Media Smartphones

HTC ChaCha und HTC Salsa ab sofort erhältlich



## AUSGEWÄHLTE THEMEN

- » Fussball WM 2010
- » Wege in die Selbständigkeit
- » Der Übergang vom Selbständigen zum Unternehmer
- » Was SEO ist und wie es Unternehmen hilft
- » Wie man SEO am besten angeht
- » Was ist eigentlich ein Bartergeschäft?
- » Klassisches Marketing vs. Online-Marketing
- » Mit Online-Singlebörsen den Partner fürs Leben finden
- » FriendScout24 nach Dating Cafe beste Singlebörse 2011

## BUSINESS-ON.DE REGIONAL

20 Portale, 400.000 Leser pro Monat.  
Klicken Sie auf Ihre Region:



Ingo Düllmann ist IT Systemadministrator der 4-advice GmbH und studiert an der Universität Bochum den Masterstudiengang IT-Sicherheit/Informationstechnik.

(Simon Schoop/Ingo Düllmann)








Fotokennzeichnung:  
Bild Nr. 1 © Klicker / pixello.de

Tags: Website Hack Datei Problem [Mitarbeiter](#)  
[Kunden](#) Angreifer [Fehler](#) Analyse  
Sicherheitslücke [Kommunikation](#)

Gefällt mir 6 Ihren XING Kontakten zeigen 5

LIKE 0 Mehr Teilen-Services 0

### Mehr zum Thema IT & Telekommunikation:

-  **Erstes Smartphone mit integriertem Beats Audio**  
HTC Sensation XE™
-  **Ein falscher Klick und es kommt ein Abo zustande**  
Neuer iPhone5-Spam
-  **Wie können Unternehmen ihre Sichtbarkeit wiedererlangen?**  
Google Panda
-  **Vorabversion von Windows 8 steht zur Verfügung**  
Microsoft
-  **Samsung legt gegen Urteil des Landgerichtes Düsseldorf bezüglich Galaxy Tab 10.1 Berufung ein**  
Berufung
-  **Die Hälfte der Deutschen fühlt sich im Internet beobachtet**  
Studie
-  **iphone 5 bald bei Vodafone und O2**  
Vorbestellungen in Kürze möglich

### Kommentar abgeben »

Ihr (Nick-)Name:

Titel für Ihren Eintrag:

Kommentar abgeben:

Bei einer Antwort möchte ich per Email benachrichtigt werden an meine Emailadresse:  (wird nicht veröffentlicht)

### Finde uns auf Facebook

**Registrieren**

Erstelle ein Konto oder **melde dich an**, um zu sehen, was deinen Freunden gefällt.



**Business News München**

Gefällt mir



**Business News München**

Der Countdown läuft...



**Oktoberfest: Letzte Aufbauarbeiten im Gange**  
[www.business-on.de](http://www.business-on.de)

Einen Tag vor Beginn des 178. Münchner Oktoberfests sind die letzten Aufbauarbeiten auf der Theresienwiese in vollem Gange.

Soziales Plug-in von Facebook