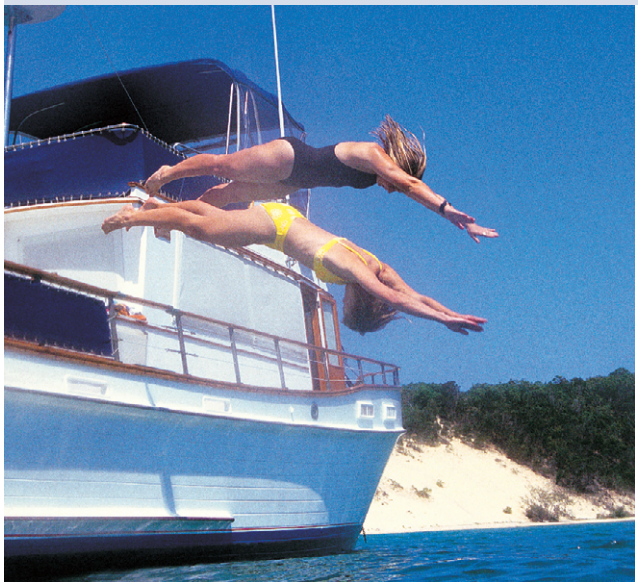
Sicherheitslücken bei Hosting-Providern, ein Update

Auf Tauchstation

Auf Sicherheitslücken hingewiesen reagieren viele Admins nicht oder nicht richtig. Selbst nachdem das Linux-Magazin 10/04 den Erfahrungsbericht eines Webhosting-Kunden veröffentlichte, behob dessen Provider nur einen Teil der Löcher. Ohne die spontane Hilfe des Hackers bestünde die Gefahr einfach weiter. Dirk P.



Im letzten Linux-Magazin berichtete ich von den gravierenden Sicherheitslücken [1] bei meinem Webhoster. Dessen Reaktion war – vorsichtig formuliert – eher zurückhaltend. Selbst meine Manipulation der privaten Website des Geschäftsführers konnte die Admins nicht zu größeren Anstrengungen bewegen. Ich hatte dafür gesorgt, dass der Server bei jeder URL dieser Domain mit einer HTML-Seite antwortete, die nur den Satz „Diese Domain wurde deaktiviert“ enthielt. Die Admins nahmen meine Änderung zwar zurück, das unsichere Passwort ließen sie aber unverändert.

Auf diesem Server hatte ich bislang noch keine Root-Rechte. Höchste Zeit, dies zu ändern. Hier läuft immer noch eine verwundbare Confixx-Installation, obwohl ein Update schon seit Wochen verfügbar ist. Ich verschaffe mir administrativen Zugriff und deaktiviere die Domain erneut. Diesmal präsentiert der Server einen Auszug aus der ».bash_history« von Root, als Beweis für meine neu erlangten Rechte. Auch diesen Eingriff machen die Admins wie erwartet rückgängig.

Das Passwort des FTP-Accounts »web637« ändert der Webhoster von »web6370« in »telefon«. Doch auch dies ist zu schwach, um John the Ripper lange standzuhalten. Als Reaktion auf mein History-Listing suchen die Admins nach der von mir benutzten Hintertür: Eine neue ».bash_history« (Listing 1) zeigt mir, dass sie dazu ein Tool names Rootkit-Hunter benutzen (Zeile 13). Meinen selbst angelegten »root2«-Account, dem ich genau wie Root die UID 0 gebe, bemerkt jedoch niemand.

Pech für die Admins, sie lassen meine leicht zu findende Hintertür einfach bestehen. Sie hätten sich nicht auf fertige Sicherheitsscanner verlassen dürfen, denn die sind nur als Hilfs- und nicht als Allheilmittel gedacht. Ich veröffentliche daher auch das neue History-File kurzzeitig auf der Domain des Geschäftsführers. Mein Root-2-Account besteht sogar einen Monat später noch.

Land in Sicht

Dabei sah es auf den Servern zwischenzeitlich recht gut aus. Die Admins hatten den Confixx-Cronjob entfernt, der unter anderem die Backup- und Restore-Requests abarbeitete. Somit waren die von mir entdeckten Sicherheitslücken nicht mehr auszunutzen. Nach und nach installierte der Hoster das Update auf die korrigierte Confixx-Version 3.0.3. Auch sonst bewegte sich einiges, die Admins gönnten ihren Systemen die Grsec-Patches [3], um künftige Angriffe schwieriger zu gestalten. Grsecurity ist aber sinnlos, wenn das System eklatante Sicherheitslücken hat, die auch ohne Buffer-Overflows nutzbar sind.

Trotz aller Gegenwehr erlange ich daher auf weiteren Servern Root-Rechte. Der Hoster war beim Deaktivieren der Backups nicht konsequent, außerdem endete seine Server-Update-Orgie verfrüht. Übrig blieben einige verwundbare 3.0-Versionen sowie 16 Server mit Confixx 2.0. Für diese ältere Version ist beim Hersteller SW-Soft [2] unverständlicherweise noch kein Sicherheitsupdate verfügbar. Hier müssten die Admins der Provider als Workaround die Backup-Funktion deaktivieren.

Klippen übersehen

Noch vor Erscheinen des Linux-Magazins 10/04 erhält der Hoster den Artikel [1] zur Einsicht. Die Admins haben erneut Gelegenheit, alle Sicherheitslücken zu beseitigen. Leserbriefe weisen aber darauf hin, dass das abgedruckte MySQL-Root-Passwort auf Server 53 weiterhin funktioniert. Auch ich stelle fest, dass einige Server noch Wochen später verwundbar sind. Der Hoster hatte nur einige Programme entfernt, etwa »ln« oder das für meine Webshell benötigte Python, aber das kann ich durch einen Upload schnell beheben.

Die Aktionen der Admins sind bestenfalls eine minimale Kindersicherung für Skript-Kiddies. Auf zwei Servern weise ich nach, dass die alten Löcher immer noch bestehen, vermutlich sind weitere betroffen. Ein sicheres Confixx 3.0.3 läuft nur auf der Hälfte der Maschinen.

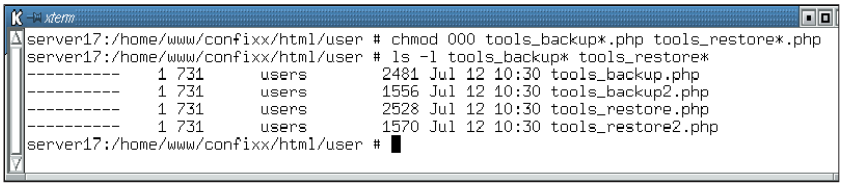


Abbildung 1: So einfach wäre es gewesen: Die Admins hätten nur per Chmod die fehlerhaften Confixx-Backup-Skripte sperren müssen, um die Sicherheitslücke zu schließen.

Doch irgendwann kann ich das traurige Schauspiel nicht mehr mit ansehen. Auf Server 53 betreibt ein Freund seine Domain, auf Server 17 liegt noch eine von mir selbst betreute Webseite. Ich beschließe daher, die Server selbst abzudichten, die dafür notwendigen Root-Rechte habe ich ja.

Server 53 spendiere ich ein neues MySQL-Root-Passwort, das ich mit »makepasswd --chars=16« generiere. Dieses trage ich auch in Konfigurationsdateien ein, damit Confixx weiterhin funktioniert. Auf beiden Servern deaktiviere ich außerdem das Backup, indem ich »chmod 000« auf die zugehörigen PHP-Dateien im Confixx-Document-Root anwende (siehe Abbildung 1).

So einfach lassen sich die Sicherheitslücken schließen. Beim Anfordern eines Backups meldet sich PHP nun mit einer Fehlermeldung (Abbildung 2). Die ist zwar hässlich, aber wenigstens sind die beiden Server sicher.

Sicherer Hafen

Mit Hilfe der Webhost-List [4] hatte ich kurz nach Verfassen des ersten Artikels nach einem neuen Anbieter gesucht. Neben der detaillierten Provider-Datenbank sind vor allem die Bewertungen anderer Benutzer interessant. Ein sicherheitstechnisches Urteil erwarte ich hier jedoch nicht. Ich entscheide mich für einen Webhoster, der für den Support sehr gute Noten erhalten hat. Meiner Meinung nach sollte der Support die Qualität der Administration und somit auch der Sicherheit widerspiegeln.

Nachdem ich die Zugangsdaten für meinen Account erhalten habe, schaue ich mich erst mal um. Und prompt finde ich das MySQL-Root-Passwort in einer für alle Benutzer lesbaren Konfigurationsdatei. Die Suche nach Sicherheitslecks geht also weiter. *(fjl)*

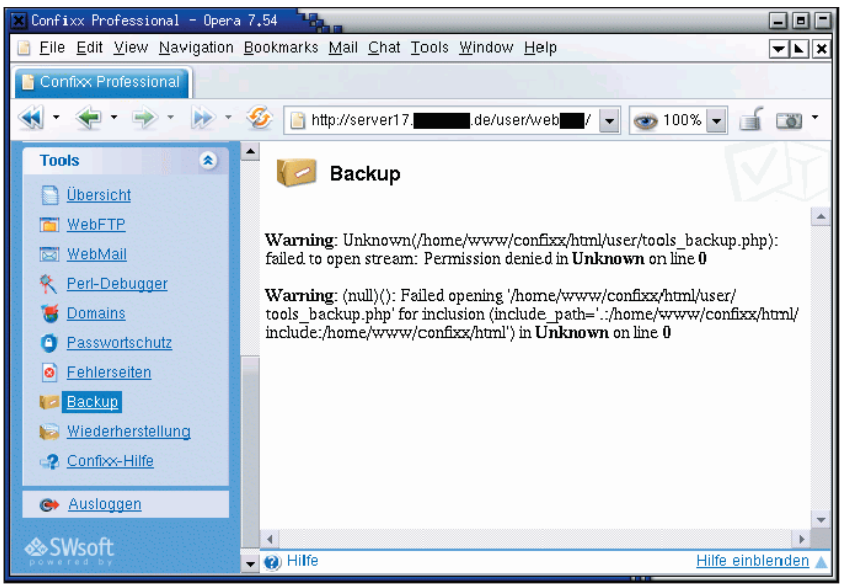


Abbildung 2: Auf Server 17 und Server 53 ist die fehlerhafte Backup-Funktion gesperrt. Die Sperre ist zwar nicht elegant (sie erzeugt eine Fehlermeldung), aber wirksam und schützt die Kunden.

Infos

[1] Dirk P., „Insel-Hüpfer – Sicherheitslücken bei Hosting-Providern, ein Erfahrungsbericht“: Linux-Magazin 10/04, S. 56
[2] SW-Soft: [http://www.sw-soft.com/de/]
[3] Grsecurity: [http://www.grsecurity.net]
[4] Liste von Webhostern: [http://www.webhostlist.de]

Der Autor

Dirk P. ist Informatiker, Programmierer und bekennender Langzeitstudent. Den ersten Kontakt mit Linux hatte er 1996, seit 1999 ist sein Computer Microsoft-freie Zone.

Listing 1: Bash-History

```
01 /root/confixx/confixx_counterscript.pl -fa -dbg
02 cd /home/www/
03 ls
04 jeo /etc/httpd/confixx_vhost.conf
05 joe /etc/httpd/confixx_vhost.conf
06 cd web637
07 ls
08 ls -al
09 last |grep web637
10 netstat -plunt
11 cd
12 ls
13 wget http://freshmeat.net/redir/rkhunter/46074/
   url_tgz/rkhunter-1.1.5.tar.gz
14 tar -zvxf rkhunter-1.1.5.tar.gz
15 cd rkhunter/
16 ./installer.sh
17 rkhunter -c
18 last |grep root
19 w
```