

Störungen von Minasol MN's ??

Beitrag von „Platzmeister“ vom 23. Dezember 2015, 23:55

So, mal hier ein Zwischenstand:

Der minasol-Server (also der von mir bei Strato gemietete Managed Server) wurde irgendwann in den letzten Woche gehackt. Dabei fiel er zuerst durch massenhaften Spam-Versand auf, weshalb die IP des Servers wohl auch auf diversen E-Mail-Blacklists erschien, was wiederum die Mail-Versandprobleme beim Wahltool erklärt. Bei einer weiteren massiven Attacke am letzten Wochenende (wahrscheinlich irgendwann am 19.12. mittags) wurden nun verschiedene Anwendungen beschädigt. Betroffen waren vor allem die neueren Versionen der Forensoftware von Woltlab, sowie der Websitebaker und fast alle Wordpress-Installationen. Nach meinen Erkenntnissen wurden MySQL-Datenbanken nicht beschädigt.

Strato hatte mich zuerst über den Spam-Versand informiert und hatte den Server wegen Überlastung vom Netz genommen. Ich habe ihn jedoch kurz danach wieder freischalten können. Das Infizierungsproblem besteht aber nach Angaben von Strato immer noch. Und weil die erste Attacke schon etwas länger zurückliegen muss verweigern sie auch die Rückspielung eines Server-Backups vom Anfang der vorigen Woche. Um den Schaden zu beseitigen, bleibt mit hoher Wahrscheinlichkeit nichts anderes übrig, als den Server komplett zu leeren und neu zu initialisieren. Dem habe ich jetzt erst einmal nicht zugestimmt, solange ich nicht eine Sicherung aller Anwendungsdaten habe. Die Sicherung des kompletten Dateisystems des Servers habe ich jetzt erst einmal gemacht (das sind komprimiert rund 9 GB) und die Datensicherung der MySQL-Datenbanken mache ich in den nächsten Tagen. Danach werde ich den Server wohl neu Initialisieren lassen.

Ich würde es begrüßen, wenn die Admins der einzelnen Projekte unabhängig von mir mal ihre Daten sichern (Webpace und Datenbank), so hätten wir eine doppelte Sicherheit. Manche Admins machen das ja bereits vorbildlich. Jeder Admin, dessen Projekt vom Hackerangriff beschädigt wurde, kann und sollte im Rahmen seiner Möglichkeiten schon mal versuchen, die Schäden durch Neu- oder Reparaturinstallation zu beheben und bei Erfolg der Arbeiten sofort wieder eine Sicherung erstellen. Denn wann konkret der Neustart durchgeführt wird, kann ich noch nicht sagen.

Soviel erst mal dazu von mir. Ich war ja bisher mit dem Server bei Strato recht zufrieden, aber die Arbeit des technischen Supports ist im Fehler- und Problemfall doch eher unbefriedigend. Und wozu ich den zusätzlichen Backup-Speicherplatz gegen zusätzliches Geld noch gemietet habe, wenn der dann doch nicht genutzt werden kann weiß ich nach dieser Aktion leider auch nicht mehr. Aber gut, aus Schaden wird man klug.

Aber nun erst mall allen ein frohes und friedliches Weihnachtsfest.