

Freitag, 9. November 2007

The day that routers died :)

Jedes Jahr treffen sich die europäischen ISPs, Exchange-Betreiber und sonstige IP-Netzwerk Interessierte um technische Aspekte der IP Netze, als auch insbesondere Zusammenschaltungsvereinbarungen zu diskutieren. Worum geht's? Eine der grossen technischen Herausforderungen, der viele Anbieter gegenüberstehen ist der Umstieg auf das IP-Protokoll Version 6. Um es kurz zu fassen: Die bisherigen IP-Adressen, wie 127.0.0.1 (IP Version 4) werden langsam knapp und so möchte man auf ein System umsteigen, welches einen grösseren Adressraum bietet. Wo ist das Problem? Für die Techniker heisst es aber, alle ihre Programme für das neue Protokoll zu wappnen, alte Hardware auszutauschen oder upzugraden. Bei den riesigen Netzen, verstreuten Komponenten und Progrämmchen ist das wohl eine Heidenarbeit, vor der sich jeder drücken will. Motivation Deswegen wurden die RIPE Teilnehmer mal in musikalischer und amüsanter Weise zu diesem Schritt motiviert: Tipp Übrigens, den Text findet man in der RIPE Datenbank im whois: http://www.ripe.net/perl/whois?form_type=simple&searchtext=POEM-RIPE55-SONG

Geschrieben von Sonnenparker in Webserver um 16:50

Montag, 5. Februar 2007

Jetzt auch Domaindiscount24 gehackt?

Da schreibe ich neulich noch über den Hacker von bösen Seiten, und paar Tage später wird schon ein beliebter deutscher Domain-Registrar gehackt. Wie im Nicit Forum zu lesen ist, erscheint nun auf den Seiten die auch bei DD24 gehostet werden eine Nachricht des Hackers. Die Message lautet: "Hacked By ahmetfener "Ärgerlich ist das, bleibt zu hoffen, dass der Provider bald entsprechnde Backups einspielt. Anspruch auf Schadensersatz? Dieser ist zumeist ausgeschlossen. Ohne die AGBs gelesen zu haben, lässt sich aber sagen, dass entsprechende SLAs (Service Layer Agreements) meist deutlich mehr kosten. Man darf sich hier übrigens nicht von Verfügbarkeitsgarantien blenden lassen. Diese sind üblicherweise auf Monate oder Jahre bezogen, dadurch ist selbst bei einem Ausfall von 24 Stunden und einer Verfügbarkeitsgarantie von 99,5% noch alles im Lot. Zum Nachrechnen: $365 * 24 * 0.005 = 43.8$ Ein Server darf also für bis zu 44 Stunden im Jahr ausfallen. Ursachen: Die Schuldigen sitzen meist vor den Rechnern. Es werden Skripte installiert die PHP SafeMode off fordern. Eingaben werden nicht überprüft, und im schlimmsten Fall werden beliebige Skripts aus dem Internet heruntergeladen oder eingebunden. Lösungen: Für die meisten semi-professionellen Anwender sei jedoch angemerkt: Ausfallsicherheit ist teuer. 99,999% ist eher eine Prestigefrage. Für euch sollte folgendes wichtig sein: regelmäßige Backups und keine sensiblen Daten auf dem Server. Dann ist alles halb so schlimm. Und was die wichtigeren Seiten betrifft? Haltet die TTL (Time-to-Live) Einträge der DNS Server niedrig und einen Backup-Server bereit. Dann kann bei Problemen der DNS-Server umgestellt werden und Kundenanfragen landen innerhalb kurzer Zeit auf einem funktionierenden Server. Es versteht sich aber von selbst, dass in der Zwischenzeit dafür gesorgt werden sollte, dass dort entweder die Lücke geschlossen ist, oder dass nur auf eine statische Seite geleitet wird, wo potentielle Kunden über die Probleme aufgeklärt werden.

Geschrieben von Sonnenparker in Webserver um 02:24

Donnerstag, 1. Februar 2007

Kann man Server wirklich absichern?

Wie heute auf bekannten Seiten zu lesen war, sind die Server von Mario Dolzer gehackt und Inhalte gelöscht worden. 25 Tausend Euro sind nun für die Aufklärung ausgelobt. Kann man Server wirklich absichern? Nun handelt es sich bei diesem Anbieter sicherlich um einen der umstritteneren Unternehmer im Internet. Was mich jedoch fraglich stimmt: Es ist davon auszugehen, dass Herr D. kompetente Techniker hat, schliesslich verfügt er über massive Besucherströme und steht schon seit Jahren als einer der "Bösen" im Schussfeld der Internetgemeinde. Er dürfte daher stetig irgendwelchen Attacken ausgesetzt sein. Umso mehr erstaunt es, dass nun Hacker erfolgreich waren. Ich frage mich ernsthaft, wie man die Sicherheit der eigenen Server sicherstellen soll, wenn es selbst jemanden mit enormen finanziellen Ressourcen und Mitarbeitern nicht gelingt. Wer jetzt Open Source ruft, oder denkt, dass es nur bösen Menschen passiert, sei an die Lahmlegung der Debian Server vor ein paar Jahren erinnert.

Geschrieben von Sonnenparker in Webserver um 23:14

Donnerstag, 11. Januar 2007

Segmentation Faults bei PHP 5.2 und Apache

Nun steht er der Blog. Hätte eigentlich schon viel früher passieren sollen, eigentlich nur kurz aptitude angeworfen und die neusten Updates eingespielt. Doch seit PHP 5.2 war das kein Vergnügen mehr - Segmentation Faults mehrten sich und die Kiste schmierte ab und zu ab. Die error.log des Apachen zeigte, dass etwa 80% der Seitenaufrufe zu einem Segmentation Fault des Child Prozesses führen. Auch das manuelle ausführen via PHP CLI zeigte zwar fast die ganze Seite, endete jedoch immer mit einem Segmentation Fault. Irgendwas musste geschehen. 1. Versuch: Alternatives Repository Erst dachte ich, es liegt an libapache2-mod-php5. Aber andere Versionen waren auf den normalen Zweigen auf die schnelle nicht zu finden. Ich habe daher mal die Pakete von dotdeb probiert. Aber irgendwie war das alles nichts. Sollte ich jetzt etwa auf immer und ewig alles selber kompilieren? PHP5, Apache, Mysql... Das würde irgendwie kein Ende nehmen. 2. Versuch: PHP5 via Fastcgi bzw. fcgid Der zweite Versuch war dann auf das Apache Modul zu verzichten. CGI schien es erstmal zu tun, Suphp war gut dokumentiert, aber es bleibt halt ein CGI Modul. Dass heißt, dass bei jedem Seitenaufruf der PHP Interpreter gestartet werden muss, anstatt, dass ein dauernder Prozess läuft und die Aufträge entgegennimmt. Die Lösung heisst: FastCGI. Hier wird zwar auch PHP via CGI eingebunden, aber der Prozess muss nicht bei jedem Aufruf neu gestartet werden. Nur leider ist die Entwicklung hier irgendwie eingestellt worden. Das Nachfolgeprojekt heisst fcgid und wird von einem Chinesen weiterprogrammiert. Es ist bestimmt sehr gut und eine elementare Doku war auf der (sehr langsam zu erreichenden) Webseite auch vorhanden, aber für einen Neuling wie mich, war das ein Overkill. Da Rechte anpassen. Irgendwo stand im Internet man sollte noch was patchen... Nicht falsch verstehen, Webserver Security ist wichtig, aber es muss auch immer den Ansprüchen genügen. Ich betreibe kein Hosting für Dritte, ich brauche kein Ausführen von Programmen für Benutzer die sich nicht sehen dürfen. Also beschloss ich diese Idee ersteinmal zurückzustellen, auch wenn mich das Konzept theoretisch überzeugt hat. Des Pudels Kern Die Lösung für mich war ein Snapshot des Pakets. Ich hatte bei meiner Recherche gesehen, dass PHP 5.2 einige Probleme verursachen kann. Eine Suche nach PHP5.2 "Segmentation fault (11)" brachte recht viele Treffer und ich hatte das Gefühl, dass es irgendwie daran liegen müsste. Schliesslich sind die Probleme immer erst mit den Updates gekommen. Da ich das Problem sowohl beim 32bit, wie auch beim 64bit Server beobachten konnte, war ein Zusammenhang mit den früher typischen AMD64 Bugs in Debian ausgeschlossen. Edlich die Lösung: back to PHP 5.1 Ich habe om Debian Snapshot Server ein älteres PHP Paket eingespielt. Dazu muss man sich dort die passenden Einträge für die sources.list von apt heraussuchen. In meinem Fall waren das: deb
[http://snapshot.debian.net/archive/pool php5deb-src](http://snapshot.debian.net/archive/pool/php5deb-src) [http://snapshot.debian.net/archive/pool php5deb](http://snapshot.debian.net/archive/pool/php5deb)
[http://snapshot.debian.net/archive/pool php-imapdeb-src](http://snapshot.debian.net/archive/pool/php-imapdeb-src) [http://snapshot.debian.net/archive/pool php-imapdeb](http://snapshot.debian.net/archive/pool/php-imapdeb)
[http://snapshot.debian.net/archive/pool php-interbasedeb-src](http://snapshot.debian.net/archive/pool/php-interbasedeb-src) [http://snapshot.debian.net/archive/pool php-interbasedeb](http://snapshot.debian.net/archive/pool/php-interbasedeb)
[http://snapshot.debian.net/archive/pool php-mcryptdeb-src](http://snapshot.debian.net/archive/pool/php-mcryptdeb-src) [http://snapshot.debian.net/archive/pool php-mcryptdeb](http://snapshot.debian.net/archive/pool/php-mcryptdeb)
[http://snapshot.debian.net/archive/pool php-pspelldeb-src](http://snapshot.debian.net/archive/pool/php-pspelldeb-src) [http://snapshot.debian.net/archive/pool php-pspelldeb](http://snapshot.debian.net/archive/pool/php-pspelldeb)
[http://snapshot.debian.net/archive/pool php5-tidydeb-src](http://snapshot.debian.net/archive/pool/php5-tidydeb-src) [http://snapshot.debian.net/archive/pool php5-tidy](http://snapshot.debian.net/archive/pool/php5-tidy) Schnell noch in Aptitude eine richtige Version ausgewählt, und seitdem schnurrt der Server wieder wie ein kleiner Jaguar. :)

Geschrieben von Sonnenparker in Debian um 18:54