



Richtlinien zur Systemverwaltung

Autor: Johnny Graber (*linux@jgraber.ch*)
Autor: Florian Frank (*florianfrank@gmx.de*)
Layout: Johnny Graber (*linux@jgraber.ch*)
Lizenz: GFDL

Eine kurze Auflistung der wichtigsten Richtlinien der Systemverwaltung.

Inhaltsverzeichnis

1 Richtlinien und Grundsätze

1 Richtlinien und Grundsätze

Dieser kurze Text geht auf die wichtigsten Grundsätze der Systemverwaltung ein. Es sind allgemein gültige Grundsätze und Richtlinien, die jeder Administrator kennen sollte.

Auch die "Heimrechner-Admins" sollten sich einige Punkte merken. Auch auf einem solchen Rechner schmerzt der Verlust der Daten..

Sollte Ihnen das Fehlen einer wichtigen Richtlinie auffallen, senden Sie uns bitte einige Zeilen dazu an unsere [Adresse](#). Wir werden Ihren Vorschlag prüfen und gegebenenfalls mit in das nächste Release aufnehmen.

- * Den root-Account nur so lange verwenden, wie unbedingt notwendig. Keinesfalls als root die tägliche Arbeit machen. Dafür sind die gewöhnlichen Benutzeraccounts.
- * Administrative Aufgaben sollten niemals müde oder in Eile ausgeführt werden.
- * Zu jeder Maschine sollte ein Maschinenbuch mit Einträgen über aufgetretene Probleme, einer Liste aller wichtigen Dateien (und deren Veränderung), einer Liste der Backups etc. geführt werden.
- * "Never touch a running system" ist out. Security-Updates müssen so bald als möglich eingespielt werden. Um immer auf dem laufenden zu sein, empfiehlt sich das Lesen der Nachrichten von [DFN-CERT](#). Deren Sicherheits-Infos werden auf zahlreichen Webseiten angeboten.
- * Immer an die [Backups](#) denken. Backup-Strategien schon vor dem Systemausbau planen. Zudem dafür sorgen, dass die Backups nicht nur erstellt, sondern auch geprüft werden.
- * Bei wichtigeren Systemen nicht nur ans Backup denken, sondern zum vornherein ein Disaster-Recovery-Plan zurecht legen.
- * Grössere Veränderungen an einer Maschine besser zuerst an einer baugleichen Maschine testen, sofern dies möglich ist.
- * Nur die Software installieren, die auch benötigt wird. Weniger Software = weniger mögliche Sicherheitslöcher.
- * Die Benutzer über Veränderungen schnellstens informieren. Nur informierte Benutzer können sich an die neuen Regeln halten.
- * Regelmässiges durchschauen der Logfiles. Vorkehrungen treffen, das bei Unregelmässigkeiten schnell gehandelt werden kann.
- * Sichere [Passwörter](#) verwenden. Keine nebeneinander liegenden Tastenkombinationen (wie asdf oder qwer), Vornamen und Geburtstage verwenden.