SelfLinux-0.13.1

Richtlinien zur Systemverwaltung

Autor: Johnny Graber (*linux@jgraber.ch*)
Autor: Florian Frank (*florianfrank@gmx.de*)
Autor: M. Kleine (*kleine_matthias@gmx.de*)
Formatierung: Johnny Graber (*linux@jgraber.ch*)

Eine kurze Auflistung der wichtigsten Richtlinien der Systemverwaltung.

1 Richtlinien und Grundsätze

Dieser kurze Text geht auf die wichtigsten Grundsätze der Systemverwaltung ein. Es sind allgemein gültige Grundsätze und Richtlinien, die jedem Administrator bekannt sein sollten.

Auch Administratoren von Heimrechnern sollten die wichtigsten Punkte verinnerlichen. Auch bei solchen Rechnern schmerzt der Verlust der Daten...

Sollte eine wichtige Richtlinie fehlen, senden Sie uns bitte einige Zeilen dazu an unsere *Adresse*. Wir werden Ihren Vorschlag prüfen und gegebenenfalls in das nächste Release von SelfLinux aufnehmen.

* Den root-Account nur so lange verwenden, wie unbedingt notwendig. Keinesfalls root für die tägliche Arbeit verwenden. Hierfür sollten ausschließlich die gewöhnlichen Benutzeraccounts genutzt werden.
* 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 Backups nicht nur erstellt, sondern auch geprüft werden.
* Bei wichtigen Systemen nicht nur ans Backup denken, sondern auch von vornherein einen Desaster-Recovery-Plan anfertigen.
* Größere Veränderungen an einer Maschine besser zuerst an einer baugleichen Maschine testen, sofern dies möglich ist.
* Nur Software installieren, die wirklich benötigt wird. Weniger Software bedeutet weniger potentielle Sicherheitslöcher.
* Auf einem Multiusersystem die Benutzer über Veränderungen schnellstens informieren. Nur informierte Benutzer können sich an neue Regeln halten.
* Regelmäßiges Sichten von Logfiles. Vorkehrungen treffen, dass bei Unregelmäßigkeiten schnell gehandelt werden kann.
* Sichere Passworte verwenden. Keine nebeneinander liegenden Tastenkombinationen (wie asdf oder qwer), Vornamen oder Geburtstage verwenden.