

Linux Systemsicherheit Teil I

Geschrieben von: Wolfgang

Montag, den 23. August 2010 um 20:39 Uhr - Aktualisiert Montag, den 23. August 2010 um 21:01 Uhr



Hier ein paar Worte über Systemsicherheit allgemein.

Systemdienste wie z.B. Webserver Apache, Tomcat, JBoss und andere Dienste sollte man aus Sicherheitsgründen nicht im root-modus laufen lassen, wie es in vielen Linux Distributionen üblich ist.

Die Dienste werden in der Regel als "root" gestartet und haben damit Systemverwalter Rechte was unter Umständen gefährlich werden kann.

Wenn es einem Angreifer gelingt einen Dienst mit einer sog. DOS-Attacke oder einem bekannten / unbekanntem Exploit ausser Gefecht zu setzen, kann der Angreifer möglicherweise root-Rechte erlangen und das System von aussen kompromitieren.

Dies ist nicht erwünscht. Daher alle Dienste wie z.B. Mail, Web und andere möglichst im User-Modus laufen lassen.

Wenn ein Dienst ausser Gefecht gesetzt wird kann der Angreifer maximal User-Rechte erlangen und das System nicht ernsthaft schädigen.

Weitere Tipps folgen noch...

euer Admin