Rootkit

Rubrik: Lexikon

Ein Rootkit ist eine Werkzeugsammlung für Software, die dazu genutzt wird, um Login-Versuche sowie Dateien und Verzeichnisse auf einem Rechner zu verstecken.

Rootkits existieren dabei für alle Betriebssysteme und haben vor allem das Ziel, bestimmte Schadprogramme (Malware) vor dem Nutzer zu verbergen. Installiert wird das Rootkit dabei ohne Wissen des PC-Administrators und kann auch bei Entdecken nicht mehr so einfach vom Rechner entfernt werden.

Es gibt dabei drei verschiedene Arten von Rootkits.

Der Kernel-Rootkit ersetzt einige Betriebssystemteile durch eigenen Schadcode zur Tarnung für seine Anwesenheit sowie zur Erweiterung der Funktionen für den Angreifer.Ein Userland-Rootkit modifiziert API-Funktionen und Speicher-Rootkits verstecken sich im Arbeitsspeicher, wobei sie nach dem nächsten Neustart des Rechners nicht mehr auffindbar sind.