Rootkit

17. Juli 2015

Root ist unter Linux der Administrator. Ein Rootkit (englisch etwa: Administratorenbausatz) ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Softwaresystem auf dem kompromittierten System installiert wird, um zukünftige Anmeldevorgänge (logins) des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken. Zweck eines Rootkits ist es, Schadprogramme (Malware) vor den Antivirenprogrammen und dem Benutzer durch Tarnung zu verbergen.

Backdoor-Funktionalitäten

Ein Rootkit versteckt normalerweise Anmeldevorgänge, Prozesse und Logdateien und enthält oft Software, um Daten von Terminals, Netzwerkverbindungen und Tastaturanschläge und Mausklicks sowie Passwörter vom kompromittierten Systems abzugreifen. Hinzu können Backdoors (Hintertüren) kommen, die es dem Angreifer zukünftig vereinfachen, auf das kompromittierte System zuzugreifen, indem beispielsweise eine Shell gestartet wird, wenn an einen bestimmten Netzwerkport eine Verbindungsanfrage gestellt wurde. Die Grenze zwischen Rootkits und Trojanischen Pferden ist fliessend, wobei ein Trojaner eine andere Vorgehensweise beim Infizieren eines Computersystems besitzt.

Technische Umsetzung

Das Merkmal eines Rootkits ist es, dass es sich ohne Wissen des Administrators installiert und dem Angreifer die Basis zum Installieren von z. B. Viren oder die Möglichkeit zu DDoS (Distributed Denial of Service) bietet. Rootkits können neue Hintertüren (backdoors) öffnen. Zudem versuchen Rootkits, den Weg ihres Einschleusens zu verschleiern, damit sie nicht von anderen entfernt werden.

Entfernung von Rootkits

Da eine hundertprozentige Erkennung von Rootkits unmöglich ist, ist die beste Methode zur Entfernung die vollständige Neuinstallation des Betriebssystems. Da sich bestimmte Rootkits im BIOS verstecken, bietet selbst diese Methode keine hundertprozentige Sicherheit. Um eine Infizierung des BIOS im vornherein zu verhindern, sollte das BIOS hardwareseitig mit einem Schreibschutz versehen werden, z. B. durch einen Jumper auf der Hauptplatine.