

# Rootkit

Wie würden Sie sich fühlen, wenn jemand ohne Ihr Wissen Zugriff auf Ihren Computer hätte? Leider lässt sich dies mit einem Rootkit durchaus bewerkstelligen, das in verschiedenen Produkttypen installiert sein kann, und mit dem sich Geräte fernsteuern lassen.

## Was ist ein Rootkit?

Ein Rootkit ist ein Programm, mit dem sich Hacker ohne Ihr Wissen Administratorzugriff auf Ihren Computer verschaffen wollen.

## Woher stammen Rootkits

Rootkits können auf verschiedene Weise installiert werden, z. B. auch durch kommerzielle Sicherheitsprodukte und scheinbar sichere Erweiterungen von Drittherstellern. Rootkits können sich nicht selbst fortpflanzen, sind jedoch Bestandteil konzertierter Angriffe.

## Wie erkennt man ein Rootkit?

Das Erkennen von Rootkits kann sehr mühsam sein. Überprüfen Sie beim Durchsuchen des Systemspeichers alle Einstiegspunkte aufgerufener Prozesse und Aufrufe von Import-Bibliotheken (von DLLs aus), die vielleicht mit einem Hook versehen oder anderweitig auf andere Funktionen umgeleitet wurden. Wenn Sie sicherstellen möchten, dass sich kein Rootkit auf Ihrem PC befindet, sollten Sie einen PC-Scanner verwenden (z. B. die kostenlosen Avast Virenschutz- und Anti-Malware-Tools).

## Wie entfernt man ein Rootkit?

Virenschutz-Software kann Rootkits und rootkit-ähnliches Verhalten erkennen. Beim Scannen nach Rootkits können die meisten Programme ein vorhandenes Rootkit anhalten, das Löschen des Rootkits selbst muss jedoch manuell vorgenommen werden.

## Wie kann man gegen Rootkits vorbeugen?

- Verwenden Sie aktualisierte Virenschutz- und Firewall-Software.