

HELPDESK

Rootkits: Sichtung des Unsichtbaren

Was sind eigentlich Rootkits? Wie kommen diese in mein System? Was bewirken sie dort und wie kann ich mich dagegen schützen?

Ein Rootkit ist ein Trojanisches Pferd mit Tarnkappe. Es ist eine Software, die sich in Computersystemen einnistet und versteckt, so dass sie mit herkömmlichen Mitteln nicht zu entdecken ist.

Die Infektion erfolgt über E-Mail-Attachments, die Installation illegaler Software oder durch das Ausnutzen von Verwundbarkeiten in Applikationen (z.B. Browser) oder Netzwerkdiensten. Wie bei Trojanern kommen Dropper-Programme zum Zuge, um den schadhafte Code einzupflanzen. Es geht aber auch anders: Ende 2005 machte Sony's Kopierschutz für Musik-CDs von sich hören, als bekannt wurde, dass dieser ein Rootkit installiert. Unter Mediendruck zog Sony die betroffenen CDs vom Markt und stellte ein Tool zum Entfernen der Tarnfunktion (nicht des Rootkits!) zur Verfügung – was zu guter Letzt noch eine Sicherheitslücke hinterliess.

Rootkits lassen sich grob in Kernel- und Userland-Rootkits einteilen. Damit wird bezeichnet, in welchem Kontext sich das Programm installiert. Es wurden auch bereits Rootkits entwickelt, die sich im BIOS einnisten, also unabhängig vom Betriebssystem agieren. Aufgrund der Kompatibilität stellt diese Kategorie aber eine kleinere Bedrohung dar.

Funktionsweise: Applikationen nutzen für die Ein- und Ausgabe die vom Betriebssystem zur Ver-

«Eine seriöse Suche nach Rootkits muss ausserhalb des Systems statt finden.»

fügung gestellten Funktionen (APIs). Damit eine Applikation weiss, wo der aufzurufende Code zu finden ist, unterhält das Betriebssystem eine sog. Syscall-Tabelle mit einer Referenz zur Speicherstelle der jeweili-



ILLUSTRATION: OWTHU

gen Funktion. Ein Rootkit manipuliert nun diese Referenz und leitet den Aufruf auf eine eigene Funktion um, welche wiederum die originale Funktion aufruft. Dies ist grundsätzlich ein erwünschtes Feature. Das Rootkit jedoch manipuliert die ausgehenden Daten, um sich zu verstecken. Im Hackerjargon wird diese Technik als cloaking (Verhüllung) bezeichnet.

Um zum Beispiel den eigenen Prozess unter Windows zu verstecken, muss sich ein Rootkit im Systemaufruf EnumProcesses einnisten. Diese Funktion liefert einen Array mit sämtlichen Prozess IDs zurück. Durch eine einfache Schleife kann das Rootkit nun seine eigene Prozess-ID entfernen, bevor es den Array zurückgibt: Der Prozess des Rootkits ist unsichtbar. Analog dazu kann es auch Treiber im Dateisystem, offene Ports oder Referenzen in der Registry verstecken.

Massnahmen und Enttarnung: Der beste Weg, sich vor Rootkits zu schützen, ist zu verhindern, dass sie überhaupt installiert werden. Dazu steuern die gängigen Sicherheitsmassnahmen wie Patching, Firewalls, Virensca-

ner und ein sinnvoller Umgang mit dem Internet bei.

Ein installiertes Rootkit lässt sich nicht durch herkömmliche Virens Scanner entdecken. Dennoch gibt es Möglichkeiten, diese Schädlinge zu finden. Einen interessanten Ansatz verfolgt «Rootkit Revealer» aus der sysinternals Sammlung. Das kompakte Gratis-Tool für Windows nutzt sowohl Systemaufrufe als auch Direktzugriffe auf Dateisystem und Registry. Diskrepanzen liefern Hinweise auf vorhandene Rootkits. Zahlreiche Falschmeldungen sind jedoch vorprogrammiert

Generell ist es falsch, über ein lokales System zu suchen. Eine seriöse Suche nach Rootkits muss ausserhalb des verdächtigen Systems stattfinden, indem zum Beispiel die Festplatte ausgebaut und in einem vertrauenswürdigen System untersucht wird. Externe Portscans oder das Mitschneiden des Netzwerkverkehrs erhöhen die Erfolgchance, da sich so Backdoor-Funktionen, Steuerbefehle und gestohlene Daten zeigen können. Wer jedoch auf Nummer sicher gehen will, installiert das Betriebssystem neu. ■

 **Archiv aller Helpdeskartikel:**
www.computerworld.ch



Der Autor
Simon Wepfer ist CTO bei der Sicherheitsberaterin Oneconsult, Thalwil. www.oneconsult.com

Jede Woche beantworten Sicherheitsexperten Ihre Leserfragen:

Haben Sie Fragen rund ums Thema IT-Sicherheit?

Schreiben Sie uns:
it-security@computerworld.ch