der Newsletter vom PC MAGAZIN vom 07. April 2008

Rootkits - die versteckte Gefahr

Weit gefährlicher als Viren oder gewöhnliche Malware sind Rootkits. Das sind Programme, die ihrerseits andere Schadprogramme verstecken. Sie merken also nicht einmal, dass Ihr PC infiziert ist. Wir zeigen Ihnen, wie Sie solche Rootkits beseitigen.

von Peter Kraft am 23.03.2008

Schon 2006 stellte das Sicherheitsunternehmen McAfee eine drastisch zunehmende Verbreitung von Mechanismen fest, die Schadprogramme auf PCs verstecken sollen: in drei Jahren um mehr als 600%. Solche Tarn-Tools, Rootkits genannt, sind auf dem Vormarsch und verstecken Trojaner, Würmer und sonstige Spyware auf immer raffinierter werdende Weise.

Das Problem: Von vielen herkömmlichen Security-Tools werden sie nicht erkannt und folglich auch nicht bekämpft. Lesen Sie hier, wie Sie den digitalen Schädlingen trotzdem die Tarnkappe entreißen und die Bedrohung

Rootkits von Musik-CDs und Filmen

Dass Rootkits nicht nur von bösen Hackern und Internet-Kriminellen verwendet werden, belegt eindrucksvoll die Affäre um das Rootkit des Musikunternehmens Sony BMG. Auf dieses wurde 2005 ein Sicherheitsexperte aufmerksam, als sein Rechner auf einmal merkwürdig reagierte -- kurz zuvor hatte er eine Musik-CD von Sony BMG in die Schublade seines CD-Players gesteckt. Was dann geschah, liest sich wie ein Krimi: Ohne jegliches Zutun des Anwenders startete ein Installationsprogramm, das den Anwender darüber informierte, die CD sei nur mit der jetzt installierten Player-Software lauffähig.

Im Hintergrund tat sich eine ganze Menge mehr! Das XPC-Rootkit von Sony BMG manipulierte Systemaufrufe, installierte Filtertreiber für die optischen Laufwerke, um Kopieraktionen zu unterbinden, und verbarg in Folge alle Dateien und Verzeichnisse mit bestimmten Namen. Anschließend kontrollierte es ständig alle Audioprozesse, was zu einer erhöhten Systemlast führte und weitere Sicherheitslöcher aufriss, die andere Programmierer von Malware für ihre Zwecke nutzten. Eine Deinstallationsroutine hatte Sony nicht vorgesehen.

Der hier beschriebene Prozess ist typisch für Rootkits: Solche Tools manipulieren und ersetzen Systemdateien, legen geheime Registry-Einträge an oder ändern Arbeitsspeicher und das gesamte Dateisystem so, dass der Anwender weder mit Windows- Bordmitteln wie Windows Explorer und Task-Manager noch mit normalen Virenscannern merkt, dass er infiltriert und ausspioniert wird. Ist erst einmal ein effizientes Rootkit auf dem Rechner, lässt sich dieser PC komplett übernehmen -- und damit auch für kriminelle Zwecke missbrauchen.

Rootkits sind deshalb mittlerweile eine der größten Gefahren, denen Internet- und Computer- Anwender heute gegenüberstehen, da sie normale Gegenmaßnahmen gegen Malware wie Sypware oder Würmer in vielen Fällen wirkungsvoll verhindern. Nicht umsonst heißt der Klassiker unter den Rootkits „Hacker Defender“: Es soll verhindern, dass man die Aktivitäten von Hackern auf seinem System unterbindet.

Auch wenn Rootkits für viele Computernutzer schwer verdauliche Kost sind, lohnt es sich im Hinblick auf ihre Abwehr dennoch, kurz einen Blick auf ihre grundlegenden Mechanismen zu

werfen. Vereinfacht ausgedrückt, verfügen Betriebssysteme wie Windows über zwei Strukturen oder Modi: Alle Basisoperationen wie Speicherzugriff, Laufwerks- und Grafiksteuerung werden im so genannten Kernel abgewickelt, während die Anwenderprogramme über die Zwischenschicht WinAPI auf diese grundlegenden Systemfunktionen zugreifen. So wird sichergestellt, dass Fehler in den Programmen nicht das gesamte System in den Abgrund reißen.

Der größten Bedrohung auf der Spur

Analog zu dieser Struktur unterscheidet man auch bei den Rootkits zwei Arten. Die so genannten Userland Rootkits machen nichts Anderes, als ihren schädlichen Programmcode in andere Anwenderprogramme zu injizieren. Hier sucht man sie in der Regel natürlich nicht und kann sie auch nicht über den Task-Manager, den Datei-Explorer oder andere Programme finden.

Noch cleverer agieren Kernel-Rootkits, die sich zum Beispiel als Gerätetreiber getarnt im Kernel verankern oder verhaken. Wenn ein solches Tool im Kernel residiert, kann das Rootkit in der Folge alle Datei- und Speicherzugriffe von anderen Programmen kontrollieren und damit auch der Verfolgung durch Malware-Scanner entgehen. Ein herausragender Vertreter seiner Art ist das Rootkit Hacker Defender. Es verbirgt sich durch Manipulation von Gerätetabellen, verankert aber für bestimmte Zusatzfunktionen nebenbei einen Gerätetreiber im Kernel – und zufällig sind auch noch ein Keylogger und eine Backdoor integriert. Die neueste Generation von Rootkits wie das FU Rootkit oder FUTo bringen zusätzlich eine neue Technik ins Spiel: die Direct Kernel Object Manipulation (DKOM), womit man Prozesse und Treiber noch besser tarnen kann.