

15.02.2006

Süddeutsche Zeitung

Computerviren mit Tarnkappe

Rootkits sind die neuen Superwaffen der Hacker - Sony BMG hat sie zuerst genutzt.

Bis vor einigen Wochen kannten bestenfalls einige Administratoren von Computer-Netzwerken den Begriff "Rootkit". So heißen Computerprogramme, die Angreifer bei einem Einbruch in ein Computersystem installieren können.

Einmal in den Tiefen des Betriebssystems versteckt, dienen Rootkits dazu, neue Einbrüche zu verbergen, Daten zu sammeln, Tastatureingaben mitzuschneiden - und derlei fiese Dinge mehr. Mit einem Rootkit erlangt ein Angreifer unentdeckt die Kontrolle über ein System.

Weltweite Bekanntheit erreichten Rootkits, als die Plattenfirma Sony BMG vor einigen Wochen einen neuen Kopierschutz für ihre CDs auf den Markt brachte. Sobald eine mit der Schutz-Software XCP versehene CD am Computer abgespielt wurde, installierte das Programm heimlich zusätzliche Software: ein klassisches Rootkit.

15 Schutzprogramme - keines findet den Rootkit

Doch das ungebührliche Verhalten von Sony blieb nicht lange unentdeckt. Was folgte, war ein weltweiter Aufschrei der Empörung, der soweit führte, dass der Konzern versprach, die betreffenden CDs zurückzuziehen.

Das Problem mit den Rootkits dürfte sich damit allerdings noch längst nicht erledigt haben, warnen die Hersteller von Computerviren-Schutzprogrammen. Im Gegenteil: "Ein Rootkit kann sich komplett vor Suchprogrammen verstecken", sagt Gernot Hacker von der Firma H+BEDV Datentechnik, dem Hersteller der Schutz-Software "Antivir". Die Viren könnten sich in Zukunft verstärkt Tarnkappen nach dem Muster des Sony-Kopierschutzes zulegen und so durch das Raster der Virens Scanner schlüpfen.

Wie real solch eine Bedrohung bereits ist, zeigt ein Test der Computerzeitschrift c't: Kein einziges von 15 Schutzprogrammen schaffte es dabei, durch Rootkits versteckte Viren im System zu entdecken.

Angesichts solcher Nachrichten frohlockt die Szene der Virenschreiber.

Warnsignal: langsamere Rechnerleistung

Seit rund einem Jahr, so erklärt c't-Redakteur Jürgen Schmidt, würden sich Virenautoren verstärkt für Rootkit-Technologien interessieren. Schmidts Prognose fällt entsprechend düster aus: "Das wird massiv zunehmen."

Für User sind das gleich mehrere schlechte Nachrichten auf einmal. Zum einen ist es sehr schwierig, überhaupt zu erkennen, wann ein Computer von einem Rootkit-Virus befallen ist. "Anzeichen für einen Befall, wie etwa die Verlangsamung von Rechnerleistung oder untypische Netzwerkkommunikation, sind oft nicht erkennbar", sagt **Oliver Karow von der Antiviren-Firma Symantec**. "Noch dazu arbeiten die Rootkits komplett im Verborgenen."

Aber auch wenn er die Infektion seines Rechners erkannt hat, wird es für den User keineswegs einfacher. "Wenn ein Rootkit erst einmal installiert ist, hat man schlechte Karten, es wieder herunterzubekommen", sagt Gernot Hacker. Herkömmliche Antivirenprogramme scheitern, weil sie den in den Tiefen des Betriebssystems versteckten Virus nicht wahrnehmen können.

"Wir sind machtlos, uns gegen das Betriebssystem zu wehren. Sonst wären wir ja auch ein Stück weit ein Rootkit", sagt Hacker. Im Prinzip gibt es zwar spezielle Software zur Entfernung einiger Rootkits, doch um solche Software zu benutzen, benötigen Nutzer oft Kenntnisse, die auch fürs Informatik-Diplom reichen dürften.

So bleibt betroffenen Usern kaum mehr übrig als eine Radikallösung: "Ich würde in so gut wie allen Fällen empfehlen, die Daten in Sicherheit zu bringen und das System komplett neu zu installieren", rät c't Sicherheitsfachmann Jürgen Schmidt.