

Ausgabe: 48/2005

Seite: 12

Zeitschrift: [COMPUTER ZEITUNG](#) »

Hacker und Malware können ihre Anwesenheit geschickt verschleiern – Problem aus der Unix-Welt schwappt hinüber auf Microsoft-Rechner

Viren und Spione tarnen sich mit Rootkits

Die jüngste Aufregung um Sonys Rootkit-verseuchte Musiksoftware zeigt: Angriffe mit Hilfe von Tarn-Tools nehmen zu. Der Schutz davor ist nicht trivial.

Erst vor kurzem entdeckte die Universität von Connecticut ein im Oktober 2003 installiertes Rootkit auf einem ihrer Server. Anderthalb Jahre lang konnte der Hacker damit seinen Einbruch auf dem Rechner mit Account-Daten von 72 000 Studenten verbergen.

Und: „Während es früher überwiegend Rootkits für Linux- und Unix-Systeme gab, sind mittlerweile auch welche für Windows und Oracle-Datenbanken verfügbar“, warnt **Oliver Karow, Sicherheitsexperte bei Symantec**. Da sich diese nur schwer lokalisieren lassen, würden wohl künftig vermehrt Würmer mit Rootkit-Funktionen auftreten. Bereits heute gibt es einige Würmer, Spyware und Trojaner, die Tarntechniken verwenden, bestätigt der McAfee-Experte Toralv Dirro den Trend zur versteckten Malware.

Im einfachsten Fall werden dabei System-/Administrator-Befehle ersetzt, so dass bei der Anzeige der laufenden Prozesse die Programme und das Login des Angreifers ausgeblendet werden. „Neben diesen Userland-Rootkits, die nur Programme ersetzen, gibt es Kernel-space-Rootkits, die Funktionen direkt im Betriebssystem verändern“, sagt Raimund Genes, Europa-Chef bei Trend Micro: „Im schlimmsten Fall hilft dann nur noch das Booten eines sauberen Systems – zum Beispiel von CD oder USB-Stick – und der Vergleich von Soll-/Ist-Zustand sowie das komplette Neuaufsetzen des Systems.“

Allerdings ist das rasche Handeln nur sinnvoll, wenn die Ursache des Problems feststeht. Denn die nachträgliche forensische Analyse gestaltet sich ausgesprochen komplex. „Nur blind neu zu installieren, stellt oft keine gute Lösung dar“, warnt Cirosec-Berater Stefan Strobel. Statt dessen sei auf der Basis einer exakten Analyse ein gezieltes Incident-Handling erforderlich.

Die Malware stoppen bevor es zu spät ist

„Auf Produktseite eignen sich Host-basierte Intrusion Prevention Systeme, um ein Einschleusen der Rootkits zu erschweren“, rät Strobel. Die Security-Softwerker feilen zudem an Hybridprodukten, die Anti-Virus und Betriebssystem-Schutz kombinieren. „Das Ziel muss sein, Spyware und Malware zu stoppen, bevor sie Rootkits installieren können“, nickt Trend Micros Genes. F-Secure kombiniert in seiner Desktop-Suite nicht nur Virenschutz, Desktop-Firewall, Intrusion Detection und Spywareschutz, sondern integriert auch den generischen Rootkit-Scanner Blacklight. „Bisher jedoch wird traditionelle Malware immer noch als das größere Problem betrachtet als versteckte“, sagt Jukka Kapanen, Product Manager der Finnen. Viele Administratoren seien noch nicht an die unsichtbare Gefahr gewöhnt.

Bis ausgefeilte Schutz- produkte verbreitet sind, müssen alt bekannte Basismaßnahmen greifen – etwa das Einspielen von Patches, damit der Angreifer nicht über ein Sicherheitsloch ins Betriebssystem eindringt und sich so Root- beziehungsweise Admin-Rechte erschleicht. Genes empfiehlt am PC außerdem eine klare Trennung zwischen Nutzer und Administrator: „Anwender sollten nicht mit Admin-Rechten unter Windows arbeiten.“ Dadurch sei es für Spyware und Malware deutlich schwieriger, Systemkomponenten zu modifizieren.

Allerdings schützen auch derartige Maßnahmen nicht vor allen Angriffen. „Es ist schwierig, ein Produkt gegen Rootkits zu entwickeln“, sagt Alexander Kornbrust von Red-Database-Security. Schließlich gebe es unzählige Varianten des verdeckten Katz- und Maus-Spiels im Cyberspace – etwa einen Buffer Overflow in einem Dienst, der mit Administrator-Rechten läuft. Dadurch könne sich ein nicht-privilegierter User doch noch eine Verwaltungshoheit ergaunern.

Sony versteckt auch Trojaner

Doch sogar kommerzielle An- bieter schrecken vor solchen Tarntechniken nicht zurück. So hat der Musikkonzern Sony in den USA auf Audio-CDs mit Rootkit-Technik verborgene Software zum Digital-Rights-Management ausgeliefert und damit einen Sturm der Entrüstung ausgelöst. In Windeseile hatten nämlich auch Autoren von Botnetz-Trojanern die Chance genutzt und sind unter Sonys Tarnmantel geschlüpft. Hersteller von Antispyware-Tools wie Symantec und Microsoft haben Sonys Software daher auf die Abschussliste gesetzt.

Lothar Lochmaier/ab