Kernel-Lecks in Betriebssystemen hebeln Sicherheitsfunktionen aus

Oliver Weiss 28/01/2008

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Der Cirosec-Berater Tobias Klein hat auf der aktuellen Sicherheitskonferenz "IT-Defense" des Unternehmens in Hamburg bislang unveröffentlichte Kernel-Schwachstellen in verschiedenen Betriebssystemen vorgestellt. Am Beispiel von Mac OS X, Sun Solaris und verschiedenen Treibern unter Windows Vista zeigte Klein, welche Auswirkungen Sicherheitslücken in Treibern oder im Kernel selbst haben können. Demnach lassen sich die Lecks zur Erweiterung der lokalen Rechte missbrauchen, aber auch ausnutzen, um Rootkits in den Kernel einzuschleusen und sämtliche im Kern des Betriebssystems implementierte Sicherheitsmechanismen – etwa das mit Solaris 10 eingeführte Zonenkonzept oder die erzwungene Treiber-Signierung unter 64-Bit-Vista – vollständig außer Kraft setzen. Einige der 2007 entdeckten Schwachstellen sind laut Klein noch immer nicht behoben, während das Beheben anderer Lücken bis zu acht Monaten gedauert haben soll.

Nach Meinung des Security-Experten wird die Suche nach Verwundbarkeiten in Betriebssystem-Kernen zunehmend interessanter. "Der Trend wird sich ganz klar in Richtung Kernel-Schwachstellen entwickeln, die entweder direkt Remote ausgenutzt werden können oder mit konventionellen Schwachstellen kombiniert werden."

Die derzeit verfügbaren Sicherheitsmechanismen konzentrierten sich primär auf die Absicherung des User-Bereichs, während Schutzmöglichkeiten auf Seiten des Kernels bislang - wenn überhaupt - nur in sehr rudimentärer Form vorhanden seien. Als in diesem Kontext viel versprechend erachtet Klein Microkernel und Hypervisor-Techniken, die allerdings noch von keinem aktuellen Mainstream-Betriebssystem umgesetzt würden. (cowo)

computerwelt.at 28.01.2008