Schwachstellen auf Kernel-Ebene umgehen sämtliche Sicherheitsfunktionen

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

Betroffen sind u.a. Windows Vista und Sun Solaris

28.01.2008 - Auf der IT-Sicherheits-Konferenz IT-Defense wurden einige bisher unveröffentlichte Schwachstellen auf Kernel-Ebene vorgestellt, mit denen sich sämtliche Sicherheitsfunktionen umgehen lassen. Betroffen sind u.a. Windows Vista und Sun Solaris.

Der cirosec-Berater Tobias Klein stellte in seinem Vortrag auf der IT-Defense neue, bisher unveröffentlichte Kernel-Schwachstellen in verschiedenen Betriebssystemen vor. Er wies darauf hin, dass einige der Schwachstellen, die er im Lauf des Jahres 2007 gefunden hatte, immer noch nicht behoben sind und die Behebung anderer Schwachstellen bis zu 8 Monaten gedauert hat.

Klein demonstrierte am Beispiel von Mac OS X, Sun Solaris sowie diversen Treibern unter Windows Vista, welche Auswirkungen Schwachstellen innerhalb von Treibern oder im Kernel selbst haben können. Neben der Erweiterung der lokalen Rechte nutzte er die Schwachstellen um Rootkits in den Kernel einzuschleusen sowie diverse Sicherheitsmechanismen, wie z.B. das in Solaris 10 eingeführte Zonenkonzept oder die erzwungene Treiber-Signierung unter Vista 64bit, komplett auszuhebeln.

Nach Meinung von Tobias Klein wird die Suche nach Schwachstellen innerhalb von Betriebssystem-Kernen immer interessanter. "Der Trend wird sich ganz klar in Richtung Kernel-Schwachstellen entwickeln, die entweder direkt Remote ausgenutzt werden können oder mit konventionellen Userland-Schwachstellen kombiniert werden", so Klein.

Im Moment konzentrieren sich die verfügbaren Sicherheitsmechanismen auf die Absicherung des Userland-Bereichs, auf Seiten des Kernels gäbe es hingegen nur sehr rudimentäre bis keine Schutzmöglichkeiten. Als vielversprechende Lösungen sieht Klein Microkernel sowie Hypervisor-Technologien. Diese werden jedoch noch von keinem aktuellen Mainstream-Betriebssystem umgesetzt.

Die IT-Defense ist eine jährlich stattfindene IT-Sicherheitskonferenz, auf der sich einige der weltweit bekanntesten IT-Security-Experten, Hacker und Buchautoren treffen, um über aktuelle IT-Sicherheitsthemen zu referieren.

Veranstalter dieses IT-Security-Kongresses ist die **cirosec GmbH**.

all-about-security.de 28.01.2008