ME-Blockade

Linux-Tüftler schalten Intels Management Engine aus

Datenschützer kritisieren die sogenannte Management Engine in allen Systemen mit Intel-Prozessoren. Durch Firmware-Modifikationen lässt sie sich bei vielen Rechnern aushebeln.

Von Christof Windeck

Seit rund zehn Jahren steckt in jedem PC, Notebook, Tablet und Server mit Intel-Prozessor auch eine sogenannte Management Engine (ME). Der italienische Programmierer Nicola Corna hat Python-Skripte entwickelt, die Funktionen der ME-Firmware blockieren.

Weil die ME Zugriff auf sämtliche Daten des Systems hat – etwa RAM, Festplatte, SSD … – und oft den Netzwerkanschluss nutzen kann, zieht sie Kritik auf sich, unter anderem von der Electronic Frontier Foundation (EFF). Mancher vermutet, dass US-Geheimdienste die ME als Hintertür nutzen können. Bisher verweigert Intel vollständige Dokumentation oder Offenlegung der ME-Firmware.

ME-Funktion

Bei der ME handelt es sich um einen eingebetteten Mikrocontroller mit eigener Firmware, der ursprünglich vor allem für die Fernwartung (Remote Management) nützlich war. Stecken bestimmte Intel-Netzwerkchips im System, kann die ME darüber unabhängig vom Betriebssystem Daten übertragen. Mittlerweile erfüllt die ME viele weitere Aufgaben, ohne die Intel-Systeme nicht einmal mehr starten.

Die von Intel signierte ME-Firmware liegt gemeinsam mit dem Code des (UEFI-)BIOS in einem SPI-Flash-Chip; sie kann Bestandteil von BIOS-Updates sein. Teile der ME-Firmware sind Huffman-kodiert, wobei das zugehörige Code-Wörterbuch an die Hardware gebunden ist. Dadurch lässt sich die ME-Firmware nur schwer analysieren. Experten haben trotzdem mehrere modulare Funktionsblöcke der ME-Firmware identifiziert (siehe c't-Link unten). Diese Vorarbeit nutzt Nicola Corna: Seine Skripte entfernen oder überschreiben Teile der ME-Firmware und sorgen dafür, dass die ME den restlichen Code weiter ausführt. Cornas Skripte funktionieren nicht bei jedem beliebigen System und derzeit nur mit Prozessoren aus CPU-Generationen vor Skylake.

Die Blockade von ME-Funktionen wirkt sich auf andere Funktionen des Systems aus: etwa auf die DRM-Funktion Protected Audio/Video Path (PAVP), ohne die sich kommerzielle 4K-Streaming-Angebote nicht mehr nutzen lassen.

Es ist leicht, an die ME-Firmware eines Rechners heranzukommen, falls sie in BIOS-Updates steckt, die man von der Webseite des Herstellers herunterladen kann. Deutlich schwieriger ist es, das gepatchte BIOS-Image in den Flash-Chip zu schreiben: Manche BIOS-Update-Tools von Mainboard- und PC-Herstellern prüfen die Integrität von BIOS-Images, bevor sie sie in den Flash-Chip schreiben – und das scheitert, wenn das jeweilige Image verändert wurde. Dann braucht man Hardware-Programmieradapter, die man direkt an den SPI-Flash-Chip des aufgeschraubten Rechners anschließen muss. Auch wenn Geräte mit der veränderten Firmware nicht mehr booten, braucht man zur Reparatur Programmieradapter.

Corna erläutert auf seiner Github-Seite, dass es keine Garantie dafür geben kann, dass die Firmware-Manipulation sämtliche unerwünschten Funktionen der ME sicher abschaltet. Ohnehin enthalten viele andere PC-Komponenten Firmware mit nicht dokumentiertem Funktionsumfang, die der ME-Patch nicht beeinflussen kann, etwa Festplatten, SSDs und Grafikkarten. Das grundsätzliche Problem, dass in modernen PCs proprietäre Firmware mit unbekannten Funktionen läuft, würde also selbst ein von Intel offengelegter ME-Code derzeit nicht lösen. *(ciw@ct.de)* c't

ME-Informationen und -Skripte:
ct.de/ydd5

Management Engine im Intel-Chipsatz

Die ME besteht aus Firmware und einem Mikrocontroller, der in jedem aktuellen Intel-Chipsatz eingebettet ist.