Wer, wie, was?

Was die Begriffe Firmware, BIOS, UEFI alles meinen können

Schnell redet man aneinander vorbei, wenn man sich über Mainboard-Firmware und deren Interaktion mit Betriebssystemen austauscht. Mit etwas Grundwissen kann man aber aus dem Kontext ableiten, wofür Begriffe wie BIOS, Firmware oder UEFI im Einzelfall stehen.

Von Thorsten Leemhuis

Es gibt immer mal wieder Zank in den Redaktionsräumen um die passende Verwendung der Bezeichnungen BIOS, Firmware und UEFI; Gleiches gilt für Begriffe wie BIOS-Setup, Legacy-BIOS sowie BIOS- und UEFI-Boot. Auch Leser fragen hin und wieder, was für was steht. Kein Wunder, denn was gemeint ist, hängt häufig von Autor und Kontext ab.

Dabei ist es im Kurzen eigentlich recht einfach: Firmware und BIOS (und oft auch UEFI) meinen das Gleiche, sofern es um die Software geht, mit der ein PC, genauer dessen Hauptplatine (das Mainboard) beim Einschalten in Gang kommt. Im Detail wird es aber komplizierter und Grenzen verschwimmen.

Gattungsbezeichnung

Firmware ist streng genommen ein Oberbegriff für Software, die eine Hardware irgendwie antreibt. Die Bezeichnung kann also wenige Kilobyte kleinen und nicht aktualisierbaren Code innerhalb von PCIe-Bridge- oder Audio-Chips eines PCs meinen, der unabhängig von Betriebssystem und Treibern den Baustein initialisiert und im Betrieb involviert ist. Manchmal meint der Begriff aber auch ein mehrere Hundert Megabyte großes und gelegentlich aktualisiertes Bündel sämtlicher Software, die irgendwo in einem Gerät werkelt.

Letzteres ist beispielsweise bei Druckern, NAS-Gehäusen, Routern oder Smart-TVs der Fall, denn bei solchen eingebetteten Systemen (Embedded Systems) gilt das Betriebssystem als Teil der Firmware. Bei Handys war das ähnlich; bei Smartphones meint der Begriff hingegen meist die Software, die unterhalb von Android oder iOS läuft – neben der Firmware für die verschiedenen Smartphone-Komponenten eben auch die Software zum Laden des Betriebssystems.

Bei PCs hingegen gehört der Boot-Loader zum Betriebssystem; in diesem Kontext meint Firmware meist hardwarenahe Software, die viele RAID-Controller, Grafikprozessoren, TV-Empfänger, LAN- und WLAN-Chips brauchen. Selbst in Prozessoren läuft eine, die **Microcode** heißt.

Unterart

Anwender kommen mit den verschiedenen Firmwares in PCs selten in Kontakt. Nur eine haben sie oft vor der Nase: Die Firmware des Mainboards, die als **BIOS** gilt. Ausgeschrieben steht das für „Basic Input/Output System“, was man mit „Grundlegendes Ein-/Ausgabe-System“ übersetzen kann. Letztlich ist diese Firmware ein Mini-Betriebssystem, das Mainboard und alle damit verbundene Hardware in Betrieb nimmt, um den Boot-Code eines mächtigeren Betriebssystems von irgendwoher in den Arbeitsspeicher laden und starten zu können.

Bis ungefähr 2008 wurden BIOSe ähnlich umständlich und antiquiert programmiert wie vor über dreißig Jahren bei den ersten PCs; aus der Zeit stammten auch viele der Mechanismen und Schnittstellen, mit denen solche BIOSe ein Betriebssystem starten und danach interagieren.

Zahlreiche Unternehmen wünschten sich etwas Moderneres und haben **UEFI** geschaffen. Das Kürzel steht für „Unified Extensible Firmware Interface“, was sich mit „einheitliche erweiterbare Firmware-Schnittstelle“ übersetzen lässt. Die UEFI-Spezifikation dreht sich allerdings weniger um die Art, wie eine Firmware programmiert wird, sondern vor allem um die Interaktion zwischen Mainboard-Firmware und Betriebssystem.

Eine den UEFI-Standard implementierende Mainboard-Firmware ist daher letztlich auch nur ein BIOS. Gemeinhin wurde UEFI bei der Einführung aber als „BIOS-Nachfolger“ klassifiziert. Zur Unterscheidung von einem klassischen BIOS (mittlerweile oft **Legacy BIOS** genannt) entstanden daher die Bezeichnungen **UEFI-Firmware** und **UEFI-BIOS**. Diese werden manchmal zu „UEFI“ verkürzt – das ist eher unpassend, schließlich steht der Begriff nicht für die Firmware, sondern für das Interface dorthin, das diesen Namen trägt.

Letztlich ist „BIOS“ daher die treffendste Bezeichnung für die Mainboard-Firmware, egal, wie sie programmiert wurde.

Einstellen

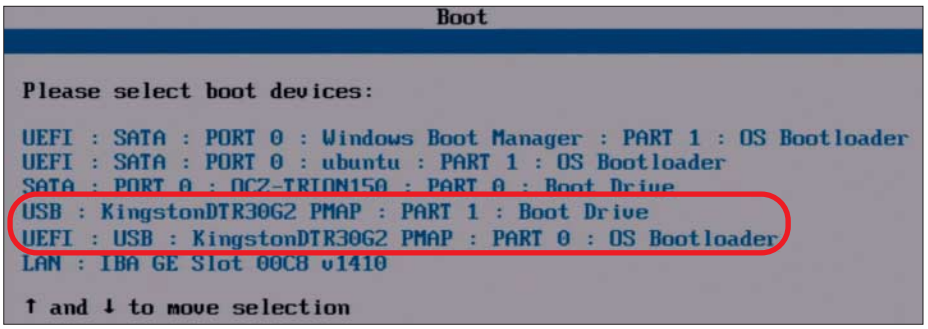
Der Begriff BIOS wird im Sprachgebrauch häufig auch verwendet, wenn in Wirklichkeit das **BIOS-Setup** gemeint ist. Diese Bezeichnung meint die in (Legacy- und UEFI-)BIOSen enthaltene Konfigurationssoftware, die Grundeinstellungen ermöglicht, die das Verhalten von Hardware und BIOS beeinflussen. Dort kann man etwa das Boot-Medium festlegen, Prozessorfunktionen ein- und ausschalten oder den Arbeitsspeicher konfigurieren.

Wie das BIOS programmiert wurde, ist im Alltag meist belanglos – daher vermeidet man Verwirrung, wenn man die Konfigurationssoftware eines BIOS immer BIOS-Setup und nicht UEFI-Setup nennt. Das Setup liefert aber meist ein starkes Indiz, wie ein BIOS programmiert wurde: BIOS-Setups mit grafischer, per Maus bedienbarer Oberfläche und anderem Klimbim deuten meist auf eine UEFI-BIOS hin; derlei war mit klassischen BIOSen selten, weil es deutlich schwerer zu programmieren war.

Auch einige andere Firmware enthält Setup-Programme. Sie sind beispielsweise bei RAID-Controllern üblich. Durch sie kann man etwa einen Datenträgerverbund unabhängig von Betriebssystemen anlegen, damit man diese dann direkt auf den Verbund installieren kann.

Solche RAID-Firmware gilt auch als „Option ROM“ oder „RAID-BIOS“, weil

das Mainboard-BIOS sie bereits während der Grundinitialisierung des Mainboards anspringt und dann zeigt; diese Firmware interagiert auch danach noch mit dem Mainboard-BIOS, insbesondere beim Booten. Ähnlich verhält es sich auch mit der Basisfirmware von Grafikchips: Mit ihr initialisiert die Mainboard-Firmware die Grafikhardware so weit, dass sie Statusmeldungen, BIOS-Setup oder Boot-Manager auf dem Bildschirm anzeigen kann. Da es hier aber nichts einzustellen gibt, bietet diese auch Grafik- oder Video-BIOS genannte Firmware kein Setup-Programm.



Bei aktivem CSM entscheidet die Wahl im BIOS-Boot-Menü, ob das BIOS einen Datenträger klassisch oder über UEFI-Mechanismen zu starten versucht.

Zweitbedeutung

Als wäre das nicht schon kompliziert genug, meinen die Begriffe BIOS und UEFI manchmal auch die Mechanismen, mit denen die Mainboard-Firmware ein Betriebssystem startet und danach interagiert. Das Problem: Von der Programmierung eines BIOS kann man nicht ableiten, welches Verfahren die Mainboard-Firmware beherrscht. Ab 2008 nutzten nämlich manche Mainboards bereits UEFI-BIOSe, die allerdings wie klassische BIOSe aussehen und Betriebssysteme auch nur klassisch starten können; das wird auch **Legacy-BIOS-Modus** genannt, was manchmal zum mehrdeutigen „BIOS-Modus“ verkürzt wird. Nur manche dieser ersten UEFI-BIOSe beherrschten auch den Betriebssystemstart mit UEFI-Mechanismen (**UEFI-Modus**).

Das änderte sich schlagartig mit der Einführung von Windows 8 im Herbst 2012: Bei PCs großer Hersteller wurde der Betriebssystemstart mit UEFI-Mechanismen über Nacht zum Normalfall, weil Microsofts Logo-Richtlinien das forderten. Oft war daher auch **Secure Boot** aktiv – eine optionale UEFI-Funktion, durch die ein UEFI-BIOS nur noch Betriebssysteme startet, die es durch verifizierbare Signaturen am Boot-Code als vertrauenswürdig einstuft.

Aus Kompatibilitätsgründen können diese UEFI-BIOSe ein Betriebssystem auch klassisch starten. Dazu muss man zuerst Secure Boot ausschalten; danach kann man dann das **Compatibility Support Module (CSM)** aktivieren, das die Funktionen eines Legacy-BIOS emuliert, die klassisches Option-ROM sowie den klassischen Start von Betriebssystemen und die Interaktion damit ermöglichen.

Achtung: Wenn man das CSM aktiviert, entscheidet sich oft erst implizit durch Boot-Reihenfolge oder Auswahl im Boot-Menü des BIOS (auch **BIOS Boot Select/BBS** genannt), wie das BIOS ein Betriebssystem zu starten versucht. Wenn man den Start über UEFI-Mechanismen nicht im BIOS-Setup deaktiviert, tauchen Datenträger daher oft zweimal in diesen Listen auf: einmal zum klassischen Start, einmal zum Boot via UEFI; meist ist das Boot-Verfahren an einem Prefix wie „CSM“, „BIOS“ oder „UEFI“ zu erkennen.

Langsam mehren sich BIOSe, die kein CSM mehr mitbringen und Betriebssysteme nur noch über UEFI-Mechanismen starten können. Das sind die ersten Vorboten vom Ende des klassischen Startverfahrens, denn Intel drängt die Hardwarehersteller dazu, ab 2020 kein CSM mehr einzubauen.

Lage

Übrigens: Firmware von Komponenten, die beim Booten (und damit vor dem Start eines Betriebssystems) gebraucht wird, steckt typischerweise auf einem nichtflüchtigen Speicherchip; sie wird meist geladen, sobald Strom anliegt. Bei Scannern oder TV-Empfängern hingegen lädt ein Treiber die Firmware meist aus einer Datei in die Hardware, wenn das Betriebssystem die Komponente initialisiert. Bei Grafikkarten und WLAN-Chips findet sich manchmal eine Mischform: Eine simple Firmware steckt in der Hardware, eine leistungsfähigere lädt der Treiber später nach.

Vom Treiber hochgeladene Firmware können die Hersteller über Betriebssystem- oder Treiber-Update leicht aktualisieren. So ein Update ist risikolos, schließlich landet die Firmware dabei typischerweise in einem flüchtigen Speicherbereich. Daher ist es kein Problem, wenn beim Einspielen etwas schiefgeht: Man muss nur den Chip oder notfalls den ganzen PC neu starten, um es erneut probieren zu können.

Bei einem Mainboard-BIOS und anderer Firmware, die in nicht-flüchtigem Speicher liegt, erfolgt das Update hingegen mit einem Flash-Programm – die gibt es nicht nur für Windows, sondern sind auch in manchen BIOSen enthalten und über das BIOS-Setup erreichbar. Sofern die Hardware keine Fallback-Maßnahmen hat, sollte beim „Flashen“ kein Stromausfall oder Absturz passieren; wenn doch, steckt womöglich eine unvollständig aktualisierte Firmware im Speicherchip, die das System nicht mehr in Gang bringt.

Apropos BIOS-Update: Dieser Tage wird dabei nicht nur das BIOS des Mainboards aktualisiert, sondern auch einige andere Firmwares – etwa die für den Netzwerkchip, für die Management Engine (MEI), den Thunderbolt-Controller oder eine Handvoll anderer Bauteile des Mainboards.

BIOS-Updates bringen auch den Microcode für den Prozessor mit, der bei jedem Systemstart in den flüchtigen Speicher des Prozessors geladen wird. Auch Windows und Linux können neue CPU-Firmware beim Booten hochschieben. Intel & Co. nutzen beide Wege zum Verteilen von Microcode, der neue Funktionen nachrüstet oder Fehler beseitigt – so etwa 2018, als es galt, Prozessor-Sicherheitslücken wie Spectre und Meltdown zu stopfen. Das zeigt, wie tief Firmware in modernen PCs verankert ist und welche Macht sie besitzt. Die Prozessorhersteller konnten dadurch letztlich einen Austausch betroffener CPUs vermeiden, wie er Mitte der Neunzigerjahre erforderlich war, um den FDIV-Bug falsch rechnender Pentium-Prozessoren zu beheben.

(thl@ct.de) c't