BIOS vs. EFI

Benjamin Molzberger IAV-1

Per Knopfdruck fährt unser Computer hoch. Doch wie geschieht dies wirklich?
Seit nun mehr 25 Jahren erweckt das BIOS unseren Computer zum Leben, es initialisiert die Hardware und startet das Betriebssystem. Seit 2008 soll das BIOS einen Nachfolger bekommen. Sein Name lautet: Extensible Firmware Interface, kurz EFI.
Was wird sich für den User ändern? Ist es nur eine Weiterentwicklung oder doch eine kleine Revolution?

Doch sehen wir uns erst einmal die Eigenschaften an von BIOS und EFI an.

BIOS:

BIOS heißt ausgeschrieben Basic Input/Output System, auf Deutsch: Basis-Eingangs-Ausgangs-System. So bezeichnet man die Firmware bei x86-PCs.
Vor dem Start des Betriebssystems initialisiert es die Hardware. Im eigentlichen Sinn arbeitet das Bios immer noch auf der Basis von 1981. Wir finden es in einem nichtflüchtigen Speicher auf der Hauptplatine eines PC und es wird unmittelbar nach dem Einschalten zum leben erweckt.

Die Hauptaufgabe besteht darin die Hardware-Komponenten beim Betriebssystem anzumelden. Seit fast mehr als 30-Jahren wird es nur mehr modifiziert und an die jeweilige Hardware angepasst. Dies hat den negativen Effekt das jeder BIOS Hersteller in nicht standardisierter Form seine Lösungen kreiert und somit auch die abenteuerlichsten Einstell-Optionen entstehen.

Bedeutung & Aufgaben

Ein alt bekanntes Problem ist das sogenannte „Bootstrapping“. Das Problem besteht darin das die Software auf einem Datenträger gespeichert ist und diese in den Hauptspeicher des PC eingelesen werden muss. Doch zum Einlesen braucht der CPU wiederum Software. Früher ist der Rechner grundsätzlich in den Pausemodus versetzten worden. Bevor gestartet wurde, musste manuell oder mit spezieller Peripherie eine minimal Software (Bootloader, Urloader oder Ladeprogramm genannt) in den Hauptspeicher laden. Meist war die Neueingabe des

Bootloader gar nicht nötig da in den 60er und frühen 70er ein Kernspeicher benutzt wurde, der seinen Inhalt beim Ausschalten nicht verlor (sogenannter Persistenzspeicher) und somit das Programm im Hauptspeicher neu startete oder sogar fortsetzte.
Bei heutigen Rechnern ist das BIOS in einem EPROM abgelegt, bei neueren ein Flash-Speicher, wo der Speicherinhalt auch ohne Netzanschluss erhalten bleibt. Somit ist die Firmware auch für portable Geräte geeignet, da nicht zwingend eine Energieversorgung benötigt wird. Somit ist eine Eingabe des Ladeprogramms unnötig.

Ein etwas anderer Konflikt ist die unterschiedliche Hardware, die jeweils eine spezielle Treibersoftware (zur Ansteuerung) für die jeweilige Konfiguration braucht. Damals musste jede Software speziell für den Rechnertyp geschrieben werden. Mit der Auslagerung der Ansteurungssoftware in den Rechnern, ist es nun möglich, das gleiche Betriebssystem auf unterschiedlichen Rechner laufen zu lassen. So bekam das BIOS die Aufgabe als Hardware Abstraction Layer (HAL) zu agieren. Moderne Betriebssysteme haben aus Performance-Gründen und zwecks höherer Flexibilität einen Rücklauf zur eigenen Treibersoftware für die Hardware. Dadurch wird das BIOS wieder allein zur Bootphase verwendet.

Welches BIOS auf dem Rechner ist, geben die jeweiligen Hersteller vor. Nachdem das BIOS vor allen anderen Programmsystemen gestartet ist führt es Reihe von Abarbeitungen durch:

-Power On Self-Test (POST)
-Initialisierung der Hardware
-Prüfung der Funktionsfähigkeit der CPU (bei Multiprozessor-Systemen: der ersten CPU)
-Überprüfung der CPU-nahen Bausteine
-Test des CMOS-RAM (Prüfsummen-Bildung)
-Check des CPU-nahen Cache-Speichers
-Überprüfung der ersten 64 Kilobyte des Arbeitsspeichers
-Prüfung des Grafik-Speichers und der Grafik-Ausgabe-Hardware
-Test des restlichen Arbeitsspeichers - dies kann bei manchen BIOS durch Tastendruck übersprungen werden
-Aufforderung zur Eingabe eines BIOS-Passworts (falls konfiguriert)
-Aufforderung zur Eingabe eines Festplatten-Passworts (falls konfiguriert)
-Darstellung eines Startbildschirms
-Möglichkeit ein BIOS-Konfigurationsmenü („BIOS-Setup“) aufzurufen
-Aufrufen von BIOS-Erweiterungen, die auf Steckkarten untergebracht sind, z. B.:

o Grafikkarten
o Netzwerkkarten
o SCSI-Karten
o RAID-Karten

-Feststellen, von welchem Datenträger gebootet werden kann und soll
-Laden des Software-Bootloader von diesem Datenträger

Die Einstellungen im BIOS kann man im gewissen Rahmen ändern und bleiben bis zur nächsten Änderung gespeichert. Dies ist während Startvorgang möglich.

Bootloader

Der Master Boot Record befindet sich im ersten Sektor der ersten Spur (Zylinder mit der Kopfnummer 0) des MBR. Im Bootsektor befindet sich das Programm der aktiven Partition, (es gibt nur eine) diese wird in den Speicher geladen und ausgeführt. Somit wird das Betriebssystem geladen und gestartet. Der Bootvorgang ist damit abgeschlossen und der Bootloader übernimmt die Kontrolle über den Rechner.
Auf dem aktiven Datenträger wird das gespeicherte Betriebssystem geladen oder es wird ein Menü zur Auswahl eines Betriebssystems angezeigt (Bootmanager). Hat das Betriebssystem die Kontrolle übernommen wird die Kommunikation mit diverser Hardware vorgenommen wie z.B.:

- Tastatur
- serielle und parallele Schnittstellen
- Systemlautsprecher
- Grafikkarte (nur Textdarstellung)
- Diskettenlaufwerke
- Festplatten

Treiberbasierten Betriebssysteme (Linux oder MS Windows) nutzen die BIOS-Dienste nicht, sie laden für jede Hardware einen eigenen Treiber. Am Anfang des Startvorgangs müssen sie trotzdem kurz auf die BIOS-Funktionen zur Ansteuerung der Festplatten zurückgreifen, um den entsprechenden Festplattentreiber zu laden.

Wo wird gespeichert

Der ROM(Read-Only-Memory) wird individuell an jedes Grundgerät angepasst. Ein ROM ist ein nicht flüchtiger Speicher der die Daten auch ohne Stromzufuhr erhält.
Flash-EEPROM oder als Kurzform Flash-Speicher, sind digitale Speicherchips, die eine persistente Speicherung garantieren. Die Art Speicher ist miniaturisiert, doch statt wie bei „gewöhnlichem“ EEPROM-Speicher (neu Flash-EEPROM) lassen sich die kleinsten adressierbaren Speichereinheiten, nicht einzeln löschen.
Sie werden dort verwendet wo Informationen persistent (nichtflüchtig) auf kleinstem Raum gespeichert werden muss. EPROM (Erasable Programmable Read-Only-Memory, wörtlich: Löschbarer, programmierbarer Nur-Lese- Speicher) sind nichtflüchtige, elektronische Speicherbausteine, die Hauptsächlich in der Computertechnik eingesetzt werden.

Sicherheit

Als Vorbeugung eines unberechtigten Zugriffs kann im BIOS-Setup eine Passwortabfrage zum Start des Rechners eingestellt werden. Leider ist dies nur eine marginale Sicherung da man über die Einstellungen bei dem physischem Zugang zum Computer leicht mit einer Manipulation die Hauptplatine aushebeln kann. Diese Sicherung ist zudem nur für das BIOS auf der entsprechenden Hauptplatine, auf der sich das ROM befindet. Tauscht man diese aus oder baut die Festplatte in ein anderen PC, sollte man problemlos auf alle Daten zugreifen können. Wirkungsvoller wäre die physische Sicherung mittels Schlösser oder Ähnlichem. Manche Hersteller haben ein festgelegtes (Recovery-, Master- oder Supervisor-)Passwort um bei Verlust des Passworts den Zugang zurück zu setzten.

Fehlerbestimmung

Die älteste und simpelste Form der Fehlererkennung ist der beepcode. Diese werden ab der ersten BIOS Version bis hin zur aktuellsten verwendet. Teils wurden Fehlermeldungen durch grafische Korrekturmaßnahmen ersetzt, was sich als Problem entpuppte wenn bei Grafikproblemen nichts mehr dargestellt werden kann.
Um die beep-codes Wiederzugeben sollte das Netzteil, Motherboard, Prozessor und der Signalgeber diese Anwendung unterstützen, da das BIOS allein keine Geräusche beherrscht. Kein Grund zur Panik ist, wenn es beim Booten ein einzigen, kurzen Piepton gibt. Dies ist nur das Ende des POST-Vorgangs. Um die Codes auszulesen muss der Hersteller des BIOS bekannt sein bei denen man auch die passende Tabelle findet um den Fehler dann zu bestimmen.
Neuere Boards bieten teilweise eine zweistellige Anzeige von Buchstaben oder Zahlen die die entsprechenden Fehler zeigt.

Update

Ist das Update wirklich nötig?
Nur wenn es wirklich nötig ist und man das nötige Know-How hat sollte man dies wagen. Ein Update ist aufgrund von Fehlern oder Problemen zu machen. Leider kann dieses sehr leicht schief gehen weil z.B. Daten fehlen etc.. Wenn man das Update begonnen hat, kann man es nicht mehr aufhalten. Ein unterbrochenes oder nicht beendetes Update kann den PC dauerhaft lahmlegen bzw. zerstören.

Freie BIOS-Alternativen

Bei den Implementierungen von BIOS handelt es sich in der Regel um proprietäre (d. h. nicht freie) Software. Z.B. Microsoft lässt es nicht zu, das die Xbox mit andere Software gestartet wird.
Sicherheitslücken bringen große Unsicherheiten mit sich da meist der Quellcode nicht offen gelegt wird und somit Fehler oft spät erkannt werden. Durch ersetzen bzw. überschreiben des Flash-ROM-Bausteins besteht die Möglichkeit z.B. den Linux-Kernel direkt zu starten. Dieses hängt aber von der Hauptplatine ab und wird meistens nur in der Computerindustrie verwendet.
Coreboot (ehemals Linux BIOS) und Open BIOS haben sich diese Dinge als Ziel gesetzt.

BIOS-Hersteller

Hier ein kleiner Überblick über ein paar Herstellern von BIOS:

- American Megatrends
- Phoenix/Award – Award und Phoenix sind fusioniert. Award hat sich auf Desktop-Produkte spezialisiert und Phoenix auf die Produkte von Servern und Laptops.
- MR BIOS
- ATI Technologies
- IBM
- Insyde H2O BIOS

EFI:

Extensible Firmware Interface kurz EFI heißt auf Deutsch: Erweiterbare Firmware-Schnittstelle.
EFI ist unterhalb des Betriebssystems verpflanzt und dient somit als zentrale Schnittstelle zwischen der Firmware und den Computer-Komponenten plus dessen Betriebssystems.
Es nimmt sehr deutlich die 64-Bit-Systeme ins Visier und soll das BIOS als Nachfolger ablösen.
Anwendung findet es teilweise schon auf Intels IA-64-Server-Architekuren. Geplant war die Einführung zu Windows Vista, das konventionelle PC auf x86 Technologie laufen lässt. Vorab gab Microsoft die Meldung heraus das Vista, EFI erst später auf der 64-bit-Variante unterstützt wird, was jedoch nie wirklich geschah.
Marktvorstoßend kam Apple mit dem iMac der vierten Generation auf den Markt und startet mit der ersten x86-Architektur die Einführung des EFIs. Es ermöglicht, dass sogar Windows auf den OS-X-Rechnern startet.,

Ziel

Es sollen mehrere Schwerpunkte gelöst werden.
Zum ersten soll die Bedienoberfläche einfacher als beim BIOS werden.
Der Flickschusterei bei BIOS soll Einhalt geboten werden und klare Richtlinien plus neue Funktionen sollen dazu kommen.
EFI stellt ein Embedded-System dar, was hochauflösende Grafikkarten unterstützt. Dank seiner Netzwerkfähigkeit kann man per Remote-Verbindungen Fehler diagnostizieren und beheben. Der User kann zusätzlich beim Systemstart wählen welche Teile des gewünschten Betriebssystems geladen werden sollen.

Geschichte

Intel war mit seiner Initiative ausschlaggebend für die Entwicklung von EFI, die einen Nachfolger für die IA64-Architektur finden mussten. 1998 gründete man die Intel Boot Initiative (IBI) die dann die Idee spezifizierte. Als eigentlicher Nachfolger wird der Firmware Foundation Code gesehen, der zu den Bedingungen der CPL (Common Public License) freigeben wird und das EFI implementiert. Das Standard BIOS nimmt ausschließlich den Real Mode her.

Unified EFI (UEFI)

Bereits 2005 wurde zu werbezwecken bzw. auch zur Weiterentwicklung von EFI das Unified EFI Forum gegründet. Außer Intel sind AMD, Microsoft, Apple und anderen PC- und BIOS-Herstellern beteiligt, damit UEFI nicht alleinig von Intel bestimmt wird. Im Januar 2006 gab man die EFI-Version 2.0 heraus.

Alternativen

Als Alternative gibt es die Firmware "coreboot" (ehemals Linux BIOS) die der GPL-Lizenz angehört. coreboot stellt das Minimalsystem dar, hier wird die Initialisierung der Hardware soweit vollzogen das ein anderes Programm (Payload) aufgerufen wird, wie z.B. Linux-Kernel, Bootloader (GRUB), Open Firmware oder andere. Technische Vorteile, von Intels Eigenentwicklung EFI, gegenüber Open Firmware sind nicht bekannt.

Techniken und Möglichkeiten

Im Vordergrund steht ganz klar die Beseitigung der Nachteile des BIOS.

EFI deckt zudem neue Spezifikationen auf wie etwa:

- Einfache Erweiterbarkeit (z. B. für Digital Rights Management)
- Eingebettetes Netzwerkmodul (zur Fernwartung)
- Preboot Execution Environment (universelles Netzwerkbootsystem)
- Unterstützung hochauflösender Grafikkarten schon ab Start des Computers
- BIOS-Emulation (Kompatibilität zu vorhandenem BIOS) durch „Compatibility Support Module“ (CSM)
- eine Shell, mit der man beispielsweise EFI-Applikationen (*.efi) aufruft
- Treiber können als Modul in das EFI integriert werden, müssen nicht mehr vom Betriebssystem geladen werden, was systemunabhängige Treiber wie bei Open Firmware ermöglicht
- betrieb im Sandbox-Modus lässt die Netzwerk- und Speicherverwaltung auf der Firmware laufen anstatt auf dem Betriebssystem
- Startauswahlmöglichkeit für installierte Betriebssysteme auf dem System, somit sind (den Betriebssystemen vorgeschaltete) Boot-Loader überflüssig

Die GUID Partition Table ist ein flexibler Nachfolger für den Master Boot Record der auf Partitionstabellen basiert. Der MBR hat nämlich ein erhebliches Manko: Festplatten-Partitionen jenseits der 2 Terabyte erkennt er nicht mehr, Speicherkapazitäten, die in den

Rechnern bald Standard sind. Doch mittels der 64-Bit-Technik, sind Größen bis 8.192 Exabyte möglich. Das sind 8 Milliarden Terabyte, genug für die nächsten Jahre.

BIOS ist noch in Assembler geschrieben, so setzt man beim Nachfolger auf die Programmiersprache C. Ein Grund dafür dürfte sein das Uni-Absolventen in modernen Hochsprachen wie C ausgebildet werden, Assembler hingegen beherrschen immer weniger.

Anstelle des gewohnten blauen Bildschirms, erwartet uns nun eine ansprechende Oberfläche mit Buttons, die sogar per Maus bedient werden kann. EFI ermöglicht dies durch Laden der Standard-Schnittstellen, wie der Maus oder der Grafikkarte. Somit müssen Treiber nicht vom Betriebssystem geladen werden und Hardwarehersteller können systemunabhängige Treiber entwickeln.
Beim Thema Overclocking hat das alte BIOS unerfahrene User davon abgeschreckt, an den sensiblen Einstellungen herumzuspielen. Beim EFI wiederum ist es geradezu einfach, seinen PC zu tackten und somit aber auch komplett gegen die Wand zu fahren. Ein gewisses Risiko das man bei manchen EFI-Herstellern durch Wahl zwischen einem Normal- und einem Experten-Modus vermeiden will.

Sicherheit

Im Vordergrund steht vor allem mehr Sicherheit.
Auf der Hauptplatine ist ein Krypto-Coprozessor – der Fritz-Chip verbaut der asymmetrische Schlüssel erzeugt und damit die gespeicherte Daten verschlüsselt. Mittels einen Hash-Algorithmus wird beim Rechnerstart eine Prüfsumme gebildet, die über die angeschlossene Hardware, BIOS-Version, ID-Betriebssystem sowie alle beim Start geladenen Systemdatei-Informationen enthält und diese überprüft. Prüfsummen werden für jedes gestartete Programm (dies beinhaltet: Versionsnummer, Seriennummer und Lizenz) gebildet. Diese Prüfsummen werden mit der Blacklist die auf Servern des TCPA-Konsortiums abgelegt ist abgeglichen.
Solche Eingriffe werden aber immer mit großer Besorgnis gesehen da es um die Sicherheit des PCs geht. Welche umfassenden Kontrollmöglichkeiten sich noch ergeben, wird die Zukunft zeigen.

Anwendungen für EFI

Sogenannte Pre-Boot-Anwendungen sollen das EFI revolutionieren.
Dies sind kleine Programme die auf einer versteckten Festplatten-Partition sind und wertvolle Dienste leisten sollen.
Welche Art von Anwendungen es gibt, hängt von dem jeweiligen Motherboard-Hersteller ab. AMI bietet nur Systemwerkzeuge an (Diagnosesoftware, übliche BIOS-Einstellungen oder Backup-Lösungen). MSI bietet Tools zum anschauen von Fotos oder Wiedergabe von MP3s ohne das Betriebssystem zu berühren.

Zugegeben ähneln diese Anwendungen sehr die eines Betriebssystems, doch gibt es auch da Grenzen. Komplexe Anwendungen die eine Exchange Server Verbindung benötigen wie in etwa Outlook sind nicht inbegriffen. Einfache POP3-Abrufe dagegen schon.
Alle diese Anwendungen sind auf dem Motherboard implementiert. Selbst einfache Spiele kann man ohne Windows zu starten zocken.
Dessen Sinn oder Unsinn bleibt dahin gestellt.

Markteinführung

Die Einführung stieß zunächst auf großem Widerstand einiger Computer- und BIOS-Hersteller. Durch den Einstieg von Apple scheint sich der Markt langsam in eine andere Richtung zu drehen, da alle neuen Macs auf Intel-Basis ausschließlich EFI verwenden.
MSI hat als erster Hersteller begonnen Mainboards auf EFI umzustellen. Allerdings handelt es sich nicht um eine EFI-Installation sondern um eine Betaversion.
2009 gaben einige Hersteller (u.a. Insyde, Intel und Phoenix) bekannt EFI zu verbauen, als Gründe werden die Kompatibilität und vor allem die verkürzte Ladezeit des Systems angeführt.
Hauptsächlicher Befürworter ist Intel, mit Einschränkungen auch Microsoft, die bereits seit Windows 2000, einige Jahre Praxiserfahrung vorweisen können. Intel setzte seit dem ausliefern des Itanium-Systeme auf EFI womit Apple dank dieser Unterstützung EFI einsetzen kann.

Kritik

EFI sollte mehr Komplexität ins System bringen.
Doch die ersten Kritiken besagen das aus es keine nennenswerte Vorteil bietet.
Zudem soll das BIOS-Problem (das die meiste Hardware zwei unterschiedliche Treiber benötigt) nicht gelöst sein. Ein vollständiges Ersetzen von Open-Source-BIOS wie Open BIOS und Coreboot soll außerdem unmöglich sein. Zwei unterschiedliche Betriebssysteme im Dualmode laufen zu lassen sei ebenso unklar, wenn im sie Grunde dieselben Aufgaben erledigen.
Coreboot wirft EFI ein mögliches Sicherheitsrisiko vor, wenn es etwa in Banken mit dem implementierten Netzwerkstack arbeitet, sei dies eine sicherheitskritische Einsatzumgebung wo Daten unbemerkt geklaut und beliebig verschickt werden können.
Da es aber auch für DRM-Zwecke benutzt werden kann, also als digitales Wasserzeichen um I/O-Datenströme zu überwachen, wäre ein quelloffenes System wie Coreboot bevorzugt.

Quellen:

www.wikipedia.de
www.intel.de
www.bios-info.de
www.supportnet.de
www.gidf.de
www.chip.de
www.heise.de