Computerhardware für Fortgeschrittene

6. aktualisierte Auflage Januar 2024

Klaus Eifert

Der Autor

Autor: Klaus Eifert, geb. 1949 in Sachsen;

- 1967–1973 Studium in Moskau: Dipl.-Ing. für Elektronik, Spezialrichtung Computerentwurf.
- 1973–1990 Arbeit im Forschungsinstitut der Metallurgie. Entwicklung und Einsatz von Großrechnern und spezialisierten PC. Programmierung von Robotertechnik und Einrichten von lokalen Rechnernetzen.
- 1990–2008 eigene Firma „Schulung und Beratung“ sowie Arbeit als Dozent in der Lehrlingsausbildung und Lehrerweiterbildung und im Computerservice.
- Seit 2005 als Autor tätig.

Angaben zu den lieferbaren und geplanten Büchern des Autors, Leseproben sowie Bestellmöglichkeiten finden Sie auf `www.eifert.net`

Impressum

verlag@eifert.net

www.eifert.net

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über `https://portal.dnb.de/opac.htm` abrufbar.

1. Auflage im Mai 2016
1. überarbeitete Auflage im August 2016
2. Auflage im Februar 2018, überarbeitet im Oktober 2018 und Februar 2019
3. Auflage im September 2019, überarbeitet im April 2020, November 2020 und Februar 2021
4. Auflage im Juli 2021, überarbeitet im Dezember 2021 und Mai 2022
5. Auflage im August 2022, überarbeitet im Dezember 2022
6. Auflage im Juli 2023, aktualisiert im Januar 2024

Gestaltung: vision2.media

Druck: Xerox Versant 280 Press.

Bindung: Buchbinderei Mönch, Leipzig

ISBN 978-3-9814657-4-7

Über dieses Buch

Dieses Buch soll Ihnen Mut machen, Ihren Computer zu reparieren, aufzurüsten und die Komponenten eines Computers auszuwählen, den Sie anschließend selbst zusammenschrauben.

Es sind auch Hintergrundinformationen enthalten, damit Sie besser verstehen, wie und warum ein Computer funktioniert. Im Buch finden Sie

- Hintergrundinformationen, die für Anfänger zu kompliziert sind,
- Anleitungen für die Fehlersuche,
- Reich bebilderte Montage- und Demontageanleitungen für den Austausch von Komponenten,
- Empfehlungen, aus welchen Komponenten Sie Ihren individuellen PC zusammenstellen sollten.

Es ist ratsam, aber nicht Bedingung, „Computerhardware für Anfänger“ gelesen zu haben.

Meine erstes Buch, „Computerhardware für Anfänger“, vermittelt grundlegende Hardware-Kenntnisse, die für jeden Benutzer eines Computers ratsam sind, ob der Computer nun ein PC, Notebook, Tablet, Smartphone oder anderes ist. Die meisten Leser des Anfänger-Buches haben ihren PC vermutlich noch nie aufgeschraubt. Dennoch enthält das Anfängerbuch einige Anleitungen, wie man den Arbeitsspeicher aufrüstet, ein defektes DVD-Laufwerk auswechselt, eine Festplatte einbaut und PC oder Notebook reinigt. Das sind einfache Tätigkeiten, dafür braucht man nur wenig handwerkliches Geschick. Die komplizierteren Anleitungen, wie man seinen PC repariert, modernisiert oder einen eigenen PC komplett selbst zusammenschraubt, fanden ebenfalls keinen Eingang in das Anfängerbuch.

Doch aus zahlreichen Zuschriften weiß ich: Auch erfahrenere Computernutzer fanden das Buch hilfreich.

Dies ist mein zweites Buch zur Hardware. Es ist an „Fortgeschrittene“ gerichtet. Ein besseres Wort ist mir nicht eingefallen. Mit „Fortgeschrittene“ meine ich nicht die Spezialisten, die regelmäßig mehrere Fachzeitschriften studieren und denen eine Fehlersuche und Reparatur locker von der Hand geht, sondern „fortgeschritten“ im Sinne von „über mein Anfängerbuch hinausgewachsen“. Das können also auch die „normalen“ Benutzer sein, die sich bisher nicht getraut hatten, ihren PC selbst zu reparieren und aufzurüsten. Die bisher nicht den Mut hatten, für ihren nächsten PC die Teile selbst auszuwählen, um ihn dann selbst zusammenzuschrauben.

Sie haben sich bisher noch nicht getraut, an Ihrem Computer herumzuschrauben? Wenn Sie sich trauen, aus dreißig Teilen nach Anleitung eine Schrankwand zu montieren, schaffen Sie das auch mit einem PC. Wobei ein PC einfacher ist: Er besteht nur aus einem Dutzend Komponenten.

- Reparieren Sie Ihren Computer selbst. In vielen Fällen sollte das gelingen. Vielleicht müssen Sie den PC doch noch in eine Werkstatt bringen (weil Sie keine Ersatzteile im Regal haben). Erklären Sie dem Techniker, welche Fehlerursachen Sie bereits ausgeschlossen haben, dann wird die Reparatur vielleicht billiger und schneller.
- Rüsten Sie den PC mit mehr Arbeitsspeicher oder einer zweiten Festplatte auf. Tauschen Sie eine Magnet-Festplatte gegen eine SSD-Festplatte aus.
- Wählen Sie die Komponenten für Ihren nächsten Computer oder für die Aufrüstung selbst aus. Im Kapitel 7 finden Sie Empfehlungen und Varianten, die von einem „einfachen“ bis zu einem „anspruchsvollen“ PC reichen. Für eine „Super-Spielmaschine“ habe ich allerdings keine genauen Empfehlungen: Was ich empfehlen könnte, wäre veraltet, bevor dieses Buch gedruckt ist.
- Bauen Sie Ihren PC selbst zusammen! Die zweite Hälfte des Buches besteht aus reichlich bebilderten Anleitungen für jede Bauetappe. Es gibt auch spezielle Anleitungen für den Austausch von Festplatte, BIOS-Batterie und Hauptplatine.

Auf meiner Website `eifert.net` unter „Hilfen“ finden Sie ein Fachwortverzeichnis, das umfangreicher ist als das am Ende dieses Buches. Dort gibt es auch Anleitungen, die ausführlicher sind als im Buch oder die im Buch nicht vorkommen.

Inhaltsverzeichnis

1 Rund um die Zentraleinheit

Die vergleichsweise einfacheren Fakten über die Hauptplatine, Chipsatz, Steckplätze und Schnittstellen wurden im Buch „Computerhardware für Anfänger“ ausführlich erklärt. In diesem Kapitel geht es um weniger bekannte Details, die für die überwiegende Zahl der Computernutzer sowohl zu schwierig als auch wenig interessant sind.

Zunächst eine kurze Erläuterung von Fachbegriffen.

BIOS

Als „**B**asic **I**nput **O**utput **S**ystem“, abgekürzt „BIOS“, wird das Programm bezeichnet, mit dem der PC nach dem Einschalten startet, Tests ausführt und das Betriebssystem lädt.

BIOS-ROM

Festwertspeicher, in dem das Startprogramm der Hauptplatine (das BIOS) gespeichert ist. Der BIOS-ROM belegt die Speicheradressen ab $FFFFF_h$ abwärts.

CMOS

Eine Halbleitertechnologie mit äußerst geringem Energiebedarf.

CMOS-RAM

Ein statischer RAM, gefertigt in CMOS-Technologie, zur Speicherung von Datum, Uhrzeit und diversen Einstellungen. Steckt seit den 286er CPUs in jedem PC.

286er

PCs werden nach der Art des verwendeten Prozessors kategorisiert. PCs mit der Intel-CPU 8088 und 8086 aus dem Jahr 1980 werden als PC/XT bezeichnet, Nachfolger waren 1982 die „286er“ CPUs mit dem i80286, es folgten 1985 die „386er“ mit i80386 und 1989 die „486er“ mit i80486-CPU. Die fünfte Generation der x86-CPUs kam 1992 heraus und hieß „Pentium“. Es folgten Pentium MMX, 2, 3, 4, Pentium Duo, Core Duo und Core Quad. Aktuelle Intel-CPUs heißen „Core“ mit dem Zusatz i3, i5, i7 und i9. Ein angehängtes „X“ steht für Spitzenexemplare mit „e**x**tremer“ Leistung.

RTC

Real **T**ime **C**lock: Eine Digitaluhr, die seit dem 286er auf jeder Hauptplatine eingebaut ist. Diese Uhr speichert jede Sekunde die aktuelle Uhrzeit in den ersten 10 Byte des CMOS-RAM, wo sie von jedem Programm abgerufen werden kann. Der RTC-Chip ist in stromsparender CMOS Technologie gefertigt.

BIOS-Batterie

Kleine Batterie, oft als Knopfzelle vom Typ 2032, welche das CMOS-RAM und den RTC versorgt, während der PC ausgeschaltet ist. Hält je nach Nutzung des PCs drei bis 10 Jahre.

BIOS-Setup

Ein Programm, mit dem einige Zustände des PCs abgefragt werden können, z. B. CPU-Temperatur und Lüfterdrehzahl. Zweitens können die im CMOS-RAM gespeicherten Einstellungen abgefragt und verändert werden, z. B. die Boot-Sequenz, die CPU-Maximaltemperatur, bei der ein Alarm erfolgt, die Art der Lüfterregelung (ob temperaturabhängig oder ständig mit voller Drehzahl) und vieles mehr. Das BIOS-Setup-Programm ist im BIOS-ROM gespeichert und wird meist mit der Taste Entf oder F2 aufgerufen.

DMA

Direct **M**emory **A**ccess (Direkter Speicherzugriff): Ein Controller, der Daten zwischen Arbeitsspeicher und Peripherie (vor allem von und zur Festplatte) schneller transportieren kann als es die CPU könnte. Die CPU gibt Quell- und Zieladresse sowie Bytezahl vor und kann sich anderen Berechnungen widmen, bis der DMA-Controller mit einem Interrupt das Ende der Übertragung meldet.

Interrupt

Meldung an die CPU über ein meist zeitkritisches Ereignis (z. B. die Meldung von der Tastatur, dass eine Taste gedrückt wurde), woraufhin die CPU die Abarbeitung einer anderen Befehlsfolge zeitweilig unterbricht, um auf das Ereignis zu reagieren.

1.1 BIOS

1.1.1 Die BIOS-Adressen

Im ersten IBM-PC arbeitete eine i8088-CPU von Intel, die einen Speicher mit 20 Adressbits verwalten konnte. Das begrenzte den Arbeitsspeicher auf 1 MB, genauer: 2^{20} = 1 048 576 Byte. Der adressierbare Speicherbereich reichte von Adresse 0 bis $FFFFF_{Hex}$ (Falls Sie sich mit Hexadezimalzahlen nicht auskennen, lesen Sie den Anhang meines Buches „Software-Grundlagen“ oder den Wikipedia-Artikel „Hexadezimalsystem“). Im Jahr 1981 war 1 MB sehr viel und RAM war unglaublich teuer.

Die PCs wurden wahlweise mit 16 oder 64 kByte RAM ausgeliefert. Bill Gates meinte 1981, „640 kB sollten genug für jedermann sein“. Daher wurden die Adressbereiche oberhalb von 640k recht freizügig vergeben.

Für den Arbeitsspeicher war der Adressbereich ab 0 bis $9FFFF_h$ reserviert (640 kB). Der darauffolgende Speicherbereich von $A0000_h$ bis $AFFFF_h$ ist für das Startprogramm einer Grafikkarte (das BIOS der Grafikkarte) vorgesehen und der darauffolgende Bereich von $B0000_h$ bis $BFFFF_h$ ist für den **B**ild**W**iederhol**S**peicher reserviert, in dem die Bildschirmausgabe zusammengestellt wird. Ab $C0000_h$ ist Platz für „BIOS-Erweiterungen“ und dahinter war Platz für einige Zusatzprogramme, z. B. ein „ROM-BASIC“.

	von	bis
Arbeitsspeicher	0	$9FFFF_h$
Grafik-BIOS	$A0000_h$	AFFFFh
Bildwiederholspeicher	$B0000_h$	$BFFFF_h$
BIOS-Erweiterungen	$C0000_h$	
Haupt-BIOS		$FFFFF_h$
BIOS-Startadresse	$FFFF0_h$	

Tab. 1.1: Speicherbelegung IBM-PC (vereinfacht)

Vom oberen Ende des adressierbaren Speichers abwärts, beginnend ab Adresse $FFFFF_h$ befindet sich das BIOS-Programm. Die CPU ist so entworfen, dass sie nach dem Einschalten auf Adresse $FFFF0_h$ ihren Startbefehl erwartet. Weil an dieser Stelle, 16 Byte vor dem Speicherende, kein Platz für ein Programm ist, befindet sich dort ein Sprungbefehl, der zum eigentlichen BIOS-Start führt.

1.1.2 Power On Self Test

Das erste Programm, welches die CPU nach dem Einschalten ausführt, ist ein Selbsttest, der „**P**ower **O**n **S**elf **T**est“, abgekürzt POST. Was sind die wichtigsten Etappen des POST?

Einige Komponenten der Hauptplatine, wie zum Beispiel die Interrupt-Controller, sind nach dem Einschalten der Betriebsspannung in einem nicht vorhersehbaren Zustand. Darum sperrt die CPU zuerst alle Interrupt-Eingänge, damit der POST ungestört ablaufen kann. Dann werden Reset-Signale und Initialisierungsbefehle an den Chipsatz und andere Komponenten gesendet. Der Tastaturcontroller wird getestet und ein Puffer für die Tastatureingaben wird eingerichtet.

Die CPU berechnet die Kontrollsumme des BIOS-ROM und vergleicht diese mit der gespeicherten Summe. Auch die Kontrollsumme des CMOS-RAM wird überprüft. Stimmt diese nicht, ist häufig die Batterie leer.

Von den ersten 64k des Speichers werden alle Bytes kurz getestet. Der restliche Speicher wird in 64k-Schritten überprüft, um festzustellen, wieviel RAM installiert ist. Der für den Speicher-Refresh zuständige erste DMA-Controller wird programmiert und der Refresh wird getestet.

Nun kann die CPU beginnen, den RAM mit der „Interrupt Vektor Tabelle“ (siehe nächste Seite) zu füllen. Der Typ der Grafikkarte wird ermittelt, der Video-Speicher und Grundfunktionen der Grafikkarte werden getestet. Wenn alles funktioniert, kann das BIOS ab jetzt Meldungen auf dem Bildschirm ausgeben.

Die Tastatur wird getestet, dabei leuchten die LEDs der Tastatur kurz auf.

Das BIOS führt weitere Tests und Initialisierungen durch, um festzustellen, welche Komponenten auf der Hauptplatine verbaut oder angesteckt sind: Gibt es serielle und parallele Schnittstellen und wie viele davon? Gibt es Diskettenlaufwerke, Festplatten oder optische Laufwerke? Die ermittelten Werte werden auf vordefinierten Speicherplätzen abgelegt, die später auch vom Betriebssystem abgefragt werden können.

1.1.3 IO Access

Das BIOS „initialisiert“ Komponenten, schickt Reset-Signale, sperrt Interruptsignale, programmiert den DMA-Controller ... Wie kommuniziert eigentlich die CPU mit den Komponenten des PCs?

Wenn die CPU mit dem Arbeitsspeicher kommunizieren will, legt sie eine Adresse an ihre Adressleitungen und nach einer winzigen Wartezeit fühlt sich eine der Speicherzellen angesprochen und sendet ihre Daten an die CPU oder empfängt Daten von der CPU zum Schreiben.

Die CPU hat ein zweites, wenig bekanntes Adressierungssystem. Wenn die CPU eine Adresse auf ihre Adressleitungen ausgibt und gleichzeitig ein Signal an ihr Pin M/IO gibt, wird von „**M**emory Access“ zu „**IO** Access“ umgeschaltet. Über diesen „**I**nput **O**utput **Access**“ könnte man sogar auf einen weiteren Speicher (RAM oder ROM) zugreifen, und in einigen Spezialsteuerungen wird das so gemacht.

IBM hat bei der Entwicklung ihres ersten PCs entschieden, den IO-Adressbereich für die Ansteuerung einiger hochintegrierter Chips zu nutzen. Für alle klassischen Komponenten ist ein Adressbereich festgelegt. Beispielsweise sendet die CPU Befehle an den ersten PIC (**P**rogrammable **I**nterrupt **C**ontroller), indem sie ein Befehlsbyte an die IO-Adresse 20_h schickt, danach werden Daten an die Adresse 21_h geschickt. Danach holt die CPU von der Adresse 21_h die Antwort des PIC, z. B. die Nummer des letzten Interrupts. Mehr dazu können Sie unter der folgenden Adresse nachlesen: `http://www.lowlevel.eu/wiki/I/O_Ports`

1.1.4 Interrupt Vektor Tabelle

Die Hersteller von Hauptplatinen können wählen, von welcher Firma sie ein BIOS für eine neue Platine anpassen und liefern lassen: AMI, Award, Phoenix und IBM/Lenovo sind die bekanntesten.

Das BIOS enthält und nutzt zahlreiche Unterprogramme (Treiber) für den Zugriff auf Massenspeicher, Tastatur, Grafikkarte und viele andere. Die Startadressen der Treiber sind natürlich in jedem BIOS anders. Die Hersteller von Betriebssystemen benutzen die BIOS-Treiber ebenfalls (ersetzen diese aber nach dem Laden meist durch bessere Treiber). Damit jedes Betriebssystem mit jedem BIOS zusammenarbeiten kann, muss es eine einheitliche Tabelle für die Startadressen der BIOS-Treiber geben. Diese **I**nterrupt **V**ektor **T**able wird vom BIOS ab Adresse 0 im Arbeitsspeicher angelegt.

In der IVT sind für jede Adresse vier Byte vorgesehen. In der Tabelle 1.2 sind einige Interrupts aufgeführt. Der Interrupt 2 ist ein **N**icht-**M**askierbarer **I**nterrupt (der sich im Unterschied zu anderen nicht sperren lässt).

Nr.	Adresse	Ereignis
0	00 - 03	CPU meldet (verbotene) Division durch Null
1	04 - 07	CPU hat Einzelschritt ausgeführt (Debugger-Testmodus)
2	08 - 0B	NMI (Fehler in RAM-Baustein)
3	0C - 0F	CPU hat Breakpoint erreicht (Debugger-Testmodus)
4	10 - 13	CPU meldet numerischen Überlauf
5	14 - 17	Print Screen (Bildschirminhalt ausdrucken)
8	20 - 23	IRQ0: Timer (alle 18,2 Sekunden vom RTC ausgelöst)
9	24 - 27	IRQ1: Tastatur (Taste wurde gedrückt oder losgelassen)
A	28 - 2B	IRQ2: Interrupt an einem der 8 Eingänge des zweiten PIC
B	2C - 2F	IRQ3: Serielle Schnittstelle 2
C	30 - 33	IRQ4: Serielle Schnittstelle 1 (Maus wurde bewegt)
D	34 - 37	IRQ5: Soundkarte
E	38 - 3B	IRQ6: Diskette
F	3C - 3F	IRQ7: Drucker
10	40 - 43	BIOS: Video-Funktionen (Grafikkarte)
20	80 - 83	DOS: Programm beenden
21	84 - 87	DOS: Funktion aufrufen
70	1C0 - 1C3	IRQ08: RTC (Echtzeituhr)
71	1C4 - 1C7	IRQ09: VGA oder Netz
72	1C8 - 1CB	IRQ10: PCI-Bus
73	1CC - 1CF	IRQ11: PCI-Bus oder SCSI
74	1D0 - 1D3	IRQ12: PS/2 Maus
75	1D4 - 1D7	IRQ13: 80287 NMI (Mathematischer Co-Prozessor)
76	1D8 - 1DB	IRQ14: Primärer Festplattencontroller
77	1DC - 1DF	IRQ15: Sekundärer Festplattencontroller

Tab. 1.2: Interrupt Vector Table (einige der ersten von 256 Einträgen)

Dieser Interrupt 2 wird bei einem Speicherparitätsfehler ausgelöst. Die CPU setzt dann das Programm an der Sprungadresse fort, die auf den Speicherplätzen 08 bis $0B_h$ bereitgestellt ist.

Die Interrupts 1 und 3 werden von Programmierern benötigt, um Maschinenspracheprogramme schrittweise testen zu können. Interrupt 5 wird von der Taste „Druck“ ausgelöst. Auf den RAM-Adressen 14h bis 17h steht eine Sprungadresse zu einer Routine, welche den Bildschirminhalt direkt zum Drucker schickt. Windows ersetzt diese Adresse und speichert den Bildschirminhalt in der Zwischenablage. Und wenn Sie ein Screenshot-Tool installieren, ersetzt dieses die auf Windows zeigende Adresse durch eine andere, eigene.

Die zu den acht Unterbrechungsleitungen IRQ0 bis IRQ7 zugehörigen Sprungadressen, die vom ersten Interrupt-Controller überwacht werden, werden vom BIOS auf den Plätzen 20_h bis $3F_h$ bereitgestellt. Seit den 286er CPUs ist ein zweiter Interrupt-Controller mit den IRQ8 bis IRQ15 dazugekommen, deren Adressen ab Interrupt 70_h zu finden sind.

Die **I**nterrupt **V**ektor **T**abelle hat Platz für 256 Adressen von je 4 Byte, ist also 1024 Byte lang. Auf die IVT folgen 256 Byte „BIOS Data Area“. In diesem Speicherbereich hält das BIOS solche Informationen bereit wie Speichergröße, Hardwareausstattung, die Anzahl und Adressen von Schnittstellen und Controllern. Dadurch bleiben von den 640 KByte des konventionellen Speichers noch knapp 639 KB übrig.

Bei alten PCs mit ISA-Karten durften Interrupts nicht doppelt belegt werden, wofür mit dem Setzen von Jumpern auf der Karte gesorgt werden musste. Seit dem PCI-Bus dürfen sich mehrere Geräte einen Interrupt teilen (das wird „IRQ-Sharing“ genannt). Der PCI-Bus sucht sich aus den 15 IRQs vier freie aus, die mit INT_A, INT_B, INT_C und INT_D bezeichnet werden. Die PCI-Spezifikation empfiehlt den Mainboard-Herstellern die nachfolgende Zuordnung zu den Steckplätzen. Haben Sie ein altes PCI-Mainboard?

INT_A	AGP, 1. und 5. PCI-Steckplatz
INT_B	2. und 6. PCI-Steckplatz
INT_C	Onboard-Sound und 3. PCI-Steckplatz
INT_D	Onboard-USB und 4. PCI-Steckplatz

Prüfen Sie im Handbuch, ob Ihr PCI-Mainboard davon abweicht. Versuchen Sie die Steckkarten so auf die Slots zu verteilen, dass jede Karte einen anderen Interrupt bekommt, um Leistungsverluste zu vermeiden.

„**PCI E**xpress“ kommt ohne diese Einschränkungen aus. PCIe arbeitet ohne Unterbrechungsleitungen und verschickt stattdessen Datenpakete, die „Message-Signaled Interrupts“ genannt werden.

1.1.5 Dual-BIOS

Unter dieser Bezeichnung hat der Hersteller Gigabyte eine Sicherheitskopie vom BIOS eingeführt. Andere Hersteller bezeichnen dieses Feature als „Multi-BIOS“ (MSI), „USB BIOS Flashback“ (ASUS) und „BIOS Selection Switch“ (ASRock).

Wenn die Hauptplatine erkennt, dass das erste BIOS defekt ist (z. B. wenn die Kontrollsumme des BIOS-ROM nicht stimmt), wird vom Ersatz-BIOS gebootet. In der Regel kann das defekte BIOS auf den Anfangszustand zurückgesetzt werden, eventuell muss dazu auf dem Mainboard ein Jumper umgesetzt werden.

Nach einem BIOS-Update des primären BIOS bleibt bei einigen Herstellern das Reserve-BIOS unverändert, bei anderen Herstellern kann man das Reserve-BIOS angleichen oder ebenfalls updaten. Es gibt auch die Variante, dass nach 10 erfolgreichen Bootvorgängen oder mit der Tastenkombination Alt-F12 während des Starts das Reserve-BIOS auf den (neuen) Stand des Haupt-BIOS upgedatet wird.

Im Prinzip ist das Dual-BIOS eine tolle Idee und hat schon viele Mainboards gerettet. Bei einem defekten BIOS sollten Sie das Mainboard-Handbuch lesen, um nichts falsch zu machen. Und manchmal geht es trotzdem daneben. Falls das Haupt-BIOS beschädigt ist, muss es zumindest noch seine eigene Kontrollsumme berechnen und entscheiden können, dass ein Wechsel zum Reserve-BIOS nötig ist. Ist auch dieser Programmteil beschädigt, hilft nur noch eine manuelle Umschaltung, falls eine solche vorgesehen ist.

Es gibt auch Grafikkarten mit einem zweiten und mitunter sogar mit einem dritten Grafik-BIOS, zwischen denen man mit einem Jumper oder einer Tastenkombination umschalten kann. So kann man ein Grafik-BIOS für Spiele updaten und modifizieren und das andere Grafik-BIOS mit Standardeinstellungen belassen.

1.2 CMOS

1.2.1 Was ist das „CMOS“?

Seit dem 286er ist das „CMOS-RAM“ Bestandteil jedes PCs. CMOS ist die Abkürzung von **C**omplementary **M**etal **O**xide **S**emiconductor und bezeichnet eine extrem stromsparende Halbleitertechnologie. Wird ein statischer RAM mit dieser Technologie gefertigt, so wird dieser als CMOS-RAM bezeichnet. Das CMOS-RAM nur als CMOS zu bezeichnen, ist also falsch.

Seit dem 286er gibt es in jedem PC einen Uhrenschaltkreis, den MC146818. Dieser RTC (**R**eal **T**ime **C**lock) ist ebenfalls in CMOS Technologie gefertigt und wird ebenso wie das CMOS-RAM von einer Batterie oder einem Miniakku versorgt, während der PC ausgeschaltet ist.

Es war naheliegend, die beiden in CMOS-Technologie gefertigten Schaltkreise zu integrieren. Seit dem 386er stecken CMOS-RAM und RTC im gleichen Chip, manchmal sogar gemeinsam mit einem winzigen Akku.

1.2.2 Was wird im CMOS-RAM gespeichert?

Der CMOS-RAM wird gebraucht, damit der Hersteller des PCs wichtige Informationen über die Hardware speichern kann. Der Anwender kann das BIOS-Setup-Programm benutzen, um die gespeicherten Werte zu lesen und zu verändern. Der CMOS-RAM befindet sich außerhalb des normalen Adress-Bereiches und kann keinen direkt ausführbaren Code enthalten. Der CMOS-RAM-Speicher hat technisch bedingt eine maximale Größe von 128 Bytes. Das nachstehende BASIC-Programm liest die Bytes von 0 bis 127 (hexadezimal: $7F_h$) aus dem CMOS-RAM und zeigt diese am Bildschirm an. Um ein Byte aus dem CMOS-RAM zu lesen, ist es nötig, ein BASIC Kommando OUT an Port 70_h zu senden, mit Angabe der CMOS-Adresse, die gelesen werden soll. Durch ein Kommando INP von Port 71_h erhält man die gewünschten Informationen.

```
10 CLS
20 FOR x = 0 TO &H7F
30 OUT &H70, x
40 PRINT USING "\ \"; HEX$ (INP(&H71));
50 NEXT x
60 PRINT " "
```

Die ersten zehn Byte sind für den Uhrenschaltkreis MC146818 reserviert: Die Werte von Sekunden, Minuten, Stunden, Tag, Monat, Jahr und Wochentag werden vom RTC jede Sekunde aktualisiert. Weitere zehn Byte sind für einen „Alarm“ vorgesehen: Man kann einen Alarmzeitpunkt festlegen, an dem der PC automatisch eingeschaltet werden soll. Die nächsten vier Byte sind für Statusinformationen vorgesehen. Die restlichen 104 Byte sind je nach BIOS-Hersteller sehr unterschiedlich belegt.

1.2.3 Wie kommen die Anfangswerte in den CMOS-RAM?

Die Werte im CMOS-RAM sind mit einer Kontrollsumme geschützt. Der **P**ower **O**n **S**elf **T**est errechnet bei jedem Start die Checksumme und vergleicht sie mit der gespeicherten Checksumme. Wenn durch einen Zufall ein Byte verändert worden ist oder durch eine schwache Batterie der gesamte Speicherinhalt verloren gegangen ist, kopiert das BIOS einen Satz Anfangswerte in den CMOS-RAM. Die Tabelle mit den Anfangswerten, den „Setup Defaults“, wird vom Hersteller der Hauptplatine zusammengestellt und vorsorglich im BIOS-ROM bereitgestellt. In manchem BIOS gibt es noch eine zweite Tabelle „Fail-Safe Defaults“ für Notfälle, z. B. wenn der PC nicht stabil läuft: In dieser Tabelle sind Beschleunigungsfunktionen abgeschaltet und der Speicherzugriff ist verlangsamt. Mit diesen Werten kann der PC eventuell „wiederbelebt“ werden.

Falls sich das BIOS-Setup noch starten lässt, können Sie den CMOS-Speicher manuell auf diese Anfangswerte zurücksetzen. Suchen Sie dazu im BIOS-Menü nach „Exit Options“ o. Ä.

1.2.4 CMOS-RAM löschen

Das Löschen bzw. Zurücksetzen aller Werte ist beispielsweise nötig, wenn Sie das BIOS-Setup-Passwort vergessen haben. Es kann auch nötig werden, wenn nach Übertaktungs-Experimenten der PC nicht mehr bootet. Wenn Sie Glück haben, wird das Problem vom BIOS erkannt und das BIOS stellt nach fünf erfolglosen Startversuchen die Standardeinstellungen wieder her. Und wenn nicht?

Dann müssen Sie den PC vom Stromnetz trennen (Stecker ziehen), bei einem Notebook müssen Sie auch den Akku herausnehmen. Schrauben Sie den PC auf und nehmen Sie die BIOS-Batterie heraus, die das CMOS mit Strom versorgt. Warten Sie eine bis zehn Minuten, bis die letzten Kondensatoren des PCs ihre Ladung verloren haben (in einem Extremfall hat es einmal zwei Stunden gedauert, bis alle 128 Byte des CMOS-RAM gelöscht waren). Setzen Sie die CMOS-Batterie wieder ein. Wenn Sie den PC starten, sollte das BIOS beim POST feststellen, dass die CMOS-Checksumme falsch ist und das CMOS-RAM mit den Werten des „Setup Defaults“ füllen. Doch verlassen Sie sich nicht darauf: Starten Sie das BIOS-Setup und setzen Sie alle Werte auf „Setup Defaults“. Stellen Sie anschließend Datum, Uhrzeit, Boot Sequenz und andere wichtige Werte neu ein und speichern Sie die Einstellungen. Nun sollte der PC starten – ohne nach einem BIOS-Passwort zu fragen.

1.3 BIOS-Update

Das BIOS-Programm ist in einem Festwertspeicher dauerhaft gespeichert, weil der PC ohne BIOS nicht starten kann. Als Festwertspeicher wird heute ein Flash-Speicher eingebaut, der mit einer speziellen Methode beschrieben werden kann. Um das BIOS vor Trojanern u. a. Schädlingen zu schützen, gibt es zwei Sicherheitsvorkehrungen:

- Das BIOS ist manchmal mit einem elektronischen Schreibschutz versehen, der über das BIOS-Setup aus- und eingeschaltet werden kann. Bei manchen alten PCs musste ein Jumper umgesetzt werden.
- Das Programm zum Durchführen des Updates ist herstellerspezifisch.

1.3.1 Risiken und Nebenwirkungen

Das Programm zum Durchführen eines BIOS-Updates ist ein Teil des BIOS und es benötigt viele der BIOS-Ressourcen, z. B. die USB-Treiber, um den USB-Stick mit dem neuen BIOS-Code lesen zu können. Deshalb wird zu Beginn eines Updates das Update-Programm und der neue BIOS-Code in den Arbeitsspeicher geladen. Dann wird das nunmehr im Arbeitsspeicher befindliche Update-Programm gestartet und beginnt, den BIOS-ROM zu löschen und mit dem neuen Code zu füllen.

Was kann geschehen, wenn Windows während des Updates abstürzt oder einfriert? Wenn ein kurzer Stromausfall eintritt oder wenn der Notebook-Akku leer wird? Das Update-Programm bricht ab mit einem nur teilweise erneuerten BIOS. Dass der PC jemals wieder startet, ist unwahrscheinlich. Sie müssen wahrscheinlich die Hauptplatine verschrotten oder an den Hersteller einschicken (was meist teurer ist als eine neue Platine). Wenn die neue Platine nicht baugleich ist oder zumindest den gleichen Chipsatz besitzt, wird Windows wahrscheinlich nicht mehr starten, und Sie werden Windows neu installieren müssen. Falls Ihre Daten vom Betriebssystem verschlüsselt wurden oder auch nur für die Mitbenutzer des PC gesperrt sind, kommen Sie mit einem neu installierten Windows nicht mehr an Ihre Daten heran. Einem BIOS-Update sollte deshalb immer eine Datensicherung vorausgehen!

Bei einem Notebook sollten Sie generell auf ein BIOS-Update verzichten. Einerseits ist kaum vorstellbar, welchen Sinn ein Update haben sollte. Andererseits ist das Risiko sehr hoch: Falls das Update fehlschlägt, müssen Sie das Notebook vielleicht wegwerfen, denn der Austausch der Hauptplatine ist zu teuer – rechnen Sie mit mindestens 200 Euro.

Auch bei einem erfolgreich durchgeführten Update kann es vorkommen, dass das neue BIOS mit Ihrer Hardware-Konfiguration nicht funktioniert. Deshalb wird in den Anleitungen meist empfohlen, das aktuelle BIOS vor dem Update zu sichern.

1.3.2 Wann ist ein BIOS-Update sinnvoll?

Wegen der genannten Risiken sollten Sie einen guten Grund haben, ein Update durchzuführen.

- Wenn Sie eine ältere CPU durch eine neue ersetzen wollen, läuft eventuell die neue CPU nicht an, wenn das BIOS zu alt ist. In diesem Fall müssen Sie die alte CPU noch einmal einbauen, das Update durchführen und es mit der neuen CPU erneut versuchen.
- Sehr alte Boards erkennen möglicherweise nicht die volle Größe Ihrer neuen Festplatte. Hier könnte ein Update helfen.
- Der Hersteller gibt für jede BIOS-Version an, welche Neuerungen es enthält und welche Fehler damit beseitigt werden. Wenn Sie in der Beschreibung auf die Ursache stoßen, warum sich Ihr PC „komisch“ verhält, ist ein Update sinnvoll.
- Der Hersteller verspricht eine Geschwindigkeitssteigerung? Bestimmt sind es nur wenige Prozent. Eine Geschwindigkeitssteigerung unter 20 % würden Sie im Alltagsbetrieb ohnehin nicht spüren. Überdies ist nur die Geschwindigkeit des BIOS-Startvorgangs gemeint, denn nach dem Start wird das BIOS nicht mehr benutzt.
- Bei manchem BIOS kann man den Startbildschirm ersetzen, z. B. durch ein eigenes Bild. Wer’s mag...

1.3.3 Durchführung eines BIOS-Updates

Manchmal werden zwei Installationsmethoden angeboten: eine DOS-Version und eine Windows-Version. In Erfahrungsberichten wird die DOS-basierte Methode als sicherer eingeschätzt – da kommt Ihnen kein Virus und kein Absturz dazwischen. Mit einem 64-Bit-Windows scheint das Risiko besonders hoch zu sein, dass ein Update fehlschlägt. Für die DOS-Methode müssen Sie eine bootfähige CD oder einen bootfähigen USB-Stick erstellen (können Sie das?) und die für das Update benötigten Dateien daraufkopieren. Doch vielleicht haben Sie Glück: Der Hauptplatine liegt eine Treiber-CD bei. Oft ist diese CD bootfähig und enthält ein Menü, mit dem man ein BIOS-Update herunterladen und installieren kann. Das scheint die am wenigsten riskante Methode zu sein.

- Stellen Sie zweifelsfrei die genaue Bezeichnung des Mainboards fest. Vielleicht ist sie auf der Platine aufgedruckt, oder Sie können sie mit einem Diagnoseprogramm wie „SiSoft Sandra“ ermitteln.
- Finden Sie heraus, welche BIOS-Version die Hauptplatine gegenwärtig benutzt. Das wird in den ersten Sekunden nach dem Einschalten angezeigt.
- Laden Sie das Update von der Website des Herstellers herunter. Wahrscheinlich müssen Sie die Dateien entpacken. Oft ist eine README-Datei mit einer englischen Installationsanleitung enthalten.
- Lesen Sie die Update-Anleitung. Übersetzen Sie diese gegebenenfalls mit dem Google Translator. Machen Sie sich Notizen oder einen Ausdruck.
- Entfernen Sie den BIOS-Schreibschutz, falls einer vorhanden ist. Dazu müssen Sie im „BIOS Features Setup“ die Option „BIOS Update“, „BIOS Flash“ o. Ä. auf „Enabled“ setzen.
- Wenn Sie ein Notebook haben: Schließen Sie es an die Netzspannung an.
- Führen Sie das Update durch. Vergessen Sie nicht zu beten. Und drücken Sie nicht entnervt nach fünf Minuten auf die Reset-Taste, falls das Update etwas länger dauert.
- Sie wollen mit „yes“ antworten und der PC reagiert nicht auf das Drücken der „Y“-Taste? Versuchen Sie es mit der Taste „Z“. Dem BIOS fehlt der deutsche Tastaturtreiber. Bei der US-Tastaturbelegung sind „Y“ und „Z“ vertauscht.
- Updates bringen manchmal neue Funktionen oder verändern vorhandene. Gehen Sie beim ersten Start nach dem Update ins BIOS und wählen Sie „Load Setup Defaults“.
- Stellen Sie gegebenenfalls den abgeschalteten BIOS-Schreibschutz wieder her.
- Testen Sie das neue BIOS gründlich, bevor Sie mit Tuningmaßnahmen anfangen.

1.4 BIOS-SIGNALTÖNE

Nach dem Einschalten des PC wird der „**P**ower **O**n **S**elf **T**est“ (Selbsttest nach dem Einschalten) ausgeführt, um grundlegende Funktionen der CPU und des Mainboards zu überprüfen.

Bild 1.1: Mini-Pieper

Im ersten Teil des POST ist die Ausgabe auf den Bildschirm noch nicht möglich (der Bildwiederholspeicher muss noch getestet und die Grafikkarte initialisiert werden). Deshalb werden eventuelle Fehlermeldungen mit kurzen und langen Pieptönen signalisiert (in der Tabelle mit K und L bezeichnet). Dazu ist meist ein kleiner Pieper („Speaker“) auf dem Mainboard aufgelötet oder beigelegt. Bei älteren Hauptplatinen muss dazu ein im Gehäuse eingebauter einfacher Lautsprecher an den „System Connector“ der Hauptplatine angesteckt werden.

Falls Ihnen das Handbuch zum Mainboard nicht zur Verfügung steht, hilft Ihnen vielleicht eine der folgenden Tabellen.

1K	POST beendet: System arbeitet ohne Fehler
2K	Problem mit Stromversorgung oder Steckkarte sitzt nicht richtig
1L	Fehler der Grafikkarte (sitzt nicht oder Strom reicht nicht)
1L 1K	Fehler der Hauptplatine
1L 2K	Fehler der Grafikkarte oder Onboard-Grafikkarte
1L 3K 1L	Fehler der Grafikkarte (GraKa)
3L	Fehlerhafte Tastatur oder Tastaturcontroller
viele 1K	Probleme mit Netzteil
viele 1L	Problem mit Arbeitsspeicher

Tab. 1.3: Signaltöne des IBM/Lenovo-BIOS

1K	System arbeitet ohne Fehler
1L	Speicherproblem: Module sitzen nicht richtig
Dauerton	Speicher- oder Videoproblem, RAM oder GraKa nicht gefunden
1L 2K	Videoproblem: GraKa defekt oder nicht richtig gesteckt
1L 3K	Tastatur-Controller fehlerhaft

Tab. 1.4: Signaltöne des AWARD-BIOS

1K	Speicherproblem: DRAM Refresh Fehler
2K	Speicherproblem: DRAM Parity Fehler
3K	Erste 64k Byte RAM (die Mindestbestückung) fehlerhaft
4K	Erste 64k RAM fehlerhaft oder Timer funktioniert nicht
5K	Genereller Prozessorfehler
6K	Gate-A20-Fehler im Tastaturcontroller
7K	Prozessor-Ausnahmefehler, BIOS kennt CPU-Typ nicht
8K	Fehler im BWS der Grafikkarte
9K	BIOS-ROM-Checksummenfehler
10K	Fehler im CMOS-RAM
11K	L2-Cache fehlerhaft, wird vom BIOS abgeschaltet
Dauerton	Netzteilfehler oder Netzteil zu schwach
1L 1K	Schwerwiegender Hauptplatinenfehler
1L 2K	Grafikkarte nicht gefunden oder Video-ROM-BIOS defekt
1L 3K	Videofehler: Defekter RAMDAC oder Monitor fehlt
1L 4K	Timer defekt
1L 5K	Prozessorfehler
1L 6K	Tastatur-Controller fehlerhaft
1L 7K	Virtual-8086-Mode-Problem
1L 8K	Fehler im Videospeicher (BWS)
3L 1K	Fehler beim Test des DOS- und Extended Memory
3K 3L 3K	Arbeitsspeicher defekt
1L	POST beendet: System arbeitet ohne Fehler

Tab. 1.5: Signaltöne des AMI-BIOS

1.5 UEFI-BIOS

1.5.1 Warum wurde eine neue BIOS-Generation notwendig?

Das BIOS von 1981 kannte weder USB noch DVD und nicht einmal Festplatten. Mehr als 30 Jahren wurde am BIOS „geflickschustert“, um das BIOS an immer neue Hardware und größere Festplatten und neue Datenträger anzupassen. Das Booten von DVD, USB-Sticks und externen Festplatten wurde hinzugefügt. Doch eine Umstellung auf ein 64-Bit-BIOS war zu aufwendig, und die Verwaltung von Festplatten über 2200 Gigabyte war nicht möglich, sie funktionieren mit dem alten „MBR-Partitionsschema“ nicht mehr.

Intel hatte ein besseres BIOS, das „**E**xtensible **F**irmware **I**nterface“ bereits 1998 entworfen. 2005 gründeten Intel, AMD, HP und weitere Firmen das „Unified EFI Forum“, um einen Standard UEFI 2.0 zu definieren. Dieses neue BIOS hat eine übersichtliche grafische Oberfläche und kann mit der Maus bedient werden. Weil CPU, RAM und Festplatte gleichzeitig statt nacheinander initialisiert werden, verkürzt sich die Zeit bis zum Booten. Das neue BIOS verwendet ein „GPT-Schema“ zur Partitionierung der Festplatte. Damit sind Festplatten bis 8 000 000 000 TB möglich (das entspricht ungefähr der gesamten Speicherkapazität aller Computer auf der Erde im Jahr 2008).

In das neue BIOS können Zusatzprogramme integriert werden, z. B. ein Datensicherungsprogramm oder ein einfacher Browser. Es könnte sogar ein Mini-Betriebssystem eingebaut werden ähnlich wie eine „Live Disk“. Damit könnte man Windows reparieren, wenn es nicht mehr funktioniert, oder Daten retten.

Um bei Bedarf ältere Betriebssysteme booten zu können, kann man die neuen Funktionen abschalten und in einem Modus „Legacy BIOS“ mit dem alten BIOS arbeiten.

Seit der Einführung von Windows 8 im Jahr 2012 wurden Hauptplatinen mit dem neuen UEFI-BIOS (**U**nified **E**xtensible **F**irmware **I**nterface) in der Version 2.3.1 ausgestattet, wodurch „Secure Boot“ ermöglicht wurde.

1.5.2 Secure Boot

Wenn „Secure Boot“ im UEFI-BIOS eingeschaltet ist, akzeptiert das BIOS nur „signierte” Bootloader. Das macht es Herstellern von Schadsoftware ohne passende Signatur nahezu unmöglich, den PC zu booten und die Kontrolle zu übernehmen. Seit Windows 11 ist die Aktivierung von Secure Boot vor der Installation und im Betrieb unbedingt notwendig.

Um zu ermitteln, ob Secure Boot schon aktiviert ist, tippen Sie „Systeminfo“ in das Suchfeld von Windows 10 ein. In der System-Übersicht unter „Sicherer Startzustand“ („Secure Boot State“) erfahren Sie, ob Secure Boot aktiv ist.

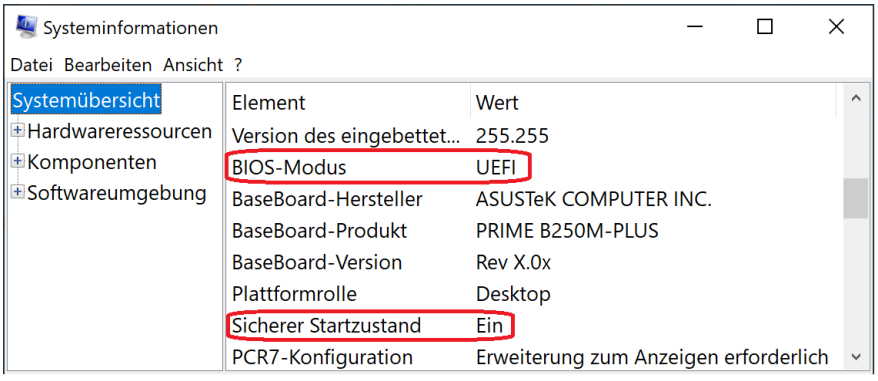

Bild 1.2: Secure Boot ist aktiviert

Überprüfen Sie auch den „BIOS Modus“: Steht dort UEFI, dann kann Secure Boot ohne weiteres aktiviert werden. Wird „Legacy (BIOS)“ oder „Vorgängerversion“ angezeigt, sind zusätzliche Schritte erforderlich.

Wenn Secure Boot nicht aktiv ist, müssen Sie ins UEFI-BIOS gehen. Aktivieren Sie dort „Secure Boot“. Wo ist bei jedem Board-Hersteller anders. In der Regel ist dieser Punkt unter „Sicherheit” zu finden.

1.5.3 Wie wird das BIOS-Setup aufgerufen?

Es gibt zwei Möglichkeiten, ins BIOS zu kommen: beim Starten des PC oder über Windows 10.

BIOS-Setup aufrufen im Startvorgang nach einem Kaltstart

Sowohl beim alten als auch beim neuen BIOS kommt man ins Setup-Programm, indem man den Startvorgang des PC im richtigen Moment mit einer Taste oder Tastenkombination unterbricht. Vorwiegend bei älteren Computern ist die Taste „**Del**ete“ (dt.: Entfernen) bzw. „Entf“) zu drücken, bei neueren Computern ist die Taste F2 zu drücken, in seltenen Fällen auch F12, F10, F8, F1, Esc, Strg-Einfg oder Strg-Esc.

Beobachten Sie den PC beim Booten genau. Auf dem Bootscreen sollte zu lesen sein, welche Taste man drücken muss, um ins BIOS zu kommen. Wenn Sie am unteren Bildschirmrand eine Meldung „Press Del for Setup“ aufblitzen sehen, haben Sie einige Sekundenbruchteile Zeit, die „Entf“-Taste zu drücken. Wenn Sie den Moment verpaßt haben, müssen Sie Windows herunterfahren, den PC aus- und einschalten und es erneut versuchen. Tipp: Fangen Sie beim zweiten Versuch einige Sekunden früher an, in schneller Folge die richtige Taste zu drücken.

Wenn Sie nicht wissen, welches die richtige Taste ist, um ins BIOS zu kommen, drücken Sie einfach die „Entf“- und „F2“-Taste in schnellem Wechsel. Eine von beiden ist bestimmt die richtige. Wenn weder „F2“ noch „Entf“ funktionieren, sollten Sie im Handbuch zur Hauptplatine oder im Internet nachschauen, welche Taste die richtige ist.

Achtung: Auch mit der richtigen Taste kommen Sie nur während des Kaltstarts (wenn der PC vor dem Einschalten stromlos war) ins BIOS-Setup-Programm, aber nicht nach dem Aufwachen aus einem Schlafzustand oder nach einem Neustart. Das liegt daran, dass nach einem „Warmstart“ das BIOS nur teilweise durchlaufen wird. Denn wozu den Speicher testen, wenn der PC eben noch funktioniert hat?

Bei einem Notebook ist es schwierig, einen Kaltstart durchzuführen, denn dazu müsste man den Stecker des Netzteils ziehen und außerdem den Akku herausnehmen.

Über Windows 10 oder 11 ins BIOS

Wenn im PC ein UEFI-BIOS steckt und Windows 10 oder 11 noch läuft, gibt es eine stressfreie Methode, ins BIOS zu kommen. Öffnen Sie die „Einstellungen“ → „Update und Sicherheit“ → „Wiederherstellung“ → „Erweiterter Start“ → „Jetzt neu starten“.

Beim nächsten Start bietet Windows die folgenden Optionen an, siehe Bild 1.3: „Fortsetzen“, „PC ausschalten“ und „Problembehandlung“. Wählen Sie „Problembehandlung“ → „Erweiterte Optionen“.

Bild 1.3: Menü Neustart-Optionen

Nun sehen Sie ein Menü wie im Bild 1.4. Hier wählen Sie „UEFI Firmware-Einstellungen“ (Hinweis: Geräten mit Legacy-BIOS fehlt diese Option) → „Neu Starten“.

Nach dem Neustart gelangt man ins UEFI-BIOS.

Bild 1.4: Neustart ins BIOS

1.6 TPM

1.6.1 Was ist TPM und wofür wird es gebraucht?

Seit dem Jahr 2014 werden immer mehr Computer mit einen „TPM-Chip“ bestückt. TPM kann auch in Mobiltelefone, Smartphones und Unterhaltungselektronik eingebaut werden. TPM steckt in Android- und Apple-Smartphones, um kontaktlose Bezahlvorgänge abzusichern. MacBooks und iMacs haben einen Sicherheitschip „T2“. Chromebooks haben einen Sicherheitschip „Titan C“. Der **T**rusted **P**latform **M**odule Chip ermöglicht es, Daten zuverlässig zu verschlüsseln und zu signieren.

Beispielsweise können Daten der eigenen Festplatte, aber auch USB-Speichersticks und externe Festplatten so verschlüsselt werden, dass sie nur auf einem einzigen PC (dem eigenen) geöffnet werden können. Der Besitzer ist davor geschützt, dass Diebe die Daten von seiner Festplatte auslesen – es gelingt weder mit einer Live-CD (eine Live-CD ist eine startfähige CD mit Betriebssystem, mit der man den PC benutzen kann, ohne auf die Festplatte zugreifen zu müssen) noch durch Anstecken der Festplatte an einen fremden PC.

Allerdings: kein Licht ohne Schatten. Wenn die Hauptplatine mit dem TPM-Chip kaputt ist, kann auch der Eigentümer seine Daten nicht mehr retten. Und wenn das Notebook verloren geht, sind die Daten auf verschlüsselten USB-Sticks verloren. Es sei denn, man hat rechtzeitig vorher einen Wiederherstellungs-Schlüssel erzeugt.

Ein Gerät mit TPM, angepasstem Betriebssystem und Software bildet zusammen eine „Trusted Computing Plattform“. Der Hersteller kann für seine „vertrauenswürdige Plattform“ Beschränkungen festlegen.

Im Zusammenwirken mit Secure Boot kann der Hersteller das Booten von jeglicher Live-CD verhindern. Von den vielen im Internet zu findenden nützlichen CDs, zum Beispiel für Windows-Reparaturen, Virensuche und Datenrettung, kann man nur von denen booten, die eine gültige Signatur besitzen. Oder man benutzt das alte „Legacy BIOS“, das Festplatten nur bis 2,2 GB zulässt. Wobei beginnend etwa seit dem Jahr 2021 bei immer mehr Hauptplatinen die Möglichkeit fehlt, zum alten BIOS zu wechseln.

1.6.2 Ist TPM 2.0 bereits aktiviert?

Um Windows 11 installieren zu können, muss TPM 2.0 im BIOS aktiviert sein. Etwa seit Sommer 2021 wurden Computer und Hauptplatinen in der Regel mit deaktiviertem TPM ausgeliefert, außer bei Business-Notebooks. Dann müssen Sie TPM im UEFI-BIOS einschalten.

So prüfen Sie, ob TPM 2.0 bereits aktiviert ist:

Tippen Sie `tpm.msc` ins Suchfeld oder an der Eingabeaufforderung ein. Unter „Status“ sehen Sie, ob TPM aktiv ist. Wenn nicht, hat der PC keinen TPM 2.0 Chip oder er ist nur nicht aktiviert.

Gehen Sie ins BIOS und versuchen Sie, TPM einzuschalten.

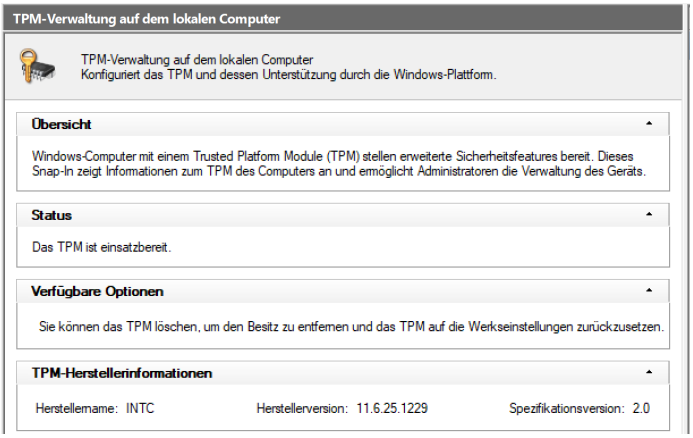

Bild 1.5: TPM 2.0 ist aktiviert

1.6.3 Die TPM-Konfiguration finden

Hier müssen Sie den passenden Eintrag zum TPM finden. Die Einstellung unterscheidet sich je nach Hersteller und Mainboard.

Das Bild 1.6 zeigt das BIOS einer ASUS-Hauptplatine mit Intel-CPU. Das TPM-Modul wird hier mit „Intel Platform Trust Technology“ (Intel PTT) bezeichnet und ist unter „Advanced“ → „PC-Host Firmware Configuration“ zu finden.

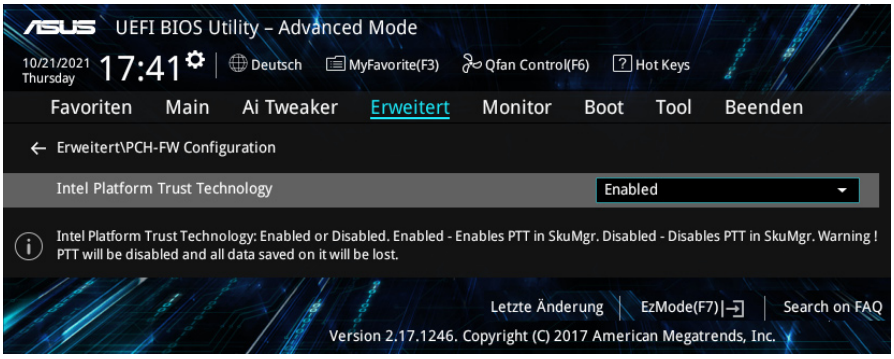

Bild 1.6: TPM-Einstellung eines ASUS-Mainboards mit Intel-CPU

Im Bild 1.7 ist das BIOS einer ASUS-Hauptplatine mit AMD-CPU gezeigt. Hier heißt der Eintrag „fTPM“. Hat man die TPM-Einstellung gefunden, muss diese aktiviert werden („Enabled“).

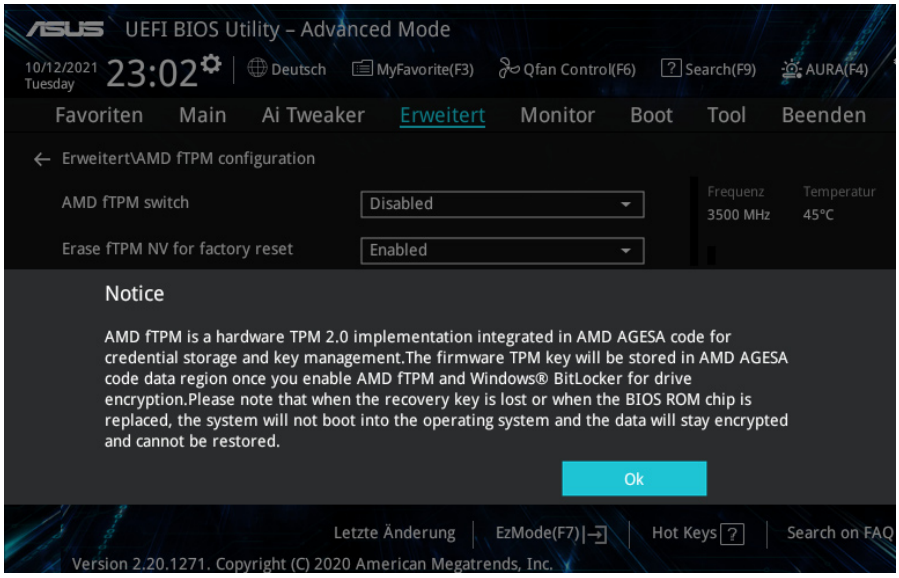

Bild 1.7: TPM-Einstellung eines ASUS-Mainboards mit AMD-CPU

Beenden Sie die UEFI-Einstellungen (im Allgemeinen mit Taste „F10“).

Überprüfen Sie nach dem Neustart mit `tpm.msc`, ob TPM jetzt aktiv ist.

1.7 BUSSYSTEME

1.7.1 Was ist ein „Bus“?

Damit die CPU mit dem Arbeitsspeicher, Festplatten- und DVD-Laufwerken sowie mit anderen peripheren Baueinheiten Informationen austauschen kann, müssen diese miteinander verbunden sein. Die beste Variante in Bezug auf die Leistungsfähigkeit wäre, die betreffenden Bauteile direkt mit speziellen Leitungen zu verbinden. Wenn man allerdings jeden von acht Steckplätzen mit je mindestens 60 Anschlüssen direkt mit der CPU verbinden müsste, würde die Zahl der „Beinchen“ der CPU und der interne Schaltungsaufwand übermäßig anwachsen. Weil diese Variante zu aufwendig ist und man das System durch die starre Verdrahtung nicht erweitern könnte, verwendet man universell nutzbare Kommunikationswege: Die Bussysteme.

Unter einem Bus versteht man ein Bündel von zusammengehörigen Leitungen, über welche die einzelnen Baugruppen eines digitalen Systems Informationen austauschen können.

Eine Busstruktur weist prinzipiell vier Gruppen von Leitungen auf:

- Versorgungsbus (Strom- und Taktversorgung, Initialisierungen, Anzeige von Hardwarefehlern)
- Datenbus (überträgt die Daten zwischen Prozessor, Arbeitsspeicher und Peripherie)
- Adressbus (überträgt die Adresse einer Speicherzelle im RAM oder eines E/A-Gerätes)
- Steuerbus (bestimmt, ob die Information gelesen oder geschrieben werden soll)

Da die Wege zum Datenaustausch von allen angeschlossenen Baugruppen gemeinsam genutzt werden, muss für eine Ordnung gesorgt werden. Zu jedem Zeitpunkt (Takt) darf nur genau eine Baueinheit die Kontrolle über den Bus haben und Informationen senden. Andere Baugruppen müssen warten, bis sie an der Reihe sind und den Bus benutzen dürfen.

John von Neumann stellte 1945 ein Konzept für den Bau eines Computers vor. In dieser „von-Neumann-Architektur“ besteht ein Computer aus der Zentraleinheit (Steuerwerk und dem Rechenwerk), dem Speicher und den Ein-/Ausgabeeinheiten. Alle Einheiten sind über einen einzigen Bus, den **Systembus** miteinander verbunden. Diese Architektur hat einen gravierenden Nachteil: Der Bus wurde immer mehr zum Flaschenhals des Systems (der sogenannte „Von-Neumann-Flaschenhals“, englischer Fachbegriff: „Von-Neumann-Bottleneck“). Moderne CPUs sind viel schneller, als die Daten über den Bus vom Speicher in den Prozessor geladen werden können.

Durch Spezialisierung und Strukturierung kann man diesen Engpass aber in gewissem Maße überwinden. Bei den ersten PCs gab es nur einen einzigen Systembus. Später bekam der Arbeitsspeicher einen eigenen Speicherbus. Als nächstes wurde der Bus für Steckkarten aufgetrennt: Seit dem Pentium 4 hat die Grafikkarte einen eigenen Bus (den AGP-Bus), der PCI-Bus versorgt alle anderen Steckplätze. Der Trend geht zu einer weiteren Spezialisierung der Busse:

- Prozessorinterne Busse
- Prozessorbus
- Speicherbus
- Systembus
- Peripherie- oder I/O-Bus
- Interrupt- oder Nachrichtenbusse

Heutige Hauptplatinen haben mindestens drei Busse:

1. Einen sehr schnellen Bus zu den Modulen des Arbeitsspeichers. Beginnend mit den Dual-Core-CPUs ist der Speicherbus doppelt vorhanden, Spitzenmodelle haben drei oder vier Speicherbusse.
2. Mehrere schnelle Busse zu den Steckplätzen (je einen für PCI und PCI-Express).
3. Einen langsamen Bus für Tastatur, Maus, USB, Diskettenlaufwerk und andere langsame Geräte.

1.7.2 ISA: Industry Standard Architecture

Im ersten IBM-PC wurde ein 8-Bit-Bus verwendet. Diese Architektur wurde von IBM nicht patentiert und konnte deshalb von vielen Herstellern nachgebaut werden. Mit der Einführung der PC-AT-Klasse mit dem ersten reinen 16-Bit-Prozessor i80286 wäre der 8-Bit-Bus zum Nadelöhr im Datenfluss geworden. Deswegen wurde mit dem PC-AT ein erweitertes Steckkartensystem eingeführt, der 16-Bit ISA-Standard.

Diesmal wurde das Bussystem präzise beschrieben! Der ISA-Bus war als weitgehend abwärtskompatibel entwickelt worden, so dass auch alte 8-Bit-Steckkarten in 16-Bit-Slots funktionierten.

Bild 1.8: Verschiedene Busse: oben: ISA 8-Bit, mitte: ISA 16-Bit, unten: EISA 32-Bit

Der ISA-Bus hat 16 Datenleitungen und 24 Adressleitungen. Die Taktfrequenz betrug je nach Hauptplatine 4,77 oder 6 oder 8 oder 8,33 MHz. Eine Übertragungsrate von max. 7 MByte pro Sekunde war möglich. Damit war der ISA-Bus optimal auf die Intel-CPU i80286 abgestimmt.

In den nachfolgenden 386er PCs und erst recht im 486er war der ISA-Bus auch in der 16-Bit-Version überfordert. Für den 386er wurden der MCA-Bus und der EISA-Bus entwickelt. Beide erreichten nur geringe Verbreitung. Speziell für die 486er wurde der „**V**esa **L**ocal **B**us“ als Nachfolger entwickelt.

Heute ist der ISA-Bus ausgestorben. Seit dem Pentium-III haben die Hauptplatinen keinen ISA-Bus mehr, und spätere Systeme schon gar nicht.

1.7.3 MCA: MicroChannel Architecture

IBM war nicht glücklich wegen der unzähligen Firmen, die Komponenten für den PC herstellten. Der ISA-Bus war ja nicht patentiert oder sonst irgendwie geschützt. Zudem war der ISA-Bus für den 386er PC nicht mehr ausreichend. Um das Jahr 1987 herum versuchte IBM mit einem neuen Steckkarten- bzw. Bussystem die Nachteile des ISA-Standards wieder wettzumachen.

Mit dem MCA-Bus (**M**icro**C**hannel **A**rchitecture) wurde ein Bussystem eingeführt, das eine wesentlich bessere Kommunikation zwischen den Bauteilen der Hauptplatine und den Steckkarten ermöglichte. Die MCA-Architektur ist technisch fast auf PCI-Niveau, aber zum ISA-Standard nicht abwärtskompatibel. Eine Busbreite von 32 Bit und ein Takt von 10 MHz ermöglichten eine Übertragungsrate von 40 MByte/s.

IBM besaß das Monopol und konnte bestimmen, wer Steckkarten und Hauptplatinen in Lizenz bauen durfte.

1.7.4 EISA: Extended Industry Standard Architecture

Die anderen Hauptplatinenhersteller waren nicht gewillt, Lizenzgebühren zu zahlen. Die Lizenzgebühren waren relativ hoch. Microchannel konnte sich deshalb nie so recht durchsetzen. Die vereinte Konkurrenz schuf ein anderes, verbessertes Bussystem. Der EISA-Bus (**E**xtended **I**ndustry **S**tandard **A**rchitecture) wurde so konstruiert, dass auch die älteren ISA-Erweiterungskarten genutzt werden konnten. Das wurde dadurch erreicht, dass der Steckplatz wie der des ISA-Busses aussah, aber über zwei Reihen Kontakte übereinander verfügte (im Bild 1.8 der untere Stecker). ISA-Karten erreichten nur die untere Kontaktebene, EISA nutzt zusätzlich die obere Kontaktreihe.

Der EISA-Bus hat einen 32-Bit Daten- und Adressbus. Seine Übertragungsgeschwindigkeit erreichte bis zu 16 MByte pro Sekunde bei 8,33 MHz.

Der EISA-Bus war der Vorgänger des PCI-Busses und ist eine Art Erweiterung des ISA-Busses mit einigen Optimierungen hin in Richtung Datendurchsatz und CPU-Entlastung – (damals) eigentlich ideal für Server!

1.7.5 VLB: VESA Local Bus

VLB wurde von der VESA entwickelt (**V**ideo **E**lectronics **S**tandard **A**ssociation, Vereinigung der Hersteller von Grafikkarten). Ziel der Gemeinschaftsentwicklung war die Erweiterung des ISA-Busses mit dem Ziel, den 16-Bit-Engpass für die Grafikausgabe zu umgehen. VESA kam 1992 auf den Markt.

Ein normaler 16 Bit ISA-Steckplatz wurde um einen zusätzlichen Steckverbinder verlängert. Dadurch kann VLB mit einer Datenbreite von 32 Bit arbeiten. Bei einer Taktfrequenz von 33 MHz ergibt das eine Datentransferleistung von max. 33,33 MHz × 4 Byte = 133 MByte/s. Maximal drei VLB-Steckplätze waren erlaubt. Eine höhere Taktfrequenz ist möglich, wenn nicht alle Slots besetzt sind: Bei zwei VLB-Karten sind 40 MHz erlaubt, eine einzelne VLB-Karte durfte mit 50 MHz getaktet werden.

Der VESA-Bus war zu sehr auf die 486er CPU zugeschnitten und konnte an die nachfolgenden Pentium-CPUs nicht angepasst werden. Die direkte Verbindung des VLB mit dem empfindlichen Prozessorbus war problematisch. Auf Boards mit einer Pentium-CPU gibt es keine VLB-Steckplätze mehr. VLB verschwand bereits 1995 vom Markt.

Für die Pentium-Prozessoren entwickelte Intel ein neues Konzept.

1.7.6 PCI: Peripheral Component Interconnect

Peripheral **C**omponent **I**nterconnect wurde 1991 von Intel speziell für den Pentium entwickelt. Die CPU wurde um einen Controller-Chip (heute nennt man das den „Chipsatz“) ergänzt. Der PCI-Bus wurde nicht mehr direkt mit dem Prozessor verbunden, sondern über diesen Controller-Chip entkoppelt. Der PCI-Bus war so weitsichtig und universell entwickelt worden, dass er auch in Apple Macintosh (seit 1995) und Alpha-Workstations zum Einsatz kam. Der PCI Bus ist bis ins Detail normiert und leicht nachzubauen.

Die Leistung von PCI konnte mehrmals gesteigert werden. Für die Weiterentwicklung und Standardisierung ist die PCI SIG (**P**eripheral **C**omponent **I**nterconnect **S**pecial **I**nterest **G**roup) zuständig – eine Interessengemeinschaft der Hersteller von Computerkomponenten. Mitglieder sind Intel, AMD, Dell, HP, NVIDIA und weitere 800 Firmen. Die 2004 verabschiedete PCI-Version 3.0 ist die letzte PCI-Version.

Speziell für Server wurde **PCI-**e**X**tended entwickelt. Der „ursprüngliche“ PCI wird als PCI-konventionell bezeichnet, um ihn von PCI-X und seinem Nachfolger PCIe unterscheiden zu können. PCI-X konnte sich nicht durchsetzen, weil das etwa gleichzeitig entwickelte konkurrierende **PCI-E**xpress (PCIe) deutlich überlegen war.

PCI Version	1.0	2.2 bis 3.0	PCI-X 1.0	PCI-X 2.0
Busbreite	32 Bit	64 Bit	64 Bit	64 Bit
Bustakt	33 MHz	66 MHz	133 MHz	266 MHz
Übertragung	133 MByte/s	533 MByte/s	1067 MByte/s	2133 MByte/s

Tab. 1.6: Daten des PCI-Bussystems

Die PCI-Komponenten müssen sich nicht auf Steckkarten befinden, sie können auch auf der Hauptplatine untergebracht werden (sogenannte „planar devices“).

Jede PCI-Komponente besitzt eine eindeutige Hardware-Kennung, die „PCI-ID“. Diese setzt sich aus drei Teilen zusammen: Class-ID: Hersteller-ID: Geräte-ID, z. B. hat der „82557B 10/100 PCI Ethernet Adapter“ von IBM die Hardware-Kennung `0200:1014:005C`. Hier bedeuten:

0200 Ethernet Network Controller, 1014 IBM und 005C für dessen 82557B 10/100 PCI Ethernet Adapter.

Die ersten beiden Ziffern der Class-ID bezeichnen eine von 22 Klassen: 01=Massenspeichercontroller, 02=Netzwerkcontroller, 03=Grafikcontroller, ... siehe `https://pci-ids.ucw.cz/read/PD/`. Wenn man auf eine Klasse dieser Tabelle klickt, werden die Unterklassen angezeigt: Bei Netzwerken (Klasse 02) z. B. 00=Ethernet, 04=ISDN.

Auf der Webseite `https://pci-ids.ucw.cz` finden Sie die „PCI Vendor and Device Lists“. In der „`pci.ids`“ finden Sie alle jemals hergestellten PCI- und PCIe-Geräte. Wenn Ihnen der Gerätemanager ein Gerät als „unbekannt“ anzeigt, finden Sie dessen Hersteller- und Gerätenummer unter dessen Eigenschaften, siehe Bild 1.3.

Bild 1.9: Hardwarekennung eines unbekannten Gerätes Die Class-ID wurde als „Audiocontroller für Multimedia“ entschlüsselt. Hersteller- und Geräte-ID stehen im „Wert“.

Welche besonderen Eigenschaften hat der PCI-Bus (und seine Nachfolger AGP und PCIe)?

Plug and Play

Vom BIOS wird jede PCI-Erweiterungskarte nach ihren Ressourcenwünschen abgefragt und konfiguriert. Konflikte der Erweiterungskarten in Bezug auf Port-Adresse, Interrupt oder DMA-Kanal kommen – theoretisch – nicht mehr vor. (DMA = Datenübertragung zwischen Speicher und Geräten ohne CPU-Beteiligung)

Interrupt-Sharing

Am ISA-Bus brauchte jedes Gerät eine eigene Interruptleitung zur CPU. Doch die Interrupts waren sehr knapp, Doppelbelegung war verboten. PCI-Komponenten können sich einen Interrupt teilen. Allerdings kommt es bei neuentwickelten Komponenten in Ausnahmefällen vor, dass die Teilung der Ressourcen wegen unsauber programmierter Treiber nicht funktioniert.

Bus-Master-Betrieb

Da der Prozessor über einen Controller (der sich im Chipsatz befindet) vom Bus entkoppelt ist, kann der PCI-Bus teils unabhängig von der CPU arbeiten. So kann beispielsweise die Festplatte Daten zum Brenner schicken, während die CPU unabhängig davon Berechnungen ausführt. Die PCI-Karte, welche die Daten sendet, ist der Master, und die Karte, welche die Daten empfängt, ist der Slave.

Für die Steuerung des Datenaustauschs tauschen die Baugruppen Steuerbefehle (Messages) aus. Der Standard erlaubt bis zu 256 verschiedene Steuerbefehle.

Multiplex-Prinzip

Seit der Version 2.1 kann der PCI-Bus 32 Leitungen für die Daten plus 32 Leitungen für Adressen haben. Durch den Multiplex-Betrieb dürfen die Hersteller die Hälfte dieser Leitungen einsparen, indem mit einem Takt zuerst die Adresse und in einem zweiten Takt das Datenwort gesendet wird.

Auf Server-Platinen gab es meist einen oder zwei „echte“ 64-Bit-Steckplätze, auf denen die Adress- und Datenleitungen gleichzeitig angesteuert wurden. Auf preiswerteren Platinen wurden meist 32-Bit-Steckplätze verwendet, die im Multiplexbetrieb genutzt wurden.