Verschil BIOS-UEFI systemen

Wat is er anders aan een UEFI systeem in vergelijking met een traditioneel systeem met BIOS? Wat kun je ermee en welke voor- en nadelen zitten er aan? Kortom wat is UEFI nu eigenlijk. Het volgende stukje gaat over de belangrijkste verschillen voor ons als consument.

UEFI is een afkorting voor Unified Extensible Firmware Interface, en is de opvolger van het bekende BIOS. Over het BIOS een kleine uitleg.

BIOS is een afkorting voor Basic Input Output Software. Zoals je kunt zien aan het eerste woord BASIC, is het een basis voorziening, een soort bibliotheek met basisinstructies om hardware en het besturingssysteem te laten communiceren. Wanneer een pc of laptop gestart wordt in BIOS systemen word er een serie tests uitgevoerd die controleert of het RAM, de videokaart, de opslagschijven, toetsenbord en andere hardware normaal functioneert. Als dat allemaal succesvol doorlopen is, zoekt het BIOS naar een opstartsector op de harde schijf en zal het systeem verder opstarten. De taak van het BIOS zit er dan op en wordt overgenomen door het besturingssysteem.

UEFI is de vervanger van het BIOS en waar BIOS een basisvoorziening is om het systeem op te starten, is UEFI meer een klein besturingssysteempje op zichzelf. UEFI is volledig platform onafhankelijk en veel uitgebreider. Het kan met alle aangesloten hardware overweg en in de praktijk betekend dit een snellere opstartsnelheid. De hardware wordt namelijk door UEFI ingeladen en niet meer door het besturingssysteem.

Inherent aan het UEFI systeem is de indeling van de harde schijf waar het systeem van opstart. De schijf waar het besturingssysteem van opstart is geformatteerd in GPT (GUID PARTITION TABLE).

Dit heeft ook weer een voordeel. GPT partities zijn beter beschermd tegen zogenaamde rootkits en virussen die zich in de opstartsector kunnen nestelen, waardoor het besturingssysteem niet meer wil opstarten. GPT-schijven hebben een backup-partitietabel die gebruikt kan worden als hoofd-partitietabel corrupt geraakt is door bijvoorbeeld een rootkit of virus. Ook kan het in specifieke situaties een voordeel zijn dat een schijf geformatteerd in GPT wel 128 partities kan bevatten. In tegenstelling tot maar 4 partities als de schijf in NTFS geformatteerd is. Het door Intel ontwikkelde EFI systeem werd in het verleden veel gebruikt voor servers, waarbij de veiligheid als belangrijkste argument werd aangevoerd. Later is dit door Microsoft verder ontwikkeld, en is de term UEFI ontstaan.

Een nadeel van een UEFI systeem kan zijn dat het vrij moeilijk is, soms onmogelijk, om een ouder Windows besturingssysteem te installeren, of bijvoorbeeld een Linux distro. Het is mogelijk om UEFI uit te zetten, en te booten in BIOS LEGACY mode, zodat ondersteunde partitie-formats kunnen worden gebruikt (NTFS, ext2, ext3 of ext4 en meer). Of de mogelijkheid om UEFI uit te zetten in de toekomst geblokkeerd wordt, is tot op vandaag niet bekend. Ook zou de SECURE BOOT optie aan of uit gezet moeten

kunnen worden, als dat niet kan zal er geen alternatief besturingssysteem geïnstalleerd kunnen worden.

Dit probleem kan ontstaan wanneer een OEM-bouwer zijn pc zodanig configureert, dat er geen ander besturingssysteem geïnstalleerd kan worden. Het zou dan onmogelijk zijn om bijvoorbeeld een dual-boot met Linux te installeren. Het Linux-front is niet zo blij met deze ontwikkeling, maar Microsoft heeft in een blog laten weten dat:

UEFI kan firmware gebruik laten maken van een veiligheidsbeleid Secure boot. UEFI Secure Boot is een onderdeel van 'Windows 8 secured boot' architectuur. Windows 8 maakt gebruik van Secure Boot om ervoor te zorgen dat de pre-OS-omgeving veilig is. Secure boot is niet bedoeld om andere OS-loaders te blokkeren, maar het is een beleid waarmee firmware de authenticiteit van componenten kan valideren.

OEM's hebben met UEFI de mogelijkheid om hun firmware aan te passen aan de behoeften van hun klanten die op deze manier een beleid omtrent hun computergebruik kunnen handhaven. Het niveau van dit beveiligingsbeleid kan aangepast worden. Vooral voor zakelijke pc's is dit belangrijk.

Microsoft beheert niet en controleert niet de instellingen van PC firmware waarmee Secure Boot in of uitgeschakeld kan worden."

Op de website van Microsoft Windows Hardware Certification Requirements staat het volgende:

VERPLICHT: inschakelen/uitschakelen Secure Boot.

De mogelijkheid om Secure Boot uit te schakelen op niet-ARM systemen kan worden verkregen doormiddel van een firmware setup. Een fysiek aanwezig gebruiker moet worden toegestaan om Secure Boot via firmware setup zonder rechten op Pkpriv (stukje code, of programmatuur) Secure Boot aan of uit te schakelen. Programmatisch uitschakelen van Secure Boot hetzij tijdens Boot Services of na het verlaten van EFI Boot Services mag niet mogelijk zijn. Het uitschakelen van secure boot mag niet mogelijk zijn op ARM systemen.

Met andere woorden, op gewone notebooks en pc's kan Secure Boot uitgeschakeld worden zonder tussenkomst van Microsoft of de leverancier, zodat alsnog een ander besturingssysteem erbij geïnstalleerd kan worden.

Was je echter van plan om in de toekomst een Windows 8 tablet te gaan kopen en daarnaast Android op te installeren, dan zou je wel eens bedrogen uit kunnen komen.

Deze tekst las ik een tijdje geleden in een nieuwsbrief.