Secure Boot

Secure Boot je funkce rozhraní UEFI, která brání spuštění neautorizovaného kódu během procesu zavádění systému. Funguje na principu digitálních podpisů a kryptografických klíčů. Pokud software, který se pokouší spustit, nemá platný podpis od důvěryhodné autority (např. Microsoft nebo výrobce PC), základní deska mu nedovolí se spustit.

Jak Secure Boot funguje?

Proces kontroly probíhá v řetězci (tzv. Chain of Trust):

```
1. **Firmware (UEFI):** Obsahuje databázi veřejných klíčů od důvěryhodných výrobců (typicky Microsoft a výrobce základní desky).
2. **Kontrola podpisu:** Před spuštěním zavaděče systému (např. Windows Boot Manager) UEFI zkontroluje jeho digitální podpis.
3. **Porovnání:** Pokud se podpis shoduje s klíčem v databázi, systém se spustí. Pokud ne (podpis chybí nebo je změněný), počítač zobrazí chybu "Security Violation" a zastaví se.
```

Proti čemu chrání?

Secure Boot je navržen k eliminaci útoků typu:

- **Rootkity:** Malware, který se maskuje hluboko v systému a je pro běžný antivirus neviditelný.
- **Bootkity:** Škodlivý kód, který nahradí legální zavaděč systému svým vlastním, čímž získá plnou kontrolu nad počítačem ještě před startem Windows/Linuxu.

Secure Boot a operační systémy

- **Windows:** Od verze Windows 8 je Secure Boot standardem. Pro instalaci **Windows 11** je jeho podpora (a aktivace) vyžadována jako jedna z minimálních hardwarových podmínek.
- **Linux:** Většina velkých distribucí (Ubuntu, Fedora, openSUSE) Secure Boot podporuje díky zavaděči zvanému „shim“, který má podpis od Microsoftu. Méně známé distribuce však mohou vyžadovat vypnutí této funkce.
- **Dual-boot:** Pokud používáte více systémů na jednom PC, Secure Boot může někdy blokovat spuštění druhého systému, pokud nemá správně vyřešené certifikáty.

Mýty a kontroverze

Kolem Secure Bootu se v minulosti objevila řada diskusí:

- **„Zámek na Windows“:** Původně existovaly obavy, že Microsoft využije Secure Boot k tomu, aby zabránil instalaci jiných systémů (Linuxu). V praxi však většina výrobců umožňuje v nastavení UEFI tuto funkci **vypnout** nebo přidat vlastní klíče.
- **Uživatelská kontrola:** Pokročilí uživatelé si mohou do UEFI nahrát své vlastní klíče a podepisovat si vlastní zavaděče, což zachovává bezpečnost i svobodu.

Srovnání: Aktivní vs. Vypnutý Secure Boot

Vlastnost	Secure Boot Enabled	Secure Boot Disabled
Bezpečnost	Vysoká (chrání proti bootkitům).	Nižší (systém je zranitelnější).
Kompatibilita	Podporuje moderní OS (Win 11).	Umožňuje starší OS a nepodepsané ovladače.
Rychlost	Žádný měřitelný rozdíl.	Žádný měřitelný rozdíl.

Související pojmy: UEFI, BIOS, Cold Boot, Rootkit, TPM, Windows 11, Kryptografie.