TPM (Trusted Platform Module)

TPM (Trusted Platform Module) je specializovaný hardware (mikročip) nebo firmwarové řešení navržené pro zajištění bezpečnosti počítače na hardwarové úrovni. Slouží k ukládání kryptografických klíčů, hesel a digitálních certifikátů.

Základní principy

TPM funguje jako „bezpečný trezor“ uvnitř počítače, který je oddělen od hlavního operačního systému. Tím zabraňuje útočníkům nebo malwaru v přístupu k citlivým datům, i když je samotný OS kompromitován.

Standardy TPM definuje konsorcium **Trusted Computing Group (TCG)**. V současnosti je standardem verze **TPM 2.0**.

Hlavní funkce

- **Generování náhodných čísel:** Používá se pro tvorbu silných šifrovacích klíčů.
- **Vzdálený monitoring (Attestation):** Schopnost prokázat, že hardware a software nebyl změněn (např. při bootování).
- **Bezpečné úložiště:** Ukládání klíčů pro šifrování disků (např. Microsoft BitLocker).
- **Hardwarová autentizace:** Podpora pro technologie jako Windows Hello.

Typy implementace

Typ	Popis
Discrete TPM (dTPM)	Samostatný fyzický čip na základní desce. Nejbezpečnější varianta.
Integrated TPM	Součást čipové sady (chipsetu).
Firmware TPM (fTPM)	Implementace v rámci bezpečného prostředí procesoru (např. AMD PSP nebo Intel PTT).
Software TPM	Čistě softwarová emulace, nejméně bezpečná.

Význam pro moderní systémy

Od vydání systému **Windows 11** se přítomnost a aktivace modulu **TPM 2.0** stala jednou ze základních hardwarových podmínek pro instalaci operačního systému. To vedlo k masovému rozšíření této technologie mezi běžné uživatele.

Související pojmy

- Kryptografie
- BitLocker

- UEFI Secure Boot