TPM (Trusted Platform Module)

TPM je specializovaný mikročip (kryptoprocesor) integrovaný na základní desce počítače, který slouží k zajištění hardwarové bezpečnosti. Na rozdíl od softwarového zabezpečení, které lze napadnout v rámci operačního systému, TPM uchovává citlivá data (šifrovací klíče, hesla, certifikáty) ve fyzicky odděleném a chráněném prostoru.

V naší společnosti je aktivní a funkční TPM čip povinným požadavkem pro všechna zařízení přistupující k firemní síti **WAN**.

Hlavní funkce TPM

V rámci naší **kybernetické bezpečnosti** využíváme TPM pro tyto účely:

- **Šifrování disků (BitLocker):** TPM uchovává dešifrovací klíč pro pevný disk. Pokud by někdo disk z laptopu vyjmul a zkusil jej přečíst v jiném počítači, data zůstanou bez TPM čipu nečitelná.
- **Ověřování integrity systému:** Při startu (bootování) TPM kontroluje, zda nebyl pozměněn BIOS/UEFI nebo zavaděč systému (např. vlivem rootkitu).
- **Bezpečné uložení identit:** TPM chrání biometrická data (Windows Hello) a digitální certifikáty pro přihlašování do **VPC**.
- **Hardwarové generování náhodných čísel:** Poskytuje vysoce kvalitní entropii pro kryptografické operace prováděné **vývojářským týmem**.

TPM v naší infrastruktuře

1. Koncová zařízení (Laptopy a Workstanice)

Všechny firemní počítače spravované **IT podporou** musí mít TPM verze **2.0**. Je to nezbytná podmínka pro běh moderních verzí Windows a mechanismů **UAC**.

2. Servery a [[VPS]]

Naše fyzické servery využívají TPM k zajištění „Root of Trust“. U **virtuálních strojů** využíváme tzv. **vTPM** (virtuální TPM), který emuluje funkce čipu pro potřeby šifrování uvnitř cloudu.

3. [[IoT zařízení]]

U průmyslových modulů a senzorů v terénu slouží TPM k unikátní identifikaci zařízení (**UID**). Tím zabraňujeme tomu, aby se do naší sítě pokusilo připojit cizí nebo podvržené zařízení.

Srovnání verzí: TPM 1.2 vs. TPM 2.0

Vlastnost	TPM 1.2	TPM 2.0 (Náš standard)
Algoritmy	Pouze SHA-1 a RSA	SHA-256, ECC a další (agilní)
Bezpečnost	Starší standard	Moderní, vyšší odolnost
Hierarchie	Jedna (Storage)	Více (Platform, Storage, Endorsement)

> **Důležité upozornění:** Pokud při startu počítače uvidíte výzvu k zadání „BitLocker Recovery Key“, znamená to, že TPM detekovalo změnu v hardwaru nebo konfiguraci. V takovém případě kontaktujte **Helpdesk**.

— **Související stránky:** ZIF, Kybernetická bezpečnost, IT Podpora, Vývojový tým, VPC, WAN, IoT zařízení