TNC (Trusted Network Communications)

TNC je otevřená architektura pro kontrolu integrity zařízení a řízení přístupu k síti (NAC - Network Access Control). Tento standard, vyvinutý skupinou Trusted Computing Group (TCG), umožňuje naší **IT podpoře** vynucovat bezpečnostní politiky dříve, než je zařízení plně vpuštěno do našeho **VPC**.

Jednoduše řečeno: TNC prověří „zdravotní stav“ vašeho počítače (např. zda máte zapnutý firewall a aktivní **TPM**) předtím, než vám dovolí otevřít systém **Jira** nebo firemní **WWW**.

Jak TNC funguje? (Proces kontroly)

Architektura TNC staví na třech základních krocích:

```
1. **Měření (Measurement):** Speciální agent na vašem zařízení (např. v rámci Windows nebo **[[Tux|Linuxu]]**) shromáždí informace o stavu systému.
2. **Ověření (Attestation):** Tato data jsou bezpečně odeslána na server, který je porovná s našimi bezpečnostními pravidly. Zde se často využívá **[[TPM]]** čip k prokázání, že data nebyla cestou podvržena.
3. **Rozhodnutí (Policy Enforcement):** Pokud zařízení vyhovuje, získá přístup. Pokud ne, je přesunuto do karantény k opravě (např. k instalaci aktualizací).
```

Význam pro naši infrastrukturu

1. Ochrana sítě [[WAN]] a [[WLAN]]

Díky TNC zabraňujeme tomu, aby se k naší síti připojila infikovaná nebo nezabezpečená zařízení (např. soukromé notebooky bez antiviru), která by mohla ohrozit naši **kybernetickou bezpečnost**.

2. Integrace s [[IoT zařízení|IoT zařízeními]]

U našich průmyslových senzorů a kontrolerů slouží TNC k ověření, že firmware nebyl neoprávněně modifikován. Zařízení bez platného „atestu“ nebude moci odesílat data do našich databází.

3. Vzdálený přístup a [[VPN]]

Při připojování z domova TNC automaticky zkontroluje, zda máte zapnuté **UAC** a zda je operační systém aktualizovaný. Tím chráníme naše **VPS** servery před útoky zvenčí.

Komponenty TNC v naší praxi

Komponenta	Funkce
AR (Access Requester)	Vaše zařízení, které žádá o přístup.
PEP (Policy Enforcement Point)	Switch nebo brána **UTM**, která fyzicky blokuje nebo povoluje provoz.
PDP (Policy Decision Point)	Centrální server, který vyhodnocuje soulad s pravidly.

Vztah k dalším standardům

TNC úzce spolupracuje s technologiemi, které již v rámci **ZIF** používáme:

- **TPM:** Poskytuje hardwarový základ pro důvěryhodné měření integrity.
- **UID:** Každé měření je spojeno s konkrétní identitou uživatele a zařízení.
- **IF-MAP:** Protokol pro sdílení informací o hrozbách mezi různými bezpečnostními prvky v síti.

> **Upozornění:** Pokud vám byl přístup k síti zamítnut z důvodu „nevyhovující integrity“, zkontrolujte v ovládacích panelech, zda jsou všechny systémové aktualizace nainstalovány, a restartujte počítač.

— **Související stránky:** ZIF, TPM, Kybernetická bezpečnost, IT Podpora, UTM, WAN, VPC, IoT zařízení