TELNET (TELecommunication NETwork)

TELNET je síťový protokol vyvinutý v roce 1969, který umožňuje uživateli vzdálený přístup k jinému počítači prostřednictvím terminálového rozhraní (**TTY**). Funguje na architektuře klient-server a standardně využívá port 23 nad protokolem TCP.

V naší **digitální architektuře** je TELNET považován za **zastaralý a nebezpečný**, a proto je jeho použití v rámci sítě **WAN** přísně regulováno.

Funkce a princip

TELNET přenáší textová data v nešifrované podobě (plain text). To znamená, že:

- Veškeré příkazy, odpovědi systému, ale i **uživatelská jména a hesla** jsou po síti posílána čitelně.
- Útočník vybavený nástrojem pro odposlech sítě může tyto údaje snadno zachytit.

Využití v naší infrastruktuře (výjimky)

Přestože je TELNET nahrazen protokolem **SSH**, naše **IT Podpora** jej stále využívá ve specifických případech:

1. Testování síťové dostupnosti

TELNET je vynikající nástroj pro ověření, zda je konkrétní port na serveru otevřený.

- **Příklad:** Příkaz `telnet server.firma.cz 80` ověří, zda na cílovém stroji běží **WWW** služba, aniž by bylo nutné otevírat prohlížeč.

2. Správa legacy zařízení

Některá starší **IoT zařízení** nebo historické síťové switche v našem skladu nepodporují moderní šifrování. V takovém případě je TELNET povolen pouze v izolované **VLAN** bez přístupu k internetu.

3. Ladění aplikací

Náš **Vývojový tým** může využívat TELNET pro interakci se surovými textovými protokoly (např. ruční posílání SMTP příkazů pro testování e-mailového serveru).

Srovnání: TELNET vs. SSH

Vlastnost	TELNET	SSH (Standard ZIF)
Bezpečnost	Žádná (otevřený text)	Silné šifrování (**TLS** úrovně)
Autentizace	Heslo	Heslo, Klíče, Biometrie
Port	23	22
Vhodné pro	Lokální testování portů	Vzdálená správa **VPS**

Bezpečnostní opatření

V rámci **kybernetické bezpečnosti** vynucujeme následující:

- **Blokování na bráně:** Naše brány **UTM** automaticky blokují veškerý TELNET provoz přicházející zvenčí.
- **Povinná migrace:** Všechny nové systémy v rámci našeho **VPC** musí mít TELNET službu deaktivovanou ve prospěch SSH.
- **Logování:** Každý pokus o použití portu 23 je zaznamenán v našem monitorovacím systému pro detekci potenciálního vnitřního útočníka.

> **Pravidlo pro administrátory:** Pokud zařízení podporuje SSH, je zakázáno používat TELNET. V případě nutnosti použít TELNET pro konfiguraci starého HW, musí být relace ukončena ihned po provedení změn.

— **Související stránky:** ZIF, TTY, SSH, WAN, IT Podpora, WWW, IoT zařízení, VPS, UTM, VPC, Kybernetická bezpečnost