TOR (The Onion Router)

TOR je svobodný software a otevřená síť, která umožňuje uživatelům anonymní komunikaci na internetu. Funguje na principu „cibulového směrování“, kdy jsou data několikrát zašifrována a přenášena přes sérii dobrovolnických uzlů (relays) po celém světě.

V rámci naší **digitální architektury** pohlížíme na TOR především jako na nástroj, který vyžaduje zvýšenou pozornost ze strany **kybernetické bezpečnosti**.

Jak TOR funguje?

Místo přímého spojení mezi vaším prohlížečem a cílovou **URL** adresou probíhá komunikace přes tři vrstvy:

```
1. **Vstupní uzel (Guard node):** Vidí vaši skutečnou IP adresu, ale neví, co posíláte.
2. **Střední uzel (Middle node):** Neví, kdo jste, ani kam data jdou. Pouze předává data dál.
3. **Výstupní uzel (Exit node):** Rozšifruje poslední vrstvu a pošle požadavek na cílový server. Cílový server vidí pouze IP adresu tohoto uzlu, nikoliv vaši.
```

Vztah k naší firemní síti

1. Bezpečnostní rizika a monitorování

V rámci naší sítě **WAN** je používání TOR prohlížeče standardně omezeno. Naše brány **UTM** sledují pokusy o navázání spojení s TOR uzly, protože:

- **Exfiltrace dat:** TOR může být zneužit k anonymnímu vynesení citlivých dat mimo naše **VPC**, aniž by byla zachycena jejich cílová destinace.
- **Malware:** Některé druhy ransomware využívají síť TOR ke komunikaci s řídicími servery (C&C).
- **Obcházení filtrů:** Umožňuje uživatelům přistupovat k blokovaným webům, což obchází naše bezpečnostní politiky.

2. Využití při penetračním testování

Náš **Vývojový tým** a bezpečnostní analytici mohou TOR využívat v izolovaném prostředí pro:

- **Testování odolnosti:** Ověřování, zda naše veřejné **WWW** služby správně filtrují anonymizovaný provoz.
- **OSINT analýzu:** Sledování úniků dat na tzv. „Darknetu“ (weby s příponou `.onion`), aby se včas odhalilo případné ohrožení našich uživatelských **UID**.

Srovnání: TOR vs. VPN vs. Proxy

Technologie	Anonymita	Rychlost	Hlavní účel
VPN	Střední (poskytovatel vás vidí)	Vysoká	Bezpečné připojení do **VPC**.
Proxy	Nízká (pouze skryje IP)	Velmi vysoká	Mezipaměť (Cache) a základní filtr.
TOR	Velmi vysoká (decentralizovaná)	Nízká	Maximální soukromí a obcházení cenzury.

Správa a pravidla IT podpory

Pro zaměstnance platí tato pravidla spravovaná přes **IT podporu**:

- **Instalace:** Instalace TOR prohlížeče na firemní laptopy podléhá schválení a mechanismům **UAC**.
- **Výjimky:** Pokud vaše práce vyžaduje anonymní výzkum, musí být prováděn v dedikovaném **virtuálním stroji** s odděleným síťovým přístupem.
- **Logování:** I když je obsah komunikace v TORu šifrován, samotný fakt, že se zařízení připojilo k síti TOR, je v našich systémech logován.

> **Upozornění:** Používání sítě TOR pro soukromé účely na firemních zařízeních je v rozporu s našimi vnitřními předpisy o používání výpočetní techniky.

— **Související stránky:** ZIF, Kybernetická bezpečnost, UTM, WAN, VPC, WWW, IT Podpora, Virtual Machine