TOR (The Onion Router)

TOR je svobodný software a otevřená síť, která umožňuje uživatelům anonymní komunikaci na internetu. Funguje na principu **„cibulového směrování“** (*onion routing*), při němž jsou data několikrát zašifrována a postupně přenášena přes sérii dobrovolně provozovaných **uzlů (relays)** rozprostřených po celém světě. Každý uzel odšifruje pouze jednu vrstvu šifry, čímž zajišťuje, že žádný jediný bod v síti nezná zároveň původ i cíl komunikace.

V rámci naší **digitální architektury** pohlížíme na TOR především jako na nástroj, který vyžaduje zvýšenou pozornost ze strany **kybernetické bezpečnosti** – jak z hlediska jeho legálního využití pro ochranu soukromí, tak z pohledu jeho možného zneužití v rámci anonymních útoků nebo distribuce nelegálních obsahů.

Jak TOR funguje?

Místo přímého spojení mezi vaším prohlížečem a cílovou **URL** adresou probíhá komunikace přes tři vrstvy uzlů, z nichž každá odhalí pouze minimální část informací:

```
1. **Vstupní uzel (Guard node):**
   Tento uzel je první v řetězci. Vidí vaši skutečnou **IP adresu**, ale nezná obsah přenášených dat ani jejich konečný cíl – data jsou v tomto bodě stále chráněna vícevrstvou šifrou.
```

```
2. **Střední uzel (Middle node):**
   Tento mezilehlý uzel nezná ani identitu původce komunikace, ani její cíl. Pouze přeposílá již částečně dešifrovaný tok dat k dalšímu uzlu.
```

```
3. **Výstupní uzel (Exit node):**
   Poslední uzel v řetězci odšifruje závěrečnou vrstvu a předá požadavek cílovému serveru. Cílový **[[webový server]]** tedy vidí pouze IP adresu výstupního uzlu, nikoli vaši skutečnou IP adresu. Na druhou stranu – pokud není komunikace dále chráněna (např. přes **[[HTTPS]]**), může vlastník výstupního uzlu číst nebo modifikovat přenášená data.
```

Důležité upozornění

Používání TOR sice zvyšuje **anonymitu** uživatele, ale není samo o sobě dostatečnou zárukou úplného soukromí. Pro maximální bezpečnost je důležité:

- vždy používat **HTTPS** (ideálně s rozšířením **HTTPS Everywhere**),
- nepoužívat torrenty přes TOR,
- nezadávat osobní údaje v prohlížeči TOR,
- nepoužívat TOR v kombinaci s jinými aplikacemi (např. běžným prohlížečem) ve stejnou dobu, což by mohlo vést k korelaci aktivity.

Související pojmy

- Anonymita
- Cenzura
- Dark Web
- Šifrování
- Proxy server
- VPN

Externí zdroje

- Oficiální stránky projektu: https://www.torproject.org/
- Dokumentace ke konfiguraci TOR Bridge: https://bridges.torproject.org/
- TOR Browser – bezpečný prohlížeč založený na Firefoxu: https://www.torproject.org/download/