Anonymita v digitálním prostředí

Anonymita je stav, kdy identita subjektu (uživatele, zařízení nebo procesu) není známa v rámci určité sady subjektů. V naší **digitální infrastruktuře** rozlišujeme mezi anonymitou navenek (vůči internetu) a interní identifikací (vůči našim systémům), která je nezbytná pro audit a **kybernetickou bezpečnost**.

Úrovně identity v naší síti

V rámci firemních procesů pracujeme s různými úrovněmi identifikace:

- **Identifikovaný stav:** Uživatel je přihlášen pod svým **UID**, jeho aktivita v systému **Jira** je logována.
- **Pseudonymita:** Uživatel vystupuje pod přezdívkou nebo ID, které přímo neodhaluje jeho jméno, ale v případě potřeby (např. bezpečnostní incident) jej **IT Podpora** dokáže dohledat.
- **Anonymita:** Systém neví, kdo požadavek poslal. V naší síti je tento stav u zaměstnanců nežádoucí z důvodu bezpečnosti.

Technologie pro zajištění anonymity

Náš **Vývojový tým** a bezpečnostní experti pracují s těmito nástroji pro ochranu soukromí a anonymizaci:

1. TOR (The Onion Router)

Jak bylo popsáno v sekci **TOR**, tato síť poskytuje nejvyšší míru anonymity pomocí vícevrstvého šifrování. V našem **VPC** je její použití omezeno na specifické bezpečnostní analýzy.

2. VPN (Virtual Private Network)

VPN skryje vaši IP adresu před cílovým serverem, ale poskytovatel VPN (naše firma) stále ví, kdo jste. Slouží k bezpečnému přenosu dat, nikoliv k úplné anonymitě.

3. Proxy servery

Fungují jako prostředník. Cílová **WWW** stránka vidí IP adresu proxy serveru, nikoliv vašeho počítače.

Anonymizace dat (Data Masking)

Při provádění **UAT** (akceptačních testů) je kritické pracovat s anonymizovanými daty:

- **Odstranění PII:** Odstraňují se osobně identifikovatelné údaje (jména, rodná čísla).
- **Zástupná data:** Místo reálných **UID** se používají náhodně generované řetězce nebo **UUID**.
- **Agregace:** Data se prezentují pouze jako celky (např. „10 uživatelů z Brna“) bez možnosti identifikovat jednotlivce.

Rizika anonymity pro firmu

V rámci **kybernetické bezpečnosti** představuje nekontrolovaná anonymita riziko:

- **Nemožnost auditu:** Pokud dojde k úniku dat z **VCS**, musíme být schopni identifikovat zdroj průniku.
- **Shadow IT:** Používání anonymizačních nástrojů k obcházení firemních filtrů na bráně **UTM**.
- **Právní compliance:** Musíme být schopni doložit, kdo má přístup k citlivým datům zákazníků.

> **Důležité pravidlo:** Anonymita na internetu neznamená beztrestnost. Veškerý provoz odcházející z naší sítě **WAN** prochází firemním firewallem, který monitoruje metadata spojení pro ochranu celé společnosti.

— **Související stránky:** ZIF, TOR, VPN, Kybernetická bezpečnost, IT Podpora, UID, UAT, UTM, WWW