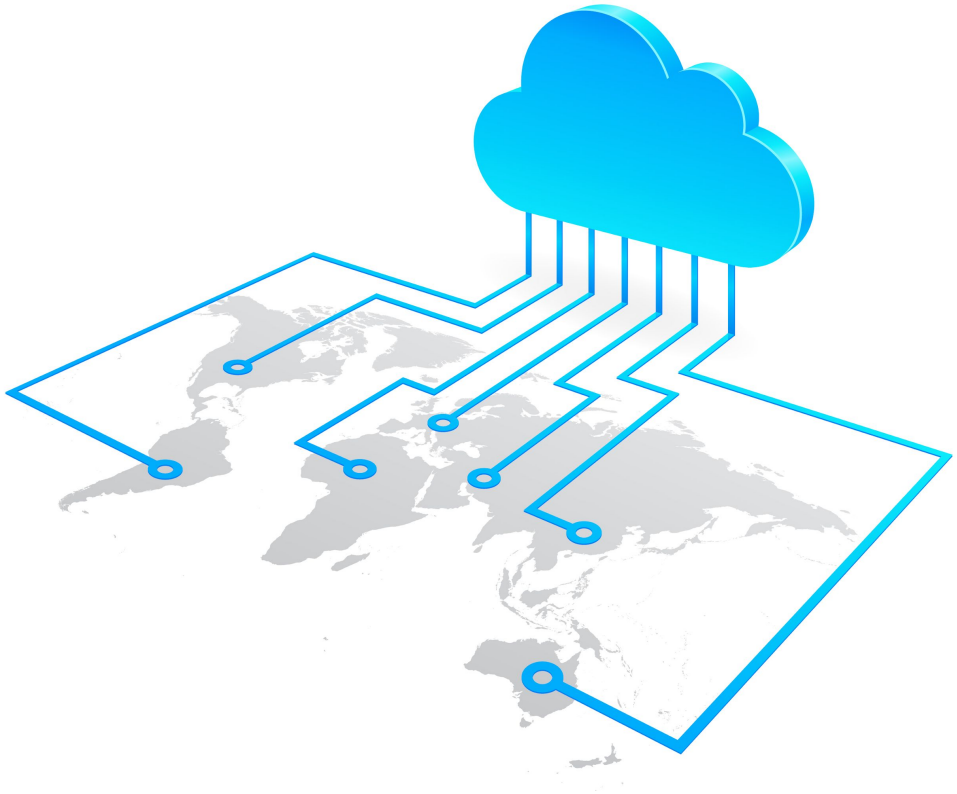
Bezpečnost cloudů a výpočetních center

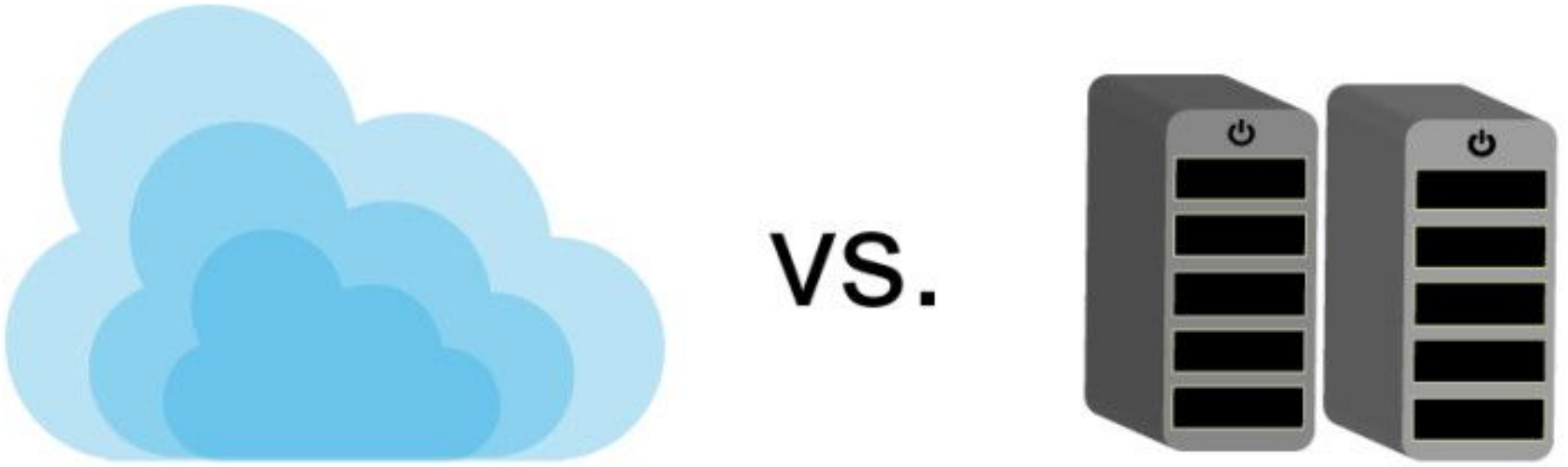
Jan Pluskal, Kamil Jeřábek

Co je to Cloud?

- Definice cloudu *The NIST Definition of Cloud Computing*
- Rozsáhlá síť vzájemně propojených vzdálených serverů po celém světě
- Rozlišujeme
  - Charakteristické vlastnosti
  - Modely nasazení
  - Modely služeb



Cloud vs klient-server



Charakteristické vlastnosti

- Samoobsluha podle potřeby
- Široká dostupnost přes síť
- Sdílení prostředků
- Rychlá pružnost
- Měřená spotřeba

Modely nasazení

- Veřejný
  - Služba poskytnuta široké veřejnosti
- Soukromý
  - Služba pouze v rámci jedné společnosti, či více společnostem samostatně
- Hybridní
  - Kombinace soukromého a veřejného
  - Navenek veřejné, propojené mezi sebou
- Komunitní
  - Infrastruktura sdílena mezi několika organizacemi

Modely služeb

- SaaS - Software as a Service
  - Určeno pro koncové uživatele
  - Nezávislost na koncovém zařízení
  - Např. Gmail, Facebook, Dropbox
- PaaS - Platform as a Service
  - Použití vývojáři (neviditelné pro uživatele)
  - Prostředí pro vývoj aplikací v různých jazycích
  - Např. Google App Engine, Red Hat OpenShift
- IaaS - Infrastructure as a Service
  - Poskytnutí celé infrastruktury
  - Virtuální datové centrum
  - Např. Google Compute Engine, Microsoft Azure Virtual Machines

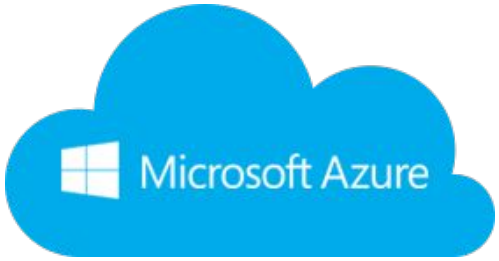
Výhody - obecně

- Menší výdaje za údržbu
- Rychlý vývoj aplikací
- Dostupnost
- Menší limitace zdroji (výpočet, úložiště)
- Rychlé přizpůsobení se potřebám zákazníka
- Jednoduché rozhraní pro správu

Nevýhody - obecně

- Veškerá data pod správou třetí strany
- Bezpečné tak jak poskytne zprostředkovatel služby
- Závislost na poskytovateli
- Dostupnost pouze přes síť
- Rozlišný právní řád (poskytovatel vs. klient)

Poskytovatelé



Zabezpečení výpočetních center

Hrozby

- Email
  - spam, podvržené emaily
- Web
  - phishing, web s malwarem
- File sharing
  - malware
- Síť
  - botnet, DDoS
- Data
  - ztráta, narušení integrity

...

Bezpečnostní politika

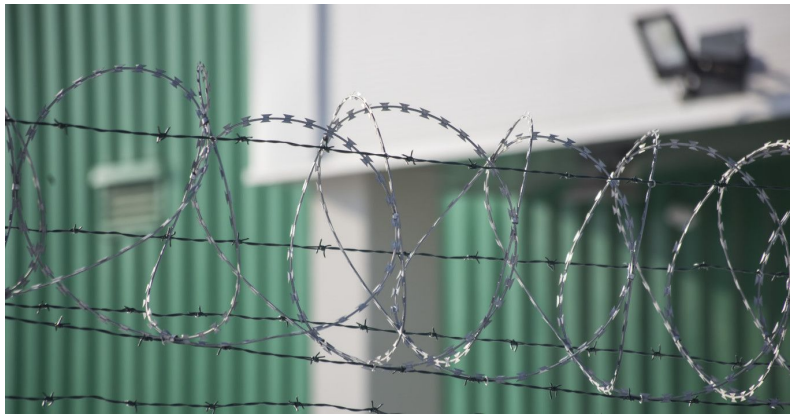
- Dokument s pravidly, kterými se musí řídit lidé s přístupem k firemním technologiím a informacím
  - Vedoucí pracovníci
  - Síťoví a bezpečnostní administrátoři
  - Lidé řešící bezpečnostní incidenty
  - Skupiny běžných uživatelů
  - Právní oddělení
- Vymezení co je povoleno a zakázáno, postup při bezpečnostních incidentech
- Soubor pravidel a postupů

Zabezpečení přístupu

- Ověření totožnosti (**Autentizace**)
- Ověření povolení přístupu (**Autorizace**)
- Účtování (**Accounting**)

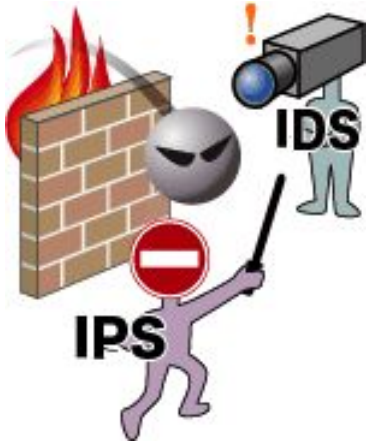
- Ověření stran
  - Jednosměrná (Telnet, FTP, HTTP)
  - Obousměrná (SSH, HTTPS)
  - Přímé ověření
  - Přes důvěryhodnou třetí stranu (Kerberos, veřejný klíč, …)

Fyzické zabezpečení a omezení přístupu



Zabezpečená komunikace

- Šifrovaná komunikace
  - HTTPS, SSH
- Firewall
- IDS (Intrusion Detection System)
  - Schopnost detekovat útoky proti síťovým zdrojům
  - Pasivní obranný mechanismus
  - Na systému či na lince
- IPS (Intrusion Prevention System)
  - schopnost zastavit útoky proti síťovým zdrojům
  - Aktivní obranný mechanismus - Detekce, Reakce, Prevence
  - Na lince
- Dostupnost



Zabezpečení dat

- Šifrovaná data na disku
- Oddělený prostor
- Duplikace
- Zálohování

Fappening