



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



KOMPETENČNÉ CENTRUM
KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnosť cloudu

Moderné technológie, bezpečnosť cloudu a IoT (Blok VII)
Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Marek Moravčík

KC KYB UNIZA, <https://kc.uniza.sk/>

marek.moravcik@fri.uniza.sk



Obsah

- Cloudové modely
 - SaaS, PaaS, IaaS
- Zásady bezpečnosti v cloude



Evolúcia a dôvera v cloud

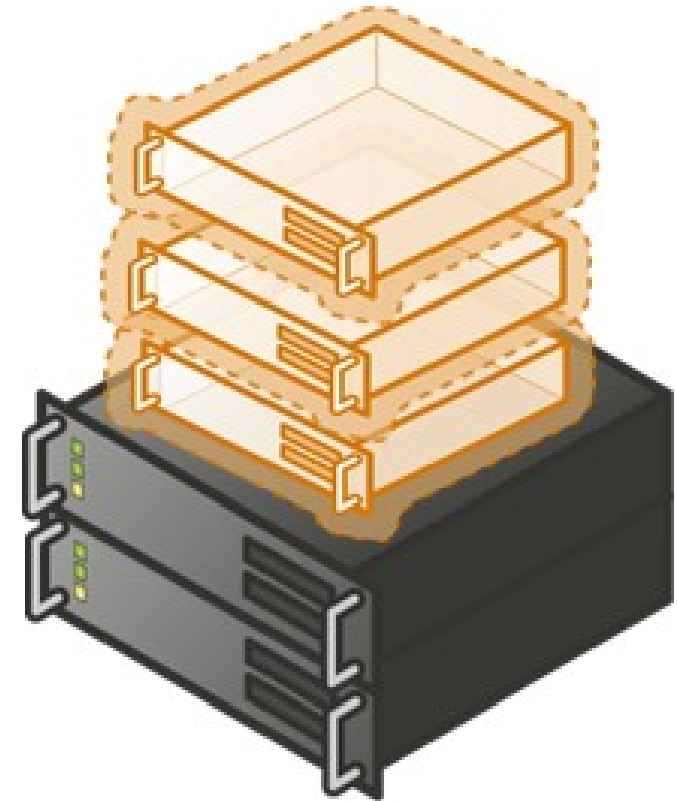
- a. Vývoj cloudových služieb a ich význam
- b. Dôvera a riziká spojené s používaním cloudu

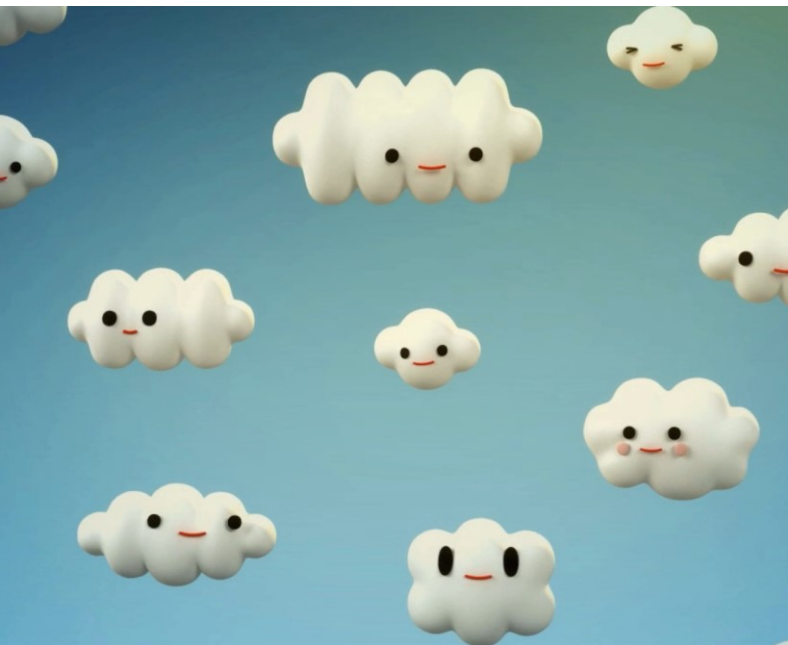
História Cloud Computingu (CC)

- 1960s – Základy: Mainframe + terminály
 - Používali sa mainframe počítače s viacerými „hlúpymi“ terminálmi – centrálné spracovanie dát pre viac používateľov = predchodca cloudu.
- 1990s – Virtualizácia & sieťové služby
 - Vývoj virtualizácie (napr. VMware v 1998) umožnil, aby na jednom fyzickom serveri bežalo viac virtuálnych strojov (VM).
 - Prvé služby typu Application Service Providers (ASP) – predchodcovia dnešného SaaS.
- 2006 – Oficiálny zrod moderného cloudu
 - Amazon Web Services (AWS) spúšťa EC2 (Elastic Compute Cloud) – prvá masovo dostupná cloud infraštruktúra na požiadanie.
 - Model IaaS (Infrastructure as a Service) sa stáva realitou – firmy si nemusia kupovať vlastné servery.

Virtualizácia

- Spúšťanie logicky oddelených programov (OS) na jednom fyzickom zariadení
- Fyzický stroj – host
- Virtuálny stroj – guest (virtual machine - VM)
- Každá VM má
 - „pocit“, že beží na vlastnom HW
 - Vlastnú vRAM
 - Vlastný priestor na HDD
 - Vlastnú MAC a IP



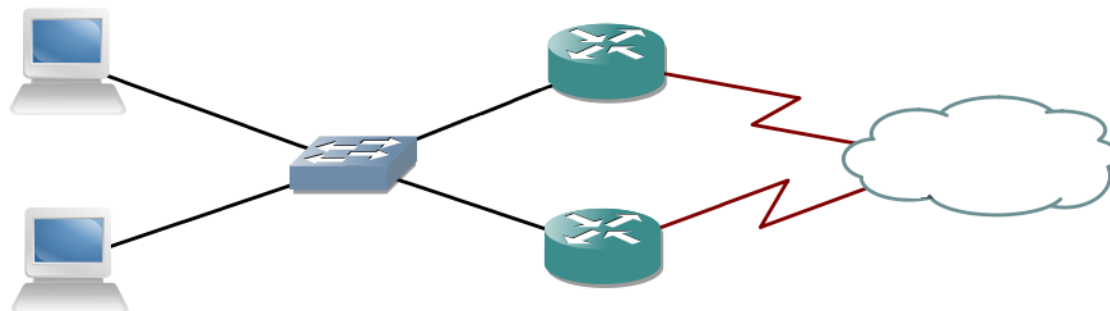


Cloudové modely

Cloud Computing (CC)

- Zdieľaný výpočtový výkon na niekoľkých zariadeniach
- Zákazník platí za službu, nie za softvér
- Pre zákazníka sa javí ako nekonečný priestor

- Prečo slovo cloud?
- V diagramoch sieťových topológií sa obláčikom znázorňuje Internet, resp. niečo ďaleko, mimo vlastnej siete

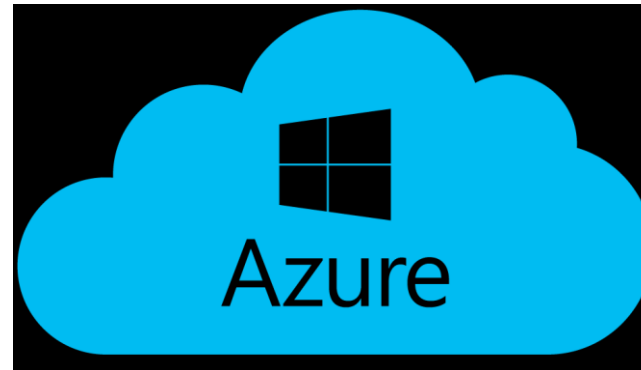


Modely CC

- Privátny cloud
 - Využívaný jednou organizáciou pre vlastné potreby
 - OpenStack, VMware ESX/ESXi
- Komunitný cloud
 - Využívaný skupinou s rovnakým spoločným záujmom
 - Prepojenie univerzít v rámci jedného výskumu
- Verejný cloud
 - Ponúkaný verejnosti
 - Amazon Web Services, Microsoft Azure
- Hybridný cloud
 - Kombinácia predošlých

Poskytovatelia verejného cloudu

- AWS – Amazon Web Services
- Microsoft Azure
- DigitalOcean
- Google cloud
- Alibaba cloud



Google Cloud Platform

Služby v CC

- Softvér ako služba (SaaS)
- Platforma ako služba (PaaS)
- Infraštruktúra ako služba (IaaS)

- Podmnožiny služieb
 - FwaaS – Firewall
 - LBaaS – Load Balancer
 - DNSaaS – Domain Name Service
 - ...

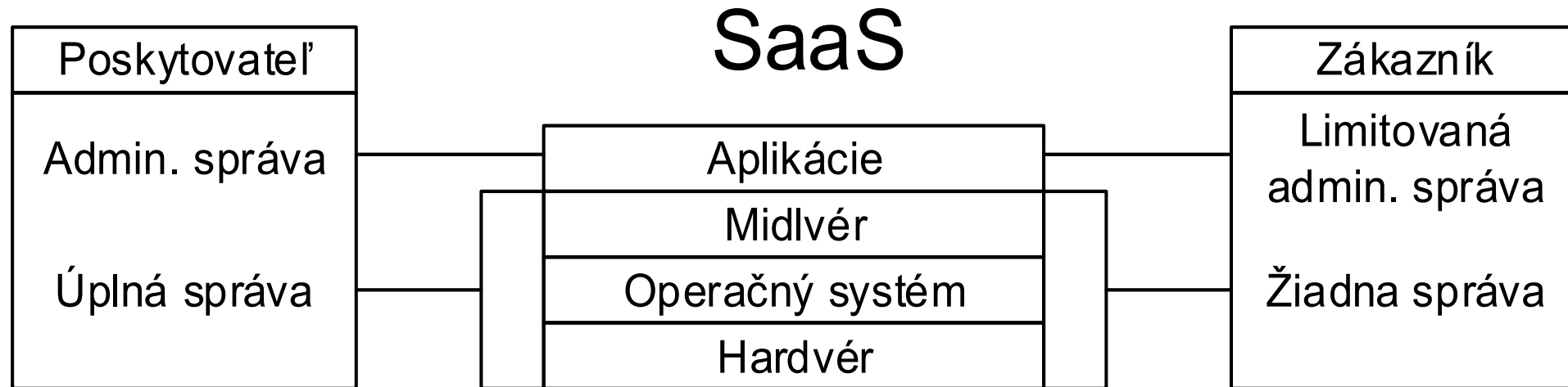
- Čokoľvek ako služba (XaaS)

Software as a Service (SaaS)

- Aplikácie dostupné cez web rozhranie, alebo klientske aplikácie
- Úložný priestor
 - Google Drive
 - Dropbox
 - MS OneDrive
- Kancelárske prostredie
 - MS Office 365
- Informačný systém
 - SAP



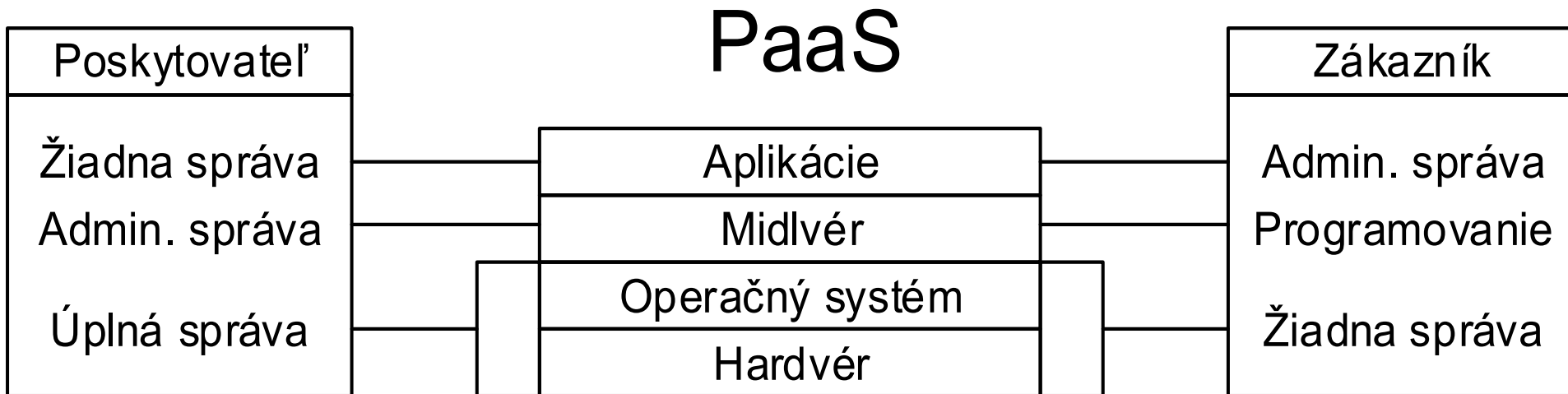
Kompetencie v CC prostredí



Platform as a Service (PaaS)

- Prostredia na beh vlastných aplikácií
- Java virtual machine
- .net prostredia
- Databázy
- Autentifikácia, Autorizácia (AAA)
- Spravidla prostredia určené vývojárom

Kompetencie v CC prostredí



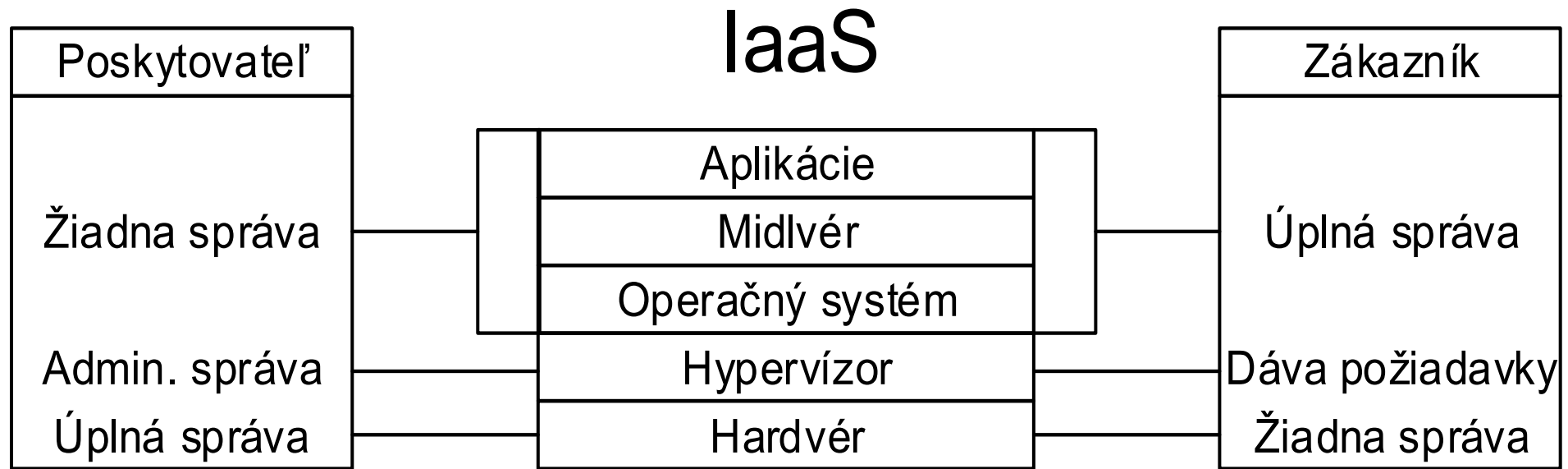
Infrastructure as a Service (IaaS)

- Poskytovateľ poskytuje „len pripojenie k internetu“
- Celková administrácia prostredia je na zákazníkovi

- Priestor pre vlastné virtuálne mašiny
- Virtuálne siete
- Firewall-ing
- Rozkladanie záťaže

- Pre skúsených administrátorov

Kompetencie v CC prostredí





Zásady bezpečnosti v cloude

Bezpečnosť používateľských dát

- Všeobecne je cloud prostredie geograficky nepredvídateľné
 - Používateľ presne nevie, kde má uložené dáta
- Poskytovateľ má prístup k dátam
 - Má ich na svojich serveroch
- Citlivé údaje je potrebné šifrovať vlastníkom
 - Šifrovanie dát pri prenose / samotného prenosu (Encryption in transit)
 - Šifrovanie uložených dát (Encryption at rest)

Šifrovanie dát pri prenose (Encryption in transit)

- Bezpečnostná technika, ktorá chráni dáta tým, že ich zašifruje **počas presunu** z jedného miesta na druhé – napríklad medzi používateľovým zariadením a serverom, medzi dvoma servermi, alebo medzi cloudovými službami.
- Účel: Zabrániť tomu, aby útočník mohol zachytiť a čítať prenášané dáta (napr. prostredníctvom „man-in-the-middle“ útoku)
- Technológie: Bežne sa používa TLS (Transport Layer Security) alebo jeho predchodca SSL

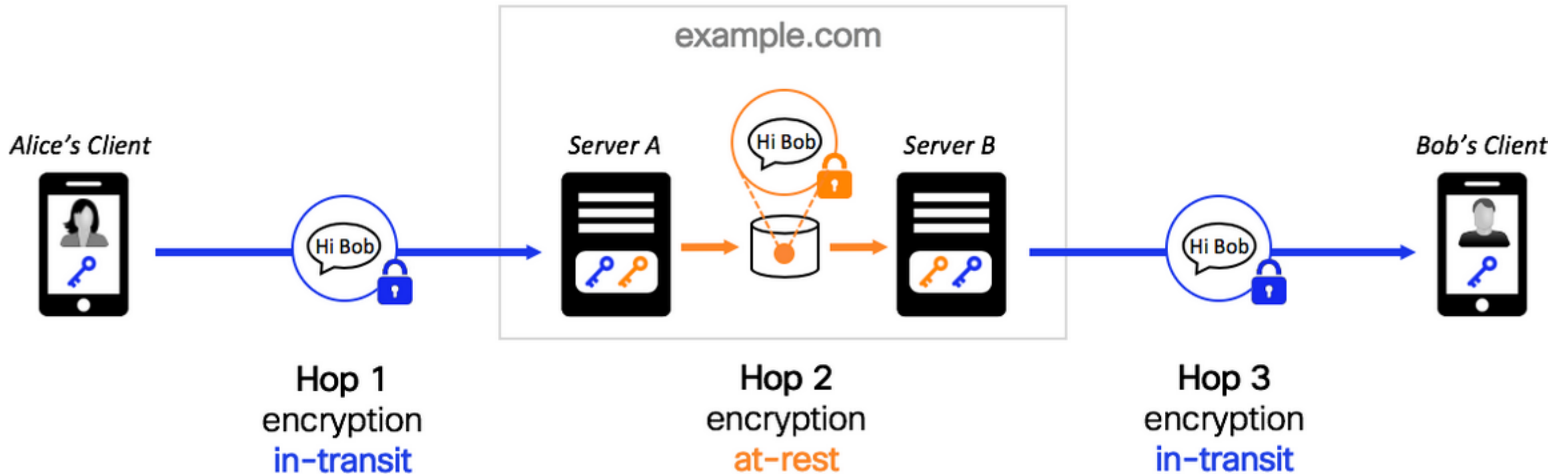
Šifrovanie uložených dát (Encryption at rest)

- Bezpečnostná technika, ktorá chráni uložené dáta pred neoprávneným prístupom – napríklad na pevných diskoch, SSD, USB kľúčoch, databázach alebo v cloude
- Znamená, že **dáta sú zašifrované, keď sú uložené** na zariadení alebo serveri – teda keď sa práve neprenášajú alebo nespracúvajú
- Prečo sa používa?
 - Ochrana dát pred krádežou, ak by niekto získal fyzický prístup k úložisku (napr. ukradnutý disk, server)
 - Splnenie bezpečnostných a legislatívnych požiadaviek (napr. GDPR, HIPAA)
 - Zamedzenie úniku citlivých informácií (napr. heslá, osobné údaje, čísla kariet)

Šifrovanie uložených dát (Encryption at rest)

- Účel: Zabrániť tomu, aby útočník mohol získať dáta, ak získa prístup k zariadeniu
 - Získanie prístupových údajov do PC, servera, databázy, ...
 - Krádež/strata notebooku, USB, ...
- Technológie používané pre šifrovanie at rest:
 - AES-256 (Advanced Encryption Standard) – často používaný štandard
 - BitLocker (Windows), FileVault (macOS), LUKS (Linux)
 - Šifrovanie databáz: napr. Transparent Data Encryption (TDE) pre SQL databázy
 - Cloudové riešenia ako AWS KMS, Azure Storage Encryption, Google Cloud KMS

Porovnanie šifrovaní



Zásady bezpečného používania cloudových služieb

- Používajte dôveryhodné/overené služby
 - Zvoľte si renomované cloudové služby (napr. Google, Apple, Microsoft)
- Šifrujte dáta
- Kontrolujte zdieľanie prístupov a oprávnení
 - Ak zdieľate súbory alebo priečinky v cloude, spravujte, kto má k nim prístup
 - Zabezpečte, aby ste poskytli prístup len tým, ktorí ho naozaj potrebujú
 - Pravidelne kontrolujte, kto má prístup k vašim dátam

Zásady bezpečného používania cloudových služieb

- Zálohujte svoje dáta
 - Ak máte možnosť, zálohujte dáta offline
- Monitorujte aktivitu
 - Mnoho cloudových služieb ponúka možnosť sledovať aktivitu na vašom účte
 - Monitorujte prihlásenia, prístup k súborom a vykonané zmeny, aby ste odhalili neautorizované prístupy
- Prečítajte si podmienky služby



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



KOMPETENČNÉ CENTRUM
KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť
Cloudové služby a ich bezpečnosť

Moderné technológie, bezpečnosť cloudu a IoT (Blok VII)
Kurz: **Špecialista kybernetickej bezpečnosti vo verejnej správe**

Marek Moravčík

KC KYB UNIZA, <https://kc.uniza.sk/>

marek.moravcik@fri.uniza.sk