Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Aplikačná bezpečnosť a bezpečnosť cloudových systémov

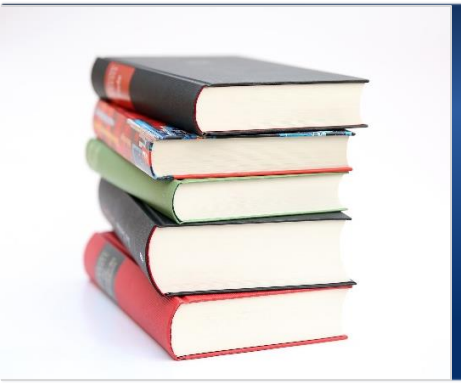
Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

Marek Moravčík

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

marek.moravcik@fri.uniza.sk



Obsah

- Zásady aplikačnej bezpečnosti
- Základy virtualizačných technológií, vývoja a údržby virtuálnych strojov
- Bezpečnostné riziká cloud computingu
- Zásady riadenia bezpečnosti prostredia cloudu

Zásady aplikačnej bezpečnosti

Vývoj aplikácií

- Bezpečné programovanie
  - Používať osvedčené bezpečnostné štandardy
  - Predchádzať bežným zraniteľnostiam (napr. SQL Injection, XSS)
  - Písať čistý, čitateľný a kontrolovateľný kód

- Overovanie vstupov
  - Nikdy neveriť vstupu od používateľa
  - Validácia vstupov na strane klienta aj servera
    - Príklad: Ochrana pred XSS útokom cez textové pole

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Verejné zoznamy zraniteľností

- OWASP
  - Open Worldwide Application Security Project - https://owasp.org/
  - Komunita poskytujúca informácie týkajúce sa najmä webovej bezpečnosti

- CVE
  - Common Vulnerabilities and Exposures - https://www.cve.org/
  - Formát je CVE-YYYY-NNNN (Napríklad CVE-2017-0144)

- KEV
  - Known Exploited Vulnerabilities
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako sa brániť?

- Aktualizácie softvéru
  - Pravidelné záplaty frameworkov, knižníc, doplnkov
  - Automatizované testovanie pri aktualizáciách

- Monitoring a logovanie
  - Sledovať, čo sa deje v aplikácii
  - Zaznamenávať chyby, pokusy o útoky, anomálie
  - Používať SIEM nástroje, notifikácie

- Nepoužívať staré knižnice, staré verzie softvérov

Aktívne sledovanie aplikácií

- Voľne dostupné, ako aj platené nástroje na aktívne skenovanie siete a aplikácií

- Nessus vulnerability scanner
  - Forky: OpenVAS, Greenbone Vulnerability Management (GVM)
- Burp Suite

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

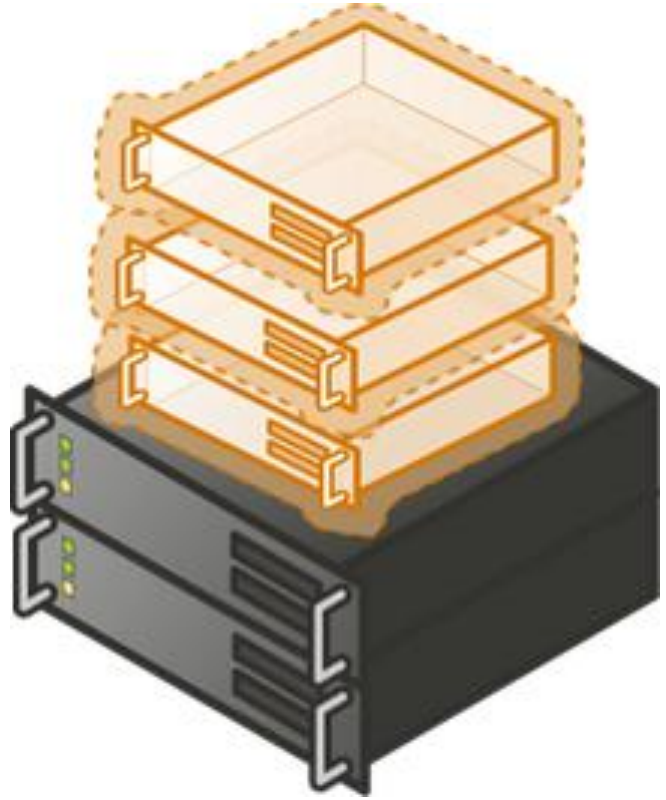
Základy virtualizačných technológií, vývoja a údržby virtuálnych strojov

Virtualizácia

- Spúšťanie logicky oddelených programov (OS) na jednom fyzickom zariadení

- Fyzický stroj – host
- Virtuálny stroj – guest (virtual machine - VM)

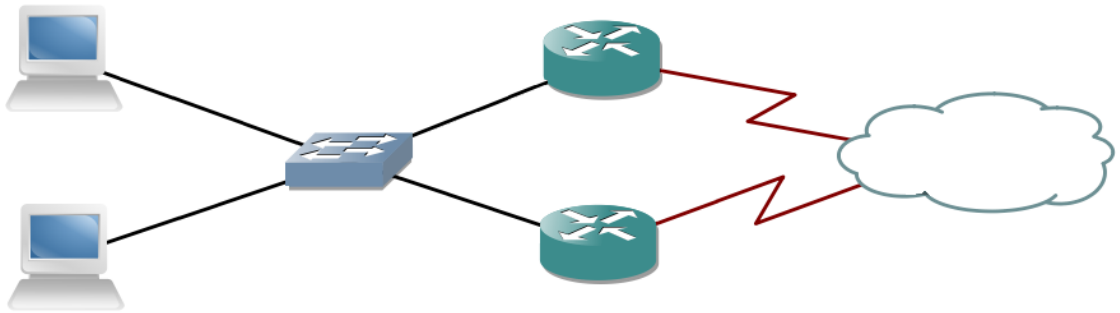
- Každá VM má
  - „pocit“, že beží na vlastnom HW
  - Vlastnú vRAM
  - Vlastný priestor na HDD
  - Vlastnú MAC a IP



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



História Cloud Computingu (CC)

- 1960s – Základy: Mainframe + terminály
  - Používali sa mainframe počítače s viacerými „hlúpymi“ terminálmi – centrálne 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

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

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)

Údržba VM a služieb v CC

- Koncový používateľ nevidí rozdiel vo „fyzickej“ a virtuálnej službe.

- Administrátor má viac možností práce s virtuálnou službou/VM
  - Zálohy/snapshoty
  - Živá migrácia
  - Škálovanie a klonovanie

- Vývojár má na výber viac prístupov k vývoju služby
  - Microservices
  - V prípade využívania verejných CC má možnosť použiť ich API/služby

Bezpečnostné riziká Cloud computingu

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)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

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)

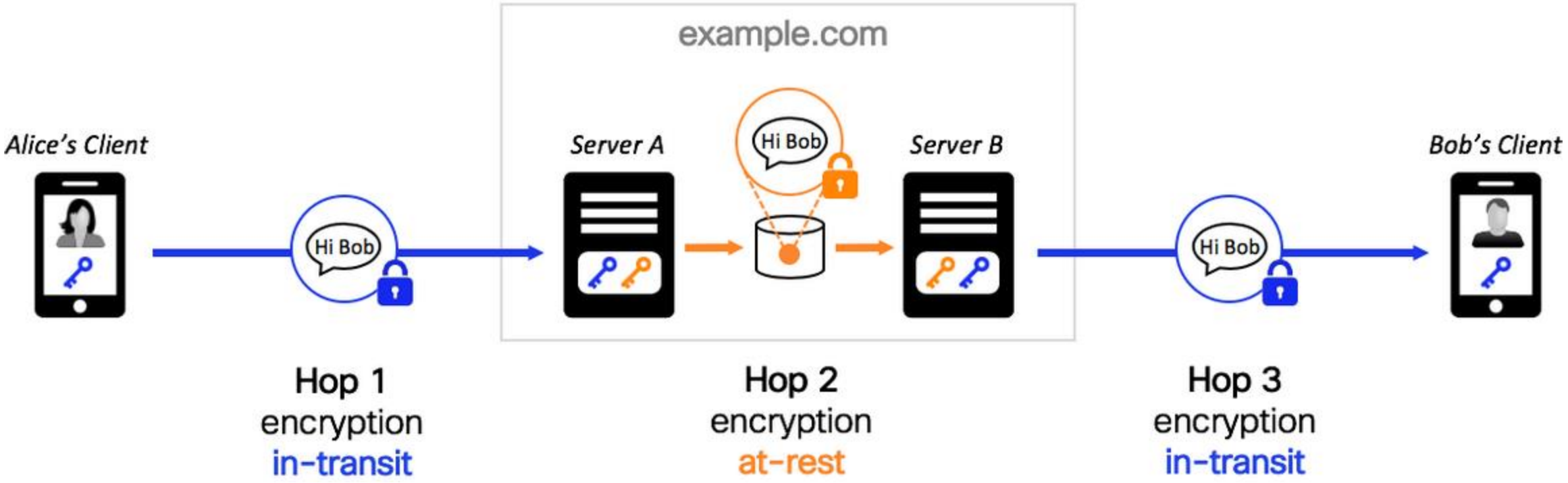
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

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 riadenia bezpečnosti prostredia cloudu

Zásady riadenia bezpečnosti prostredia cloudu

- Súbor pravidiel, odporúčaní a praktík

- Organizácia ich prijíma na zabezpečenie bezpečného a zodpovedného využívania cloudových služieb

- Cieľom je
  - minimalizovať riziká
  - zabezpečiť súlad s legislatívou a normami
  - podporovať efektívne riadenie informačnej bezpečnosti v cloudovom prostredí

Zodpovednosti v CC prostredí

- Definovanie zodpovedností medzi poskytovateľom cloudových služieb (CSP) a zákazníkom (organizáciou) – tzv. model zdieľanej zodpovednosti
- Zriadenie interných politík, ktoré určujú, kto má na starosti výber, správu a kontrolu cloudových služieb
- Pravidelné kontroly/audity, či sa dané politiky a smernice dodržiavajú

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

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

Aplikačná bezpečnosť a bezpečnosť cloudových systémov

Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

Marek Moravčík

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

marek.moravcik@fri.uniza.sk