kyndryl

Seminar Cloud Security AFCEA
Josef Krýcha

Cloud vs On-Premise Security

Josef Krýcha, CISSP, CCSP, CSSLP, CISA, CISM, CRISC

Bezpečnosti IT/ICT se věnuji od roku 2010

2010 - 2014	Státní správa
2014 - 2016	Bezpečnost ve finančním sektoru (ČSOB, Deutsche Bank)
od 2017	Konzultant bezpečnosti a bezpečného vývoje informačních systémů
2020 - 2022	Oracle
od 2022	Kyndryl

Obsah příspěvku

01 Rozdíly v pojetí bezpečnosti mezi **cloudovým** a **on-premise** modelem

02 Odlišná bezpečnostní rizika

03 Způsoby zabezpečení

Základní charakteristiky cloudových služeb

NIST SP 800-145 definuje “cloud” jako model umožňující snadný **síťový přístup** ke **sdíleným** a **konfigurovatelným** výpočetním prostředkům, které jsou poskytované s **minimální** potřebou řízení nebo **interakce** s poskytovatelem.

1. Síťový přístup
2. Služba na vyžádání (on-demand)
3. Sdílení zdrojů
4. Měřené služby

Související rizika

Odepření služby (DoS, DDoS)

Ztráta důvěrnosti a integrity dat

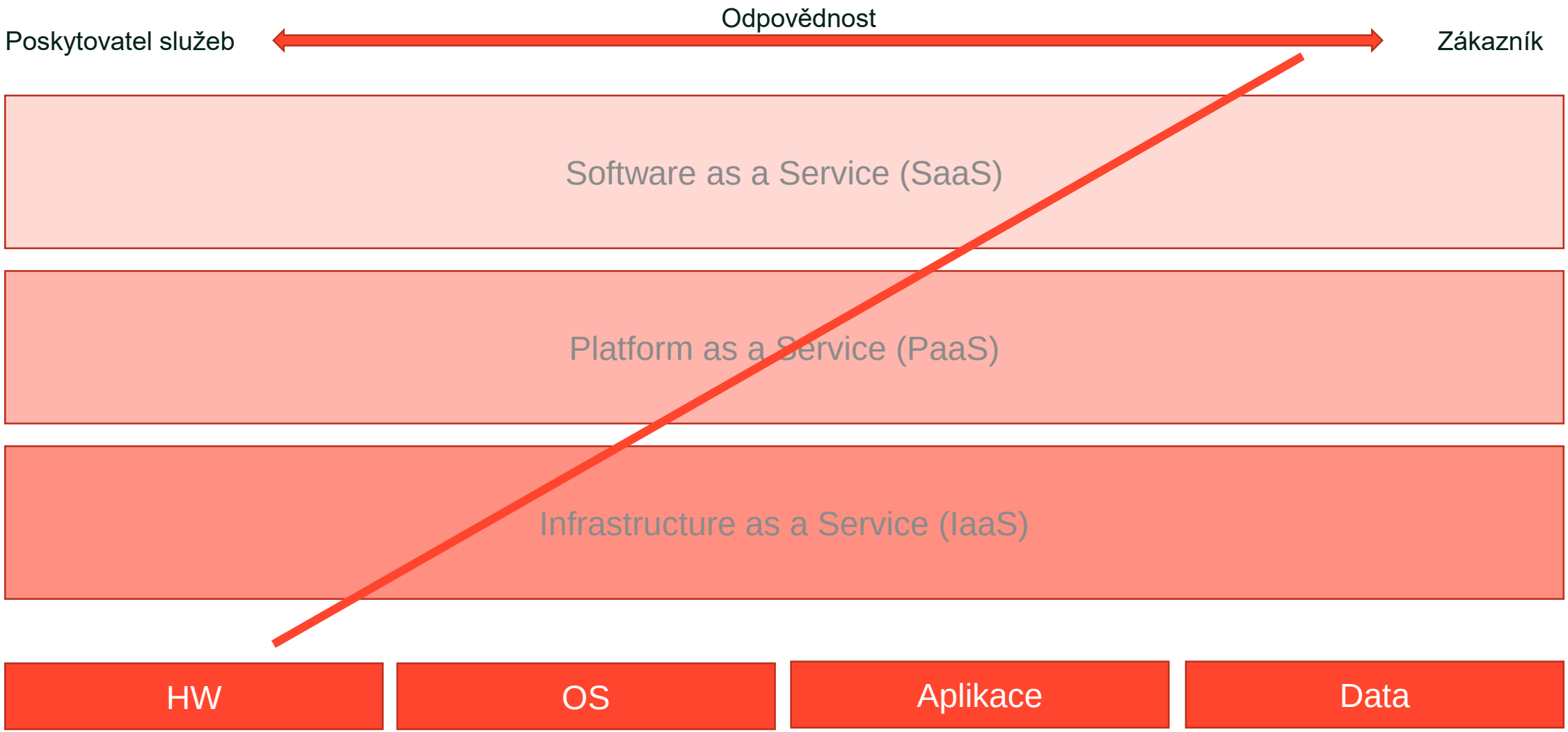
Ztráta dostupunosti dat

Soulad s legislativou a normami

Finanční ztráty

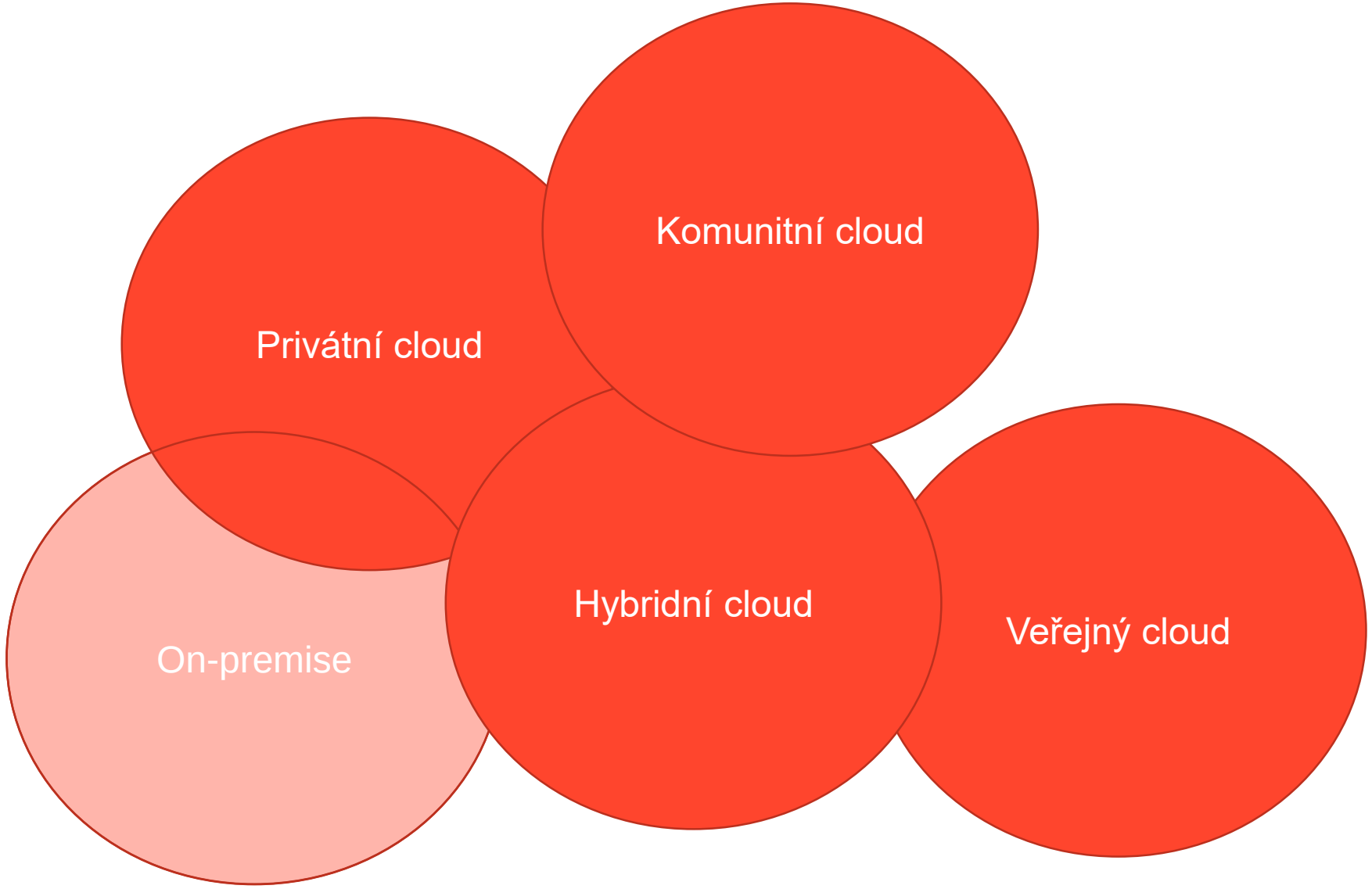
Rozdíly mezi cloud a on-premise řešením

Odpovědnost za bezpečnost podle modelu cloudové služby



Rozdíly mezi cloud a on-premise řešením

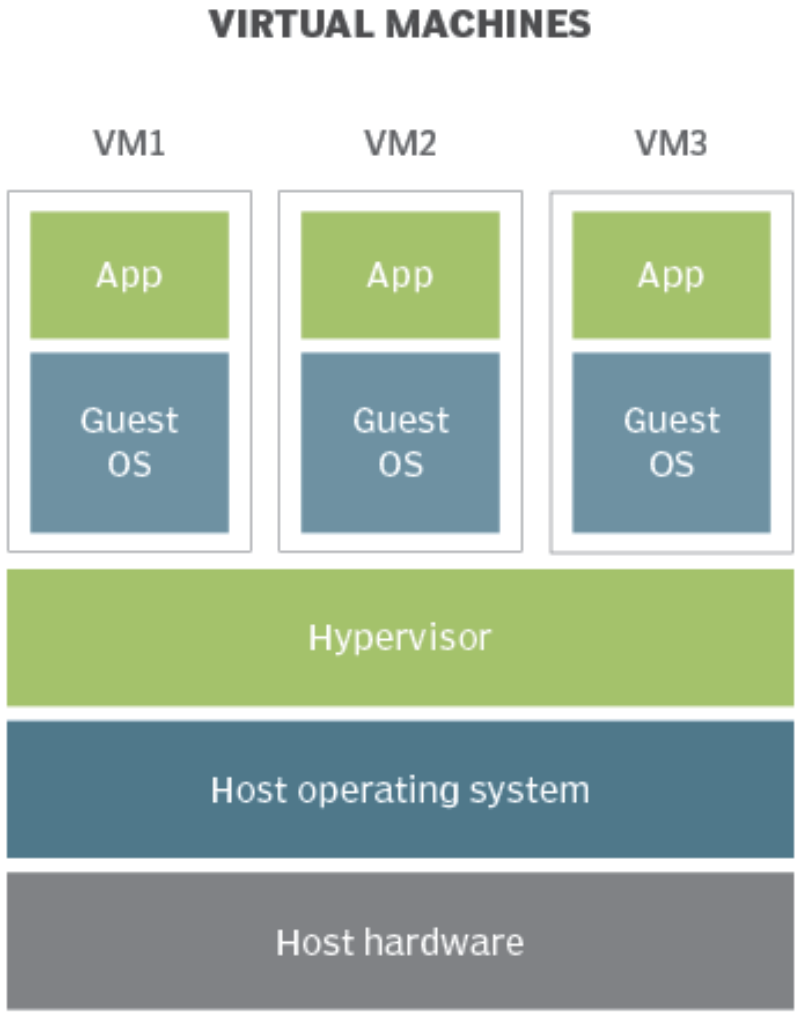
Rozdíly v zabezpečení podle modelu nasazení cloudu

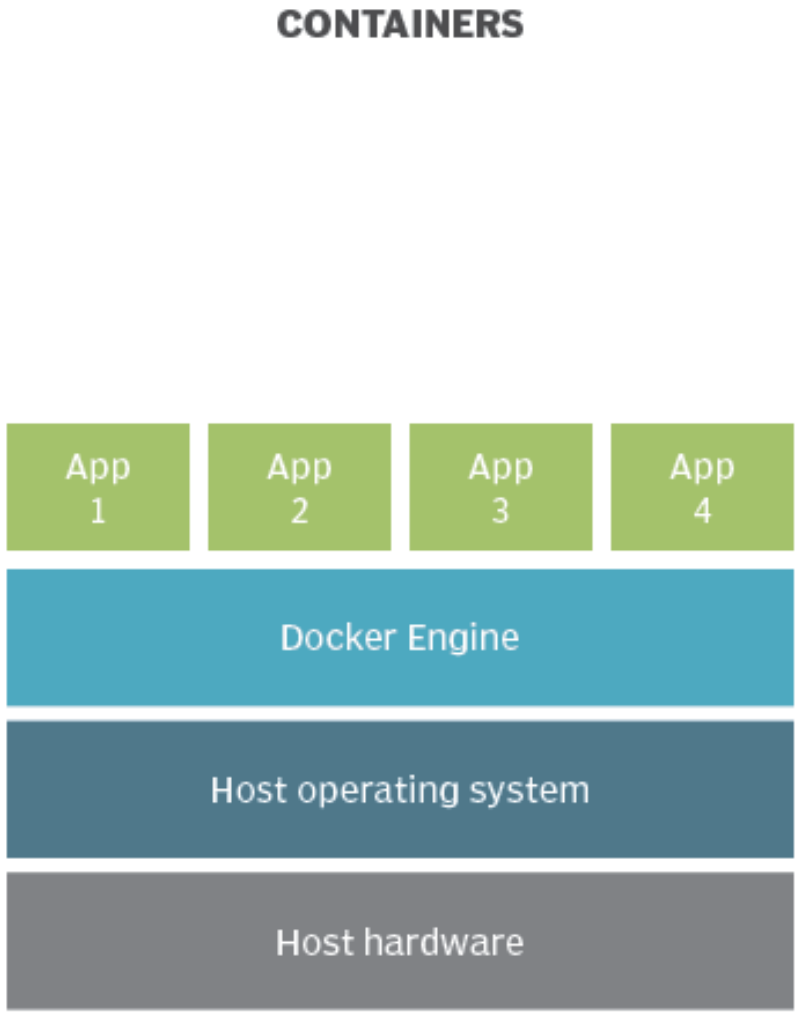


kyndryl

Rozdíly mezi cloud a on-premise řešením

Sdílení zdrojů: Úspora vs. Riziko

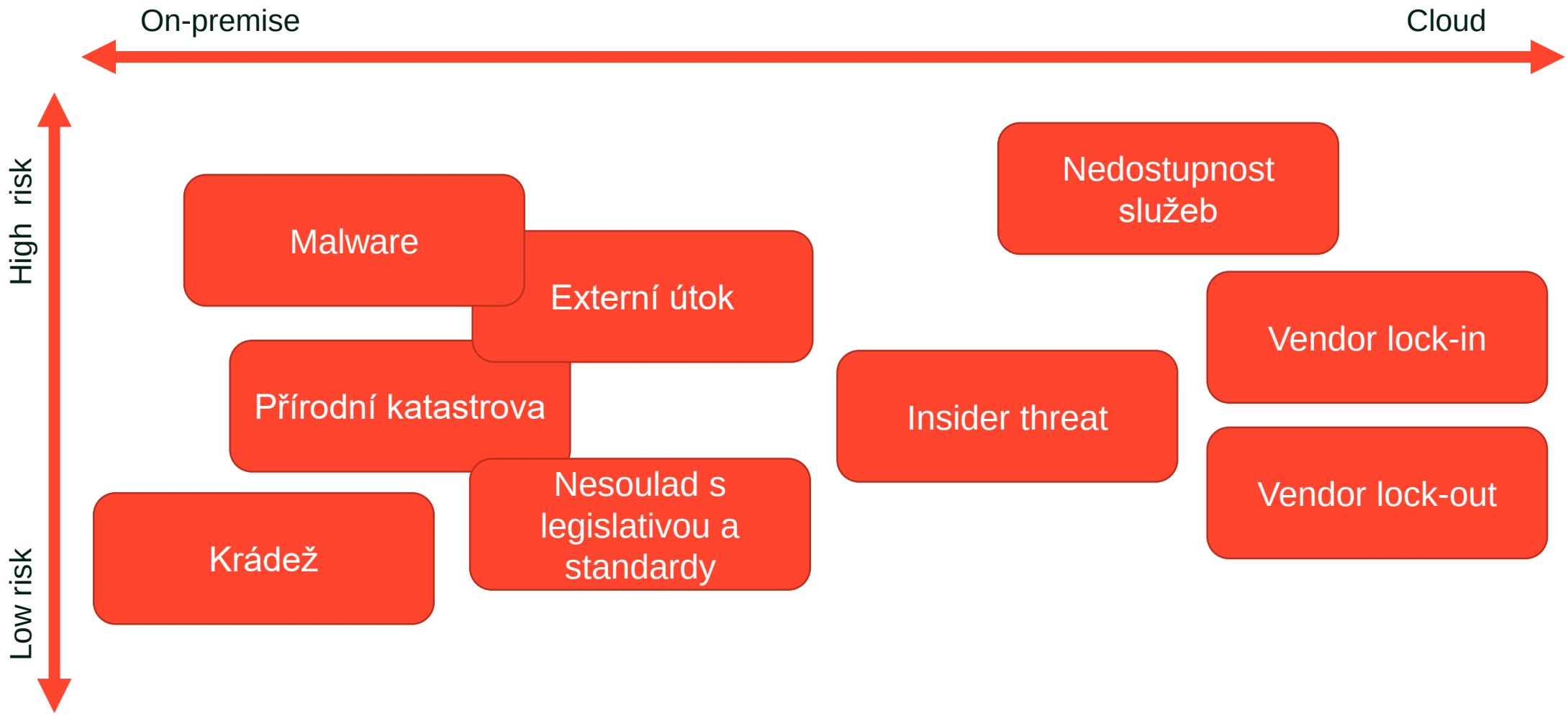




kyndryl

Odlišná bezpečnostní rizika

Porovnání rizik



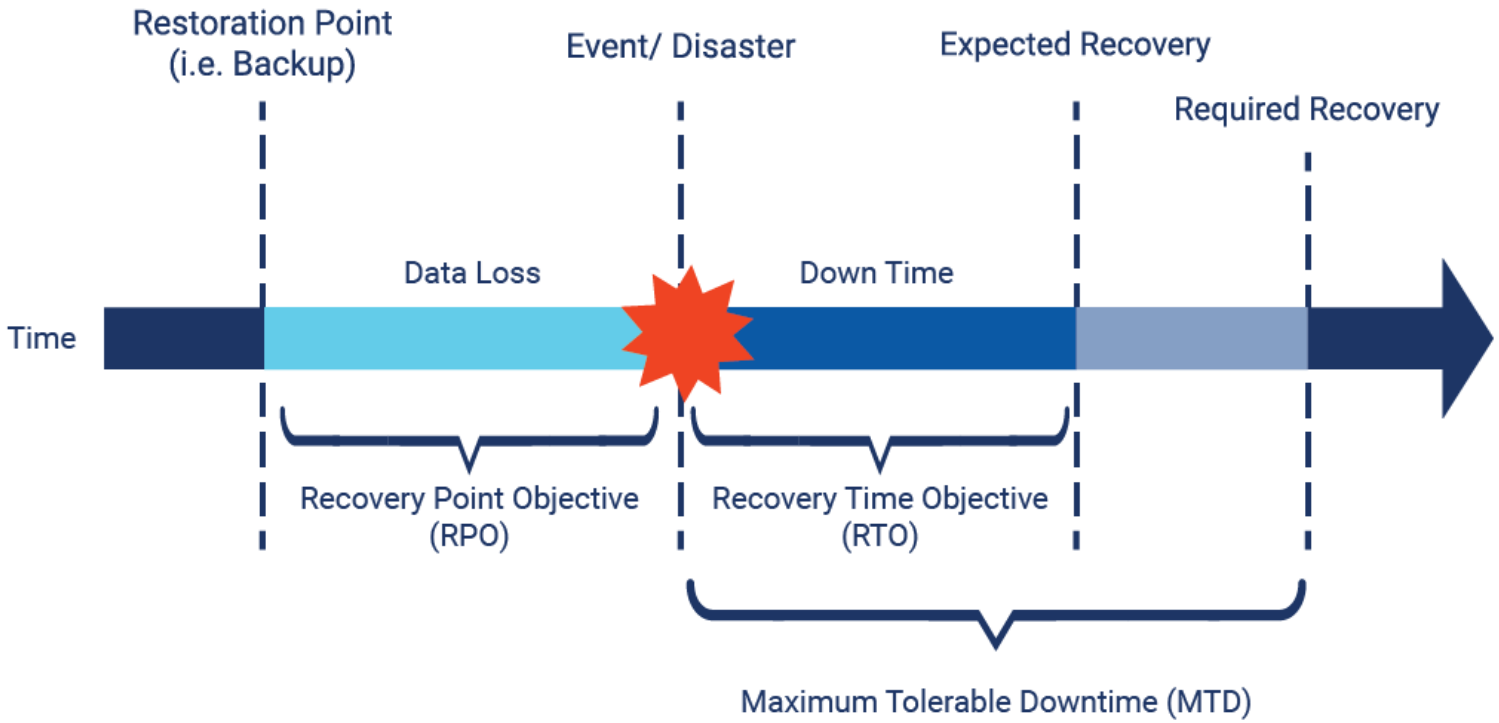
Způsoby zabezpečení

Jak mitigovat rizika při použití cloudových služeb?

1. Pečlivý výběr poskytovatele cloudových služeb

2. Jediné skutečně vymahatelné věci jsou:
   a. **Smlouva**
   b. **Service Level Agreement**
      - MTD
      - RTO
      - RPO
      - Propustnost
      - Dostupnost

3. Pojištění



kyndryl

Způsoby zabezpečení

Hodnocení bezpečnosti cloudových služeb

Cloud Controls Matrix (CCM):
https://cloudsecurityalliance.org/research/cloud-controls-matrix/
https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

A&A	Audit and Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption and Key Management
DCS	Datacenter Security
DSP	Data Security and Privacy
GRC	Governance, Risk Management and Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging and Monitoring
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

Děkuji za pozornost.

Q & A ?