MUNI
LAW

Bezpečnost cloudových technologií

Jakub Klodwig

15.5.2021

Proč cloud computing?

- Výdaje na ICT se v ČR mezi lety 2012 - 2016 téměř zdvojnásobily (monitor.statnipokladna.cz)
- Zavedení cloudových řešení ve veřejném sektoru může snížit provozní náklady na IT o 10 – 50 % (EY 2021)
- Průměrná doba návratnosti 6 měsíců (PwC)
- Přechodem na cloudové řešení lze zredukovat uhlíkové emise až o 30 – 90 % (Deloitte 2016)
- Výrazně pozitivní zkušenosti z VB či DN, kde byl zaveden státní eGC (Souhrnná analytická zpráva)

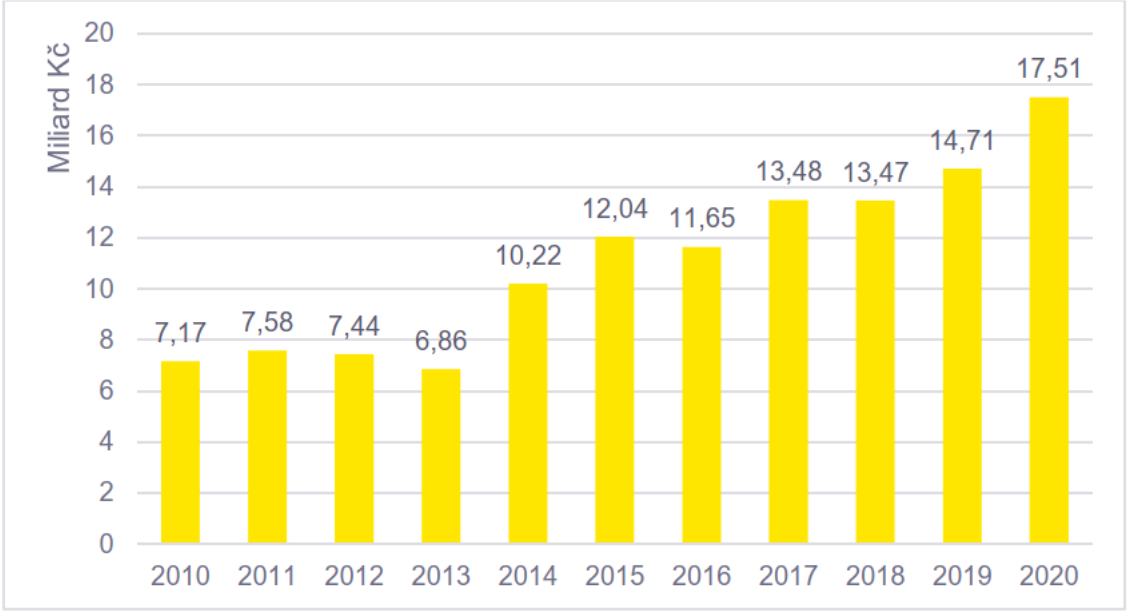
MUNI LAW

Etablování cloud computingu

- Světový trh CC v roce 2020 371.4 mld. USD
- Český trh CC v roce 2019 rostl o 27 % na 19 mld. Kč

- Rychlá, dostupná, škálovatelná, levná
- Bezpečná…?

- 60 % provozní náklady
- 36.6 mld. Potenciál úspory

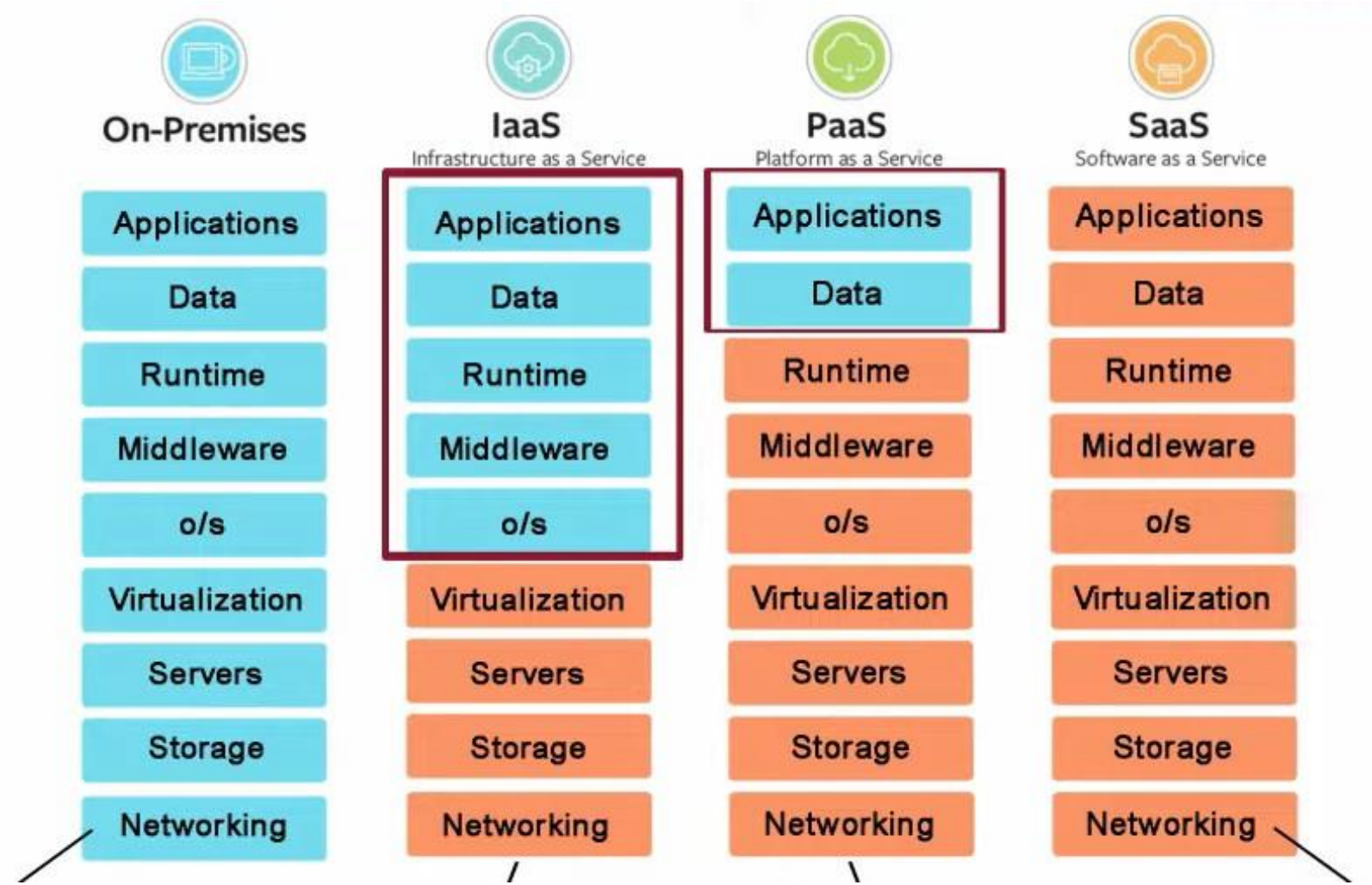


Graf 2: Výdaje organizačních složek státu státních fondů na vývoj, rozvoj a provoz všech informačních systémů a služeb v letech 2010-2020 (zdroj dat: Monitor státní pokladny).

MUNI
LAW

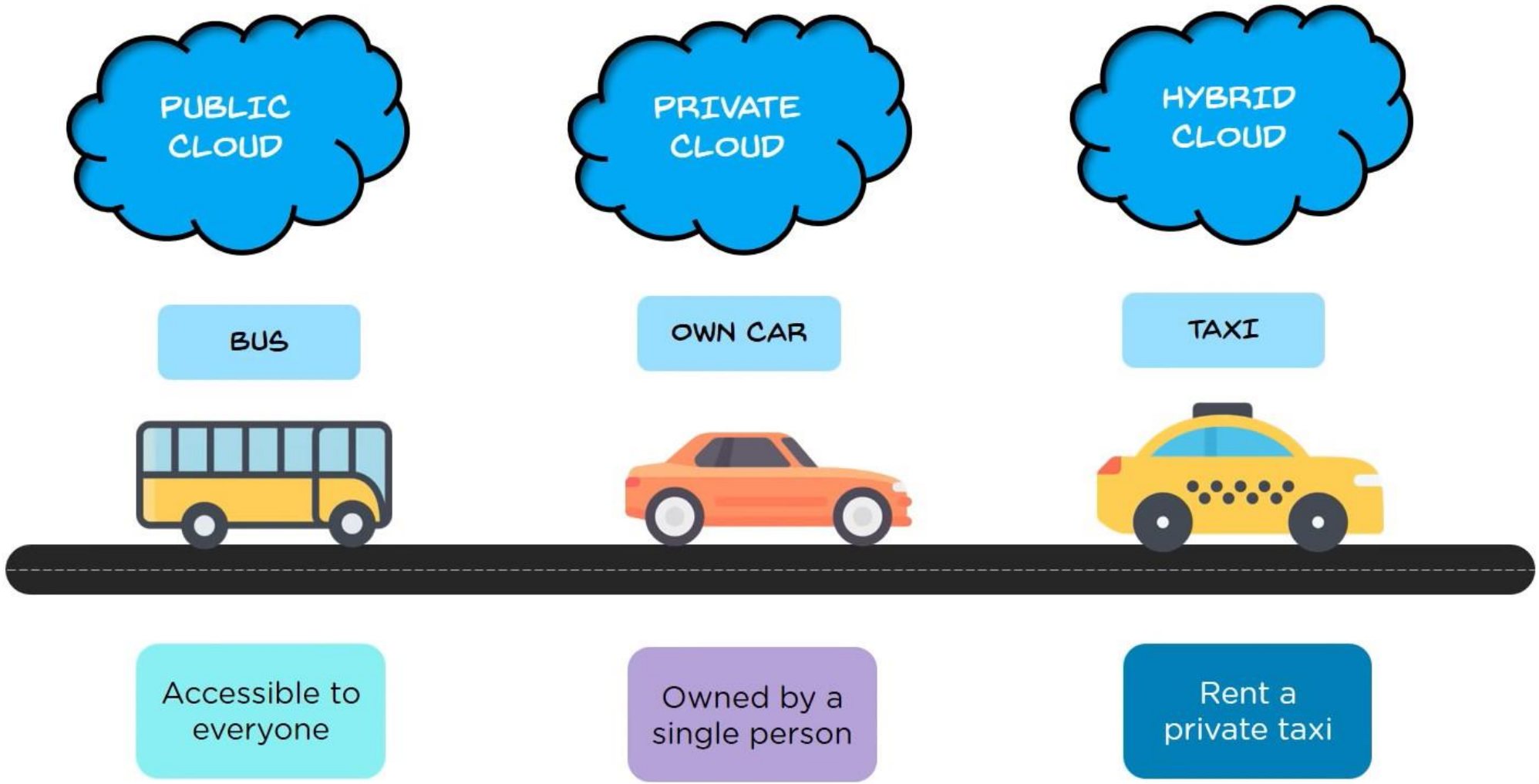
Druhy cloud computingu (CC)

Obchodní model CC



MUNI LAW

Modely zavedení CC

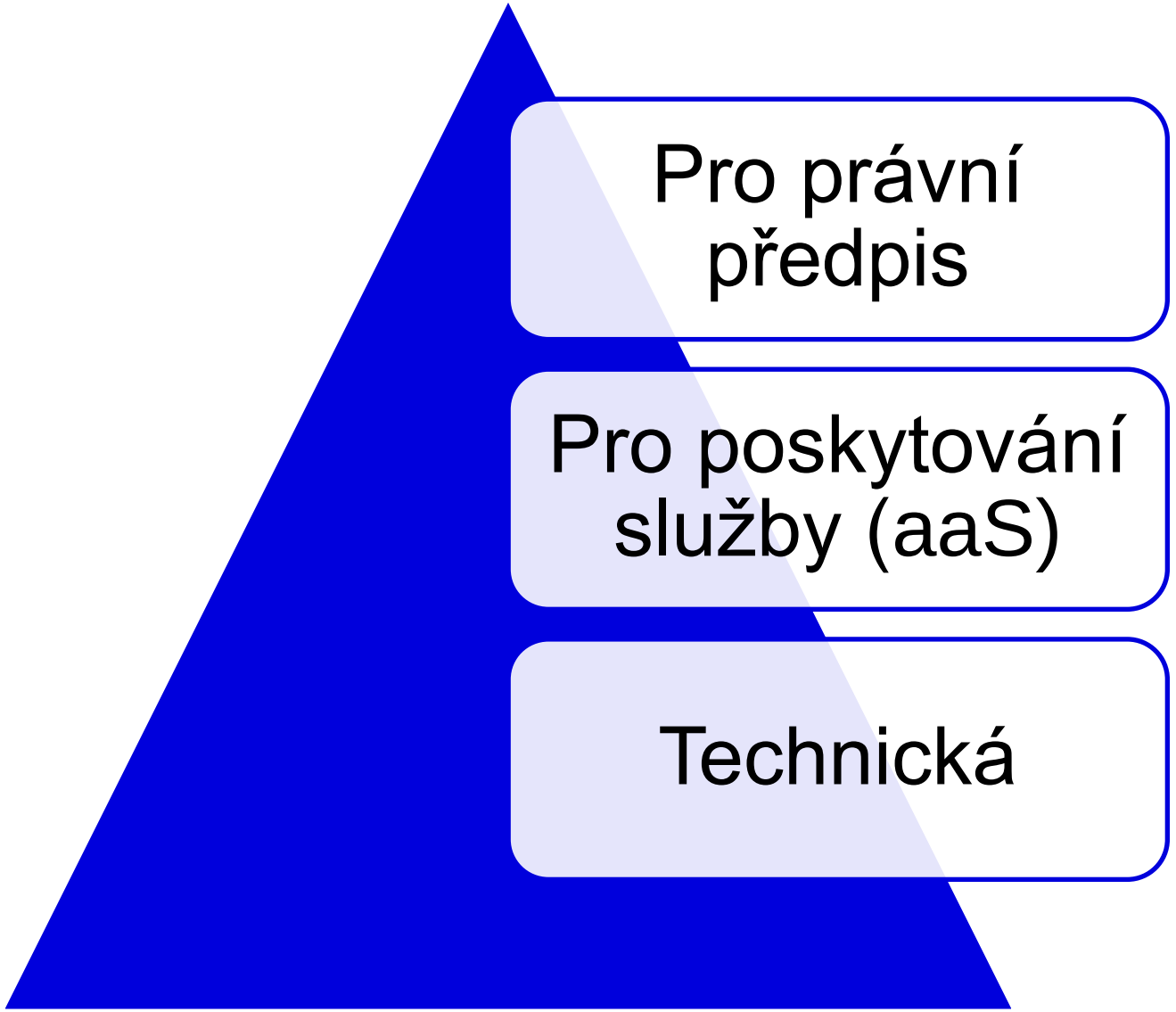


MUNI LAW

MUNI
LAW

Definice cloud computingu (CC)

Definice cloud computingu



MUNI LAW

What is cloud computing?

- *„**Cloud computing** is the paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand.“*

- *„**Cloud service** is one or more capabilities offered via cloud computing invoked using a defined interface.“*
  - Evropský systém certifikace kybernetické bezpečnosti pro cloudové služby (EUCS)

Co je to cloud computing?

– *„**Cloudové služby** (cloud computing) je obecný technický termín označující ICT prostředky (výpočetní zdroje, úložiště, aplikace) a související služby poskytované typicky vzdáleně prostřednictvím komunikačních sítí jako služba externího poskytovatele s definovanými parametry kvality, realizovaná na sdílených platformách pro více uživatelů (multi-tenant). Dalšími typickými znaky cloudových služeb jsou vysoká míra flexibility a dynamického škálování alokovaných prostředků.“*

– Souhrnná analytická zpráva projektu eGovernment

Definice cloud computingu v legislativě

– § 2 písm. l) bod. 3 ZKB

*„… **digitální službou** služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá (…) v provozování **cloud computingu**, který umožňuje přístup k rozšířitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet“*

– § 2 písm. x) ZoISVS (návrh DEPO)

*„… **cloud computingem** způsob zajištění provozu informačního systému veřejné správy nebo jeho části prostřednictvím dálkového přístupu k sdílenému technickému nebo programovému prostředku, který je zpřístupněný poskytovatelem cloud computingu a nastavitelný správcem informačního systému veřejné správy“*

MUNI LAW

MUNI
LAW

Právní úprava cloud computingu (CC)

Unijní regulace CC

- Evropská agentura pro bezpečnost sítí a informací (ENISA)
- Evropský systém certifikace kybernetické bezpečnosti pro cloudové služby (EUCS)
  - Certifikace kybernetické bezpečnosti cloudových služeb
  - Stanovuje kyberbezpečnostní standardy pro všechny členské státy
  - Vychází z ISO/IEC 17788, ISO/IEC 27000 a ISO/IEC 17000.
  - Počítá s přímým prověřováním nezávislými orgány posuzujícími shodu (PenTesty, Audity, …)
- Tři bezpečnostní úrovně EUCS:
  - ‘**basic**’, – bezpečnostní minimum
  - ‘**substantial**’ – obchodní úroveň
  - ‘**high**’ – nejmodernější metody zabezpečení

Zákonná úprava

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

- § 2 l) Digitální služby
- § 3 Povinné osoby
- § 4 odst. 5 Povinnost pro OVM ve smlouvě s poskytovatelem služeb cloud computingu zajistit, že budou dodržována bezpečnostní pravidla

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

- Hlava VI. § 6i - § 6z – pouze pro ISVS
- Novela DEPO, sněmovní tisk 756
- Vrácena Senátem do PS s připomínkami dne 29.4.2021

MUNI LAW

Povinné osoby dle ZKB

- Poskytovatel služby elektronických komunikací § 3 a)
- Osoba zajišťující významnou síť § 3 b)
- Správce/provozovatel KII § 3 c,d)
- Správce/provozovatel VIS § 3 e)
- Správce/provozovatel ISZS § 3 f)
- Provozovatel základní služby § 3 g)
- Poskytovatel digitální služby § 3 h)

- OVM poptávající cloud computing § 4/5
  - Osoby dle § 3 c) až g), které jsou OVM a poptávají CC

MUNI LAW

Nezbytné náležitosti smlouvy

Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou **povinny si ve smlouvě** s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována **bezpečnostní pravidla** pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase. Dalšími nezbytnými náležitostmi smlouvy jsou

a) zakotvení povinnosti poskytovatele služeb **respektovat bezpečnostní politiku** odběratele služeb,
b) stanovení úrovně poskytovaných služeb,
c) systém **schvalování subdodavatelů** služby cloud computingu,
d) podmínky ukončení smluvního vztahu z pohledu bezpečnosti,
e) řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,
f) určení vlastníka uchovávaných dat,
g) dohoda o **důvěrnosti** smluvního vztahu,
h) stanovení **úrovně ochrany dat** z pohledu důvěrnosti, dostupnosti a integrity,
i) pravidla **zákaznického auditu**,
j) stanovení povinnosti poskytovatele služeb **informovat odběratele o** kybernetických bezpečnostních **incidentech** souvisejících s plněním smlouvy.

MUNI LAW

Nezbytné náležitosti smlouvy II

- § 6 písm. e) ZKB

*„Prováděcí právní předpis stanoví (…) obsah a rozsah **bezpečnostních pravidel** pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, včetně **bezpečnostních úrovní** pro využívání cloud computingu orgány veřejné moci.“*

- **Vyhláška o** obsahu a rozsahu **bezpečnostních pravidel** pro orgány veřejné moci využívající služby poskytovatelů cloud computingu (VCC č. 2)
- **Vyhláška o bezpečnostních úrovních** pro využívání cloud computingu orgány veřejné moci (VCC č. 3)

Digitální služba

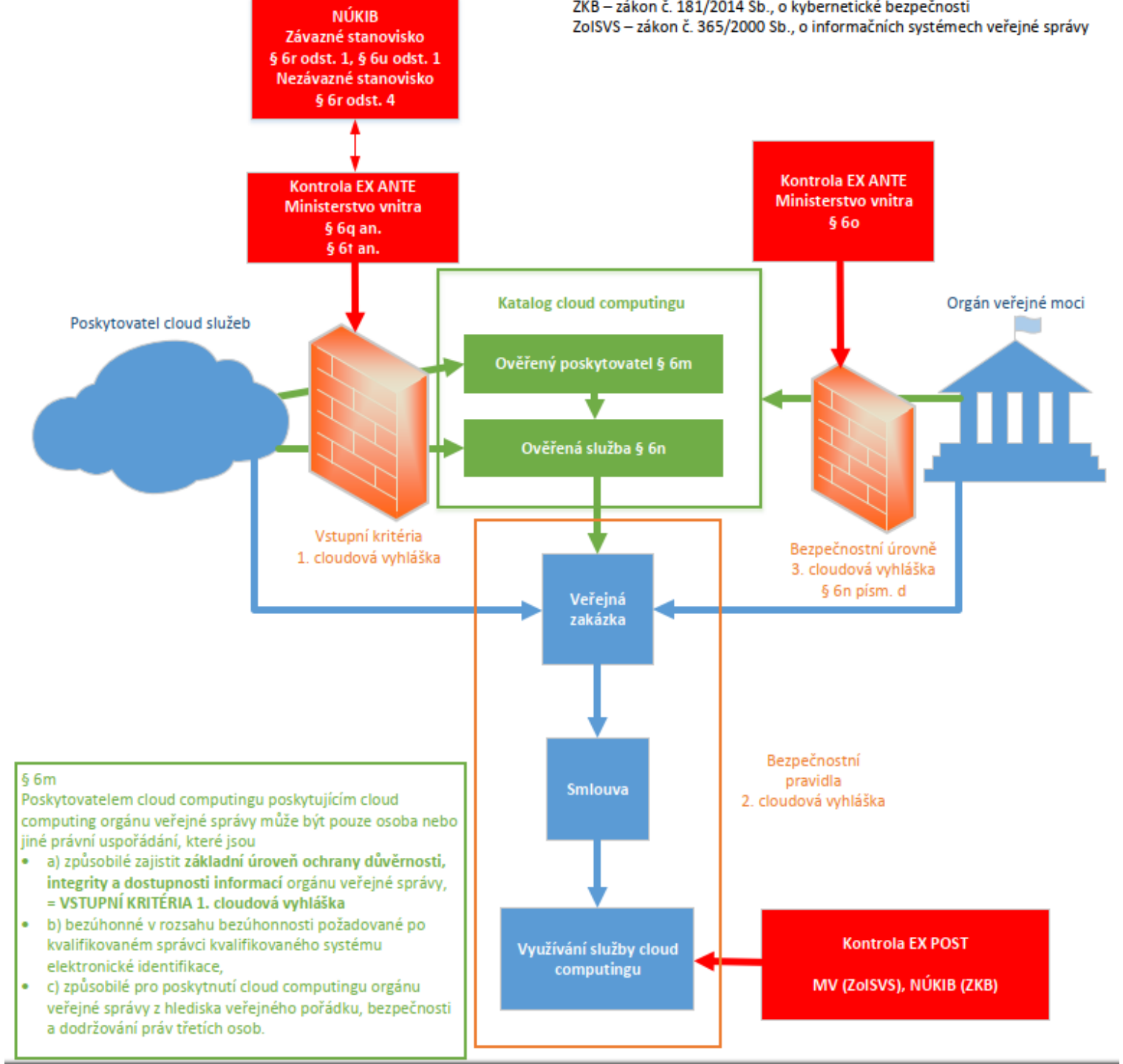
- § 2 písm. l) „Digitální službou služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá v provozování
  - online tržiště,
  - internetového vyhledavače,
  - cloud computingu.
- Institut ze směrnice NIS
- Výjimka de minimis (50 zaměstnanců a roční obrat pod 20 mil. eur)
- Povinnosti vůči národnímu CERT
  - Hlášení povinných údajů,
  - bezpečnostních incidentů a
  - provádění bezpečnostních opatření

ZoISVS

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
  - Hlava VI. § 6i - § 6z
  - Novela DEPO, sněmovní tisk 756
  - Vrácena Senátem do PS s připomínkami dne 29.4.2021

- Katalog CC:
  - Veřejný seznam, který je středobodem regulace kybernetické bezpečnosti CC
  - Zapisuje se do něj
    1. Poptávky OVS po službách CC
    2. Nabídky CC pro OVS
    3. CC aktuálně využívaný OVS

ZKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti
ZoISVS – zákon č. 365/2000 Sb., o informačních systémech veřejné správy



MUNI LAW

Cloudové vyhlášky

- **1. Cloudová vyhláška - Vstupní kritéria**
  - § 12 odst. 2 ZoISVS
  - Bude předána do Legislativní radě vlády
- **2. Cloudová vyhláška – Bezpečnostní pravidla**
  - § 6 ZKB
  - V meziresortním řízení
- **3. Cloudová vyhláška – Bezpečnostní úrovně**
  - § 6 ZKB
  - Vypořádány připomínky z meziresortního řízení

MUNI LAW

Srovnání české a evropské regulace

Čl. 16 odst. 10 NIS
Úroveň zabezpečení nabízeného cloud computingu:

ČR:		**EU:**
Nízká	-	substantial
Střední	-	high
Vysoká	x	***Veřejná bezpečnost***
Kritická	x	***Národní bezpečnost***

Bezpečnostní požadavky

- Ukládání dat pouze v EU
- Transparentnost zpracování údajů na jakémkoli místě
- Na žádost zahraničních zemí neposkytovat údaje o klientech
- SLA
- Peeringový uzel v ČR
- Plán kontinuity provozu
- Zeměpisná vzdálenost dvou datových center (pro zálohování)
- Šifrování
- ČSN ISO 27001
- Audity

Optimistický Závěr

- Česká republika je v cloud computingu napřed oproti většině vyspělých zemí světa
- V současnosti již je zavedený legislativní rámec pro nákup CC veřejným sektorem
- Brzy bude přijata očekávaná prováděcí legislativa v souladu s připravovanou evropskou certifikací (1,2 BU)
- Aktuálně je již 8 zapsaných nabídek v katalogu CC

Kritický Závěr

- Nemožnost OVM v současnosti nakupovat služby CC
- Nedostatečně zpracovaná legislativa, která byla přijata bez dostatečné přípravy procesů, doprovodných prováděcích předpisů a komunikace s ostatními zapojenými subjekty (úřady, vendory)
- Definiční nedostatky (OVM x OVS)
- Protahující se příprava cloudových vyhlášek
- Posuzování nabídek CC na základě Metodiky MV, bez zákonného zmocnění
- Nedostatek personálních kapacit

MUNI
LAW

Děkuji za pozornost

Jakub.Klodwig@law.muni.cz