

POVINNOSTI OBCÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

1. Března 2022
TLP: WHITE

Jakub Klodwig
Odbor regulace - NÚKIB
Masarykova univerzita



Proč kybernetická bezpečnost?

Rostoucí závislost na kyberprostoru a ICT

Vláda, armáda, policie, finanční instituce, energetika, průmysl, zdravotnictví, samosprávy
Vedení registrů, zpracovávání obrovského množství osobních údajů

Nové technologie = nová rizika

IoT, Smart Grid,
Smart Cities, E-Health,
sítě 5G, AI

Rostoucí trend kyberkriminality





Kybernetické útoky s globálním dopadem – Stuxnet 2009, Red October 2007, ...

Kybernetické útoky destruktivní – Shamoon 2012, Aurora 2007, Farewell 1982, ...

Politicky motivované aktivity – destrukce, sabotáž (Ukrajina 2022, 2013, Gruzie 2008, Estonsko 2007, ...)

Kybernetická špionáž

Státní (OPM 2015, Kukaččí vejce 1986, ...)

Korporátní (intelektuální vlastnictví, F-35 JSF, ...)

Hacktivismus (Anonymous)

Kriminální kybernetická aktivita

Krádeže osobních a finančních dat

Zdravotnická dokumentace (vydírání)

Ransomware (zašifrování dat) – Ryuk (+ Emotet, Trickbot) 2019, Wanna Cry 2018, ...



Hackeri zaútočili na pražský IPR. Skrze jeho systémy těžili kryptoměny, institut se obává ztráty dat

ČESKO



Michal Bernáth 22. června 2021 9:50, aktualizováno 16:05

PRAHA - Institut plánování a rozvoje hlavního města Prahy (IPR) se stal terčem kybernetického útoku. Serveru Lidovky.cz to potvrdil jeho ředitel Ondřej Boháč.

Hackeri využili kapacitu institutu k těžení kryptoměn.



10 příspěvků

Datové systémy olomouckého magistrátu napadli ve středu ráno hackeri. Kybernetický útok byl podle radnice velmi silný a navíc přišel v den, kdy chodí na úřad více lidí. Agendy byly po celý den mimo provoz.

Kyberútoky se nevyhýbají ani městům a jejich úřadům

Datum: 30. 7. 2021, zdroj: Lesensky.cz, rubrika: [Veřejná správa online](#)

Kyberbezpečnost je v Česku v posledních letech stále častěji skloňovaným pojmem. S hackerskými útoky se nesetkávají jen tuzemské podniky, ale také ministerstva, nemocnice či města a jejich úřady. Nejde přitom o jednotky případů, měsíčně se může jednat až o stovky „bezpečnostních incidentů“. S detekcí potenciálních rizik a jejich eliminací IT specialistům pomáhají i umělé inteligence.





- Cílem je zajistit (kyber)bezpečnost nejvýznamnějších služeb a institucí
 - **Zajištění bezpečného fungování informační společnosti České republiky**
 - **Zajištění veřejného zájmu na bezpečnosti** – (zejména preventivně)
- Těchto cílů je dosaženo na základě stanovení **minimálních požadavků na standardní zabezpečení** u daných subjektů a zajištění vládnímu dohledovému pracovišti možnosti mít **přehled o kybernetické bezpečnostní situaci** u těchto subjektů v reálném čase.
- Performativní pravidla.
- Vládní CERT
- Varován, Reaktivní opatření, Ochranné opatření NÚKIB



- Povinné osoby (§ 3 ZKB):
 - poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),
 - orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
 - správce a provozovatel **informačního systému kritické informační infrastruktury**,
 - správce a provozovatel komunikačního systému kritické informační infrastruktury,
 - správce a provozovatel **významného informačního systému**,
 - správce a provozovatel **informačního systému základní služby**, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),
 - provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a
 - poskytovatel digitální služby.

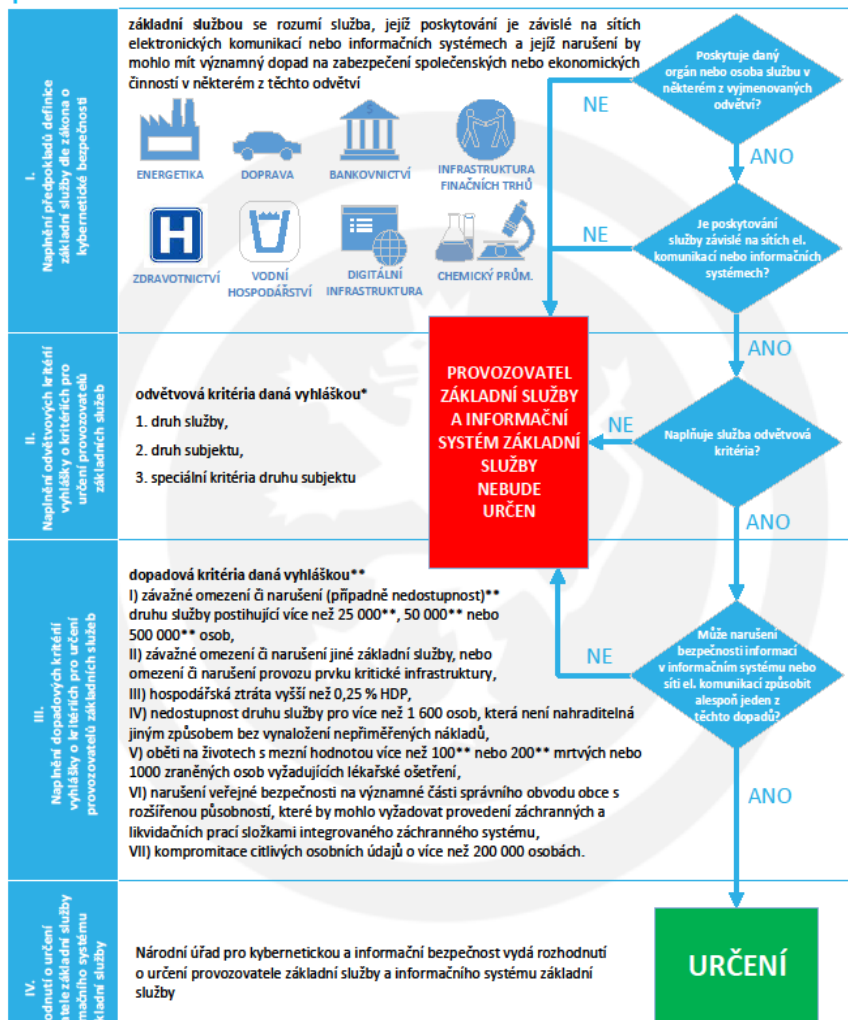
Schéma zákona o kybernetické bezpečnosti



Základní služba



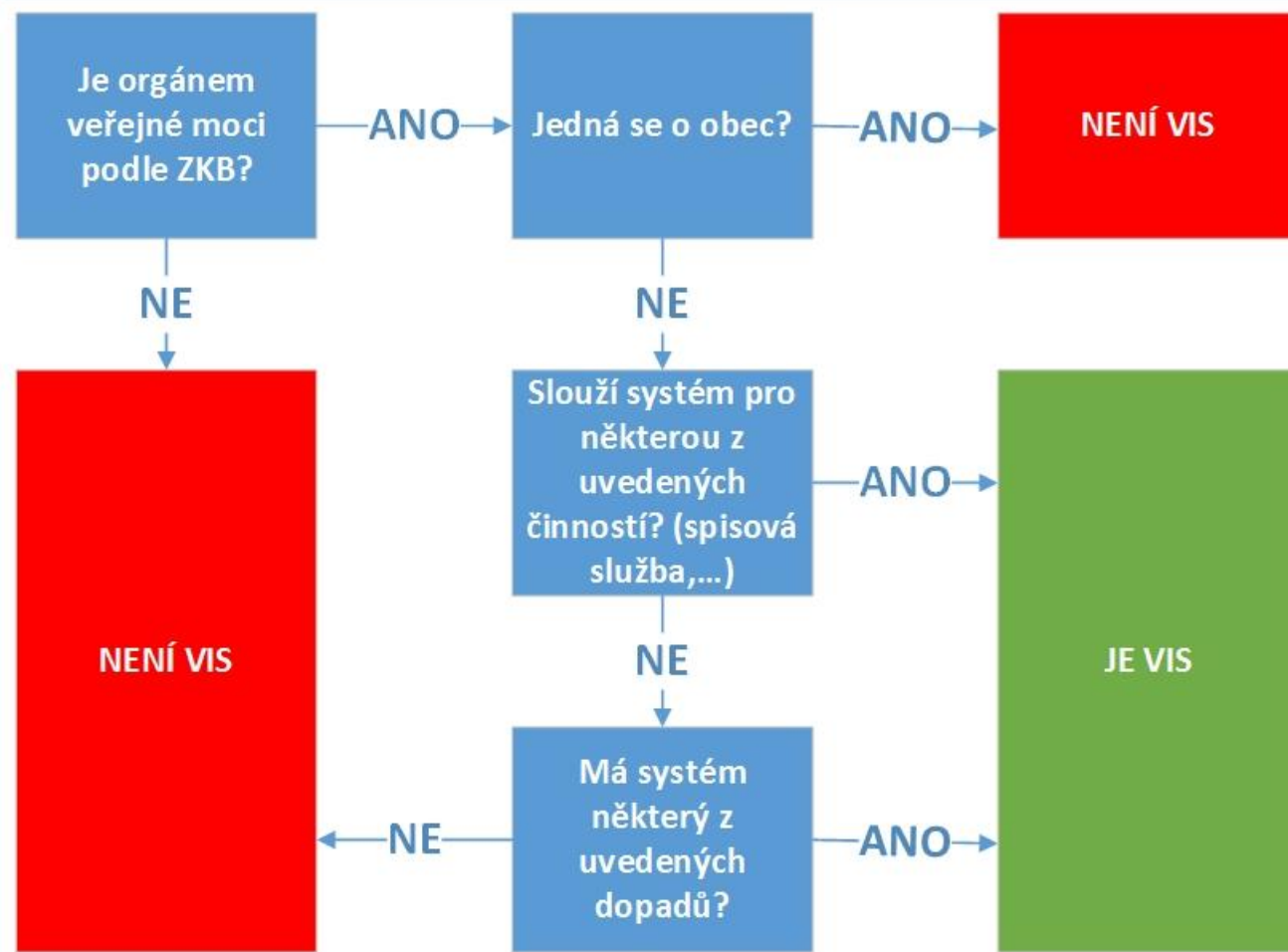
Proces určení provozovatele základní služby a informačního systému základní služby dle zákona o kybernetické bezpečnosti a vyhlášky o kritériích pro určení provozovatelů základních služeb



* liší se v rámci jednotlivých služeb

Významný informační systém

Zjednodušené schéma cíle změny vyhlášky č. 317/2014 Sb., o významných informačních systémech





- **Zavádění bezpečnostní opatření (§ 4 a § 5).** – odpovědnost každého subjektu
 - jsou uvedeny ve vyhlášce o kybernetické bezpečnosti č. 82/2018 Sb.
 - Minimální bezpečnostní standard NÚKIB ([zde](#))
- **Hlášení kontaktních údajů (§ 16).**
 - Vládní CERT x Národní CERT
- **Hlášení incidentů (§ 8).**
 - Vládní CERT x Národní CERT
- **Provádění reaktivních a ochranných opatření (§ 13 a násl.).** – odpovědnost každého subjektu
 - NÚKIB vydává formou opatření obecné povahy nebo rozhodnutí.



Organizační bezpečnostní opatření:

- a) systém řízení bezpečnosti informací,
- b) řízení rizik,
- c) bezpečnostní politika,
- d) organizační bezpečnost,
- e) stanovení bezpečnostních požadavků pro dodavatele,
- f) řízení aktiv,
- g) bezpečnost lidských zdrojů,
- h) řízení provozu a komunikací,
- i) řízení přístupu osob,
- j) akvizice, vývoj a údržba,
- k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- l) řízení kontinuity činností a
- m) kontrola a audit.



Technická bezpečnostní opatření:

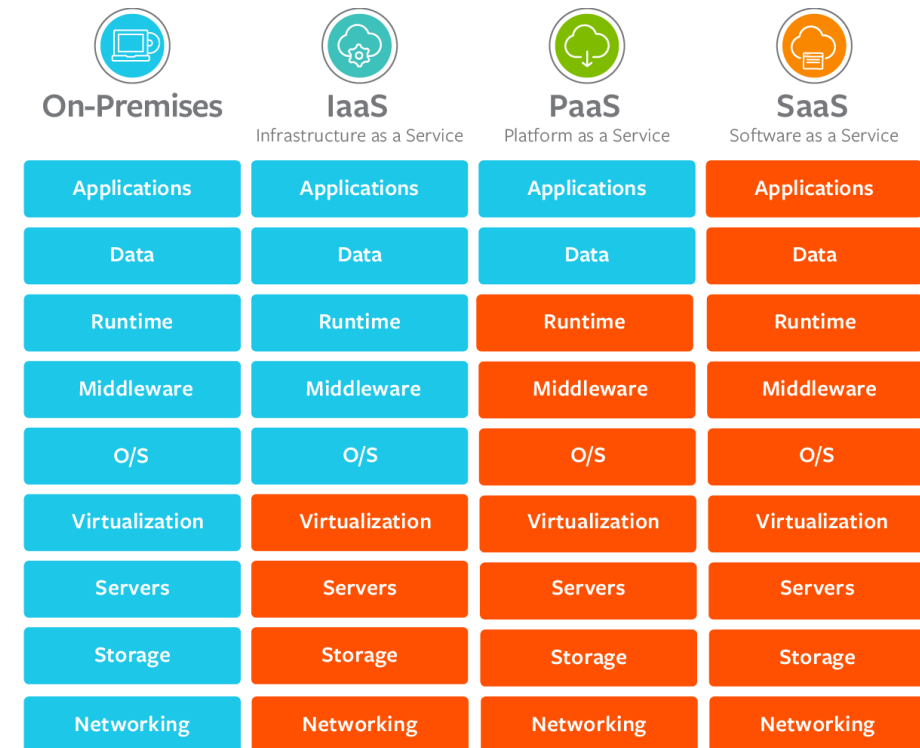
- a) fyzická bezpečnost,
- b) nástroj pro ochranu integrity komunikačních sítí,
- c) nástroj pro ověřování identity uživatelů,
- d) nástroj pro řízení přístupových oprávnění,
- e) nástroj pro ochranu před škodlivým kódem,
- f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,
- g) nástroj pro detekci kybernetických bezpečnostních událostí,
- h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- i) aplikační bezpečnost,
- j) kryptografické prostředky,
- k) nástroj pro zajišťování úrovně dostupnosti informací a
- l) bezpečnost průmyslových a řídicích systémů.



Nová regulace cloud computingu

- „... **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**“

- *Typy cloud computingu:*
 - *Software as a service*
 - *Platform as a service*
 - *Infrastructure as a service*

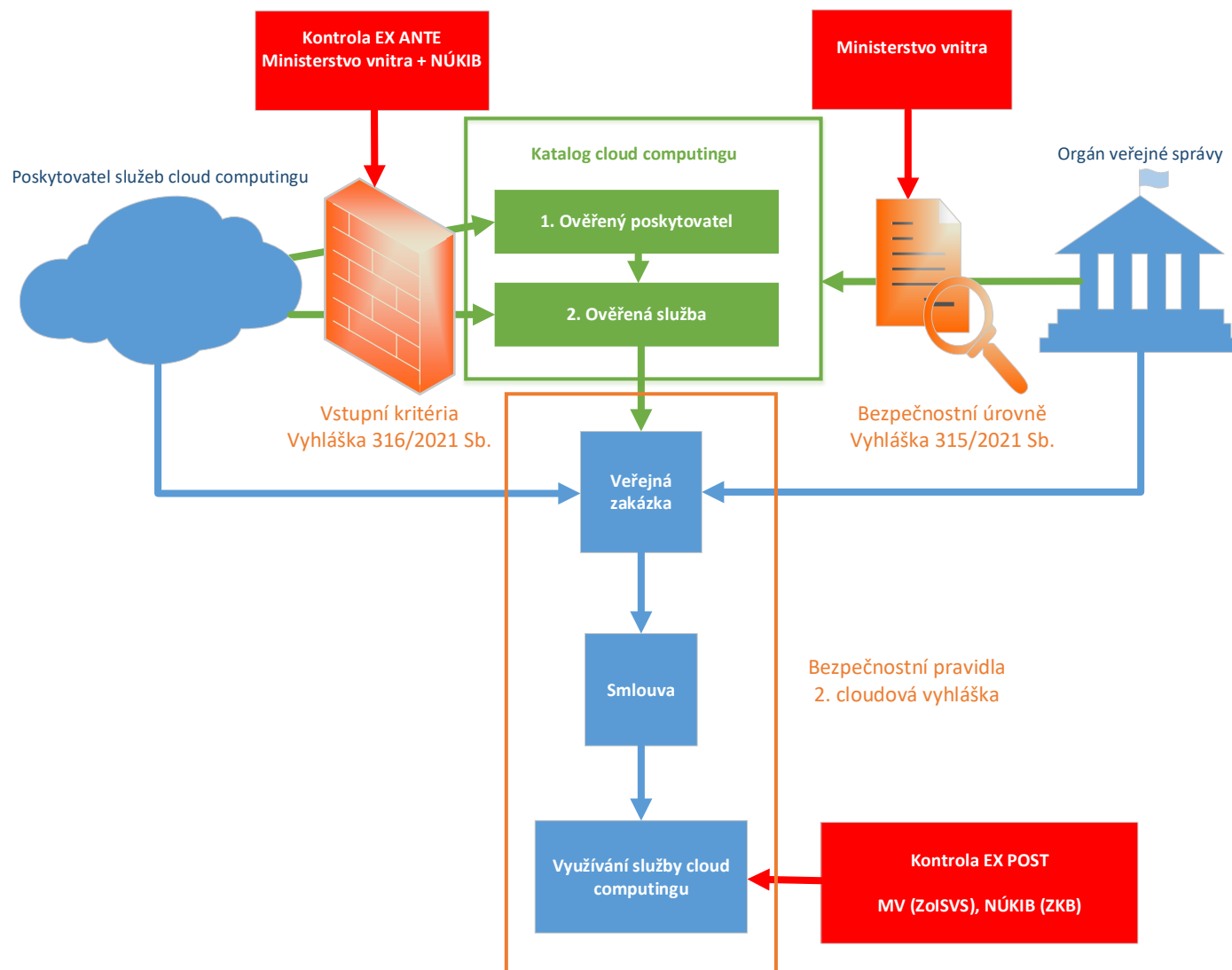




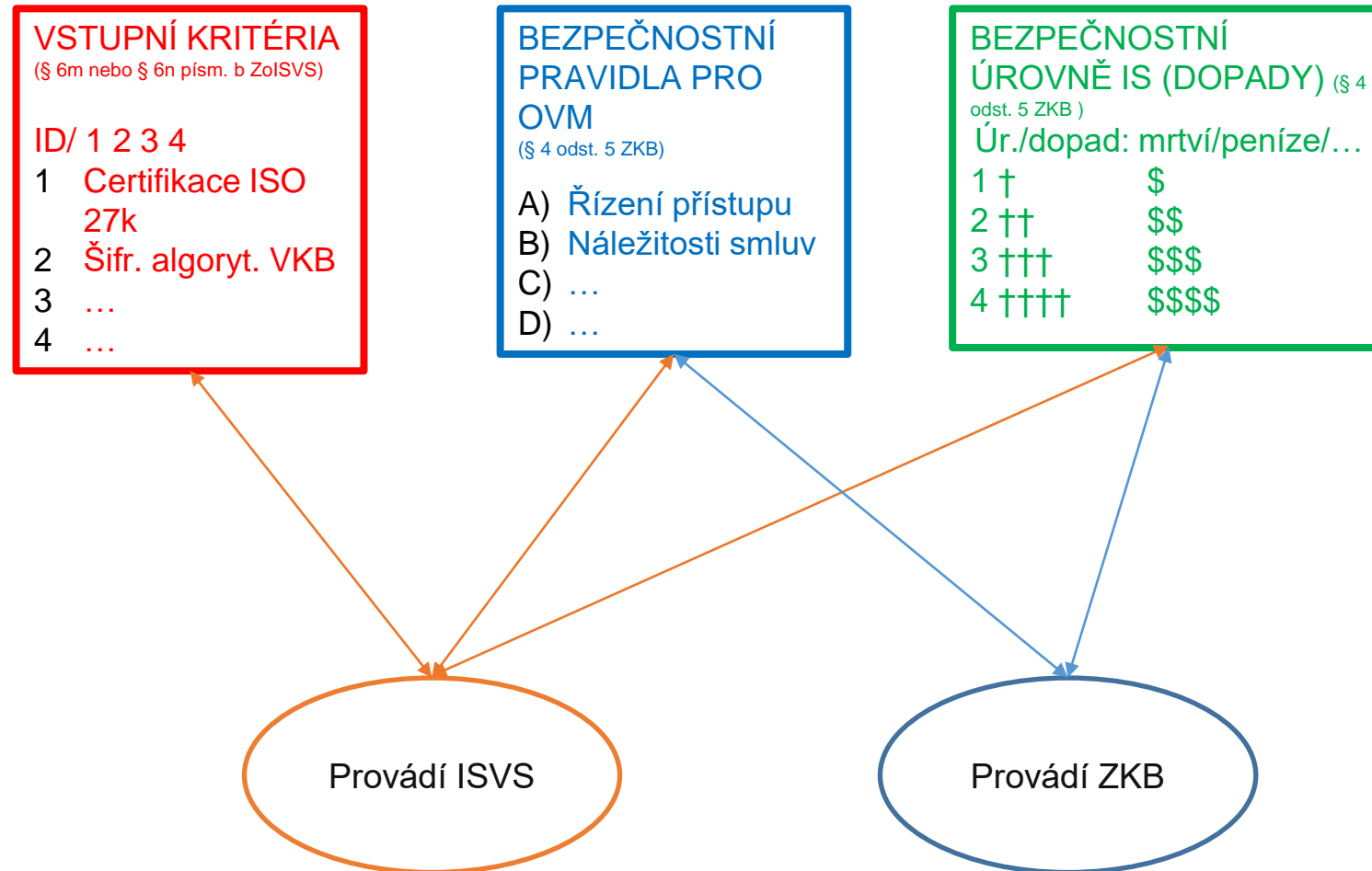
- Cloudové služby mohou přispět k ekonomičtějšímu a díky centrálnímu řízení, dohledu a aktualizaci i bezpečnějšímu provozu informačních systémů.
- Využití cloudových služeb jak v soukromém, tak i ve veřejném sektoru rychle roste.
- Cloudové služby přináší nová rizika, zejména co se týče místa zpracování dat, které je často neznámé jednotlivým zákazníkům využívajících cloudové služby.

- Veřejné 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)

Schéma regulatorního rámce cloud computingu



Dva zákony a tři cloudové vyhlášky





- **Zákon o informačních systémech veřejné správy (§ 6i - § 6z)**
 - Orgány veřejné správy = státní orgány nebo orgány územních samosprávných celků (vč. obcí)
 - Cloudové služby rozděleny do 4 úrovní podle požadavků na bezpečnost
 - Jednotliví dodavatelé služeb cloud computingu musí splnit vstupní požadavky
 - Naplnění požadavků posoudí NÚKIB a MV
- **Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu**
 - Tzv. vyhláška o vstupních kritériích
 - Sada požadavků a podmínek, které musí poskytovatel cloudových služeb splnit aby je mohl dodávat orgánům veřejné správy
 - Účinná od 1. 9. 2021



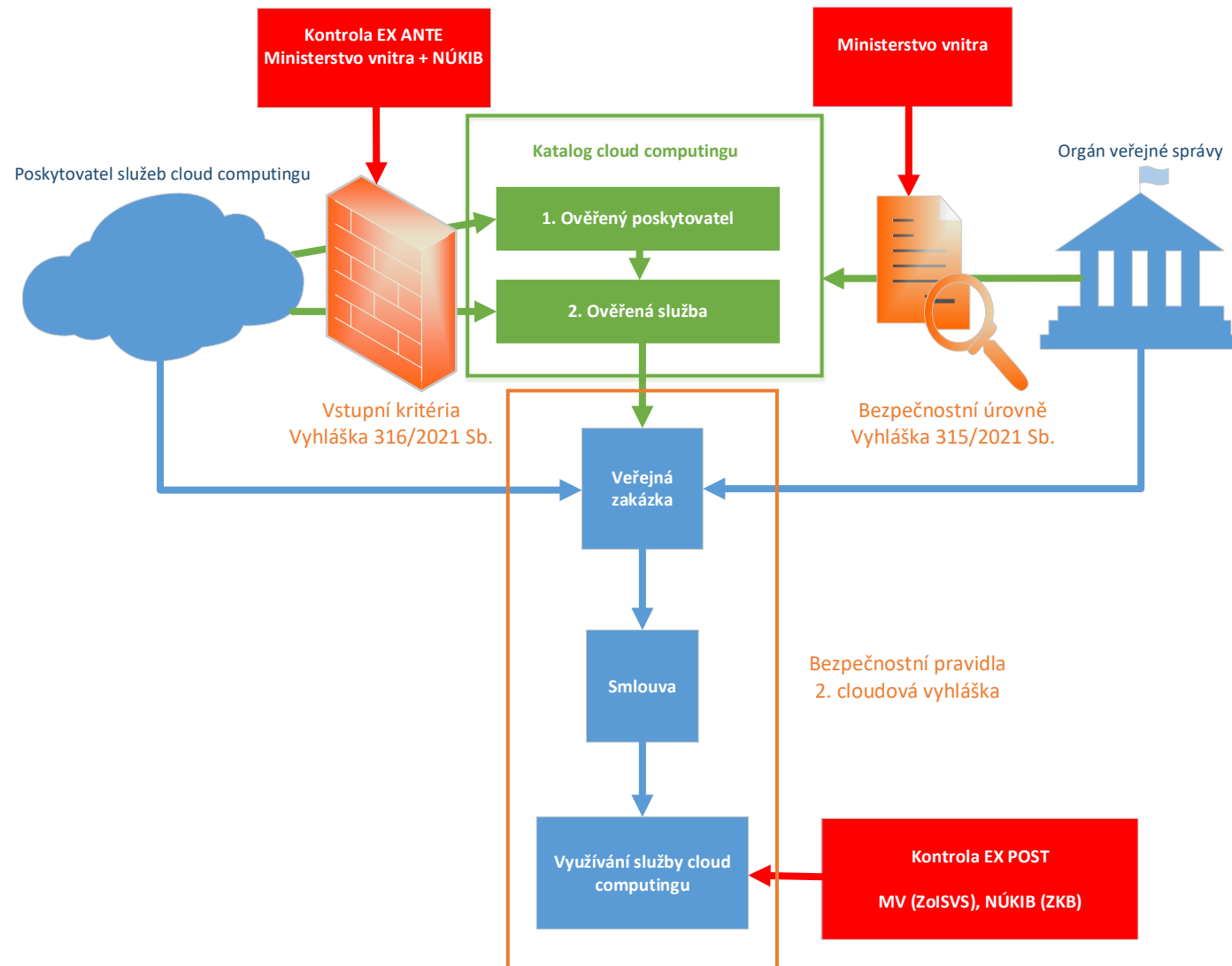
- **Zákon o kybernetické bezpečnosti**

- Orgány veřejné moci = osoba které byla svěřena působnost v oblasti veřejné správy
- Čl. 4 odst. 5 ZKB: *„Orgány veřejné moci jsou povinny před uzavřením smlouvy s poskytovatelem služeb cloud computingu zařadit poptávaný cloud computing do bezpečnostní úrovně s ohledem na povahu dotčeného informačního nebo komunikačního systému podle prováděcího právního předpisu a zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem (...)“*

- **Vyhláška o bezpečnostních pravidlech** (připravuje se)

- Každá z kategorií systémů (1-4) bude mít stanovena příslušná bezpečnostní opatření (C5, EUCS, VKB)
- Bude obsahovat povinná a volitelná bezpečnostní pravidla – celkem cca 250 pravidel (povinná 46)
- Požadavky: certifikace ISO, C5, SOC 2[®] Type 2, smluvní závazky poskytovatel, čestná prohlášení OVM

Schéma regulatorního rámce cloud computingu - ZoISVS





○ **Zákon č. 261/2021 Sb., Čl. LXXXI**

- OVS využívalo CC nebo **uzavřelo** (rámcovou) smlouvu před 1. 9. 2021 = může tento CC využívat **do 31. 12. 2023**
- CC **v katalogu** před 1. 9. 2021/zapsaný dle podmínek před 1. 9. 2021 = může využívat **do 31. 12. 2023**
- OVS zahájilo využívání CC od 1. 9. 2021 do 31. 1. 2022 = může využívat do **31. 12. 2022**

pozn. v případě, že daný CC splňuje aktuální podmínky – zapsán v katalogu, splňuje požadavky cloudových vyhlášek – lze využívat bez časového omezení



Doporučení na závěr

- **Neignorovat kybernetickou bezpečnost**
 - Zavádět z vlastní iniciativy přiměřená bezpečnostní opatření
 - Zohledňovat (proti)opatření NÚKIB
- **Přijmout minimální bezpečnostní standard**
 - zjednodušené principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro organizace, které nespádají pod regulaci ZKB (výsledek spolupráce NÚKIB, MV a NAKIT)
 - [Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály \(nukib.cz\)](https://www.nukib.cz)
- **Vzdělávací materiály**
 - Online webináře: Dávej kyber, Kurz rizikového chování na internetu, Kurz pro manažery kybernetické bezpečnosti ...
 - Rozcestník osvětových materiálů: [NUKIB \(GUEST\)](#)
- **Směrnice NIS II**
 - Přinese zásadní rozšíření povinných subjektů (vč. obcí)





Dotazy?

Děkuji za pozornost!

j.klodwig@nukib.cz
regulace@nukib.cz