KYBERNETICKÁ BEZPEČNOST A CLOUD COMPUTING

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

9. listopadu 2021
TLP: WHITE

Jakub Klodwig
Odbor regulace - NÚKIB
Masarykova univerzita

Obsah

- Úvod do zákona o kybernetické bezpečnosti
- Zákon o kybernetické bezpečnosti optikou obce
- Nová regulace cloud computingu
- Doporučení na závěr

Úvod do zákona o kybernetické bezpečnosti

Cíle zákona o kybernetické bezpečnosti

- Cílem je:
  - **Zajištění bezpečného fungování informační společnosti České republiky**
    - **(tzv. zajištění realizace práva na informační sebeurčení)**
  - **Zajištění veřejného zájmu na bezpečnosti**
    - **(tzv. ochrana nedistributivních práv státu).**

- 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.
- Bezpečnost je základ.
- Performativní pravidla.

Povinné osoby dle zákona o kybernetické bezpečnosti

- 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

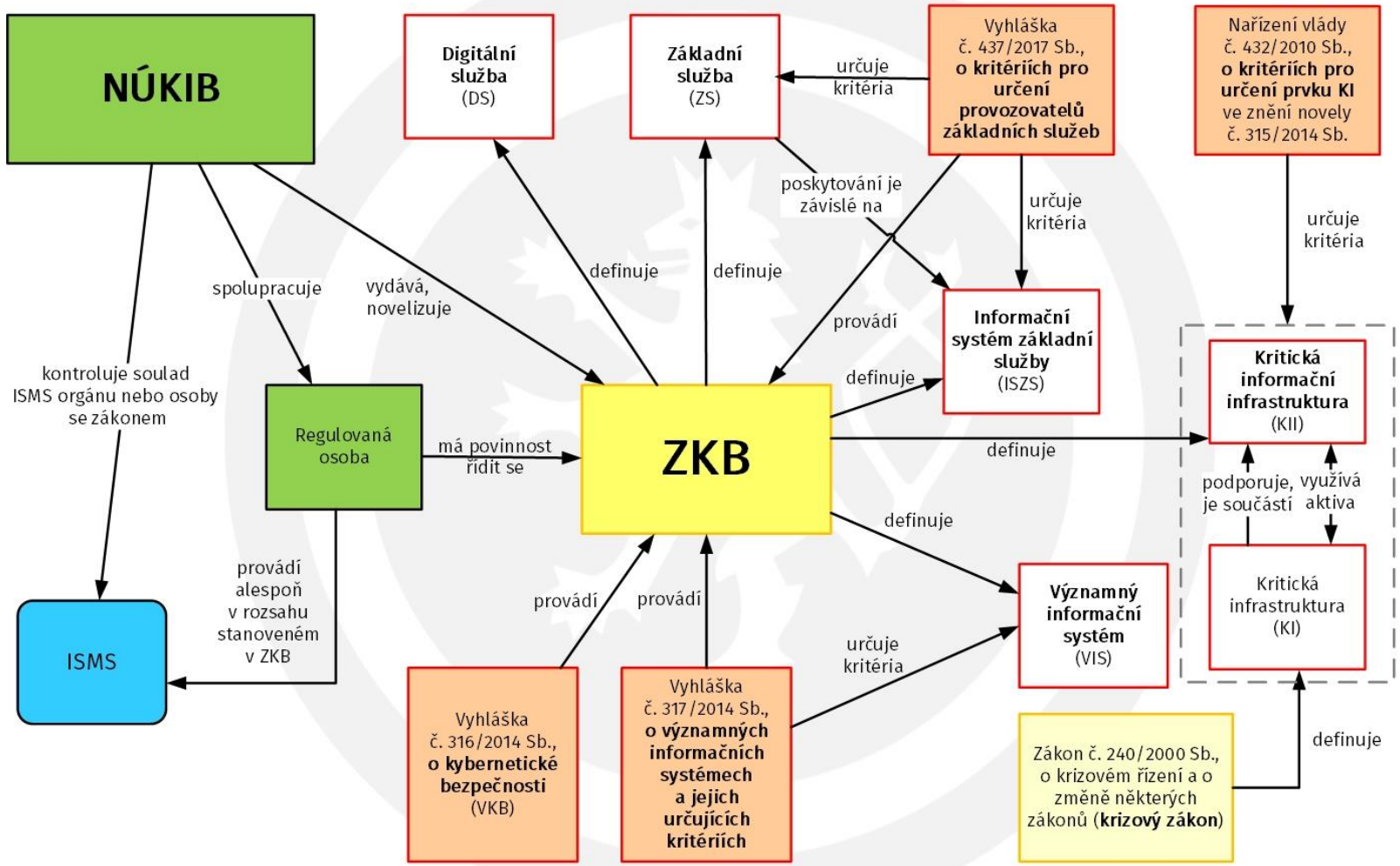


Schéma zákona o kybernetické bezpečnosti

Kritická informační infrastruktura

Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb.

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

Jsou dána tato průřezová kritéria:

(Průřezová kritéria podle § 1 nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb.)

a) Více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací delší než 24 hodin.

b) Mezní hodnota hospodářské ztráty je větší než 0,5 % HDP (např. v r. 2013 = 19,4 mld. Kč).

c) Omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125 000 osob.

Může mít narušení bezpečnosti informací (důvěrnosti, dostupnosti, integrity) Vašeho IS nebo KS za následek **ALESPOŇ** jedno z výše uvedených průřezových kritérií?

ANO

NE

Váš IS nebo KS v tuto chvíli není kritickou informační infrastrukturou. Může však být významným informačním systémem (jste-li orgánem veřejné moci), viz. schéma o významných informačních systémech, dostupné na webu www.GovCERT.cz.

Jsou dána tato odvětvová kritéria v oblasti kybernetické bezpečnosti:

(Odvětvová kritéria podle nařízení vlády č. 432/2010 Sb. ve znění novely č. 315/2014 Sb., příloha - odvětví VI., část G.)

a), b) Ovlivňuje Váš IS nebo KS významně nebo zcela činnost určeného prvku KI a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším jak 8 hodin?

c) Je Váš IS spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 tis. osobách?

d) Je Váš systém komunikačním systémem, který zajišťuje připojení nebo propojení prvku KI s kapacitou garantovaného datového přenosu min. 1 Gbit/s?

e) Odvětvová kritéria pro určení prvku KI uvedená v písm. A. – F., odvětví VI. přílohy nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb., se použijí přiměřeně pro oblast KB, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

Splňuje Váš IS nebo KS **ALESPOŇ** jedno z výše uvedených odvětvových kritérií?

NE

ANO

Jsou dána tato odvětvová kritéria (odvětví VI. Komunikační a informační systémy)

A. Technologické prvky pevné sítě elektronických komunikací:
a) centrum řízení a podpory sítě,
b) řídící ústředna,
c) mezinárodní ústředna,
d) transitní ústředna,
e) datové centrum,
f) telekomunikační vedení.

B. Technologické prvky mobilní sítě elektronických komunikací:
a) centrum řízení a podpory sítě,
b) ústředna mobilní sítě,
c) základnová řídící jednotka sítě pokrývající strategickou lokalitu,
d) základnová stanice sítě pokrývající strategickou lokalitu,
e) datové centrum.

C. Technologické prvky sítí pro rozhlasové a televizní vysílání:
a) vysílací zařízení pro šíření televizního nebo rozhlasového signálu určených pro informaci obyvatelstva za krizových situací vysílacím výkonem nad 1 kW k zajištění rozhlasového a televizního vysílání veřejnoprávního provozovatele
b) řídící pracoviště provozu,
c) datové centrum,
d) síť pro rozhlasové a televizní vysílání k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele.

D. Technologické prvky pro satelitní komunikaci:
a) hlavní pozemní satelitní přijímací a vysílací stanice,
b) Evropský globální navigační družicový systém,
c) pozemní řídící a komunikační středisko,
d) pozemní propojovací síť.

E. Technologické prvky pro poštovní služby:
a) centrální a regionální výpočetní středisko, středisko centrálního snímání a úložiště dat,
b) sběrný přepravní uzel,
c) řídící a mezinárodní pošta,
d) poštovní dopravní infrastruktura.

F. Technologické prvky informačních systémů:
a) řídící centrum,
b) datové centrum,
c) síť elektronických komunikací,
d) technologický prvek zajišťující provoz registru doménových jmen „CZ" a zabezpečení provozu domény nejvyšší úrovně „CZ".

G. Oblast kybernetické bezpečnosti:
viz. předchozí blok vlevo

Váš IS nebo KS splňuje podmínky pro zařazení do kritické informační infrastruktury.

Jste organizační složkou státu?

ANO

NE

Váš IS nebo KS určí jako KII vydáním opatření obecné povahy NÚKIB. Podle § 2, písm. b) zákona č. 181/2014 Sb. se Váš KS nebo IS stává prvkem kritické informační infrastruktury.

NÚKIB navrhne Ministerstvu vnitra zařadit Váš IS nebo KS do seznamu, který bude následně předložen vládě ČR. Vláda ČR rozhodne usnesením a navrhovaný IS nebo KS určí v příloze k tomuto usnesení prvkem KI. Podle § 2, písm. b) zákona č. 181/2014 Sb. se Váš KS nebo IS stává prvkem kritické informační infrastruktury.

Více informací o procesech určování a posuzování, včetně povinností orgánů a osob, naleznete na www.GovCERT.cz

Použité zkratky: IS - informační systém, KB - kybernetická bezpečnost, KI - kritická infrastruktura, KII - kritická informační infrastruktura, KS - komunikační systém, NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost, OOP - opatření obecné povahy

Schéma zákona o kybernetické bezpečnosti

Základní služba

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

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

I. Naplnění předpokladů definice základní služby dle zákona o kybernetické bezpečnosti

základní službou se rozumí služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví

ENERGETIKA, DOPRAVA, BANKOVNICTVÍ, INFRASTRUKTURA FINAČNÍCH TRHŮ, ZDRAVOTNICTVÍ, VODNÍ HOSPODÁŘSTVÍ, DIGITÁLNÍ INFRASTRUKTURA, CHEMICKÝ PRŮM.

Poskytuje daný orgán nebo osoba službu v některém z vyjmenovaných odvětví? — NE

Je poskytování služby závislé na sítích el. komunikací nebo informačních systémech? — NE

ANO

II. Naplnění odvětvových kritérií vyhlášky o kritériích pro určení provozovatelů základních služeb

odvětvová kritéria daná vyhláškou*

1. druh služby,
2. druh subjektu,
3. speciální kritéria druhu subjektu

Naplňuje služba odvětvová kritéria? — NE

PROVOZOVATEL ZÁKLADNÍ SLUŽBY A INFORMAČNÍ SYSTÉM ZÁKLADNÍ SLUŽBY NEBUDE URČEN

ANO

III. Naplnění dopadových kritérií vyhlášky o kritériích pro určení provozovatelů základních služeb

dopadová kritéria daná vyhláškou**

I) závažné omezení či narušení (případně nedostupnost)** druhu služby postihující více než 25 000**, 50 000** nebo 500 000** osob,
II) závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury,
III) hospodářská ztráta vyšší než 0,25 % HDP,
IV) nedostupnost druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,
V) oběti na životech s mezní hodnotou více než 100** nebo 200** mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření,
VI) narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému,
VII) kompromitace citlivých osobních údajů o více než 200 000 osobách.

Může narušení bezpečnosti informací v informačním systému nebo síti el. komunikací způsobit alespoň jeden z těchto dopadů? — NE

ANO

IV. Rozhodnutí o určení provozovatele základní služby a informačního systému základní služby

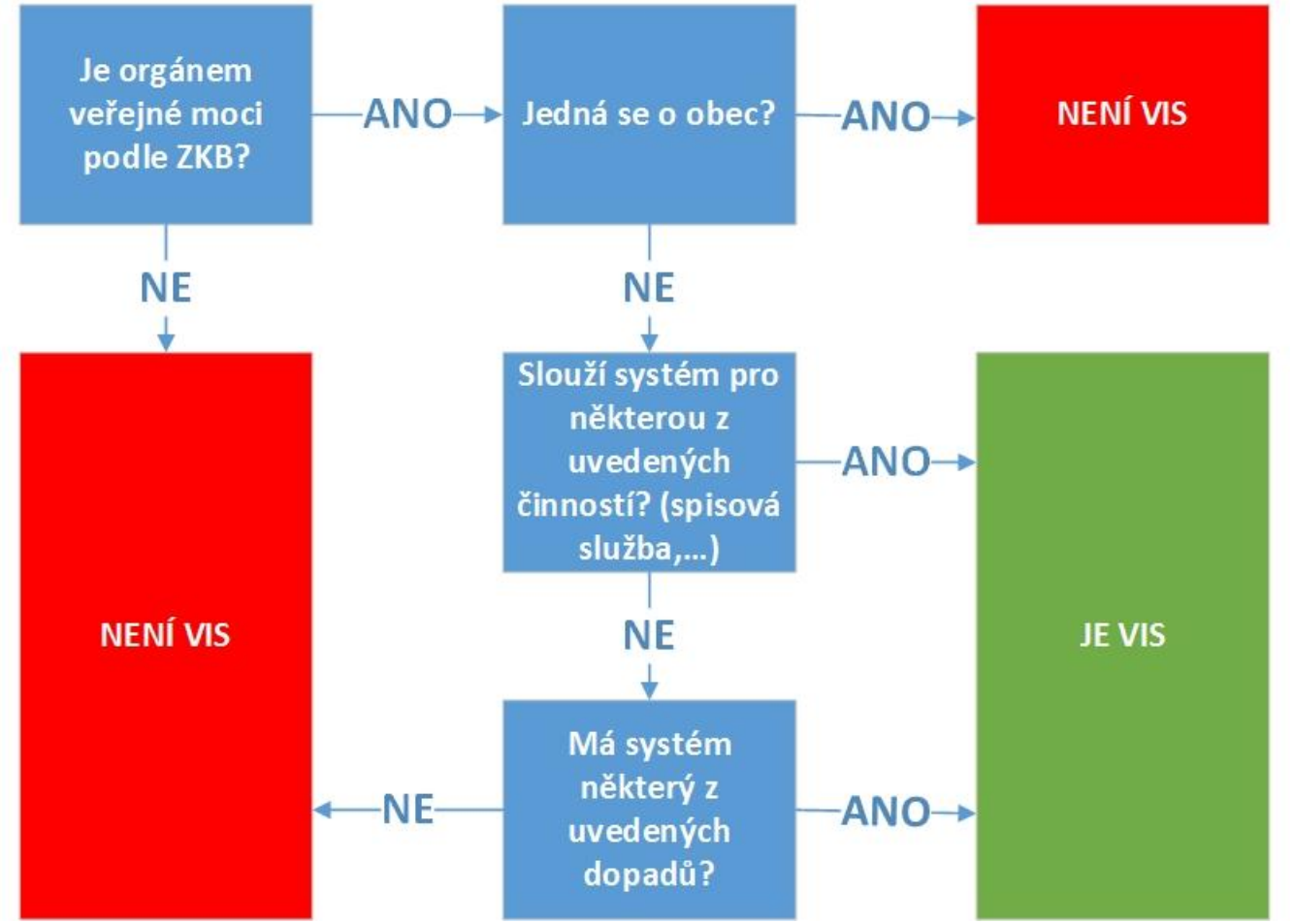
Národní úřad pro kybernetickou a informační bezpečnost vydá rozhodnutí o určení provozovatele základní služby a informačního systému základní služby

URČENÍ

* liší se v rámci jednotlivých služeb

Významný informační systém

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



Zákon o kybernetické bezpečnosti optikou obce

- **Zavádění bezpečnostní opatření (§ 4 a § 5).** – odpovědnost každého subjektu
  - jsou uvedeny ve vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat **(vyhláška o kybernetické bezpečnosti).**
- **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.

Zákon o kybernetické bezpečnosti optikou obce

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.

Zákon o kybernetické bezpečnosti optikou obce

Technická bezpečnostní opatření:

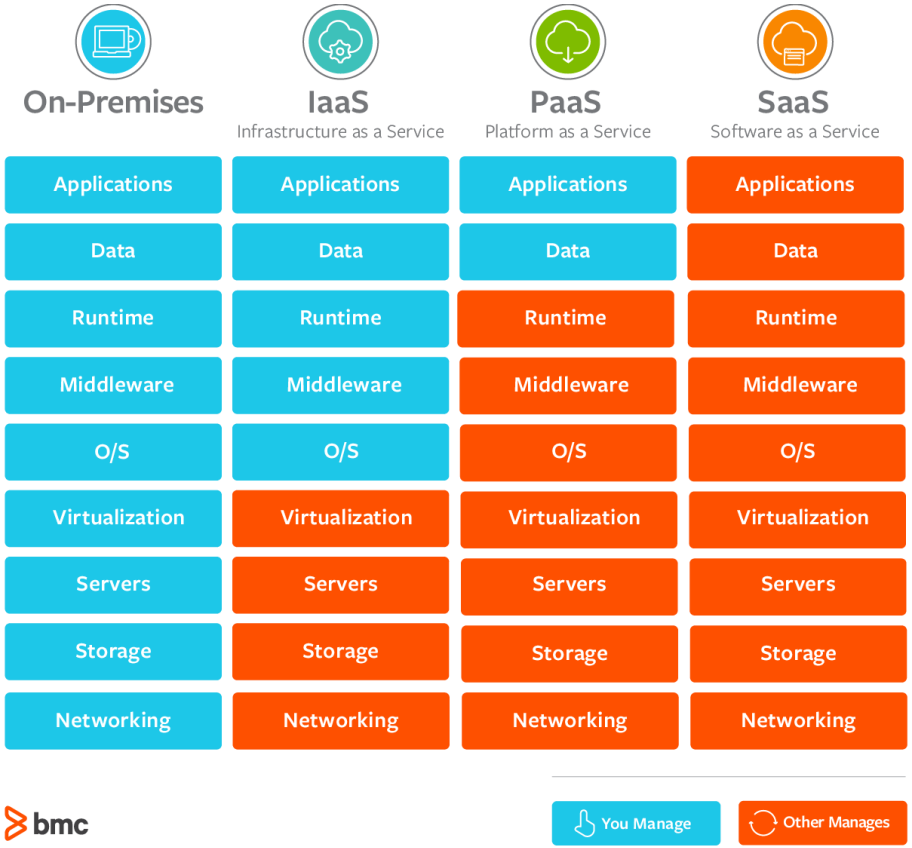
a) fyzická bezpečnost,
b) nástroj pro ochranu integrity komunikačních sítí,
c) nástroj pro ověřování identity uživatelů,
d) nástroj pro řízení přístupových oprávnění,
e) nástroj pro ochranu před škodlivým kódem,
f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů 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 řídících systémů.

Nová regulace cloud computingu

Co je to cloud computing

- *„… **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*



Proč regulovat cloud computing

- 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.

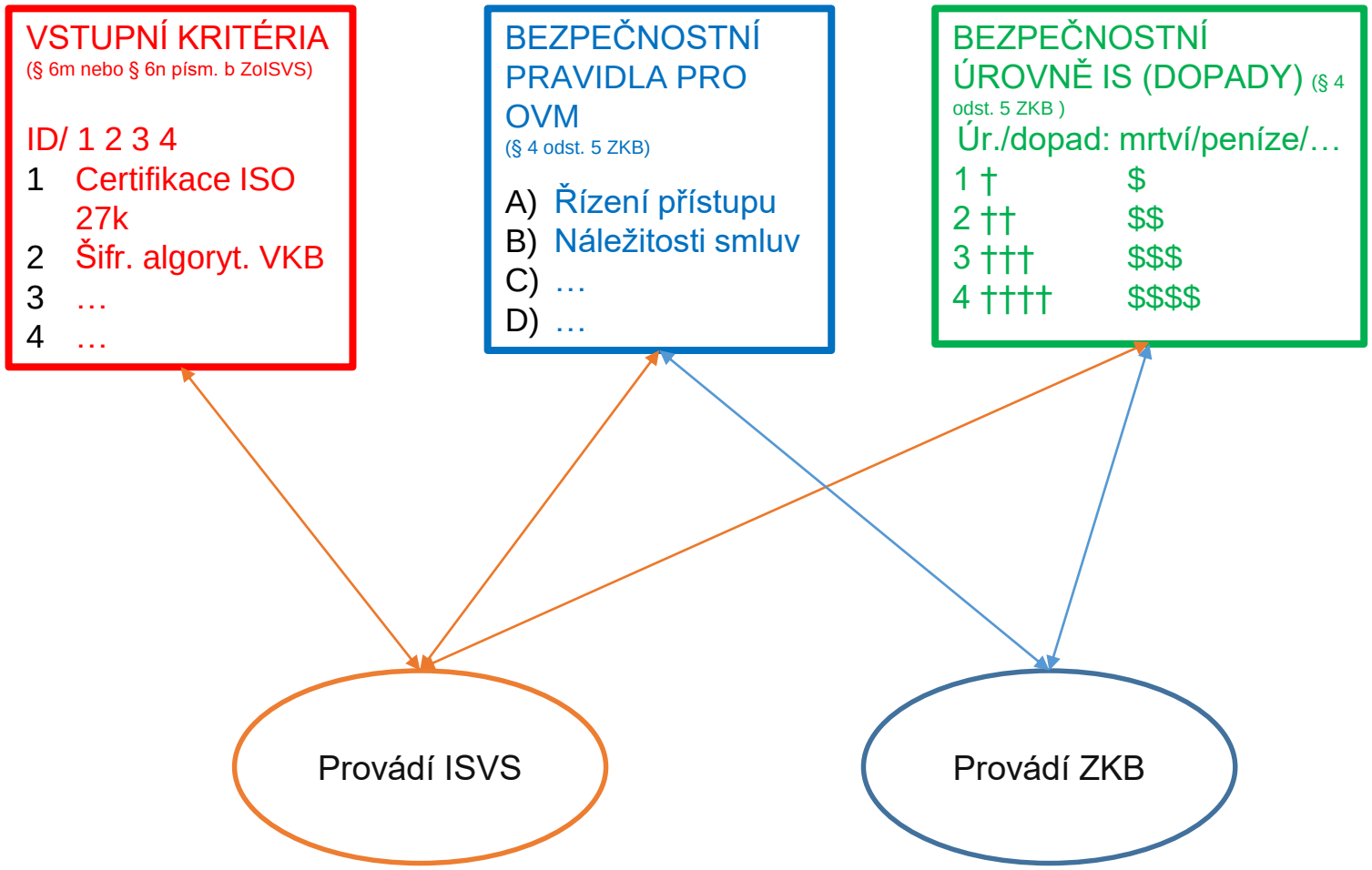
- Výdaje na ICT se v ČR mezi lety 2012 - 2016 téměř zdvojnásobily

(monitor.statnipokladna.cz)

- Zavedení cloudových řešení ve veřejném sektoru může snížit provozní náklady na IT o 10 – 50 %

(EY 2021)

Dva zákony a tři cloudové vyhlášky



I. Vstupní kritéria

- **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

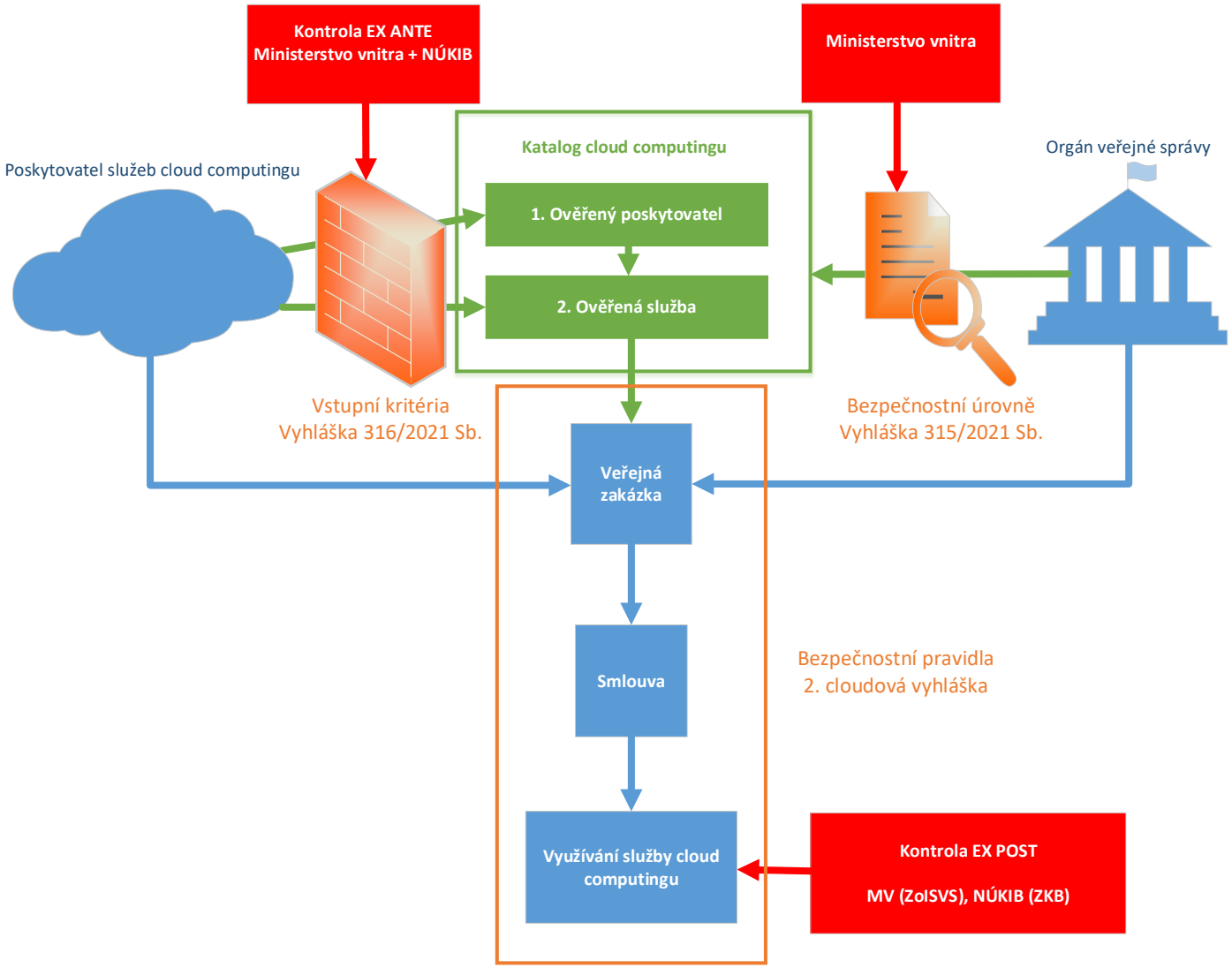
- **Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu**
  - Tzv. vyhláška o vstupních kritériích
  - Sada požadavků a podmínek, které musí poskytovatel cloudových služeb splnit aby je mohl dodávat orgánům veřejné správy
  - Účinná od 1. 9. 2021

II. Bezpečnostní pravidla

- **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



Přechodná ustanovení

- **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 využívaní 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

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 nespadají pod regulaci ZKB (výsledek spolupráce NÚKIB, MV a NAKIT)
  - Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály (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

Tato prezentace vznikla za podpory projektu "Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur" reg. č.: CZ.02.1.01/0.0/0.0/16_019/0000822 financovaného z EFRR.