CUSEC

Základy regulácie kybernetickej bezpečnosti a súvisiacich oblastí

Modul 2 - Základy právnej úpravy kybernetickej bezpečnosti
Časť 2

Doc. JUDr. Jozef Andraško, PhD.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality
CUSEC

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

PP SR

CUSEC

- **Národná stratégia pre informačnú bezpečnosť SR**
  - 27. august 2008
- **Akčný plán informačnej bezpečnosti pre roky 2009 - 2013**
  - 19. január 2010
- **Legislatívny zámer zákona o informačnej bezpečnosti**
  - 25. február 2010
- **Návrh zákona o informačnej bezpečnosti**
  - október 2014 (**legislatívny proces zastavený**)

PP SR

CUSEC

- **Koncepcia kybernetickej bezpečnosti SR na roky 2015-2020**
  - 17. jún 2015
- **Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020**
  - 19. január 2016
- **Návrh zákona o kybernetickej bezpečnosti**
  - máj 2017
- **Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti**
  - účinný od 1. apríla 2018
  - okrem čl. I § 12 ods. 6, ktorý nadobúda účinnosť 25. mája 2018

CUSEC

Čo a prečo?

Predmet

Audit KB a dohľad

Riadenie a zabezpečenie KB

Jednotky CSIRT

Správa v oblasti KB

- **podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti**
  - postavenie a povinnosti prevádzkovateľa základnej služby,
  - bezpečnostné opatrenia,
  - hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti,
  - riešenie kybernetického bezpečnostného incidentu,
  - opatrenia proti produktom IKT, službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu,

- **správa v oblasti kybernetickej bezpečnosti**
  - organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
  - úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti,
  - národnú stratégiu kybernetickej bezpečnosti,
  - národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy,
  - jednotný informačný systém kybernetickej bezpečnosti,
  - súčinnosť a výmenu informácií,

- **organizácia a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov** (ďalej len „jednotka CSIRT“) a ich akreditáciu

- **audit kybernetickej bezpečnosti a dohľad** nad plnením povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona

CUSEC

Kde a koho?

Pôsobnosť

CUSEC

pozitívna

- informačné systémy zriadené a prevádzkované v pôsobnosti Ministerstva obrany Slovenskej republiky v rozsahu určenom ústredným orgánom spôsobom podľa § 33 ods. 5.

(5) Ústredný orgán, ktorým je Ministerstvo obrany Slovenskej republiky, plní úlohy, ktoré mu vyplývajú z tohto zákona, prostredníctvom Vojenského spravodajstva.[34])

- osobu, ktorá poskytuje službu DNS, službu registrácie názvu domény, službu cloud computingu… , **ak má/nemá trvalý pobyt, miesto podnikania alebo sídlo** na území Slovenskej republiky,

§ 2 Pôsobnosť zákona

(1) Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti.

Pôsobnosť

CUSEC

Negatívna

- požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,

- osobitné ustanovenia o úlohách a oprávneniach spravodajskej služby pri ochrane kybernetického priestoru podľa osobitného predpisu,1)

- ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,2)

- požiadavky na zabezpečenie sietí a informačných systémov v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu,3)...

Pôsobnosť orgánov verejnej moci

CUSEC

- **NBÚ**

pre jednotlivé sektory/podsektory

- ústredný orgán (MD, MF, MH, MO, MV, MZ, MŽP, MIRRI, SŠHR)

- iný orgán štátnej správy
  - ministerstvá a ostatné ústredné orgány štátnej správy, ktoré nie sú ústredným orgánom
  - GP, NKÚ, ÚPDZS, ÚOOÚ, ÚRSO..

NBÚ

CUSEC

- **Úlohy** (a-af)
- na účely zabezpečenia plnenia úloh **môže uzatvoriť písomnú dohodu o spolupráci s fyzickou/právnickou osobou**
- zriaďuje Národné centrum kybernetickej bezpečnosti (SK CERT)
  - má **postavenie národnej jednotky CSIRT**
- je **správcom** a **prevádzkovateľom jednotného informačného systému kybernetickej bezpečnosti (JIS KB)**
- **akredituje** jednotky CSIRT

NBÚ

CUSEC

- je vnútroštátnym orgánom pre **certifikáciu kybernetickej bezpečnosti** a **orgánom posudzovania zhody** podľa osobitného predpisu

- rozhoduje o **blokovaní škodlivého obsahu alebo škodlivej aktivity**, ktorá smeruje do kybernetického priestoru Slovenskej republiky alebo z kybernetického priestoru Slovenskej republiky (ďalej len „blokovanie“) a zabezpečuje vykonanie tohto rozhodnutia alebo vykonáva blokovanie na základe žiadosti.

NBÚ (§ 27a)

CUSEC

- Úrad môže rozhodnutím **zakázať alebo obmedziť používanie** **konkrétneho produktu, procesu, služby** alebo **tretej strany** na poskytovanie služby ak zistí, že takéto používanie

  – neumožňuje alebo zásadným spôsobom **sťažuje udržanie kybernetickej bezpečnosti**, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo

  – ohrozuje **bezpečnostné záujmy** Slovenskej republiky.

GENERAL TECHNOLOGY

The HUAWEI ban explained: A complete timeline and everything you need to know

What has happened to HUAWEI since May 2019? Here's a full summary of the HUAWEI ban.

By C. Scott Brown • December 12, 2022

Regulované subjekty

Od 1.1.2025

PZS
PKZS

Od 1.8.2021
do 31.12.2024

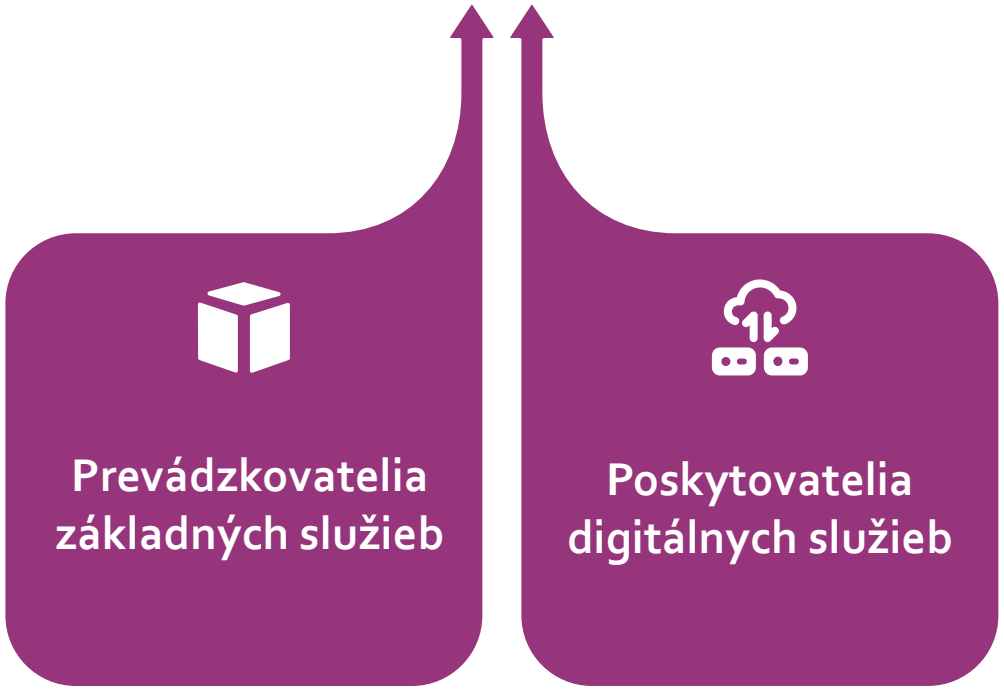
PZS (2 ZS)
PDS

Do 31.7.2021

PZS (3 ZS)
PDS

Regulované subjekty

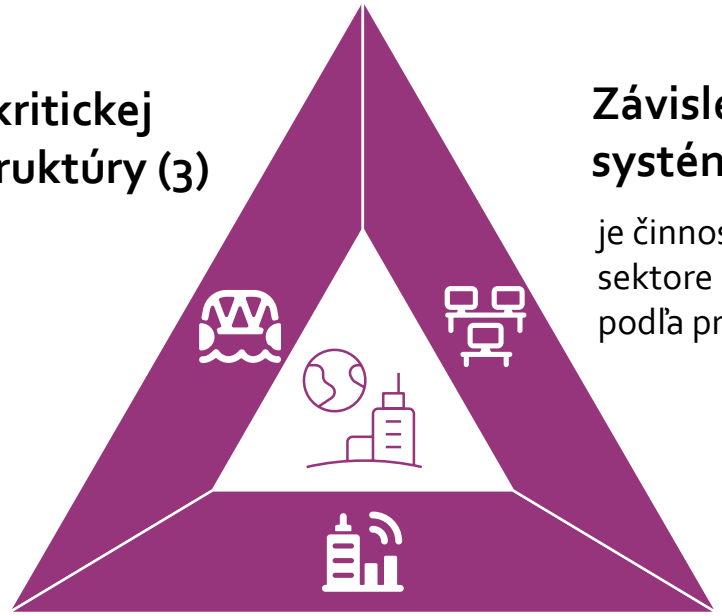
Do 31.7.2021


Prevádzkovatelia základných služieb
Poskytovatelia digitálnych služieb

CUSEC

Základné služby

Prvky kritickej infraštruktúry (3)



Závislé od sietí a systémov (1)

je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,

Informačné systémy verejnej správy (2)

Do 31.7.2021

10. Verejná správa	Bezpečnosť	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sa týkajú bezpečnosti Slovenskej republiky**	Ministerstvo vnútra Slovenskej republiky
	Informačné systémy verejnej správy	**správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy** v pôsobnosti povinnej osoby podľa zákona č. 275/2006 Z. z. podporujúci služby verejnej správy, služby vo verejnom záujme a verejné služby	Úrad podpredsedu vlády pre investície a informatizáciu
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	

Do 31.7.2021

Závislé od sietí a systémov (1)

je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,

- V ZoKB - identifikačné kritériá **prevádzkovanej služby**
  - **dopadové**
  - **špecifické**

- ak subjekt tieto kritériá **prekročí (naplní),** následne možno hovoriť o tom, že má po procese zaradenia postavenie **PZS**

Do 31.7.2021

(2) Dopadové kritériá sú určené všeobecne záväzným právnym predpisom, ktorý vydá úrad, a zohľadňujú najmä

a) počet používateľov využívajúcich základnú službu,

b) závislosť ostatných sektorov podľa *prílohy č. 1* od základnej služby,

c) vplyv, ktorý by mohli mať kybernetické bezpečnostné incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti a záujmy štátu alebo na bezpečnosť štátu,

d) trhový podiel prevádzkovateľa služby,

e) geografické rozšírenie z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť,

f) význam prevádzkovateľa základnej služby z hľadiska zachovania kontinuity poskytovania služby.

(3) Špecifické sektorové kritériá zohľadňujú kritériá určené všeobecne záväzným právnym predpisom, ktorý vydá úrad.

VEREJNÁ SPRÁVA

Prevádzkovateľ služieb (príloha č. 1 k zákonu)	**Špecifické sektorové kritériá** (jednotlivo)	**Dopadové kritériá** (jednotlivo) **Dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť:**
Orgán verejnej moci.	Služba, ktorá je na základe vyhodnotenia rizík v rámci organizácie definovaná ako podstatná služba v jednom podsektore a) bezpečnosti, b) informačných systémov verejnej správy, c) obrany, d) spravodajské služby, alebo e) utajovaných skutočností vo vzťahu k fungovaniu príslušného ústredného orgánu podľa zákona.	Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ktoré postihuje viac ako 1 000 osôb. Obmedzenie či narušenie prevádzky prvku kritickej infraštruktúry. Obmedzenie či narušenie prevádzky siete a informačného systému, ktoré môže mať: negatívny vplyv na fungovanie orgánu verejnej moci, vplyv na výkon činnosti orgánu verejnej moci pri zaisťovaní prípravy na krízové situácie, vplyv na obmedzenie výkonu alebo ohrozenie pôsobnosti organu verejnej moci. Viac ako jedna zranená osoba vyžadujúca lekárske ošetrenie. Narušenie verejného poriadku, verejnej bezpečnosti, mimoriadnu udalosť alebo tieseň, ktorá môže vyžadovať vykonanie záchranných prác, alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.

PL. ÚS 25/2019 (e-KASA)

CUSEC

- V oblasti kybernetickej bezpečnosti zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoKB"), ako aj zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoITVS") stanovujú finančnej správe ďalšie konkrétne povinnosti v oblasti bezpečnosti. **Systém e-kasa prevádzkovaný finančnou správou zjavne musí spadať pod pojem „základnej služby"** podľa jednej alebo viacerých alternatív v rámci § 3 písm. k) ZoKB. Z čl. 3 smernice č. 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, ktorých je ZoKB implementáciou, je zrejmé, že vyňatie z tohto režimu je možné len pri zabezpečení vyššej osobitnej ochrany, ktorej v tomto prípade niet. Vzhľadom na zákonnú povinnosť podľa § 17 ods. 1 ZoKB existuje **povinnosť finančnej správy posúdiť a následne notifikovať Národný bezpečnostný úrad (ďalej len „NBÚ") o prekročení dopadových kritérií** podľa § 18 ZoKB. Keďže e-kasa je plošný systém, na ktorý sú naviazané obchodné transakcie v celej krajine v reálnom čase, je pomerne ťažké si predstaviť záver, že tieto kritériá nie sú splnené.

- NBÚ zaradí **základnú službu (1)** do **zoznamu ZS** a jej prevádzkovateľa do **registra PZS**:
  - na základe **oznámenia** prevádzkovateľom tejto služby
  - na základe **podnetu ústredného orgánu**
  - z **vlastnej iniciatívy**

- NBÚ **v spolupráci s príslušným ústredným orgánom** zaradí **základnú službu (2)** do zoznamu ZS a jej prevádzkovateľa do registra PZS

- NBÚ zaradí **základnú službu (3)** do zoznamu ZS a jej prevádzkovateľa do registra PZS **zo zákona**

Do 31.7.2021

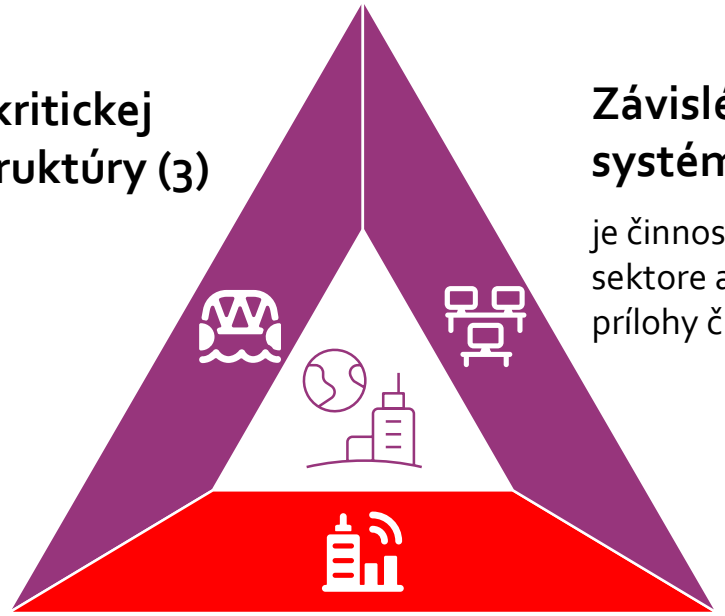
Regulované subjekty

Od 1.8.2021
do 31.12.2024

CUSEC

Základné služby

Prvky kritickej infraštruktúry (3)



Závislé od sietí a systémov (1)

je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1

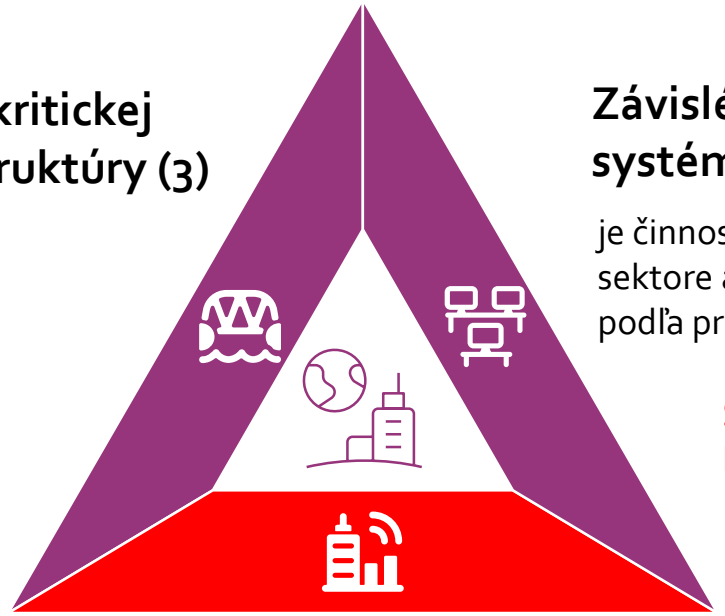
Informačné systémy verejnej správy (2)

Od 1.8.2021
do 31.12.2024

CUSEC

Základné služby

Prvky kritickej infraštruktúry (3)



Závislé od sietí a systémov (1)

je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1

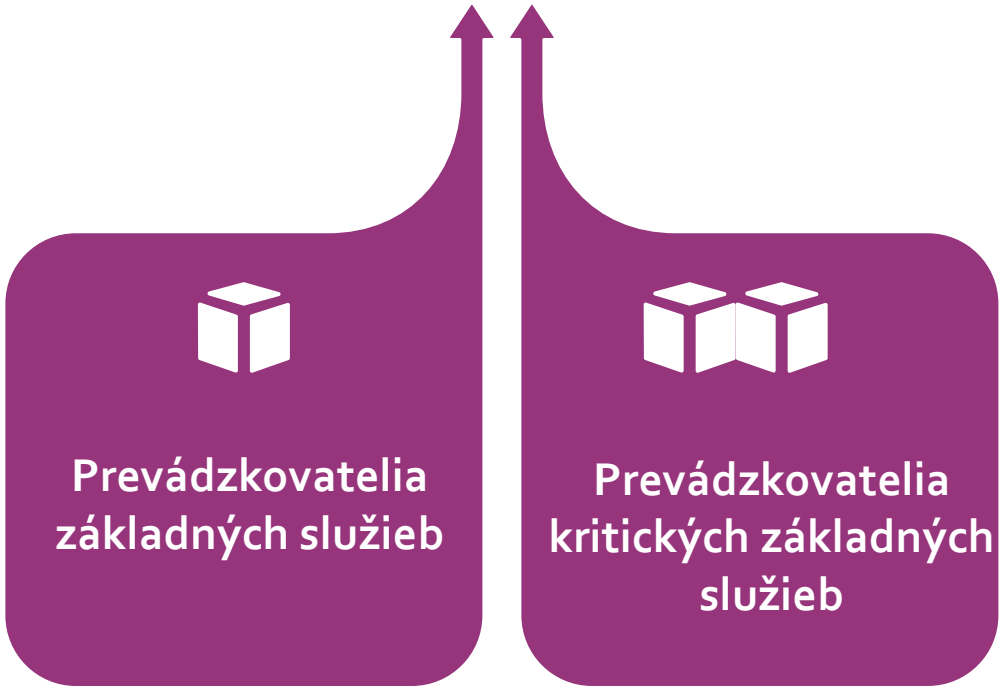
Sektor - Verejná správa
Podsektor - ISVS

Informačné systémy verejnej správy (2)

Od 1.8.2021
do 31.12.2024

Regulované subjekty

Od 1.1.2025


Prevádzkovatelia základných služieb
Prevádzkovatelia kritických základných služieb

Prevádzkovateľ základnej služby (PZS)

PZS

Kľúčové subjekty (essential entities)
Dôležité subjekty (important entities)

- NIS 2?

- Prevádzkovateľom základnej služby je ten, **kto je zapísaný v registri prevádzkovateľov základnej služby**.

367

ZÁKON

z 27. novembra 2024

o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov

Kritické subjekty

b) základnou službou služba kritického subjektu, ktorá má zásadný význam z hľadiska zachovania životne dôležitých spoločenských funkcií alebo hospodárskych činností, vrátane ochrany verejného zdravia, bezpečnosti alebo životného prostredia a ktorá je uvedená v prílohe č. 1,

Zápis PZS

CUSEC

Do registra prevádzkovateľov základnej služby sa zapisuje

a) **ústredný orgán štátnej správy** a iný štátny orgán s celoštátnou pôsobnosťou,

b) **kritický subjekt**,

c) osoba **bez ohľadu na splnenie podmienok veľkosti pre stredný podnik**, ktorá vykonáva činnosť v niektorom zo sektorov podľa **prílohy č. 1 alebo prílohy č. 2** a ktorá .... (**1-9**)

1. je podnikom poskytujúcim verejnú elektronickú komunikačnú sieť alebo verejnú elektronickú komunikačnú službu,

2. je poskytovateľom dôveryhodnej služby,

3. je správcom TLD,

4. poskytuje službu DNS,

5. je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou,

6. poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,

7. poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko najmä v sektore, v ktorom by takéto narušenie alebo zásah mohli mať cezhraničný vplyv,

8. je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo

9. je subjektom hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu,[23])

y) kľúčovou službou služba pre zachovanie dôležitých spoločenských oblastí alebo hospodárskych činností, pri ktorej dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo v sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť

1. ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb,

2. obmedzenie alebo narušenie kritického subjektu, jeho základnej služby alebo kritickej infraštruktúry,

3. hospodársku stratu vyššiu ako 0,1 % hrubého domáceho produktu podľa údajov z bezprostredne predchádzajúceho rozpočtového roka, alebo

4. hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 eur,

z) významným vplyvom na verejný poriadok, bezpečnosť alebo verejné zdravie vplyv, pri ktorom dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo v sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť narušenie verejného poriadku, bezpečnosti, ohrozenie verejného zdravia, mimoriadnu udalosť alebo tieseň, ktorá môže

1. vyžadovať vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni,

2. spôsobiť viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo úmrtie aspoň jednej osoby.

aa) významným systémovým rizikom riziko narušenia systému, ktoré môže mať závažné negatívne dôsledky alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo ohrozuje bezpečnostné záujmy Slovenskej republiky,

Zápis PZS

CUSEC

d) **štátny orgán vykonávajúci pôsobnosť v najmenej dvoch okresoch a vyšší územný celok**, ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie; ustanovenie písmena a) tým nie je dotknuté,

e) **osoba, ktorá spĺňa najmenej podmienky veľkosti pre stredný podnik** a vykonáva činnosť v niektorom zo sektorov podľa

- **prílohy č. 1** (SEKTORY S VYSOKOU ÚROVŇOU KRITICKOSTI) alebo
- **prílohy č. 2** (INÉ KRITICKÉ SEKTORY).

Zápis PZS

CUSEC

f) **mesto**, ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,

g) **správca informačnej technológie verejnej správy**23a),

h) osoba, ktorá poskytuje **službu registrácie názvu domény** bez ohľadu na splnenie podmienok veľkosti pre stredný podnik alebo

i) **tretia strana**, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu.

Zápis PZS

CUSEC

- Ten, kto vykonáva činnosť podľa odseku 1 je povinný **do 60 dní odo dňa, kedy činnosť začne vykonávať, oznámiť to úradu**.

- Oznámenie podľa predchádzajúcej vety **musí obsahovať**
  - názov, sídlo a kontaktné údaje vrátane elektronických adries, verejných IP adries a telefónnych čísel,
  - zoznam členských štátov Európskej únie, v ktorých vykonáva činnosť alebo poskytuje službu,
  - názov, sídlo a kontaktné údaje zástupcu podľa § 21 ods. 1.

Noví PZS

Zápis PZS

CUSEC

- **NBÚ zapíše** do registra prevádzkovateľov základnej služby osobu podľa odseku 1
  - po **predchádzajúcej konzultácii** s príslušným ústredným orgánom, a to z **vlastnej iniciatívy** alebo na základe **odôvodnenej žiadosti** osoby podľa odseku 1, alebo
  - na **návrh príslušného ústredného orgánu**.

- **oznámi** bezodkladne prevádzkovateľovi základnej služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti

- **doručí** do elektronickej schránky

- osobitné **rozhodnutie sa nevydáva**

SP vylúčený

Prevádzkovateľ kritickej základnej služby (PKZS)

Kritická ZS

CUSEC

- výkon pôsobnosti **ústredného orgánu štátnej správy**10) alebo **iného štátneho orgánu s celoštátnou pôsobnosťou**,
- **činnosť v sektore podľa prílohy č. 1**, okrem sektoru verejná správa, ak ju vykonáva **osoba, ktorá prekračuje limity veľkosti určené pre stredný podnik**,23c)
- kvalifikovaná dôveryhodná služba,
- správa TLD,
- služba DNS,

Veľký podnik

Kritická ZS

CUSEC

- poskytovanie **verejnej elektronickej komunikačnej siete alebo verejnej elektronickej komunikačnej služby osobou**, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik,
- vykonávanie **činnosti** alebo **existencia postavenia** podľa § 17 ods. 1 písm. c) piateho až deviateho bodu,
- poskytovanie **základnej služby kritickým subjektom**, alebo
- **informačná činnosť a elektronické služby**, vykonávané s použitím **informačnej technológie verejnej správy**,23a) určených úradom.

5.	je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou,
6.	poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
7.	poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko najmä v sektore, v ktorom by takéto narušenie alebo zásah mohli mať cezhraničný vplyv,
8.	je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo
9.	je subjektom hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu,[23])

Prevádzkovateľ KZS

CUSEC

PKZS

- ak prevádzkovateľ základnej služby vykonáva **aspoň jednu** z kritických základných služieb, je **prevádzkovateľom kritickej základnej služby** a túto skutočnosť je **povinný oznámiť** úradu.

- skutočnosť, že prevádzkovateľ základnej služby prevádzkuje kritickú základnú službu, ako aj každú zmenu v týchto skutočnostiach, zapíše úrad **do registra prevádzkovateľov základnej služby**;

- na toto oznámenie a spôsob zápisu, ako aj na povinnosť oznamovania zmien a na ich zápis sa primerane použije § 17 ods. 3

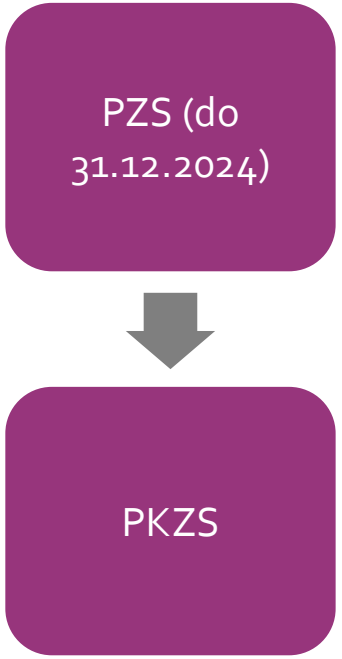
PZS po novele?

Prechodné ustanovenia (§ 34b)

CUSEC

- **Prevádzkovateľ základnej služby** podľa tohto zákona v znení účinnom do 31. decembra 2024 sa považuje za **prevádzkovateľa kritickej základnej služby** podľa tohto zákona v znení účinnom od 1. januára 2025.

- Úrad môže do 31. decembra 2026 **aj z vlastnej iniciatívy rozhodnúť, ktorá z osôb podľa odseku 1 nie je prevádzkovateľom kritickej základnej služby** z dôvodu, že nespĺňa podmienky podľa § 18 ods. 1 v znení účinnom od 1. januára 2025.



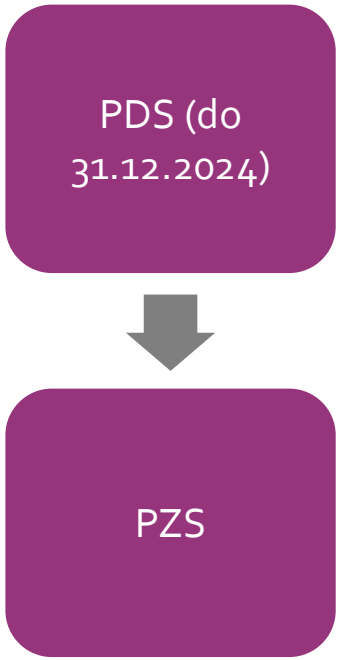
PDS po novele?

Prechodné ustanovenia (§ 34b)

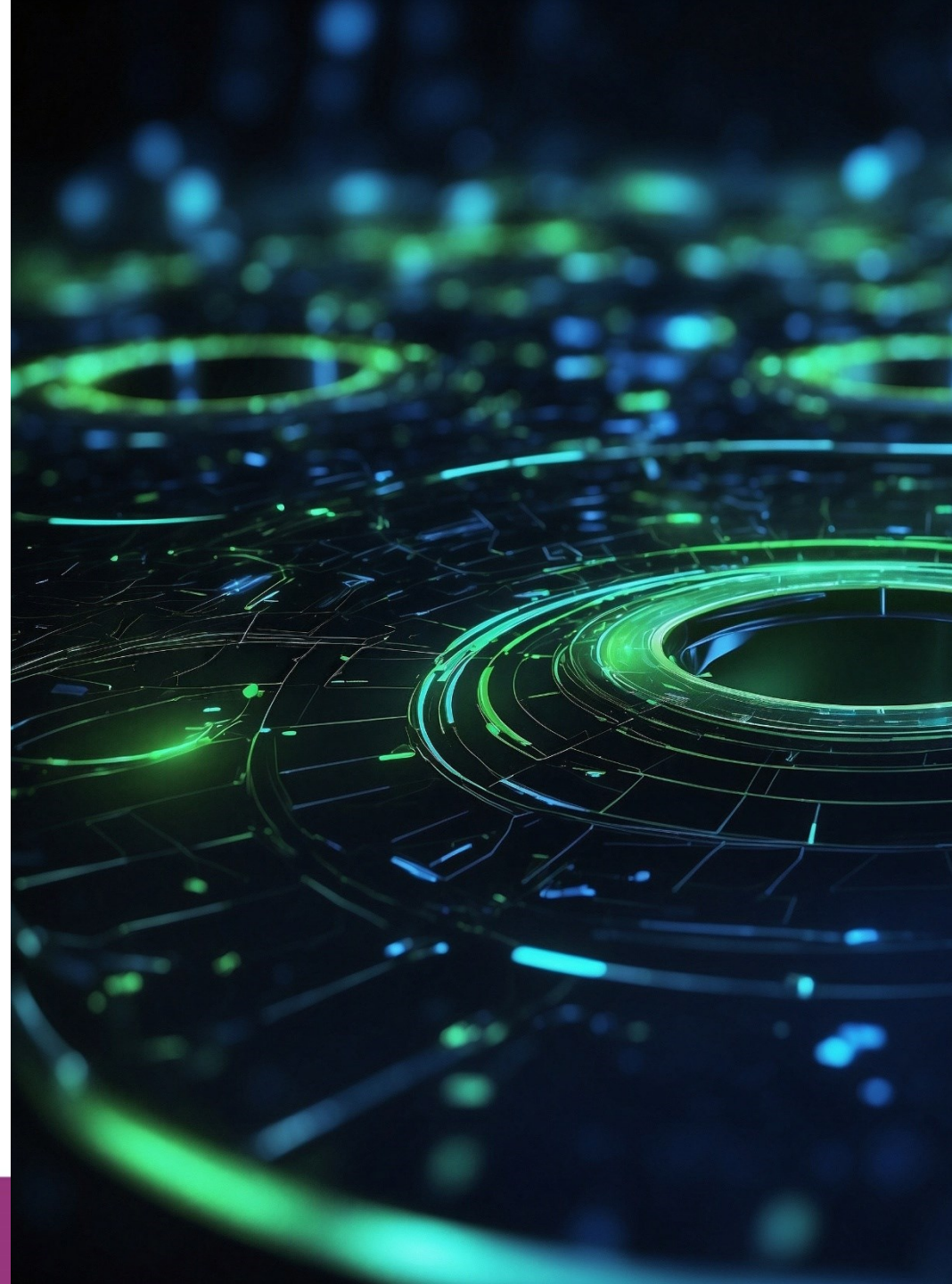
CUSEC

- **Poskytovateľ digitálnej služby** podľa tohto zákona v znení účinnom do 31. decembra 2024 sa považuje za **prevádzkovateľa základnej služby** podľa tohto zákona v znení účinnom od 1. januára 2025.

- Úrad môže **aj z vlastnej iniciatívy do 31. decembra 2026 rozhodnúť, ktorá z osôb podľa odseku 3 nie je prevádzkovateľom základnej služby** z dôvodu, že nespĺňa podmienky podľa § 17 ods. 1 v znení účinnom od 1. januára 2025.



Ak PZS spadá do viacerých sektorov/podsektorov?



- prevádzkovateľ základnej služby **spadá**
  - pod viaceré sektory alebo
  - pod rôzne ústredné orgány

- pôsobnosť podľa ZoKB je určená **úradom** na základe **predchádzajúcej konzultácie** s dotknutým **prevádzkovateľom základnej služby a ústredným orgánom**

Výmaz PZS

Výmaz PZS

CUSEC

- NBÚ môže **vymazať** prevádzkovateľa základnej služby **z registra prevádzkovateľov základnej služby**
  - na základe **odôvodnenej žiadosti** prevádzkovateľa základnej služby, po **predchádzajúcej konzultácii s príslušným ústredným orgánom**, najneskôr do 60 dní odo dňa doručenia odôvodnenej žiadosti,
  - na základe **oznámenia ústredného orgánu**, alebo
  - z **vlastnej iniciatívy** v odôvodnených prípadoch.

CUSEC

Ako a kedy?

Bezpečnostné opatrenia

Oznamovacie povinnosti

Iné povinnosti

Bezpečnostné opatrenia

Bezpečnostné opatrenia

CUSEC

- Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby **v závislosti od vykonanej analýzy rizík prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia** najmenej v rozsahu bezpečnostných opatrení podľa § 20 a vykonávať ich s cieľom zabezpečovania kybernetickej bezpečnosti a odolnosti.

- Na účely plnenia povinnosti podľa prvej vety prevádzkovateľ základnej služby **prijíma, dodržiava a vykonáva** sektorové bezpečnostné opatrenia, ak sú ustanovené;24) povinnosť prijímať opatrenia podľa § 20 ods. 4 tým nie je dotknutá.

- Osoba poskytujúca niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa § 2 ods. 2 plní bezpečnostné opatrenia podľa **osobitného predpisu**.24a)".

Bezpečnostné opatrenia

CUSEC

- realizované na základe vykonanej **analýzy rizík**
- určuje pravdepodobnosť vzniku škodlivej udalosti
- s prihliadnutím na
  - bezpečnostné metodiky a politiky úradu,
  - najnovšie bezpečnostné trendy a medzinárodné normy
- v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti

Bezpečnostné opatrenia

CUSEC

- **analýza politického rizika tretej strany**

- politické riziko sa **posudzuje najmä vzhľadom** na
  - plnenie záväzkov z medzinárodných zmlúv,
  - možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy,
  - analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany,
  - analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií,
  - informácie špecifické pre cudzí štát a informácie spravodajskej služby o možných kybernetických hrozbách pre záujmy Slovenskej republiky.

Bezpečnostné opatrenia

CUSEC

- určenie manažéra kybernetickej bezpečnosti
  - nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií
  - spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,
- detekciu kybernetických bezpečnostných incidentov
- evidenciu kybernetických bezpečnostných incidentov
- postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
- určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
- pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania

Bezpečnostné opatrenia

CUSEC

- určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok prevádzkovateľa základnej služby

- zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené roly

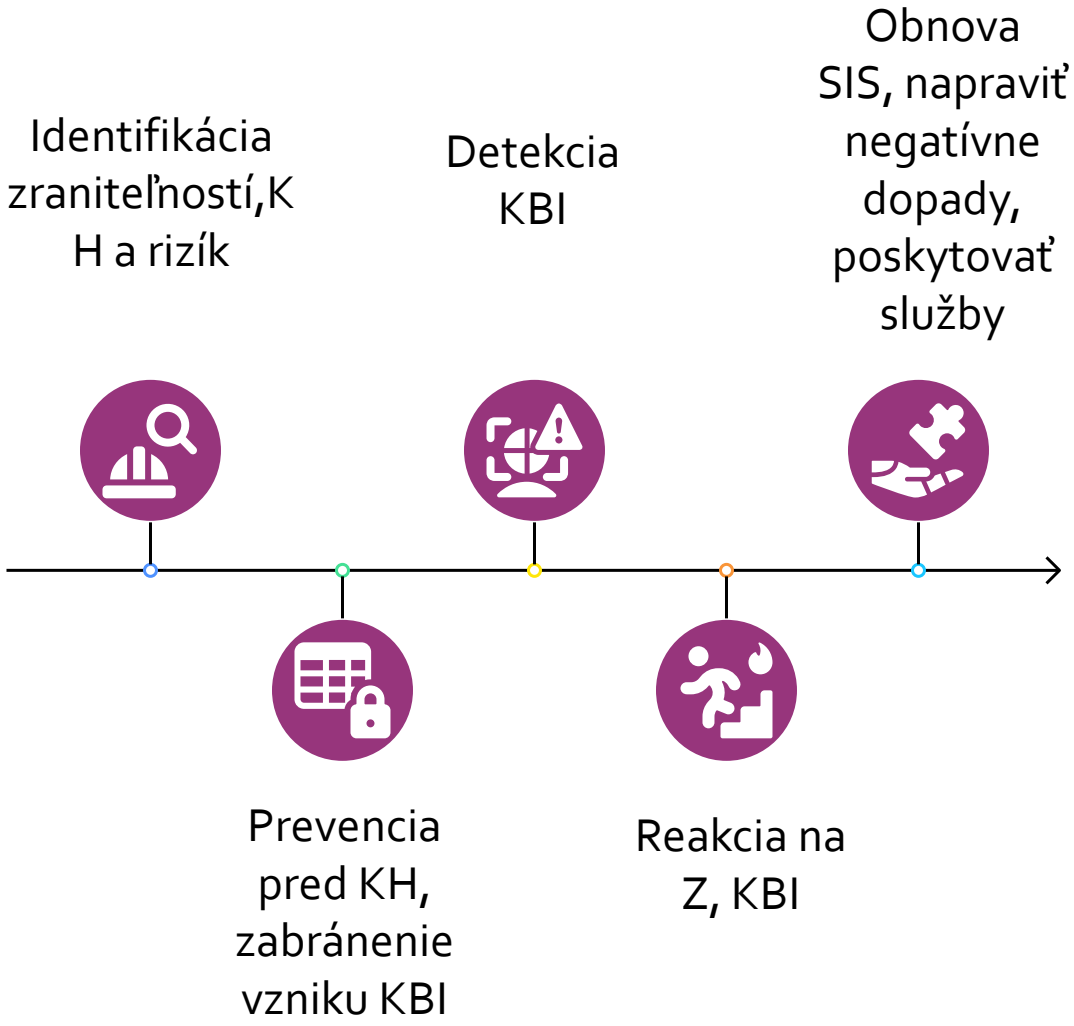
- určenie konkrétnej osoby alebo konkrétnych osôb zodpovedných za schvaľovanie bezpečnostných opatrení, dohľad, kontrolu a audit, zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie,

- vzdelávanie a budovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti.

Bezpečnostné opatrenia

CUSEC

- Vyhláška Národného bezpečnostného úradu 227/2025 Z. z. o bezpečnostných opatreniach


Identifikácia zraniteľností,K H a rizík
Detekcia KBI
Obnova SIS, napraviť negatívne dopady, poskytovať služby
Prevencia pred KH, zabránenie vzniku KBI
Reakcia na Z, KBI

Bezpečnostné opatrenia

CUSEC

- PZS je povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom **tretej strany**, **uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení** a **notifikačných povinností** podľa ZoKB počas celej doby výkonu tejto činnosti;

- pri uzatvorení zmluvy sa vykonáva **analýza rizík**

- tretia strana je počas trvania zmluvného vzťahu povinná vykonávať a realizovať bezpečnostné opatrenia **v súlade s písomnou zmluvou a ZoKB** a je povinná podrobiť sa **kontrole** plnenia týchto opatrení **zo strany PZS**

Bezpečnostné opatrenia

CUSEC

- ak ide o zmluvu uzatvorenú s prevádzkovateľom základnej služby, ktorý prevádzkuje **kritickú základnú službu**, kontrolu môže vykonávať aj **NBÚ**;

- na tento účel má **tretia strana** **postavenie PZS**.

- uzatvorenie zmluvy nesmie brániť v hospodárskej súťaži.

PL. ÚS 25/2019 (e-KASA)

CUSEC

- Akýkoľvek útok na e-kasu alebo únik dát z nej môžu mať nedozerné dôsledky pre dotknutých podnikateľov, ich podnikateľskú činnosť a obyvateľstvo. Ako dôsledok má finančná správa niekoľko **zásadných bezpečnostných povinností vrátane povinnosti prijať bezpečnostné opatrenia v personálnej a technologickej oblasti, povinnosti detegovať, evidovať, oznamovať NBÚ a aktívne riešiť bezpečnostné incidenty (§ 19, § 20 ZoKB), ako aj povinnosti podrobovať sa dohľadu NBÚ a nezávislým auditom (§ 28, § 29 ZoKB).**

CUSEC

Oznamovacie povinnosti

Kto?

Čo?

Komu?

Lehota?

Incidenty

Hrozby

Udalosti

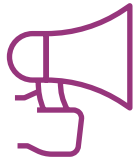
Zraniteľnosti

Incidenty

Hlásenie KBI

CUSEC

- **kybernetickým bezpečnostným incidentom** udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov



závažný kybernetický bezpečnostný incident

Hlásenie KBI

CUSEC

- Prevádzkovateľ základnej služby je **povinný informovať** v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente

- za predpokladu, že by sa plnenie zmluvy stalo nemožným, ak úrad nerozhodne inak

Hlásenie KBI

CUSEC

- Za **závažný kybernetický bezpečnostný incident** sa považuje **rozsiahly kybernetický bezpečnostný incident** a **kybernetický bezpečnostný incident**, ktorý

  – spôsobil alebo môže spôsobiť **závažné narušenie fungovania prevádzkovateľa základnej služby**, alebo škodu, inú ujmu na majetku alebo ušlý zisk vo **veľkom rozsahu**,

  nad 650 000 eur

  – zasiahol alebo môže zasiahnuť iné **osoby** tým, že im spôsobí **škodu, inú ujmu alebo ušlý zisk** v značnom rozsahu.

  nad 250 000 eur

Hlásenie KBI

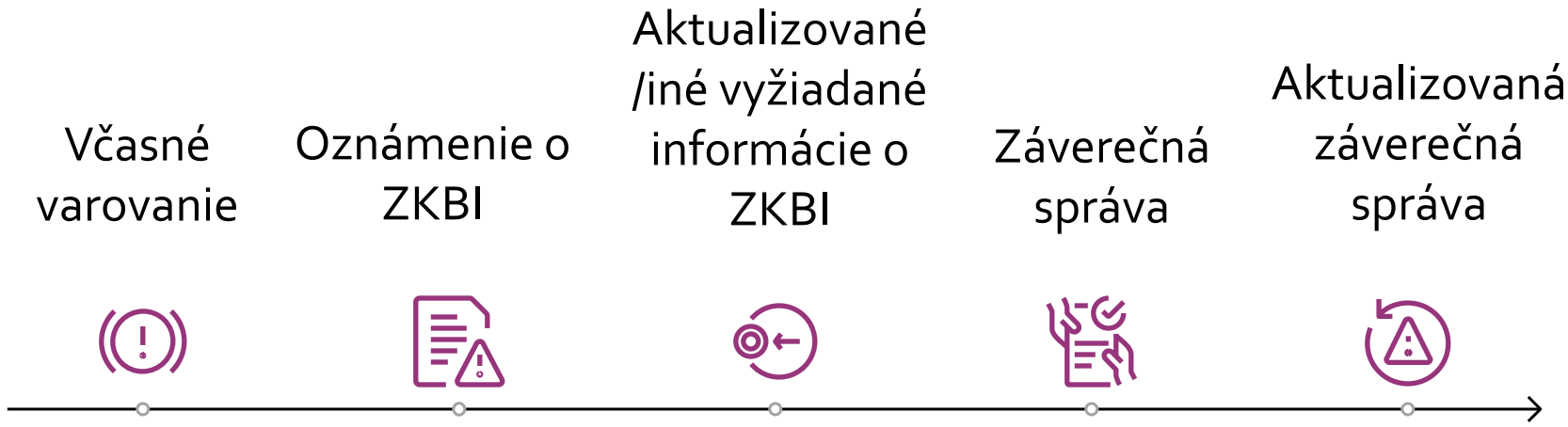
CUSEC

- **rozsiahly kybernetický bezpečnostný incident**

- kybernetický bezpečnostný incident, ktorý spôsobí narušenie na úrovni **presahujúcej schopnosť Slovenskej republiky naň reagovať**, alebo ktorý má významný vplyv aspoň na **dva členské štáty** Európskej únie,

Vyhláška č. 226/2025 Z. z.

CUSEC



Druh	Lehota	Obsahové náležitosti (v prípade potreby)
včasné varovanie	bez zbytočného odkladu, avšak najneskôr do **24 hodín** od zistenia ZKBI	• či závažný kybernetický bezpečnostný incident mohol byť spôsobený protiprávnym konaním, alebo či môže mať cezhraničný vplyv • uvádza sa tiež vplyv na poskytovanie dôveryhodných služieb (ak PZS je poskytovateľ DS)
oznámenie o ZKBI	bez zbytočného odkladu najneskôr do **72** hodín od zistenia ZKBI *poskytovateľ dôveryhodných služieb do 24 hodín	• aktualizujú sa a dopĺňajú informácie z včasného varovania, • sa uvádza prvotné posúdenie kybernetického bezpečnostného incidentu, jeho závažnosti a následkov
aktualizované alebo iné vyžiadané informácie o priebehu ZKBI	- na žiadosť toho, kto prevádzkuje jednotku CSIRT - v určenej lehote	

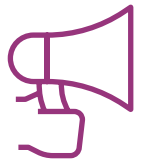
Druh oznámenia	Lehota	Obsahové náležitosti
záverečná správa	najneskôr **jeden mesiac** po nahlásení oznámenia o ZKBI	• podrobný opis ZKBI vrátane jeho závažnosti a následkov, • druh kybernetickej hrozby alebo hlavnú príčinu, ktorá pravdepodobne kybernetický bezpečnostný incident spôsobila, • zavedené a prebiehajúce opatrenia a • cezhraničný vplyv, ak existuje,
aktualizovaná záverečná správa (prebiehajúce ZKBI-cezhraničné)	• do **30 dní** odo dňa obnovy riadnej prevádzky siete a informačného systému • ak ide o ZKBI **s cezhraničným vplyvom**	
aktualizovaná záverečná správa + ďalšie aktualizované alebo iné vyžiadané informácie (prebiehajúce ZKBI)	• do **30 dní** odo dňa, keď sa KBI vyriešil	

Hrozby

Hlásenie

CUSEC

- **významnou kybernetickou hrozbou** kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má **potenciál spôsobiť závažný kybernetický bezpečnostný incident** alebo môže mať **iný závažný vplyv na sieť a informačný systém subjektu** alebo **používateľov služieb** subjektu tým, že spôsobí **značnú škodu**



významnú kybernetickú hrozbu, o ktorej sa dozvie

CUSEC

Oznamovacie povinnosti (NIS 2 čl. 23)

- **Významné kybernetické hrozby**

- Členské štáty v náležitých prípadoch zabezpečia, aby kľúčové a dôležité subjekty **bez zbytočného odkladu** oznámili **príjemcom** **svojich služieb**, ktorí potenciálne **čelia významnej kybernetickej hrozbe**, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať.

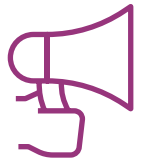
- Subjekty **v prípade potreby** týchto príjemcov informujú aj **o samotnej významnej kybernetickej hrozbe**.

Udalosti

Hlásenie

CUSEC

- **udalosťou odvrátenou v poslednej chvíli** udalosť, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo,



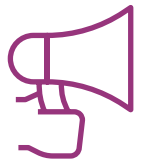
udalosť odvrátenú v poslednej chvíli, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident,

Zraniteľnosti

Hlásenie

CUSEC

- **zraniteľnosťou** akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou,



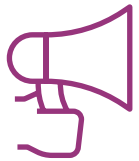
zraniteľnosť ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí môže byť zneužitá na spôsobenie závažného kybernetického bezpečnostného incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika.

Dobrovoľné hlásenie

CUSEC

- prevádzkovateľ základnej služby + **iná osoba**

- **môžu** hlásiť dobrovoľne nad rozsah povinnosti:
  - kybernetický bezpečnostný incident,
  - kybernetickú hrozbu alebo
  - udalosť odvrátenú v poslednej chvíli.



- NBÚ spracováva a analyzuje dobrovoľné hlásenia **v rozsahu, v akom to úradu umožňujú technické podmienky a kapacity** tak, aby nedošlo k neprimeranému zaťažovaniu subjektov a obmedzeniu medzinárodnej spolupráce.

- osobe, ktorá nie je prevádzkovateľom základnej služby, dobrovoľné hlásenia nezakladajú žiadne práva ani povinnosti podľa ZoKB

Iné spôsoby hlásenia

CUSEC

- Na hlásenie **závažných kybernetických bezpečnostných incidentov** alebo na zaistenie kybernetickej bezpečnosti môže úrad namiesto postupu podľa § 8 ods. 6 **uzatvoriť písomnú zmluvu o odlišnom spôsobe a forme hlásenia** kybernetických bezpečnostných incidentov s prevádzkovateľom základnej služby, pri ktorom je to odôvodnené jeho postavením, alebo rozsahom alebo obsahom činnosti.

Iné povinnosti

Iné povinnosti

CUSEC

- **riešiť** kybernetický bezpečnostný incident

- **spolupracovať** s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu
  - poskytnúť potrebnú súčinnosť,
  - ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

- v čase kybernetického bezpečnostného incidentu **zabezpečiť dôkaz alebo dôkazný prostriedok** tak, aby mohol byť použitý v trestnom konaní

- **oznámiť** orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol **spáchaný trestný čin**, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

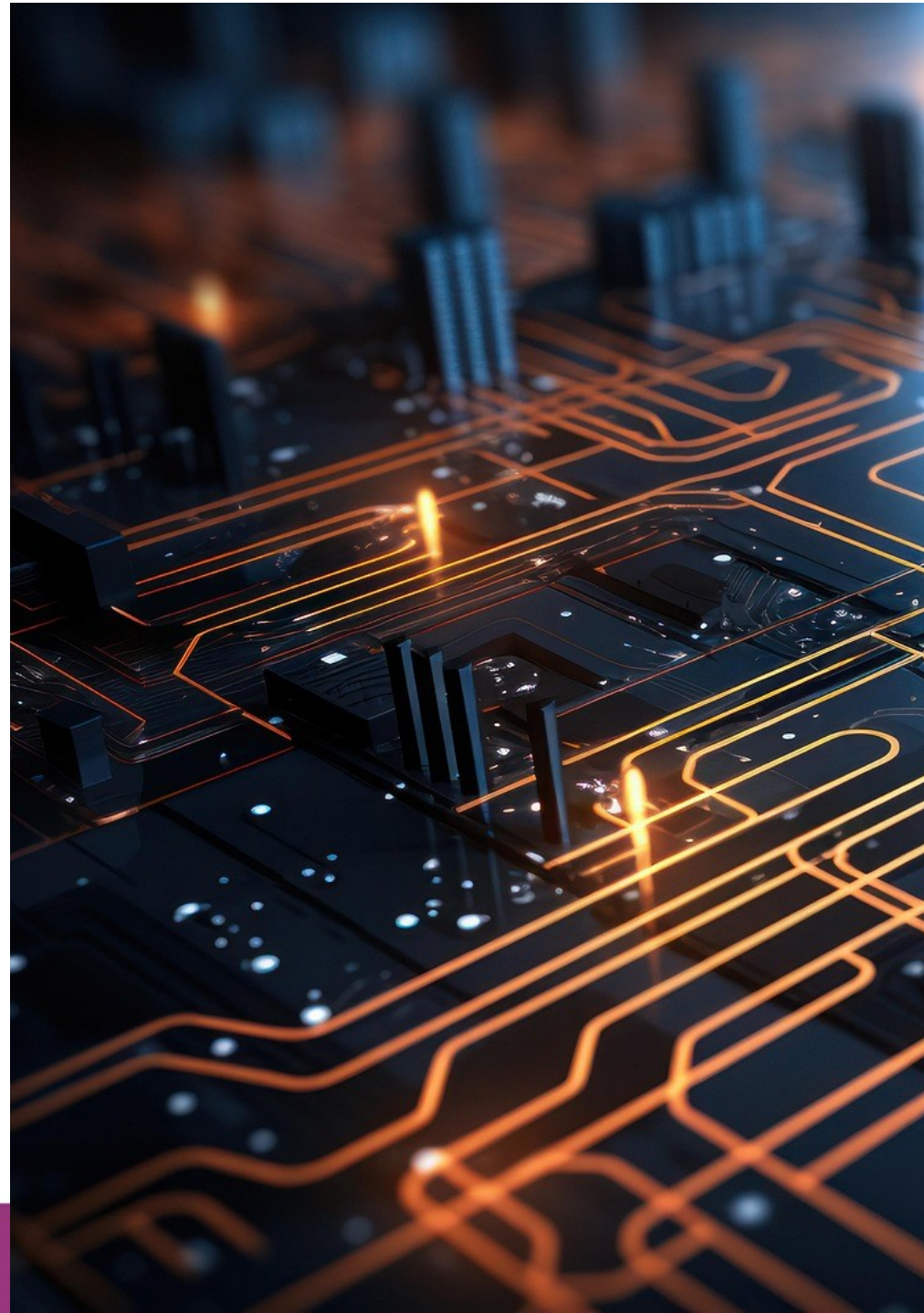
Iné povinnosti

CUSEC

- **analyzovať závislosti** svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu,

- **vytvoriť a zaviesť účinný mechanizmus včasného informovania štatutárneho orgánu a zodpovedných vedúcich zamestnancov** o:
  - kybernetických hrozbách,
  - zraniteľnostiach,
  - kybernetických bezpečnostných incidentoch,
  - udalostiach odvrátených v poslednej chvíli,
  - možných dopadoch kybernetických bezpečnostných incidentov,
  - výsledkoch analýzy rizík a stavu implementácie ošetrenia rizík

CSIRT



Národná jednotka CSIRT

Vládna jednotka CSIRT

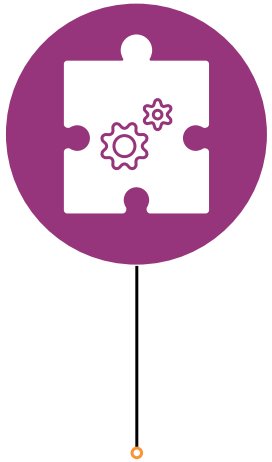
Akreditovaný CSIRT

- ÚO môže využívať Národné centrum kybernetickej bezpečnosti
- môže pre svoj sektor/podsektor zriaďovať a prevádzkovať akreditovanú jednotku CSIRT
- alebo využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, ak sa tak zmluvne dohodnú

Jednotný informačný systém kybernetickej bezpečnosti

Komunikačný systém

pre hlásenie a riešenie kybernetických bezpečnostných incidentov



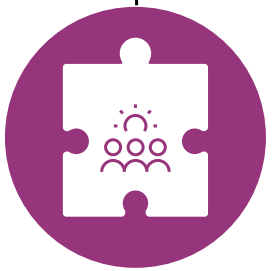
Centrálny systém

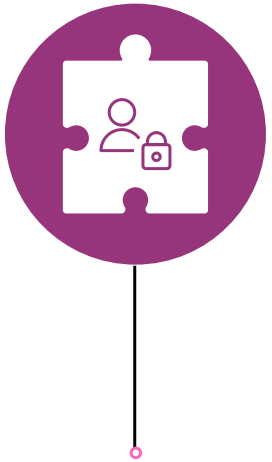
včasného varovania

.

Verejná časť

- registre (PZS, ÚO)
- zoznamy (A-CSIRT)
- výstrahy, varovania.





Neverejná časť

- NBÚ
- Jednotka CSIRT
- PZS
- NBS, ÚOOÚ, ÚREKPS
- Iný OVM

Audit

AUDIT

CUSEC

- overenie plnenia povinností podľa ZoKB
- posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa ZoKB a osobitných predpisov
- preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených ZoKB

- PKZS – vykonanie **auditu** do dvoch rokov odo dňa zaradenia do registra PZS
- PZS – vykonanaie auditu **samohodnotením** do dvoch rokov odo dňa zaradenia do registra PZS
  - JISKB
  - MKB
  - audit do 5 rokov odo dňa zaradenia

Vyhláška č. 493/2022 Z. z.

AUDIT

CUSEC

- Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti

- Prevádzkovateľ základnej služby je povinný predložiť **záverečnú správu o výsledkoch auditu** úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do **30 dní** od ukončenia auditu.

- NBÚ môže **kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby alebo požiadať certifikovaného audítora kybernetickej bezpečnosti**, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.

Dohľad

CUSEC

Vybavovanie sťažností

Kontrola

Opatrenia na nápravu

Schvaľovanie dohody o náprave

Správne delikty, ukladanie pokút

DOHĽAD

CUSEC

- Ak úrad zistí **nedostatky v činnosti prevádzkovateľa základnej služby spočívajúce v plnení povinností prevádzkovateľa základnej služby** podľa tohto zákona alebo povinností uložených na základe tohto zákona, podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov, môže **uložiť** prevádzkovateľovi základnej služby **povinnosť**
  - **vykonať audit** kybernetickej bezpečnosti a vykonať odporúčania podľa výsledkov tohto auditu v určenej lehote,
  - **prijať opatrenia** na nápravu,
  - **informovať** dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti, alebo
  - **zakázať poskytovať službu** do času nápravy nezákonného stavu, ak je takéto opatrenie nevyhnutne potrebné z dôvodu bezprostredného ohrozenia života alebo zdravia, iné opatrenia v rámci dohľadu neboli účinné a nebola vykonaná náprava v lehote určenej úradom;
    - to neplatí ak ide o prevádzkovateľa základnej služby, ktorý je **orgánom verejnej moci,** alebo ktorý poskytuje službu na základe povinnosti uloženej zákonom alebo na jeho základe.

DOHĽAD

CUSEC

- Ak prevádzkovateľ základnej služby, ktorý prevádzkuje **kritickú základnú službu**, nesplní **povinnosť** podľa odseku 1 písm. a) alebo písm. b), ani v **dodatočnej lehote** určenej vo výzve úradu, môže úrad podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov:
  - **zakázať štatutárnemu orgánu** prevádzkovateľa základnej služby alebo **členovi štatutárneho orgánu** prevádzkovateľa základnej služby, jeho **vedúcemu zamestnancovi na najvyššej úrovni riadenia** zodpovednému za príslušnú činnosť alebo výkonom tejto činnosti poverenému **splnomocnencovi vykonávať ich funkciu, zamestnanie alebo činnosť** u prevádzkovateľa základnej služby, a to až do doby splnenia týchto povinností.

- Ustanovenie prvej vety sa nepoužije, ak ide o prevádzkovateľa základnej služby, ktorý je **orgánom verejnej moci**, na ktorý sa vzťahuje tento zákon.

Vykonať A, vykonať odporúčania A

Prijať opatrenia na nápravu

SANKCIE

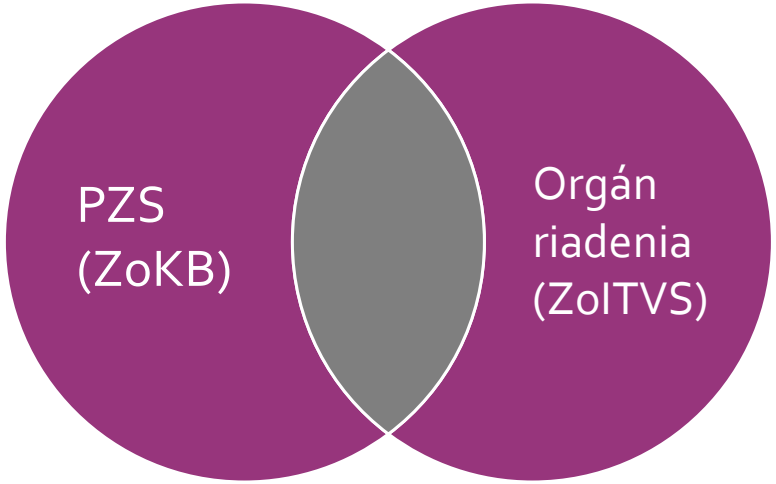
CUSEC

- **Priestupky**
- pokuta 100 - 5000 eur

- **Správne delikty**
- pokuta od 300 eur až do 500 000 EUR
- pokuta od 300 eur až do **7 000 000 EUR** alebo do výšky 1,4 % celkového celosvetového ročného obratu za predchádzajúce účtovné obdobie, podľa toho, ktorá suma je vyššia
- od 500 eur do **10 000 000** eur alebo do výšky 2 % celkového celosvetového ročného obratu za predchádzajúce účtovné obdobie, podľa toho, ktorá suma je vyššia...

KZS

ZoKB vs. ZoITVS


PZS
(ZoKB)
Orgán
riadenia
(ZoITVS)

- **§ 1 ods. 3**

Tento zákon **sa vzťahuje** aj na **správcov**, ktorí sú **prevádzkovateľmi základnej služby**[2a]) alebo poskytovateľmi digitálnej služby[2b]) podľa osobitného predpisu;[3]) ich povinnosti a oprávnenia podľa osobitného predpisu[3]) týmto zákonom nie sú dotknuté.

OP - ZoKB

Zákon č. 95/2019 Z. z.

- **§ 18 ods. 1 a 2**

1. Povinnosť správcu, ktorý je prevádzkovateľom základnej služby,[20]) prijať a realizovať bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov ustanovuje osobitný predpis.[21])

2. Správca, ktorý je prevádzkovateľom základnej služby,[20]) **prijíma a realizuje** bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe podľa tohto zákona a osobitného predpisu,[21]) **ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti ako ustanovuje osobitý predpis.**[22])

PL. ÚS 25/2019 (e-KASA)

CUSEC

- Ako dôsledok má finančná správa niekoľko zásadných bezpečnostných povinností vrátane povinnosti prijať bezpečnostné opatrenia v personálnej a technologickej oblasti, povinnosti detegovať, evidovať, oznamovať NBÚ a aktívne riešiť bezpečnostné incidenty (§ 19, § 20 ZoKB), ako aj povinnosti podrobovať sa dohľadu NBÚ a nezávislým auditom (§ 28, § 29 ZoKB). **Podobné povinnosti pritom prevádzkovateľovi e-kasy vyplývajú aj zo ZoITVS, pričom tie sa uplatnia, ak sú prísnejšie [§ 2 ods. 2 písm. e) ZoKB], ako napríklad § 23 ods. 3 ZoITVS pri notifikácii bezpečnostných incidentov.** NBÚ, ako aj iné štátne orgány v tomto smere disponujú aj širokou možnosťou vykonávať kontrolu na poli bezpečnosti.

CUSEC

PZS (ZoKB) a orgán riadenia (ZoITVS)

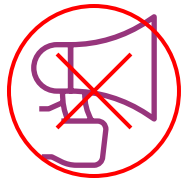
- Orgán riadenia je povinný:

- **ak je zaradený do registra prevádzkovateľov základných služieb** alebo poskytovateľov digitálnych služieb podľa osobitného predpisu,[3])

- nahlasovať spôsobom podľa osobitného predpisu[3]) **aj kybernetický bezpečnostný incident**,[24]) **na ktorý sa nevzťahuje povinnosť nahlasovania** podľa osobitného predpisu;[3])

PZS (ZoKB) – sektor VS + iný Orgán riadenia (ZoITVS)

- orgán riadenia ktorý je prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby **aj v inom sektore ako je sektor verejná správa <u>nie je povinný</u>** hlásiť:



  - **kybernetický bezpečnostný incident**, **na ktorý sa nevzťahuje povinnosť nahlasovania**
    - obyčajné KBI

Orgán riadenia (ZoITVS)

- Orgán riadenia, **ktorý nie je prevádzkovateľom základnej služby**[2a)] alebo poskytovateľom digitálnej služby[2b)] podľa osobitného predpisu[3)] je povinný:

  - nahlasovať **kybernetický bezpečnostný incident**[24)] **vládnej jednotke CSIRT**,
  - **bezodkladne riešiť kybernetický bezpečnostný incident** a prijať opatrenia na zníženie rizika[27)] vyplývajúceho zo zraniteľnosti bezodkladne po tom, ako sa o kybernetickom bezpečnostnom incidente alebo zraniteľnosti dozvedel,
  - **viesť evidenciu** kybernetických bezpečnostných incidentov, postupov na riešenie kybernetických bezpečnostných incidentov,
  - **určiť a zverejniť na svojom hlavnom webovom sídle kontaktné údaje na kontaktný bod** alebo primeraný počet kontaktných bodov na nahlasovanie kybernetického bezpečnostného incidentu.

CUSEC

Ďakujem za pozornosť!