INFORMAČNÁ A KYBERNETICKÁ BEZPEČNOSŤ

Prezentácia
2019/2020
22. apríla 2020

JUDr. Jozef Andraško, PhD.

CC-BY 2.0

PREHĽAD

- informačná bezpečnosť
- kybernetická bezpečnosť
- právna úprava
  - EÚ
  - národná úroveň

čo je bezpečnosť?

BEZPEČNOSŤ

je založená na ochrane **aktív**

pred rôznymi **hrozbami**

pri určitej **zraniteľnosti**

BEZPEČNOSŤ

je založená na ochrane **aktív**

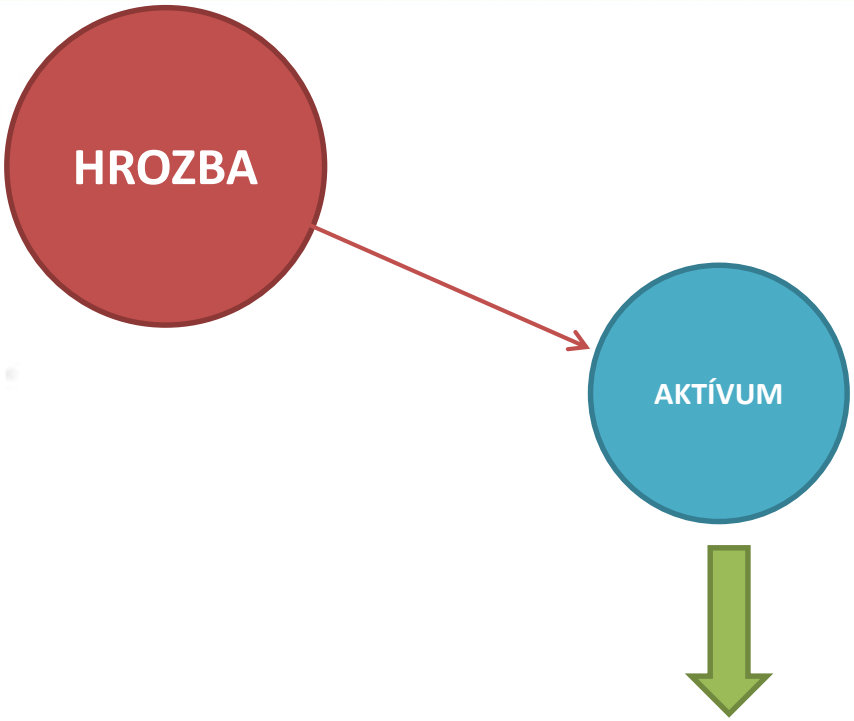
akých?

pred rôznymi **hrozbami**

vieme ju odstrániť?

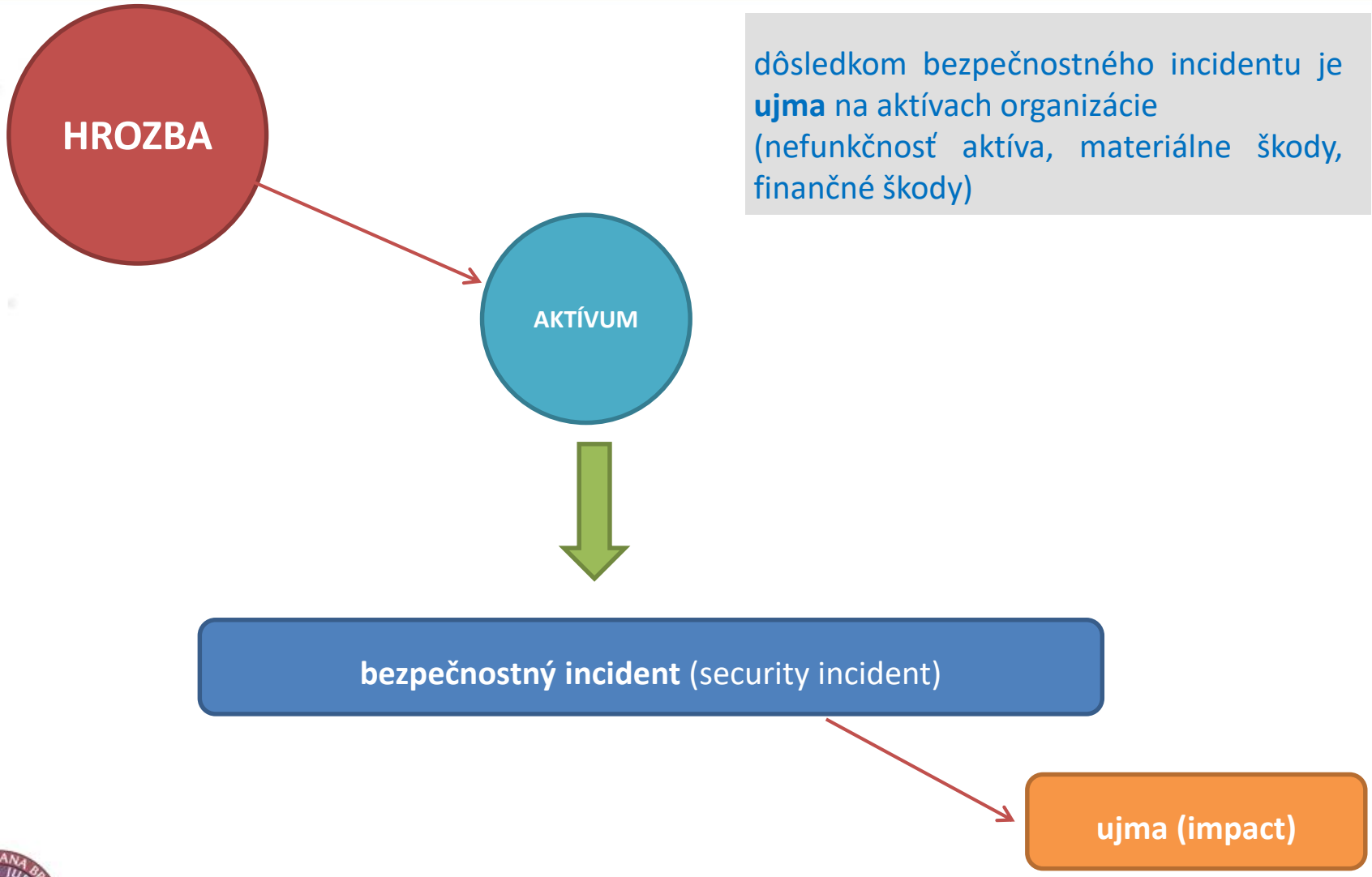
pri určitej **zraniteľnosti**

čo je zraniteľné?



v prípade ak bude **hrozba** voči aktívu **naplnená** (zraniteľnosť zneužitá hrozbou) a spôsobí **narušenie požadovaného stavu** aktíva

bezpečnostný incident (security incident)



dôsledkom bezpečnostného incidentu je **ujma** na aktívach organizácie (nefunkčnosť aktíva, materiálne škody, finančné škody)

- **je potrebné prijať opatrenia!**
  - znižujú dopady bezpečnostných incidentov na aktíva
  - môžu odstraňovať zraniteľnosť aktív
  - šifrovanie citlivej informácie, zálohovanie údajov

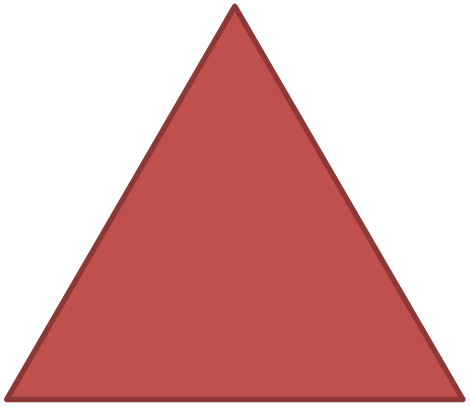
Informačná bezpečnosť - pojem

INFORMAČNÁ BEZPEČNOSŤ

- **ISO/IEC 27000:2018** Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

- *zachovanie **dôvernosti, integrity** a **dostupnosti** informácií.*

- **CIA** - *Confidentiality, Integrity, Availability*



dôvernosť

DÔVERNOSŤ

- bezpečnostná požiadavka na zaistenie **dôvernosti** informácie
- **informácia je chránená pred prezradením neoprávneným osobám**
- osobné údaje, informácie týkajúce sa bezpečnosti štátu
- **informácia ≠ údaj**

integrita

INTEGRITA

- bezpečnostná požiadavka na zaistenie **integrity údajov**
- údaje sú chránené pred **náhodnou alebo úmyselnou modifikáciou**, ktorá by mohla mať vplyv na platnosť údajov
- ochrana údajov v rámci transakcií, kde dochádza k platbe (modifikácia sumy)

dostupnosť

DOSTUPNOSŤ

- informácie a služby, ktoré poskytujú osobám a organizáciám, **musia byť dostupné používateľovi kedykoľvek, keď o to požiada**

- webová stránka

INÉ BP

- autentickosť,
- súkromnosť,
- anonymita,
- pseudonymita,
- nepopretie pôvodu,
- nepopretie doručenia,
- dosledovateľnosť

Kybernetická bezpečnosť - pojem

KYBERNETICKÁ BEZPEČNOSŤ

- **ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity**

- zachovanie dôvernosti, integrity a dostupnosti informácií v **kybernetickom priestore**

- **KB = IB kybernetického priestoru**

čo je kybernetický priestor?

KYBERNETICKÝ PRIESTOR

- **neexistuje jednoznačná, všeobecne akceptovaná definícia**

1.

- systém systémov (SoS) zložený z rôznych **digitálnych zariadení spojených počítačovými sieťami, pripojenými na Internet** pozostávajúceho z

a) technickej informačnej a komunikačnej infraštruktúry (počítače, komunikačné kanály, aktívne prvky komunikačných sietí),

b) programového vybavenia a údajov potrebných na prevádzku informačnej a komunikačnej infraštruktúry z bodu a),

c) aplikačného programového vybavenia zariadení uvedených v bode a),

d) údajov spracovávaných zariadeniami uvedenými v bode a), **ktoré neslúžia na prevádzku** technickej informačnej a komunikačnej infraštruktúry (**aplikačné údaje**),

e) vykonávaných činností a poskytovaných služieb prostredníctvom technických zariadení, programového vybavenia a údajov uvedených v bodoch a) - d),

f) vzťahov medzi entitami (ľuďmi, organizáciami a pod.) vznikajúcimi a pretrvávajúcimi na základe interakcií realizovaných podľa bodu e).

KYBERNETICKÝ PRIESTOR

2.

- virtuálny systém informácií, vzťahov, činností, ktoré vznikajú pri spracovaní informácií prostredníctvom digitálnych IKT, ktorý však **neexistuje v materiálnej forme**

- komplexné prostredie, ktoré vzniklo **interakciou ľudí, softvéru a služieb na Internete** prostredníctvom **zariadení a sietí, technológií k nemu pripojených**, ktoré **neexistuje v žiadnej fyzickej podobe** (ISO/IEC 27032:2012)

KYBERNETICKÝ PRIESTOR

- priestor, ktorý neexistuje v materiálnej podobe?
- **nemožno ho chápať izolovane od jeho technologických komponentov, z ktorých je tvorený**
- okrem technologickej úrovne má kybernetický priestor aj **sociálno-technickú úroveň**, v rámci ktorej sa vykonávajú rôzne kybernetické aktivity

PRÁVNA ÚPRAVA IB A KB

- EÚ
- PP SR

PRÁVNA ÚPRAVA IB A KB

- EÚ
- PP SR

Smernica NIS

SMERNICA NIS

Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 **o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov** v Únii

SIETE A INFORMAČNÉ SYSTÉMY

elektronická komunikačná sieť v zmysle článku 2 písm. a) smernice 2002/21/ES

každé **zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení**, z ktorých jedno alebo viaceré vykonávajú na základe **programu automatické spracúvanie digitálnych údajov**, alebo

digitálne údaje, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú **prostredníctvom prvkov** uvedených v písmenách a) a b) **na účely ich prevádzkovania, používania, ochrany a udržiavania**

SMERNICA NIS

- **bezpečnosť sietí a informačných systémov**

- *„schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje **dostupnosť, autentickosť, integritu** alebo **dôvernosť** uchovávaných, prenášaných alebo spracúvaných **údajov alebo súvisiacich služieb** poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.“*

neobsahuje pojem kybernetická bezpečnosť

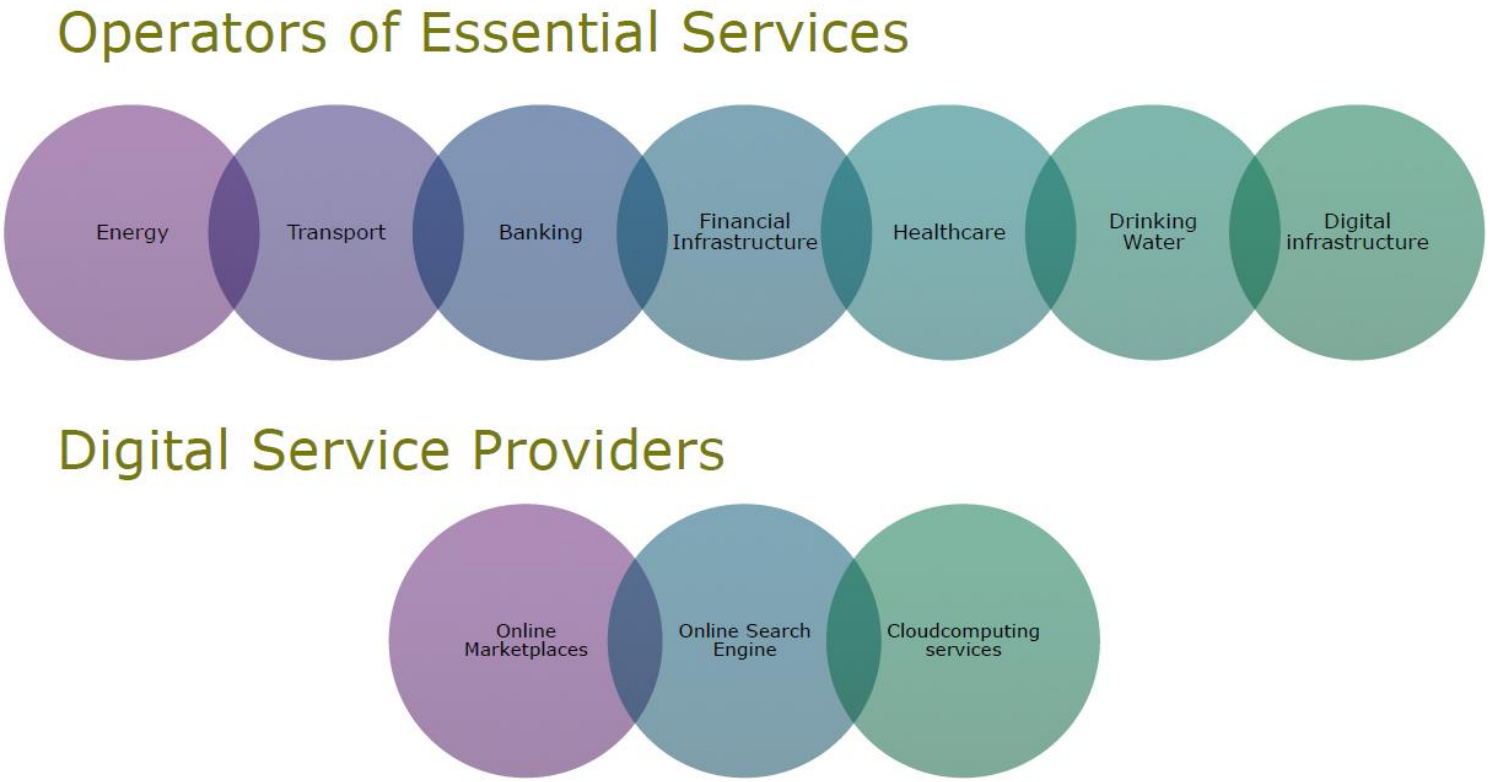
SMERNICA NIS

- stanovuje **opatrenia** na dosiahnutie **vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov** v rámci Európskej únie s cieľom zlepšiť fungovanie vnútorného trhu

SMERNICA NIS

- **kľúčové hospodárske subjekty:**
  - **prevádzkovatelia základných služieb** a
  - **poskytovatelia digitálnych služieb**

do 9. mája 2018



PZS

- členské štáty **zodpovedné za určenie subjektov**, ktoré spĺňajú kritériá vymedzenia pojmu PZS

minimálna harmonizácia

• verejný alebo súkromný subjekt, ktorého typ sa uvádza v prílohe II Smernice NIS (odvetvie-pododvetvie-typ subjektu)

• kritériá stanovené v článku **5 ods. 2** Smernice NIS

NIS kritériá na identifikáciu PZS

• subjekt poskytuje službu, ktorá má **zásadný význam** z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;

• poskytovanie tejto služby je **závislé od sietí a informačných systémov** a

• incident by **mal závažný rušivý vplyv** na poskytovanie uvedenej služby.

• čl. 6 smernice NIS – medziodvetvové faktory

PZS

- v dôsledku procesu identifikácie by členské štáty mali prijať **vnútroštátne opatrenia**, ktorými sa určia **subjekty**, ktoré podliehajú povinnostiam v oblasti bezpečnosti sietí a informačných systémov

Rec. 25
• prijať **zoznam** všetkých PZS alebo

• prijať také **vnútroštátne opatrenia**, ktoré umožnia určiť, ktoré subjekty podliehajú povinnostiam v oblasti bezpečnosti sietí a informačných systémov

Čl. 5 ods. 5
• Členské štáty pravidelne a aspoň každé dva roky od 9. mája 2018 **preskúmavajú** a v prípade potreby **aktualizujú** zoznam identifikovaných PZS

PZS

- ČŠ majú povinnosť **určiť** do **9. novembra 2018 PZS** pre každé odvetvie a pododvetvie uvedené v prílohe II Smernice NIS

- na tento účel každý členský štát zostaví **zoznam služieb** uvedených v odseku 2 písm. a).
  - službu, ktorá má **zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností**;

Rec. 22,23, čl. 5 ods. 2 (a)
zoznam základných služieb
• všetky služby poskytované na území daného členského štátu, ktoré spĺňajú požiadavky Smernice NIS
• referenčný bod umožňujúci identifikáciu PZS

Smernica NIS nestanovuje požiadavky na základné služby a dokonca tento pojem ani nedefinuje

PRÁVNA ÚPRAVA IB A KB

- EÚ
- PP SR

PP SR

- **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

- **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

Pôsobnosť zákona

Zákon o KB upravuje:

- **organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti**,
- **národnú stratégiu** kybernetickej bezpečnosti,
- **jednotný informačný systém** kybernetickej bezpečnosti,
- organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „**jednotka CSIRT“) a ich akreditáciu**,
- postavenie a povinnosti **prevádzkovateľa základnej služby a poskytovateľa digitálnej služby**,
- bezpečnostné opatrenia,
- systém zabezpečenia kybernetickej bezpečnosti,
- kontrolu nad dodržiavaním tohto zákona a audit.

Zákon o KB upravuje:

- **organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti**,
- **národnú stratégiu** kybernetickej bezpečnosti,
- **jednotný informačný systém** kybernetickej bezpečnosti,
- organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „**jednotka CSIRT“) a ich akreditáciu**,
- postavenie a povinnosti **prevádzkovateľa základnej služby a poskytovateľa digitálnej služby**,
- bezpečnostné opatrenia,
- systém zabezpečenia kybernetickej bezpečnosti,
- kontrolu nad dodržiavaním tohto zákona a audit.

Pôsobnosť orgánov verejnej moci

- **NBÚ**

pre jednotlivé sektory/podsektory

- ústredný orgán (NBÚ, MD, MF, MH, MO, MV, MZ, MŽP, SIS, ÚPVII, VS)
- iný orgán štátnej správy
  - ministerstvá a ostatné ústredné orgány štátnej správy, ktoré nie sú ústredným orgánom
  - GP, NKÚ, ÚPDZS, ÚOOÚ, ÚRSO..

NBÚ

- **má plniť úlohy, ktoré nevie splniť**
- na účely zabezpečenia plnenia úloh **môže uzatvoriť písomnú dohodu o spolupráci s fyzickou osobou**
- má **postavenie národnej jednotky CSIRT**
- je **správcom** a **prevádzkovateľom** **jednotného informačného systému kybernetickej bezpečnosti (JIS KB)**
- **akredituje** jednotky CSIRT

pôvodne v návrhu zákona aj s PO (utajenie)

NBÚ akreditovaný zo zákona

PZS a PDS

PZS v ZoKB

PZS - § 17

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

preveruje NBÚ podnet?

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

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

základnou službou **služba**, ktorá je zaradená v zozname základných služieb a

(A) závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,
(B) je informačným systémom verejnej správy, alebo
(C) je prvkom kritickej infraštruktúry,

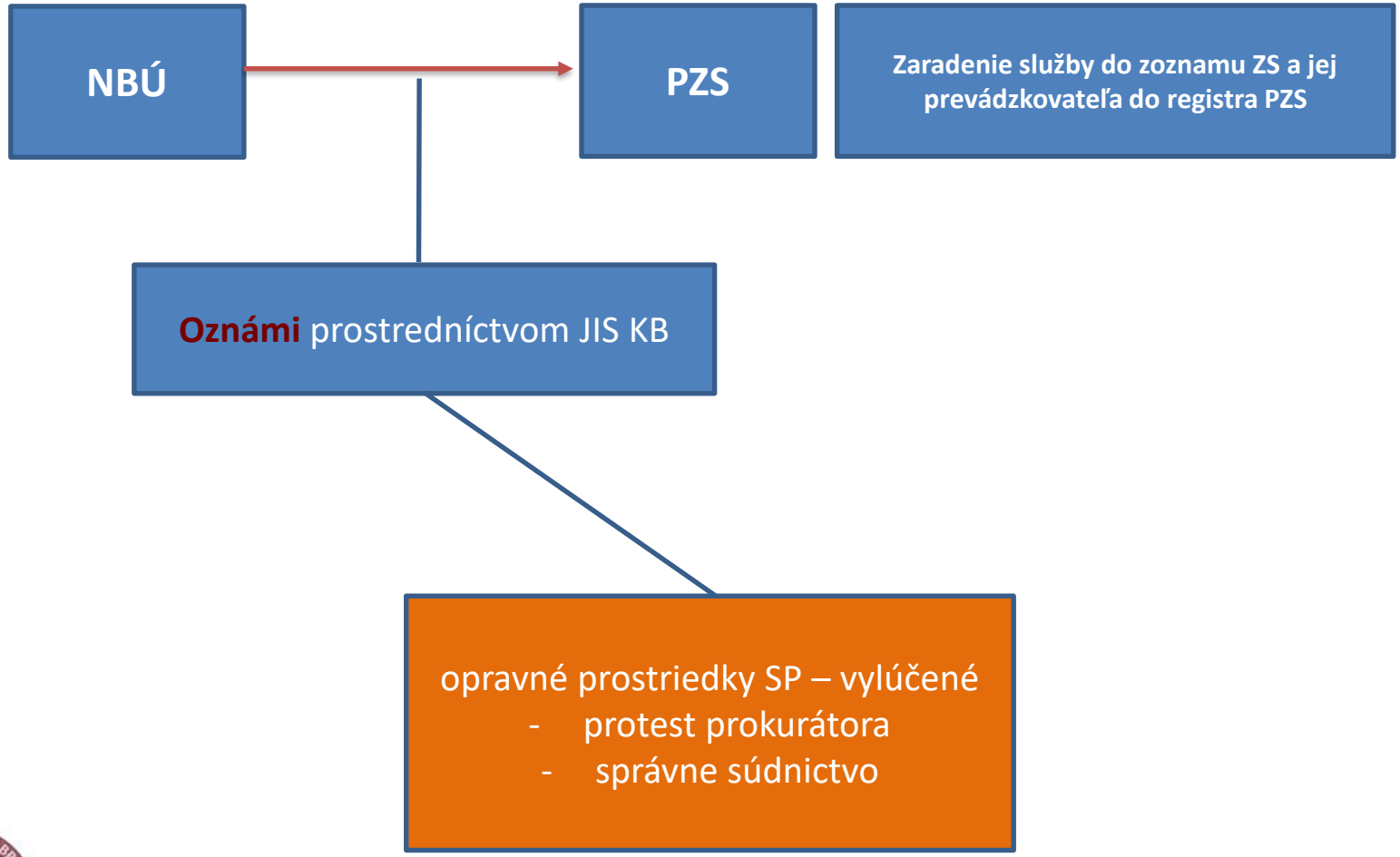
PZS

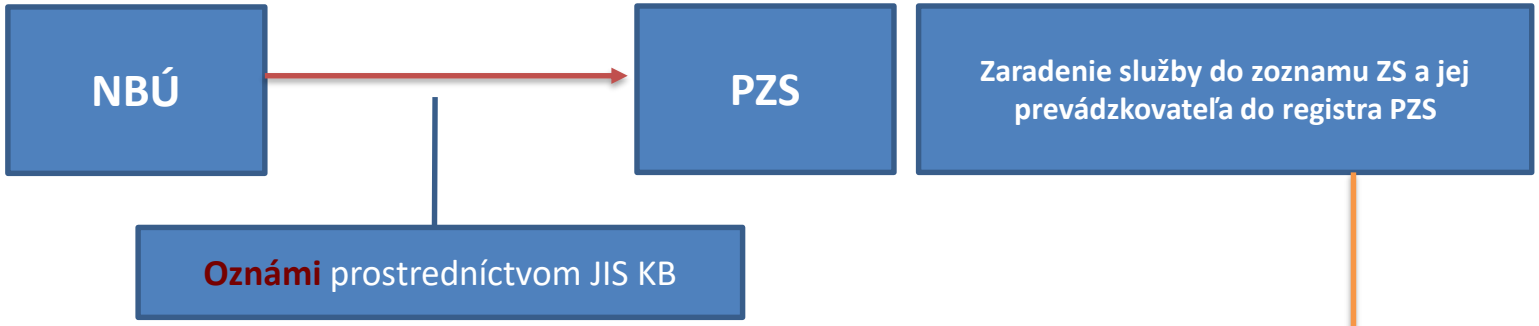
- **Zoznam základných služieb**
- **Register PZS**

UV o sektorových a prierezových kritérií na určenie prvkov kritickej infraštruktúry a zoznam prvkov kritickej infraštruktúry a ich zaradenie do sektorov kritickej infraštruktúry

Register prevádzkovateľov základných služieb

Prevádzkovateľ základnej služby	Základná služba	IČO	Sektor	Podsektor
Prevádzkovateľ základnej služby zaradený v zozname prvkov kritickej infraštruktúry schváleného uznesením vlády Slovenskej republiky č. 347/2018 alebo informačné systémy k nemu priamo pripojené	Služba, ktorá je prvkom kritickej infraštruktúry alebo je k nemu priamo pripojená			
BENESTRA, s.r.o.	IP - Transit- poskytovateľ služby výmenného uzla internetu na účel prepájania sietí, ktoré sú z technického a organizačného pohľadu oddelené, DNS - poskytovateľ služieb systému doménových mien na internete	46 303 502	Digitálna infraštruktúra	
Energotel, a.s.	Poskytovateľ služby výmenného uzla internetu na účel prepájania sietí, ktoré sú z technického a organizačného pohľadu oddelené; poskytovateľ služieb systému doménových mien na internete	35 785 217	Digitálna infraštruktúra	
Komerční banka, a.s., pobočka zahraničnej banky	Poskytovanie bankových produktov a služieb - platobný styk	47 231 564	Bankovníctvo	
Letové prevádzkové služby Slovenskej republiky, štátny podnik	ATC služba riadenia letovej prevádzky EUROCAT 2000	35 778 458	Doprava	Letecká doprava
MBS spol. s r.o.	Poskytovanie služieb systému doménových mien na internete	30 228 018	Digitálna infraštruktúra	
Národná diaľničná spoločnosť, a.s.	Služba elektronického výberu mýta; služba elektronická dialničná známka, centrálny riadiaci systém tunelov; informačný systém dialnic a rýchlostných ciest	35 919 001	Doprava	Cestná doprava
Orange Slovensko, a.s.	Služba výmenného uzla internetu na prepájanie sietí (IXP);	35 697 270	Digitálna infraštruktúra	


NBÚ
PZS
Zaradenie služby do zoznamu ZS a jej prevádzkovateľa do registra PZS
Oznámi prostredníctvom JIS KB
opravné prostriedky SP – vylúčené
- protest prokurátora
- správne súdnictvo



Ak činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov vykonáva pre PZS niekto iný (tretia strana)?

- musí uzatvoriť zmluvu s dodávateľom

Ak poskytuje službu v inom ČŠ?

- Musí byť identifikovaný aspoň v 1
- NBÚ – príslušný orgán

do 6 mesiacov odo dňa oznámenia
PZS povinnosť prijať a dodržiavať všeobecné bezpečnostné opatrenia (§ 20) a sektorové bezpečnostné opatrenia, ak sú prijaté
+ ďalšie povinnosti (hlásenie závažných KBI...)

PZS - § 18

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

Vyhláška č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).

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

Vyhláška 164/2018

ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)

- názov je zavádzajúci
- kritéria pre určenie PZS

Len na základnú službu
(A)
NIE ZS (B), (C)

§ 1

Táto vyhláška určuje identifikačné kritériá základnej služby podľa § 3 písm. k) prvého bodu

- prevádzkovaná služba spĺňa identifikačné kritériá základnej služby, **ak spĺňa aspoň jedno dopadové kritérium a aspoň jedno špecifické sektorové kritérium**, ak je uvedené v prílohe č. 1 (V, § 2)

- ak prevádzkovateľ služby podľa prílohy č. 1 zistí, že **došlo k prekročeniu špecifických sektorových kritérií**, oznámi to úradu do 30 dní odo dňa, keď prekročenie zistil v rozsahu podľa § 17 ods. 5 **aj v prípade, ak neprekročí dopadové kritériá** (ZoKB, § 18 ods. 4)

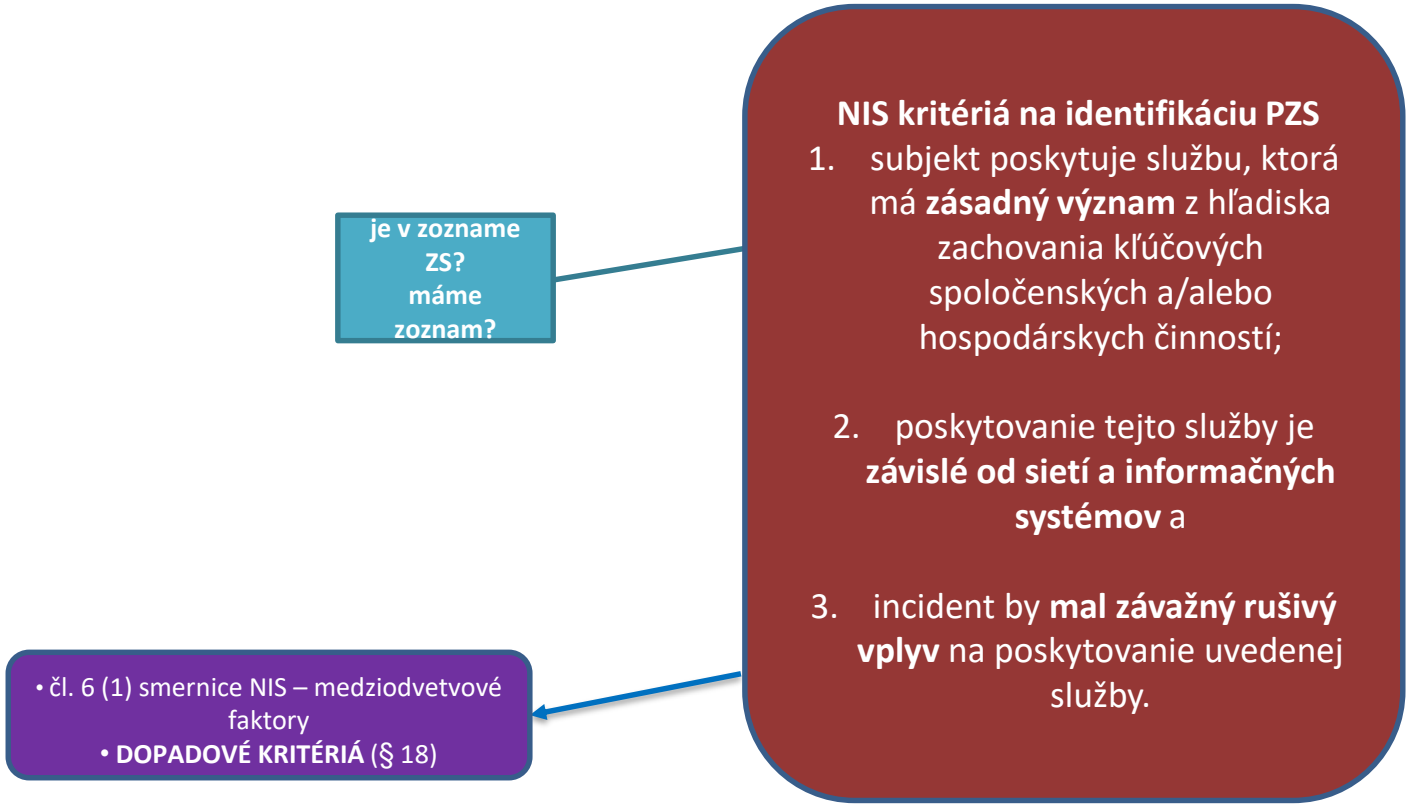
subjekt + opis činnosti

špeciálne kritériá druhu subjektu

Čl. 6 smernice NIS
faktory pre určenie závažnosti rušivého vplyvu na poskytovanie základnej služby

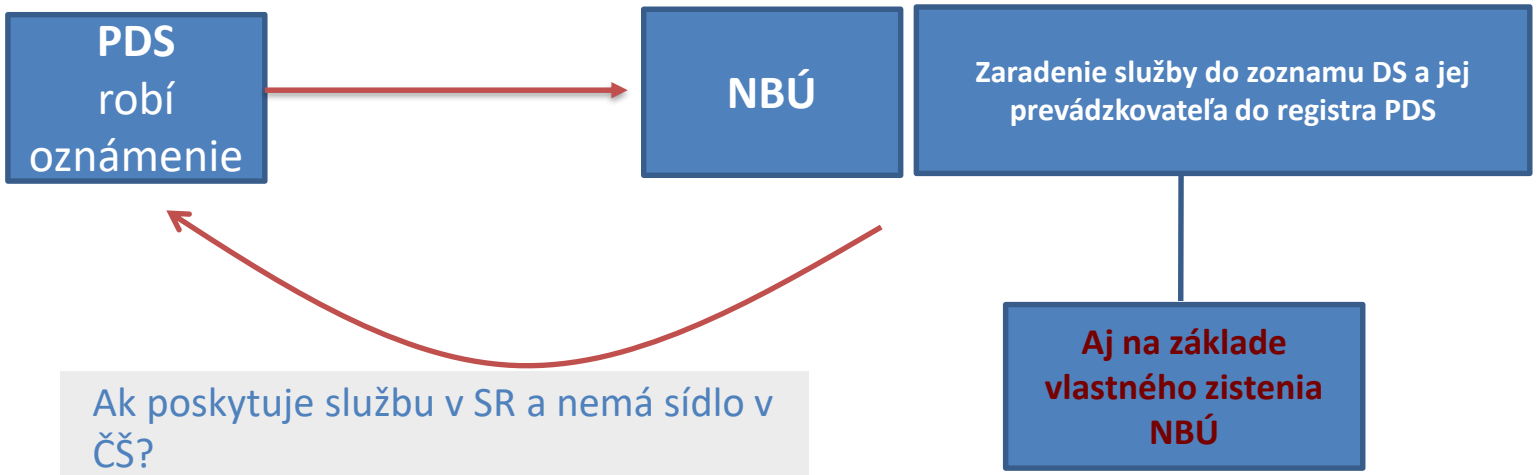
Ropa a ropné produkty

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:**
Prevádzkovateľ zariadenia na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu.	a) Zariadenia na ťažbu, spracovanie, rafináciu alebo úpravu ropy s inštalovanou ročnou výrobnou kapacitou minimálne 2 000 000 t ročne. b) Zásobník alebo komplex zásobníkov s kapacitou najmenej 20 000 m^3. c) Skladovacie zariadenie na LPG s kapacitou najmenej 20 000 m^3. d) Produkty s kapacitou prepravy produktov viac ako 2 000 000 t ročne. e) Prenosové zariadenie na ropu. f) Technický dispečing využívaný na prevádzkovanie rafinérie, skladu, prenosového zariadenia na ropu alebo k ťažbe, spracovaniu, alebo úprave ropy.	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 či narušenie prevádzky inej základnej služby alebo prvku kritickej infraštruktúry. 3. Hospodársku stratu vyššiu ako 0,1 % HDP. 4. Hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 eur. 5. Viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo stratu jedného života. 6. 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.


je v zozname ZS?
máme zoznam?
NIS kritériá na identifikáciu PZS
1. subjekt poskytuje službu, ktorá má **zásadný význam** z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;
2. poskytovanie tejto služby je **závislé od sietí a informačných systémov** a
3. incident by **mal závažný rušivý vplyv** na poskytovanie uvedenej služby.
• čl. 6 (1) smernice NIS – medziodvetvové faktory
• **DOPADOVÉ KRITÉRIÁ** (§ 18)

PDS

- **Online- trhovisko**
- **Internetový vyhľadávač** — maximálna harmonizácia
- **Cloud computing**



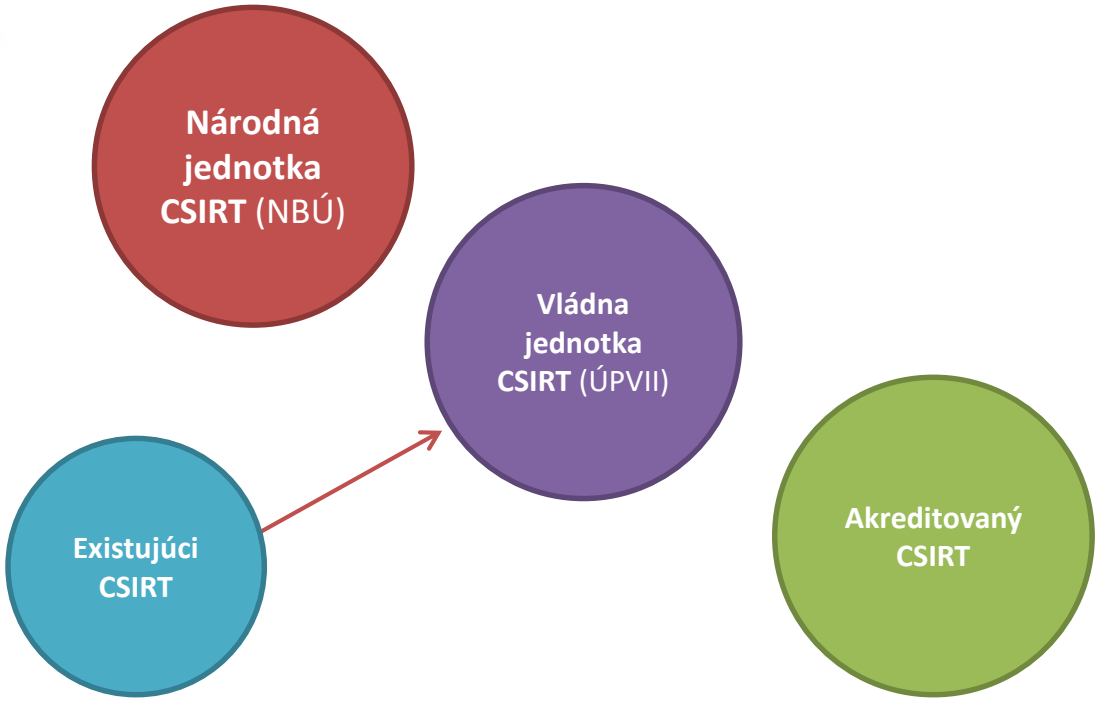
Ak poskytuje službu v SR a nemá sídlo v ČŠ?

- ustanoví zástupcu v SR ak nie je ustanovený v inom ČŠ

Ak má sídlo/zástupcu SR ale S/IS má v inom ČŠ?

- NBÚ – príslušný orgán

CSIRT



Zodpovedajú za riešenie kybernetických bezpečnostných incidentov a vykonávajú preventívne služby a reaktívne služby
(pred, počas, po incidente)

- každý ÚO pre svoj sektor/podsektor zriaďuje a prevádzkuje akreditovanú jednotku CSIRT
- alebo využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, ak sa tak dohodnú

Jednotný informačný systém kybernetickej bezpečnosti

- **ISVS**
- správca a **prevádzkovateľ** NBÚ
- PZS/PDS hlási KBI + dobrovoľné hlásenie

KOMUNIKAČNÝ SYSTÉM
pre hlásenie a riešenie kybernetických bezpečnostných incidentov

CENTRÁLNY SYSTÉM
včasného varovania

VEREJNÁ ČASŤ
- registre (PZS, PDS, KBI)
- zoznamy (ZS, DS, A-CSIRT)

NEVEREJNÁ ČASŤ
- NBÚ
- Jednotka CSIRT
- PZS, PDS
- NBS, ÚOOÚ
- Iný OVM

JIS KB – JEDINÝ KANÁL?

Na účely hlásenia kybernetických bezpečnostných incidentov a zaistenia funkcionality jednotného informačného systému kybernetickej bezpečnosti môže NBÚ uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s prevádzkovateľom základnej služby.

ĎAKUJEM

ZA POZORNOSŤ!