Novela zákona o kybernetickej bezpečnosti z perspektívy aproximácie práva EÚ

tzv. BALÍČEK pre oblasť kybernetickej bezpečnosti

Rada EÚ – *dňa 22. marca 2021* prijala *„Závery Rady o stratégii kybernetickej bezpečnosti EÚ pre digitálnu dekádu“*

1. **návrh nariadenia Európskeho parlamentu a Rady (EÚ) o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014 (tzv. nariadenie DORA) (- 2022/2554)**

2. **smernica Európskeho Parlamentu a Rady o odolnosti kritických subjektov (tzv. smernica CER) (- 2022/2557)**

3. **smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 (tzv. smernica NIS 2.0) (- 2022/2555)**

Návrh smernice EP a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii

Identifikované nedostatky (potreba zmeny)

ČO SMERNICA NIS 2 PRINÁŠA

- **odstránenie identifikovaných prekážok** vnútorného trhu pre kľúčové a dôležité subjekty
- **zlepší vytváranie a fungovanie jednotného trhu** prostredníctvom: ***stanovenia jasných, všeobecne uplatniteľných pravidiel o rozsahu pôsobnosti smernice NIS***
- **harmonizovanie pravidiel** uplatniteľných v oblasti riadenia kybernetického rizika a oznamovania incidentov

Návrh smernice EP a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 (tzv. smernica NIS 2.0)

NBÚ

NIS2

Hlavné výzvy spojené s transpozíciou smernice NIS 2.0

VÝZVY

- ★ národná stratégia KB
- ★ nové odvetvia a pododvetvia uvedené v prílohách
- ★ koordinované zverejňovanie informácií o zraniteľnostiach a európska databáza zraniteľností
- ★ národný rámce pre riadenie kybernetických kríz
- ★ dohľad ex post
- ★ bezpečnostné požiadavky a oznamovanie incidentov
- ★ zmena identifikácie PZS
- ★ register kľúčových a dôležitých subjektov
- ★ CSIRT-y a ich technické spôsobilosti

Novela zákona o KB č. 69/2018 Z. z.

NIS2

Hlavné zmeny zákona spojené s transpozíciou smernice NIS 2.0

PRINCIPIÁLNA ZMENA

1. **rozsah pôsobnosti** ***(size cap = stredné podniky = odporúčanie 2003/361/EU) – (§ 1 a 2 ZoKB)***

2. **nové subjekty** bez ohľadu na veľkosť (aprox. 5-6 tisíc) **– (§ 17 a príslušné prílohy)**

3. ustanovujú sa **povinnosti** členských štátov v oblasti **dohľadu** a **presadzovania** odvetvové právne akty – **(§ 29a až 29n)** - dohoda o náprave

4. **národné stratégie** budú obsahovať nové **prvky/politiky – (§ 7)**

5. **národný rámec pre riadenie kybernetických kríz**/ Sieť národných CSIRT-ov/ - **(§ 7 – národný plán reakcie)**

6. **hlásenia** / koordinované zverejňovanie zraniteľnosti / EU databáza zraniteľnosti – (§ 24)

Ďalšie zmeny, ktoré zákon prináša

- Upravujú sa základné pojmy. (§ 3 - kybernetická hrozba a udalosť odvrátená v poslednej chvíli)
- Podporuje sa certifikácia oblasti kybernetickej bezpečnosti. (§5)
- Podporuje sa koordinované riešenie zraniteľností prostredníctvom Národnej jednotky CSIRT (§6 ods. 5, 6 a 7)
- V kontexte posilnenia kontroly a dohľadu, dopĺňa sa osobná zodpovednosť štatutárov. (§ 29j ods. 4)
- Novela vyhlášky o audite (cena, samohodnotenie)
  Novela vyhlášky o bezpečnostných opatreniach
- Posilní sa funkcia manažéra kybernetickej bezpečnosti
- Výnimky zostávajú, nerozširujú sa. (postup pre výmaz regulovaného subjekt z registra)
- Modifikácia zavedeného sankčného mechanizmu. (§29n a §31)
- zodpovednosť za plnenia bezpečnostných opatrení pre subjekty v rámci dodávateľského reťazca

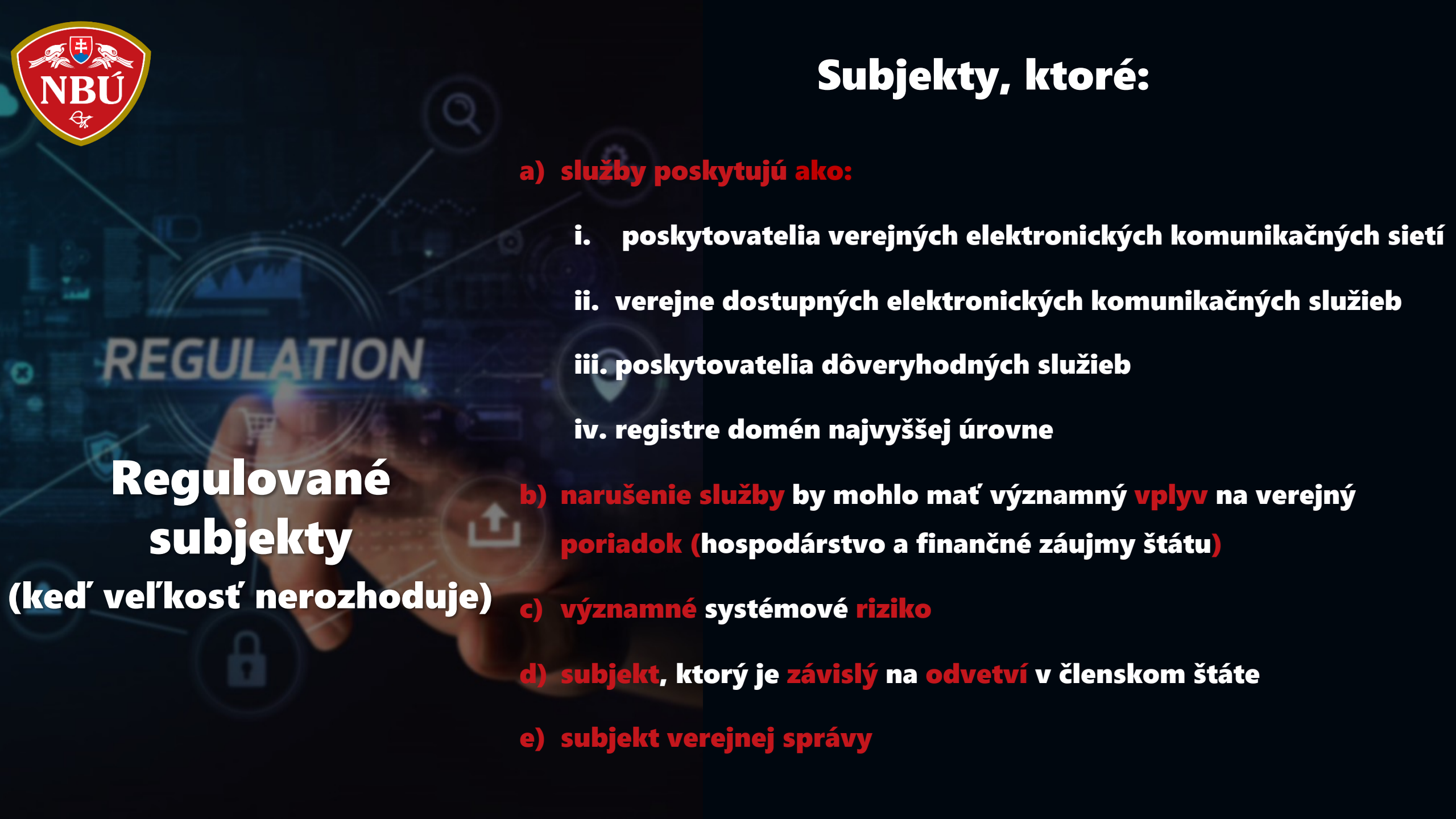
Regulované subjekty (základné kritérium)

STREDNÉ podniky stanovené v článku 2 ods. 1 prílohy k odporúčaniu 2003/361/ES

1. verejné alebo súkromné subjekty (podniky) uvedeného druhu
2. zamestnávajú 50 a viac zamestnancov
3. ročný obrat predstavuje aspoň 10 mil. Eur a/alebo ročná súvaha (bilančná suma) je viac ako 10 mil. Eur

HRANIČNÉ HODNOTY (článok 2)

Kategória podniku	Počet pracovníkov	Ročný obrat	alebo	Ročná bilančná suma
STREDNÉ podniky	< 250	≤ 50 mil. €	alebo	≤ 43 mil. €
MALÉ podniky	< 50	≤ 10 mil. €	alebo	≤ 10 mil. €
MIKRO podniky	<10	≤ 2 mil. €	alebo	≤ 2 mil. €



Regulované subjekty
(keď veľkosť nerozhoduje)

Subjekty, ktoré:

a) **služby poskytujú ako:**
   i. poskytovatelia verejných elektronických komunikačných sietí
   ii. verejne dostupných elektronických komunikačných služieb
   iii. poskytovatelia dôveryhodných služieb
   iv. registre domén najvyššej úrovne

b) **narušenie služby** by mohlo mať významný **vplyv** na verejný **poriadok (**hospodárstvo a finančné záujmy štátu**)**

c) **významné** systémové **riziko**

d) **subjekt**, ktorý je **závislý** na **odvetví** v členskom štáte

e) **subjekt verejnej správy**

Regulované subjekty - primerané opatrenia

KRITICKÉ (KĽÚČOVÉ) a DÔLEŽITÉ subjekty

1. sú povinné prijať vhodné a primerané technické, operačné a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov

2. zohľadňujú sa všetky riziká s cieľom chrániť siete a informačné systémy a fyzické prostredie uvedených systémov pred incidentmi

3. prihliada sa na najnovšie, resp. na relevantné európske a medzinárodné normy, ako aj na náklady na vykonávanie opatrení

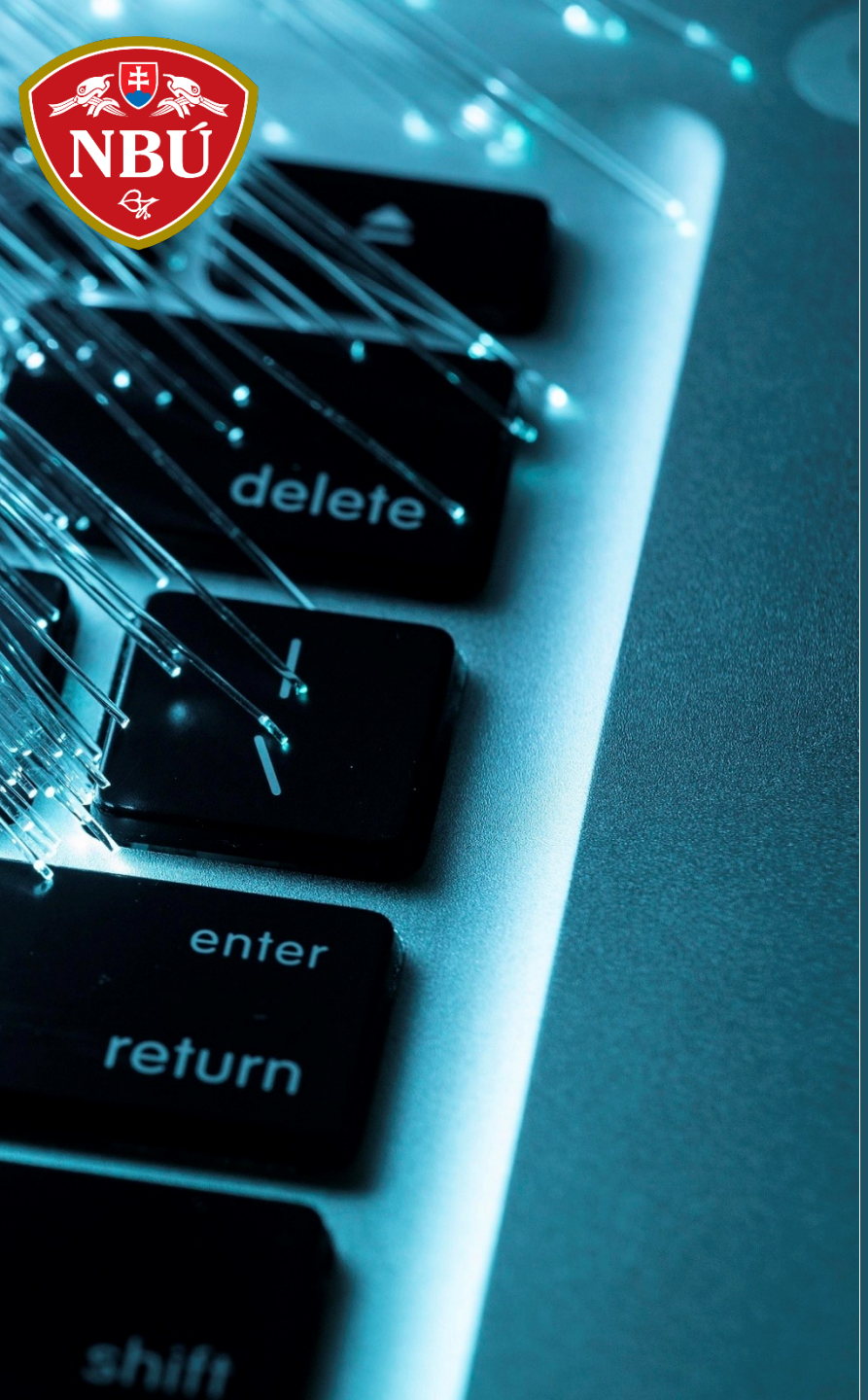
4. nemali by sa zbytočne vytvárať prekážky v podnikateľskej činnosti a mal by minimalizovať vplyv na podnikateľskú činnosť dotknutého subjektu

§ 20 Bezpečnostné opatrenia ods. 1 *(ciele)*

1. identifikovať zraniteľnosti, kybernetické hrozby a riziká,
2. preventívne chrániť informačné aktíva pred kybernetickými hrozbami a zabrániť vzniku incidentov,
3. detegovať nežiaduce udalosti a incidenty,
4. reagovať na identifikované zraniteľnosti a incidenty a minimalizovať ich vplyv na informačné aktíva a
5. obnoviť informačné aktíva, napraviť negatívne dopady po vzniku incidentu a uviesť poskytované služby do požadovaného stavu.

§ 20 Bezpečnostné opatrenia ods. 2 *(oblasti)*

1. organizáciu a riadenie informačnej a kyber bezpečnosti,
2. správa zraniteľností,
3. správu aktív a riadenie kybernetických hrozieb a rizík KB,
4. riadenie udalostí a kyberbezpečnostných incidentov,
5. riadenie kontinuity činností, obnova systému po havárii a krízové riadenie,
6. bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov, aplikácii a konfigurácii,
7. postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,
8. kryptografické opatrenia a zásady používania kryptografie,
9. bezpečnosť a spôsobilosti ľudských zdrojov,
10. správa identít a prístupov,
11. bezpečnosť pri prevádzke informačných systémov a sietí,
12. systémovú, sieťovú a komunikačnú bezpečnosť, monitorovani zaznamenávanie a hlásenie udalostí,
13. ochrana záznamov, ochrana súkromia a označovanie info



§ 20 Bezpečnostné opatrenia ods. 4
(*mnimálne opatrenia*)

1. určenie manažéra kybernetickej
2. detekcia a evidencia kybernetických bezpečnostných incidentov
3. postupy riešenia a riešenie kybernetických bezpečnostných incidentov
4. určenie kontaktnej osoby pre prijímanie a evidenciu hlásení
5. pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania
6. určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok PZS a zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené role,
7. určenie konkrétnej osoby, ktorá je zodpovedná za schvaľovanie bezpečnostných opatrení
8. využívanie a obstarávanie certifikovaných produktov IKT, výrobkov, služieb IKT a procesov IKT
9. bezpečnosť dodávateľského reťazca a dodržiavanie základnej kybernetickej hygieny

SEKTORY PO NOVOM

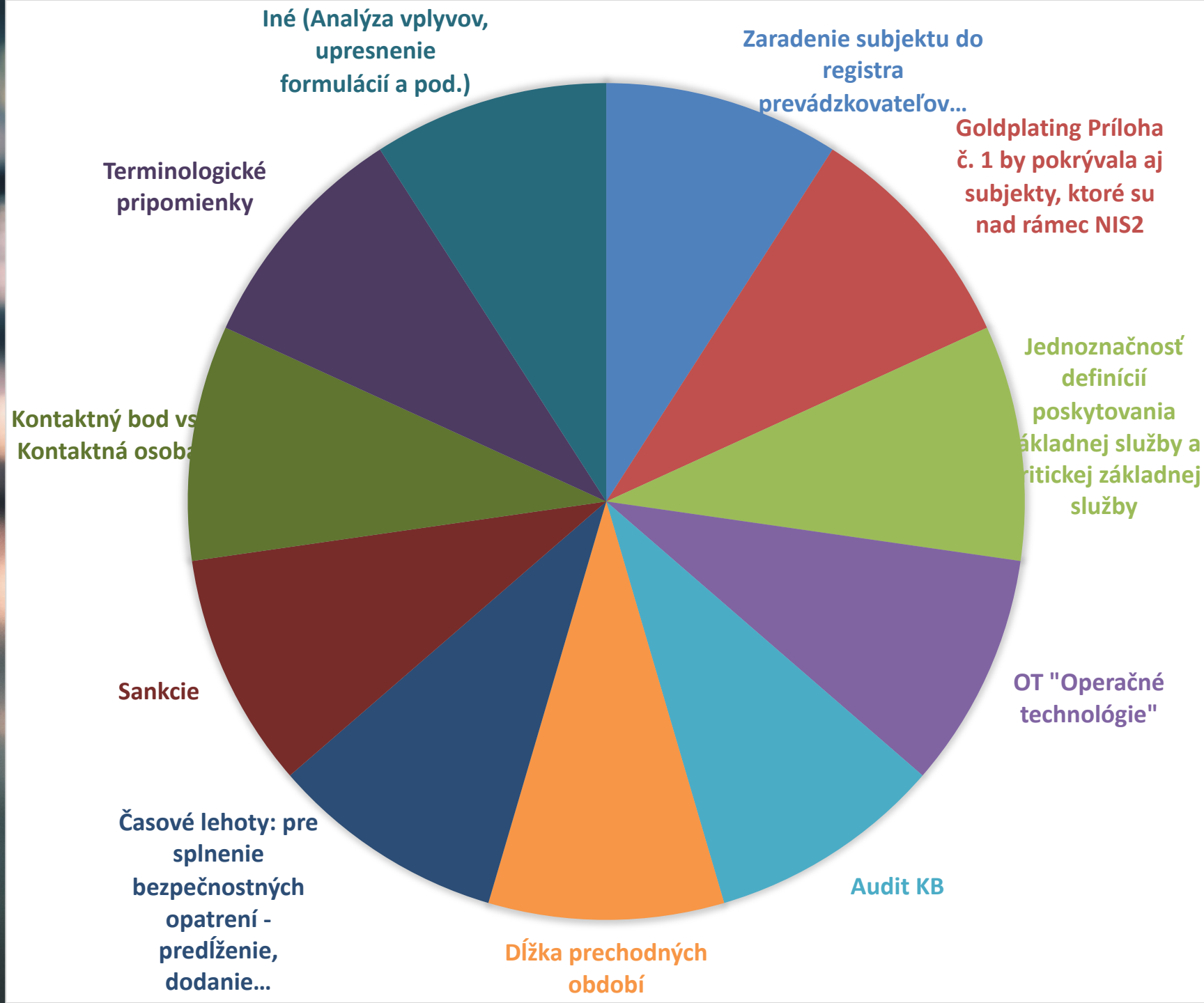
zákon č. 69/2018 Z. z.	Smernica NIS 1.0	Smernica NIS 2.0	
		kľúčové subjekty	– dôležité subjekty
bankovníctvo	energetika	energetika	poštové a kuriérske služby
doprava	doprava	doprava	**odpadové hospodárstvo**
digitálna infraštruktúra	bankovníctvo	bankovníctvo	výroba a distribúcia chemických látok
elektronické komunikácie	infraštruktúry finančných trhov	infraštruktúry finančných trhov	**výroba a distribúcia spracovanie potravín**
energetika	zdravotníctvo	zdravotníctvo	výroba: **- zdravotníctvo**
infraštruktúry finančných trhov	digitálna infraštruktúra	priemysel	**- elektron. zariadenia** **- stroje a zariadenia**
pošta	dodávka a distribúcia pitnej vody	pitná voda a distribúcia pitnej vody	**- počítačové, elektr. a optické výrobky**
priemysel		**odpadová voda**	**- motorové vozidlá**
voda a atmosféra		**riadenie služieb IKT**	**- dopravné prostriedky**
dodávka a distribúcia pitnej vody		verejná správa	poskytovatelia digitálnych služieb
verejná správa		**vesmír**	**výskum**
zdravotníctvo			

Aktuálny stav legislatívneho procesu – a čo nás čaká ?

Počas roka 2023 a rok 2024

- prebehla právna analýza textu smernice NIS 2
- identifikovali a komunikovali sa hlavné prijímané zmeny
- NBÚ úspešný v projekte EÚ – NIS 2 SK implementácia (1.10.2023)
- január až marec 2024 interné konzultácie/konzultácie s komunitou
- **aktuálne text novely zákona predložený do MPK od 30.5.2024 a MPK bolo ukončené 19.6.2024**
- predloženie na rokovania Vlády SR jún 2024 následne NR SR
- predpokladaná účinnosť najneskôr k 01. 01. 2025

Výsledky medzirezortného pripomienkového konania



Cieľ, ktorý chceme dosiahnúť

- správna odozva/reakcia na aktuálne výzvy práva EÚ a medzinárodné záväzky
- kompaktná, ucelená, zrozumiteľná národná legislatíva (postavená na princípe „user´s friendly“), ktorá je harmonizovaná s právom EÚ
- pri tvorbe EÚ legislatívy snaha o uniformný postup členských štátov
- nastavenie účinnej a aktívnej spolupráce medzi odvetviami s dopytom po kybernetickej bezpečnosti a dodávateľskými odvetviami, medzi výskumnými a priemyselnými komunitami a medzi nimi, medzi výskumnými a inovačnými komunitami v oblasti kybernetickej
- budovanie odvetvových kapacít

...AKO ĎALEJ ?

ĎAKUJEM ZA POZORNOSŤ

René Baran

tel.: +421 2 6869 2350 | GSM: +421 903 993 163
rene.baran@nbu.gov.sk | www.nbu.gov.sk

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD