

Připravovaná novela zákona o kybernetické bezpečnosti

Dopad 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)**

- 1. reakcia na nárast kyberneticko-bezpečnostných hrozieb**
- 2. hodnotenia fungovania smernice NIS, ktoré bolo vykonané na účely posúdenia vplyvu, sa identifikovali tieto problémy:**
 - a. nízka úroveň kybernetickej odolnosti podnikov pôsobiacich v EÚ**
 - b. nejednotná úroveň odolnosti v jednotlivých členských štátoch a odvetviach**
 - c. nízka úroveň spoločnej situačnej informovanosti a nedostatočná spoločná reakcia na krízu**



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

ČO SMERNICA NIS 2 PRINÁŠA

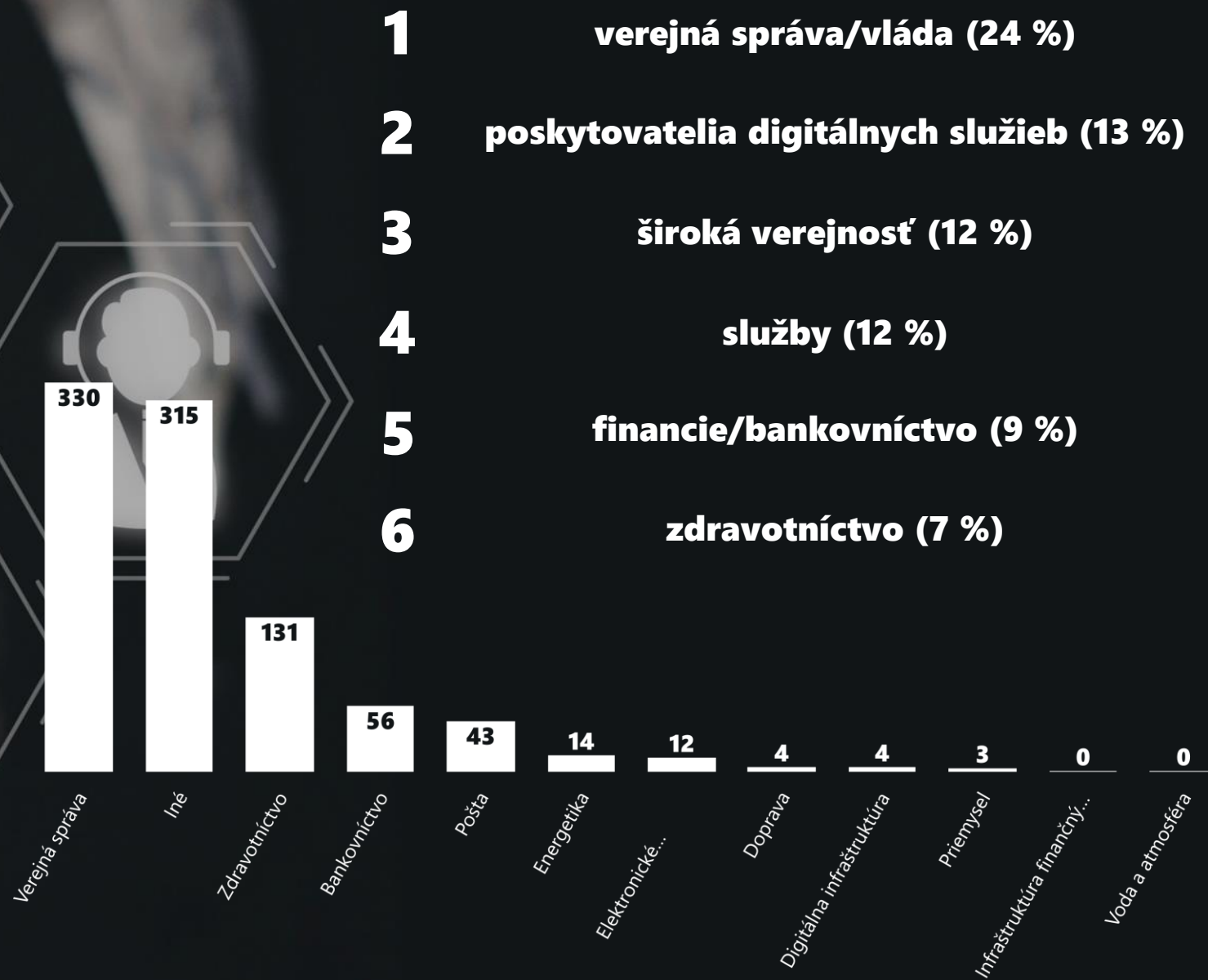
**Identifikované nedostatky
(potreba zmeny)**

- ❑ **odstránenie identifikovaných prekážok** vnútorného trhu pre kľúčové a dôležité subjekty
- ❑ **zlepši 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



Hrozby kybernetickej bezpečnosti v Európskej únii (nahlásené incidenty)

**INCIDENT
MANAGEMENT**





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 príprava a finalizácia textu do MPK



predloženie na rokovania Vlády SR jún 2024 následne
NR SR



predpokladaná účinnosť najneskôr k 01. 01. 2025



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

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

★ bezpečnostné požiadavky
a oznamovanie incidentov

★ zmena identifikácie PZS

★ register kľúčových a
dôležitých subjektov

★ CSIRT-y a ich
technické spôsobilosti

★ dohľad ex post

Novela
zákona o KB
č. 69/2018
Z. z.



PRINCIPIÁLNA ZMENA

NIS2

**Hlavné zmeny
zákona spojené s
transpozíciou
smernice NIS 2.0**

- 1 rozsah pôsobnosti** (*size cap = stredné podniky = odporúčanie 2003/361/EU*)
- 2 nové subjekty** bez ohľadu na veľkosť (aprox. 5-6 tisíc)
- 3 ustanovujú sa povinnosti** členských štátov v oblasti **dohľadu a presadzovania** odvetvové právne akty
- 4 národné stratégie** budú obsahovať nové **prvky/politiky**
- 5 národný rámec pre riadenie kybernetických kríz/** Sieť národných CSIRT-ov/
- 6 hlásenia** / koordinované zverejňovanie zraniteľnosti / EU databáza zraniteľnosti



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

Regulované subjekty (základné kritérium)

HRANIČNÉ HODNOTY (článok 2)

Kategória podniku	Počet pracovníkov	Ročný obrat	alebo	Ročná bilančná suma
STREDNÉ podniky	< 250	≤ 50 mil. €	alebo	≤ 43 mil. €
MALÉ podniky	< 5	≤ 10 mil. €	alebo	≤ 10 mil. €
MIKRO podniky	<10	≤ 2 mil. €	alebo	≤ 2 mil. €



Subjekty, ktoré:

**Regulované
subjekty
(keď veľkosť
nerozhoduje)**

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

c) významné systémové riziko

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

e) subjekt verejnej správy



KRITICKÉ (KLÚČOVÉ) a DÔLEŽITÉ subjekty

Regulované subjekty - primerané opatrenia

- 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

- 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.**

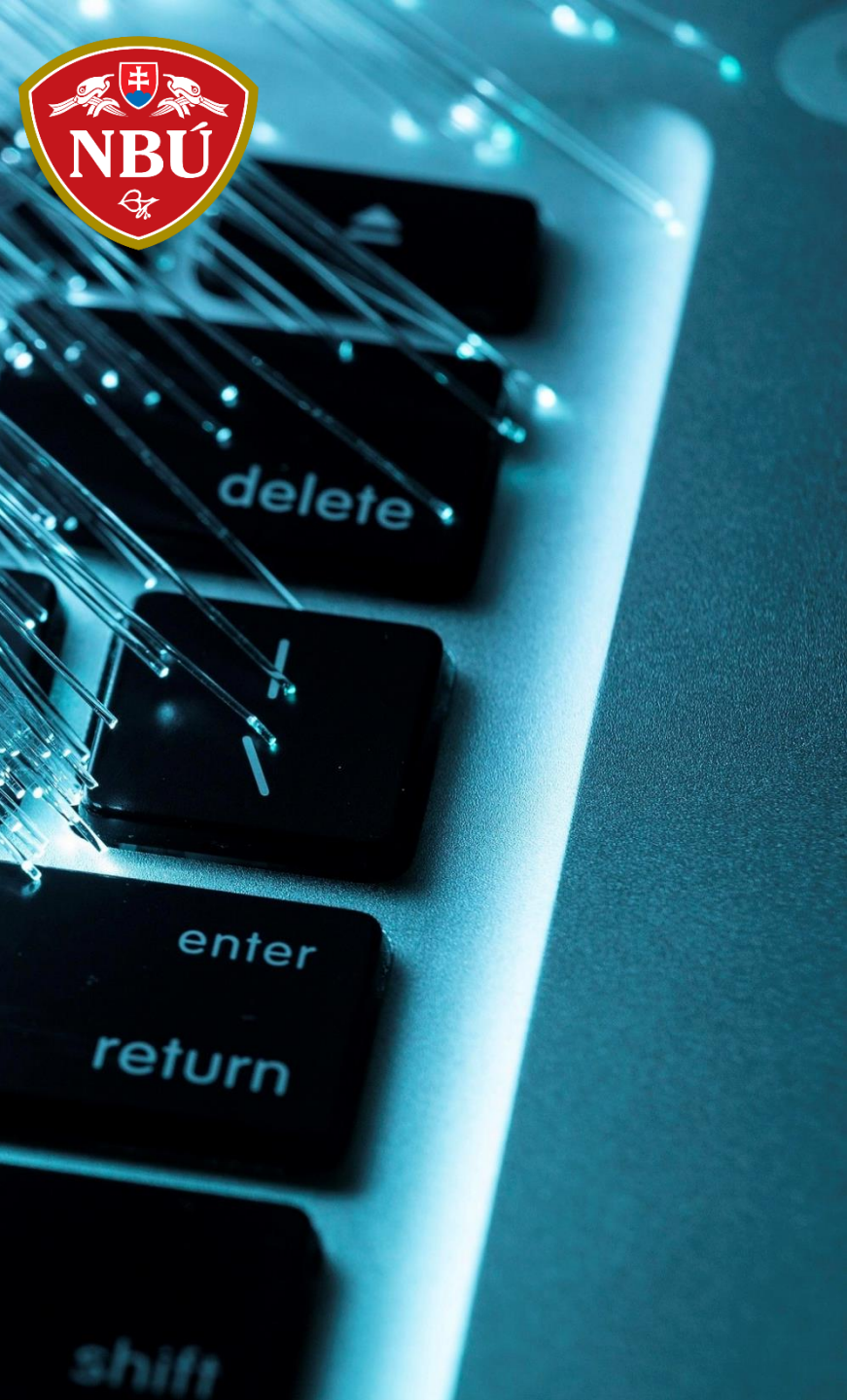
**Bezpečnostné
opatrenia
po novom**



Bezpečnostné opatrenia po novom

§ 20 Bezpečnostné opatrenia ods. 2

- 1. analýzu rizík a bezpečnosti informačných systémov,**
- 2. riešenie kybernetických bezpečnostných incidentov,**
- 3. reakciu na kybernetické bezpečnostné incidenty,**
- 4. zotavenie sa z kybernetických bezpečnostných incidentov**
- 5. kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii a krízové riadenie,**
- 6. bezpečnosť dodávateľského reťazca,**
- 7. bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov (zraniteľnosti),**
- 8. zásady a postupy posudzovania účinnosti prijatých bezpečnostných opatrení na riadenie kybernetických rizík,**
- 9. základnú kybernetickú hygieny a odbornú prípravu,**
- 10. zásady a postupy používania kryptografie alebo šifrovania,**
- 11. bezpečnosti ľudských zdrojov,**
- 12. zabezpečenie riadenia bezpečnosti v súvislosti so zamestnanca s náležitým zohľadnením opatrení,**



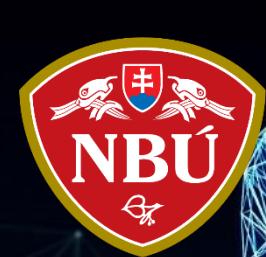
§ 20 Bezpečnostné opatrenia ods. 4

- 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 centrálnemu systému včasného varovania**
- 6. určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok PZS a zabezpečenie primeraného vzdelávania a preškolovania pre všetky zavedené role,**
- 7. prijatie politiky konkrétnej menovitej zodpovednosti osoby**
- 8. využívanie a obstarávanie certifikovaných produktov, výrobkov, služieb a procesov podľa osobitného predpisu a**
- 10. dodržiavanie základnej kybernetickej hygieny podľa osobitného predpisu**



SEKTORY PO NOVOM

zákon č. 69/2018 Z. z.	Smernica NIS 1.0	Smernica NIS 2.0 klúčové 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			



Ďalšie zmeny, ktoré zákon prináša

- Podporuje sa **koordinované riešenie zraniteľností prostredníctvom Národnej jednotky CSIRT.**
- Podporuje sa **certifikácia v oblasti kybernetickej bezpečnosti.**
- Upravujú sa **základné pojmy. Národná stratégia a krízový plán.**
- Posilňuje sa **kontrola a dohľad, dopĺňa sa osobná zodpovednosť štatutárov (podľa vzoru zákona o bankách).**
- Novela vyhlášky o audite (cena, samohodnotenie)**
- Posilní sa funkcia manažéra kybernetickej bezpečnosti**
- Výnimky zostávajú, nerozširujú sa**



Cieľ, ktorý chceme dosiahnuť

- ❑ **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

