NOVELA ZÁKONA č. 69/2018 Z. z. o KYBERNETICKEJ BEZPEČNOSTI

Road show NIS2
Košice, Banská Bystrica, Nitra, Bratislava
október 2024

Transpozícia NIS2 – povinná jazda ale nie len...

Transpozícia smernice (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (**smernica NIS 2**)

Úprava zákona na základe skúseností z praxe

- Spresnenie niektorých definícií
- Flexibilnejšia aplikácia opatrení
- Zjednodušenie hlásení incidentov
- Podrobnejšia úprava oprávnení úradu v rámci dohľadu

Návrh zákona, ktorým sa mení zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti bol predložený NRSR dňa 4.10.2024 – ČPT: 508

Základná zmena koncepcie NIS2

Predmetom regulácie nie je kybernetická bezpečnosť vo vzťahu k základným službám ale **kybernetická bezpečnosť a odolnosť kľúčových subjektov** a celých sektorov voči aktuálnym kybernetickým hrozbám.

Kľúčové zmeny

- **Rozšírenie** pôsobnosti zákona **na nové subjekty**
- **Identifikácia regulovaného subjektu** na základe jeho zaradenia do sektora
- **Aplikácia bezpečnostných opatrení** na základe rizikovej analýzy
- **Úprava bezpečnosti dodávateľského reťazca**
- **Úprava hlásenia incidentov**
- Koordinované zverejňovanie zraniteľností
- Audit a samohodnotenie
- **Certifikácia** bezpečnosti IKT produktov a služieb

Rozšírenie pôsobnosti zákona a identifikácia subjektov (PZS)

Prevádzkovateľom základnej služby (PZS) je (bez ohľadu na sektor):

- **ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou,**
- **kritický subjekt,**
- **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,
- **mesto,** ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
- **správca ITVS** po predchádzajúcej konzultácii s príslušným ústredným orgánom,
- **osoba, ktorá poskytuje službu registrácie názvu domény** bez ohľadu na splnenie podmienok veľkosti pre stredný podnik alebo
- **tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti,** má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu

Rozšírenie pôsobnosti zákona a identifikácia subjektov (PZS)

PZS sú ďalej subjekty zaradené do sektorov podľa prílohy 1 a 2:

- ak sú **minimálne stredným podnikom** (min. 50 zamestnancov a obrat alebo súvaha 10mil. Eur a viac)

- **bez ohľadu na veľkosť:**
  - je podnikom poskytujúcim verejnú EK sieť alebo verejnú EK službu,
  - je poskytovateľom dôveryhodnej služby,
  - je správcom TLD,
  - poskytuje službu DNS,
  - je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou,
  - poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
  - poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko pre celý sektor vykonávanej činnosti, najmä ak by takéto riziko mohlo mať cezhraničný vplyv,
  - je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo
  - je subjektom hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu,

SEKTORY S VYSOKOU ÚROVŇOU KRITICKOSTI (príloha 1)	INÉ KRITICKÉ SEKTORY (príloha 2)
Energetika (vykurovanie, chladenie, vodík)	Poštové a kuriérske služby
Doprava	Odpadové hospodárstvo
Financie	Výroba a distribúcia chemických látok
Zdravotníctvo	Výroba a distribúcia spracovanie potravín
Voda a atmosféra (odpadová voda)	Výroba (zdrav. pomôcky, elektro, výpočtová technika, optika, stroje a zariadenia, motorové vozidla, iné dopr. prostriedky)
Digitálna infraštruktúra	Poskytovatelia digitálnych služieb
Riadenie služieb IKT	Výskum
Verejná správa	
Vesmír	

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Rozšírenie pôsobnosti zákona a identifikácia subjektov (PKZS)

Kritickou základnou službou je:

- výkon pôsobnosti **ústredného orgánu štátnej správy alebo iného štátneho orgánu s celoštátnou pôsobnosťou,**
- **činnosť v sektore podľa prílohy č. 1,** okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá **presahuje podmienky veľkosti pre stredný podnik** (min. 250 zamestnancov a obrat 50 mil. EUR alebo súvaha 43mil. EUR a viac),
- **kvalifikovaná dôveryhodná služba,**
- **správa TLD,**
- **služba DNS,**
- **poskytovanie verejnej EK siete alebo verejnej EK 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,**
- informačná činnosť a elektronické služby, vykonávané s použitím **ITVS** určených úradom**.**

Extrateritoriálna pôsobnosť zákona

Extrateritoriálna pôsobnosť zákona:

- v plnom rozsahu - sa týka sa subjektov, ktoré poskytujú službu DNS, službu registrácie názvu domény, službu cloud computingu, službu dátového centra, sieť na sprístupňovanie obsahu, riadenú službu, bezpečnostnú službu, službu online trhu, službu internetového vyhľadávača alebo platformu služieb sociálnej siete, ale nemajú sídlo alebo miesto podnikania na území SR a spĺňajú ďalšie špecifické podmienky (§2 ods. 2 a §21),

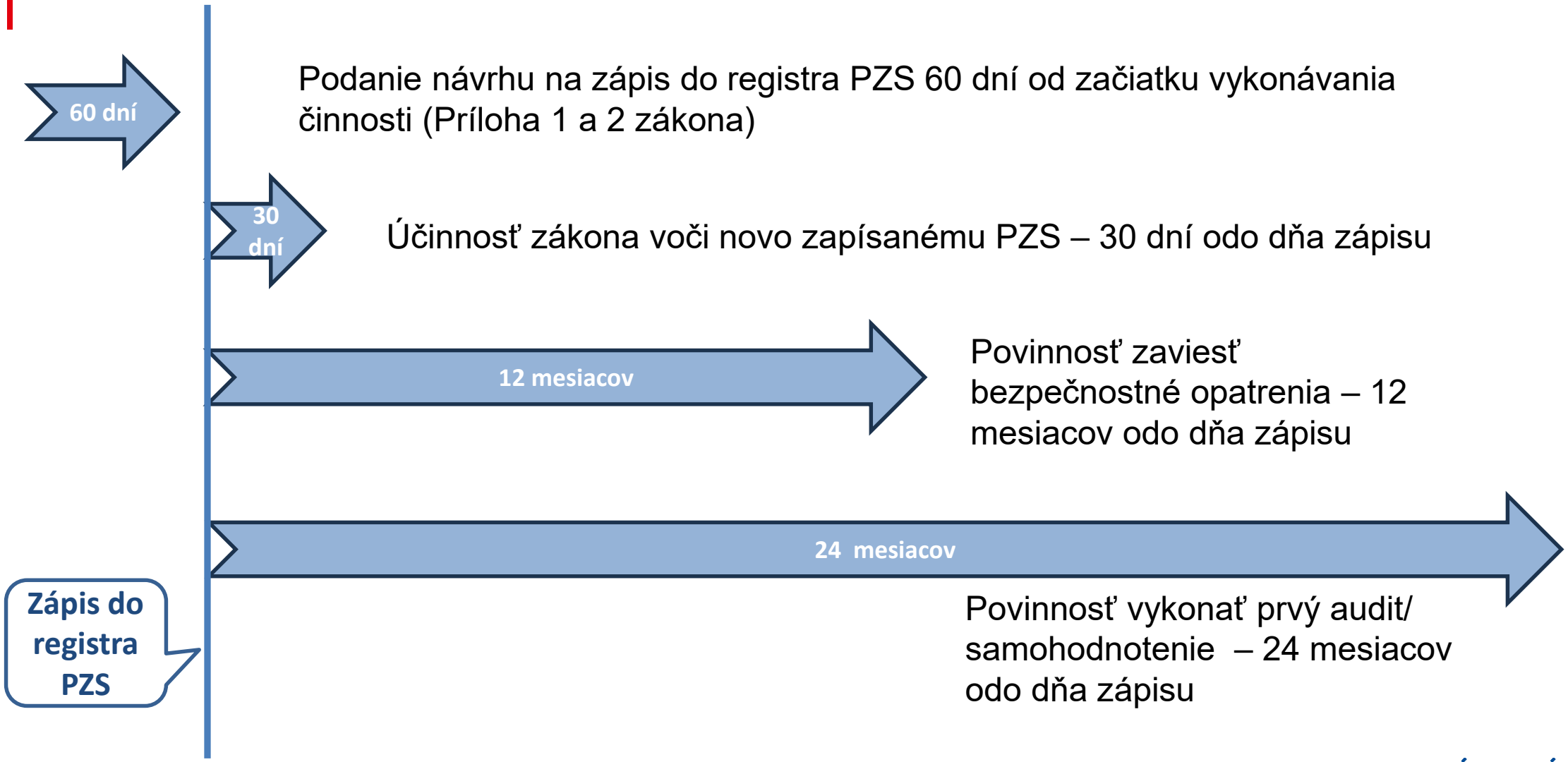
- v obmedzenom rozsahu – sa týka tretích strán (dodávateľov), ktoré nemajú sídlo alebo miesto podnikania na území EÚ a poskytujú služby alebo vykonáva činnosti na území Slovenskej republiky:
    - musia mať ustanoveného zástupcu na území SR alebo iného členského štátu EÚ, v ktorom tiež poskytujú služby alebo vykonávajú činnosti
    - môžu sa dostať do postavenia PZS ak by išlo o tretiu stranu s významným vplyvom na KB, ktorá je dodávateľom PKZS

Pôsobnosť zákona vs. sektorové úpravy

Sektor/podsektor	Bezpečnostné opatrenia/ bezp. štandard		Hlásenie (riešenie) incidentov		Pravidelný audit s povinnosťou predkladať záznam autorite	
	Zákon o KB	Sektor. úpr.	Zákon o KB	Sektor. úpr.	Zákon o KB	Sektor. úpr.
Finančné subjekty v pôsobnosti nariadenia DORA (napr. Banky)	✗	✓	✓ ←	✓	✓*	✗*
Jadrová energetika a jadrové zariadenia	✓ ✗ ✗ ✓	✗ ✓ ✓ ✗	✓	✗*	✓	✗*
Správcovia ITVS			✓ →	✓	✓	✗
Informačné systémy a siete podľa zákona o ochrane US	✗	✓	✓	✗	✓	✗

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Základné lehoty pre prevádzkovateľa základnej služby



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Aplikácia bezpečnostných opatrení

- Nová štruktúra všeobecných bezpečnostných opatrení (§20 ods. 1 a 2)
- Podrobnejší popis bezpečnostných opatrení bude obsahovať vyhláška
- **Rozsah a spôsob implementácie bezpečnostných opatrení na základe rizikovej analýzy**
- Ak existuje **sektorový bezpečnostný štandard,** opatrenia sa aplikujú na jeho základe pri zachovaní základných spôsobilostí riadiť informačnú bezpečnosť, hlásiť a riešiť incidenty a pod. (§20 ods. 6)
- **Povinnosť zaviesť bezpečnostné opatrenia do 12 mesiacov odo dňa zápisu do registra PZS**

Úprava bezpečnosti dodávateľského reťazca

Tretia strana - dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre PZS.

- **PZS je povinný uzatvoriť s treťou stranou zmluvu** o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
- Tretia strana je povinná zaviesť a vykonávať bezpečnostné opatrenia podľa zmluvy a zákona
- Tretia strana je povinná podrobiť sa kontrole plnenia požiadaviek zmluvy a zákona zo strany PZS
- Tretia strana, ktorá nemá sídlo alebo miesto podnikania na území EÚ je povinná ustanoviť zástupcu na území EÚ (v krajine kde vykonáva svoju činnosť)

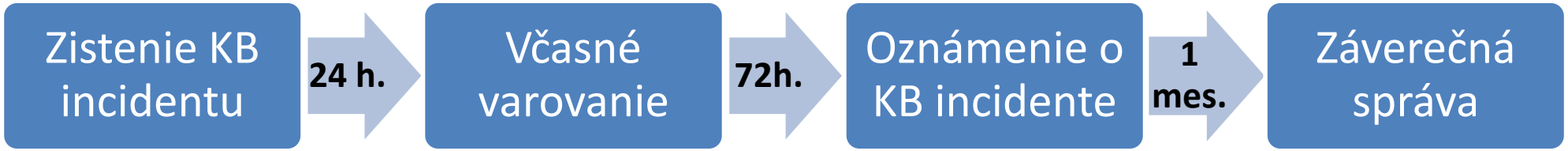
Tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, má uzatvorenú zmluvu s PZS, ktorý prevádzkuje kritickú základnú službu **má postavenie PZS**

- PKZS je povinný úradu hlásiť uzatvorenie zmluvy s takouto treťou stranou a aj jej ukončenie
- tretia strana sa **zapisuje do registra PZS**
- tretia strana povinná plniť bezpečnostné opatrenia podľa zákona a **podlieha dohľadu zo strany NBÚ**
- tretej strane je možné uložiť **povinnosť riešiť KB incident** alebo vykonať reaktívne opatrenie v čase krízy

Úprava hlásenia kybernetických bezpečnostných (KB) incidentov

PZS je povinný:

- **hlásiť závažný KB incident NBÚ** prostredníctvom jednotného informačného systému kybernetickej bezpečnosti



- **hlásiť ďalšie dôležité udalosti:**
  - významnú kybernetickú hrozbu, o ktorej sa dozvie,
  - udalosť odvrátenú v poslednej chvíli, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident,
  - zraniteľnosť, ktorá môže byť zneužitá na spôsobenie závažného KB incidentu a PZS ju nevie efektívne odstrániť alebo minimalizovať riziko jej zneužitia

Ostatné udalosti môže PZS hlásiť dobrovoľne. Rovnako tak aj akákoľvek iná osoba.

Zraniteľnosti a ich koordinované zverejňovanie

Aktívne vyhľadávanie zraniteľností

- oprávnenie národnej jednotky CSIRT vykonávať automatizovanú detekciu zraniteľností v rámci kybernetického priestoru SR
- aj sektorové jednotky CSIRT v rámci svojej konštituencie
- pomoc PZS pri ich mitigácii

Koordinované zverejňovanie zraniteľností

- mediácia a koordinácia pri zistení zraniteľnosti, jej analýze a zverejňovaní
- účelom je ochrana výskumníka/ nahlasovateľa a PZS resp. výrobcu alebo poskytovateľa IKT produktu alebo služby
- cieľom je analýza zraniteľnosti, jej katalogizácia (CVE) a koordinované zverejnenie s minimalizáciou negatívnych dopadov na zúčastnené strany

Audit a samohodnotenie

Povinnosť vykonať audit:

- PZS prvý audit do 2 rokov od zapísania do registra PZS a následne v periodicite podľa vyhlášky
- Audit vykonáva certifikovaný audítor kybernetickej bezpečnosti podľa príslušnej schémy
- **PZS, ktorý neposkytuje kritickú službu,** môže audit vykonať aj tzv. **samohodnotením**.
- Samohodnotenie vykonáva manažér kybernetickej bezpečnosti
- PZS, ktorý si zvolil vykonanie audit samohodnotením musí vykonať prvý **audit prostredníctvom certifikovaného audítora do 5 rokov** a následne v periodicite podľa vyhlášky
- Podrobnosti o audite upravuje vyhláška

Certifikácia kybernetickej bezpečnosti

- Systémom certifikácie kybernetickej bezpečnosti je súbor pravidiel a postupov na riadenie jednotlivých schém certifikácie kybernetickej bezpečnosti.

- Schéma certifikácie kybernetickej bezpečnosti je súbor pravidiel, technických požiadaviek, technických noriem a postupov, ktoré sa uplatňujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov IKT, služieb IKT alebo procesov IKT.

- Certifikáciu kybernetickej bezpečnosti pre úrovne záruky základná, významná a vysoká podľa osobitého predpisu vykonáva len akreditovaná osoba.

- Akreditovanou osobou pre certifikáciu kybernetickej bezpečnosti pre úroveň záruky vysoká môže byť len Národný bezpečnostný úrad

Jaroslav Ďurovka, CISM
Riaditeľ Národného centra kybernetickej bezpečnosti