Čo nám prináša nová regulácia v oblasti kybernetickej bezpečnosti

Eset Security Days 2025
Bratislava, 9. 4. 2025

Nový regulačný rámec kybernetickej bezpečnosti

Akt o kybernetickej bezpečnosti (CSA)
Nariadenie (EU) 2019/881

Akt o kybernetickej odolnosti
Nariadenie (EU) 2024/2847
– účinné 11.12.2027

NIS2 Smernica (EU) 2022/2555
- účinná 17.10.2025

DORA nariadenie (EU) 2022/2554
– účinné 17.1.2025

Delegované a vykonávacie nariadenia EK k DORA

Vykonávacie nariadenie Komisie (EÚ) 2024/2690 pre digitálny sektor
- **účinné 17.10.2025**

Zákon č. 195/2019 Z. z. o ITVS

Vyhláška ÚPVSRpII č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení ITVS

Sektorová regulácia

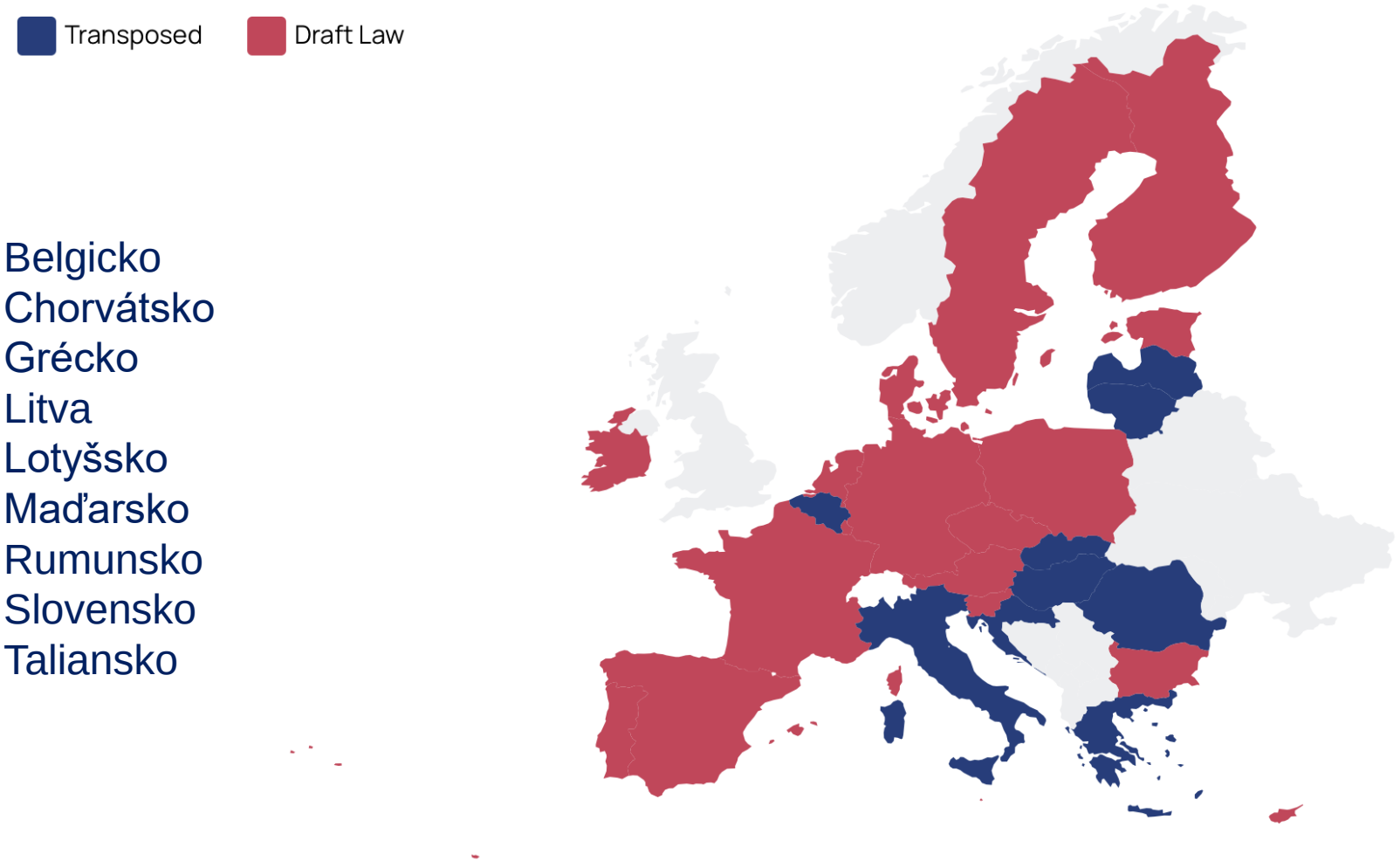
Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- novela účinná od 1.1.2025

Vyhlášky NBÚ

Nová vyhláška o bezpečnostných opatreniach a vyhláška o nahlasovaní – v príprave

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Stav transpozície NIS2 v členských štátoch EÚ (stav k 6.3.2025)



Belgicko
Chorvátsko
Grécko
Litva
Lotyšsko
Maďarsko
Rumunsko
Slovensko
Taliansko

(c) European Cyber Security Organization, ecs-org.eu, April 2, 2025

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

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 alebo obrat / 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	

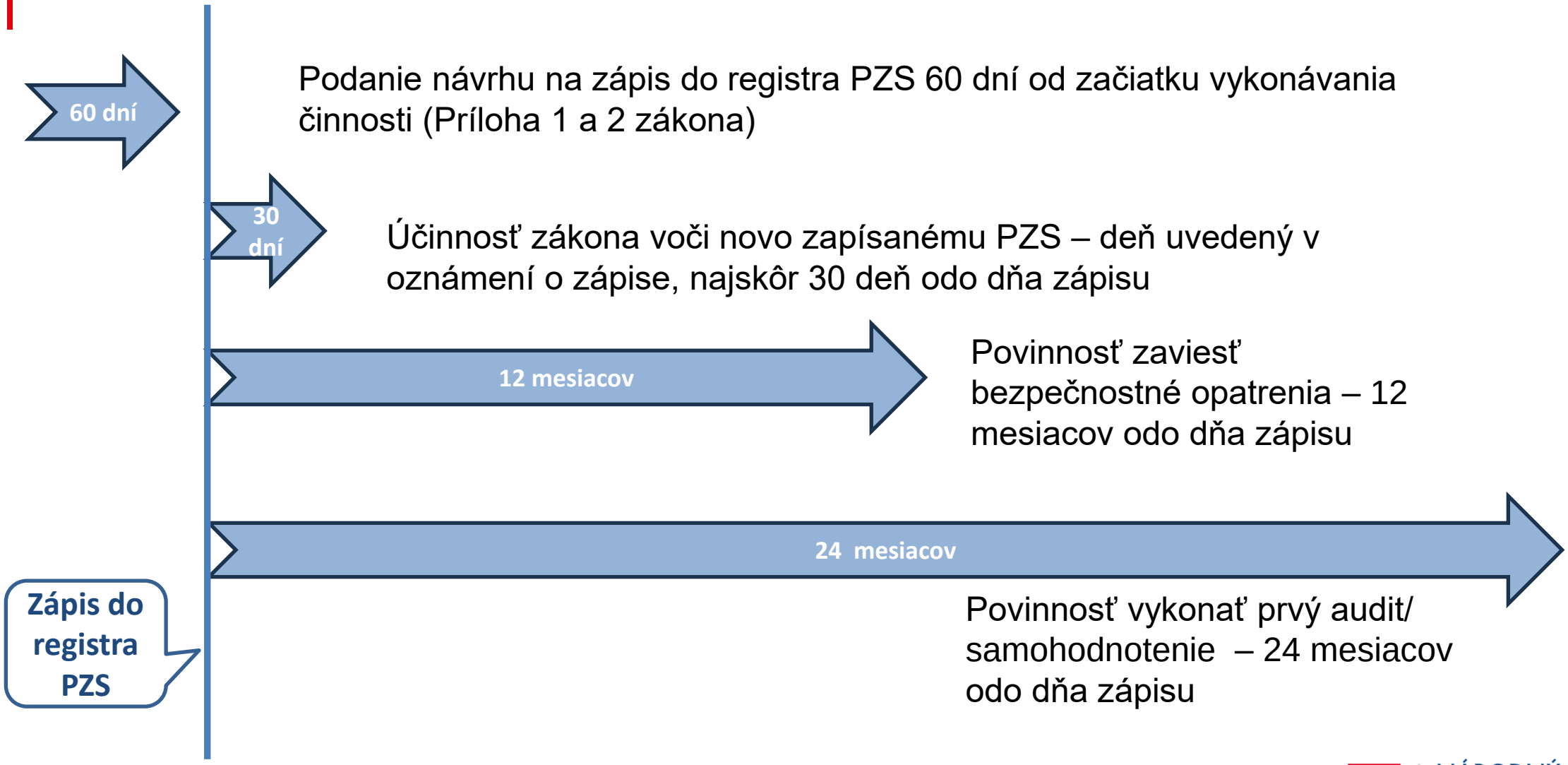
NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

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 alebo obrat 50 mil. EUR / 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**.**

Základné lehoty pre prevádzkovateľa základnej služby



Aplikácia bezpečnostných opatrení

- Nová štruktúra všeobecných bezpečnostných opatrení (§20 ods. 1 a 2)
- Rozsah a spôsob implementácie bezpečnostných opatrení na základe rizikovej analýzy
- Povinnosť zaviesť bezpečnostné opatrenia do 12 mesiacov odo dňa zápisu do registra PZS
- **Aplikovateľné bezpečnostné opatrenia (podľa §20 zákona):**
  - **Povinné ciele opatrení a minimálne požiadavky - §20 ods. 1 a 4**
  - Všeobecné - vyhláška NBÚ, ktorou sa ustanovuje sa ustanovuje obsah bezpečnostných opatrení ... – *v príprave*
  - Sektorové – vyhláška iného ústredného orgánu v spolupráci NBÚ – *zatiaľ nevydané*
  - **Sektorové – na základe osobitných právnych predpisov:**
    - **ITVS - zák č. 95/2019 Z.z. a príslušné vyhlášky**
    - Finančný sektor - DORA a príslušné RTS(es)
    - Digitálne sektory – Vykonávacie nariadenie EK č. 2024/2690

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)

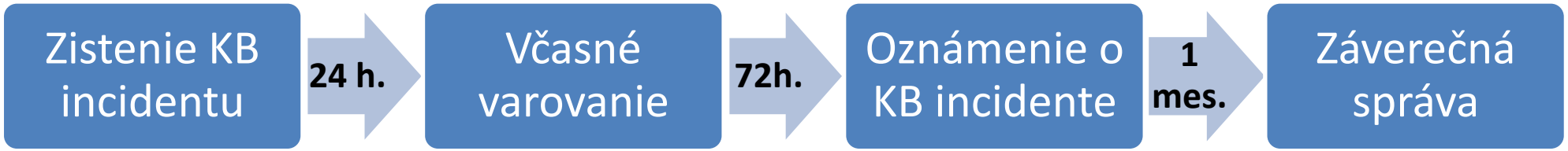
Tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, má uzatvorenú zmluvu s PZS, ktorý prevádzkuje kritickú základnú službu **má postavenie PZS**

- 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

Nové vyhlášky NBÚ - indikatívny obsah

Vyhláška o bezpečnostných opatreniach

- Základná štruktúra:
  - obsah a rozsah bezpečnostných opatrení
  - obsah a štruktúra bezpečnostnej dokumentácie
  - podrobnosti k riadeniu rizík
- Príloha obsahuje zoznam až 152 bezpečnostných opatrení a uvedením aplikovateľnosti na IT a OT systémy a na PZS alebo PKZS

Vyhláška o nahlasovaní

- Podrobnejšie kritériá na určenie závažného KB incidentu
- Vzťah k nahlasovaniu incidentov podľa osobitných predpisov
- Nahlasovanie iných udalostí (§24 ods. 5 ZoKB)
- Podrobnosti o obsahu a spôsobe hlásenia

Ide zatiaľ iba pracovné verzie obsah vydaných vyhlášok sa môže byť iný ako je tu uvedené.

Jaroslav Ďurovka, CISM
Riaditeľ Národného centra kybernetickej bezpečnosti

Dodatočné informácie

Definície

1. 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
   a. 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,
   b. obmedzenie alebo narušenie kritického subjektu, jeho základnej služby alebo kritickej infraštruktúry,
   c. hospodársku stratu vyššiu ako 0,1 % hrubého domáceho produktu podľa údajov z bezprostredne predchádzajúceho rozpočtového roka, alebo
   d. hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 eur,

2. 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
   a. vyžadovať vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni,
   b. spôsobiť viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo úmrtie aspoň jednej osoby,

3. 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,

4. osobou, ktorá je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická osoba, ktorej narušenie z dôvodu kybernetického bezpečnostného incidentu môže vyžadovať vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.