Kybernetická bezpečnost v praxi – NIS2 v České republice – zkušenosti z roku 0 po NIS2

Antonín Šefčík

NGSS
Next Generation
Security Solutions

Směrnice NIS 2

- EU přichází s aktualizací požadavků na kybernetickou bezpečnosti v nová směrnici o kybernetické bezpečnosti **SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)**

- Publikace finálního znění směrnice NIS2 proběhla v **prosinci 2022**. Transpoziční lhůta (tj. lhůta, ve které musí členské státy směrnici promítnout do národního práva) je stanovena na **21 měsíců**

- NIS2 již nehledá systémy důležité pro společnost, ale definuje **celé služby důležité pro její fungování**

NIS 2 - požadavky

Směrnice stanovuje okruhy bezpečnostních opatření, které mají členské státy rozpracovat ve svých právních předpisech a uložit je budoucím povinným osobám:

- **Analýza rizik** a **politiky bezpečnosti informací**
- Zvládání **incidentů**
- **Kontinuita činností** včetně zálohování, zotavení (disaster recovery) a krizového řízení
- Bezpečnost v rámci **dodavatelského řetězce**
- Bezpečnost v rámci **pořízení, vývoje a údržby systémů**
- Politiky a postupy pro **hodnocení účinnosti bezpečnostních opatření** (tj. audit)
- Praktiky **základní počítačové hygieny a vzdělávání** v oblasti kybernetické bezpečnosti
- Politiky a postupy týkající se **využívání kryptografie**
- **Bezpečnost lidských zdrojů**, **řízení přístupů** a **aktiv**
- Využívání **vícefaktorového ověření identity**, bezpečných komunikačních nástrojů a nástrojů pro nouzovou komunikaci

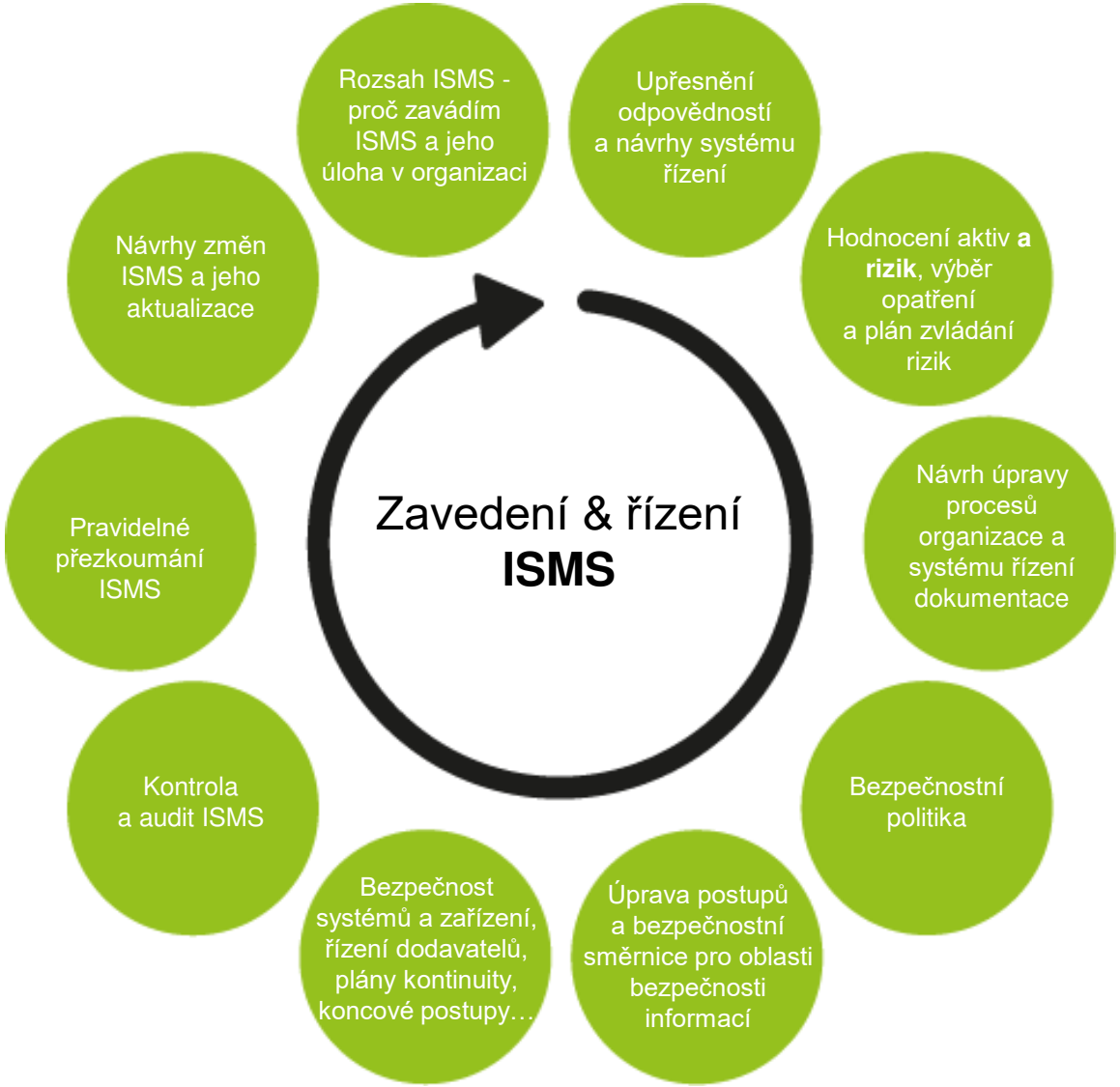
Odvětví regulovaných služeb

1. **Veřejná správa**
2. Energetika – Elektřina
3. Energetika – Ropa a ropné produkty
4. Energetika – Plynárenství
5. Energetika – Teplárenství
6. Energetika – Vodík
7. Výrobní průmysl
8. Potravinářský průmysl
9. Chemický průmysl
10. Vodní hospodářství
11. Odpadové hospodářství
12. Letecká doprava
13. Drážní doprava
14. Vodní doprava
15. Silniční doprava
16. Digitální infrastruktura a služby
17. **Finanční trh (DORA)**
18. Zdravotnictví
19. Věda, výzkum a vzdělávání
20. Poštovní služby
21. Vojenský průmysl
22. Vesmírný průmysl

Jaký je stav

- Kybernetickou bezpečnost **budou muset zavést tisíce organizací**
- U stávajících organizací – povinných osob se jedná o **prohloubení již zavedených požadavků**
- U tisíců organizací se **však jedná o zavedení nových požadavků**, u většiny v režimu nižších povinností, minimálně u stovek však v režimu vyšších povinností
- Je na co navázat?
    - ISMS dle **ISO/IEC 27001** (a další případné normy)
    - **Informační systémy veřejné správy** (Informační koncepce, bezpečnostní dokumentace informačního systému veřejné správy)
    - Krizové řízení
    - Dosavadní opatření fyzické bezpečnosti
    - ….

Jak na to – zavést ISMS



Jedná o **zavedení a provoz ISMS** s:

- vymezeným rozsahem
- výběrem opatření na základě hodnocení rizik
- který má zavedené role a opatření
- je pravidelně auditován a hodnocen

Zavádění ISMS – možný postup

1. Určení jaké požadavky kybernetické bezpečnosti se na mne budou vztahovat (nižší X vyšší)
2. Provedení srovnávací analýzy současného stavu kybernetické bezpečnosti vůči požadavkům stávající vyhlášky, minimálního bezpečnostního standardu nebo návrhům vyhlášek
3. Provedení identifikace a hodnocení aktiv, případně provedení analýzy dopadů.

Výše uvedené analytické kroky je možné realizovat v roce 2023, vlastní zavádění pak doporučujeme realizovat v roce 2024 po vydání nového zákona a navazujících vyhlášek.

4. Dokončení procesu zvládání rizik – návrh bezpečnostních opatření
5. Implementace vybraných bezpečnostních opatření zahrnuje návrh postupů, jejich popis v bezpečnostní dokumentaci, příprava a realizace technických opatření, rozpracování plánů kontinuity, školení …
6. Provedení interního auditu a přezkoumání ISMS uzavírá celý cyklus zavedení systému řízení bezpečnosti informací.
7. Přezkoumání ISMS

Na co si dát pozor

- Navázat na to co již bylo v oblasti bezpečnosti zavedeno
- Připravit si plán zavedení
- Počítat s časovou a projektovou náročností, vyčlenění zdrojů
- Jednotný systém řízení bezpečnosti informací
- Neopakovat chyby spojené s GDPR

Děkuji za pozornost