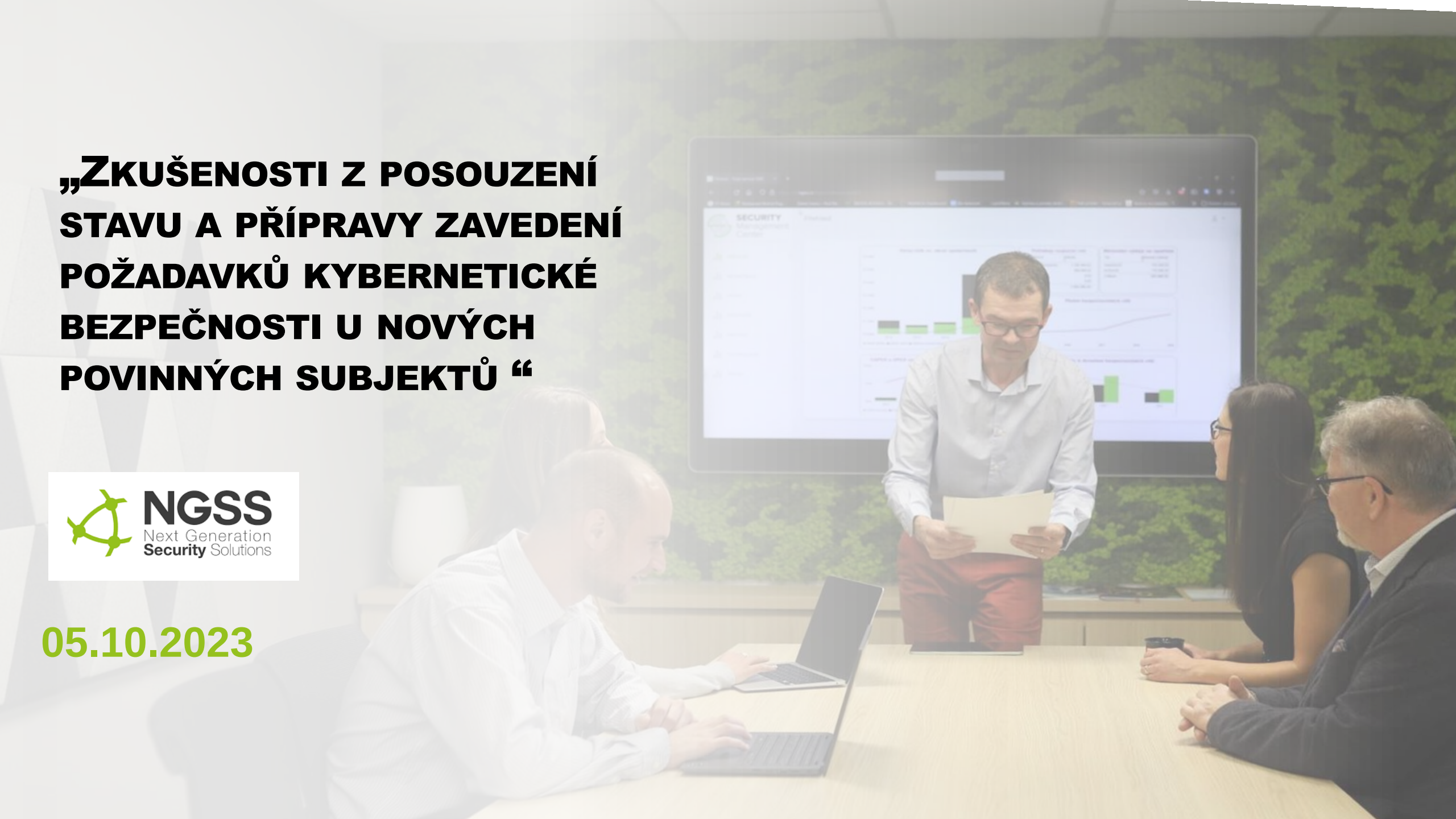
„Zkušenosti z posouzení stavu a přípravy zavedení požadavků kybernetické bezpečnosti u nových povinných subjektů “



NGSS
Next Generation
Security Solutions

05.10.2023

Výchozí stav

- Kybernetickou bezpečnost **budou muset zavést tisíce organizací**
- U stávajících povinných osob (organizací) se jedná většinou o **prohloubení již zavedených požadavků**
- U tisíců organizací se **však jedná o zavedení nových požadavků**, u většiny v režimu nižších povinností, minimálně u stovek možná až tisíců však v režimu vyšších povinností
- Výchozí stav se liší v závislosti na tom, zda organizace:
  - je již povinnou osobou
  - provozuje systém řízení bezpečnosti informací (úroveň?)
  - má zavedený některý ze systémů řízení managementu
  - již řeší krizové řízení
  - využívá strukturované řízení
  - řeší projektové řízení
  - a další …

Zaznamenané tendence

- Nezavádím systém řízení bezpečnosti, ale jen bezpečnostní požadavky
- Nevím co je rozsah
- Manažera kybernetické bezpečnosti chci jednoznačně outsourcovat
- Kybernetická bezpečnost se týká jen IT
- Bezpečnostní postupy a jejich zdokumentování jen zvyšují administrativu

X

Snaha

- Ochránit organizaci před hrozbami
- Řešit kybernetickou bezpečnost
- Promýšlení zejména technických řešení

Režim nižších povinností

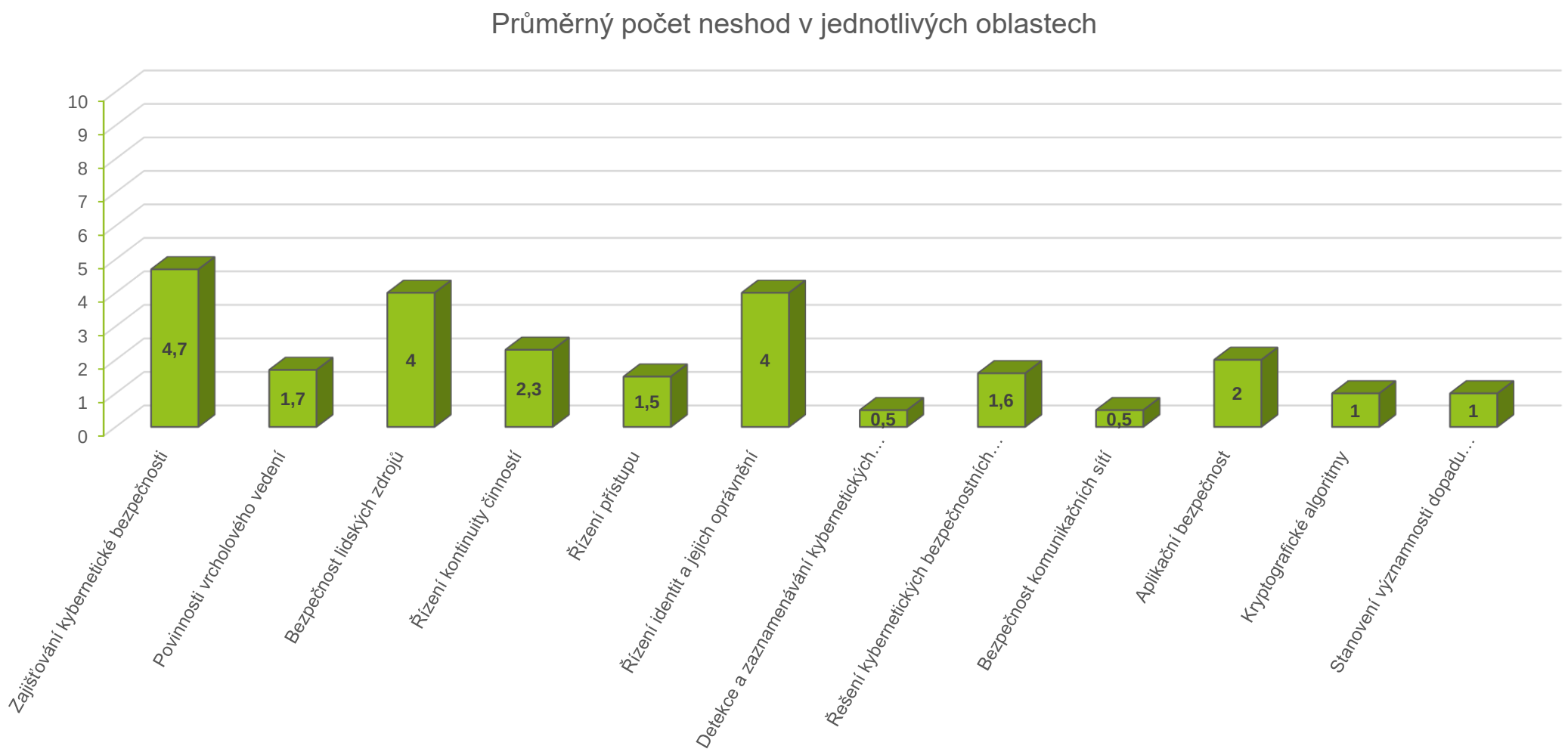
- U organizací, které mají zavedený systém řízení bezpečnosti informací se jedná o mírnou úpravu
- U stávajících povinných osob (s bezpečnostními orgány) zaznamenána tendence dostat se do vyšších povinností
- U tisíců organizací, které doposud neřešily kybernetickou bezpečnost se ukazuje jako problematické:
  - Pochopení systému řízení bezpečnosti informací
  - Určení odpovědností s důrazem na osobu odpovědnou za kybernetickou bezpečnost
  - Není bezpečnostní dokumentace - Bezpečnostní politika ani další politiky požadované vyhláškou nejsou vytvořeny
  - Práce s dodavateli se omezuje na smlouvu o mlčenlivosti
  - Minimální rozlišení incidentů
  - Chybí dvoufaktorová autentizace, jednoduchá hesla a sdílené účty

Úroveň opatření - nižší povinnosti

- **Řízení přístupu**
- **Detekce a zaznamenávání KBU**
- **Bezpečnost komunikačních sítí**
- **Kryptografické algoritmy**

- Zajišťování kybernetické bezpečnosti

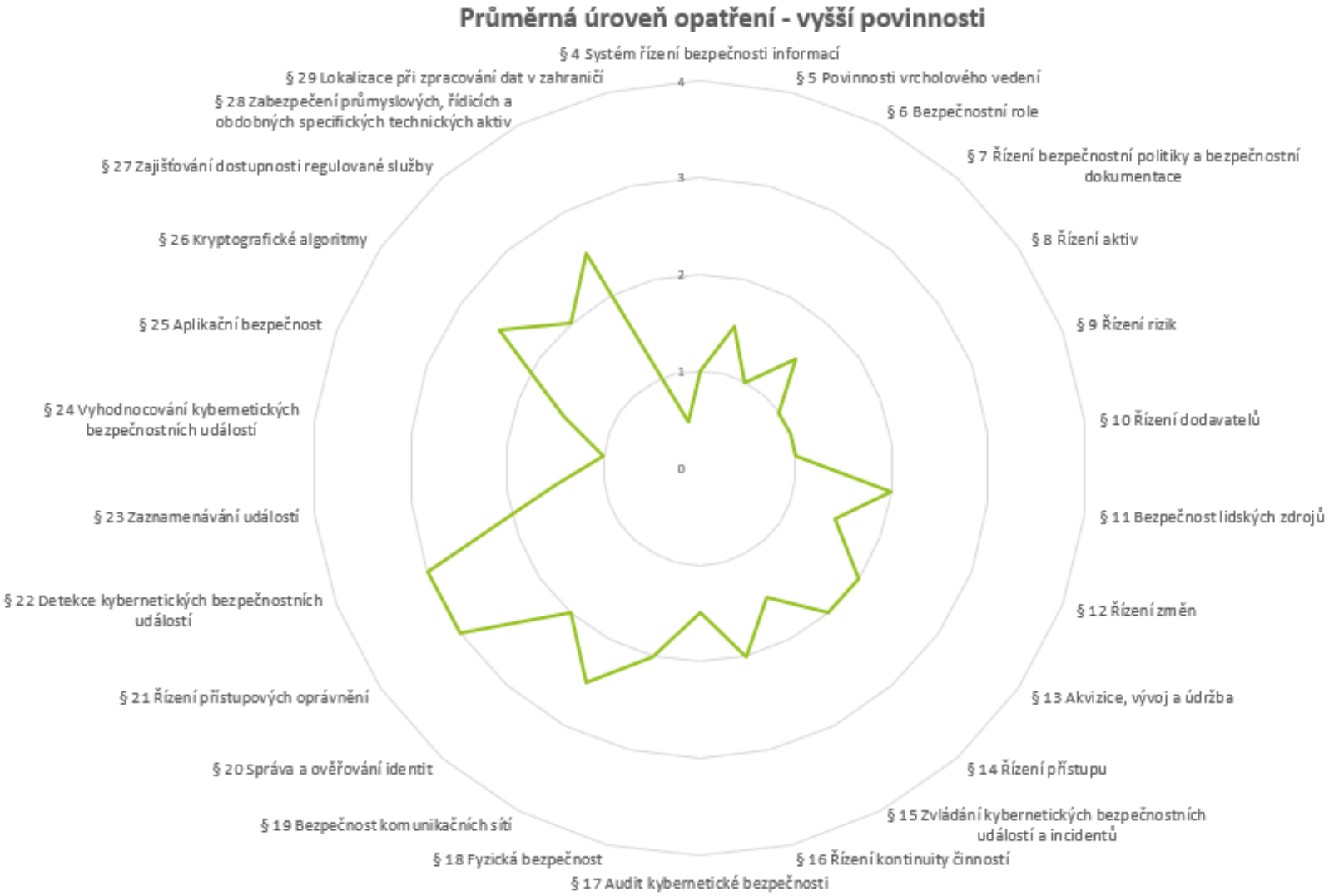
Neshody - nižší povinnosti



Režim vyšších povinností

- Stávajících povinné osoby rozvíjejí existující sytém řízení bezpečnosti informací
- Složitá situace u nových subjektů:
  - Role manažera je směřována na vedoucího IT
  - Není jim jasné proč by měli zřizovat některé role – zejména architekta kybernetické bezpečnosti
  - Je pro ně složité orientovat se v oblasti řízení aktiv a především analýzy rizik
  - Nízká míra popisu bezpečnostních procesů
  - Slabě řešena bezpečnost dodavatelů
  - Chybí popisy k technickým opatřením
  - Nejsou zpracovány havarijní plány, ani plány kontinuity činností
  - Slabší vyhodnocování

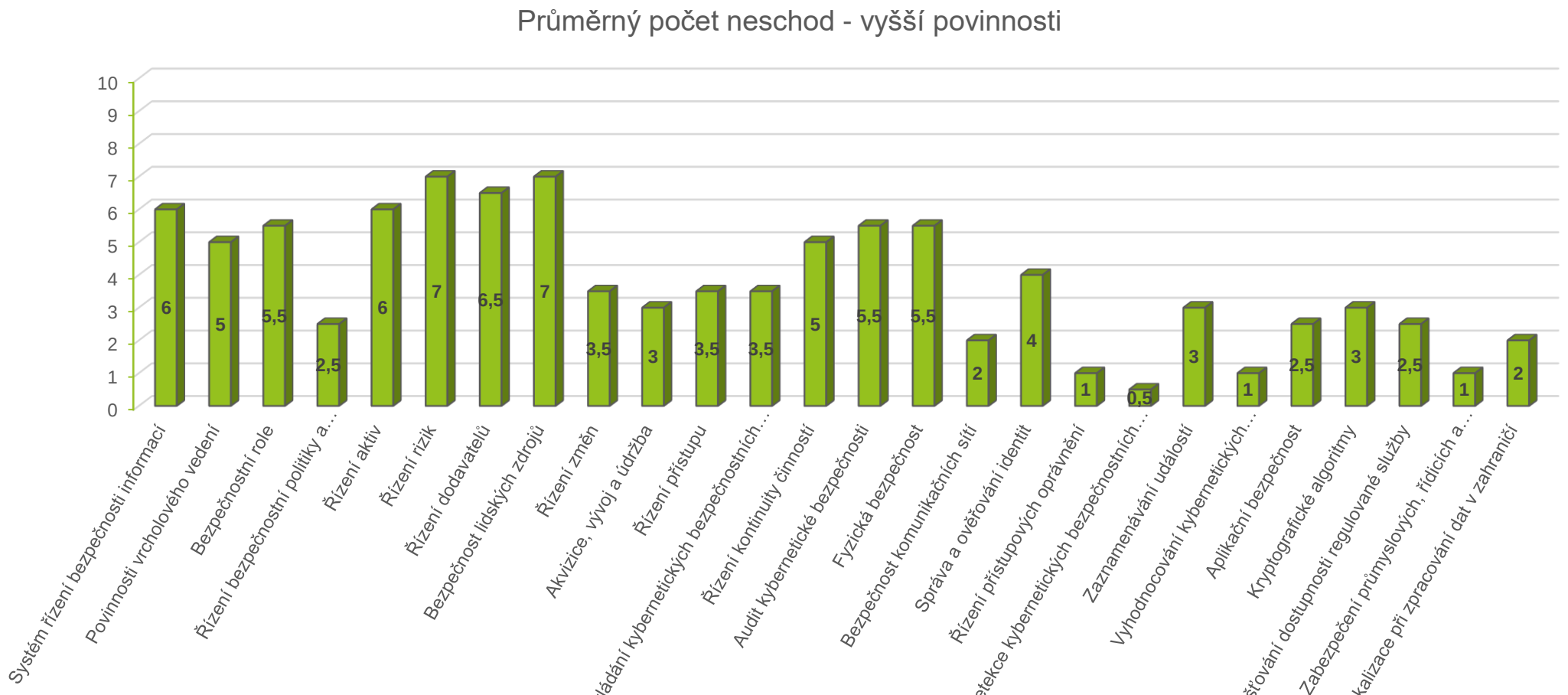
Úroveň opatření - vyšší povinnosti



- **Řízení přístupových oprávnění**
- **Detekce kybernetických bezpečnostních událostí**

- Lokalizace při zpracování dat v zahraničí
- Systém řízení bezpečnosti informací
- Bezpečnostní role
- Řízení aktiv
- Řízení rizik
- Řízení dodavatelů

Neshody - vyšší povinnosti



Co je možné využít

- ISMS dle **ISO/IEC 27001** (a další případné normy)
- ISVS – Informační systémy veřejné správy (Informační koncepce, bezpečnostní dokumentace informačního systému veřejné správy)
- Krizové řízení
- Dosavadní opatření fyzické bezpečnosti
- Systémy managementu
- Ochrana osobních údajů
- Popsané procesy IT (ITIL…)
- Plány obnovy
- ….

NIS 2 – důraz na služby

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

- Podstatné je určit **služby a stanovit rozsah, který je potřebný pro zajištění jejich chodu**

Následně zavést **systém řízení bezpečnosti informací,** který:

- má za cíl **ochránit zpracovávané informace** a
- k dosažení cíle **zavede sadu bezpečnostních opatření**
- vybraných na základě **ohodnocení aktiv/rizik**
- je pravidelně **auditován a hodnocen**

Zavedení SŘBI / zajištění KB

1. Provedení srovnávací analýzy současného stavu kybernetické bezpečnosti vůči požadavkům příslušné vyhlášky
2. Upřesnění rozsahu SŘBI a zahájení hodnocení aktiv a rizik a přijetí bezpečnostních opatření k určení možných rizik a návrhu jejich pokrytí

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

3. Dokončení hodnocení rizik a přijetí bezpečnostních opatření k pokrytí zjištěných rizik
4. Implementace vybraných bezpečnostních opatření zahrnuje návrh postupů, jejich popis v bezpečnostní dokumentaci, zpracování plánů kontinuity a DRP a rozpracování do návrhu záznamů systému řízení bezpečnosti informací
5. Provedení interního auditu a přezkoumání SŘBI

Na co si dát pozor

- Navázat na to co již bylo v oblasti bezpečnosti zavedeno
- Počítat s časovou a projektovou náročností, vyčlenění zdrojů
- Připravit si plán zavedení s důrazem na upřesnění Rozsahu SŘBI:
  - Charakteristika regulované služby
  - Jaké informační systémy SŘBI pokrývá
  - Posouzení vnitřních podmínek a závislostí SŘBI
  - Základní odpovědnosti a struktura řízení SŘBI
  - Návrh postupu zavedení SŘBI včetně způsobu zdokumentování zásad a postupů SŘBI
  - Přehled primárních aktiv (informací)
  - Rozhraní s ostatními procesy organizace
  - Interní a externí zainteresované strany zavádění SŘBI včetně možných významných dodavatelů
  - Zdroje na zajištění kybernetické bezpečnosti
  - Hranice SŘBI vůči vnějšímu světu

Děkuji za pozornost

Antonín Šefčík

asefcik@ngss.cz

+ 420 601 307 992