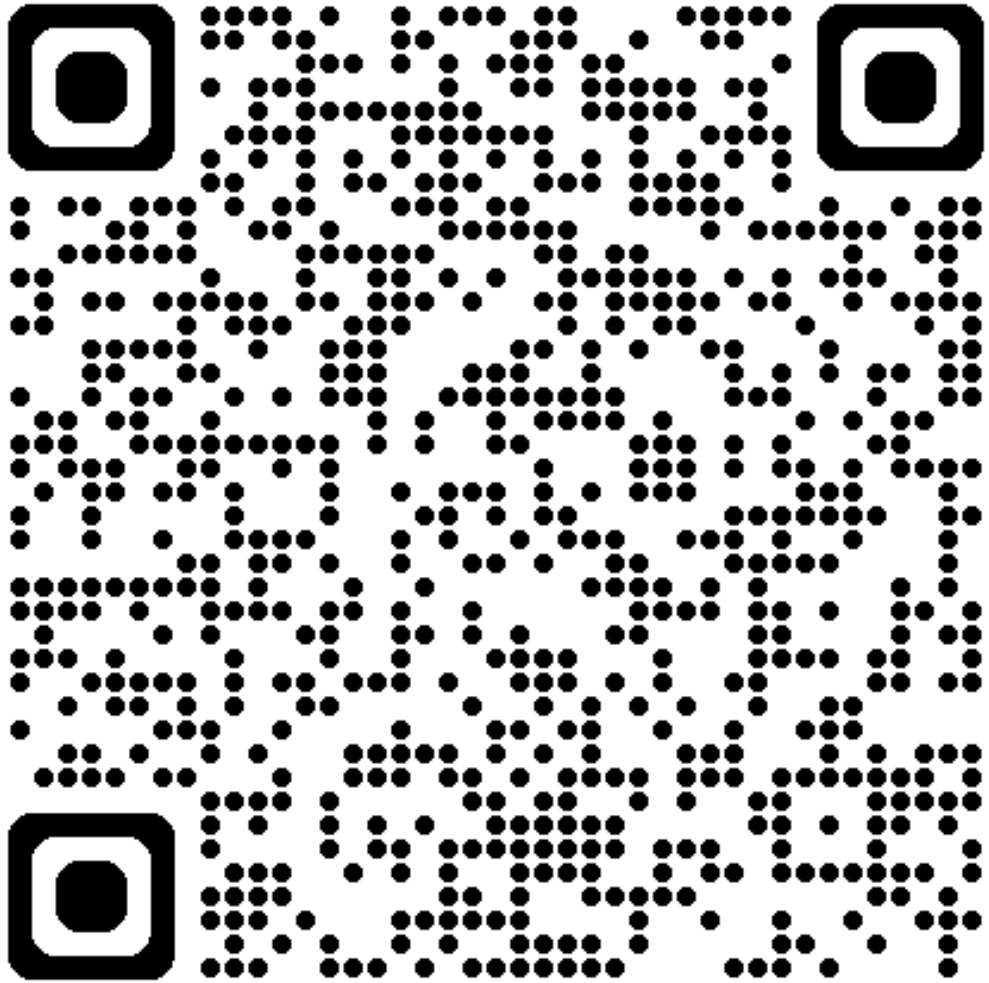
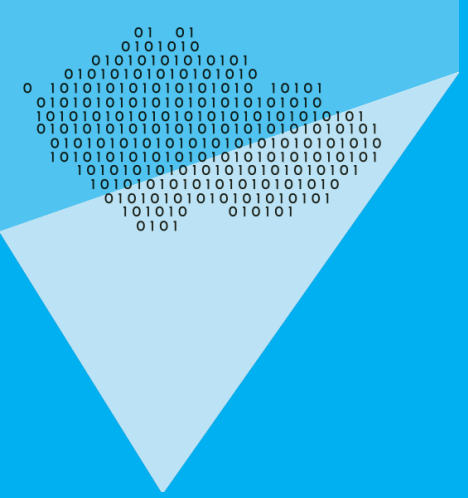
Národní strategie kybernetické bezpečnosti

2026

CSNOG 2026
TLP:CLEAR

Petr Procházka
Oddělení národních strategií a politik NÚKIB





Strategický kontext

V jakém prostředí strategii aktualizujeme?

Strategický kontext

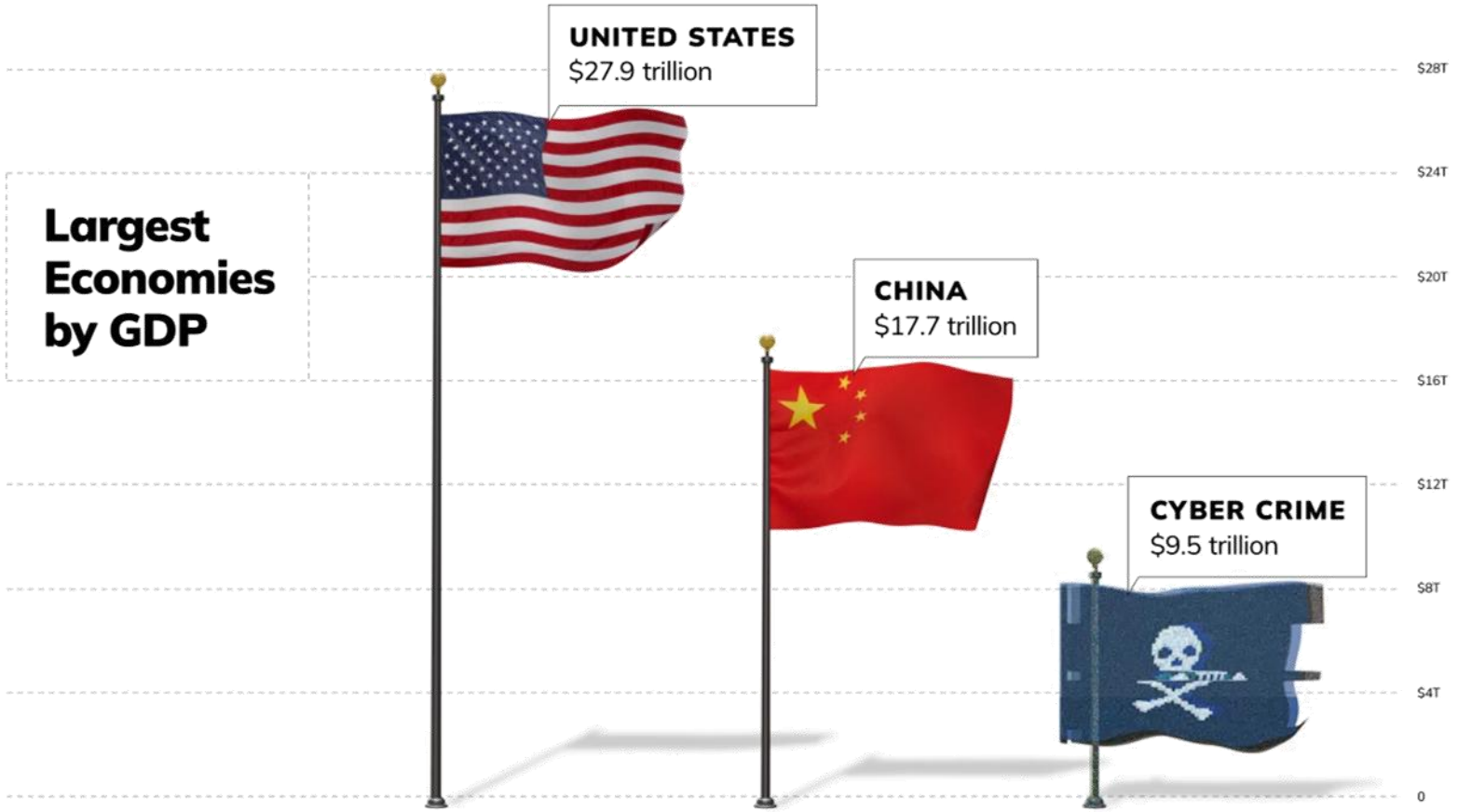
191

bilionů Kč

Škody způsobené kyberkriminalitou

(Cybersecurity Ventures, 2025)

Strategický kontext



(Bloomberg, 2024)

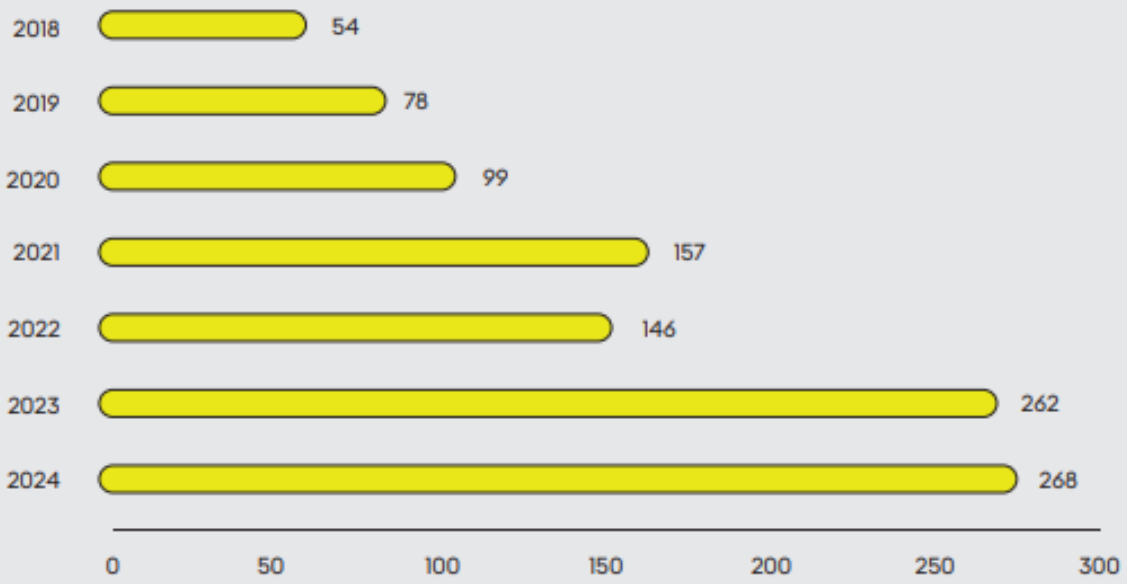
Strategický kontext

268 Incidentů řešených NÚKIB v 2024

(NÚKIB, 2025)

Strategický kontext

NÚKIB v roce 2024 evidoval celkem 268 kybernetických bezpečnostních incidentů, což je dosud nejvyšší evidovaná hodnota.



(Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024)

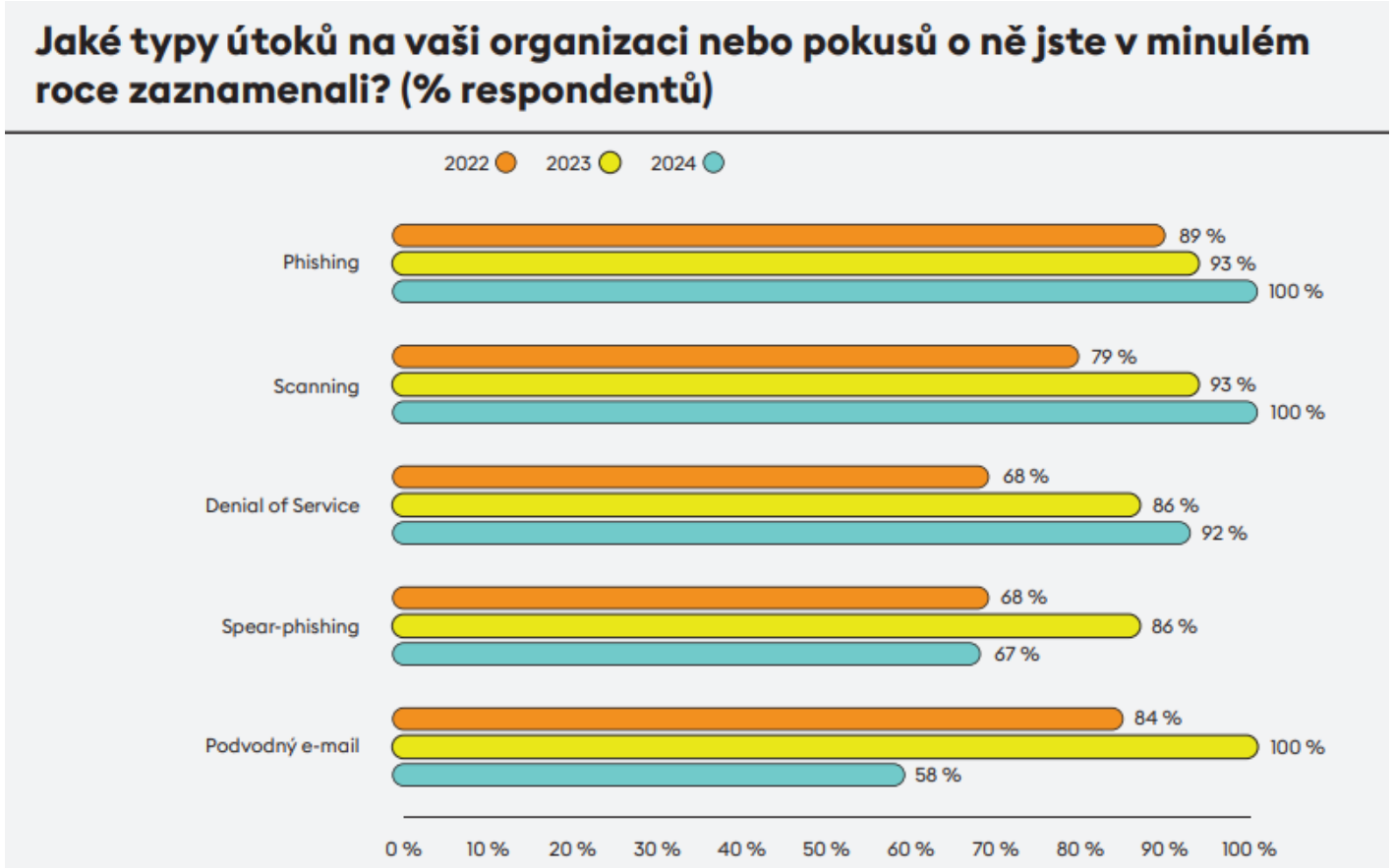
Strategický kontext

1984

Počet útoků na organizaci za týden

(Check Point, 2025)

Strategický kontext



(Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024)

NSKB 2026

ZSKB 2024

Vize a cíle Česka 2026-2030(?)

Jaké budou kroky státu a společnosti v následujících letech?

Vize

Česko bude **bezpečným** a **digitálně vyspělým** státem s odolnou informační infrastrukturou, **vzdělanou, kriticky myslící a inovativní** společností a **silnými** mezinárodními i domácími partnerstvími, s jejichž pomocí zajistí **efektivní ochranu a prosazování** svých zájmů v kyberprostoru.

Strategické oblasti

Fenomén oblasti: množství a rychlost útočníků & domino efekt dodavatelů

Fenomén oblasti: množství a rychlost útočníků & domino efekt dodavatelů

51 s/48 min

Doba do rozšíření útočníka v síti

10 dnů

Aktivita útočníka do detekce

(CrowdStrike, 2025; Mandiant, 2024)

Fenomén oblasti: množství a rychlost útočníků & domino efekt dodavatelů

Geopolitika:

- Vzrůstá aktivita státních aktérů (vč. APT napojených na RF a ČLR)
- Útoky zlevňují, množství aktérů hrozeb a jejich schopnosti rostou

Problém:

- Významně se liší úroveň zabezpečení organizací
- Rizika dodavatelského řetězce
- Financování nedostačuje

Fenomén oblasti: množství a rychlost útočníků & domino efekt dodavatelů

Co s tím:

- Posílit dostupnost sdílených služeb kybernetické bezpečnosti a proaktivní detekci a reakci
- Bezpečné dodavatelské řetězce (standardy, certifikace, podpora bezpečných řešení)
- Efektivnější nakládání se zdroji, sjednocování architektury a data governance

Fenomén oblasti: málo lidí, velký potenciál

Fenomén oblasti: málo lidí, velký potenciál

300 000

Chybějících expertů v EU

(Cyber Skills Academy, 2024)

Fenomén oblasti: málo lidí, velký potenciál

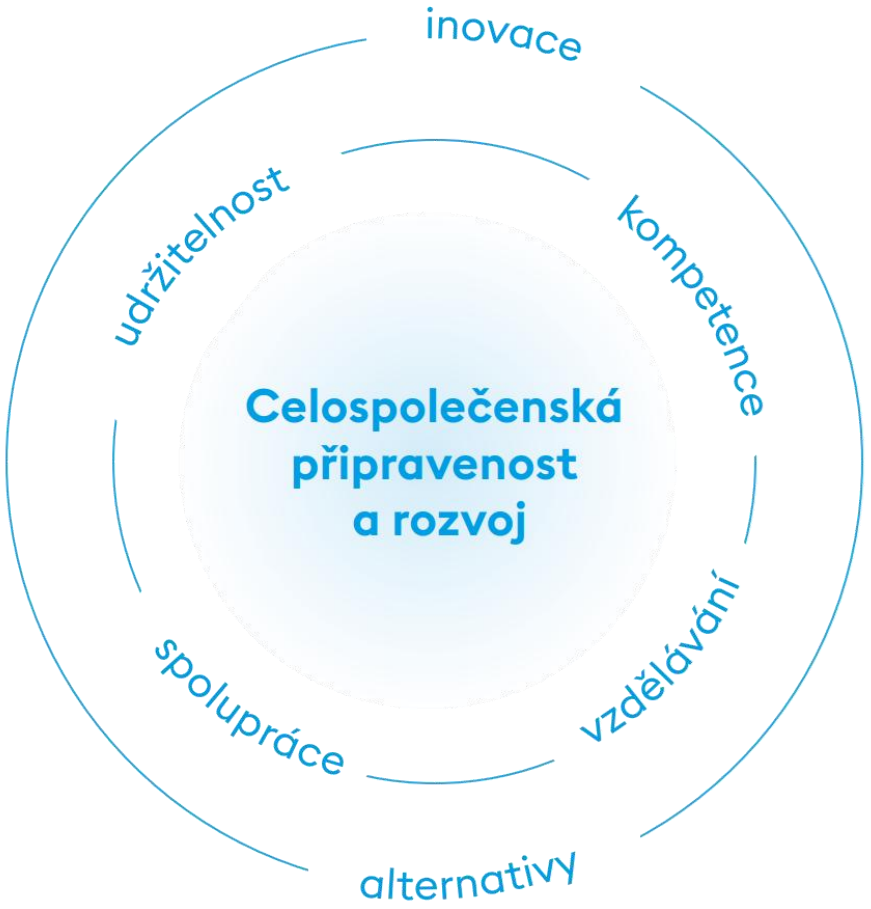
Problém:

- ČR i celá EU trpí nedostatkem expertů
- Phishing a sociální inženýrství zůstávají nejlevnější cestou útoku
- Složité nebo neexistující procesy omezují připravenost státu na krize

Fenomén oblasti: málo lidí, velký potenciál

Co s tím:

- Posilování počtů a motivace expertů
- Zvyšování znalostí a gramotnosti společnosti
- Sdílení informací a spolupráce
- Podpora výzkumu a inovací, včetně vzniku bezpečných technologických alternativ



Investice se vyplácí

Organizace, které investovaly do bezpečnostních nástrojů zahrnujících umělou inteligenci a automatizaci, zaznamenaly v průměru snížení nákladů na únik dat o **38,4 milionu korun českých** a zkrácení doby k identifikaci a řešení incidentu o **108 dní**.

(ENISA, 2024)

Fenomén oblasti: proměnlivé prostředí a tlak na změnu mezinárodního řádu

Fenomén oblasti: proměnlivé prostředí a tlak na změnu mezinárodního řádu

19/27

Počet států s dokončenou transpozicí NIS2

(European Cyber Security Organisation, 2025)

Fenomén oblasti: proměnlivé prostředí a tlak na změnu mezinárodního řádu

Problém:

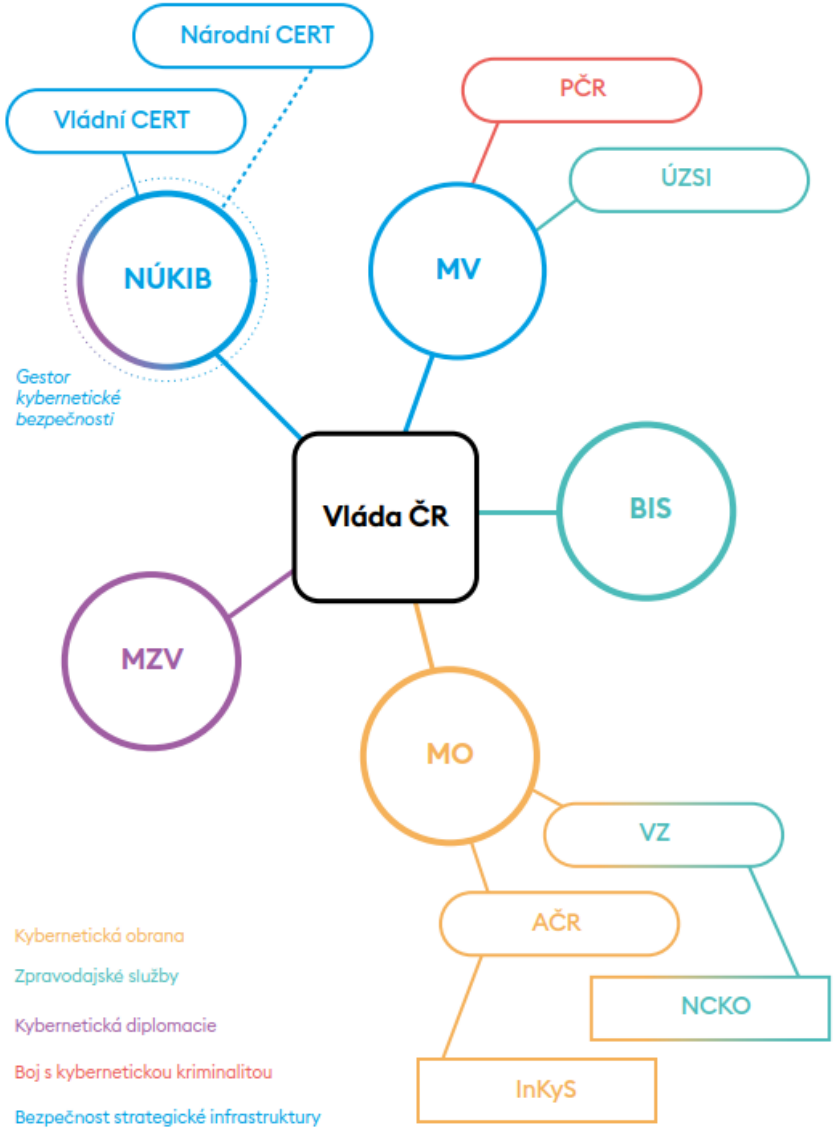
- Státní a na ně napojení aktéři aktivně působí vůči Česku a jeho spojencům v kyberprostoru nepřátelsky
- Dochází k tlakům na změnu mezinárodního řádu a snahy o kontrolu a fragmentaci Internetu
- Zvyšující se složitost a množství EU regulace

Fenomén oblasti: proměnlivé prostředí a tlak na změnu mezinárodního řádu

Co s tím:

- Posilovat pro Česko výhodná mezinárodní partnerství
- Aktivně prosazovat zájmy Česka – vzhledem k mezinárodnímu právu i normám EU
- Chránit otevřený, bezpečný a svobodný Internet
- Hledat společnou EU cestu k diverzifikaci technologií

Jak to provést



Co si z toho odnést?

1. Budovat odolnost musíme ve svých organizacích všichni – samotný stát to nezvládne.
2. Investice do bezpečnosti jsou levnější než řešení škod.
3. Strategie je rámec pro praktická rozhodnutí a investice, akční plán konkrétní kroky státu.
4. Bavme se spolu, spolupracujme a dávejme si zpětnou vazbu.

Děkuji za pozornost a zůstaňme v kontaktu!

petr.prochazka@nukib.gov.cz

LinkedIn