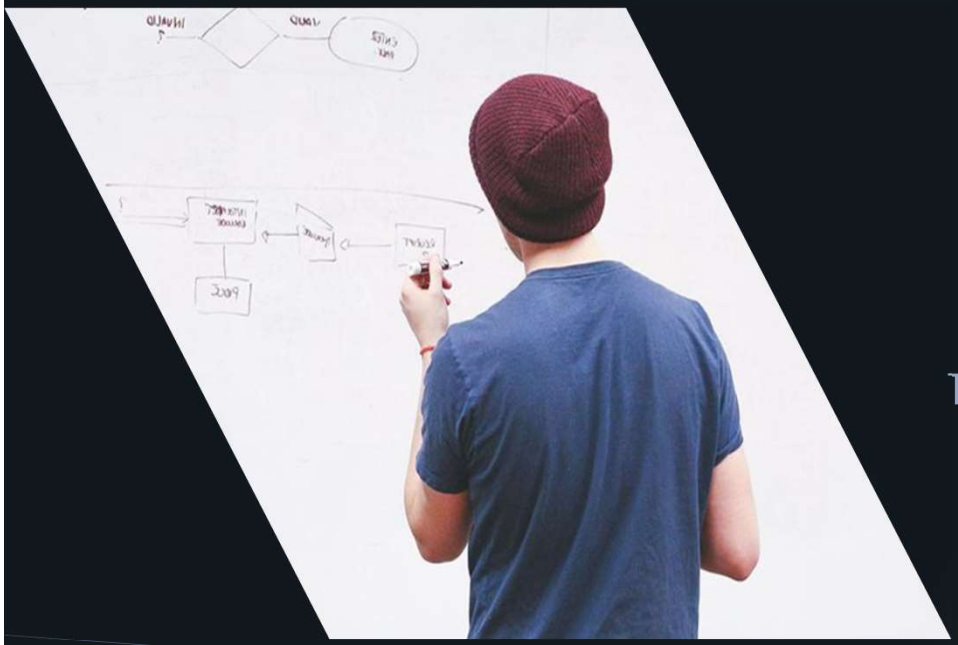
Kybernetická bezpečnost

Výzvy nejen pro veřejnou správu v nejbližších letech

GEOINFORMACE VE VEŘEJNÉ SPRÁVĚ 2024

GEPRO

> Kybernetické bezpečnosti se věnujeme, chceme se podělit o věci, které se vás také mohou týkat.



Obsah:

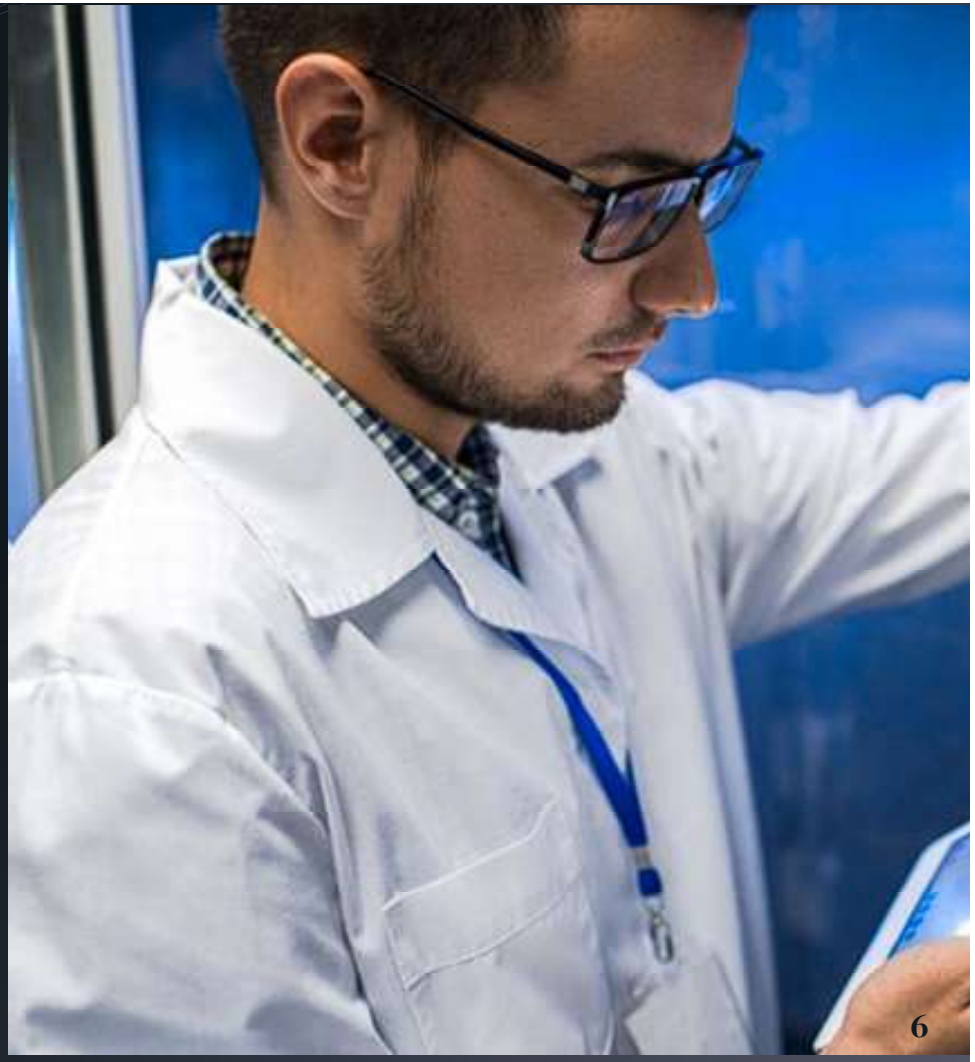
1. Co je kybernetická bezpečnost a proč ji řešit
2. Co a pro koho se chystá
3. Jak se to nemá dělat
4. Pochvala NÚKIBu

1.
Co je kybernetická bezpečnost

Co nám hrozí?

- Zevnitř
  - Neoprávněné přístupy k datům
  - Poškození a ztráta dat
  - Narušení procesů a fungování
- Zvenčí
  - Zneužívání a vytěžování informací
  - Útoky – ovládnutí systému, změny dat, krádeže, zašifrování obsahu a vydírání

Kybernetická bezpečnost je systém opatření, které zajistí, že předchozí slide můžeme zapomenout.



Pilíře bezpečnosti

- Management
  - Proškolený management, pro který je téma důležité
  - Dobře zvládnutá analýza
  - Auditovatelnost a trvání na pravidlech
- Kvalitní IT zázemí a IT tým
  - Zkušený personál
  - Adekvátní systémové a technické prostředky
  - Bezpečný software a kvalitní dodavatelé
- Proškolení zaměstnanci

2.

Co a pro koho se chystá

Současnost a výhled

- V současnosti máme
  - Zákon o kybernetické bezpečnosti (implementuje NIS1)
  - Evropskou směrnici NIS1
  - ISO rodiny 27000
  - Široká doporučení v rámci Best practices
- Klíčová změna, která se chystá a nevyhneme se jí
  - Evropská směrnice NIS2
  - V našem právním pořádku se očekává letos
  - Změny se stanou závazné (povinné) v průběhu roku 2025

Proč se o tom bavím zde?

> **Přísnější směrnice EU o kybernetické bezpečnosti NIS 2 se v Česku podle odhadů dotkne nejméně 6000 soukromých i státních subjektů. Uloží jim rozsáhlé povinnosti, za jejichž nesplnění budou hrozit pokuty ve výši desítek milionů korun.**

Tomáš Kudělka
Director, Management Consulting
KPMG Česká republika


Kromě toho může dopadnout na
dodavatele povinných subjektů,
jejich organizační složky atp.

3.

Špatné příklady z praxe

státní, soukromé společnosti, zdravotnická zařízení – dále uváděné informace jsou čerpány z veřejně publikovaných zdrojů

Příklad 1: léta 2019, 2021

- 2019
  - Výpadek systémů na tři týdny
  - Škoda (vč. omezení výkonů) 59 mil. Kč
- 2021
  - 13. března 2021, výpadek 4 týdny
- 2021
  - 27. března 2021, výpadek 10 dnů

Příklad 2: rok 2022

- Zašifrování dat + vydírání
- Úplný útok – systémy účetní, provozní aj.
- Řada selhání
  - Útočníkům se podařilo dostat do systému
  - Útočníci nebyli dlouhodobě odhaleni
  - Selhaly také zálohy
- Účet jen za obnovu systémů 30 mil. Kč

Příklad 3: rok 2023

- Banky
- DDoS útok
- Obnova v řádech hodin

4.

Chvála NÚKIBu

A proč je radno na úřad upozornit

- NIS2 se týká většiny Evropy, ale my máme velmi komplexní informační stránku nis2.nukib.cz
- Nastavený režim, kdy jsou pravidelně a transparentně zveřejňována doporučení, analýzy rizik a informace pomáhají firmám i státní správě
- NÚKIB ochotně funguje také jako prostředník, poskytuje informace

Děkuji za pozornost!

josef.brozek@gepro.cz