

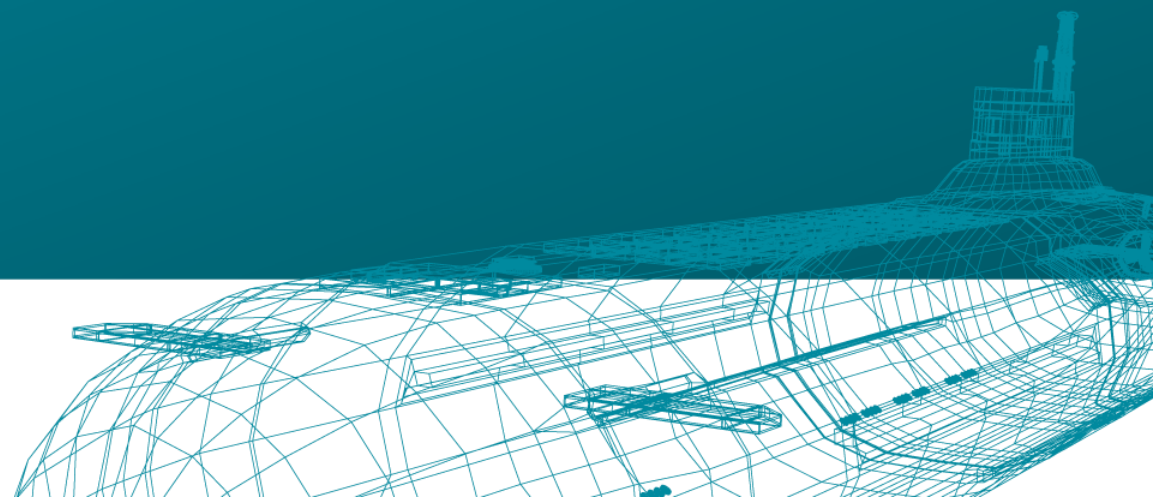
# Úroveň znalostí bezpečnostních rolí podle Zákona o kybernetické bezpečnosti

Michal Zedníček

Security consultant

[michal.zednicek@alef.com](mailto:michal.zednicek@alef.com)

ALEF NULA, a.s.



## › ZKB

- Prevence před možnými incidenty
  - Organizační opatření
  - Technická opatření
- Vyřešení následků možných incidentů
  - Řešení KBI

# Lidské zdroje

- › Podle ZKB patří regulace chování lidí mezi Organizační opatření
- › Regulace vzdělání o informační bezpečnosti patří mezi nejvýraznější regulace
  - Můžeme mít výborné procesy
  - Můžeme mít výborné technické nástroje
  - Procesy a technologie nepomáhají, když se lidé procesy neřídí a nezvládají práci s technickými nástroji

# Lidské zdroje

- › Chování lidí se odvíjí od vzdělání a přirozené inteligence
  - S přirozenou inteligencí musíme pracovat
  - Vzdělání můžeme/musíme ovlivnit

# Vzdělání

- › Musíme určit, kdo potřebuje vzdělávat
  - › Musíme určit, jak se bude kdo vzdělávat
- =
- › Musíme zavést podle ZKB „Plán rozvoje bezpečnostního povědomí“

# Vzdělání

- › Plán rozvoje bezpečnostního povědomí (§9 Vyhlášky o kybernetické bezpečnosti):
  - Forma, obsah a rozsah potřebných školení všech rolí
  - Poučení všech rolí formou vstupních a pravidelných školení
  - Vede přehledy školení
  - KII hodnotí účinnost plánu rozvoje bezpečnostního povědomí

# Vzdělání

- › ZKB neřeší dlouhodobé vzdělávání
  - Je práce univerzit a podobných institucí
  - Cílem takové instituce je na trh práce dovést člověka s velmi kvalitním vědomostním zázemím a velkým přesahem znalostí z různých oborů
- › ZKB řeší krátkodobé vzdělávání
  - Odpovědnost standardně na správcích KII/VIS
  - Rychlé, efektivní proškolení všech rolí
  - U některých rolí velká míra specializace docílená intenzivní formou vzdělávání

# Vzdělání

- › Jaké jsou role podle ZKB?
  - Manažer Kybernetické bezpečnosti
  - Architekt kybernetické bezpečnosti
  - Auditor kybernetické bezpečnosti
  - Garant aktiva
  - Administrátor
  - Uživatel
  - Dodavatel



- › Manažer kybernetické bezpečnosti potřebuje
  - Znalost ZKB
    - 1denní kurz „**Zákon o kybernetické bezpečnosti**“
    - Cíl: Seznámení s požadavky zákona č. 181/2014 Sb., včetně vyhlášek
  
  - Odbornou znalost postupů při řízení informační bezpečnosti
    - 2denní kurz „**Manažer kybernetické bezpečnosti**“
    - Cíl: Seznámení s podstatou bezpečnostních opatření a efektivními přístupy k jejich zajištění

- › Architekt kybernetické bezpečnosti potřebuje
  - Znalost ZKB
    - 1denní kurz „**Zákon o kybernetické bezpečnosti**“
    - Cíl: Seznámení s požadavky zákona č. 181/2014 Sb., včetně vyhlášek
  - Odbornou znalost postupů při řízení informační bezpečnosti
    - 2denní kurz „**Manažer kybernetické bezpečnosti**“
    - Cíl: Seznámení s podstatou bezpečnostních opatření a efektivními přístupy k jejich zajištění
  - Obrovské množství technických znalostí
    - 5denní kurz „**Architekt kybernetické bezpečnosti**“
    - Cíl: Seznámení s bezpečnostními oblastmi technických opatření a efektivními přístupy k jejich zajištění

- › Auditor kybernetické bezpečnosti potřebuje
  - Znalost ZKB
    - 1denní kurz „**Zákon o kybernetické bezpečnosti**“
    - Cíl: Seznámení s požadavky zákona č. 181/2014 Sb., včetně vyhlášek
  
  - Auditorský certifikát
    - 5denní kurz „**Auditor kybernetické bezpečnosti**“ s testem
    - Cíl: Připravit účastníky na efektivní provádění auditů kybernetické bezpečnosti na úrovni certifikačních auditorů pro normu ISO/IEC 27001:2013

# Vzdělání

- › Garant aktiva potřebuje:
  - Znalost ZKB
    - 1denní kurz „**Zákon o kybernetické bezpečnosti**“
    - Cíl: Seznámení s požadavky zákona č. 181/2014 Sb., včetně vyhlášek
  
  - Znalost svěřeného aktiva
    - Běžný technický kurz u důvěryhodných lektorů

# Vzdělání

- › Administrátor potřebuje:
  - Znalost svěřeného technického aktiva
    - Běžné technické kurzy u důvěryhodných lektorů

# Vzdělání

- › Uživatel potřebuje:
  - Obecné bezpečnostní povědomí
    - 60 min. eLearning kurz s testem

# Vzdělání

- › Dodavatel potřebuje:
  - Seznámení s řízením informační bezpečnosti správce KII/VIS, aby nenarušoval informační bezpečnost
    - Předávání informací na míru podle požadavků správce KII/VIS

# Certifikace

- › NBÚ nestanovil certifikační program
- › NBÚ spoléhá na správce KII/VIS
  - Riziko slabých rolí
  - Nekontrolovaná úroveň vzdělání lidských zdrojů v oblasti informační bezpečnosti



# Úroveň vzdělání

- › Bezpečnostní incidenty z poslední doby (např. „Česká pošta“ malware) v celé řadě organizací prověřily stav bezpečnostního povědomí – bohužel ostrým testem.

# Úroveň vzdělání

- › Správce KII/VIS
  - Je podle ZKB odpovědný, že nebude docházet ke KBI
  - Je podle ZKB odpovědný za vzdělání zaměstnanců

# Děkuji za pozornost

Michal Zedníček  
[michal.zednicek@alef.com](mailto:michal.zednicek@alef.com)