Organizační dopady při řešení kybenetické bezpečnosti

Ing. Zdeněk Seeman, CISA, CISM

Mgr. Tomáš Rydvan

Organizační dopady při řešení kybernetické bezpečnosti

Ing. Zdeněk Seeman, CISA, CISM

Mgr. Tomáš Rydvan

Účel příspěvku

- Podrobnější pohled na
  - organizační bezpečnost
    - obsazení rolí v oblasti kybernetické bezpečnosti
    - logiku jejich fungování
  - Způsoby zajištění obsazení rolí
    - Interní
    - Externí

Co je ZKB „na jednom slidu“

- Impelementovat technická opatření
- Imeplementovat organizační opetření
  - Mimo jiné stanovit role a odpovědnosti
- Ustavit procesy ..... reakce na kybernetické události a incidenty

Bezpečnostní opatření v ZKB

- Technická opatření
  - 12x subkategorie
- Organizační opatření
  - 13x subkategorie

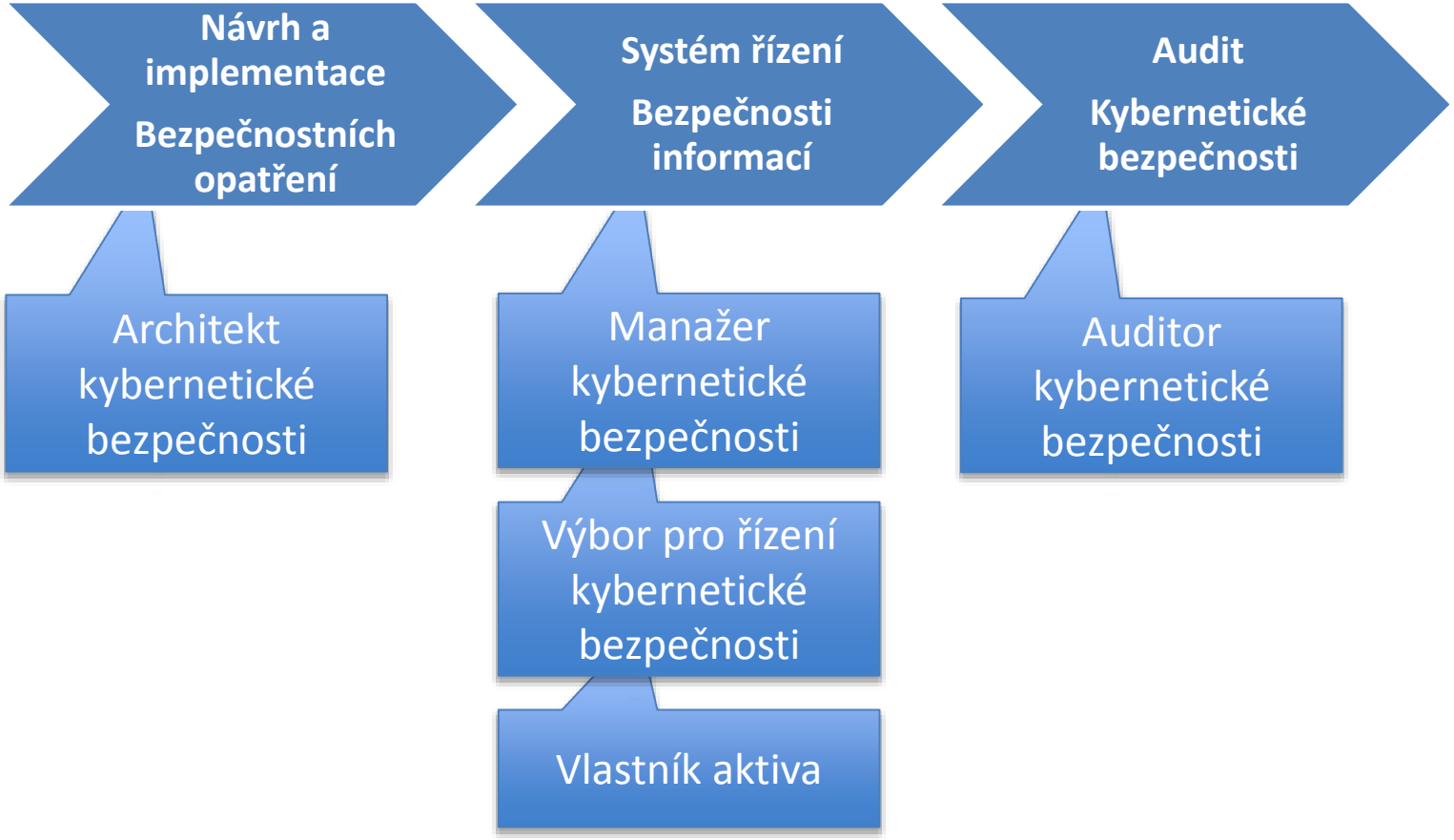
- Organizační bezpečnost (§6 VKB)
  - Ustavení rolí a orgánů
  - Definuje oddělení rolí
  - Definuje povinné činnosti

- Bezpečnostní dokumentace (§28 VKB)
  - Bezpečnostní politika
  - Vnitřní závazné předpisy
  - Záznamy o řízení bezpečnosti

Organizační bezpečnost

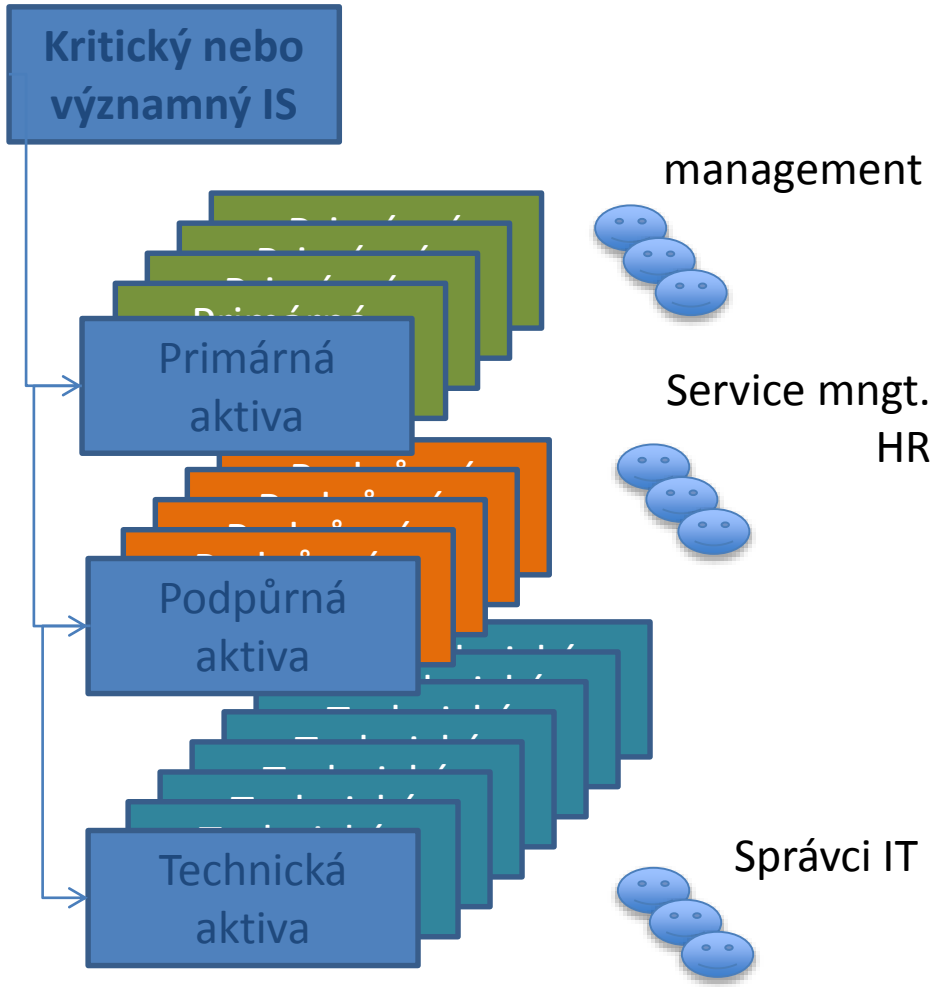
- Bezpečnostní role (a orgán) ustavené vyhláškou (§6)
- Ostatní „bezpečnostně relevantní“ role

Role ZKB v e fázích životního cyklu IS



Odbočka č. 1 – Aktiva vlastníci aktiv

- Dle § 8 řízení aktiv
  - Identifikuje aktiva
    - Primární a podpůrná
  - Určí garanty aktiv
  - Doporučení: Udržujte spodní desítky



Role vlastník aktiva

- Definice dle §2 vyhl. 316/2014
- Aktivum
  - Primární aktiva
    - Typicky koncová služba
  - Podpůrná aktiva
    - Technické aktivum
    - Zaměstnanci
    - dodavatelé
- Zcela interní role
  - Vazba na interní organizační útvary
    - Vedoucí pracovníci
  - Dostatečné rozhodovací pravomoce (rozpočet)
- Rozumná struktura aktiv
  - Jednotky, max. spodní desítky
  - Využití stávajících vazeb mezi IS a útvary
    - Součást stávajících pracovních povinností

Role Manažer kybernetické bezpečnosti

- Definice dle §6 vyhl. 316/2014
- Odpovědnost za „systém řízení“ bezpečnosti informací
  - Lze chápat v kontextu ČSN ISO/IEC 27001 …..ISMS
- Provozní role
  - komunikaci mezi mngmt a výkonnými rolemi
- Řídí: rizika a aktiva, lidské zdroje, provoz a komunikace, řízení přístupu…
- (téměř) interní role
  - důraz na vykonávající osobu
  - min dlouhodobý kontrakt
  - Statut externího zaměstnance
- Úzká vazba na vedení organizace
  - „B-1“ level
- Organizace setkání výboru kybernetické bezpečnosti
- Dostupný pro krizové situace
  - Může mít částečný úvazek
  - Ale musí být rychle dostupný

Role architekt kybernetické bezpečnosti

- Definice dle §6 vyhl. 316/2014
- Odpovědniost za návrh a implementaci
- Projektová role

- Částečně „Projektová“ role, částečně provozní
- Výstavbové projekty lze „sourcovat“ externě
- Interně udržovat koncepci a směrování architektury

Výbor pro řízení kybernetické bezpečnosti

- Definice dle vyhlášky § 6, odst. 7
- Zajišťuje “celkové řízení a rozvoj” a “koordinaci činností”
- Interní řídící orgán - Rozhodovací pravomoci
  - Účast managementu organizace
- Pravidelné setkání
  - Typicky 2 -3 měsíce
  - Organizuje manažer KB
- Mimořádné jednání
  - Výskyt kybernetické události / incidentu

Ostatní role pro kybernetickou bezpečnost

- V rámci provozu jsou ještě další důležité role
  - Správci bezpečnostních technologií
  - Správa bezpečnostních funkcí IS
  - Řízení lidských zdrojů
  - Fyzická ostraha budovy
- Nutné identifikovat a nastavit úrovně služeb (SLA)
  - Specifikovat služby a metriky
  - V případě potřeby aplikovat postupy jak se dostat z "vleku dodavatele"

Bezpečnostní dokumentace

- ZKB ukládá povinnost vést BD
  - Obsah BD stanoven v § 28 VKB
  - Struktura v příloze č. 4 VKB – doporučená
- BD vede správce ISKII, KSKII a VIS
  - Aktualizace BD
  - Záznamy o provedených činnostech v BD musí být úplné a dohledatelné
  - Dokumentace záznamů o provedených činnostech

Nástroje plnění povinností dle ZKB

- Nutné vyhodnocení a identifikace rizik (*due diligence)* ve vztahu k povinnostem dle ZKB
- Vnitřní nástroje zajištění KB:
  - Zavedení vnitřních postupů v oblasti KB
    - » Přijetí vnitřní politiky KB
    - » Systémová opatření
    - » Kritéria výběru kvalifikovaných zaměstnanců
    - » Implementace interních opatření

Nástroje plnění povinností dle ZKB

- Vnitřní nástroje zajištění KB:
  - Nastavení struktury řízení KB – alokace odpovědností
    - » Vnitřní opatření nemohou ukládat individuální povinnosti jednotlivým zaměstnancům
    - » Nutnost vymezení povinností zaměstnanců ve vztahu ke KB v pracovních smlouvách
- Externí nástroje zajištění KB:
  - Outsourcing
    - » vhodné zachovat si kontrolu a řízení rizik KB

Interní nástroje

- Výhody vnitřních nástrojů
  - Kontrola
  - Znalost vnitřních procesů
- Nevýhody vnitřních nástrojů
  - Omezená odpovědnost za škodu
  - Povinnosti zaměstnavatele vzhledem k zaměstnancům

Outsourcing

- Výhody externích nástrojů
  - Smluvní volnost úpravy vztahů
  - Odpovědnost za škodu bez zákonného limitu
- Nevýhody externích nástrojů
  - Veřejné zakázky
  - Kontrola

Děkujeme za pozornost

Ing. Zdeněk Seeman, CISA, CISM

S4S, s.r.o

zdenek.seeman@s4sconsulting.cz

Mgr. Tomáš Rydvan

Řanda Havel Legal advokátní kancelář, s.r.o.

Tomas.rydvan@randalegal.com