Zkušenosti z naplňování ZKB: Audit shody se ZKB

Ing. Martin Konečný,

14. 9. 2016

Národní centrum
kybernetické
bezpečnosti

Obsah

- Přístup NBÚ ke kontrolám ZKB
- Příprava a průběh
- Statistika
- Nejčastější typy zjištění
- Dotazy

KONTROLA SHODY SE ZKB

- **Kontroly dodržování ZKB ≈≈≈ Audit ISMS / *„Audit ZKB“***
- Kontroly zahájeny na zač. r. 2016
- Správci KII a VIS je zasíláno **oznámení o plánované kontrole** (cca 14 - 30 dní před kontrolou do DS)
- Povinným subjektům je poskytnut „**Průvodce auditem**“
- **Program auditu** – posloupnost auditních činností
- **Délka auditu** v kontrolované organizaci:
  - audit VIS trvá cca 2 až 3 dny,
  - audit KII – cca 2 až 8 dní

OBSAH AUDITU ZKB I.

- **Zaměřený** zejm. **na plnění požadavků dle vyhlášky** č. 316/2014 Sb., **o kybernetické bezpečnosti u konkrétních KII a VIS**.

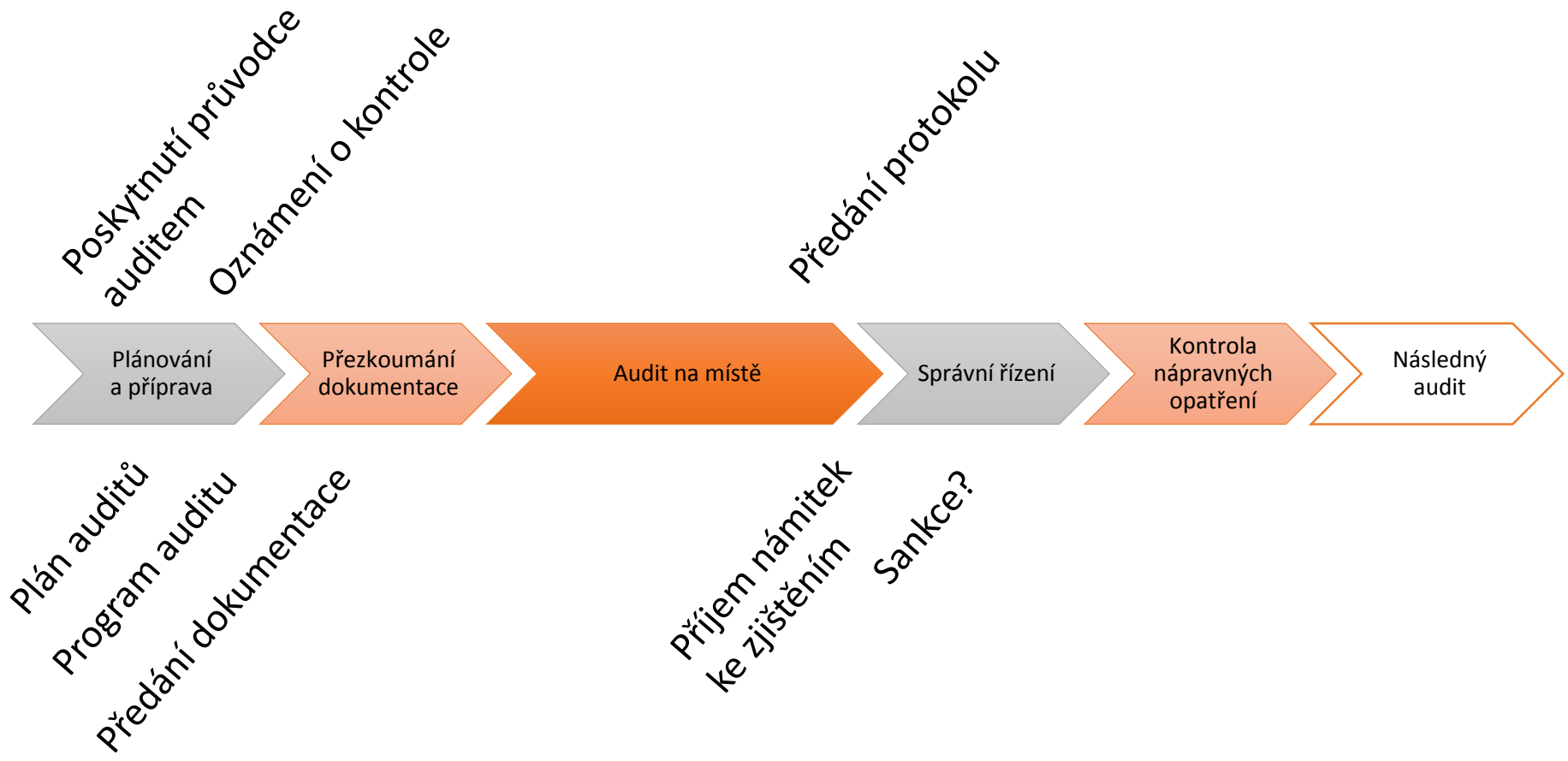
- **Prováděný v souladu s Kontrolním řádem**
  - Zákon č. 255/2012 Sb., o kontrole.

OBSAH AUDITU ZKB II.

Kontrolovaná bezpečnostní opatření

- **Cca 100 - 150 kontrolních bodů z oblastí:**
  - **Organizační opatření**
    Povinná dokumentace, řízení aktiv a rizik, bezpečnost lidských zdrojů, řízení dodavatelů, řízení provozu a komunikací, akvizice/vývoj a údržba, …..
  - **Technická opatření**
    Fyzická bezpečnost, řízení přístupů, ochrana před škodlivým kódem, ochrana a monitoring sítě, aplikační bezpečnost, dostupnost služeb, …..
  - **Zvládání incidentů**
    Detekce kybernetických bezpečnostních událostí a jejich zvládání.

Proces auditu ZKB



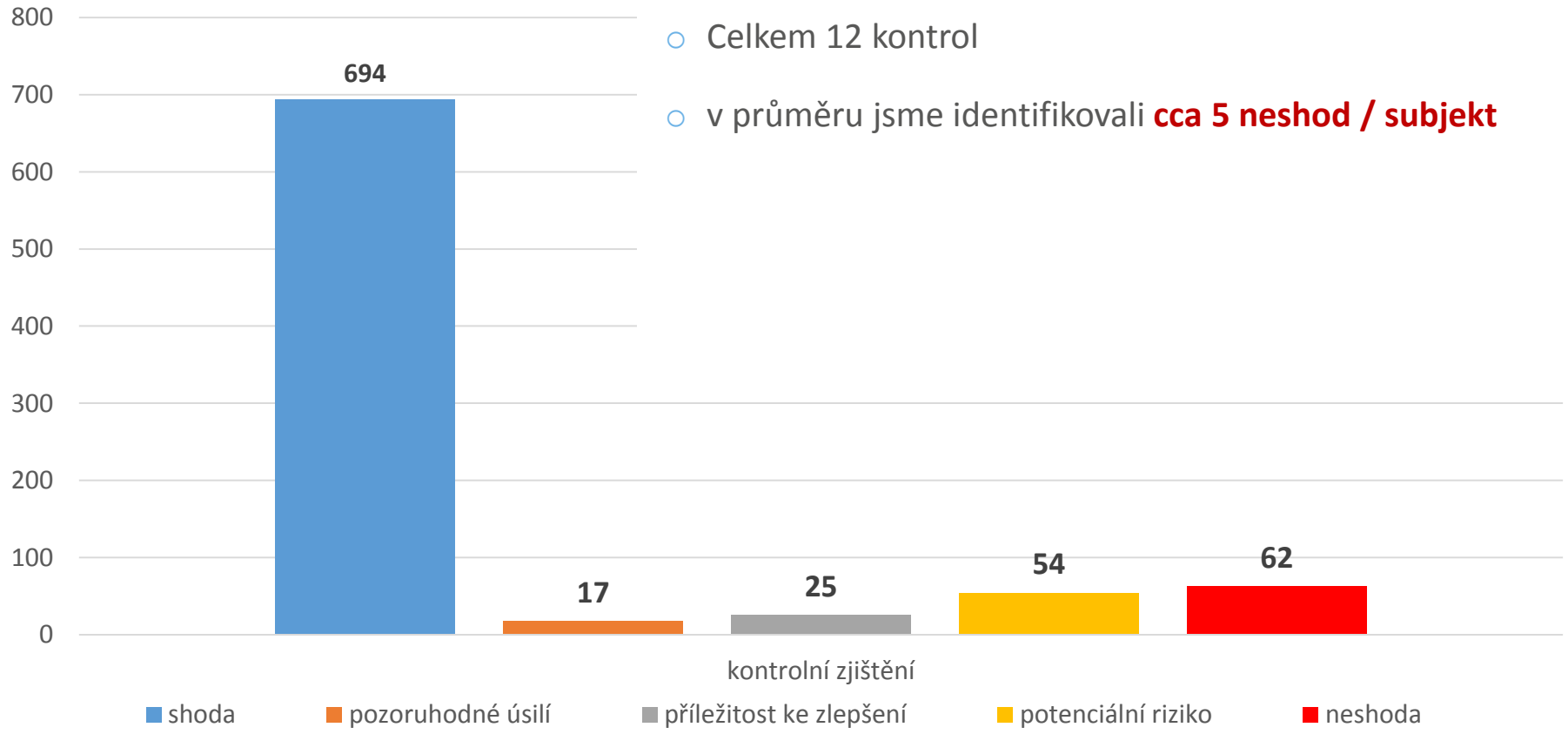
KLASIFIKACE (TYPY) AUDITNÍCH ZJIŠTĚNÍ

- **Neshoda** (důvod k zahájení správního řízení (udělení sankce))
  - Neshodou se rozumí nesplnění požadavku podle stanovených kritérií nebo odchýlení praxe od dokumentovaných postupů.
- **Příležitost ke zlepšení**
  - Příležitost ke zlepšení je typ zjištění, které má charakter doporučení a vychází ze zkušeností kontrolujícího.
- **Potenciální riziko**
  - Touto formou kontrolující upozorňuje na možné riziko.
- **Pozoruhodné úsilí**
  - Vyjadřuje ocenění nadstandartní snahy plnění požadavků v dané oblasti.
- **Shoda**

Přidaná hodnota auditu ZKB?

„ZDARMA !“

STATISTIKA – Audity ZKB v r. 2016 (únor – září)



- Celkem 12 kontrol
- v průměru jsme identifikovali **cca 5 neshod / subjekt**

NEJČASTĚJŠÍ AUDITNÍ ZJIŠTĚNÍ I.

- **Nedostatečná podpora vedení**
- **Předložená dokumentace** není platná / řízená / úplná
- **Nedodržování interně** stanovených postupů (např. pro klasifikaci aktiv a manipulaci s aktivy)
- **Nedostatky formálního charakteru**

NEJČASTĚJŠÍ AUDITNÍ ZJIŠTĚNÍ II.

- Nedostatečné **řízení aktiv a rizik**
  - Klasifikace aktiv
  - AR často jen záležitostí IT
  - AR vytvořená externí organizací za účelem shody se ZKB
- **SoA**
  - neexistence
- **RTP**
  - Často nerespektuje výsledky AR nebo vůbec neexistuje

NEJČASTĚJŠÍ AUDITNÍ ZJIŠTĚNÍ III.

- Přístup všechno outsourcovat
  - Obrovská závislost na dodavatelích (neřízená)
- Řízení kontinuity činností
  - DRP a jejich testování

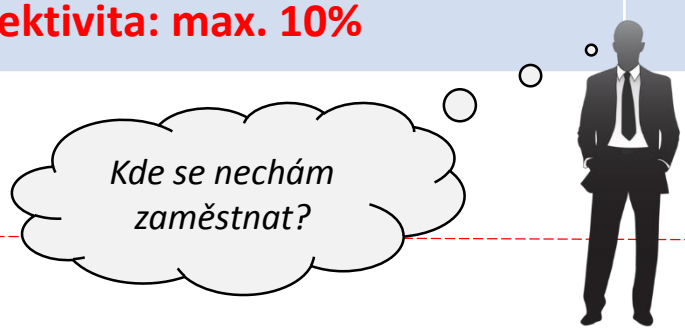
NEJČASTĚJŠÍ AUDITNÍ ZJIŠTĚNÍ IV. – BCM, outsourcing, …

	SW KII	DC	Správa sítě	Servery a OS	Správa virtualizace	Správa dat	Internet	Konzultační služby	Koordinace
Správce KII									?
Dodavatel A	X								
Dodavatel B		X							
Dodavatel C			X						
Dodavatel D	X			X		X			
Dodavatel E					X				
Dodavatel F							X		
Konzultant (1 … N)								X	?

NEJČASTĚJŠÍ AUDITNÍ ZJIŠTĚNÍ V.

Když 2 správci KII dělají totéž, není to totéž, aneb poznej správný přístup:

Organizace A (státní správa)	Organizace B (státní správa)
• Roli manažera KB zastává externí konzultant (firma A) • Bezpečnostní politiky definuje externí organizace na zakázku (firma B) • Analýzu rizik provádí externí organizace (firma C)	• Roli manažera KB zastává vlastní zaměstnanec • Manažer KB definuje bezpečnostní politiky • Manažer KB koordinuje oblast řízení KB • Manažer KB se stará o bezpečnostní povědomí • …
Náklady / rok: min. 1 500 000 Kč	**Náklady / rok: do 500 000 Kč („tabulková“ mzda)**
Efektivita: max. 10%	**Efektivita: 95%**



Děkuji za pozornost

Národní centrum kybernetické bezpečnosti