

Kontrola plnění zákona o kybernetické bezpečnosti
(průběh a zkušenosti z kontrol, častá zjištění a problémy)
s využitím podkladů © NÚKIB Pavla Jelečková

Aleš Špidla
Manažer kybernetické bezpečnosti
Generální finanční ředitelství
Prezident ČIMIB

Průběh kontroly plnění ZKB

- Kontrolované subjekty: správci a provozovatelé KII, PZS a VIS
- Předmět kontroly: systémy PZS, KII a VIS
- § 30, 31 ZKB „orgány a osoby uvedené v § 3 ZKB c), d) a e) zavedou **bezpečnostní opatření podle § 4 ZKB odst. 2 nejpozději do 1 roku ode dne určení/naplnění určujících kritérií...**“
- Kritéria kontroly: ZKB a prováděcí vyhláška
- Obsah kontroly: cca 100 – 150 kontrolních bodů
- Organizační opatření
- Technická opatření
- Zvládání incidentů

Průběh kontroly plnění ZKB

- **Průběh kontroly plnění ZKB**

- Plánování
 - Přezkum dokumentace
 - Kontrola na místě
 - Příprava protokolu
 - Předání protokolu
-

- Správní řízení
- Nápravná opatření
- Následná kontrola

Průběh kontroly plnění ZKB

■ Plánování

- Navázání kontaktu s kontrolovaným subjektem (neoficiální/oficiální)
- **Oznámení o plánované kontrole**
- Příprava podkladů, harmonogramu kontroly
- Sestavení kontrolního týmu

■ Přezkum dokumentace

- Přezkum dodané dokumentace
- Analýza informací
- Příprava pokladů k interview
- Příprava harmonogramu kontroly v kooperaci s kontrolovaným subjektem

Průběh kontroly plnění ZKB

- **Kontrola na místě**
 - 3 až 5 dnů
 - Zahájení kontroly na místě
 - **Vzorkování**
 - Interview s respondenty, pozorování, testování, přezkum dokumentů
- **Příprava protokolu**
 - Ověřování tvrzení
 - Přezkum další dokumentace
 - Finální formulace zjištění a jejich klasifikace
- **Předání protokolu**
 - Předání protokolu o kontrole
 - Vysvětlení podstaty zjištění, možnost prezentace manažerského shrnutí pro top management
- **Začíná běžet lhůta zpravidla 15 dnů pro podání námitek**

Průběh kontroly plnění ZKB

Klasifikace kontrolních zjištění

- Neshoda - Nesplnění požadavku podle stanovených kritérií kontroly nebo odchýlení praxe od dokumentovaných postupů v organizaci.
- Potenciální riziko - Upozornění na možné riziko.
- Příležitost ke zlepšení - Doporučení vycházející ze zkušeností kontrolního týmu.
- Pozoruhodné úsilí - Nadstandardní hodnocení dané oblasti.
- Shoda - Splnění požadavků podle stanovených kritérií kontroly.

Průběh kontroly plnění ZKB

- **Správní řízení**
 - V případě zjištění klasifikovaného jako neshoda
 - Předání podkladů na právní odbor NÚKIB
- **Nápravná opatření**
 - Kontrolovaný subjekt informuje o plnění nápravných opatření vedoucího kontrolního týmu u kontrolních zjištění klasifikovaných jako neshoda
- **Následná kontrola**
 - Kontrola zavedení nápravných opatření

Statistika

- **Počet provedených kontrol a metodických podpor**
 - 24 x kontrola
 - 36 x metodická podpora
- **Počet kontrolovaných systémů v rámci 24 kontrol**
 - 17 VIS
 - 26 KII

Častá zjištění a problémy

- **Nedostatečná podpora vedení** organizace v oblasti kybernetické bezpečnosti. Kybernetická bezpečnost je mnohdy vnímání jako zbytečnost
- **Nízké bezpečnostní povědomí** o kybernetické bezpečnosti napříč organizací
 - Neprobíhají školení BOZP/KB
- **Nevhodné organizační zařazení** kybernetické bezpečnosti v organizaci. Neoddělená bezpečnost od provozu
- **Nedostatečné personální obsazení** v oblasti kybernetické bezpečnosti. Neobsazené bezpečnostní role, jejich nezastupitelnost. Poddimenzovanost útvarů odpovědných za kybernetickou bezpečnost
- **Nákup technologie z důvodu požadavku ve vyhlášce** Např. nákup SIEM, ale dále s ním nikdo nepracuje

Častá zjištění a problémy

- **Bezpečnostní dokumentace**
 - Nereflektuje požadavky konkrétní organizace
 - Není platná, řízená, úplná, neaktuální
 - Zdlouhavé procesy schvalování dokumentace
- **Nedodržování interně stanovených postupů** – např.
 - Klasifikace aktiv, manipulace dle klasifikace atp.
 - Reálné nastavení politiky hesel je v rozporu se schválenou politikou organizace
- **Privilegované účty pro vrcholové vedení**
 - Vrcholové vedení disponuje mnohdy bezdůvodně privilegovanými účty
 - Instalace škodlivého software

Častá zjištění a problémy

- **Nesystematický přístup k řízení aktiv a rizik v oblasti kybernetické bezpečnosti**
 - Analýza rizik je často záležitostí jen IT
 - Mnohdy je vytvořená pouze za účelem shody se ZKB
 - Neschválené metodiky
- **Prohlášení o aplikovatelnosti (SoA), Plán zvládnání rizik (RTP)**
 - Neexistence
 - Nepochopení účelu dokumentu
 - Nereflektuje výsledky provedené analýzy rizik
 - Neaktuálnost
- **Neřízený outsourcing, neřízení dodavatelů**
 - Snaha vše outsourcovat, protože je to „jednodušší, levnější, ...“
 - Obrovská neřízená závislost na dodavatelích
 - Nedostatečná kvalita uzavíraných smluv – kdo je za co zodpovědný
 - Neprobíhá kontrola dodržování stanovených pravidel, směrnic a politik

Častá zjištění a problémy

■ **Kontinuita činností**

- Nejsou definovány důležité procesy, činnosti organizace a cíle kontinuity činností pro případ neočekávané události
- Neexistence strategie kontinuity činností a havarijních plánů
- „Testujeme až naostro“
- Do testů nejsou zapojeny všechny významné zainteresované strany - vedení s dostatečnou rozhodovací pravomocí, dodavatel, atp.)

Děkuji za pozornost.

**Ing. Aleš Špidla
Manažer kybernetické bezpečnosti
Prezident ČIMIB**