Implementace ZKB

Ing. Miroslav Jaroš

Energetický regulační úřad

Miroslav.Jaros@eru.cz

Bezpečnost informací v ERÚ

- *ERÚ je správcem IS s názvem Jednotný informační systém ERÚ („JIS“)*
- *Bezpečnost informací JIS je řízena v souladu s normou ISO/IEC 27001:2013*
  - *To znamená, že bezpečnost informací je citlivě vnímána na VŠECH úrovních organizace*
  - *To znamená, že TOP management ERÚ převzal vůdčí roli závazek plnění povinností normy*
  - *To znamená, že ŘÍDÍME rizika*
  - *To znamená, že řídíme zdroje a přidělujeme potřebné KOMPETENCE jednotlivým rolím*
  - *To znamená, že školíme personál na UŽIVATELSKOU BEZPEČNOST*
  - *To znamená že jsme zavedli a UDRŽUJEME bezpečnostní dokumentaci*
  - *To znamená, že všechny aktivity v ICT prostředí pečlivě PLÁNUJEME*
  - *To znamená, že ICT prostředí MĚŘÍME podle předem daných kritérií a provádíme audity*
  - *To doufáme znamená, že se neustále ZLEPŠUJEME*

ZKB a ERÚ

- *JIS byl určen vyhláškou 317/2014 Sb. jako „Významný Informační Systém - VIS“*
- *Od 1. ledna 2015 běží překlenovací lhůta*
  - *Do 30 dnů od tohoto data jsme odevzdali kontaktní údaje na NBÚ*
  - *Ve 12 měsících od tohoto data je naším cílem připravit JIS do souladu se zákonem*

ZKB a ERÚ

Energetický regulační úřad

- *Určili jsme si milníky naší přípravy implementace ZKB*
  - *GAP analýza – posouzení stavu stávajícího prostředí JIS proti požadavkům ZKB*
    - *Bezpečnostní audit stavu*
    - *Návrh nápravných opatření*
  - *Implementace nápravných opatření dle GAP analýzy*
  - *Vnitřní audit ZKB*

ZKB, ERÚ a aktuální stav

- *Máme zpracovanou GAP Analýzu*
- *Máme připravené projekty na implementaci kritických nápravných opatření*

Energetický regulační úřad

Gap analýza

Michal Zedníček

Vedoucí auditního týmu, externí organizace

Michal.Zednicek@alef.com

GAP analýza

- *Definice cílů Gap analýzy*
- *Určení rozsahu etalonu*
- *Určení metodiky*
- *Určení výstupů*

GAP analýza - Cíle

- *Formální – soulad se zákonem (rozsah VIS)*
- *Věcný – odolné prostředí (rozsah KII)*
- *Praktický – najít rozumnou rovnováhu mezi ISMS podle ZKB a ISO/IEC 27001:2013*

GAP analýza - Etalon

- *VIS řízení je do budoucna neudržitelné*
  - *Chybí hodnocení podpůrných aktiv a jejich rizik*
  - *Přezkoumání1x za 3 roky není použitelné v praxi*
  - *Ad…*
- *ERÚ chce pokračovat v certifikaci ISO/IEC 27001:2013, ISMS VIS a ISMS ISO27000 se rozchází*

- *Bude sledován etalon KII i VIS pro sjednocení s ISMS dle ISO/IEC 27001:2013*

GAP analýza - Metodika

- *Podrobný audit – je potřeba mít celý obraz.*
- *Podklad auditu – metodika dodavatele GAP analýzy, definice cca 450 oblastí, základem vyhláška 316/2014 Sb. („§“ VoKB)*
- *Silné auditorské (ISO27000) a technické know-how*
- *Potřebné role v týmu:*
  - *Projektový manager se znalostí ZKB a ISO/IEC 27001:2013*
  - *Auditor ISO/IEC 27001:2013.*
  - *Specialisté na síťovou bezpečnost*
  - *Specialisté na aplikační bezpečnost*
- *Délka trvání auditu cca 2 měsíce*
- *Audit opřen o princip EN ISO 19011:2011*

GAP analýza - Výstupy

- *Podrobná analýza všech oblastí*
  - *Interview*
  - *Ověření*

GAP analýza - Výstupy

- *Hlavní organizační nápravná opatření*
  - *Sjednocení přístupu k hodnocení aktiv podle ZKB (nyní ISO/IEC 27001:2013).*
  - *Úprava analýzy rizik – aktualizace Plánu zvládání rizik.*
  - *Přesnější definice kompetencí v organizační struktuře.*
  - *Nastavení standardů pro externí dodavatele.*

GAP analýza - Výstupy

- *Hlavní technická nápravná opatření*
  - *Úprava nastavení autentizačních mechanismů*
  - *Změna ochrany integrity sítě (změna segmentace sítě)*
  - *Zvýšení úrovně zabezpečení proti škodlivému kódu*
  - *Optimalizace sběru událostí a aktivní vyhodnocování KBU/KBI*
  - *Změna kryptografických prostředků*
  - *Zavedení testování zranitelností aplikací*
  - *Aktualizace operačních systémů bezpečnostních nástrojů a ICT prostředků obecně*

GAP analýza - Výstupy

- *Dokumentace*
  - *Změna formátu bezpečnostní dokumentace pro praktické využití a nastavení procesu řízení změn.*
- *KBI*
  - *Změna kategorizace KBI*
  - *Nastavení procesu zvládání KBI*

GAP analýza - Shrnutí

Energetický regulační úřad

- *ERÚ si je vědom potřeb řízení bezpečnosti informací.*
- *ISMS je zavedený a funkční ve smyslu ISO/IEC 27001:2013.*
- *ISMS plně neodpovídá ZKB.*
- *ERÚ naplánoval další kroky k souladu se ZKB a obecnému zvýšení úrovně bezpečnosti informací.*

Energetický regulační úřad

Děkuji za pozornost.