Procesy kybernetické bezpečnosti

Ondřej Steiner, S.ICZ a.s.

14. 4. 2015

Agendy

- Zákon o KB
- Systém řízení bezpečnosti informací
- Implementace ukončená
- Po uplynutí krátké doby
- Po uplynutí delší doby
- Průběžné činnosti
- Procesy řízení KB

Zákon o KB

- **Roky 2014 a 2015 „roky kybernetické bezpečnosti“**
  - Zákon č. 181/2014 Sb. o kybernetické bezpečnosti
  - Vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti
- **Uvedená legislativa požaduje implementovat**
  - Technická opatření - FW, čipové karty, OTP, šifrování, IDS, IPS, sběr logů, SIEM, load-balancery, ...
  - Organizační opatření – bezpečnost lidských zdrojů, řízení přístupu, incident, change a release management, …
  - Organizační opatření – **Systém řízení bezpečnosti informací**

Systém řízení bezpečnosti informací

- **Minimální rozsah vyhláška**
  - Vyhláška č. 316/2014 Sb., § 3 odst. (1)

Úvodní kroky (např. pomocí subdodavatele)

- **Stanovení hranic systému řízení**
- **Provedení analýzy rizik, výběr způsobu zvládání rizika vč. návrhu opatření**
- **Vytvoření a schválení bezpečnostních politik**
  - Politika řízení bezp. informací
  - Ostatní „standardizační" politiky

Implementace ukončená

- **Pozn: Dále předpokládáme KII, na VIS se uplatní v přiměřené míře**

- **Implementace ukončena**
  - Syst. řízení implementován
  - Politiky schváleny a vydány
  - Opatření implementována (nebo probíhá implementace)
  - … dodavatel odchází

Po uplynutí krátké doby

- **Po uplynutí krátké doby (např. po měsíci)**

- **Správce IS … monitoruje účinnost bezpečnostních opatření**
  - Definování metrik (inspirace ISO/IEC 27004)
  - Měření základních hodnot (base measures) a výpočet odvozených hodnot (derived measures)
  - Analýza těchto hodnot, porovnání s indikátory, tvorba výsledků měření

Po uplynutí delší doby - I.

- **Po uplynutí delší doby (max. 1 rok)**

- **Správce IS … zajistí provedení auditu kybernetické bezpečnosti**
  - Audit procesů ISMS, pokrytí a efektivita (intervaly revize, rozsah revize, AR, ...)
  - Audit jednotlivých technických a organizačních opatření (včetně monitoringu)
  - Pravidla a procesy auditu, výběr nezávislého auditora (interní/externí), případné proškolení, tvorba checklistů, provedení auditu a vytvoření zprávy z auditu obsahující "nálezy" a "doporučení"

Po uplynutí delší doby - II.

- **Správce IS … vyhodnocuje vhodnost a účinnost bezpečnostní politiky**
  - Na základě výsledků monitoringu, specifických kontrol, auditu, penetračních testů, aktualizované analýzy rizik, zjištěných příčin kybernetických bezpečnostních incidentů, atd.

- **Správce IS … zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací**
  - Aktualizace AR vč. zvládání rizik
  - Posouzení výsledků monitoringu, kontrol, auditu, …

Po uplynutí delší doby - III.

- **Správce IS … aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci**
  - Na základě vyhodnocení účinnosti politiky a systému řízení
  - Na základě připravovaných změn (např. změna org. struktury)

Průběžné činnosti

- **Správce IS … řídí provoz a zdroje …, zaznamenává činnosti …**
  - Standardní management - operativní řízení
  - Záznam jednotlivých akcí pro prokazování při následném auditu

Procesy řízení KB

- **Pro výše uvedené činnosti**
  - Monitorování bezp. opatření
  - Audit opatření a systému řízení
  - Vyhodnocení vhodnosti a účinnosti bezp. politiky a systému řízení
  - Aktualizace systému řízení a další dokumentace
- **nezapomenout zavést procesy, které budou**
  - mít definované vstupy
  - mít definované výstupy
  - využívat zdroje
  - mít vlastníka

Děkuji za vaši pozornost

Ondřej Steiner
ondrej.steiner@i.cz
+420 224 271 260

ICZ a.s.
Sekce Bezpečnost
www.i.cz