

Tvorba bezpečnostních politik v oblasti informační bezpečnosti

11.5.2010

Ing. Pavel Růžička



Bezpečnostní politiky:

- Základní dokumentace popisující strategii zabezpečení informační bezpečnosti (nejen v oblasti ICT)
- Obsah musí pokrývat veškeré aspekty zabezpečení ochrany organizace v oblasti **informační bezpečnosti**
- Z pohledu standardizace bezpečnostních politik se zpravidla vychází ze standardů ISO (ISO/IEC 27001 a 27002)



Ustanovení ISMS čl.4.2.1 dle ISO/IEC 27001:2005

- Definování rozsahu a hranice ISMS
- **Návrh politiky ISMS (bezpečnostní politiky)**
- Analýza a řízení rizik
- Prohlášení o aplikovatelnosti
- Získání souhlasu vedení společnosti s navrhovanými zbytkovými riziky a povolení k zavedení a provozu ISMS

Následuje implementace v rámci ISMS



Nástroje řízení ve standardu ISO/IEC 27001 v oblasti bezpečnostních politik:

Příloha A, cíle řízení a opatření, část A.5
Bezpečnostní politika

A.5.1.1 Dokument politiky bezpečnosti informací

A.5.1.2 Přezkoumání politiky bezpečnosti informací



Bezpečnostní politiky obvykle obsahují tyto oblasti:

- Vztahy s třetími stranami
- Zajištění bezpečnosti informací v rámci organizace
- Dodržování dokumentovaných postupů
- Zabezpečení práv, řízení přístupu a komunikací
- Vzdálený přístup
- Soulad s požadavky
- Personální procesy
- Fyzická bezpečnost
- Plány kontinuity a plány obnovy



- Dokumentace bezpečnostních politik je jedním z **klíčových prvků systému** bezpečnosti informací a je vyžadován standardem ISO/IEC 27001:2005, Politika ISMS je zpravidla nadřazena bezpečnostní politice (čl. 4.2.1 b))

- Politika ISMS a bezpečnostní politika **musí**:
 - Určit rámec pro stanovení hlavních zásad pro systém řízení bezpečnosti informací
 - Stanovit cíle a postupů pro systém řízení bezpečnosti,
 - Popsat vazby na ostatní již platné dokumenty strategií
 - Popisovat kritéria pro hodnocení rizik

- Dokument politik(y) bezpečnosti informací podléhá **schválení vedením** (v souladu se standardem ISO/IEC 27001:2005), vedení tímto aktem **přijímá vrcholově závazek v oblasti bezpečnosti informací**



- Dokumenty **Politiky ISMS a bezpečnostní politiky** musí odrážet hlavní požadavky organizace na obecnou bezpečnost informací, musí být zahrnut soulad se zákonnými požadavky a soulad ostatními regulatorními normami,
- Obecné povědomí vedení organizace a zaměstnanců o obsahu dokumentů Politiky ISMS a bezpečnostní politiky v konkrétních podmínkách
- Dokumenty politik musí být **pravidelně přezkoumávány**, zpravidla na roční bázi nebo na základě impulsu důležitých změn majících vliv na chod společnosti



2 přístupy tvorby bezpečnostních politik:

- Tvorba pomocí interních zdrojů
 - Hrozba zaujatosti
 - Nekomplexní pohled
 - Nižší náklady

- Využití externích zdrojů
 - Vyšší náklady
 - Objektívni pohled
 - Využití komplexních opakovatelných metodik



Pro optimální postup při tvorbě úplné bezpečnostní politiky je třeba provedení těchto kroků:

- Provedení situačního auditu
 - požadavky ISO 27001, příloha „A“ a nástroje 27002
- Analýza rizik
 - využití opakovatelné metodiky pro analýzu rizik
- Definice bezpečnostních politik organizace dle výsledků
- Realizace a tvorba bezpečnostní dokumentace nižší úrovně – cíle a postupy
- Průběžná realizace osvěty – udržování bezpečnostního povědomí u vedení a u zaměstnanců.



Opravdu kvalitní bezpečnostní politiku lze sestavit pouze na základě kvalitně provedené analýzy rizik a průmět výsledků

- Problematika výběru vhodné metodiky pro analýzu rizik
 - Využití standardních metodik
 - Tvorba metodiky „na míru“



Dotazy

