

Máte data v bezpečí?

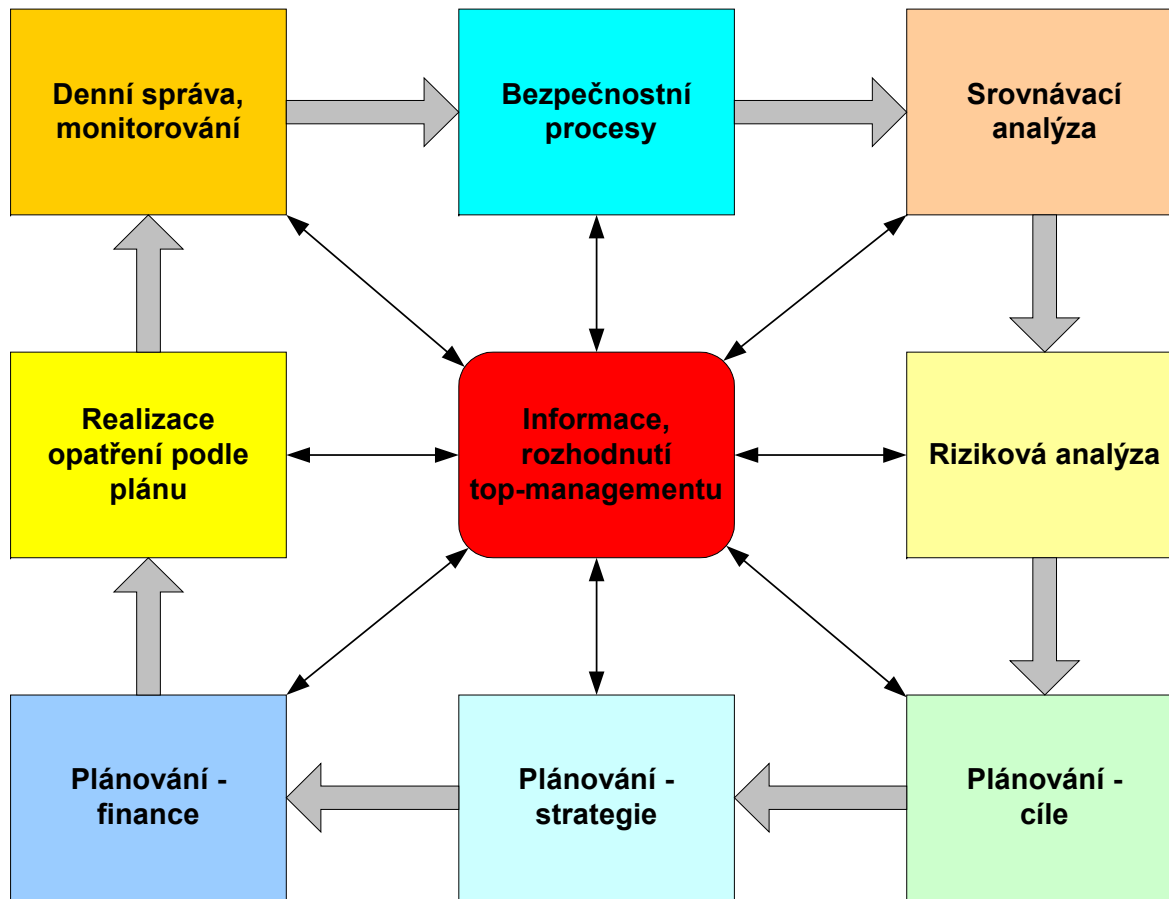
**Jan Brodský, Pavel Sekanina, ANECT a.s.,
Josef Šustr, Corpus Solutions, a.s.**



24. října 2004



Cyklus bezpečnosti



Začít je třeba u top-managementu!

- Ochrana informací by měla být chápána jako součást business aktivit
 - Analyzovat a vyhodnotit stav bezpečnosti
 - Prezentovat zjištěná rizika a potřeby řešení
- Předložit k rozhodnutí jen reálná řešení
 - Prioritně zavést pořádek do aktivit řízení a zajišťování informační bezpečnosti
- Učinit strategická rozhodnutí – bez nich to nepůjde!

Základní procesy, odpovědnost

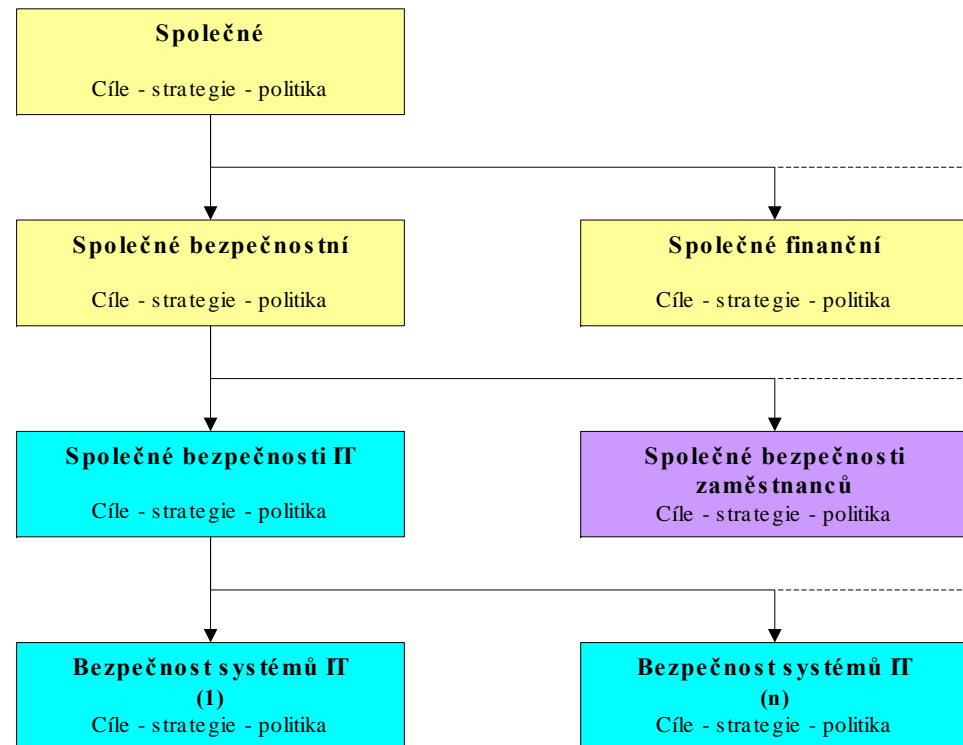
- Osvědčené metodologie
 - ČSN ISO/IEC 17799 a BS7799-2 (ISMS)
 - univerzálně použitelné, www.csni.cz
 - COBIT
 - manažerské přístupy, www.isaca.org
 - ČSN ISO/IEC 21827 (SSE-CMM)
 - výkon správy IT, www.sse-cmm.org
 - ITIL
 - obecné návody pro řízení IT služeb, www.ogc.gov.uk
- Bezpečnostní manažer
 - klíčová úloha bezpečnostního manažera
 - diskutabilní je „rozpuštění“ úkolů BM mezi více rolí
 - vhodná kvalifikace - manažer

Srovnávací a riziková analýza

- Srovnávací analýza
 - Porovnání stavu bezpečnostních procesů s etalonem (např. BSI-DISC)
 - bezpečnostní audit (zpravidla až v dalším kole)
- Riziková analýza
 - Ocenění aktiv, hrozby, rizika
 - Nástroje typu CRAMM
 - Musí následovat návrh protiopatření

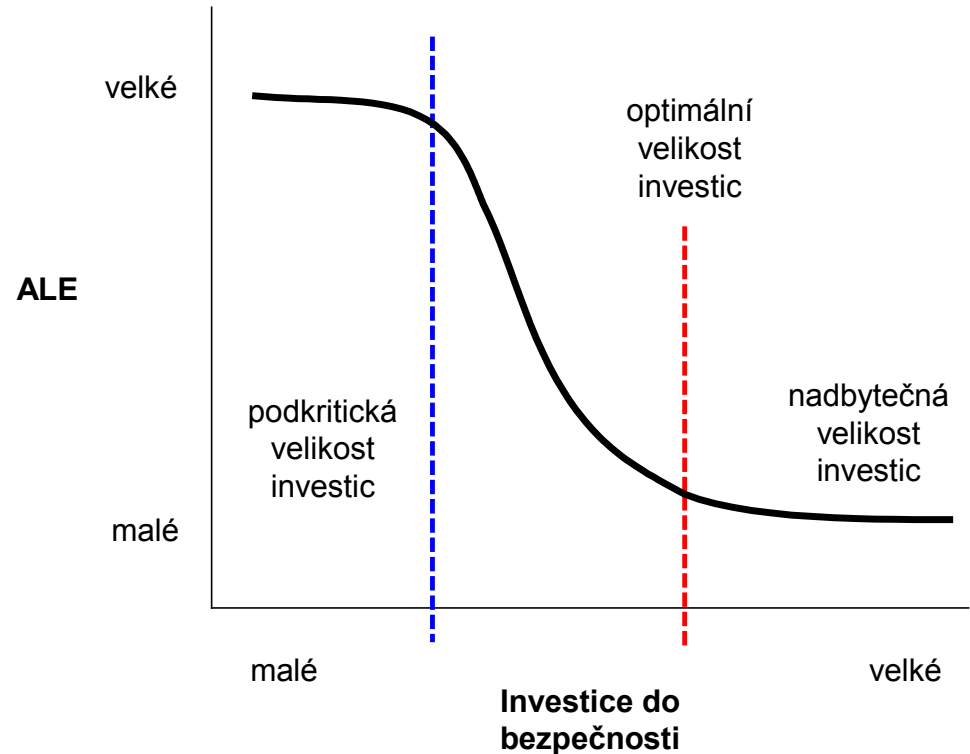
Plánování – cíle, strategie, politiky

- Cíle - **čeho** má být dosaženo (dlouhodobé plánování)
- Strategie - **jak** dosáhnout cílů (střednědobé plánování)
- Politika - **pravidla** pro dosažení cílů (krátkodobé plánování)



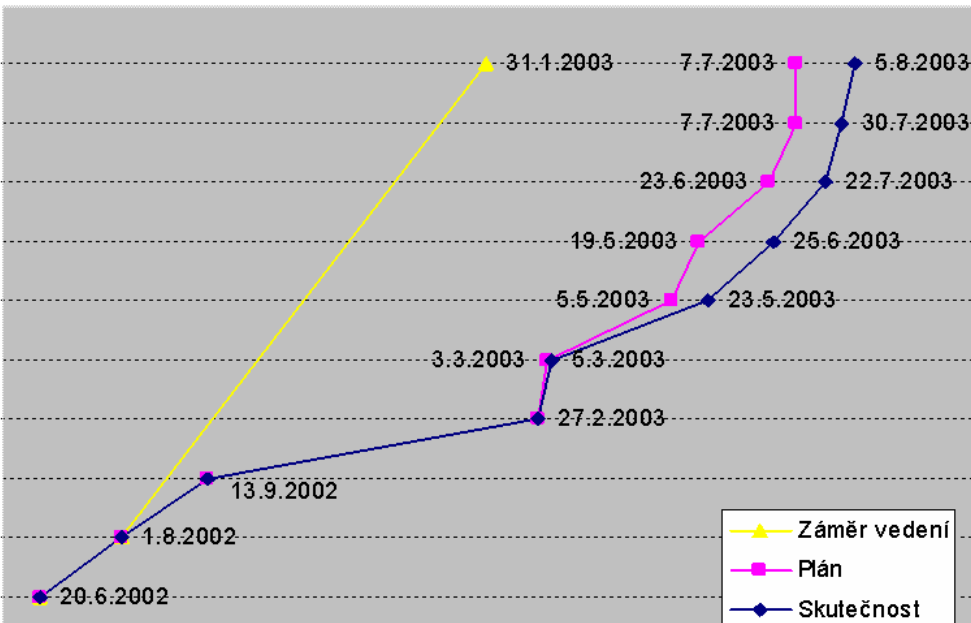
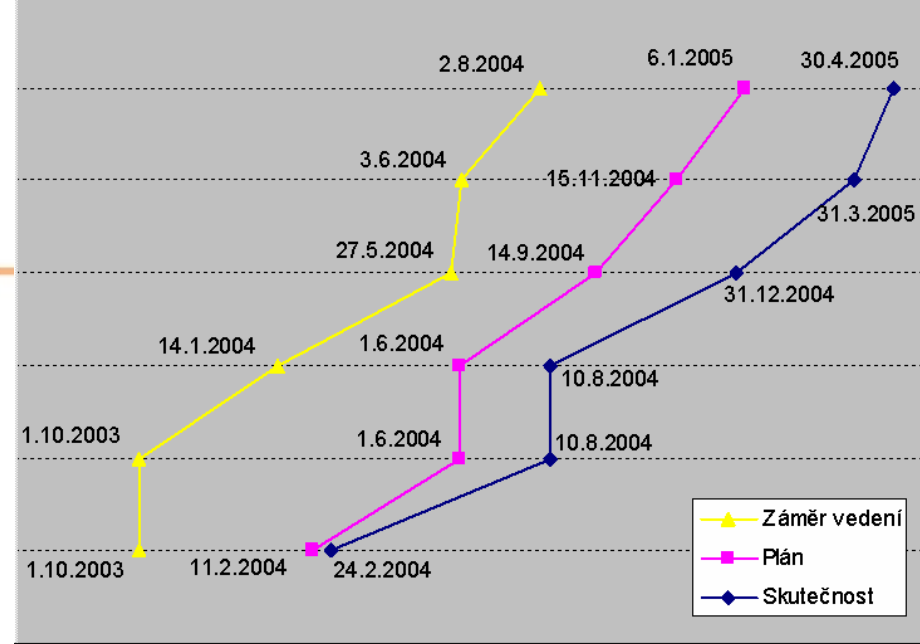
Plánování - finance

- Náklad, investice, pojištění?
- Lineární nárůst nákladů
- Procesní pohled
 - Audity
 - Vyzrálост procesů
- Finanční pohled
 - Přínosy, úspory (ALE)
 - ROI, návratnost
- Správa hodnot (Value management)



Realizace

- Projektové řízení
- Sladění ISMS s ostatními projekty organizace
 - Plány obnovy funkčnosti, OUS, řízení jakosti ISO



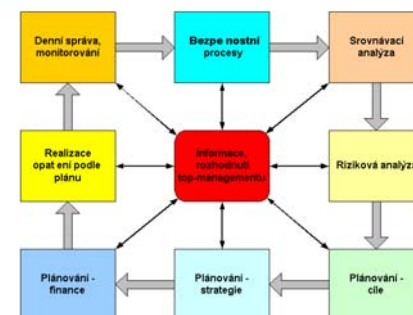
● Pro úspěch je klíčová

- Podpora top managementu
- Důvěra zaměstnanců a jejich pocit, že bezpečnost je neomezuje ani neohrožuje
- Aktivní podíl zaměstnanců na tvorbě a dodržování politiky



Denní správa, monitorování

- Plán údržby a monitorování a auditů
- Osvěty není nikdy dost – zvyšovat povědomí
- Technické monitorování
 - měření specifických parametrů,
 - prohlížení log souborů, ...
 - Incidenty
 - závady jako zranitelnost vůči průnikům, ...
- Procesní monitorování
 - odchylky jako neshody v systému kvality
- Nápravná opatření proti zjištěným závadám a neshodám



Dokonalý systém byl vytvořen již dávno.

Naším cílem je dodat jej k vám.

