

Bezpečnostní monitoring

Jiří Rosenmayer

jiri.rosenmayer@anect.com

23. říjen 2005



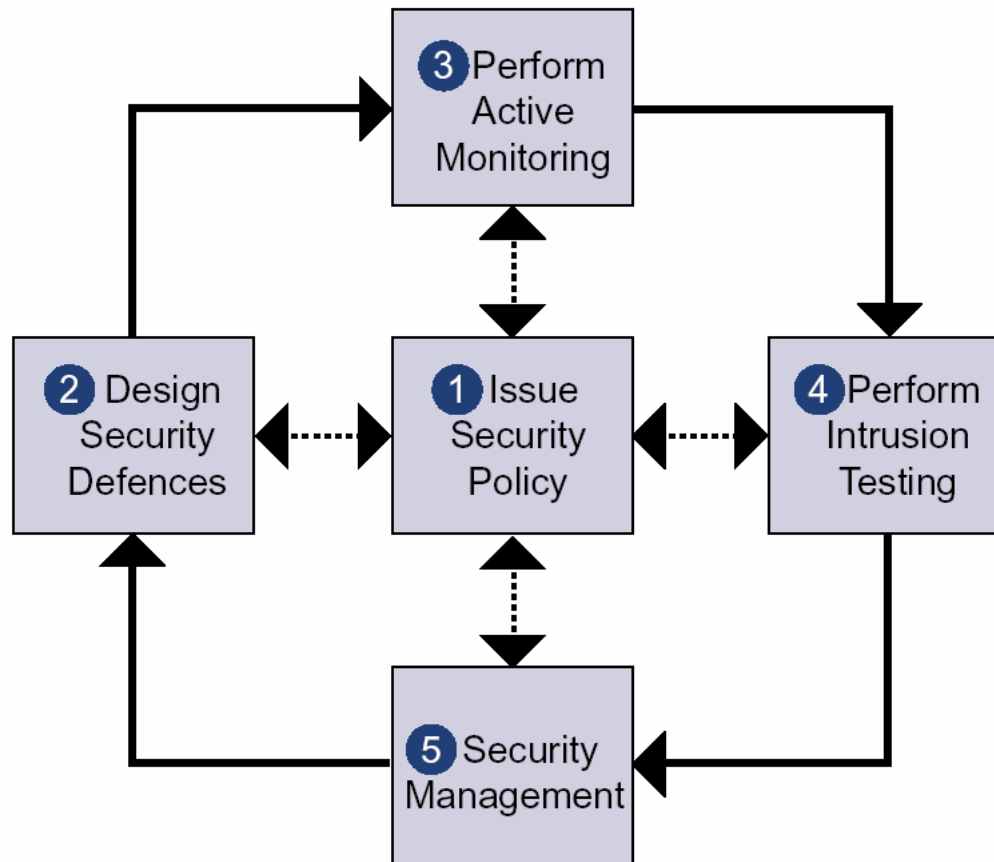
www.anect.com



Obsah prezentace

- Místo a význam bezpečnostního monitoringu
- Technické nástroje monitorování
- Proč nestačí samotné nástroje?
- Komplexní pohled
- Různé podněty pro zlepšování
- Shrnutí

Motivace – bezpečnost



Zdroj: IT Governance – IT Security
Governance - Guidance for Board
Directors and executive management

Motivace – ISO/IEC 17799:2005

- Risk Assessment
- Security Policy
- Organizing Info Security
- Asset Management
- Human resources
- Physical & environment
- Communications & Operations Management
- Access Control
- Info. Systems Acquisitions, Development and Maintenance
- **Security Incident Management**
- Business Continuity Management
- Compliance

Proč bezpečnostní monitoring?

- Žádná prevence není absolutně účinná.
- Nebytné je sledovat stav prostředí a správně reagovat na nestandardní chování.
- Potřeba včas odhalit všechny bezpečnostní slabiny a přiměřeně na zjištění reagovat.
- Získávat objektivní informace o skutečných rizicích a správně s nimi pracovat.

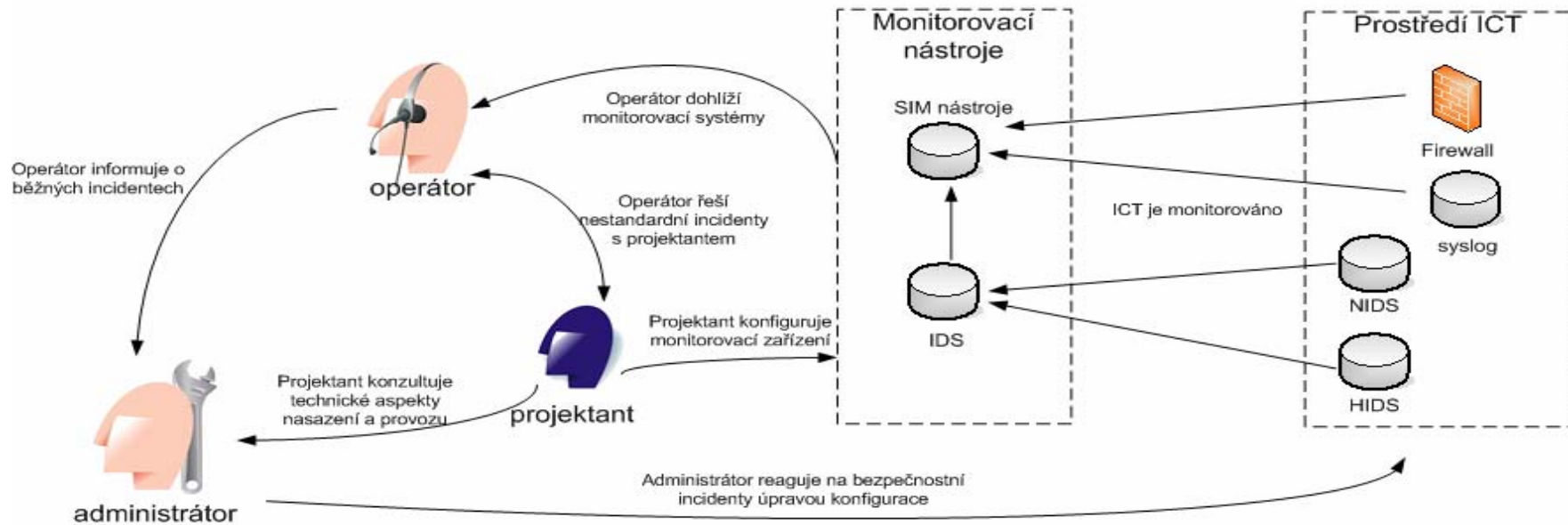
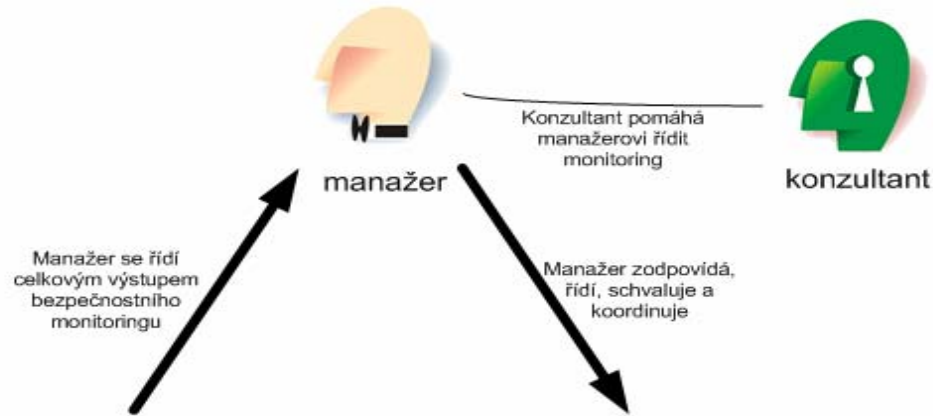
Technické nástroje monitoringu

- Technologie IDS (Intrusion Detection System)
 - odhalení pokusů o průnik do komunikační sítě nebo do informačního systému včetně upozornění na nestandardní stavy prostředí.
- Technologie IPS (Intrusion Prevention System)
 - varianta technologie IPS, u které jsou prohloubeny schopnosti automatického reagování na bezpečnostní incidenty.
- Technologie SIM (Security Information Management)
 - sběr, analýza a vyhodnocení různých typů bezpečnostních událostí (firewall, IDS, antivirové systémy, radius servery, VPN servery, ...).

Proč nástroje nestačí?

- Důležité normy a doporučení
 - ISO/IEC 17799:2005 – Soubor postupů pro management bezpečnosti informací,
 - ISO/IEC TR 18044:2004 – Management incidentů bezpečnosti informací,
 - NIST SP 800-61 – Směrnice pro správu incidentů,
 - ITIL (IT Infrastructure Library) Service Support.
- Potřeba definovat procesy a pravidla jejich realizace.
- Potřeba integrovat procesy do prostředí organizace a jejího ICT.

Monitoring bezpečnosti



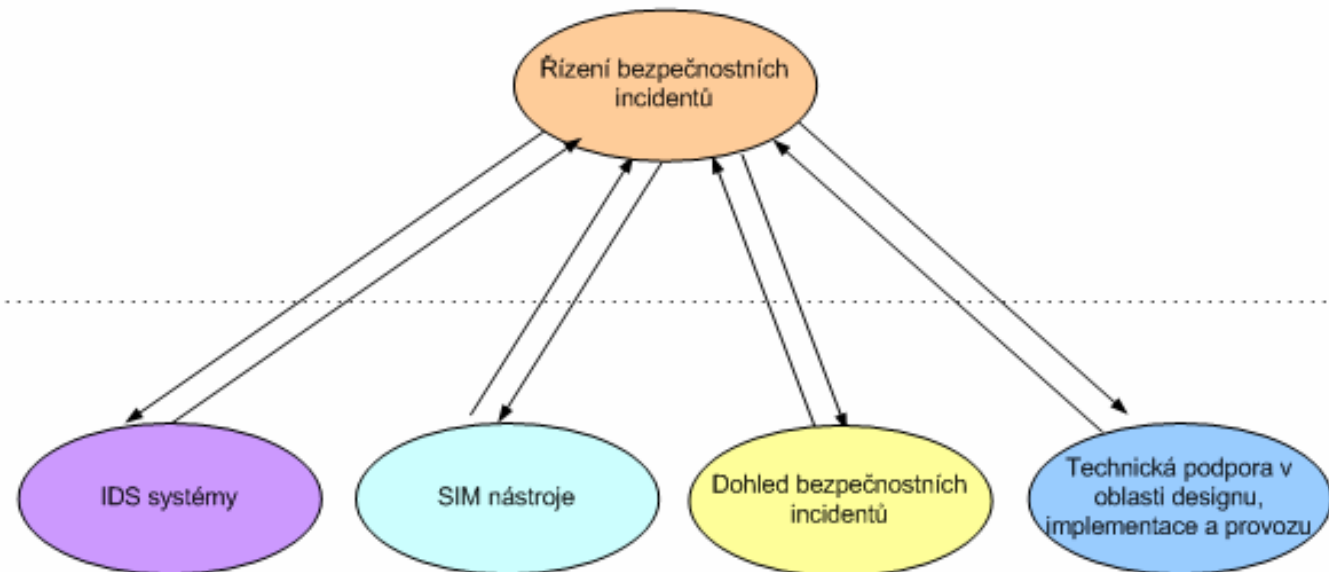
Monitoring bezpečnosti

Monitoring bezpečnosti

Celkové řízení monitoringu bezpečnosti na úrovni managementu společnosti.

Výsledky monitoringu bezpečnosti mohou přinést optimalizace (ICT, ISMS, řízení rizik, síťe).

Úroveň detekce bezpečnostních incidentů a následné reakce



Použití PDCA – Plan, Do, Check, Act

- **Plán a prvotní implementace**
 - zavedení politiky řízení bezpečnostních incidentů,
 - zavedení schématu řízení bezpečnostních incidentů,
 - vybudování Information Security Incident Response Team – ISIRT,
 - design a implementace IDS, SIM nástrojů,
 - školení lidí zodpovědných za monitoring incidentů,
 - informování zaměstnanců.
- **Provoz**
 - detekce a reportování incidentů,
 - sběr dat potřebných k došetření incidentu,
 - reakce na incidenty,
 - obnova po incidentu.
- **Kontrola výstupů**
 - identifikace užitečných ponaučení z incidentů,
 - identifikace možných zlepšení (prevenčních metod), které incidentům mohou zamezit,
 - identifikace možných zlepšení fungování řízení incidentů jako celku.
- **Zlepšování**
 - revize pohledu managementu na celkovou bezpečnost,
 - zlepšení řízení rizik,
 - zlepšení schématu řízení incidentů,
 - zavedení opatření, které omezí incidenty,
 - rekonfigurace prvků ICT,
 - rekonfigurace detekčních nástrojů.

Různé podněty pro zlepšování

- Optimální nastavení technických parametrů nástrojů.
- Integrace podnětů bezpečnostního monitoringu do provozních procesů ICT.
- Podrobná analýza varování s cílem zlepšit fungování ICT.
- Využití poznatků z monitoringu pro zpřesnění informací o rizicích.
- Využití znalosti slabin pro zlepšování managementu bezpečnosti.

Shrnutí

- Nasazení samotných nástrojů selhává (např. IDS)
 - incidenty je potřeba řešit (nástroje to neumí),
 - je žádoucí celkově řídit bezpečnostní incidenty.
- Bezpečnostní monitoring
 - řízení bezpečnostních incidentů,
 - design a nasazení IDS/IPS,
 - design a nasazení SIM,
 - konzultace v oblasti designu a provozu,
 - dohled incidentů DC ANECT.
- Klíčové je využití při provozu s cílem trvalého zlepšování bezpečnosti.
- Monitorování je drahé – slouží k identifikaci zlepšení obranných funkcí.

Dokonalý systém byl vytvořen již dávno.

Naším cílem je dodat jej k vám.



www.anect.com

