eTrust™ Security Command Center
Security Management under control

Ivan Masný, CISM
EMM, s.r.o.
31.5.2005

EMM®

Agenda

- Čo nás k tomu vedie
- Ako na to
- Záver (čo vlastne získame)

Čo nás k tomu vedie

Scenár

- Pracovník front office vykoná povolenú (ale neautorizovanú) operáciu nad údajmi zákazníka
- Pracovník systémov podpory modifikuje záznamy o vykonanej operácii
- O vykonanej operácii nie je záznam v zákazníckom systéme

Dopad

- Priamy (finančná strata)
- Nepriamy (dobré meno, strata zákazníka)
- Nemožnosť zdokumentovať incident pre potreby stíhania

RIZIKO JE REÁLNE

Potreby

- Eliminácia útokov na ICT
  - Kevin Mitnick: „Základom obrany sú štyri A: autentizácia, autorizácia, admnistrácia, audit.“
- Efektívne riadenie bezpečnostných systémov
  - Gartner - 4% IT rozpočtov tvorí bezpečnostný HW a SW (FW, VPN, antivir, antispam, IPS, IDS, ...)
- Splnenie požiadaviek legislatívy a regulačných orgánov

(zdroje:Computerworld 112005, Computerworld 142005)

Ako na to

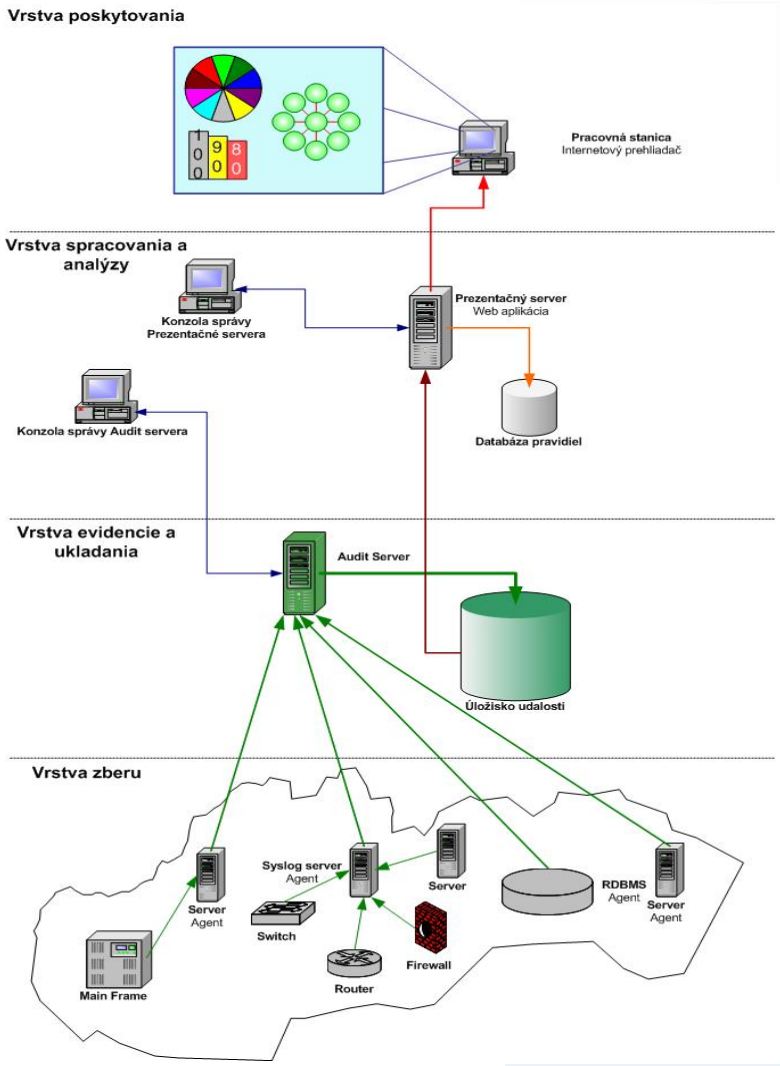
Koncepcia

- Centralizovaný, ale modulárny systém
- Centralizovaný zber sledovaných udalostí
- Centrálne vyhodnocovanie sledovaných udalostí
- Redukcia a korelácia sledovaných udalostí
- Správa incidentov
- Preukázateľnosť nepovolených aktivít

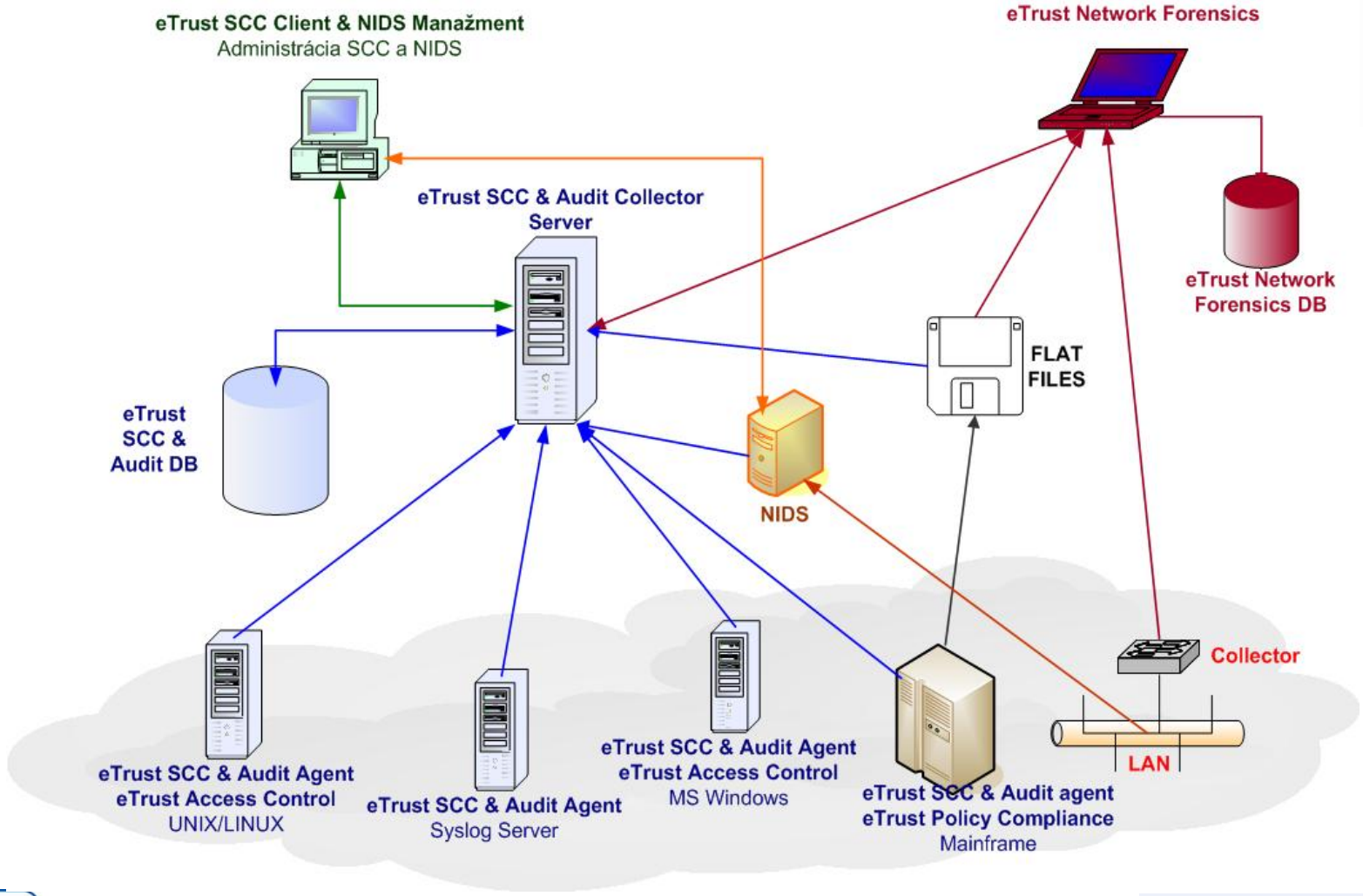
Model riešenia

4 základné vrstvy:

- Vrstva zberu
- Vrstva evidencie a ukladania
- Vrstva spracovania a analýzy
- Vrstva poskytovania



Architektúra riešenia



Fázy projektu

- Analýza a návrh
  - Analýza súčasného stavu
  - Návrh architektúry riešenia
- Inštalácia a konfigurácia pilotného projektu
- Plošná inštalácia
  - Inštalácia a konfigurácia SW komponentov
  - Integrácia a konfigurácia špeciálnych aplikácií a systémov
  - Kustomizácia systému
  - Integrácia s Help Desk riešením
  - Testovacia prevádzka
  - Akceptačné testovanie a zavedenie do rutinnej prevádzky

Fázy projektu (pokračovanie)

- Spracovanie dokumentácie
  - Zálohovanie
  - Prevádzkové predpisy

Záver
(čo vlastne získame)

Hlavné prínosy

- *e*Trust™ Security Command Center
  - Centrálny prehľad o aktuálnej bezpečnostnej situácii v organizácii
  - Identifikovanie a stanovenie priorít pre bezpečnostne relevantné udalosti
  - Efektívne riadenie bezpečnostných rizík v reálnom čase
  - Korelácia bezpečnostných rizík s aktívami organizácie
  - Zlepšenie možností vyšetrovania a prijatia následných opatrení pre identifikované bezpečnostné incidenty
  - Vytvorenie mostu medzi Network Operations Centers (NOC) a Security Operations Centers (SOC)

EMM®

eTrust™ Security Command Center
Security Management under control

Ivan Masný, CISM
EMM, s.r.o.
31.5.2005

EMM®