Risk Analysis Consultants

www.rac.cz

v0050420

Komplexní bezpečnostní audit

Jak mít detailní přehled o důležitých informacích organizace?

Marián Svetlík

svetlik@rac.cz

17. února 2010

SECURITY 2010

RiskAnalysisConsultants

Osnova

- Audit bezpečnosti informací a problémy při detailním hodnocení
- Jak mít detailní přehled o důležitých informacích organizace
- Kde jsou hranice monitoringu
- Audit a bezpečnost na jedné lodi

Míra detailu auditu informační bezpečnosti

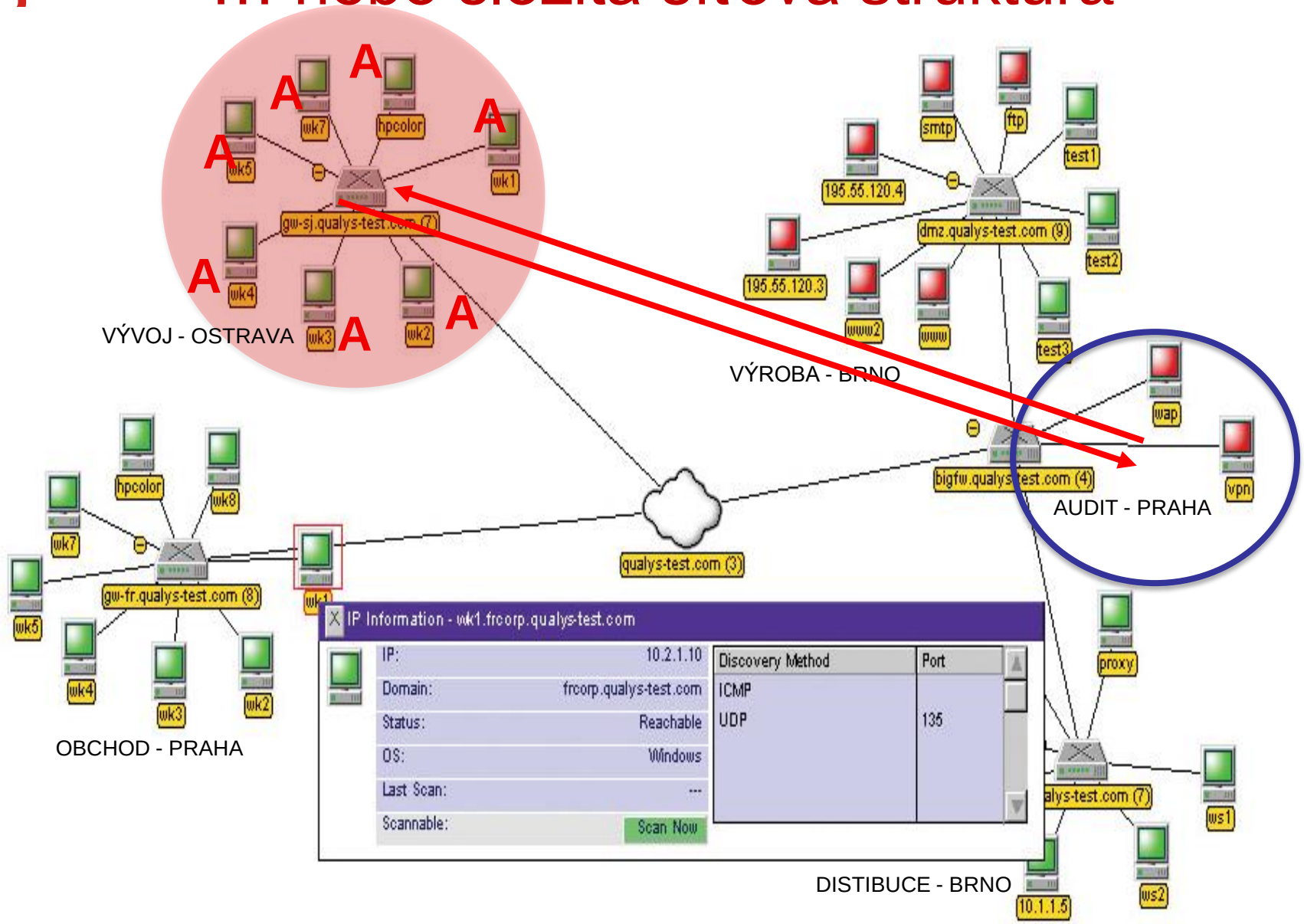
- Oblasti (bezpečnostní opatření)
  - organizační
  - administrativní
  - personální
  - technická
  - fyzická
- Detailnost (hloubka auditu)
  - existence
  - funkčnost
  - kvalita

Periodický vs. ad-hoc audit

- Periodický audit
  - ověřuje se míra souladu mezi deklarovaným (předpokládaným) stavem nebo progresem a skutečností
- Ad-hoc audit
  - to samé jako periodický, jen neplánovaně
  - cokoliv dalšího (rozuměj např. interní šetření)

Matice náročnosti

… nebo složitá síťová struktura



Monitoring nebo audit?

- Ochrana soukromí zaměstnanců?
- Ochrana osobních údajů?
- Ochrana aktiv organizace?

Až u nás nastane efektivní rovnováha těchto zdánlivě protichůdných požadavků, bude možné realizovat systémy typu e-Discovery

e-Discovery a bezpečnost informací

- e-Discovery má nezastupitelné místo v systému reakcí na bezpečnostní incidenty.
- Již od prvního vydání normy ISO/IEC TR 18 044 v roce 2004 je e-Discovery věnována pozornost v celkovém systému IRH.
- Obdobně tomu je i v ISO/IEC 27002, kde přibyla samostatná kapitola o IRH v rámci které má sběr a vyhodnocení důkazů (jinak digitální forenzní analýza) své místo.
- e-Discovery se oficiálně dostává z oblasti forenzních aplikací do základních požadavků na ochranu bezpečnosti informací obecně, jako součást preventivních bezpečnostních opatření.

Děkuji za pozornost