Bezpečnostní novinky v Microsoft Windows Server 2008

Jaroslav Maurenc

Account Technology Specialist

Microsoft Česká republika

Microsoft

Dnešní program

- Read-Only Domain Controller (RODC)
- Bitlocker
- Windows Firewall
- Network Access Protection (NAP)

Windows Server 2008

READ-ONLY DOMAIN CONTROLLER

Microsoft

Pobočková dilemata

Možnost 2:
Plnohodnotný DC na pobočce

- Pobočkový správce s právy administrátora nebo vzdálená správa
- **V případě napadení riziko pro celopodnikovou AD**

Počet zaměstnanců**: 25-500**

WAN: **Přetížená, nespolehlivá**

Bezpečnost: **Nic moc**

Správce**: Bez specializace**

Microsoft

Read-Only Domain Controller

Oddělení rolí správců

- Správce RODC nemusí být členem Domain Admins
- Ochrana proti nechtěnému zásahu do AD

Jednosměrná replikace

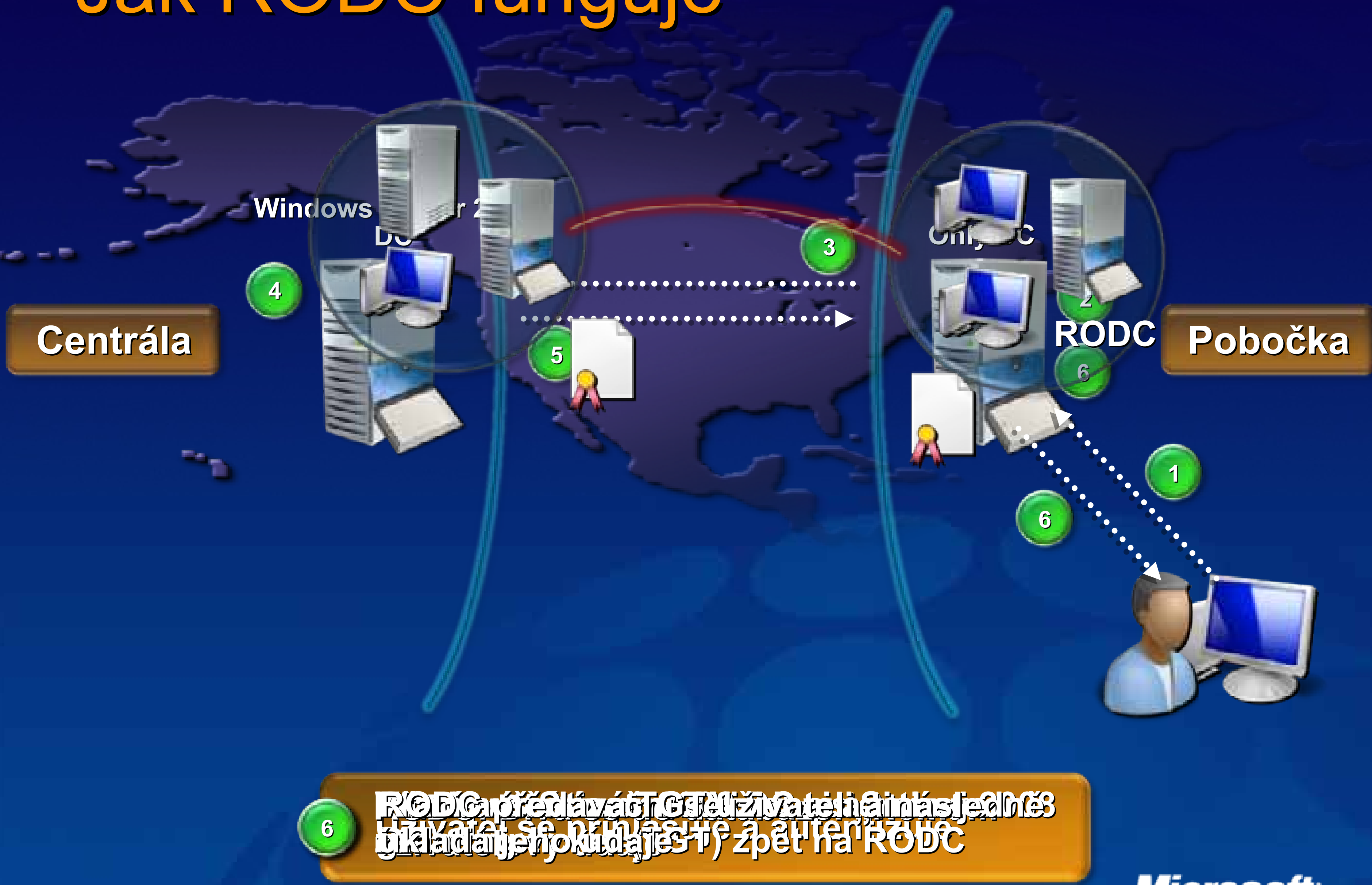
- Replikace pouze ve směru DC->RODC
  - Změny z RODC nejsou replikovány na hlavní řadič AD

Hesla nejsou standardně cachována

- Nastavení politiky definuje, co všechno RODC bude ukládat (cachovat)
- Nastavením politiky lze zabránit replikaci atributů schématu na RODC

Microsoft

Jak RODC funguje



Microsoft

Read-Only Domain Controller

Modely správy

- **Neukládá detaily účtů** (default)
  - **Pro**: Bezpečné
  - **Proti**: Nemožný offline přístup. Nutná WAN pro přihlášení
- **Uložení/cache pouze několika účtů – Doporučeno**
  - **Pro**: Udržuje rozumný poměr mezi bezpečností a produktivitou
  - **Proti**: Vyžaduje podrobnější administraci
- **Většina účtů uložena/cached**
  - **Pro**: Jednoduchá správa účtů a hesel
  - **Proti**: Omezená bezpečnostní výhody oproti plnému DC

Microsoft

Windows Server 2008

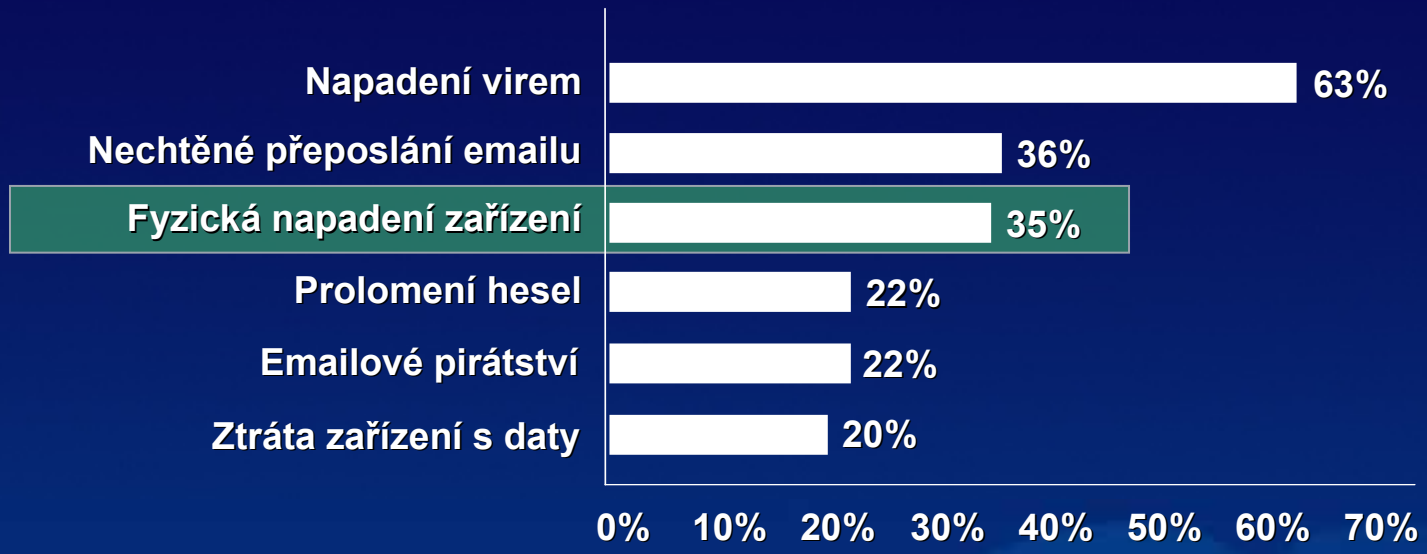
BITLOCKER

Microsoft

Ochrana proti útokům

- Ukradený server
  - Krádež citlivých dat
  - Možnost dalšího zneužití vůči firemní síti
- Prolomení systému pomocí instalace alternativního operačního systému
- Ideální pro situace, kdy nemáte 100% fyzickou kontrolu nad serverem
- BitLocker vás ochrání pouze při startu systému a neřeší útoky z prostředí OS

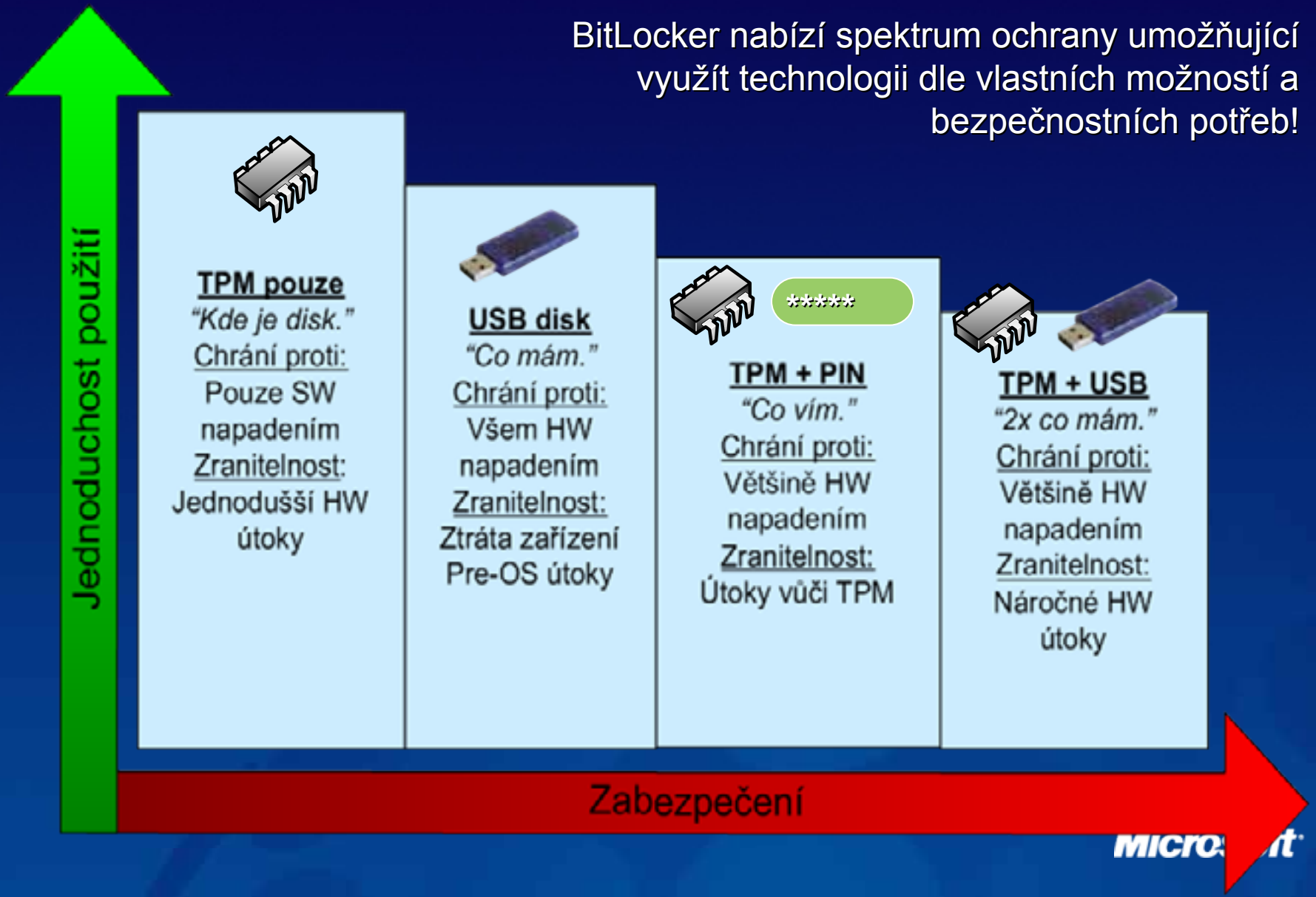
Největší úniky informací



Microsoft

Různé typy ochrany

BitLocker nabízí spektrum ochrany umožňující využít technologii dle vlastních možností a bezpečnostních potřeb!



BitLocker™

Nasazení s TPM

Instalace Windows Server 2008

- Vyžadován oddíl o minimální velikosti 1500MB
- Během instalace systém kontroluje správnou verzi TPM (v1.2) a BIOS skrze Plug and Play

Zapnutí Bitlocker

1.Ovládací panel – Bitlocker (ve Windows Server 2008 nutné nainstalovat)

2.Instalátor ověří, zda je splněn požadavek na rozdělení disků a jejich formát

3.Instalátor zapne BitLocker pro Windows oddíl

4.Instalátor ověří, zda byl TPM čip inicializován

5.Správce vybere metodu obnovu klíče

6.Instalátor pokračuje šifrováním oddílu

7.Instalátor šifruje oddíl na pozadí a informuje uživatele o procesu pomocí ikony na hlavním panelu

Microsoft

Obnova dat

- BitLocker™ umožňuje klíče automaticky ukládat a archivovat v Active Directory
  - Centralizované správa klíčů (vyžaduje rozšíření schéma AD)
- Možnost zálohování klíčů a hesel na USB disk, tiskárnu nebo do konkrétní složky
- Obnovovací heslo zná administrátor
  - Obnova může probíhat za chodu
  - Windows pokračují v práci, jako obvykle

Microsoft

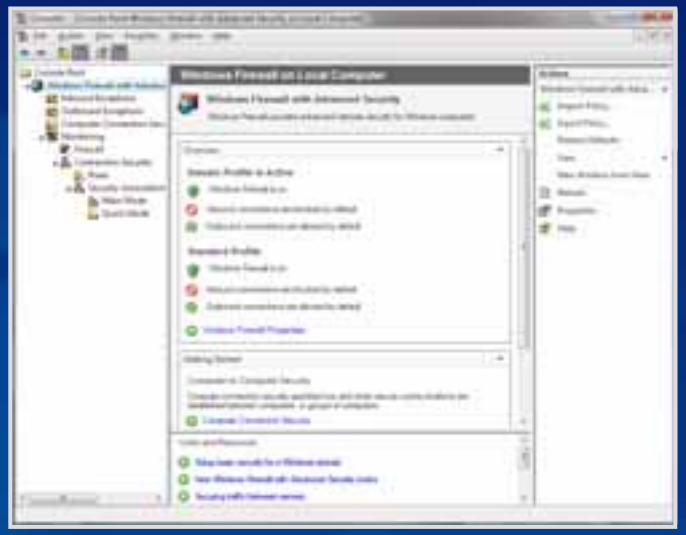
Windows Server 2008

WINDOWS FIREWALL

Microsoft

Windows Firewall s rozšířenou bezpečností

- Kombinovaný firewall a správa IPSECu
  - Nové nástroje pro správu – Windows Firewall with Advanced Security snap-in do MMC
  - Omezuje konflikty a koordinaci nastavení mezi technologiemi
- Pravidla firewallu více promyšlená a komplexní
  - Nastavují bezpečnostní požadavky jako autentizaci nebo šifrování
  - Umí požadavky na počítače a uživatele z Active Directory
- Filtrace odchozího provozu
- Zjednodušená politika ochrany redukuje nároky na komplexní správu



Microsoft

Windows Firewall

- Windows Firewall je nyní automaticky povolen
- Narozdíl od předchozích verzí nyní firewall po zapnutí nezastaví veškerý síťový provoz
- Možnost exportu a importu nastavených pravidel
- Plus: Role-based instalace automaticky přednastaví patřičné porty a další nastavení k zajištění maximální bezpečnosti
- Mínus: Když něco omylem přenastavíte, neexistuje (zatím) žádné tlačítko „obnovit síťové nastavení podle role“

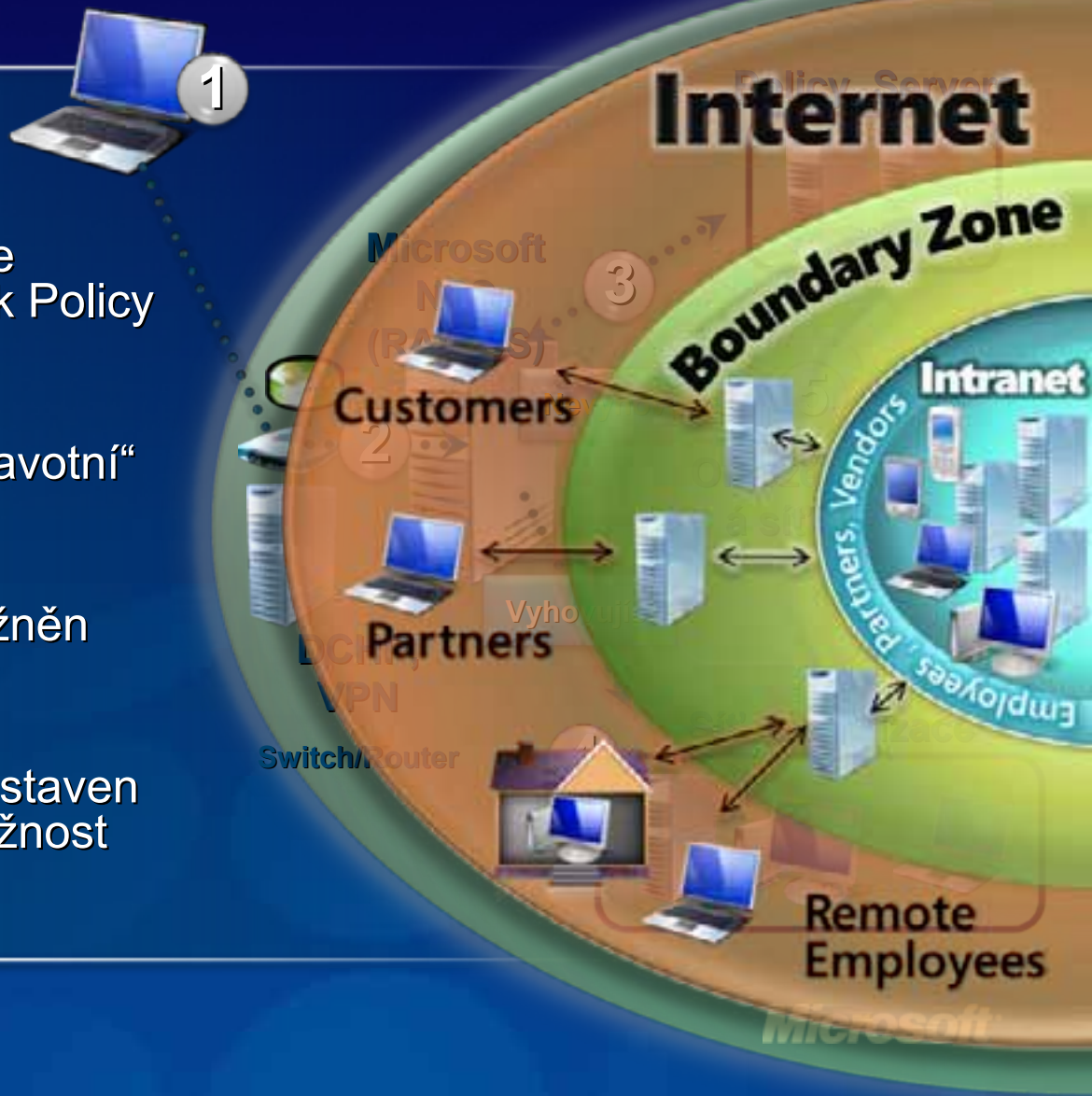
Windows Server 2008

NETWORK ACCESS PROTECTION

Microsoft

Network Access Protection
Jak to funguje?

1. Klient vyžaduje přístup
2. „Zdravotní“ stav klienta je posílán na NPS (Network Policy Server - RADIUS)
3. NPS ověří stav vůči „zdravotní“ politice
4. Pokud vyhovuje, je umožněn přístup
5. Pokud nevyhovuje, je nastaven omezený přístup pro možnost nápravy



Možnosti „vynucení“ NAP

- DHCP
- VPN
- 802.1X (Switch, Access point, Router)
- Terminálový přístup
- IPSec

Co musíte o NAPu vědět?

- Požadované technologie jsou vestavěny ve Windows Server 2008, Windows Vista a Windows XP SP3
- NAP spolupracuje prakticky se všemi switchi/AP na trhu a používá standardní protokoly
- Nejsou pro nasazení potřeba žádné další licence pro NAP pokud již máte Windows CAL
- NAP "agent" není ve skutečnosti agent, je to služba, která běží na počítači a je možné ji spravovat pomocí Group Policy
- NAP není řešení bezpečnosti, je to řešení zdraví sítě
- NAP spolupracuje se Cisco NAC (Network Admission Control) framework
- NAP Statement of Health (SOH) protokol byl přijat jako TNC/TCG standard
- *Není NAP agent pro Windows Server 2003!*

Microsoft

Otázky?