



LEADING EDGE 2009

Kaj imata s tem NAP in IPSec?

Miha Pihler, MCSA, MCSE, MCT, CISSP, Microsoft MVP

miha.pihler@telnet.si

- www.krneki.net/blog
- SloWUG (www.slowug.si)
 - 14.10.2009 – Zanimiva predavanja!
 - Za člane je cenejši obisk Tech-Ed Europe
- miha.pihler@telnet.si

Kaj NAP NE rešuje

- NAP ne rešuje problema zlonamernih uporabnikov
- Zlonamerni uporabnik ima lahko na omrežju računalnik skluden z NAP politiko – in lahko izvaja napade na ostale sisteme!

Kaj NAP rešuje

- Računalniki, ki jih nimamo pod upravljanjem
 - Gosti iz drugih omrežij
- Računalniki, ki niso v skladu s politiko uporabe
 - Nimajo nameščenih popravkov
 - Nimajo nameščenega protivirusnega programa
 - ...
- VPN povezave
 - Računalniki, ki so redko v fizičnem omrežju
 - ...

Kaj NAP rešuje

- Sistem, ki ni zdrav je izoliran od ostalih sistemov, ki so zdravi
- Omogoča odpravljanje pomanjkljivosti

Vloga NAP

- Preverjanje zdravja
 - Osnovno preverjanje zdravja ob priklopu na omrežje
- Zagotavljanje zdravja
 - Nameščanje popravkov, definicij, ...
- Omejevanje dostopa
 - V primeru, da sistem ni zdrav lahko omejimo dostop do virov

Vloga NAP

- Zmanjšuje verjetnost okužbe omrežja
- Varovanje omrežje preko izolacije pred nezdravimi odjemalci

Komponente NAP

- Aktivni imenik (Active Directory)
- NAP odjemalci
 - Windows XP SP3 ali novejši operacijski sistemi
- “NAP enforcement points” (NAP točke prisile)
 - Health Registration Authority (HRA)
 - Windows IIS in certifikatna agencija
 - Network Access Devices
 - Stikala in brezžične dostopne točke
 - VPN strežnik
 - DHCP strežnik

Komponente NAP

- NAP health policy strežniki (ex. IAS in RADIUS)
 - Windows 2008 strežnik z NPS servisom
 - Hrani zahteve po zdravju sistema
 - Izvaja preverjanje zdravja
- Health Requirement Servers
 - Preverja trenutno varnostne zahteve
 - Npr. št. zadnje različice definicij antivirusnega programa

Komponente NAP

- Izolirano omrežje
 - Remediation strežniki
 - Omogočajo posodabljanje (zdravljenje) sistemov
 - Odjemalci, ki ne podpirajo NAP storitev
- System Health Agents (SHAs)
 - Na NAP odjemalcu
- System Health Validators (SHV)
 - Na NAP strežinku

Komponente NAP

- SHA in SHV

- SHA sporoči status računalnika SHV
- V Windows XP SP3 ali novejšem OS najdemo SHA, ki spremlja in nadzira "Windows Security Center"
- SHA generira "System Statement of Helth" (SSoH) ter ga posreduje NAP "Health policy" strežniku, ki preveri posredovanje podatke
- NAP strežnik odgovori z "System Statement of Health Response" (SSoHR), ki lahko vsebuje informacije o:
 - - zdravlju sistema
 - - zdravljenju sistema

Komponente NAP

- Enforcement Client (EC)

- IPsec EC
- 802.1x EC
- VPN EC
- DHCP EC
- TS Gateway EC

- Enforcement Server (ES)

- IPsec ES
- DHCP ES
- TS Gateway ES

IPSec izolacija

- Možno je izolirati računalnike med seboj
 - Kdo sme komunicirati s kom?
 - Lahko preprosto določimo kako smejo med seboj komunicirati člani domene
- Preprečuje dostop do strežnikov odjemalcem, ki niso del domene
 - S tem preprečujemo napade in okužbe
- Pri IPSec izolaciji se ne preverja stanje računalnika!

IPSec izolacija

- Ne zahteva:
 - CA Strežnika
 - Za avtentikacijo se uporablja Kerberos
 - NAP, HRA ter ostalih servisov

Kam od tu naprej?

- DirectAccess
 - NAP
 - IPSec

Viri

- [Windows Firewall with Advanced Security: Step-by-Step Guide: Deploying Windows Firewall and IPsec Policies](#)
- [Step-by-Step Guide: Demonstrate NAP IPsec Enforcement in a Test Lab](#)
- [Step-by-Step Guide: Demonstrate NAP DHCP Enforcement in a Test Lab](#)

- www.krneki.net/blog
- SloWUG (www.slowug.si)
- miha.pihler@telnet.si