Eesti Infotehnoloogia Kolledž

WINDOWS SERVER 2012 TURVAMEETMETE RAKENDUS KORPORATIIVVÕRGUS

REFERAAT

ÕPPEAINE : WINDOWS SERVER 2012 ADMINISTREERIMINE

Jüri Olevsoo
ÕPPERÜHM A22

Tallinn 2013

WINDOWS SERVER 2012 TURVAMEETMETE RAKENDUS KORPORATIIVVÕRGUS

Korporatiivvõrgus võib töötada korraga mitmed sajad arvutid ning võtgu topoloogi võib haatrata kõiki meie maakera regioone. Üle on mingug suurte infokoguste pärast „pilve tehnoloogiale“ selleks et kõik kasutajad oma infole ligipääsu saals peab väga hoolikalt kontrollima kasutajaid ja nende masinaid.

VÕRK: POLICY SERVICE JA LIGIPÄÄS

Praegu on väga populaarne tehnoloogia BYOD (BRING YOUR OWN DEVICE) eri ettevõtetes, see eeldab seda, et töötajatel on kasutusel oma masinad mida hooldavad nad ise. See on kõigile väga kasulik: ettevõte ei pea koguaeg täiendama enda arvutiparki ja töötajad saavad kasutada enda lemmik läpparit või tahvelarvutit tööl ning ei pea kohanema tööarvutiga. Kuid alati on oht, et kasutaja võib enda lõbuks välja lülitada updated, konfigureerida tulemüüri või siis töötada vana antiviirusega. See tõstab tunduvalt turvariski, kuna antud tegevus ei ohusta ainult nende arvutit vaid kogu ettevõtte arvutivõrku. Selleks, et vältida seda turvariski ettevõtte võrgus peab kontrollima kasutajate arvutite olekut.

Funktsioon NETWORK ACCESS PROTECTION, mis tekkis WINDOWS SERVER 2k8ga, kontrollib kasutaja süsteemi vastavalt võrgu poliitikale. Vastavalt kontrollitava masina seadistusele valib siis server, kas lubada talle püsiva või ajutise ligipääsu. Kõik sündmused masinate kontrollist salvestatakse logidesse ning süsteemi administraator omab pidevat ülevaadet olukorrast.

Karantinis, allvõrgus asuvad korrektsiooni serverid (REMEDIATION SERVERS) annavad resurrsi selleks, et võrku tulevad masinad saaks võimaluse kõrvaldada leitud puudused (antiviiruse andmebaas ja WSUS uunduste server).Pealekõikide probleemide kõrvaldamise süsteem taasühendab masinad ja kontrollib, kas kõik on normis ning kas masinale saab anda juurdepääsu tööks ühis võrgus. Kogu ühendusaja vältel süsteem kontrollib, kas ühendunud masin vastab seadud nõutele (poliitikatele-POLICY’tele) ja kui masin ei vasta seatud tingimustele siis paigutatakse ta karantiini (karantiini paigutamine toimub ka juhul kui näiteks masin teeb mõne lubamattu toimingu, mis läheb vastuollu administraatori seatud

kriteeriumitega). Põhimõtteliselt kontroll ja karantiin- need on mõlemad NAP'i kontrollitavad- ülejäänu kontroll on teostatav teiste mehhanismidega. NAP'i seadistusel kasutatakse erinevaid kohustuslikke mehhanisme nagu DHCP, VPN. Ipsec, IEEE 802,1x jne.

Kaughallatavale süsteemile (juurdepääsu tahtvale masinale) paigaldatakse NAP klient pool, mis koosneb NAP agendist, süsteemi kontrolli agendist (WINDOWS SECURITY HEALTH AGENT) ja süsteemi kohustaja kliendist (NAP ENFORCMENT CLIENT). Viimane mainitu vastutab ka masina suhtluse eest. Kogutud andmed saadetakse süsteemi poliitika serverile (NPS-NETWORK POLICY SERVER) SHV-sõnumi (SYSTEM HEALTH VALIDATOR) näol.

WINDOWS SECURITY HEALTH AGENT on lisatud kõikidesse WINDOWS operatsioonisüsteemidesse alates WINDOWS XP sp3-s, toetatud on ka integreerimine CISCO NETWORK ADMISSION CONTROL'iga. Turul on ka lahendusi mis pakuvad NAP funktsionaalsust ka OS X'ile ja Linux opsüsteemidele. Näiteks Symanteci poolt toodetud Symantec Endpoint Protection omab endas lisamooduleid, mis laseb kontrollida süsteemi NPS abil.

Network Policy and Access Service'i rolli saab kasutada oma NPS püsti saamiseks serveril või proxy serveril RADIUS-el ja süsteem kontrollib siis RADIUS serverile ühinduvate RADIUS klientide valmisolekut kontrollitud ühenduseks (ethernet kommutaatorid 802.1x toega ja hotspot'id). Kõik vastavad seadistamistoimingud toimuvad netsh või siis serveri administraatorliidese abil (netsh nps).

Windows 2008-s on NPS saanud võimaluse kasutada mitmeid SHV konfiguratsioone, mis võimaldab kontrollida nii LAN kui VPN liitumisi. Ka on tekitatud mitmeid standardvorminguid (template), mis tagavad juba eelseadistuse ja annavad võimaluse kiirelt importida NPS konfiguratsiooni.NPS serveri seadistamiseks saab kasutada ka visruaalset serverit (HYPER-V realseerimine), klastereid ei toetata.

NPS seadistamine toimub rollide ja komponentide lisamisega, seadistamisel märgistame ära

Network Policy and Access Service ja jälgime ekraanil olevaid juhendeid. Saab valida kolme valikuvõimaluse vahel:

1) NETWORK POLICY SERVER- kasutatakse erinevate ühendumisvõimaluste korral, milleks on VPN, WIFI, REMOTE SERVER või siis 802.1x kommutaatorid.

2) HRA- komponent mis vastutab sertifikaatide väljastamise eest klientidele, kes vastavad kontrolli kriteeriumitele. Kasutatakse ainult Ipsec protokolli põhjal.
3) HCAP- laseb ühendada MS võrgu kaitse koos CISCO võrgu kontrolleriga.

HRA puhul peab seda seostama sertifitseerimiskeskusega. Sertifikaate saab väljastada nii võrgus registreeritud kui ka anonüümsetele kasutajatele. Kui NPS toimib domeeni võrgus siis on eelistatavam ainult võrgus registreeritud kasutajatele sertifikaatide väljastamine. Policy'd annavad võimaluse seadistada grupid (windows, arvutid või siis kasutajate grupid), HCAP'i (kasutajate grupid ja paigutamine), piiranguid nädalapäevade ligipääsuna, ligipääsudokumendid, IP klassid, opsüsteemid ja arhitektuurid ka laseb valida poliitikate kriteeriumid masina jõudluse vallas ning ka teisi parameetreid.

Igal domeeni kontrolleril, mis töötab SERVER 2012-l peab sama seadistus olema poliitikate template'de suhtes, annab seadistada KERBEROS turvaseadistuse alt.

Windows Server 2012-s tekkis võimalus seadistada NPS-i ja teisi operatsiooni konsoolist POWERSHELL'i abil.

Näitena võimalus seadistada ja paigaldada 13-komandletist koosnevat seadistust:

```
PS> ADD-WindowsFeature NPAS-Policy-Server -includemanagementtools
PS> Import-Module NPS
PS> Get-Command -Module NPS
```

Komandlet EXPORT/IMPORT NPS CONFIGURATION laseb salvestada või taastada NPS-serveri konfiguratsiooni. See on alternatiiviks NETSH NPS EXPORT/IMPORT ile.

```
PS> Export-NpsConfiguration -Path C:\NPSTemp -Path Npsconfig.xml
```

Fail sisaldab RADIUS klientide andmeid seetõttu peame hoolitsema, et keegi sellele ligipääsu ei saaks. Nüüd teisel serveril impordime antud faili:

```
PS> Import-NpsConfiguration -Path C:\Npsconfig.xml
```

DÜNAAMILINE HALDAMINE

Kasutajad võivad ühenduda ettevõtte võrguga eri ligipääsupunktide kaudu, need võivad olla nii avalikud võrgupunktid kui ka kaitstud võrk. Kautaja on üks aga äri riskid, mis võrguku sisenemisega kaasnevad on erinevad. Praegusel ajal on väga tähtis turvalisuse küsimus kuna suurem osa infoleketest on põhjustatud insider'ite poolt (lokaalkasutajad, kes võivad infot lekitada nii tahtlikult kui tahtmatult). Selleks, et piiritleda võimalikke juurdepääse moodustatakse suur hulk kasutatjate gruppe, mis väga raskendab administreerimist ning sellega kaasnevat arusaamist selleks mis õigusi keegi omab. Väiksemgi administraatori poolne eksitus ja kasutaja poolt omav dokument võib asuda juba vales kohas ja sellele võivad omada ligipääsu isikud, kes seda ligipääsu omama ei peaks.Kaasaja ettevõtted vajavad haldamiseks niisuguseid mehhanisme, mis lekke põhjuse ära kõrvaldaks nagu seda on DLP-Data Leak Prevention. Osalist kaitset saab pakkuda ka õiguste haldamise teenus (Rights Managment Services) aga see ei kõrvalda kõiki probleeme. Selleks, et olukorda lahendada on Windows Server 2012-l dünaamilise kontrolli tehnoloogi (DYNAMIC Access Controls DAC).

Tehnoloogia baseerub kolmel põhimõistel:

1) Dokumendi klassifitseerimine- kasutaja poolsete täägide abil klassifitseeritakse dokumendi juurdepääsu võimalused;
2) Poliitikad- tavaliselt neid kehtestavad üks või mitmed reeglid, mis on tingigitud kasutaja seadustustest (Active Directory põhised)
3) Audit- laiemad auditeerimise poliitikad, mis annavad võimaluse ligipääsuks konfidentsiaalsele infole.

DAC intergreerimine toimub RMS-iga koos ning laseb reaalajas kaitsta dokumenti mis omab vastavat täägi. Seadistus annab võimaluse automaatselt liigitada dokumenti, see toimub failiserveril installides/konfides File Resource Manager'i.

Windows Server 2012-l on lisatud uus mehhanism mis kontrollib ligipääsu andnud resursi indifitseerimist- claims. Peale SID turvaindifikaatoir kasutaja arvutist liidetakse dokumendile ka claims atribuut mis annab võimaluse kontrollida kes võib antud dokumenti hallata.

DAC-i üks huvipakkuvaid omadusi on võimalus osaliselt integreeruda, administraator siis ipaigaldab DAC-i ilma blokeerimise võimalusteta, ainult audit-i režiimis. See annab adminnile võimaluse näha kes ja kuhu üritab saada või sai ligipääsu, mis tagab selle, et administraator oskab blokeeringuid paigaldades vältida kasutajate kaebusi, et nad ei saa neile harva vaja minevatele resurrsidele ligipääsu.DAC pakub suurepärast võimalust teavitada kasutajat sellest, miks ta ei saa dokumendile ligipääsu, näidates talle informeerivat kirja, mida ta peaks tegema, et dokumenti saaks vaadata. Näiteks see võib olla asutusesisese kasutamise deklaratsioon, mida kinnitades kasutaja saab dokumendile, mis ei ole otseselt tema tööga seotud, ligipääsu. Peale antud deklaratsiooni kinnitamist „claims" uuendub ning kasutaja saab ligipääsu. Poliitikat saab seadistada ACTVE DIRECTORY ADMINISTRATIVE CENTER'i

abil, seal asub 8 alalõiku sisaldav seadistus. Iga alalõigu puhul peab administraator valima vastavad seadistamisnormid.

Esimeses alalõigus on võimalus valida üle 100 Active Directory valiku, mis võivad „claims“is kajastuda. Valiku kergendamiseks on võimalus valida filtrit, mis siis kitsendab valikuvariante.

Teise sammuna järgneb konktreetsete resursside valimine RESOURCE PROPERTIES, mis laseb valida konkreetsete failide ja kaustade klassifikatsiooni. Kolmas samm on tsentraliseeritud juurdepääsu konfigureerimine- CENTRAL ACCESS RULES,kus saab valida otseseid resurrse ja nendele ligipääsu, mis vastavad kasutaja grupile.

Peale poliitikate loomist peab nad sisestama ka failiserverisse. Selleks avatakse GROUP POLICY EDITOR-i ja valime arvuti seadistamise-> Poliitikad-> Windowsi seadistamine-> Faili süsteem -> KEskne juurdepääsu poliitika. Alapunktides valime KESKSETE JUURDEPÄÄSU POLIITIKATE HALDAMINE ja sealt siis poliitika, mida rakendada tahame.

Auditi seadistamiseks tuleb avada LAIENDATUD POLIITIKATE AUDIT-> POLIITIKA AUDIT-> Objektide JUURDEPÄÄS, seal siis tekib uus valikuvõimaluse punkt AUDIT KONTROLLIMAKS TSENTRALISEERITUD POLIITIKAT. Siis tuleb seda poliitikat rakendada, selleks lähme faili või kausta seadistuse parameetritesse ja valime LISAVALIKUD-> TSENTRALISEERITUD POLIITIKA ning vlimse vajaliku poliitika. POWERSHELL pakub võimalust vaatamaks kõiki tsentraliseeritud poliitikat käsu abil:

```
PS> Get-ADCentralAccessPolicy -Filter *
```

Lisaks mainitud turvameetmetele soovitan ka tähelepanu pöörata Windows Server 2012 kasutaja tuvastamis võimalusele WINDOWS AZURE APPFABRIC abil (http://en.wikipedia.org/wiki/AppFabric)

Veel üheks turvalisuse tõstmise võimaluseks on kasutusele võtta WINDOWS BIOMETRIC FRAMEWORK, mis on alates WINDOWS 7-st kasutusele tulnud MICROSOFTI näpujälje põhjal tuvastamise mehhanism (enne oli realiseeritav ainult teiste tarkvaralahenduste tootjate toodetega) http://msdn.microsoft.com/en-us/library/windows/desktop/dd401507(v=vs.85).aspx.