



Ylläpito takaa turvan

Yrityksen tärkein ja luottamuksellisin tieto on yleensä palvelimissa. Niiden suojaaminen on yhä tärkeämpää, kun uudet virukset pääsevät läpäisemään palomuurit nykyistä todennäköisemmin.

Tietohallinnon suunnauksissa ollaan palaamassa takaisin viime vuosikymmenien hajautetuista ratkaisuista keskitettyihin ratkaisuihin. Työasemat vakioidaan mahdollisimman pitkälti, ja samassa yhteydessä kaiken käyttäjien tekemän datan tallennus siirtyy omista työasemista palvelimille. Käyttäjäprofiilit ladataan palvelimelta ja kaikki sähköpostit sijaitsevat sähköpostipalvelimen tietokannassa.

Jos käyttäjän työasema sekoaa tai levy hajoaa, hän pystyy jatkamaan työskentelyään toisella koneella.

Kun kaikki kriittinen data on palvelimilla, niiden varmuuskopiointi on toimittava luotettavasti. Palvelimien hinta-suorituskyky-suhte on parantunut muutamassa vuodessa samalla tavalla kuin työasemien. Varsinkin suurikokoisten levyjärjestelmien rakentaminen on edullisempaa kuin aikaisemmin. Valitettavasti varmuuskopiointijärjestelmien hinta-kapasiteettisuhte ei ole kehittynyt yhtä suotuisasti.

Mikäli yritys haluaa varmistaa pitemmällä aikavälillä tarvittavan levykapasiteetin ja haluaa riittävän laajennus- ja suorituskykykasvupolun, kannattaa harkita SAN-talennusverkon (Storage Area Network)

käyttöä perinteisten tiedostopalvelimien sijasta.

SUOJAA VERKON AKTIIVILAITTEET

Lähiverkossa tarvitaan normaalisti yksi reunakytkin jokaista 24:ää tai 48:aa käyttäjää kohden sekä palvelinhuoneeseen keskitetty pääkytkin, joka yhdistää reunakytkimet, palvelimet ja ulkoiset internet-yhteydet toisiinsa. Lisäksi tarvitaan yksi tai useampi reititin liikenteen ohjaamiseksi oikeisiin verkko-osoitteisiin.

Kaikkien näiden lähiverkon aktiivilaitteiden pitää sijaita valtuissa lukittavissa tiloissa, ja niiden hallinta ja niihin tehdyt muutokset pitää dokumentoida hyvin ja ajantasaisesti.

Laitteissa tarvittavien käyttäjätunnusten ja salasanojen pitäisi noudattaa samanlaista, riittävän monimutkaista käytäntöä kuin lähiverkon järjestelmänvalvojien tapauksessa: salasanoissa 14 merkkiä, kolmea eri merkkisarjaa, lukitus riittävän monen väärän yrityksen jälkeen.

Internet-yhteyden suojaksi tarvitaan palomuuuri. Pienemmissä yrityksissä palomuuuri saatetaan ostaa palveluna yhteyden palveluntarjoajalta (isp), mutta suuremmissa yrityksissä muurin hallinnasta ja määrittelyistä halutaan vastata itse.

Mikäli muuria ei ole, vaan tietoturva on toteutettu esimerkiksi internet-yhteyden reitittimen pääslistoilla, on palomuurin hankkimisen lähiverkon tietoturvan kehittämisen ykköskohde. Palomuurien hintataso on laskenut, ja muurimarkkinoilla on useita edullisia "mustia purkkeja", joiden murtaminen ja ohittaminen edellyttävät yleensä määritysvirhettä muurin asetuksissa.

MIETI KÄYTTÖ-OIKEUDET HUOLELLA

Tiedostopalvelimien resursseihin tarvittavat käyttöoikeudet on suunniteltava huolella. Yleensä tullaan toimeen kolmella eri käyttöoikeustasolla, joista kaksi ensimmäistä ovat peruskäyttäjille ja kolmas järjestelmänvalvojille.

Yleisimmin tarvitaan sitä, että käyttäjillä on lukuoikeus jaettuun resurssiin. Se sallii kansioden selaamisen, tiedostojen ja ohjelmien avaamisen ja käynnistämisen sekä niiden kopioimisen. Se ei salli tiedostojen tai kansioden luomista, muuttamista tai poistamista eikä näiden käyttöoikeuksien muuttamista. Tällaisia vain lukemiseen tarkoitettuja resursseja ovat esimerkiksi verkosta ajettavat sovellukset sekä erilaisten mallipohjien jakamiseen tarkoitettut kansiot.

Toinen oikeustaso on muutoin sama kuin ensimmäinen taso, mutta käyttäjällä on lisäksi muutosoikeus tiedostoihin ja kansioihin: hän voi luoda, muuttaa ja poistaa niitä. Tällaiset oikeudet pitää olla esimerkiksi käyttäjän kotihakemistoon.

Kirjoitusoikeuksia ei pidä toteuttaa antamalla peruskäyttäjille täysiä oikeuksia (full control), koska

täydet oikeudet tarkoittavat myös oikeutta muuttaa suojauksia. Käyttäjät voisivat jopa estää muiden käyttäjien, myös järjestelmänvalvojan, pääsyn tiedostoihin.

Täydet oikeudet annetaan vain järjestelmänvalvojille. Mikäli näiden kolmen käyttöoikeustason sijaan tai lisäksi tarvitaan jotain erikoisoikeuksia, pitäisi niihin aina olla selkeä syy.

Mikäli yrityksessä on kaikille käyttäjille tarkoitettu jaettu levyresurssi, pitää myös sen käyttöoikeuksien määrittelyssä olla huolellinen. Hyvä käytäntö on, että käyttäjälle annetaan kaikkiin kansioihin lukuoikeus, mutta kirjoitusoikeus vain omaan kansioon. Tällöin käyttäjävirhe tai virusepidemia ei aiheuta muiden käyttäjien tiedostojen tuhoutumista tai saastumista.

Sen sijaan verkossa olevaan käyttäjän omaan kotihakemistoon ei anneta mitään käyttöoikeutta muille kuin itse käyttäjälle ja yrityksen tietoturvaliitosta riippuen järjestelmänvalvojille. Käyttäjän pitää voida luottaa siihen, että palvelimelle tallennettavat tiedostot ovat suojassa.

TURVA-AUKOT OVAT JATKUVA UHKA

Kahden viimeisen vuoden aikana tietoturva-ammattilaisten suurin huoli on siirtynyt työasema- ja palvelintasolla Microsoftin tuotteista löytyneisiin kriittisiin tietoturva-aukkoihin. Aukkoja on kaikissa tuotteissa, mutta kun Microsoftin tuotteet ovat erittäin yleisesti käytössä, niiden aukot ovat paha riski.

Ne mahdollistavat pahimmillaan vakavat tietoturvuudot käyttäjän työaseman kautta. Jos



▲ Windowsupdate-sivuston kautta onnistuu helposti pienen konemäärän tai kotikoneiden päivittäminen. Kriittiset turva-korjaukset ovat ajan tasalla, kun kohdassa "Tärkeät päivitykset ja ServicePack-päivitykset" kohdassa lukee 0.

###

!)
! 5 7 7 #
8

! 5 7

www.win-dowsupdate.com

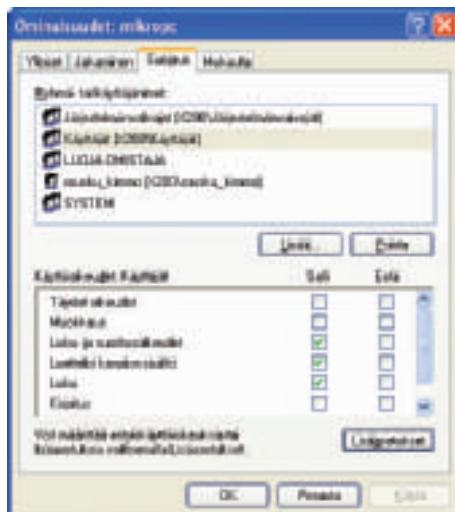
AUTOMAATTIPÄIVITYSTYSEN ASETUKSET

" # \$%%%
4 ,1 6
" # 2,
(9

###

MONTA TAPAA AUTOMATISOIDA

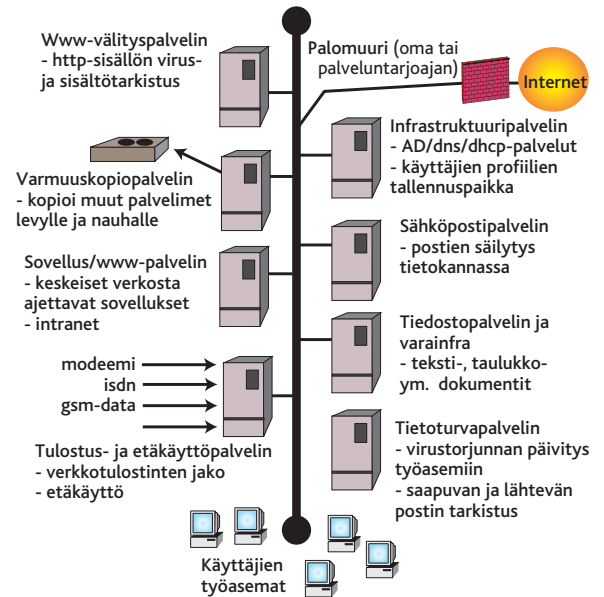
0
(" # \$%%%
1 " # 2,
3
4 5
6 ! 5
7 " # 8



◀ Mikropc-kansioon on käyttäjät-ryhmään kuuluville käyttäjillä "Luku- ja suoritusoikeudet". Peruskäyttäjän oikeuksia voi kasvattaa antamalla lisäksi kirjoitusoikeuden, mutta muokkaus- ja täydet oikeudet on tarkoitettu lähinnä järjestelmänvalvojille.

" # \$%%% & '
(

Palvelimien työnjako



▲ Keskitetyn palvelinratkaisun rakentaminen vaatii vähintään muutamia palvelimia. Jos kaikki palvelinroolit sijoitetaan yhteen palvelimeen, ei saavuteta riittävää suorituskykyä ja vikasietoisuutta.