

Työasemaympäristön sähkönsäästöohjeet

Liite 2, Energiatehokkuuden huomiointi työasemaympäristön ylläpidossa

Motiva Oy

3.12.2010

1. Yhteenveto

Seuraavat suositukset on tarkoitettu erityisesti organisaatioiden työasemien elinkaarenhallinnasta ja päivityksistä vastaaville **IT-ammattilaisille**.

Työasemaympäristön ylläpitoa koskevien suositusten tiivistelmä:

- Huolehtikaa, että työasemavakion virranhallinta-asetukset ovat energiatehokkaat. Harkitkaa sitä, että työasemat oletusarvoisesti siirtyvät virtakytkimestä horrostilaan
- Mikäli investointi on perusteltavissa, käytäkää nykyaikaista keskitettyä työasemaympäristön hallintatyökalua, joka tukee etäkäynnistystä. Jaelkaa tietoturvapäivitykset mahdollisimman tehokkaasti, tarvittaessa työajan jälkeen hyödyntäen työasemien etäkäynnistystä ja etäsammutusta
- Jos etäkäynnistyksen käyttäminen ei ole mahdollista, päivittäkää työasemaympäristöt työaikana vaiheistettusti, jotta lähiverkko ei kuormitu liikaa
- Ellei organisaation toiminnasta johtuen työasemaympäristöjen päivittäminen ole mahdollista työpäivän aikana eikä etäkäynnistystäkään voida käyttää, ajoittakaa tyypilliset turvapäivitykset kuukausikelloon sijoitettaviin huoltoikkunoihin. Ohjeistakaa käyttäjiä jättämään työasemat päälle näiden huoltoikkunoiden mukaisesti.

Aikaisemmin työasemien keskitetyn päivittämismenettelyn on katsottu edellyttävän työasemien pitämistä päällä iltaisin ja viikonloppuisin. Tätä perustellaan yleensä seuraavilla tekijöillä:

- Tietoturvasyistä työasemaympäristö on saatava päivitettyä hallitusti ja keskitetysti – käytetään päivitysskriptejä tai keskitettyä työasemaympäristön hallintaohjelmistoa.
- Tietoturvapäivitykset on saatava jaeltua mahdollisimman tehokkaasti ja nopeasti turvapäivitysten saapumisen jälkeen.
- Tietoturvapäivitykset halutaan jakaa ennen kuin työntekijät aloittavat varsinaisen työnsä.
- Päivitysten jakelu työntekijöiden työasemien käynnistyksen yhteydessä tai heti sen jälkeen kuormittaa tietoliikenneverkkoa liikaa, koska ihmiset tulevat suurin piirtein samaan aikaan töihin.
- Turvapäivityksien arvioidaan hankaloittavan tarpeettomasti työntekijöiden normaalia työtä, mikäli ne jaeltaisiin käynnissä oleviin työasemiin työpäivän aikana.
- Päivitykset tulee järjestää siten, että IT-osasto tms. voi varmistua siitä, että kaikki työasemat on päivitetty samaan versioon.

Edellä olevat seikat perustuvat tietoturvallisuuteen sekä käyttäjien ns. epäsuorien IT-kustannusten minimointiin. Näitä on kuitenkin hyvä tarkastella hiukan laajemmin.

Jatkuvan päälläolon riskit ja haasteet

Edellä listatuista seikoista johtuen usein katsotaan, että työasemien tulee olla päällä myös iltaisin ja viikonloppuisin. Luonnollisesti tämä on varsin epäedullinen työasemaympäristön sähkönkulutuksen kannalta, mutta tähän liittyy muitakin arvioitavia tekijöitä.

Valvomaton päällä oleva työasema muodostaa aina suuremman tietoturvariskin kuin työasema, joka ei ole päällä. Tietoturvariskit ja -aukot ovat olleet olemassa jo tyypillisesti kuukausia ennen kuin niihin saadaan tietoturvapäivitys. Vaikka riski tietoturva-aukon väärinkäytöksille kasvaakin sen myötä, kun asia tulee julkiseksi, ovat vielä päivittämättömät työasemat olleet alttiita tietoturvahyökkäyksille niin kauan kuin tietoturvariskikin on ollut olemassa. Tarkkaan ottaen työasemat ovat useimpien haavoittuvuuksien kohdalla olleet alttiita näille hyökkäyksille koko **päällä oloaikansa**.

Jatkuvasti päällä oleva tietokone on siis **yli kolminkertaisen ajan** altis tyypillisimmille tietoturvahyökkäyksille kuin tietokone, joka sammutetaan työpäivän jälkeen.

Toki varsinaisen käytön aikana tietyt tietoturvariskit ovat jonkin verran suurempia kuin pelkän päällä olon aikana. Tämä ei kuitenkaan koske kaikkia riskityyppejä vaan joissakin tietoturva-aukoissa riittää, että kone on päällä ja kytkettynä tietoliikenneverkkoon.

Useimmat tietoturvapäivitykset voidaan jakaa esimerkiksi aamupäivän aikana ilman merkittävää lisäriskiä noiden muutaman tunnin käytön aikana. Vain kaikkein vakavimmissa virus-, mato- tai uhkaepidemioissa turvapäivitykset tulee jaella välittömästi.

Jatkuva päällä olo lyhentää myös kuluvien osien, kuten tuulettimien elinikää ja nostaa jonkin verran laitteen tulipaloriskiä.

2. Etäkäynnistys ja sammutus

Tietoturvan kannalta olisi paras, jos työasemaympäristö voitaisiin haluttaessa päivittää keskitetysti **JA** työasemat pitää pois päältä silloin, kun niitä ei käytetä. Keskitetyn päivitysmenettelyn kohdalla tähän voidaan päästä kahdella eri tavalla:

- Pyritään toteuttamaan päivitykset normaalina työaikana tai
- Etäkäynnistetään työasemat päivitystä varten iltaisin tai viikonloppuisin ja päivityksen jälkeen etäsammutetaan ne.

Tyypilliset tietoturvapäivitykset voidaan useimmissa työasemien hallintajärjestelmissä ja kirjautumisskripteissä asettaa asentumaan taustalle siten, ettei tästä aiheudu käyttäjälle kohtuutonta haittaa.

Jos kuitenkin organisaatio on hyvin laaja ja esimerkiksi tietoliikenneverkkojen kapasiteetin rajoitusten takia päivitysten asennus on hidasta ja aiheuttaa häiriöitä käyttäjille. Tällöin IT-asiantuntijat voivat etsiä ratkaisua työasemien **etäkäynnistyksestä**.

Liite 2, Energiatohokkuuden huomiointi työasemien ylläpidossa

Lähes kaikissa alle seitsemän vuotta vanhoissa työasemissa on mahdollisuus työasemien etäkäynnistykseen ns. **Wake On Lan (WOL)** –standardin mukaisesti.

Kun työaseman WOL-toiminnallisuus on asetettu päälle, lähiverkon pääkäyttäjällä on mahdollisuus keskitetysti aina tarvittaessa käynnistää pois päältä oleva työasema, tehdä siihen tarvittavat huoltotyöt ja lopuksi sammuttaa se. Tämä koko ketju voidaan automatisoida sopivilla työkaluilla.

Jotta WOL-etäkäynnistystä voi käyttää, on tehtävä seuraavat toimenpiteet:

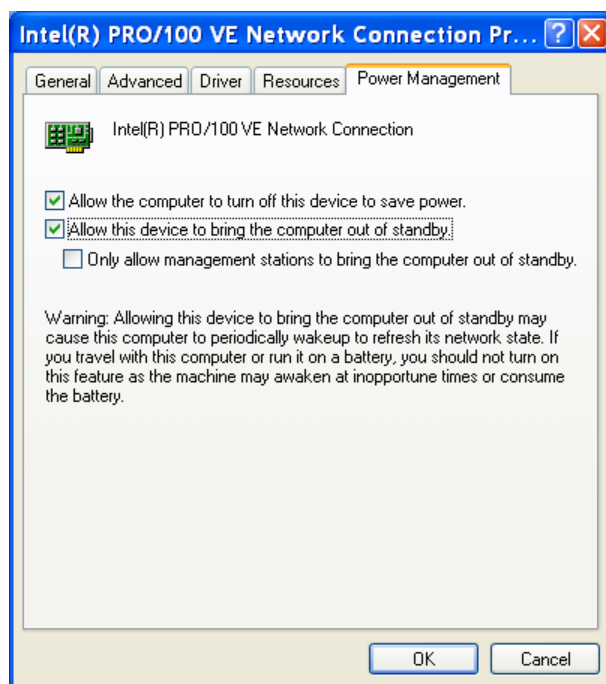
1. WOL-toiminnallisuus on asetettava päälle sekä työaseman BIOS-asetuksista että verkkoasetuksista. Tämä kannattaa jatkossa sisällyttää työasemavakioon
2. Jos työasemia halutaan hallita eri verkkosegmentistä, kuin missä työasemat sijaitsevat, tulee verkkosegmenttejä erottavat reitittimet ja palomuurit parametroida siten, että ne välittävät WOL-käynnistyspaketit oikein. Tämä edellyttää ns. SDB (Subnet Directed Broadcasts)-asetusten määrittämistä sekä luonnollisesti näiden tukea kyseisiltä verkon aktiivilaitteilta.
3. Työasemien verkkokorttien MAC-tunnukset tulee kerätä ja listata.
4. Itse käynnistämiseen tarvitaan vielä sitä tukeva ohjelmisto. Tätä tarkoitusta varten on toteutettu räätälöityjä omia sovelluksia. Näiden lisäksi keskeisimmät uudet työasemaympäristön hallintajärjestelmät tukevat WOL-käynnistystä.

2.1. Miten WOL oikein toimii, miten sen saa päälle?

WOL-ominaisuuden ollessa käytössä tietokoneen verkkokortti jää koneen ollessa pois päältä tarkkailemaan sille tulevaa verkkoliikennettä ja käynnistää koneen, mikäli havaitsee käynnistämiskomennon sisältävän ns. **taikapaketin** (eng. Magic Packet), jossa on verkkokortin oma MAC-osoite itse asiassa 16 kertaa toistettuna.

Taikapaketin lähetyksessä käytetään yhteydetöntä UDP-protokollaa.

WOL-toiminnallisuus ei verkkokortissa yleensä ole oletusarvoisesti päällä, vaan se joudutaan asettamaan erikseen. Sen saa päälle valitsemalla verkkoasetuksista lähiverkkoon liitetty verkkokortti ja valitsemalla tämän ominaisuuksien tehonhallintaa koskevasta välilehdestä kohta, jossa kortin sallitaan käynnistävän itse tietokoneen.



Verkkokortin lisäksi myös työaseman emolevyn ja virtalähteen tulee tukea WOL-toiminnallisuutta. Vanhemmissa laitteissa, mikäli verkkokorttia ei ole integroitu suoraan emolevylle, verkkokortin ja emolevyn väliin tulee kytkeä myös WOL-toiminnallisuuden mahdollistava kaapeli.

WOL-toiminnallisuus pitää usein asettaa päälle myös työaseman BIOS-määrittämisistä. Tämän toteuttaminen vaihtelee laitekohtaisesti.

Myös uusissa Apple Macintosh –tietokoneissa on tuki WOL-etäkäynnistykselle. Kaikkein uusimmissa käyttöjärjestelmäversioissa (Mac OS X Snow Leopard) tämä¹ on oletusarvoisesti päällä. Vanhemmissa käyttöjärjestelmäversioissa tämä asetetaan energiansäästöpaneelistä. Applen omaa Apple Remote Desktop –sovellusta voidaan käyttää hallinnoimaan ja lähettämään muita MACeja herättäviä taikapaketteja, mutta kuten Windows ja Linux-tietokoneille, myös Applen Macintosh –tietokoneille on useita vapaasti ladattavia kolmannen osapuolen sovelluksia vastaavaan tarkoitukseen.

1. Verkon aktiivilaitteiden asetukset

Jotta etäkäynnistyksen voisi tehdä keskitetysti eri verkkosegmentteihin, myös reitittimien ja palomuurien tulee tukea WOL-toiminnallisuutta. Useimmissa aktiivilaitteissa tämä on mahdollista, mutta ei välttämättä oletusasetuksilla. Esimerkiksi yleisesti käytettävien Ciscon reitittimien käyttöjärjestelmäversioita 12.0 lähtien WOL-etäkäynnistyksen edellyttämä toiminnallisuus on oletusarvoisesti estetty.

¹ Kyseisessä käyttöjärjestelmässä ominaisuuden nimi on Wake On Demand

Liite 2, Energiatohokkuuden huomiointi työasemien ylläpidossa

Eri reititinmallien WOL-asetusten asettaminen on laitekohtaista ja tästä saa parhaiten tietoa laitevalmistajien tukisivustoilta.

2. MAC-osoite

MAC-osoite on verkkosovittimen ethernet-verkossa yksilöivä osoite. Se on useimmiten fyysisesti kirjoitettu jo tehtaalla kortille. Osoite koostuu 12 heksadesimaalisesta numerosarjasta, joista ensimmäinen on valmistajan itselleen varaa etuliite ja jälkimmäinen juokseva sarjanumero. MAC-osoitteet ovat muotoa: XX-XX-XX-XX-XX-XX heksadesimaaleina.

Työasemien MAC-tunnukset kannattaa kirjata ylös jo työasemien asennuksen yhteydessä. Yleensä ne löytyvät myös laitekirjanpidosta.

Yksittäisen työaseman verkkokorttien MAC-osoitteet löytää Windows 2000 ja XP -ympäristössä kirjoittamalla komentoikkunassa `ipconfig /all`.

3. WOL-käynnistystä tukevat ohjelmistot

WOL-käynnistys tehdään toiselta työasemalta tai palvelimelta erillisellä tätä tukevalla sovelluksella. WOL-käynnistystä varten on kehitetty lukuisia kokonaisvaltaisia ja yksinkertaisempia ohjelmia. Osa näistä on kaupallisia, IT-ammattilaisille tarkoitettua ja osa vapaasti Internetistä ladattavissa. Osa on ilmaisia ja osaa voi kokeilla tyypillisesti 30 päivää ennen varsinaista ostopäätöstä. Esimerkkejä tällaisista ohjelmistoista löytyy seuraavien linkkien takaa:

- Kotimainen kattava hallintaohjelmisto:
http://www.greensnapper.fi/index.php?option=com_frontpage&Itemid=1&lang=fi
- <http://www.datasynergy.co.uk/products/wakeman/wolmanutility.aspx>
- <http://software.bootblock.co.uk/?id=wakeonlanex2>
- <http://www.depicus.com/wake-on-lan/wake-on-lan-gui.aspx>
- <http://www.gillit.com/wol>
- <http://www.macupdate.com/info.php/id/15779/wakeonlan>

Tyypillisistä työasemaympäristön keskitetyistä hallintajärjestelmistä kaikki merkittävimmät tuotteet pystyvät hyödyntämään WOL-etäkäynnistystä. Esimerkiksi Microsoftin System Centerin, IBM Tivolin, Symantec Altiris Client Management Suiten, LanDeskin Landesk Management Suiten sekä Novell Zenworksin uusimmat versiot tukevat kaikki WOL-etäkäynnistystä keskitetyksi hallittuna. Microsoftin toinen työasemaympäristöön laajasti käytetty tuote Microsoft SMS 2003 ei valitettavasti suoraan tue WOL-etäkäynnistystä, mutta siihen on saatavissa saumattomasti integroituvia kolmannen osapuolen lisäsovelluksia, joilla tämä tuki toteutetaan.

Myös monet lähiverkon hallintatyökalut tukevat WOL-toiminnallisuutta.

2.2. WOL-turvallisuus

WOL-toiminnallisuuden käyttöä on rajoittanut epäily sen turvallisuudesta. Keskeisin turvallisuusepäily koskee sitä, että sammutetussa tietokoneessa ei voida hyödyntää ns. korkeamman tason protokollia, kuten TCP/IP:tä, koska tämä protokollakerros ei ole kyseisessä tietokoneen tilassa päällä. WOL-kutsu lähetetäänkin ns. OSI-tason 2 datalinkkikerroksessa yleislähetysenä (broadcast) kaikille verkkokorteille. Tietokoneen herättävään ns. taikapakettiin kuvataan kuitenkin herätettävän tietokoneen MAC-osoite, joka on kaikille verkkokorteille yksilöllinen, joten yleislähetysenä lähetettävä herätekutsu ei luonnollisesti herätä kaikkia ko. verkkoon kuuluvia laitteita.

Tätä ohjetta varten haastateltujen tietoturva-asiantuntijoiden kommenttien perusteella WOL-toiminnallisuuden asettaminen työasemissa päälle ja oikein parametroituna verkon aktiivilaitteille **EI** lisää olennaisesti työasemaympäristön tietoturvariskejä. WOL-ratkaisun turvallisuutta voidaan perustella seuraavilla seikoilla:

- WOL-etäkäynnistys edellyttää, että käynnistettävän työaseman verkkokortin yksilöllinen tunniste, ns. MAC-osoite on käynnistävän tahon tiedossa
- WOL-käynnistykseen voi tehdä vain siitä lähiverkosta, jossa työasemakin on tai verkkoon erikseen määritellyn etähallintayhteyden kautta. Käynnistyneen koneen tietoturvasävy on siis sama kuin normaalistikin sen ollessa päällä kyseisessä verkossa
- WOL-käynnistämällä ei voi tehdä mitään muuta kuin käynnistää juuri tietty kone.
- Käynnistyessään työasema käyttäytyy, kuten siihen olisi kytketty virta virtakytkimestä. WOL-käynnistykseen yhteydessä ei vielä kirjauduta käyttöjärjestelmään sisään.
- WOL-toiminnallisuuden avulla ei voi ”nuuskia” verkossa olevien laitteiden osoitteita, sillä siinä käytetään ns. yhteydetöntä UDP protokollaa. Työasema ei kuittaa vastaanottamiaan käynnistyskomentoja.
- Vaikka joku taho saisikin toistaiseksi tuntemattomalla, kierolla tavalla työasemia käyntiin WOL-toiminnallisuudella, niiden tietoturva on tällöinkin huonoimmillaan samalla tasolla kuin työasemissa, joita pidetään jatkuvasti päällä.

Seuraavat linkit sisältävät englanninkielistä lisätietoa Wake On Lan – toiminnallisuudesta ja sen käyttöönnotosta.

- <http://en.wikipedia.org/wiki/Wake-on-LAN>
- <http://www.intel.com/support/network/sb/cs-008459.htm#2>

WOL-turvallisuutta parantavia lisäteknikoita

Laittevalmistajat ovat lähteneet kehittämään Wake On Lanin etäkäynnistysturvallisuutta eteenpäin lisäteknikoilla. Osa verkkokorttien valmistajista tukevat ns. ”SecureOn”-lisäteknikkaa. Siinä verkkokortille voidaan asettaa lyhyt muuttaman bitin heksadesimaalinen salasana. Tämän jälkeen kyseiseen verkkokorttiin voidaan antaa ulkoisia komentoja vain, jos tämä salasana tunnetaan. SecureOn –tekniikassa taikapakettiin liitetään kohdetietokoneen verkkokortin MAC-osoitteen lisäksi vielä kyseisen verkkokortin salasana. Kyseinen tietokone herää vain, jos sekä MAC-osoite että salasana ovat oikeita.

Joihinkin tietokoneisiin on jo BIOS-tasolle tehty lisämäärittämiä WOLin turvallisuuden parantamiseksi. Esimerkiksi Intelin vPro-tekniikkaan kuuluu ns. Intel AMT-komponentti, joka käyttää standardia TLS-turvatekniikkaa, jonka avulla etähallintakutsuille, kuten WOL, voidaan luoda oma turvattu kanava.

Nämä täydentävät turvatekniikat ovat varsin uusia, eikä niitä vielä valitettavasti tueta kovin laajasti.

3. Päivitysten kuukausikello

Ellei IT-asiantuntijoilla ole mahdollisuutta käyttää etäkäynnistysominaisuuksia eikä päivittää työasemia päivisin, kannattaa päivitykset kerätä tiettyihin kuukauden päiviin tai viikonloppuihin ns. **huoltoikkunoihin**. Suosittelemme käytettäväksi erityisesti Microsoftin käyttöjärjestelmillä varustetuissa työasemaympäristöissä kuukaudessa kahta huoltoikkunaa – toista Microsoftin kuukausittaisiin turvapäivityksiin ja toista muihin työasemaympäristön sovellusten päivityksiin. Kriittiset ja yllättävät päivitykset voidaan joutua jakelemaan näiden huoltoikkunoiden ulkopuolella, mutta tästä kannattaa joka tapauksessa tiedottaa erikseen.

Microsoftin turvapäivitykset julkistetaan joka kuukauden toinen tiistai. Näitä varten voidaan varata huoltoikkuna esimerkiksi seuraavan viikon tiistain ja keskiviikon väliselle yölle tai muuhun ajankohtaan siten, että IT-asiantuntijat ehtivät testaamaan päivitysten toimivuuden.

Muille sovelluskohtaisille päivityksille voidaan varata toinen huoltoikkuna esimerkiksi kuukauden ensimmäisen tiistain ja keskiviikon väliseen iltaan ja yöhön.

Tällä menettelyllä työasemat on työajan jälkeen jätettävä päälle vain kahtena tiistaina kuukaudessa. Muina päivinä työasemat suljetaan työpäivän jälkeen. Kun tämä käytäntö liitetään käyttäjäohjeeseen, koulutetaan käyttäjille ja siitä pidetään systemaattisesti kiinni, käyttäjät tottuvat tuttuun rytmiin melko nopeasti. Tällä menettelyllä parannetaan sekä työasemaympäristön tietoturvaa ja hallittavuutta että säästetään sähköä.

Tätä menettelyn noudattamista ja tehoa parantaa, jos työasematuki pystyy lähettämään sopivalla ohjelmistolla kuvaruutuviestin käyttäjien tietokoneisiin ennen huoltoikkunaa ja muistuttaa, että poikkeuksellisesti tänään on hyvä jät-

Liite 2, Energiatohokkuuden huomiointi työasemien ylläpidossa

tää työasemat päälle. Vaikka osa käyttäjistä rutiininomaisesti sammuttaisikin työasemansa huoltoikkunan aikana, suuri osa työasemista jätetään kyseisenä päivänä kuitenkin päälle ja voidaan päivittää normaalin työajan jälkeen. Ne koneet, joita ei muistettu jättää huoltoikkunan ajaksi päälle, voidaan hyvin todennäköisesti päivittää lähiverkon ruuhkautumatta seuraavana aamuna, koska iso osa työasemista on tällöin jo päivitetty.