

**Kun periaatteet on mietitty,  
on käytännön toimien  
aika tietoturvan  
vahvistamisessa.  
Suojaukset ja salaukset  
säädetään koneen  
kriittisyyden mukaan  
niin työpaikalla kuin kotona.**

**V**aikka tietokoneen arvokain osa on usein sen tietosisältö, varkaita voi kiinnostaa keskusyksikkö helposti myytävien komponentteineen.

Tämän takia kriittistä tietoa sisältävät koneet pitäisi lukita vajjerilla. Sama koskee kotikoneita ja etenkin kannettavia. Satunnainen varas valitsee kiiressä niitä koneita, jotka lähtevät helposti mukaan.

Työpaikalla kannattaa harkita omaisuuden turvamerkittämistä, jolloin varastettu omaisuus pystytään palauttamaan omistajalleen. Merkintä myös heikentää laitekoneisuuden kiinnostavuutta, koska varas joutuu myymään turvamerkityn laitteen komponentteittain.

**SETUP TORJUU  
ASIATTOMAT**

Vaikka sivullinen olisi syystä tai toisesta päässyt koneen ääreen, hän ei saa päästä käynnistämään konetta. Koneen biosin setup-määrittämisestä asetetaan käynnistyssalasana. Yrityskäytössä käynnistyssalasanana voi olla jopa yleisesti tunnettu, kunhan se on riittävän monimutkainen.

Setup-määrittysten muutta-

minen pitää suojata eri salasanalla kuin käynnistyssalasanalla. Kaikissa koneissa voidaan käyttää tähän samaa salasanaa, joka on vain tietohallinnon tiedossa.

Setupiin pääset napauttamalla koneen käynnistyksen yhteydessä ruudussa näkyvää näppäinyhdistelmää, esimerkiksi toimintanäppäintä F2 tai F12.

Mikäli setup mahdollistaa omistaja- ja muiden tietojen määrittämisen, kannattaa tiedot myös syöttää, koska ne näkyvät yleensä koneen käynnistyessä. Varastettu kone on siten helpompi palauttaa.

Setupista pitää vielä estää koneen käynnistyminen muilta kuin kiintolevyltä eli c-aseimalta. Jos kone päästään käynnistämään a-aseimalta, rompulta tai verkkokortin kautta, voidaan sen tietoturva murtaa krakkerointiohjelmilla.

Myös valmistajakohtaisiin suojaustoimintoihin kannattaa perehtyä.

**PITÄVÄT  
SALASANAT**

Jos asiaton kuitenkin saa koneen käyntiin, tietoturva on käyttäjien salasanojen sekä tiedostojen salauksen varassa. Salasanakäytäntöjä käsiteltiin MikroPC:ssä 3/2003 s. 55. Tär-

keintä on muuttaa sisäänrakennettujen tunnusten, kuten järjestelmänvalvojan, salasanat pois oletussanoista.

Yritysten toimialueilla tulee huolehtia tarkkaan siitä, ketkä käyttäjät kuuluvat toimialueen järjestelmänvalvoja- tai administrators -ryhmiin. Näiden käyttäjien salasanat ovat kriittisimpiä.

Käyttäjätunnistusta voidaan tehostaa melkoisesti erillisten toimikorttien avulla.

**LEVYN SALAAMISESSA  
ON RISKINSÄ**

Kaikkein luottamuksellisin tieto tulee suojata salakirjoittamalla se koneen kiintolevylle. Tällaiseen salaukseen käytettyä salausavainta tai erillistä salasanaa ei pystytä helposti

selvittämään.

Salakirjoitus voidaan toteuttaa joko Windows 2000/XP-käyttöjärjestelmien omalla encrypting file system (efs) tai kaupallisilla erikoisohjelmilla. Kaupalliset ohjelmat maksavat laajemmissakin lisenssimalleissa kohtalaisen paljon.

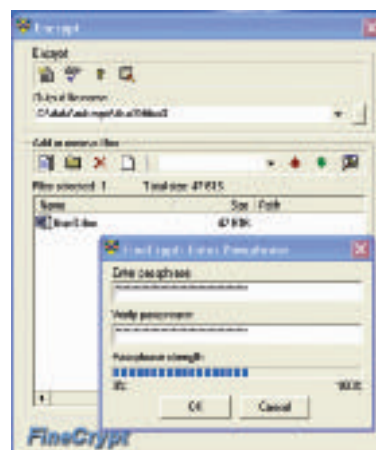
Salakirjoituksen käyttöönotto yrityksessä vaatii huolellista suunnittelua. Pitää miettiä, kuinka menetellään esimerkiksi jos käyttäjätunnus vahingossa poistetaan, sillä tällöin ei ole käyttäjätunnusta, jolla tiedostoihin pääsee. Efs tarjoaa palautusmahdollisuuden, mutta sen käyttö tulee huolella suunnitella ja myös harjoitella etukäteen.

Kotikäyttäjä voi efs:n avulla

◀ *Sataprosenttisen hankalan salasanan voi muodostaa jostain ulkoa muistettavasta virkkeestä, esimerkiksi Maamme-laulun pohjalta. FineCryptillä salattaessa alkuperäinen tiedosto jää edelleen levyllä, josta sen voi poistaa ohjelman Wipe-toiminnolla.*



# Työasema turvalliseksi



suojata tiedostot napauttamalla kansiota hiiren oikealla painikkeella ja valitsemalla Ominaisuudet|Lisäasetukset sekä "Suojaat tiedot salaamalla sisältö". Toiminto kannattaa kohdistaa koko kansiorakenteeseen.

Salattujen tiedostojen varmuuskopiointiin kannattaa kiinnittää erityistä huomiota, koska jos efs:n kanssa tulee ongelmia, ainoa keino palauttaa tiedostot on varmuuskopiot.

Lisätietoa efs:n käyttämisestä Windows 2000/XP:ssä löytyy artikkelisarjan www-sivujen linkkikokoelmasta.

Uusimmassa Office XP:ssä voi suojata tiedostot salasalla. Päinvastoin kuin aikaisemmissa Office-versioissa, näiden salasanojen murtamiseen ei löydy aivan heti internetistä apuohjelmaa.

Oletuksena tietoliikenne kulkee tcp/ip-protokollaa käytettäessä salaamattomana sekä yrityksen sisäverkossa että internetissä, paitsi sisäverkossa esimerkiksi käyttäjätunnukset ja salasanat sekä www-liikenteessä ssl-suojattu asiointi. Tietoliikenneyhteydet voivat olla suojattuja esimerkiksi ssh-suojauksella.

Yleensä yrityksen sisäverkossa tietoliikenteen salakirjoitukselle ei nähdä pakottavaa tarvetta. Riskianalyyssissä voi ilmetä tiettyjä työasemia ja palvelimia, joiden liikenteen suojaaminen onkin tärkeää.

Mikäli on tarve luottamukselliseen tietojenvälitykseen internetissä, yhteys rakennetaan useimmiten virtuaalilähiverkkona, vpn-tekniikoilla. Vpn:llä voidaan suojata myös sisäverkon liikennettä tai etäkäyttäjien yhteyksiä.

Jatkuvasti yleistyvien langattomien wlan-yhteyksien vpn-suojaus on suositeltava, paitsi jos halutaan nimenomaan suojaamaton yhteys

\$ %  
&'(' '\*+  
&),-



esimerkiksi yleisötilojen asiakaspäätteisiin.

Windows 2000/XP mahdollistaa tietoliikenteen suojaamisen IpSec-protokollalla työasemien ja palvelimien välillä. Myös IpSecin käyttöönotto vaatii tarkkaa suunnittelua ja testausta. Lisätietoa tästäkin löytyy sarjan linkkisivustosta.

Ensimmäisenä salattavana kohteena on useimmiten sähköposti. Yleisimpien (etenkin Microsoftin) sähköpostiohjelmistojen mukana ei tule helpposti toteutettavaa salaustointia.

Onneksi markkinoilla on muutama hyvin edullinen salaustavaihtoehto, joista suosituin on PGP (Pretty Good Privacy). Siitä voi hakea yksityiskäyttöön tarkoitettua ilmaisversion osoitteesta

. Valmistajalla on myös tuotteita kiintolevyn salakirjoitukseen (PGP Disk). Yksinkertaisempi ilmaisohjelma on FineCrypt, jonka voi ladata osoitteesta

Virustorjunnan yleisin puute on se, että torjuntaohjelmien päivitysväli on säädetty liian harvaksi. Torjunnan järjestämistä on käsitelty MikroPC:ssä 10/2002 s. 56. Peruskäyttäjän olisi hyvä oppia tarkistamaan, että virustentarkistusohjelma on päällä ja että sen versio on riittävän tuore.

Internetin ja yrityksen oman verkon välissä tulee olla joko ohjelmallinen tai laitepohjainen palomuuuri. Pelkkä reititin ei riitä. Kotikäytössä suosittelen ohjelmallisen palomuurin (ZoneAlarm tai vastaava) käyttämistä kaikissa internet-yhteyksissä, myös mo-

deemi- tai isdn-käytössä.

Mikäli kotona on useampi kone, voi vaivattomasti vaihtoehto olla erillinen palomuurilaite. Siinä olisi hyvä olla myös reititin, langattoman wlan-verkon tukiasema sekä muita keskeisiä verkkopalveluita. Laitteiden hinta on halvimmillaan alle 150 euroa.

Viimeisen vuoden aikana yleistyneet spyware- eli nuuskijahjelmistot pyrkivät selvittämään käyttäjän verkkokäyttäytymistä. Pahimmillaan ne edelleenlähettävät luottamuksellisia tiedostoja käyttäjän

koneelta.

Nuuskijoita voidaan etsiä samoilla periaatteilla kuin viruksia: etsimällä merkkijonoja, tunnettuja tiedostoja sekä rekisterimerkintöjä. Nuuskijoitakin on päivitettävä jatkuvasti. Tunnetuimpia torjuntajoukkoja ovat ilmainen SpyBot sekä AdAware, josta on olemassa myös maksulliset versiot.

Nykyisen roskapostin määrä voi jopa ylittää oikean sähköpostin määrän. Roskapostia voidaan torjua joko keskitetysti sähköpostin sisältötarkistuksella ennen kuin se tuodaan postipalvelimelle tai työaseman omalla sähköpostiohjelmalla. Edellinen tapa on tehokkaampi.

Roskapostia voidaan poimia otsikkoon ja viestin sisältöön liittyvien avainsanojen avulla. Useat roskapostiaajat välttävät filteeröinnin lähettämällä merkkijohjaisten sijasta grafiikka-



" . \* ,  
/  
0