



Varmista nopea toipuminen

Tietoturvassa keskitytään usein ennaltaehkäisyyn ja unohdetaan se, että mahdollisesta vahingosta pitää pystyä toipumaan nopeasti.

Vaikka tietoturva on kunnossa, vahinkoja saattaa tapahtua. Yritykselle on ensiarvoisen tärkeää, että toiminnan katkot jäävät mahdollisimman lyhyiksi.

Tämä tarkoittaa selkeitä toimintaohjeita ja dokumentaatiota: toipumissuunnitelmaa ja jatkuvuussuunnitelmaa.

Myös kotikäyttäjän ja yksittäiskäyttäjän kannattaa suunnitella toipuminen ennakkoon.

TIEDOT TURVAAN KESKITETYSTI

Käyttäjän omilla tiedostoilla pitää olla selkeä tallennuspaikka, joka varmuuskopioidaan asianmukaisesti. Muutoin esimerkiksi työaseman päivittäminen uuteen käyttöjärjestelmäversioon kloonaustekniikalla on hankalaa, koska datatiedostojen takuvarma talteenotto vaatisi koko koneen kopiointia, jotteivät vahingossa väärin paikkoihin tallennetut tiedostot häviä päivityksessä.

Mikäli datatiedostojen varmistaminen jää pelkästään

käyttäjän vastuulle, ongelmia syntyy varmasti. Tässä suositelen ehdottomasti keskitettyä, palvelimella toteutettua ratkaisua.

Kotikäyttäjälle paras apuväline on uudelleenkirjoittava cd-rw-asema ja isompia datatiedostoja käsiteltäessä kirjoitettava dvd-rw-asema.

Usb-muistikortti on uusi hyvä vaihtoehto, kunhan korttien kapasiteetti kasvaa riittä-

vän suureksi ja hinta laskee nykyisestä. Muistikorteissa on tietoturvaan liittyviä vaaroja, esimerkiksi kortti saattaa unohtua väärään koneeseen. Tämän takia korttien tietoturva- ja salasanaominaisuuksia kannattaa ehdottomasti käyttää.

KÄYTTÄJÄPROFIILI TAKAA TOIMINNAN

Jotta yrityksissä saadaan minimoitua esimerkiksi laiterikon tai käyttäjän virheiden aiheuttamat tuotantokatkot, tulisi kaikki data ja käyttäjään liittyvä tieto tallentaa palvelimille.

Keskeisessä asemassa on käyttäjäprofiili, joka sisältää käyttäjän sekä käyttöjärjestel-

mään että ohjelmiin liittyvät oletusasetukset. Sen lisäksi sekä työvälineohjelmilla tuotettavat datatiedostot että sähköposti olisi hyvä tallentaa palvelimille.

Käyttäjäprofiilia voidaan käyttää apuvälineenä ohjaamaan datan tallennus oikeisiin paikkoihin, mutta dataa ei saa tallentaa profiiliin. Muuten profiili kasvaa jopa satoihin megatavuihin ja verkkoon tai verkosta pois kirjautuminen kestää nopeassakin verkossa ärsyttävän kauan.

Kun käyttäjäprofiili sijaitsee palvelimella, se latautuu käyttäjän koneeseen joka kerta kun hän kirjautuu verkkoon. Kun hän kirjautuu ulos, profiili tallentuu taas palvelimelle mahdollisine muutoksineen. Jos käyttäjä kirjautuu verkkoon toisella työasemalla, hän saa profiilin avulla tutun työskentely-ympäristönsä.

Kun vielä sähköposti sijaitsee tietokannassa postipalvelimella, onkin kaikki keskeinen käyttäjään liittyvä tieto hallinnassa. Käyttäjä voi kirjautua vapaasti miltä tahansa lähiverkon työasemalta ja käyttöympäristö, data ja sähköposti ovat käytettävissä.

MITEN TOIVUTAAN VIRUSTAUDISTA?

Jos virus yrittää koneeseen sähköpostin liitetiedoston kautta, kannattaa viestin lähettäjälle tästä luonnollisesti ilmoittaa. Mikäli virus yrittää

Isot tiedostot varmasti talteen

- Tallenna tekemäsi työ talteen säännöllisesti ja eri nimillä (esimerkiksi 0205muistio001.doc, seuraavaksi 0205muistio002.doc jne) siltä varalta, että tiedoston rakenne särkyy ja sitä ei saa auki. Tällöin voit palata edelliseen toimivaan kopioon.
- Tallenna tekemäsi tiedostot säännöllisesti jollekin apumuistille tai työpaikallasi sinulle kerrottuun sijaintipaikkaan, josta ne varmuuskopioidaan säännöllisesti.
- Tarkista käyttämiesi ohjelmien automaattisen varmuuskopiointin tallennusväli ja muut tallennusasetukset. Automaattitallennus kannattaa asettaa tehtäväksi vähintään 10 minuutin välein, jos tallennus ei hidasta työskentelyä koneella.
- Vältä yhdistelemästä suoraan usealla eri ohjelmalla tehtyjä dataa. Siirrä ne esimerkiksi rtf-muotoisina tai leikepöydän kautta ja liitä ne kohdeohjelmaan Muokkaa | Liitä määräten -valinnalla käyttäen vaihtoehtoa "Muotoilematon Unicode-teksti". ■



~WP0452.doc	1 kt	Microsoft Word -ai...	1.5.2003 23:27
~CP974A.tmp	1 kt	TMP-tiedosto	1.5.2003 23:31
~CP95AD.tmp	1 kt	TMP-tiedosto	1.5.2003 23:39
~CP5124.tmp	1 kt	TMP-tiedosto	2.5.2003 7:14
~CP5144.tmp	1 kt	TMP-tiedosto	2.5.2003 7:14
~CP763C.tmp	1 kt	TMP-tiedosto	2.5.2003 7:28

\$ % &

!

"#

tarttua www-sivuston kautta, postia voi lähettää sivuston ylläpitäjälle. Tällöin kannattaa kertoa esimerkiksi löydety viruksen nimi, käyttämäsi torjuntaohjelma ja sen tarkempi päivitysversio sekä koneesi käyttöjärjestelmä.

Mikäli virus on omassa koneessasi ja saat muualta siitä ilmoituksen, ensimmäinen asia on estää sen edelleen leviäminen ja omien tiedostojesi mahdollinen vuotaminen maailmalle. Kotikäytössä tämä tarkoittaa internet-yhteyden katkaisemista. Modeemi- tai isdn-yhteys katkaistaan soitto-ohjelmasta. Laajakaistayhteys voidaan katkaista irrottamalla verkkokaapeli.

Yrityksessä käyttäjillä tulisi olla selkeät ohjeet, mitä tehdään, jos virustorjuntaohjelma rääkäisee viruksesta. Tietohallinnolla tulisi olla selkeä ohjeistus omaan toimintaan siltä varalta, että työasemiin tai lähiverkkoon pääsee leviämään esimerkiksi kokonaan uusi, aikaisemmin tuntematon tuholainen. On paljon helpompaa miettiä nuo asiat etukäteen kuin yrittää improvisoida paniikissa. On muistettava, että virus ehkä estää sähköpostin käytön tiedotusvälineenä.

Riippuu viruksesta, käyttöjärjestelmästä, saastuneiden koneiden lukumäärästä, inter-

net-yhteyden tyypistä ja lukuisista muista seikoista, kuinka virus saadaan poistettua.

Jos virus on erityisen ähräkä, pitää poisto-operaatio suunnitella huolella. Väärälaisella poistoyrityksellä saataan aiheuttaa lisävahinkoja. On tärkeä estää viruksen pääsy palvelimille ja myös pitää palvelimet puhtaina poisto-operaation ajan.

Tiedostojen hävittäminen on helppoa, valitaan tiedostot ja napautetaan Del-näppäintä – vai kuinka? Windows-järjestelmissä tiedosto siirtyy tässä vaiheessa yleensä vasta roskakoriin, josta se on helppo palauttaa. Kun olet tyhjentänyt roskakorin tai poistettaessa pidit vaihtonäppäintä pohjassa, tiedosto on turvallisesti poistettu – vai onko?

Ei ole. Ainoastaan levykijanpidossa tiedosto on merkitty poistetuksi, fyysisesti se on levypinnalla kunnes sen päälle kirjoitetaan jokin uusi tiedosto. Siten tiedosto voidaan parhaassa tai pahimmassa tapauksessa palauttaa jopa pitkien aikojen päästä.

Luottamuksellisten tiedostojen poistoon tai siirtoon kannattaa käyttää jotain erikoisohjelmaa, joka kirjoittaa vapautuvaan levykohtaan sa-

Nimi	Koko	Tyyppi	Muokattu
Application Data		Tiedostokansio	21.4.2003 20:13
Cookies		Tiedostokansio	2.5.2003 6:59
Käynnitysvalikko		Tiedostokansio	19.9.2002 12:04
Local Settings		Tiedostokansio	19.9.2002 12:04
Malli		Tiedostokansio	19.9.2002 12:04
Omist tiedostot		Tiedostokansio	2.5.2003 0:27
Start		Tiedostokansio	15.4.2003 16:16
Suodatt		Tiedostokansio	1.5.2003 17:48
Tuotantoprosessi		Tiedostokansio	19.9.2002 12:04
Työpöytä		Tiedostokansio	15.4.2003 16:30
Äänitied.		Tiedostokansio	17.4.2003 20:58
Tietokonekäyttö		Tiedostokansio	17.4.2003 21:36
Yksittäiset tiedostot		Tiedostokansio	2.5.2003 7:17
ntuser.dat	1 200 kt	DAT-tiedosto	25.4.2003 23:47
ntuser.dat.LOG	1 kt	Tekstitiedosto	2.5.2003 7:19
ntuser.ini	1 kt	Kokoonpanosuhteet	25.4.2003 23:47
ntuser.pol	1 kt	PCI-tiedosto	15.4.2003 9:40

tunnaisia merkkejä useaan kertaan. Jos joku yrittää tutkia levyntarkasteluohjelmilla entisen tiedoston sijaintikohtaa, ei hän saa siitä enää selkoa.

Joskus sattuu, että vahingossa poistettu tiedosto pitäisi pysyä palauttamaan. Jos tiedostoa ei ole hävitetty edellä kuvatulla tavalla tietoturvallisesti, voidaan käyttää netistä saatavia ohjelmia, jotka kykenevät tällaiseen undelete-toimintoon. Ne pystyvät palauttamaan tiedostoja myös tiedostopalvelimen levyiltä.

Mikäli esimerkiksi jokin Office-ohjelma on kaatunut niin, että käyttäjällä oli tallentamatonta tietoa, eikä ohjelman automaattinen varmuuskopiointi ole toiminut, kannattaa tutkia tilapäiset tie-

dostot sisältävä temp-kansio (joita voi olla useampikin), ohjelman oletustallennuskansio, c-aseman juurihakemisto sekä ohjelmassa määritetty automaattisen varmuuskopiointin kansio.

Jos näistä paikoista löytyy samana päivänä tehtyjä tiedostoja, ne kannattaa avata ja tutkia, vaikka niiden kolmikirjaiminen tiedostomääre olisi mikä tahansa. Jos häviksissä oleva tiedosto on erityisen tärkeä, kannattaa myös kokeilla tiedostojen palautusta undelete-ohjelmilla samoista sijainneista.

Temp-kansion sijainnin näet komentokehoteesta komentamalla set. Office-ohjelmien oletuskansioiden sijainnit saat tarkistetuksi valinnasta Työkalut|Asetukset|Oletuskansiot.