<KAINALOJUTTU Sepon verkkorekisterijuttuun>

Windows- ja viruspäivitysvaroituksia

Lokakuun 2005 puolivälistä alkaen tietotekniikkaosasto on ryhtynyt lähettämään työasemien vastuuhenkilöille sähköpostia Windows-korjauspäivityksistä huolehtivan WSUS-palvelun ja F-Securen virustorjunnan keskitetyn hallinnan havaitsemista ongelmista, kuten epäonnistuneista päivitysten asennuksista, löytyneistä viruksista ja ohjelmiston toimintahäiriöistä. Ilmoitukset eivät tarkoita, että viesteissä mainitut koneet olisivat aiheuttaneet verkossa häiriötä, vaan tiedotukset ovat lähinnä tukihenkilöille tarkoitettuja vihjeitä siitä, että asianomaisia koneita pitäisi tutkia lähemmin.

Raportteja lähetetään erikseen kummastakin palveluista kerran viikossa, jos hälytysarvot ylittyvät. Mahdollisesti jossakin suuremmassa virusepidemiatapauksessa saatetaan raportteja lähettää myös tämän normaalin viikkoaikataulun lisäksi.

Santtu Saastamoinen
Tietotekniikkaosasto

<ESIMERKKI>

WSUS-varoitusviestissä välitetään saatesanoin varustettuna seuraavanlainen raportti:

```
kone Last reported status: 25.9.2005 15:19:50
IP: 128.214.xxx.xxx

Koneen rekisteritiedot:
Nimi:            xxxx.xxxx.helsinki.fi
Ethernet-osoite: XXXXXXXXXXXX
IP-osoite:       128.214.xx.xx
Laitos:          xxxxx (A00000)
Rakennus:        xxxx, xxxx, xxxx (xxxxxx)
VLAN:            xxxxx <http://www.helsinki.fi/atk/yhteydet/verkko.html#xxxxx>
DHCP-ryhmä:      hki (hki=normaali, mobile=liikkuva kone)
Koneen tiedot:   xxxxxxxxxxxxxx
Viim. päivitys:  20001023-0817
Päivittäjä:      vastuuhenkilo@helsinki.fi

Seuraavissa WSUS-asennuksissa on tapahtunut virhe:
Update Rollup 1 for Windows 2000 Service Pack 4 (KB891861)
```

Vastaavasti virustorjunnan keskityn hallinnan havaitsemista ongelmista lähetetään seuraavanlainen raportti:

```
kone Windows XP 5.1 ID: xxxx
Antivirus version: 5.59
 : FSAVWK570-04,FSAVWK571-01,FSAVWK
 : 11390
Virus definitions version: 2005-11-01_01
Realtime scanning status: Enabled
Client Security version: 5.57
Automatic update agent version: 6.74
Firewall version: 5.74
Firewall securitylevel: 9iHYbasic
Last contact (management server): 1.11.2005 11:31:51 GMT
DNS NAME: xxxxx.xxx.helsinki.fi
```

IP: 128.214.xxx.xxx

Koneen rekisteritiedot:
Nimi: xxxxx.xxx.helsinki.fi
Ethernet-osoite: xxxxxxxxxxxx
IP-osoite: 128.214.xxx.xxx
Laitos: Xxxxxx (A00000)
Rakennus: Teollisuuskatu 23 (07701)
VLAN: xxxxx <http://www.helsinki.fi/atk/yhteydet/verkko.html#xxxxx>
DHCP-ryhmä: hki (hki=normaali, mobile=liikkuva kone)
Koneen tiedot: | xxxxx| xxxxxxxxxxxxxxxxx
Viim. päivitys: 20040713-1638
Päivittäjä: vastuuhenkilo@helsinki.fi

F-secure unique id: XXXX-XXXX-XXXX-XXXX

--ALERTS--
31.10.2005 13:31:39 GMT Infection found: EICAR_Test_File Action: Unspecified COUNT: 1

</ESIMERKKI>