205 Tietokoneet ja verkot: tietoturva
205 Computers and networks: data security

Kuvaus
Description

Yrityksen verkossa oleva Windows-palvelin ja -työasema tulee varustaa keskitetysti hallitulla F-Securen tietoturvaratkaisulla. Tarkoitukseen valitut tuotteet ovat seuraavat:

- hallintajärjestelmä F-Secure Policy Manager v. 10.00
- työasemaohjelmisto F-Secure Client Security v. 9.10
- palvelinohjelmisto F-Secure Anti-Virus for Windows Servers v. 9.00

The office IT environment (Windows workstation and server) shall be secured with centrally managed security solution developed by F-Secure. The selected products consist the following:

- centralized management solution F-Secure Policy Manager v. 10.00
- anti-virus solution for workstations F-Secure Client Security v. 9.10
- anti-virus solution for servers F-Secure Anti-Virus for Windows Servers v. 9.00

Ohjelmistot tarvittavine asennuskoodeineen on ladattu valmiiksi muistitikulle.

All programs with keycodes needed are available in usb stick

Käytettävissä oleva ohjelmistodokumentaatio on samassa jaossa kuin itse ohjelmistot.

All needed documentation can be found from the same location.

Hallintajärjestelmän asennus (3p)
Installing the central management solution (3p)

Windows-palvelimeen asennetaan F-Secure Policy Manager- hallintajärjestelmä.

F-Secure Policy Manager will be installed on Windows server.

1. Hallintapalvelimen työasemia ja palvelimia palvelevaksi portiksi asetetaan 81 oletusarvon sijasta. Hallintakonsolin palvelinportiksi asetetaan 8090 ja webraportoinnin palvelinportiksi 8091. Raportointipalveluun on päästävä mistä hyvänsä työasemasta. Policy Managerin ylläpitäjän salasanaksi valitaan F-Secure (1)

1. All managed workstations and servers should communicate with the central management server using port 81 instead of the default value. The management console communication port for the server should be set to 8090 and the port for web reporting interface to 8091. The Web reporting service should not be restricted from other sources than local address. (1)

2. Aseta työasemien pollausväliksi 30 sekuntia oletuksen sijaan, muista asettaa palvelimen osoite keskitettyyn hallintaan. (1)

2. The polling interval for all managed objects (workstations, servers) should be set to 30 seconds instead of default value. Do not forget set the server address for centralized management.(1)

3. Luo Policy Manageriin keskitetysti hallittavia työasemia ja palvelimia varten omat haarat hallintapuuhun. Huom: AD-importointi mahdollinen. Tallenna asetukset. (1)

3. Then create the necessary structure for managed workstations and servers into the policy management structure. Please observe that you may use the importing feature from the Active Directory (when available). Please do not forget to save the changes you made.(1)

Työaseman tietoturva-asetukset keskitetyssä hallinnassa (6p)
Security policies for centrally managed workstations (6p)

1. Palomuurisäännöt Office-profiiliin. Työasemiin voi ottaa yhteyttä etätyöpöytäohjelmalla (rdp). Vihje: Firewall Services sisältää valmiita määrityksiä eri käyttötarkoituksiin kuten palvelumäärityksen rdp:lle. (2)

1. Firewall rules in Office profile. Rdp are used for remote connections. Hint: there are several pre-configured services available for different purpose like remote control in Firewall Services section. (2)

2. Työasemien pitää voida jakaa levyä ja kirjoittimia ollessaan paikallisverkossa (lähiverkkomaskista käytetään nimitystä [myNetwork] palomuurisäännöstössä) (1)

2. In local office network (network mask naming convention as [myNetwork]) local disk sharing and printer sharing should be possible. (1)

3. Työasemissa otetaan käyttöön verkkokaranteeni, jos työasemien virustunnisteet ovat 10 päivää vanhempia. (1)

3. For security reasons the network quarantine will take effect if the virus definitions are older than 10 days in workstations trying to connect into company´s network. (1)

4. Käyttäjä ei saa kytkeä reaaliaikaista virustorjuntaa ja palomuuria pois päältä. (1)

4. For security reasons users are not allowed to switch off the real-time virus protection of firewall services.

5. Selaussuojauksen ja hakukonetulosten mainetarkistus on oltava päällä. (1)

5. The browsing protection and the reputation service for search engines and webmail must be switched on. (1)

Työasema-asennus (2p)
Installation on workstation (2p)

Työasemaan tulee asentaa F-Secure Client Security. Yrityksen mikrotuki haluaa, että ohjelmisto asennetaan esiasennettavana ja valmiiksi määritellyt tietoturva-asetukset sisältävänä msi-pakettina työasemaan. Paketin asennustapa on vapaasti valittavissa. (1)

The mighty IT has decided that all workstations should be installed with F-Secure Client Security configured as standard-based msi-package (with all pre-configured policy settings as described above). You can freely decide which installation method is suitable. (1)

Työasema liitetään Policy Managerin työasemahaaraan (1).

The workstation should be imported in appropriate path (workstation branch). (1)

Varmista, että työasema kommunikoi keskitettyyn hallintaan.

Please make sure that the communication between the workstation (Client Security) and Policy Manager Server works correctly.

Palvelinasennus (2p)

Installation on server (2p)

Palvelimeen tulee asentaa F-Secure Anti-Virus for Windows Servers manuaalisesti ja ohjelmiston tulee olla keskitetyssä hallinnassa. (1)

The next step is to install F-Secure Anti-Virus for Windows Servers manually and make it work with centralized management. (1)

Palvelin liitetään Policy Managerin palvelinhaaraan (1)

The server should be imported in appropriate path (server branch). (1)

Varmista, että palvelin kommunikoi keskitettyyn hallintaan.

Please make sure that the communication between the server (Anti-Virus for Windows Servers)) and Policy Manager Server works correctly.

Toiminnan varmistus (2p)
Functionality checklist (2p)

1. Mene työasemalla verkko-osoitteeseen eicar.org ja lataa sieltä eicar.com-testaustiedosto.
1. In workstation just browse to eicar.org and run eicar.com

2.Tee sama testi palvelimella käyttäen eicar.zip-tiedostoa
2. In server use eicar.zip instead

3. Mene työasemasta käsin F-Secure Web Reporting-palveluun ja jätä hälytysnäkymä auki (1/2)
3. In workstation open the Web Reporting service using the web browser, leave it open (1/2)

4. Jätä Policy Manager Console auki hälytysvälilehdeltä. (1/2)
4. Please leave the Alerts tab open in Policy Manager Console (1/2)

5. Lopuksi tarkista, että työasemassa ja palvelimessa on ajantasaiset tunnisteet, jätä käyttöliittymän lisäasetukset välilehti näkyviin (1)
5. The last one, please check that the virus definitions are up-to-date leaving the user interface advanced settings open both in workstation and server. (1)