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

Tehtävän yleinen osuus (1p)
General information

Yritys on hankkinut F-Secure Protection Service for Business-lisenssin. Ylläpitäjän tehtävänä on asentaa tietoturvaohjemistot työsemaan ja palvelimeen sekä ylläpitää ohjelmistojen tietoturva F-Securen pilvipohjaisen hallintaportaalin kautta (PSB)

Your company ordered F-Secure Protection Service for Business license for one Windows workstation and server. Your task is to install the software and maintain the security settings using cloud-based F-Secure administration portal (PSB)

Yrityksen hankkimat ohjelmistot ovat muistitikulla ja niiden hallinnointiin tarvittavat aktivointikoodit ovat erillisessä paperissa.

All the necessary software can be downloaded from the internet. Activation codes are located in a separate appendix.

HUOM.Kilpailijalla on käytössä yrityspostilaatikko jota käytetään tilin luomiseen. Yrityspostilaatikon salasana toimitetaan erillisessä liitteessä.
taitaja2015.xx@yrityspostilaatikko.fi (xx=kilpailijan numero)

NOTE! You have a business mailbox which is used to create the account. Business mailbox password is provided in a separate appendix.
taitaja2015.xx@yrityspostilaatikko.fi (xx=competitor number)

Hallintaportaalin osoite on:
The portal address is:
https://psb-live.sp.f-secure.com

Perustoimenpiteet:
Basic actions:

1. Ylläpitäjä määrittelee yrityksensä tiedot portaaliin
   Vaaditut tiedot ovat:
   - yrityksen nimi eli Taitaja_xx
   - käyttäjätunnus Taitaja_xx
   - salasana Taitaja_xx
   - käyttäjätunnuksena käytettävä sähköpostiosoite

   The administrator defines all necessary company information in portal
   Required information consists of:
   - company name Taitaja_xx
   - username Taitaja_xx
   - password Taitaja_xx
   - the email address as accounts username

2. Asentaa työasemaohjelmiston (PSB for Workstations), varmistaa päivitysten toimivuuden (kommunikointi toimii portaalin kanssa)

   Installs the workstation software (PSB for Workstations), ensures that updates are working (communication works between the client and the portal)

Työaseman tietoturva-asetukset (7p)
Security policies for workstations (7p)

3. Palomuurisäännöt tehdään perustuen Open Office-profiiliin (nimeä uusi profiili Office_rdp_share). Työasemiin voi ottaa yhteyttä etätyöpöytäohjelmalla (rdp).

   Firewall rules will be defined using Open Office profile (new profile named as Office_rdp_share). Rdp are used for remote connections.

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

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

5. Määrittele luomasi profiili oletukseksi käyttöön yrityksen työasemissa.

   Configure the profile you created as a default for the company's workstations.

6. Käyttäjä ei saa kytkeä reaaliaikaista virustorjuntaa ja palomuuria pois päältä.

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

7. Selaussuojauksen ja hakukonetulosten mainetarkistus on oltava päällä, lisäksi käyttäjä ei saa päästä estetyille sivuille

   The browsing protection and the reputation service for search engines and webmail must be switched on, the user not allowed to continue to blocked pages

8. Määrittele, että Software Updater asentaa puuttuvat kriittiset ja tärkeät päivitykset päivittäin klo 14.

   Define that Software Updater installs missing critical and important updates daily at 2pm.

9. Määrittele, että windows backup prosessi (wbadmin.exe) poissuljetaan reaaliaikaisesta tarkistuksesta.

   Define that windows backup process (wbadmin.exe)is excluded from real-time scanning.

10. Määritä, että virushälytyksistä lähtee sähköposti osoitteeseen taitaja2015.alert@yrityspostilaatikko.fi

    Define that virus alerts are delivered to email address taitaja2015.alert@yrityspostilaatikko.fi

11. Lisää http://ict-academy.fi luotetuiksi sivuiksi Internet selainsuojaukseen

    Add http://ict-academy.fi as a trusted site to Internet browsing protection

12. Asenna host palvelimeen F-secure asiakasohjelmisto

    Install F-secure client to the host server

13. Määrittele sovellushallinta kysymään aina uusista sovelluksista

    Configure application control to always ask about new software

14. Luo työaseman työpöydälle kansio "Tools" ja sinne PowerShell skripti, joka sammuttaa F-securen palvelut käytöstä väliaikaisesti. Luo myös PowerShell skripti joka käynnistää palvelut. Varmista, että käyttäjän pitää vain tupla-klikata kuvaketta.

    Create a folder named "Tools" to the workstations desktop and inside the folder two PowerShell scripts. One script which stops the f-secure and other that starts the f-secure. Ensure that the user only needs to double click the shortcut.

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

1. Mene työasemalla verkko-osoitteeseen eicar.org ja lataa sieltä eicar.com-testaustiedosto.

   In workstation just browse to eicar.org and run eicar.com

2. Jätä portaali auki profiilieditorin tartunnat-välilehdellä.

   Please leave the portals Infections-tab opened

   Lopuksi tarkista, että työasemassa ja palvelimessa on ajantasaiset tunnisteet, jätä käyttöliittymän lisäasetukset välilehti näkyviin

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.

Muista, että työaseman pollaus hallintaan on oletuksena 60 minuuttia. Pollauksen voi myös tehdä käsin.

Please remember that the default polling interval between the client and portal is 60 minutes. Polling can be done also manually.