WINDOWS-TYÖASEMAN JA REITITTIMEN SUOJAUS PÄIVITYKSILLÄ JA OHJELMISTOILLA

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Kyberuhkien hallinta- ja suojautumiskeinona Windows-työasema suojataan päivityksillä ja ohjelmistoilla. Windows-työasema päivitetään Windows Updaten kautta ja tarkistetaan päivitykset manuaalisesti (OpenAI, 2025). Otetaan automaattiset päivitykset käyttöön ja varmistetaan, että päivitysten asennusaikataulu on asetettu sopivaksi. Tarkistetaan myös valinnaiset päivitykset, jotka voivat sisältää ajuri- ja ominaisuuspäivityksiä.

Ajurien ja laiteohjelmistojen päivittämisessä käytetään laitehallintaa sen tarkistukseen, tarvitseeko jokin laite päivitettyjä ajureita (OpenAI, 2025). Ajurit voidaan ladata laitevalmistajan verkkosivustolta, jos Windows Update ei tarjoa niitä. UEFI:n päivitystä ei voi tehdä virtuaalikoneessa, koska sen UEFI on osa hypervisor-ohjelmistoa. Fyysisessä laitteessa viimeisin päivitystiedosto ladattaisiin valmistajan sivuilta (Mikrobitti, 2025). Windows-koneella yleensä vain käynnistetään asennus ja sen jälkeen kone käynnistetään uudelleen.

Työasema voidaan suojata haittaohjelmien torjuntasovelluksilla kuten WithSecure ja Windows Defender sekä palomuureilla, jotka konfiguroidaan yrityksen tietoturvakäytänteiden mukaan. Varmistetaan, että Windows Defender on käytössä ja ajan tasalla (OpenAI, 2025). Tämä hoituu

Windowsin asetusten kautta. Suoritetaan täysi järjestelmätarkistus mahdollisten haittaohjelmien löytämiseksi. Varmistetaan, että palomuuri on käytössä ja konfiguroidaan sen säännöt tarvittaessa sallimaan vain tarpeellinen liikenne.

2 Ympäristö

Windows-työasemana käytetään wks1win10_22H2_x64-virtuaalikonetta win10-physio VMware Workstation Pro 17 -ohjelmassa. Koneesta tehtiin heti snapshot (Snapshot 1) ennen avaamista. Muistia on 4 GB, prosessoreita on 4, kovalevyn (NVMe) koko on 60 GB ja verkkoadapteri on NAT. Koneen käyttäjätunnus on ”asennus” ja salanasana ”asennus”. VMware Toolsit päivitettiin heti.

3 Päivitykset

3.1 Windows Update

Windows-työasema päivitettiin Windows-updaten kautta (Asetukset > Päivitykset ja suojaus > Windows Update) ja käynnistettiin uudelleen. Päivitykset on listattu Kuva 1. Otettiin käyttöön asetus ”Hanki uusimmat päivitykset heti, kun ne ovet käytettävissä” (Kuva 2). Valinnaisissa päivityksissä oli Broadcom Inc.:in Display 9.17.9.4. -ohjainpäivitys, joka ladattiin ja asennettiin. Koneesta otettiin snapshot ”20250125” ja kone varmuuskopioitiin OneDriveen ja ulkoiselle kovalevylle.

Kuva 1. Windows-työaseman päivitykset Windows-updaten kautta.

Kuva 2. Asetus ”Hanki uusimmat päivitykset heti, kun ne ovet käytettävissä” käytössä.

3.2 Ajurit

Laitehallinnasta tarkistettiin, tarvitseeko jokin laite ajureiden päivitystä. Päivitettiin Tietoliikenneportin (COM1) ajurit etsimällä ohjaimia automaattisesti. Ei käyty läpi kaikkia järjestelmälaitteet-kohdan Generic Bus - ja PCI Express -pääporttilaitteita.

3.3 Laiteohjelmistot

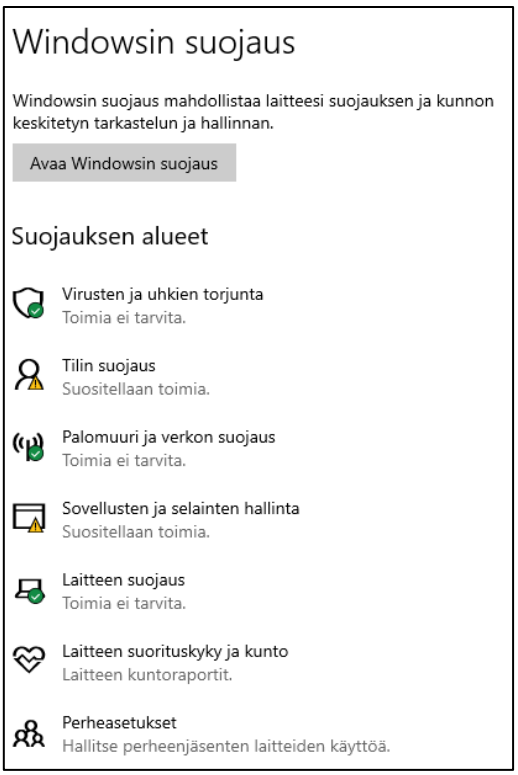
Tarkistettiin joitain laitteita valmistajan verkkosivustolta uusien versioiden varalta. Verkkosovittimelle ei löydy uutta versiota eikä myöskään emolevylle (Intel, 2015).

Reitittimen laiteohjelmisto päivitettiin reitittimen verkkosivun http://192.168.1.1/FirmwareUpgrade #maintenance kautta (Maintenance > Firmware Upgrade). Uusin versio ladattiin Zyxelin verkkosivulta (Zyxel Networks, 2024).

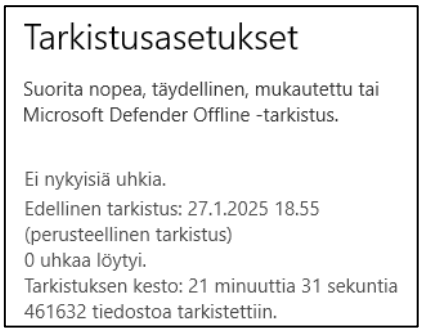
4 Ohjelmistot

4.1 Windowsin suojaus

Työasema on automaattisesti suojattu Microsoftin virustorjunta- ja tietoturvaohjelmistolla Windowsin suojaus. Varmistettiin, että se on käytössä ja ajan tasalla Windowsin asetusten kautta (Asetukset > Päivittäminen ja suojaus > Windowsin suojaus (OpenAI, 2025). Kuva 3 mukaisesti virusten ja uhkien torjunta, palomuuri ja verkon suojaus sekä laitteen suojaus olivat kunnossa. Toimia suositeltiin tilin suojauksessa sekä sovellusten ja selainten hallinnassa, joista jälkimmäinen otettiin käyttöön. Suoritettiin Virusten ja uhkien torjunta -kohdassa perusteellinen tarkistus, jossa ei löytynyt uhkia (Kuva 4).



Kuva 3. Windowsin suojaus ennen Sovellusten ja selainten hallinnan käyttöönottoa.



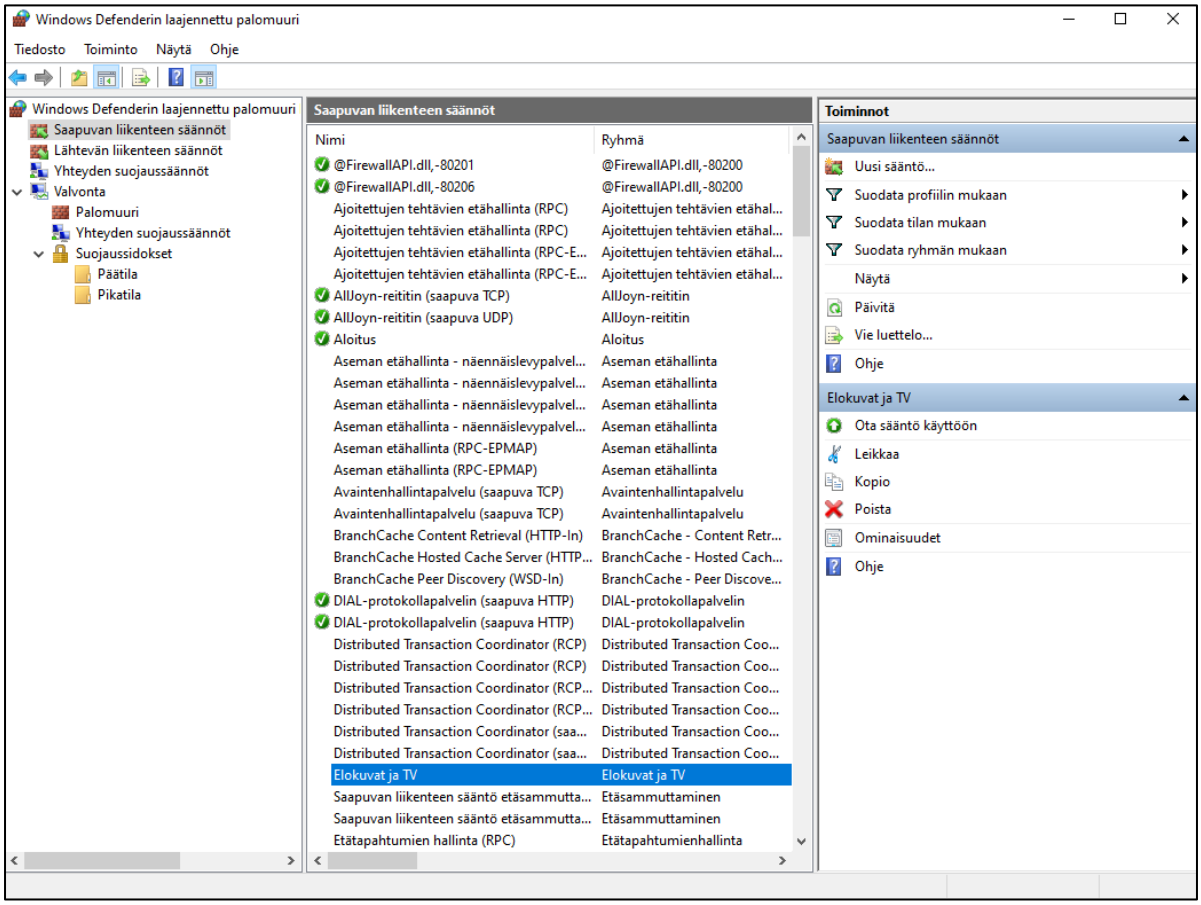
Kuva 4. Virusten ja uhkien torjunta -kohdan perusteellisen tarkistuksen tulos.

4.2 Windowsin palomuuri

Yrityksellä ei ole vielä tässä vaiheessa tietoturvakäytänteitä, joten perehdyttiin yleisesti Windowsin palomuuriin (Microsoft, Windows Firewall overview, 2025) ja tutustuttiin sen asetuksiin (Asetukset > Päivittäminen ja suojaus > Windowsin suojaus > Palomuuri ja verkon suojaus). Windowsin palomuuri on mukana käyttöjärjestelmässä ja oletuksena päällä sekä tukee IP-suojausta (IPsec). Se suodattaa lähtevää ja tulevaa verkkoliikennettä mm. IP-osoitteen ja -protokollan sekä porttinumeroiden mukaan. Se voidaan konfiguroida suodattamaan liikennettä koneeseen asennettujen palveluihin ja ohjelmiin pohjautuen. Suojausasetukset riippuvat verkon profiilista eli siitä, onko verkko yksityinen, julkinen vai toimialueverkko. Oletuksena palomuuri estää kaiken paitsi pyydetyn tai säännön salliman tulevan liikenteen ja sallii kaiken paitsi säännön kieltävän lähtevän liikenteen.

Suositus on, että säilytetään palomuurin oletusasetukset aina, kun mahdollista (Microsoft, Windows Firewall rules, 2025). Usein ensimmäisenä muokataan palomuurin profiileja käyttämällä sääntöjä esimerkiksi ohjelman sallimiseksi. Sääntö kannattaa luoda jokaiselle profiilille, mutta ottaa käyttöön vain siinä, jossa sitä tarvitaan. Tulevan liikenteen sääntöjä luodessa kannattaa olla täsmällinen. Säännöt kannattaa dokumentoida hyvin.

Windows palomuuri voidaan kofiguroida eri työkaluilla, kuten Windowsin suojaus (Palomuuri ja verkon suojaus), Ohjauspaneeli (Järjestelmä ja suojaus > Windows Defenderin palomuuri tai firewall.cpl), Windows Defenderin laajennettu palomuuri (Palomuuri ja verkon suojaus > Lisäasetukset tai wf.msc), komentorivityökalut ja Configuration Service Provider (CSP) (Microsoft, Windows Firewall tools, 2025). Aktiivisessa hyökkäyksessä voidaan käyttää Shield Up -tilaa (Palomuuri ja verkon suojaus > Yksityinen/Julkinen verkko tai Toimialueverkko > Saapuvat yhteydet), jossa estetään kaikki saapuvat yhteydet.



Kuva 5. Saapuvan liikenteen sääntöjä Windows Defenderin laajennettu palomuuri -työkalussa.

Poistettiin käytöstä saapuvan ja lähtevät liikenteen sallivat säännöt Elokuvat ja TV (Microsoft Zune Video -sovelluspaketti) ja Game Bar (Microsoft Xbox Gaming Overlay -sovelluspaketti) Windows Defenderin laajennettu palomuuri -työkalulla (Kuva 5). Otettiin snapshot ”20250128” ja varmuuskopioitiin virtuaalikone ulkoiselle kovalevylle.

Lähdeluettelo

Intel. (27. Tammikuu 2015). *Download Drivers & Software*. Noudettu osoitteesta https://www.intel.com/content/www/us/en/download-center/home.html

Microsoft. (28. Tammikuu 2025). *Windows Firewall overview*. Noudettu osoitteesta https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/

Microsoft. (28. Tammikuu 2025). *Windows Firewall rules*. Noudettu osoitteesta https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/rules

Microsoft. (28. Tammikuu 2025). *Windows Firewall tools*. Noudettu osoitteesta https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/tools

Mikrobitti. (27. Tammikuu 2025). *Opas: Uefi-ohjelmiston päivittäminen tekee tietokoneesta turvallisemman, vakaamman ja nopeamman*. Noudettu osoitteesta https://www.mikrobitti.fi/neuvot/opas-uefi-ohjelmiston-paivittaminen-tekee-tietokoneesta-turvallisemman-vakaamman-ja-nopeamman

OpenAI. (20. Tammikuu 2025). *ChatGPT*. Noudettu osoitteesta https://chatgpt.com/

Zyxel Networks. (22. Tammikuu 2024). *Zyxel CPE Devices [Firmware] - Advanced Downloads Firmwares and other resources*. Noudettu osoitteesta https://support.zyxel.eu/hc/en-us/articles/4403361365778-Zyxel-CPE-Devices-Firmware-Advanced-Downloads-Firmwares-and-other-resources