2021

Kannettavan tietokoneen salaus

JULKUNEN NOA

Sisällys

Laitteen fyysinen suojaus

Kaikki keinot, jotka estävät ilkivaltaa, ovat fyysistä tietoturvallisuutta. Erilaisia suojauskeinoja on esimerkiksi kulunvalvonta, kameravalvonta, lukitusjärjestelmä ja vartiontipalvelut. Myös turva-alueet lisäävät fyysistä tietoturvallisuutta > tiettyyn huoneeseen ei ole vapaa pääsy jokaisella. Myös datan tallennuspaikka on fyysistä turvallisuutta, mihin tiedot tallennetaan, onko tallennuspaikka fyysisesti varastettavissa

Local admin GPO-asetukset

Local administrator asetuksien avulla voidaan ehkäistä muiden käyttäjätunnusten käyttämisen tietokoneella taikka estää yhteyden tietokoneeseen internetin kautta. Yleisesti GPO – asetuksia käytetään rajoittamaan tietokoneelle pääsyä, joka tekee siitä turvallisemman.

Käyttäjäkirjautumisen rajoittaminen

Kun tietokoneen käyttäjiä rajoitetaan, paranee tietoturva. Tietoturvaa voi parantaa entisestään lukitsemalla tilin tietyksi ajaksi, jos salasana kirjoitetaan monesti väärin. Myös kirjautumisajan rajoittaminen parantaa tietoturvaa, ettei esimerkiksi yöllä voi käyttää tietokonetta.

Bios-asetukset ja tietoturva

Biosin asetuksia voi muuttaa tietoturvallisempaan suuntaan esimerkiksi lisäämällä BIOSIN käyttöä varten salasanan, jotta henkilöt joilla ei ole oikeutta käyttää konetta ei pääse muuttamaan muita asetuksia. Myös tietokoneen käynnistymisen ulkoisilta käynnistysasemilta voi rajoittaa BIOSIN kautta. (Boot device priority > tietokone käynnistyy oikealta levyltä automaattisesti)

Kryptaus ja salakirjoittaminen

Kiintolevyn salaus estää tietojen päätymistä vääriin käsiin, jos kone päätyisi vääriin käsiin. Jos levyn kytkee toiseen laitteeseen, tarvitsee se silti salauksen purkamista / salasanaa jotta tietoihin voi päästä käsiks.

Levyosiointi

Jos tietokoneen levyn osioi eri osiin, on siitä monia hyötyjä kuten parempi turvallisuus jos haittaohjelma pääsee Windows – osioon (levyosio missä windows on) se ei pääse tietoihin käsiksi jotka ovat toisessa osiossa. Myös helppokäyttöisyys ja järjesetelmällisyys, helpompi varmuuskopioida koko levy kuin koko tietokone valiten tiedostot jotka haluaa varmuuskopioida. Toisaalta useampi levyosionti voi viedä turhaa tilaa.

Remote wipe

Tietokoneen joutuessa varastetuksi voi sen sisällön pyyhkiä pois toiselta tietokoneelta, jolloin varas ei hyödy sen sisällöstä. Microsoft tarjoaa Microsoft Intunen jonka avulla toimenpiteen voi suorittaa. On myös sovelluksia kuten Prey, joka tekee saman.

VPN ja tietoliikenteen suojaus

VPN piilottaa oman ip – osoitteen ja salaa datan, joka liikkuu julkisessa verkossa. Ottamalla asetuksen ”Use a proxy server for your LAN” käyttöön, tekee tietokoneen käytöstä turvallisemman julkisissa verkoissa.

Security baseline for Windows 10

Security baseline for Windows on .zip paketti, jonka voi ladata microsoftin sivuilta. Paketin idea on muokkaa muokkaa järjestelmäasetuksia turvallisemmaksi. Sen tarkoitus on myös paljastaa alueita ympäristöstä, jotka eivät ole turvallisia.

Lähteet

https://blog.seclion.fi/turvallisuus/fyysinen-tietoturvallisuus

https://www.theseus.fi/bitstream/handle/10024/11928/2007-12-03-18.pdf;jsessionid=CE992E76A4A508DE9E6CC3AF8CBE35FD?sequence=1

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-h--securing-local-administrator-accounts-and-groups

https://www.tomshardware.com/reviews/bios-beginners,1126-10.html

https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-wstation-boot-sec.html

https://personaldatasecurity.wordpress.com/windows-10-kovalevyn-salaus/

https://fi.wikipedia.org/wiki/Kiintolevyn_osiointi

https://searchmobilecomputing.techtarget.com/definition/remote-wipe

https://www.thewindowsclub.com/remote-wipe-windows-10

https://www.globalsign.com/en/blog/staying-safe-using-public-wifi

https://systemcenterdudes.com/how-to-use-the-windows-10-security-baseline/