Tallennusvälineiden tyhjennys ja uusiokäyttö

Sisällys

1 Ohjeen tausta ja tarkoitus

Liikenne- ja viestintävirasto Traficomin tehtäviin kuuluvista tietojärjestelmien arvioinneista ja hyväksynnistä säädetään laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004, kv-titulaki), turvallisuusselvityslaissa (706/2014) ja laissa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista (1406/2011, arviointilaki).

Kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti esimerkiksi EU:n ja Naton turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien tulee läpikäydä hyväksyntäprosessi (akkreditointi). Kansallista turvallisuusluokiteltua tietoa käsitteleviin viranomaisten tietojärjestelmiin ei kohdistu lainsäädännöstä yleistä velvoitetta tietojärjestelmän hyväksynnälle (akkreditoinnille). Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, tiedonhallintalaki) mukaisesti viranomaisen tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Viranomaisen tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti (13 §). Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) mukaisesti tarpeettomaksi käynyt turvallisuusluokiteltu asiakirja on tuhottava tavalla, jolla kyseiselle turvallisuusluokalle riittävän luotettavasti estetään tietojen palauttaminen sekä kokoaminen uudelleen kokonaan tai osittain (15 §).

Tämän ohjeen tarkoituksena on tukea organisaatioiden riskienhallintaa turvallisuusluokiteltua tietoa sisältävien tallennusvälineiden tyhjennyksessä ja uusiokäytössä. Ohjetta voidaan hyödyntää myös muun salassa pidettävän tiedon suojaamiseen. Ohjeessa kuvataan yleisimmät edellytykset tallennusmedioiden luotettavaan, todennettavissa olevaan tyhjennykseen ja uusiokäyttöön. Ohjeessa käsitellään myös sellaisia tyhjennysmenetelmiä, joiden todennettavuudessa on oleellisia puutteita ja joiden käyttöön liittyy vain osin hallittavissa olevia riskejä.

2 Määritelmät

- *Kiintolevyllä* tarkoitetaan tässä ohjeessa tietokoneen kiintolevyväylään (SATA, PATA, SCSI, SAS, M.2 ja vastaavat)[1] kytkettävää massamuistia.
- *Magneettisella kiintolevyllä* tarkoitetaan tässä ohjeessa magneettisella aineella päällystetyn levyn ja lukupään muodostamaa kiintolevyä.
- *SSD-kiintolevyllä* (solid-state drive) tarkoitetaan tässä ohjeessa datan pysyväisluontoisesti mikropiireille tallentavaa kiintolevyä.
- *Yhdistelmäkiintolevyllä* (hybrid hard drive) tarkoitetaan tässä ohjeessa perinteisen magneettisen ja esimerkiksi SSD-kiintolevytekniikan yhdistävää kiintolevyä.
- *Komentokielellä* tarkoitetaan käskykantaa, jota käytetään kiintolevyjen ja muiden tallennuslaitteiden ohjaamiseen (esim. ATA, SCSI tai NVMe)
- *Integroiduilla muistipiireillä* tarkoitetaan tässä ohjeessa yksittäisiä pysyvään tallennukseen tarkoitettuja laitteeseen integroituja eMMC-, NAND- ja UFS-muistipiirejä. Tällaisia muisteja käytetään joissakin kannettavissa, mobiililaitteissa, reitittimissä yms.

[1] USB-väylä ei tässä sisälly kiintolevyväylän määritelmään.

- *Tallennusvälineellä* tarkoitetaan tässä ohjeessa magneettisia kiintolevyjä, SSD-kiintolevyjä, integroituja muistipiirejä, muistikortteja sekä USB-muistitikkuja.
- *Isäntälaitteella* tarkoitetaan sitä laitetta, johon tallennusväline on fyysisesti kytketty kiinni.
- *Tyhjennyksellä* tarkoitetaan tässä ohjeessa tiedon hävittämistä tietokoneen kiintolevyltä tai muulta tallennusvälineeltä siten, että sen palauttaminen olisi kannattamatonta käytettävät resurssit huomioon ottaen.
- *Kiintolevyn tai muun tallennusvälineen elinkaarella* tarkoitetaan tässä ohjeessa aikaa kiintolevyn tai muun tallennusvälineen ensimmäisestä käyttöönotosta sen luotettavaan fyysiseen tuhoamiseen. Toisin sanottuna tyhjennys ei katkaise kiintolevyn tai muun tallennusvälineen elinkaarta.
- *Organisaatiolla* tarkoitetaan tässä ohjeessa tahoa (tiedon haltijaa), jonka hallussa tietoa sisältävä kiintolevy tiedon luovuttaneen viranomaisen valtuuttamana on.
- *Näkyvällä kapasiteetilla* tarkoitetaan tässä ohjeessa kiintolevyn täyttä käytettävissä olevaa kapasiteettia[2]. Näkyvä kapasiteetti sisältää myös mahdolliset HPA (Host Protected Area), DCO (Device Configuration Overlay), ja muilla vastaavilla toiminnoilla piilotetut alueet.
- *Kiintolevyn salauksella* tarkoitetaan tässä ohjeessa koko kiintolevyn[3] salausta yleisesti luotettavana pidetyllä menetelmällä, kuten LUKS-, Veracrypt- taikka Bitlocker-ohjelmistolla. Kiintolevyohjaimen tekemää salausta ei tässä ohjeessa tulkita yleisesti luotettavaksi[4].

3 Ohjeen kattavuus

Tämä ohje kattaa pysyväisluonteisesti tietoa tallentavia tallennusvälineitä, joissa tyhjennys voidaan luotettavasti todentaa, kuten:

- Magneettiset kiintolevyt
- NAND-muistitekniikkaan perustuvat SSD-kiintolevyt

Riskienhallintapohjaisesti käytettävät tyhjennysmenetelmät kattavat myös:

- Laitteiden sisältämät integroidut, pidempiaikaiseen tallennukseen tarkoitetut eMMC-, UFS- ja NAND-muistipiirit.
- USB-muistitikut
- Muistikortit (SD, miniSD, microSD, SDHC, MMC yms.)
- Mobiililaitteet

Tämä ohje ei käsittele jatkuvaa virransyöttöä vaativan väliaikaisen muistin tyhjennystä (kuten SRAM taikka DRAM), optisia medioita (CD-, DVD- ja BD-levyt), magneettisia nauhoja (LTO ja vastaavat) taikka levykkeitä.

[2] Käyttäjän kohdistettavissa olevat muistialueet.
[3] Pois luettuna mahdollisesti järjestelmän käynnistymisen vaatima lyhyt selväkielinen osa.
[4] Kiintolevykontrollerien tekemien salausten implementaatiot voivat poiketa toisistaan, ja voivat sisältää heikkouksia.

4 Todennettavissa olevat tyhjennysmenetelmät

Todennettavissa olevat tyhjennysmenetelmät ovat menetelmiä, joissa tyhjennyksen onnistuminen voidaan todentaa. Todennuksen voi suorittaa lukemalla kaikki levyn saavutettavissa olevat alueet ja tarkastamalla niiden sisällön vastaavan niitä arvoja, jonka tyhjennysprosessin odotetaan sinne asettavan. Todennuksen tulee raportoida tyhjennyksen epäonnistumisesta, jos todennettavat arvot eivät vastaa odotettuja.

4.1 Ylikirjoitus

Vain ylikirjoitukseen perustuvassa tyhjennysmenetelmässä moderneilla kiintolevyillä[5] ja muilla tallennusvälineillä tulee toteutua vähintään kolminkertainen ylikirjoitus sekä ylikirjoituksen todennus. Ylikirjoituksen todennuksessa tulee todentaa ylikirjoituksen onnistuminen koko kiintolevyn tai muun tallennusvälineen kapasiteetille.

Kolminkertaisella ylikirjoituksella tarkoitetaan menettelyä, jossa kiintolevyn tai muun tallennusvälineen koko isäntälaitteelle näkyvälle kapasiteetille[6] kirjoitetaan ensimmäisellä kierroksella tietty binäärinen arvo, toisella kierroksella edellisen komplementtiarvo ja kolmannella kierroksella pseudosatunnaisesti valittu arvo[7]. Kolminkertaisen ylikirjoituksen ja ylikirjoituksen todennuksen toteuttavia standardeja ovat esimerkiksi seuraavat:

- U.S DoD 5220.22-M
- National Computer Security Center (NCSC-TG-025)
- U.S. Navy Staff Office Publication NAVSO P-5239-26

Ylikirjoituksen onnistumisen tarkastaminen voidaan suorittaa lukemalla valittu pseudosatunnainen arvo kiintolevyltä tai muulta tallennusvälineeltä, ja tarkastamalla sen vastaavuus algoritmin samalla siemenarvolla muodostamaa arvoa vastaan.

4.2 Laiteohjelmiston suorittama tyhjennys

Laiteohjelmiston suorittamalla tyhjennyksellä tarkoitetaan tyhjennystä, jossa käytetään hyväksi kiintolevyn tai muun tallennusvälineen laiteohjelmistoon rakennettuja komentoja. Tällaisia ovat esimerkiksi ATA-komentokielen "SECURITY ERASE UNIT"-komento, SCSI-komentokielen "SANITIZE"-komento ja NVMe-komentokielen "SANITIZE"-operaatio.

Laiteohjelmiston suorittaman tyhjennyksen onnistuminen voidaan tarkastaa kirjoittamalla ennen tyhjennystä tunnettuja datakuvioita laitteelle ja tarkastamalla tyhjennyksen jälkeen ovat muistialueet tyhjentyneet vai ovatko datakuviot edelleen näkyvissä laitteen levypinnalla.

4.2.1 ATA-komentokieltä käyttävät laitteet

ATA-komentokieltä käyttävissä laitteissa laiteohjelmiston suorittama tyhjennys voidaan toteuttaa seuraavasti:

[5] Luvussa 12.1 on käsitelty erityistapauksia vanhempien kovalevyjen tyhjennykseen.

[6] Sisältäen kaikki levyosiot, mukaan lukien käynnistysosion ja mahdolliset piilotetut osiot sekä myös levytilan, jota ei ole osioitu sekä HPA- ja DCO-alueet sekä muilla vastaavilla tavoilla piilotetut alueet.

[7] Ensimmäisellä kierroksella voidaan kirjoittaa oktetti esimerkiksi arvolla 00110101, toisella kierroksella arvolla 11001010 ja kolmannella (yhden oktetin osalta esimerkiksi) arvolla 10010111.

- Asetetaan käytettäväksi "Enchanced Erase Mode" ("ERASE MODE"-arvoksi on asetetaan "1").
- Suoritetaan "SECURITY ERASE UNIT"-komento.
- Tyhjennyksen jälkeen tarkastetaan tyhjennyksen onnistuminen koko kapasiteetille

4.2.2 SCSI-komentokieltä käyttävät laitteet

SCSI-komentokieltä käyttävissä laitteissa laiteohjelmiston suorittama tyhjennys voidaan toteuttaa seuraavasti:

- Asetetaan tyhjennystyypiksi "Block Erase" asettamalla "SERVICE ACTION"-kentän arvoksi "02" ("BLOCK ERASE").
- Tämän jälkeen suoritetaan "SANITIZE"-komento
- Tyhjennyksen jälkeen tarkastetaan tyhjennyksen onnistuminen koko kapasiteetille

4.2.3 NVMe-komentokieltä käyttävät laitteet

NVMe-komentokieltä käyttävissä laitteissa laiteohjelmiston suorittama tyhjennys voidaan toteuttaa suorittamalla "SANITIZE"-operaatio seuraavasti:

- Kaikkien NVMe-muistin sisältämien nimiavaruuksien suojaustaso asetetaan kirjoitussuojaamattomaan tilaan ("No Write Protect")
- Kaikki isäntäkoneen muistialueet otetaan pois käytöstä ("Host Memory Buffer"-alueet)
- Otetaan pois käytöstä pysyvä muistialue -toiminnallisuus ("Persistent Memory Region")
- Asetetaan tyhjennystyypiksi "Block Erase" asettamalla "Sanitize Action field" on arvoon "010b" ("Start a Block Erase Sanitize operation")
- Otetaan pois käytöstä muistialueiden vapauttaminen tyhjennyksen jälkeen asettamalla "No-Deallocate After Sanitize"-bitti "Sanitize"-komennossa arvoon "1"
- Otetaan pois käytöstä rajoittamaton poistuminen tyhjennyksestä asettamalla "Allow Unrestricted Sanitize Exit"-bitti asetetaan arvoon "0"
- Tyhjennyksen jälkeen tarkastetaan tyhjennyksen onnistuminen koko kapasiteetille

4.3 Tyhjennysmenetelmät eri laitetyypeille

Tässä luvussa käsitellään, millaisia eri todennettavissa olevia tyhjennysmenetelmiä voidaan eri laitetyypeille käyttää.

4.3.1 Magneettiset kiintolevyt

Magneettisille kiintolevyille voidaan käyttää tyhjennysmenetelmänä ylikirjoitusta. Menettely on esitetty luvussa 4.1.

4.3.2 SSD-kiintolevyt

SSD-kiintolevyn tyhjennyksessä tulee toteuttaa seuraavat vaiheet annetussa järjestyksessä:

1. Koko SSD-kiintolevyn isäntälaittelle näkyvän kapasiteetin ylikirjoitus pakkautumattomalla (pseudosatunnaisella) datalla vähintään kaksinkertaisesti
2. Vaiheessa 1 tehdyn ylikirjoituksen onnistumisen todentaminen
3. SSD-kiintolevyn laiteohjelmiston (firmware) tyhjennyskomennon tai -komentojen suoritus. Eri komentokielien käyttämiä tyhjennyskomentoja on käsitelty luvussa 4.2.
4. Vaiheessa 3 tehdyn tyhjennyksen onnistumisen todentaminen. Todennus tulee kohdistaa koko tyhjennetylle alueelle.

SSD-kiintolevyn tyhjennys on aina kohdistettava koko SSD-kiintolevyn näkyvälle kapasiteetille, osiokohtainen tyhjennys ei ole mahdollista. Luotettava tyhjennys ei ole mahdollista sellaisille SSD-kiintolevyille, jotka eivät tue laiteohjelmistotason tyhjennyskomentoja. Tilanteissa, joissa yksikin tyhjennyksen tai todentamisen vaihe päättyy virheeseen, on SSD-kiintolevyä kohdeltava kuin se edelleen sisältäisi kaiken siellä ennen tyhjennysprosessin aloittamista olleen datan.

4.4 Ohjelmistot tiedon hävittämiseen

Tiedon luotettavaan hävittämiseen tulee käyttää ensisijaisesti tiedon omistajan hyväksymää ohjelmistoa. Ohjelmiston oikeellinen toiminta tulisi pystyä osoittamaan luotettavasti ja ohjelmiston avulla todentamaan ja raportoimaan tyhjennyksen suorittamisen onnistuminen. Käytettävän ohjelmiston tulee olla ajantasainen ja ohjelmistossa tulee olla myös todennettu tuki hävittämisen kohteen käyttämään tekniikkaan[8]. Tyhjennykseen soveltuvia Kyberturvallisuuskeskuksen NCSA-toiminnon arvioimia ohjelmistoja löytyy listattuna[9] Kyberturvallisuuskeskuksen www-sivuilta.

Esimerkiksi hävitettäessä tietoa SSD-kiintolevyltä, on aina käytettävä ohjelmistoa ja algoritmia, jotka on tarkoitettu nimenomaan SSD-kiintolevyllä sijaitsevan tiedon hävittämiseen. Vastaavasti SSD-levyillä sijaitsevan tiedon hävittämiseen käytettyä menetelmää ei tule käyttää magneettisella kiintolevyllä olevan tiedon hävittämiseen, ellei kyseistä menetelmää ole tarkoitettu myös magneettisille kiintolevyille. Tiedon hävittämiseen mobiililaitteista tulee käyttää siihen tarkoitettua ohjelmistoa.

Hävittämiseen käytettävän ohjelmiston eheydestä tulee pystyä varmistumaan. Tiedon hävittämisen toteuttavan ohjelmiston koodi tulee suorittaa luotetusta ja todennettavissa olevasta lähteestä, esimerkiksi käynnistyvältä (boot) CD-ROM-levyltä taikka käynnistyvältä USB-muistitikulta, jonka eheys pystytään todentamaan. Ohjelmiston sisältämä media tulee myös säilyttää fyysisesti turvallisessa paikassa. Mikäli hävittämiseen käytetyn ohjelmiston käyttö edellyttää käynnistystä lähiverkosta (LAN boot), tulee lähiverkon olla suojattu hävitettävän tietoaineiston turvallisuusluokan mukaisesti.

[8] Esimerkiksi SSD-kiintolevyjä tyhjentävän ohjelmiston tulee ylikirjoituksen lisäksi osata suorittaa tarvittavat firmware-komennot levyn tyhjentämiseksi.

[9] https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat?toggle=Elinkaaren%20hallinta%20%28Ylikirjoitustuotteet%29

Hävitykseen käytettävän ohjelmiston tulee pystyä tuottamaan raportti tyhjennyksestä. Raportista on käytävä ilmi tyhjennyksen kohteen todellinen kapasiteetti sekä tyhjennyksen onnistumisaste. Onnistumisasteella tarkoitetaan tietoa siitä, kuinka suuri osa kohdistetusta alueesta tyhjennettiin onnistuneesti ja kuinka suureen osaan tyhjennys ei onnistunut, esimerkiksi vioittuneen levyalueen tai muun syyn takia. Jos tyhjennys ei ole täysin onnistunut, tulee levyä käsitellä kuin se sisältäisi vielä kaiken sille ennen tyhjennystä tallennetun tiedon.

4.5 Luotettavan tyhjennysmenettelyn muut edellytykset

4.5.1 Henkilöstö ja ulkoistaminen

Turvallisuusluokkien IV, III, II tai I kiintolevyjen tyhjentämisen voi toteuttaa vain organisaation nimetty henkilö, jolle on myönnetty käsittelyoikeudet[10] kyseessä olevan turvallisuusluokan tietoon. Turvallisuusluokkien III ja IV kiintolevyjen tyhjennyksen voi toteuttaa myös organisaation ulkoistuskumppani, mikäli muutkin luotettavan tyhjennysmenettelyn edellytykset täyttyvät ulkoistuskumppanin toiminnassa.

4.5.2 Toteutustapa tyhjennyksen hallintaan

Organisaatiolla tulee olla todennettavissa oleva toteutustapa suojattavaa tietoa sisältävien kiintolevyjen tyhjennyksen hallintaan. Eräs yleinen toteutustapa on turvallisuusluokkien IV, III, II ja I tietoja sisältävien kiintolevyjen tyhjennysrekisterin ylläpitäminen. Rekisteriin kirjataan vähintään:

1. Kohteen tunnistetieto (kiintolevyn sarjanumero)
2. Valmistajan nimi
3. Kohteen luokittelu (turvallisuusluokka, tarvittaessa tiedon omistaja)
4. Tyhjennysmenetelmä
5. Tyhjennyksen loki (raportti tyhjennyksen onnistumisesta)
6. Vastuuhenkilö (tyhjennyksen suorittaja)
7. Aika ja paikka
8. Todistaja, jonka on oltava organisaatioon kuuluva henkilö[11]
9. Uudelleenkäyttökohde ja sen luokittelu[12]

4.5.3 Kiintolevyn tyhjennyksen todentaminen

Ennen kuin kiintolevyä voidaan luovuttaa uudelleenkäyttöön, tulee tyhjennystapahtuman onnistuminen todentaa. Mikäli jotain kohteena olevaa kiintolevyn osaa ei ole pystytty kokonaisvaltaisesti tyhjentämään, esimerkiksi vioittuneen levysektorin takia, levyä ei voida toimittaa uudelleenkäyttöön.

[10] Kansallisten turvallisuusluokiteltujen tietojen tuhoamiseen perusmuotoinen henkilöturvallisuusselvitys, kansainvälisten turvallisuusluokiteltujen tietojen tuhoamiseen PSC (Personnel Security Clearance) ko. turvallisuusluokalle.

[11] Suositeltava turvallisuusluokilla IV ja III, edellytys turvallisuusluokilla II ja I.

[12] Tavoitteena mahdollistaa kiintolevyjen seuranta niiden elinkaaren ajan ja estää muun muassa turvallisuusluokan II aineistoa sisältäneiden kiintolevyjen kulkeutuminen ympäristöihin, jotka eivät ole organisaation hallinnassa. Voidaan toteuttaa myös muilla menettelyillä, esimerkiksi rajaamalla uusiokäyttö luokituskohtaisesti vain organisaation hallinnassa oleviin turvallisuusluokan IV, III, II ja I ympäristöihin.

Tyhjennyksen onnistuminen tulee todentaa vähintään tyhjennykseen käytetyn ohjelmiston tuottaman raportin pohjalta. Tiedon omistajat asettavat todentamiselle usein lisävaatimuksia erityisesti turvallisuusluokkien III, II ja I kiintolevyjen osalta. Tyypillinen asetettava lisävaatimus on tiedon omistajan riskiarviossa määrittelemillä tiheyksillä, osuuksilla ja menetelmillä toteutettavien pistokokeiden[13] järjestäminen. Tilanteissa, joissa tyhjennyksen onnistumista ei pystytä luotettavasti todentamaan, ei levyä tule luovuttaa uudelleenkäyttöön ja tulee levy tuhota fyysisesti[14] elinkaarensa lopussa.

4.5.4 Tallennusvälineiden salaus

Koko tallennusvälineen kattavaa salausta[15] suositellaan kaikkiin ympäristöihin, joissa medialle tullaan jossain sen elinkaaren vaiheessa tallentamaan suojattavaa tietoa. Salausta edellytetään muun muassa suojattavaa tietoa sisältävien kannettavien tietokoneiden kiintolevyille, mikäli niitä viedään elinkaarensa aikana turvallisen fyysisen tilan ulkopuolelle.[16] Myös kiintolevyn uudelleenkäyttö edellyttää joissain tapauksissa salauksen käyttöä. Salauksella pystytään vähentämään suojattavaan tietoon kohdistuvien uhkien aiheuttamia riskejä kiintolevyn elinkaaren aikana, mutta salausta ei voida kuitenkaan pitää tyhjennyksen korvaavana menettelynä.

Laiteohjelmistotason salauksella suojatun SSD-kiintolevyn tiedot ovat tyypillisesti saatavilla selkokielisessä muodossa suoraan kiintolevyväylän kautta. SSD-kiintolevyjen laiteohjelmistotason salausta ei tässä ohjeessa tulkita siten kiintolevyn salaukseksi.

4.5.5 Laitteiden fyysinen säilytys ja käsittely

Tyhjennettäväksi osoitettujen tallennusvälineiden säilytys tulee ennen tyhjennystä tai tyhjennyksen mahdollisesti epäonnistuessa järjestää niiden sisältämän tiedon turvallisuusluokan mukaisesti. Jos kyseessä on esimerkiksi integroitu muistipiiri, jota ei pystytä laitteesta irrottamaan, tulee tällöin koko laiteen säilytys järjestää laitteen sisältämän tiedon turvallisuusluokan mukaisesti.

4.6 Kiintolevyjen tyhjennys ja uusiokäyttö turvallisuusluokittain

Luvun 5 ja 6 mukainen tyhjennys magneettisille sekä SSD-kiintolevyille, edellä mainituin ehdoin ja rajauksin, on riittävä kaikkien turvallisuusluokkien tietoa sisältäville kiintolevyille. Kiintolevyn elinkaaren[17] mittainen käyttö salattuna mahdollistaa uusiokäytön laajemmalla turvallisuusluokka-alueella kuin salaamattoman kiintolevyn osalta. Uusiokäyttömahdollisuudet on kuvattu turvallisuusluokittain taulukossa 1.

Mikäli kiintolevyn haltijuus siirtyy organisaation ulkopuolelle, on uusiokäytön luokitus tyhjennyksen kannalta rinnastettava julkiseen tietoon. Toisin sanottuna kiintolevyn uusiokäyttö organisaation hallinnan ulkopuolella tai ylipäänsä luovuttaminen organisaation ulkopuolelle on mahdollista vain silloin, kun taulukon 1 oikeanpuoleisessa sarakkeessa on maininta "julkinen".

---

[13] Pistokokeilla tarkoitetaan tyhjennysympäristöön ja -prosesseihin kohdistuvia hallinnollisia ja teknisiä tarkastuksia, joilla pyritään varmistumaan tyhjennysprosessien oikeellisesta toiminnasta. Joissain erityistapauksissa (tyypillisesti käsiteltäessä suuria määriä ja/tai korkeiden turvallisuusluokkien tietoa) myös tyhjennettyihin kiintolevyihin kohdistetaan teknisiä, usein erityisohjelmistoja ja/tai testauslaboratoriota edellyttäviä tarkastuksia.

[14] Silppuaminen, sulattaminen tai jokin muu viranomaisen hyväksymä menettely.

[15] Ohjelmistopohjaiset salausratkaisut, kuten esimerkiksi LUKS, Bitlocker tai Veracrypt

[16] Tietoturvallisuuden auditointityökalu viranomaisille (Katakri 2020), kohta I-18.

[17] Kiintolevyn tulee olla ollut kokonaan salattuna aina, kun sillä on ollut suojattavaa tietoa.

Sarake 1: Kiintolevyn elinkaarensa aikana sisältämien tietojen korkein turvallisuusluokka ennen tyhjennystä.	**Sarake 2:** Suositus uudelleenkäytöstä **tyhjennyksen jälkeen** saman organisaation ympäristössä (turvallisuusluokka) tai organisaation hallinnan ulkopuolella (julkinen)
I salaamaton	I
I salattu	I, II
II salaamaton	I, II
II salattu	I, II, III, IV
III salaamaton	II, III
III salattu	II, III, IV, julkinen
IV salaamaton, magneettinen kiintolevy	III, IV, julkinen
IV salaamaton, SSD-kiintolevy	III, IV
IV salattu	III, IV, julkinen
julkinen	IV, julkinen

5 Muita tyhjennysmenetelmiä

Tässä luvussa kuvataan sellaisia tyhjennysmenetelmiä, joille tyhjennystoiminnallisuuden oikeellista toimintaa ei voida yleisesti todentaa riittävän luotettavasti. Mikäli tällaisia menetelmiä käytetään turvallisuusluokitellun tiedon suojaamiseen, tulee käytön ja siihen liittyvien jäännösriskien olla tietoon määräämisvallassa olevan viranomaisen hyväksymiä.

5.1 Salaukseen perustuva tyhjennys

Salaukseen perustuvan tyhjennyksen käyttö tarkoittaa laitteelle tallennetun tiedon salaamista vahvalla algoritmilla ja tiedon tuhoamisvaiheessa tuhoamalla salaukseen käytetyt avaimet. Tätä menetelmää käytetään esimerkiksi uusissa matkapuhelimissa. Menetelmän käyttäminen vaatii sitä, että laite on salattuna koko käyttöikänsä ajan luotettavasti toteutetulla ja tarpeeksi vahvalla salausalgoritmilla ja kaikki sinne tallennettava tieto ja niiden kopiot tallennetaan salattuna. Menetelmää ei voida käyttää jos:

- Laitteelle on tallennettu suojattavaa tietoa ennen salauksen käyttöönottoa
- Ei ole tiedossa onko laitteelle tallennettu suojattavaa tietoa ennen salauksen käyttöönottoa

Tiedon salaamiseen käytettävien komponenttien tulisi olla standardin FIPS-140-2 tai FIPS-140-3 mukaisia.

Tiedon tuhoamisvaiheessa on huolehdittava, että tiedon salaamiseen käytetty avain ja avaimen kaikki kopiot (ml. avaimien mahdolliset varmuuskopiot muilla medioilla) tuhotaan luotettavasti. Jos organisaatiolla ei ole täyttä varmuutta kaikkien avainten luotettavasta tuhoamisesta, voidaan salaukseen perustuvaa tyhjennystä käyttää ainoastaan yhdessä muiden tyhjennysmenetelmien kanssa.

Salaukseen perustuvassa tyhjennyksessä todennusta tyhjennyksen onnistumisesta ei voida tehdä yhtä luotettavasti kuin muissa menetelmissä. Tämän vuoksi menetelmää voidaan käyttää vain organisaation oman riskiarvion pohjalta. Varmuuteen vaikuttaa esimerkiksi käytetyn salausmenetelmän toteutus sekä salaukseen käytettävien avainten avainhallinta.

5.2 Muita tyhjennysmenetelmiä eri laitetyypeille

5.2.1 Yhdistelmäkiintolevyt

Yhdistelmäkiintolevyjen tyhjennysmenetelmien tehokkuutta ei ole vielä pystytty osoittamaan luotettavasti. Tällä hetkellä ainoa luotettavana pidettävä menetelmä tietojen hävittämiseen yhdistelmäkiintolevyiltä on levyjen fyysinen tuhoaminen.

Salaukseen perustuvaa tyhjennystä käytettäessä on huomioitava, että salaus tulee ottaa käyttöön laitteen elinkaaren alussa, eikä sitä voida ottaa myöhemmin käyttöön, jos kiintolevylle on jo tallennettu suojattavaa tietoa.

5.2.2 Mobiililaitteet

Useat uudemmat mobiililaitteiden käyttöjärjestelmät (kuten Apple IOS v. 10 eteenpäin, Android v. 10 eteenpäin) ovat tehty käyttämään tiedostokohtaista tietojen salausta. Näissä järjestelmissä yksittäiset tiedostot ovat salattuna omilla tiedostokohtaisilla avaimillaan. Tiedostokohtaiset avaimet ovat salattuna avaimet salaavalla avaimella (KEK, *Key Encryption Key*).

Näissä järjestelmissä salaukseen perustuva tyhjennys perustuu siihen, että järjestelmästä tuhotaan tiedostokohtaiset avaimet salaava avain (KEK).

Mobiililaitteiden tyhjennyksessä tulee huomioida seuraavia asioita:

- Salausavaimet tulee tuhota myös mahdollisista mobiililaitteesta otetusta varmuuskopiosta.
- Laitteeseen liitettävät erilliset muistikortit tulee irrottaa laitteesta ja tuhota erikseen. Nämä muistikortit eivät välttämättä ole salattuja, joten näihin ei voida hyödyntää salaukseen perustuvaa tyhjennystä. Myöskään laitteen palautus tehdasasetuksille ei tyypillisesti tyhjennä erillisiä muistikortteja.
- Riskiarvioissa tulee huomioida mahdolliset havaitut tai havaitsemattomat ohjelmistovirheet salauksen ja avaintenkäsittelyn toteutuksessa.
- Varsinkin Android-laitteissa tulee myös huomioida erot eri valmistajien toteutuksissa. Kaikki valmistajat eivät välttämättä tue tiedostokohtaista tietojen salausta, vaikka se pääsääntöisesti uudemmissa malleissa on käytössä.
- Älypuhelimissa riskin voi aiheuttaa myös laitteeseen tehdyt muutokset (kuten laitteen *roottaus*[18]). Tällöin ei voida olettaa laitteen toimivan täysin niin kuin se on suunniteltu ja tyhjennyksen tapahtuvan onnistuneesti.

[18] Laitteen "roottauksella" tarkoitetaan pääkäyttäjätason oikeuksien saamista laitteeseen. Se antaa käyttäjälle mahdollisuuden muokata ja hallita laitteen järjestelmätiedostoja ja asetuksia enemmän kuin normaalit käyttäjät pystyvät.

- Mobiililaitteiden tyhjennyksessä varsinkin Android-puhelimissa tulee käyttää tarkoitukseen soveltuvaa luotettavaa ohjelmistoa[19], joka myös tarkastaa ja raportoi tyhjennyksen onnistumisesta.

5.2.3 USB-muistitikut, integroidut muistipiirit ja muistikortit (SD, miniSD, microSD yms.)

USB-muistitikut ovat laitteita, jotka käyttävät SCSI-komentokantaa kommunikoidessaan isäntäkoneen kanssa. Yleisesti USB-muistitikut eivät kuitenkaan tue SCSI-komentokielen tyhjennykseen tarkoitettuja komentoja.

Integroiduissa muistipiireissä on käytössä eri tekniikoita, kuten eMMC, UFS ja NAND. Muistipiiritekniikat voivat tarjota turvallisia *Secure Erase*-komentoja. Näiden saatavuus ja toteutukset voivat kuitenkin vaihdella merkittävästi.

Muistikortit ovat pienikokoisia ja tavallisesti irrotettavia tallennusvälineitä, joita voidaan käyttää esimerkiksi puhelimissa tai digikameroissa. Tavallisesti näiden muistisirut perustuvat NAND-tekniikkaan. Muistikortit saattavat tarjota turvallisia *Secure Erase* -komentoja. Näiden saatavuus ja toteutukset voivat kuitenkin vaihdella merkittävästi.

Tämän vuoksi sopivia tyhjennysmenetelmiä USB-muistitikuille, integroiduille muistipiireille ja muistikorteille ovat ylikirjoitus, salaukseen perustuva tyhjennys tai fyysinen tuhoaminen.

USB-muistitikkuja, integroituja muistipiirejä tai muistikortteja ylikirjoitettaessa tulee kuitenkin huomioida muistipiirien ominaisuuksia, kuten kuluneiden lohkojen tasainen kuluminen (*wear-leveling*). Tämän vuoksi kaikki data ei välttämättä päädy ylikirjoitetuksi koko muistialueelle, vaan muistitikun ohjauslogiikka voi siirtää datan eri paikkoihin muistissa.

Tämän vuoksi näiden laitteiden luotettavasta tyhjentämisestä ei ole vielä riittävää näyttöä ja ainoa luotettavana pidetty menetelmä on laitteiden fyysinen tuhoaminen esimerkiksi sulattamalla tai silppuamalla tarpeeksi pieniksi[20] kappaleiksi. Varsinkin muistikortteja silputtaessa tulee kuitenkin huomioida laitteen hyvin pieni koko sekä suuri tiheys tallennetulle tiedolle.

Laitteiden poistuessa käytöstä käyttöikänsä päätteeksi ne tulisi kuitenkin myös ylikirjoittaa sekä säilyttää turvallisessa paikassa riskien pienentämiseksi tilanteissa, joissa laitteita tarvitsee esimerkiksi säilöä tai kuljettaa ennen lopullista tuhoamista.

6 Poikkeuksia ja erityistapauksia

6.1 Vanhojen magneettisten kiintolevyjen ylikirjoitus ja uusiokäyttö

Kolminkertainen ylikirjoitus on riittävä vain vuoden 2001 jälkeen valmistettuihin, yli 15 Gt:n magneettisiin kiintolevyihin. Vanhemmille tai kapasiteetiltaan pienemmille levyille yleisesti luotettavana pidettävä menettely edellyttää seitsemänkertaista ylikirjoitusta kaikilla turvallisuusluokilla.

6.2 Kiintolevyn palauttaminen tiedon luovuttajalle

Tilanteissa, joissa kiintolevyllä on elinkaarensa aikana ollut *vain yhden tiedon luovuttaneen viranomaisen* suojattavaa tietoa:

[19] Lista Traficomin Kyberturvallisuuskeskuksena arvioimista ohjelmistoista on saatavilla osoitteessa https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat?toggle=Elinkaaren%20hallinta%20%28Ylikirjoitustuotteet%29

[20] Silppukokoja käsitellään turvallisuusluokitellun tiedon osalta Katakri 2020-ohjeen kohdassa I-21

- Organisaatio voi palauttaa kiintolevyn organisaation ulkopuoliselle tiedon luovuttaneelle viranomaiselle tiedon turvallisuusluokasta ja tyhjennyksestä riippumatta.

Tilanteissa, joissa kiintolevyllä on elinkaarensa aikana ollut *useamman tietoa luovuttaneen viranomaisen* suojattavia tietoja:

- Palauttaminen on mahdollista, mikäli taulukossa 1 kuvatut edellytykset uusiokäytölle tyhjennyksen jälkeen organisaation hallinnan ulkopuolella täyttyvät[21] kaikkien tiedon luovuttaneiden viranomaisten kohdalla.
- Mikäli edellisen kohdan edellytykset eivät täyty, kiintolevyn palauttaminen organisaation hallinnan ulkopuolelle on mahdollista vain kaikkien tietoa luovuttaneiden viranomaisten erillishyväksyntään perustuen.

6.3 Luokituksen laskemisen ketjuttaminen

Luokituksen laskemista ei voida ketjuttaa. Esimerkiksi salatun kiintolevyn luokituksen laskeminen turvallisuusluokasta II turvallisuusluokalle IV on mahdollista onnistuneen tyhjennyksen jälkeen, mutta levyn uudelleen tyhjentämällä ei luokitusta voida laskea edelleen julkiseksi.

6.4 Muut kuin turvalllisuusluokkien IV, III, II ja I uusiokäyttöympäristöt

Uusiokäyttöympäristöt, jotka eivät ole tarkoitettu turvallisuusluokkien IV, III, II tai I tiedon käsittelyyn, tulkitaan ympäristöiksi, jotka eivät ole organisaation hallinnassa. Tällaisia ovat esimerkiksi vain julkisen tiedon käsittelyyn tarkoitetut ympäristöt.

6.5 Yhdistelmäkiintolevyjen tyhjennys ja uusiokäyttö

Yhdistelmäkiintolevyjen tyhjennysmenetelmien tehokkuutta ei ole vielä pystytty osoittamaan luotettavasti. Tällä hetkellä ainoa luotettavana pidettävä menetelmä suojattavien tietojen hävittämiseen yhdistelmäkiintolevyiltä on levyjen fyysinen tuhoaminen.

6.6 Vanhat Apple IOS- (IOS v. 7 ja vanhemmat) ja Android-käyttöjärjestelmät (Android v4 ja vanhemmat)

Vanhemmat Apple- ja Android käyttöjärjestelmät eivät salaa tiedostojärjestelmiään, joten salaukseen perustuvan tuhoamisen käyttäminen ei ole näissä teknisesti mahdollista.

6.7 Demagnetoinnin soveltuvuus HAMR[22]-, MAMR-[23], SSD- ja yhdistelmäkiintolevyjen tyhjentämiseen

Voimakkaisiin magneettikenttiin perustuvat magneettisten kiintolevyjen demagnetointilaitteet ("degausserit") eivät luotettavasti tuhoa tietoa HAMR- tai MAMR-teknologiaa hyödyntävistä kiintolevyistä taikka SSD- ja yhdistelmäkiintolevyiltä. Demagnetointilaitteet eivät siis sovellu näiden medioiden luotettavaan tyhjentämiseen.

---

[21] Taulukon 1 sarakkeessa 2 maininta "julkinen".

[22] *HAMR-kiintolevyillä* (Heat Assisted Magnetic Recording) tarkoitetaan magneettisia kiintolevyjä, joiden kapasiteettia voidaan suurentaa väliaikaisesti levyä kuumentamalla kirjoittaessa.

[23] *MAMR-kiintolevyillä (Microwave Assisted Magnetic Recording)* tarkoitetaan magneettisia kiintolevyjä, joiden kapasiteettia voidaan suurentaa käyttämällä mikroaaltoja hyväksi kirjoituspäässä

7 Ohjeen voimassaolo ja jatkokehitys

Ohje on voimassa toistaiseksi ja sitä päivitetään tarvittaessa. Kehitysehdotukset ja lisätietokyselyt pyydetään lähettämään osoitteeseen ncsa (at) traficom (piste) fi

8 Lisätietoa

1. NIST 800-88. Guidelines for Media Sanitization. National Institute of Standards and Technology. 2006. URL: http://csrc.nist.gov/publications/nistpubs/80088/NISTSP800-88_with-errata.pdf
2. Australian Government Information Security Manual. Department of Defence. 2011. URL: http://www.asd.gov.au/infosec/ism/index.htm
3. ITSG-06. Clearing And Declassifying Electronic Data Storage Devices. Communications Security Establishment. 2006. URL: http://www.asd.gov.au/publications/Information_Security_Manual_2014_Controls.pdf
4. Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille. Kansallinen turvallisuusviranomainen. 2020. URL: http://www.defmin.fi/katakri.
5. Hughes, G & Coughlin, T. Tutorial on Disk Drive Data Sanitization. Center for Magnetic Recording Research. University of California. URL: http://cmrr.ucsd.edu/people/Hughes/documents/DataSanitizationTutorial.pdf
6. Wei, M., Grupp, L., Spada, F. & Swanson, S. Reliably erasing data from flashbased solid state drives. Proceedings of the 9th USENIX conference on File and storage technologies (FAST'11). 2011. URL: http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf
7. DIN 66399-2:2012-10. Office machines - Destruction of data carriers - Part 2: Requirements for equipment for destruction of data carriers. 2012.
8. NSA/CSS Requirements for Magnetic Degaussers. 2021. URL: https://www.nsa.gov/portals/75/documents/resources/everyone/media-destruction/NSA_CSS%20Requirements%20for%20Magnetic%20Degaussers.pdf?ver=GSo5EEFg-tTBI6fS8Dahmg%3D%3D
9. IEEE Standard for Sanitizing Storage 2883-2022. Cybersecurity and Privacy Standard Committee of the IEEE Computer Society
10. National Institute of Standards and Technology Special Publication 800-88 Revision 1. 2014. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf