26.10.2016

Kiintolevyjen elinkaaren hallinta

Ylikirjoitus ja uusiokäyttö

1 Johdanto

Viestintäviraston NCSA-toiminnon tehtäviin kuuluu toimiminen turvallisuusjärjestelyt hyväksyvänä viranomaisena (SAA, Security Accreditation Authority). NCSA-toiminnon suorittamissa tietojärjestelmätarkastuksissa eräs tarkastettava kohde on suojattavaa tietoa sisältävien kiintolevyjen elinkaaren hallinta. Tässä ohjeessa kuvataan yleisimmät edellytykset elinkaaren hallinnan hyväksyttävään toteutukseen kiintolevyjen ylikirjoituksen ja uusiokäytön osalta.

2 Määritelmät

- *Kiintolevyllä* tarkoitetaan tässä ohjeessa tietokoneen kiintolevyväylään (PATA, SATA, SCSI, SAS 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.
- *Kiintolevyn elinkaarella* tarkoitetaan tässä ohjeessa aikaa kiintolevyn ensimmäisestä käyttöönotosta sen luotettavaan fyysiseen tuhoamiseen. Toisin sanottuna hyväksytty ylikirjoitus ei katkaise kiintolevyn elinkaarta.
- *Organisaatiolla* tarkoitetaan tässä ohjeessa tahoa (tiedon haltijaa), jonka hallussa tietoa sisältävä kiintolevy tiedon omistajan 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.

3 Ylikirjoitusmenetelmät

3.1 Magneettiset kiintolevyt

Ylikirjoitukseen hyväksyttävässä menetelmässä tulee toteutua vähintään kolminkertainen ylikirjoitus sekä ylikirjoituksen todennus. Kolminkertaisella

[1] USB-väylä ei tässä sisälly kiintolevyväylän määritelmään.
[2] Käyttäjän kohdistettavissa olevat muistialueet.
[3] Pois luettuna mahdollisesti järjestelmän käynnistymisen vaatima lyhyt selväkielinen osa.

ylikirjoituksella tarkoitetaan menettelyä, jossa kiintolevyn koko käyttäjälle näkyvälle kapasiteetille kirjoitetaan ensimmäisellä kierroksella tietty binäärinen arvo, toisella kierroksella edellisen komplementtiarvo, ja kolmannella kierroksella pseudo-satunnaisesti valittu arvo[4]. Kolminkertaisen ylikirjoituksen ja ylikirjoituksen todennuksen toteuttavia standardeja ovat esimerkiksi seuraavat:

- British HMG Infosec Standard 5, Enhanced Standard
- U.S. Navy Staff Office Publication NAVSO P-5239-26

3.2 SSD-kiintolevyt

Ylikirjoitukseen hyväksyttävässä menetelmässä tulee toteutua seuraavat vaiheet annetussa järjestyksessä:

1. Koko SSD-kiintolevyn käyttäjälle näkyvän kapasiteetin ylikirjoitus pakkautumattomalla (pseudosatunnaisella) datalla vähintään kaksinkertaisesti
2. Vaiheessa 1 tehdyn ylikirjoituksen onnistumisen todentaminen
3. SSD-kiintolevyn laiteohjelmiston (firmware) ylikirjoituskomennon tai -komentojen suoritus[5]
4. Vaiheessa 3 tehdyn ylikirjoituksen onnistumisen todentaminen.

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

3.3 Yhdistelmäkiintolevyt

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

4 Ylikirjoitusohjelmistot

Ylikirjoitukseen tulee käyttää ohjelmistoa, jonka oikeellinen toiminta on pystytty osoittamaan luotettavasti. Tällaisia ohjelmistoja ovat esimerkiksi Viestintäviraston NCSA-toiminnon hyväksymät ylikirjoitustuotteet. Käytettävässä ohjelmistossa tulee olla myös todennettu tuki ylikirjoituksen kohteen käyttämään tekniikkaan. Esimerkiksi SSD-kiintolevyn ylikirjoittamiseen on aina käytettävä ohjelmistoa ja algoritmia, jotka on hyväksytty nimenomaan SSD-kiintolevyn ylikirjoittamiseen. Vastaavasti SSD-ylikirjoitusmenetelmää ei tule käyttää magneettisen kiintolevyn ylikirjoittamiseen, ellei kyseistä menetelmää ole hyväksytty myös magneettisille kiintolevyille.

Ylikirjoitusohjelmiston eheydestä tulee pystyä varmistumaan. Ylikirjoitustoteutuksen ohjelmistokoodi tulee suorittaa luotetusta ja todennettavissa olevasta lähteestä, esimerkiksi käynnistyvältä (boot) CD-ROM-levyltä. Mikäli ylikirjoitusohjelmiston käyttö edellyttää käynnistystä lähiverkosta (LAN boot), tulee lähiverkon olla suojattu ylikirjoitettavan tietoaineiston suojaustason mukaisesti.

[4] Ensimmäisellä kierroksella voidaan kirjoittaa oktetti esimerkiksi arvolla 00110101, toisella kierroksella arvolla 11001010 ja kolmannella (yhden oktetin osalta esimerkiksi) arvolla 10010111.
[5] ATA secure erase, enhanced secure erase tai vastaavat.

Ylikirjoitusohjelmiston tulee pystyä tuottamaan raportti ylikirjoitustapahtumasta. Raportista on käytävä ilmi ylikirjoituksen kohteen todellinen kapasiteetti sekä ylikirjoitustapahtuman onnistumisaste. Onnistumisasteella tarkoitetaan tietoa siitä, kuinka suuri osa kohdistetusta alueesta ylikirjoitettiin onnistuneesti, ja kuinka suureen osaan ylikirjoitus ei onnistunut, esimerkiksi vioittuneen levyalueen tai muun syyn takia.

5 Hyväksyttävän ylikirjoitusmenettelyn muut edellytykset

5.1 Ylikirjoitushenkilöstö ja ulkoistaminen

Suojaustasojen IV, III, II tai I kiintolevyjen ylikirjoituksen voi toteuttaa vain organisaation nimetty henkilö, jolle on myönnetty käsittelyoikeudet[6] kyseessä olevan luokan tietoon. Suojaustasojen III ja IV kiintolevyjen ylikirjoituksen voi toteuttaa myös organisaation ulkoistuskumppani, mikäli muutkin hyväksyttävän ylikirjoitusmenettelyn edellytykset täyttyvät ulkoistuskumppanin toiminnassa.

5.2 Toteutustapa ylikirjoitusten hallintaan

Organisaatiolla tulee olla todennettavissa oleva toteutustapa suojattavaa tietoa sisältävien kiintolevyjen ylikirjoitusten hallintaan. Eräs yleinen hyväksyttävissä oleva toteutustapa on suojaustasojen IV, III, II ja I tietoja sisältävien kiintolevyjen ylikirjoitusrekisterin ylläpitäminen. Rekisteriin kirjataan hyväksyttävissä toteutuksissa vähintään:

1. Kohteen tunnistetieto (kiintolevyn sarjanumero)
2. Valmistajan nimi
3. Kohteen luokittelu (suojaustaso, tarvittaessa tiedon omistaja)
4. Ylikirjoitusmenetelmä
5. Ylikirjoituksen loki (raportti ylikirjoituksen onnistumisesta)
6. Vastuuhenkilö (ylikirjoittaja)
7. Aika ja paikka
8. Todistaja, jonka on oltava organisaatioon kuuluva henkilö[7]
9. Uudelleenkäyttökohde ja sen luokitus[8]

5.3 Ylikirjoituksen todentaminen

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

Ylikirjoituksen onnistuminen tulee todentaa vähintään ylikirjoitusohjelmiston tuottaman raportin pohjalta. Tiedon omistajat asettavat todentamiselle usein lisävaatimuksia erityisesti suojaustasojen III, II ja I kiintolevyjen osalta. Tyypillinen asetettava lisävaatimus on tiedon omistajan riskienarvioinnissa määrittelemillä tiheyksillä, osuuksilla ja menetelmillä toteutettavien pistokokeiden[9] järjestäminen. Tilanteissa,

---

[6] Kansallisten suojaustasojen tietojen tuhoamiseen perusmuotoinen henkilöturvallisuusselvitys, kansainvälisten luokiteltujen tietojen tuhoamiseen PSC (Personal Security Clearance) ko. suojaustasolle.

[7] Suositeltava suojaustasoilla IV ja III, pakollinen suojaustasoilla II ja I.

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

[9] Pistokokeilla tarkoitetaan ylikirjoitusympäristöön ja -prosesseihin kohdistuvia hallinnollisia ja teknisiä tarkastuksia, joilla pyritään varmistumaan ylikirjoitusprosessien oikeellisesta toiminnasta. Joissain erityistapauksissa (tyypillisesti käsiteltäessä suuria määriä ja/tai korkeiden suojaustasojen tietoa) myös ylikirjoitettuihin kiintolevyihin kohdistetaan teknisiä, usein erityisohjelmistoja ja/tai testauslaboratoriota edellyttäviä tarkastuksia.

joissa ylikirjoituksen onnistumista ei pystytä luotettavasti todentamaan, tulee levy tuhota fyysisesti[10].

5.4 Kiintolevyjen salaus

Koko kiintolevyn salausta suositellaan kaikkiin ympäristöihin, joissa kiintolevylle tullaan jossain sen elinkaaren vaiheessa tallentamaan suojattavaa tietoa. Salausta edellytetään muun muassa suojattavaa tietoa sisältävien kannettavien tietokoneiden kiintolevyille, mikäli niitä viedään elinkaarensa aikana hyväksytyn fyysisen tilan ulkopuolelle.[11] Myös kiintolevyn uudelleenkäyttö edellyttää joissain tapauksissa salauksen käyttöä. Salauksella pystytään pienentämään suojattavaan tietoon kohdistuvien uhkien aiheuttamia riskejä kiintolevyn elinkaaren aikana, mutta salausta ei voida kuitenkaan pitää ylikirjoituksen korvaavana menettelynä.

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

6 Ylikirjoitus ja uusiokäyttö suojaustasoittain

Luvun 3 mukainen ylikirjoitus, edellä mainituin ehdoin ja rajauksin, on riittävä kaikkien suojaustasojen tietoa sisältäville kiintolevyille. Kiintolevyn elinkaaren[12] mittainen käyttö salattuna mahdollistaa uusiokäytön laajemmalla suojaustasoalueella kuin salaamattoman kiintolevyn osalta. Uusiokäyttömahdollisuudet on kuvattu suojaustasoittain taulukossa 1.

Mikäli kiintolevyn haltijuus siirtyy organisaation ulkopuolelle, on uusiokäytön luokitus ylikirjoituksen 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".

Taulukko 1: Uusiokäyttömahdollisuudet suojaustasoittain

Sarake 1: Kiintolevyn elinkaarensa aikana sisältämien tietojen korkein suojaustaso ennen ylikirjoitusta.	**Sarake 2:** Uudelleenkäyttö ylikirjoituksen jälkeen mahdollista saman organisaation ympäristössä (suojaustaso) tai organisaation hallinnan ulkopuolella (julkinen)
I salaamaton	I
I salattu	I, II
II salaamaton	I, II
II salattu	I, II, III, IV
III salaamaton	I, II, III
III salattu	I, II, III, IV, julkinen
IV salaamaton, magneettinen kiintolevy	I, II, III, IV, julkinen
IV salaamaton, SSD-kiintolevy	I, II, III, IV
IV salattu	I, II, III, IV, julkinen
julkinen	I, II, III, IV, julkinen

[10] Silppuaminen, sulattaminen, tai jokin muu viranomaisen hyväksymä menettely.
[11] Tietoturvallisuuden auditointityökalu viranomaisille (Katakri 2015), kohdat I 16 ja I 22.
[12] Kiintolevyn tulee olla ollut kokonaan salattuna aina, kun sillä on ollut suojattavaa tietoa.

7 Poikkeuksia ja erityistapauksia

7.1 Vanhojen magneettisten kiintolevyjen ylikirjoittaminen ja uusiokäyttö

Kolminkertainen ylikirjoitus on riittävä vain vuoden 2001 jälkeen valmistettuihin, yli 15 Gt:n magneettisiin kiintolevyihin. Vanhemmille tai kapasiteetiltaan pienemmille levyille edellytetään seitsemänkertaista ylikirjoitusta kaikilla suojaustasoilla.

7.2 Kiintolevyn luovuttaminen tiedon omistajalle

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

- Organisaatio voi luovuttaa kiintolevyn organisaation ulkopuoliselle tiedon omistajalle tiedon suojaustasosta ja ylikirjoituksesta riippumatta.

Tilanteissa, joissa kiintolevyllä on elinkaarensa aikana ollut *eri tiedon omistajien* suojattavia tietoja:

- Luovutus on mahdollista, mikäli taulukossa 1 kuvatut edellytykset uusiokäytölle ylikirjoituksen jälkeen organisaation hallinnan ulkopuolella täyttyvät[13] kaikkien tiedon omistajien kohdalla.
- Mikäli edellisen kohdan edellytykset eivät täyty, kiintolevyn luovuttaminen organisaation hallinnan ulkopuolelle on mahdollista vain kaikkien tiedon omistajien erillishyväksyntään perustuen.

7.3 Luokituksen laskemisen ketjuttaminen

Luokituksen laskemista ei voida ketjuttaa. Esimerkiksi salatun kiintolevyn luokituksen laskeminen suojaustasolta II suojaustasolle IV on mahdollista, mutta levyn uudelleen ylikirjoittamalla ei luokitusta voida laskea edelleen julkiseksi.

7.4 Muut kuin suojaustasojen IV, III, II ja I uusiokäyttöympäristöt

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

7.5 Yhdistelmäkiintolevyjen ylikirjoitus ja uusiokäyttö

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

7.6 Demagnetoinnin soveltuvuus SSD- ja yhdistelmäkiintolevyjen tyhjentämiseen

Voimakkaisiin magneettikenttiin perustuvat magneettisten kiintolevyjen demagnetointilaitteet ("degausserit") eivät luotettavasti tuhoa tietoa SSD- ja yhdistelmäkiintolevyiltä. Demagnetointilaitteet eivät siis sovellu näiden medioiden luotettavaan tyhjentämiseen.

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

8 Lisätietoa

1. NIST 800-88. Guidelines for Media Sanitization. National Institute of Standards and Technology. 2006. URL: http://csrc.nist.gov/publications/nistpubs/800-88/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 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Kansallinen turvallisuusviranomainen. 2015. 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 flash-based 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.