OULUN AMMATTIKORKEAKOULU

Ilkka Rekilä

IT-OMAISUUDEN TIETOTURVALLINEN KÄYTÖSTÄPOISTO

IT-OMAISUUDEN TIETOTURVALLINEN KÄYTÖSTÄPOISTO

Ilkka Rekilä
Opinnäytetyö
Kevät 2024
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma

Tekijä(t): Ilkka Rekilä
Opinnäytetyön nimi: IT-omaisuuden tietoturvallinen käytöstäpoisto
Työn ohjaaja(t): Perttu Hietala
Työn valmistumislukukausi ja -vuosi: Kevät 2024 Sivumäärä: 35

Opinnäytetyö oli toiminnallinen ja sen tavoitteena oli suunnitella sekä toteuttaa IT-omaisuuden tietoturvallinen käytöstäpoisto toimeksiantajalle Oura Health Oy. Yrityksessä ei ollut järkevää tapaa hävittää vanhoja laitteita tietoturvallisesti.

Toteutuksessa käytettiin Blancco Technology Groupin kehittämiä laitteiden tyhjennykseen spesialisoituneita ohjelmistoja, jotka varmistivat säännösten mukaisen tietojen tyhjentämisen. Tietojen tyhjennys takaa, ettei sensitiivistä dataa pääse laitteiston käytöstäpoiston aikana pois yrityksestä.

Opinnäytetyön tuloksena keksittiin järkevä ratkaisu IT-omaisuuden tietoturvalliseen sekä ekologiseen käytöstäpoistoon. Yritys toimii jatkossa vaatimustenmukaisesti tämän prosessin osalta.

Asiasanat: käytöstäpoisto, IT-omaisuudenhallinta, tietoturva, sensitiivinen data, vaatimustenmukaisuus, riskienhallinta, ekologisuus

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems

Author(s): Ilkka Rekilä
Title of thesis: Secure IT-asset disposal
Supervisor(s): Perttu Hietala
Term and year when the thesis was submitted: Spring 2024
Number of pages: 35

The idea of this thesis was to create a secure way to retire devices from Oura Health Oy. The company did not have any dedicated solution for the device retirement.

The implementation utilized a company specialized in device wiping called Blancco Technology Group, which provided software for compliant data destruction. Data sanitization ensures that sensitive data cannot leak out of the company.

The outcome was positive. A reasonable solution was devised for the secure and environmentally friendly disposal of devices. Company will have a compliant solution for the future.

Keywords: IT asset disposal, IT asset management, information security, sensitive data, compliance, risk management, ecological

SISÄLLYS

1 JOHDANTO

Opinnäytetyön toimeksiantajana toimii vuonna 2013 perustettu älysormuksiin keskittyvä yritys Oura Health Oy. Yritys tunnetaan Oura Ring -älysormuksesta, joka seuraa muun muassa unta, aktiivisuutta, sykettä sekä veren happipitoisuutta. Oura on myynyt kirjoitushetkellä yli miljoona älysormusta. (Oura Health Oy 2024.)

Opinnäytetyön tarve huomattiin, kun yrityksellä ei ollut järkevää tapaa tietoturvallisesti hävittää käytöstä poistuvia tai jo poistuneita laitteita. Teoriaosuudessa käsitellään yleisesti tietoturvaa, riskienhallintaa, omaisuudenhallintaa, tietojen tyhjennystä, vaatimustenmukaisuutta sekä sensitiivistä eli arkaluontoista dataa.

Opinnäytetyön tavoitteena on saada yritykselle tietoturvallinen tapa tyhjentää laitteet ja varmistaa niiden vaatimustenmukaisuus raporttien avulla. Opinnäytetyön toiminnallisessa osuudessa otetaan käyttöön työkalut, jotka varmistavat laitteiden elinkaaren päättämisen oikealla tavalla. Lopuksi kerron, miten opinnäytetyön tulos vaikuttaa toimeksiantajaan, itseeni sekä ulkopuolisiin henkilöihin.

2 KESKEISET KÄSITTEET

Tässä luvussa käsittelen yleisiä käsitteitä, joita tullaan käyttämään myöhemmin opinnäytetyön aikana.

IT-omaisuudenhallinta

IT-omaisuudenhallinta (eng. IT asset management, ITAM) on prosessi, joka varmistaa, että yrityksen laitteet ovat hallinnoitu, asennettu, ylläpidetty, päivitetty ja hävitetty oikealla tavalla. Lyhykäisyydessään tämä prosessi varmistaa, että arvokkaita laitteita käytetään ja jäljitetään oikein. (Atlassian 2024.)

IT-omaisuuden käytöstäpoisto

IT-omaisuuden käytöstäpoisto (eng. IT asset disposal, ITAD) tarkoittaa laitteiden asianmukaista hävittämistä. Prosessi sisältää tietojen tyhjennyksen, laitehallinnasta laitteen poistamisen ja laitteen kunnon mukaan sen tuhoamisen, kierrättämisen tai lahjoittamisen. ITAD on keskeinen osa tietotekniikan elinkaarenhallintaa, sillä se auttaa hahmottamaan IT-omaisuuden elinajan päättymistä, hallitsemaan kustannuksia sekä varmistamaan tietoturvan. Se tarkoittaa elinkaaren loppuvaihetta, jossa laite poistetaan käytöstä eikä se ole enää yhteydessä yrityksen laitehallintaan. (CDW 2021.)

Tietojen tyhjennys

Tietojen tyhjennys on tärkeä osa elinkaarta. Tarpeettomaksi, vanhentuneeksi tai mitättömäksi katsottu data täytyy hävittää oikealla ja tietoturvallisella tavalla. Tietojen tyhjennys on prosessi, jossa tarkoituksella, pysyvästi ja peruuttamattomasti poistetaan tai tuhotaan laitteelle tallennetut tiedot, jotta niitä ei voida palauttaa. Laitteisiin ei jää käyttökelpoista dataa, jota voisi palauttaa edes edistyneiden työkalujen avulla. (Blancco 2017.)

Vaatimustenmukaisuus

Vaatimustenmukaisuus (eng. Compliance) viittaa velvollisuuteen noudattaa ennalta annettuja sääntöjä. Sen noudattaminen vähentää riskejä, parantaa yrityksen mainetta sekä lisää luottamusta asiakkaiden kanssa. Jos yritys ei noudata näitä vaatimuksia, sitä voidaan rankaista suurilla sakoilla laajuuden mukaan tai vastuussa olevaa johtajaa voidaan rankaista vankeudella. (Myra Security 2024.)

Sensitiivinen data

Sensitiivinen tai arkaluontoinen data tarkoittaa kaikkea dataa, jota halutaan suojata luvattomalta paljastumiselta. Tietojen suojaaminen on pakollista laillisista tai eettisistä syistä. Arkaluotoiseen dataan sisältyy henkilötiedot, luottamukselliset tiedot sekä kaikki data, joka ennalta luokitellaan arkaluontoiseksi. Henkilötietoihin lukeutuvat muun muassa: etnisyys, poliittiset mielipiteet, uskonto, geneettiset tiedot, terveystiedot, seksuaalisuus, rikosrekisteri tai rikkomukset. (CSC 2024.)

3 TIETOTURVA JA RISKIENHALLINTA

Tässä luvussa käsitellään tietoturvaa ja riskienhallintaa yleisesti, sillä ne liittyvät IT-omaisuudenhallintaan. IT-omaisuuden käytöstäpoistoon liittyy riskejä, kuten tietovuodot sekä laitteiston fyysinen turvallisuus kuljetuksen aikana. Hyvällä tietoturvasuunnitelmalla voidaan estää nämä riskit sekä muut uhkat.

3.1 Mikä on tietoturva

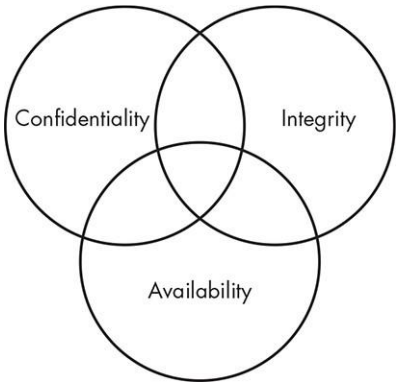
Tietoturva (eng. Information security, InfoSec) on joukko turvallisuustoimia, jotka suojaavat sensitiivisten tietojen väärinkäytöltä, tuhoamiselta, hävittämiseltä ja ei-toivotulta pääsyiltä. Tietoturva kattaa fyysisen ja digitaalisen turvallisuuden sekä kyberturvallisuuden. (Microsoft 2024.)

Tietoturva sekoitetaan useasti kyberturvallisuuteen, mutta oikeasti kyberturvallisuus on tietoturvan alla oleva yksi osuus (Cisco 2024). Tietoturva voidaan ajatella laaja-alaisena terminä, joka kattaa kaikki tiedot, eikä vain ainoastaan kyberturvallisuudessa käsiteltyjä tietoja. Tietoturva jaetaan moniin osiin, kuten tietoturvan hallintaan, sovelluksien turvallisuuteen, pilviturvallisuuteen, salauspohjainen koodaus (eng. Cryptographic encoding), infrastruktuurin turvallisuuteen sekä riskienhallintaan. (Coursera 2024.)

Tietoturvan tärkeys on kasvanut paljon viime vuosina, sillä tietoturvaan kohdistuvat hyökkäykset lisääntyvät hurjasti sekä yritykset keräävät sensitiivistä dataa enemmän ja tietoja yleisesti käsitellään nykypäivänä enemmän. Uusien teknologien takia tietoturva on myös tärkeämpää vuosi vuodelta. Tietojen väärinkäytön estämiselle sekä ei-toivottujen pääsyjen takia vankan tietoturvapohjan toteuttaminen on tärkeää. Lisäksi tietoturva on tärkeää, jotta yritys saavuttaa vaatimustenmukaisuuden ja sen myötä noudattaa vaadittavia lakeja, standardeja sekä määräyksiä. (Coursera 2024.)

3.2 Tietoturvamalli

Kun puhutaan tietoturva-asioista, on hyvä olla malli, jota voi käyttää pohjana. Andress (2019, luku 1) mainitsee kirjassaan, että hyvänä esimerkkipohjana toimii CIA-malli, joka tulee sanoista Confidentiality eli luotettavuus, Integrity eli eheys ja Availability eli saatavuus. Kuviossa 1 näkyy CIA-malli.



KUVIO 1. CIA-malli

Luottamuksellisuus viittaa siihen, että kenellä on oikeus nähdä tietoja. Esimerkkinä ihminen, joka nostaa pankkiautomaatista rahaa. Ainoastaan nostavalla henkilöllä on pankkikortti sekä tiedossa sen PIN-koodi. Pankkiautomaatin omistaja luottamuksellisesti hallinnoi tilinumeroa, tilin varoja sekä muita nostoon vaadittavia tietoja. Pankki luottamuksellisesti työskentelee pankkiautomaatin kanssa, kun varat on nostettu. Eli yksinkertaisuudessaan ainoastaan vaadittuihin tietoihin on oikeanlainen pääsy oikeilla tahoilla. (Andress 2019, luku 1.)

Eheys on tapa estää ihmisiä muokkaamasta tietoja ei-halutulla tavalla. Jotta eheys säilytetään, pitää estää tavat muokata tietoja, mutta myös pystyä palauttamaan ne tällaisen tilanteen sattuessa. Esimerkkinä tiedostot, joille annetaan eri oikeuksia. Tiedoston kirjoitus- ja lukuoikeudet on tärkeä antaa vain niitä tarvitseville. (Andress 2019, luku 1.)

Saatavuus viittaa tarpeeseen, milloin tietoihin pitää päästä käsiksi. Joskus verkkohyökkäyksen tai muun ongelman takia tiedot eivät ole saatavilla. Kun tällaisen hyökkäyksen takana on ulkoinen taho, sitä kutsutaan DoS-hyökkäykseksi. (Andress 2019, luku 1.)

3.3 Laitteen tietoturvan saavuttaminen

Se miten tietoturvaa käytetään, riippuu suojattavasta tuotteesta. Kuten Andress kirjassaan hyvin sanoo: “onko järkeä käyttää miljardeja, jotta voi suojata äidin keksireseptin”. Samaa voi miettiä IT-omaisuudesta, että esimerkiksi kannattaako diaesityksiin käytettyä tietokonetta suojata samalla tavalla kuin asiakastietoihin käytettyä tietokonetta? Nykypäivänä lähes joka tilanteessa tiedot ovat tärkeämpiä, kun fyysinen omaisuus. (Andress 2019, luku 1.)

Jokainen voi pitää henkilökohtaiset laitteensa turvassa päivittämällä uusimpiin ja vakaisiin päivityksiin, käyttämällä vahvoja salasanoja, lataamalla sovelluksia vain luotettavista lähteistä, olemalla avaamatta vieraiden sähköpostin liitteitä ja olemalla liittymättä tuntemattomiin julkisiin verkkoihin. (Andress 2019, luku 1.)

3.4 Yritystietojen herkkyys ja riskit

Ylimääräinen ja sensitiivinen data pitäisi aina poistaa. Yrityksiin kohdistuu tietoturvahyökkäyksiä, joilla voidaan kaapata erittäin sensitiivistä ja yksityistä dataa. Yritykset usein säilyttävät sensitiivistä dataa liian pitkään, koska he eivät tiedä, tarvitaanko sitä myöhemmin tai heillä ei ole tarvittavia taitoja poistaa sitä oikein. Sakot ovat suuria, jos niitä ei noudata. (Stegon 2022.)

Yritykset saavat suuria sakkoja, jos ne eivät noudata vaadittuja säännöksiä. Esimerkkinä Tanskan pankki ei ollut dokumentoinut datan poistamisesta tai niiden käsittelystä vaadittuja dokumentointeja. Tämän seurauksena he saivat 1,3 miljoonan euron sakot GDPR-säännösten noudattamatta jättämisestä. GDPR-lakia noudattamatta jättämisestä tuleva sakko saattaa olla jopa 20 miljoonaa euroa tai neljä prosenttia yrityksen vuosittaisesta tuotosta. (Stegon 2022.)

Toisena esimerkkinä mieleeni tulee paljon otsikoissa pyörinyt tapaus Vastaamo-tietomurrosta. Tämä tapaus kertoo hyvin mielestäni yritystietojen herkkyydestä ja tietoturvahyökkäyksen riskeistä. Vastaamo oli suomalainen psykoterapiakeskus, jonka tietokantaan toteutettiin tietomurto marraskuussa 2018 (Rimpiläinen 2020). Yhteensä yli 33 000 ihmisen potilastiedot anastettiin ja ladattiin Tor-verkkoon (Mantsinen 2023). Kirjoitushetkellä tästä tietomurtotapauksesta on käynnissä oikeudenkäynti.

Koska tietomurtoja yritetään joka 40 sekunnin välein ja kiristyshaittaohjelmat ovat kasvussa, yritysten tietoturvallisuus on tärkeämpää kuin koskaan. Riskienhallinnalla pystytään torjumaan osa haavoittuvuuksista ja suunnittelemaan sitä, mitä tehdään mahdollisessa riskitilanteessa. (Hyperproof 2024.)

3.5 Riskienhallinta

IT-omaisuuden riskienhallinnassa keskitytään uhkiin, jotka kohdistuvat yrityksen laitteistoihin, verkkoihin ja tietoihin. Riskienhallintaa pitäisi käsitellä yrityksessä tasaisin väliajoin, esimerkiksi vuosittain ja myös suurien muutosten tapahtuessa, esimerkiksi yrityskauppojen jälkeen, uusien teknologioiden käyttöönotossa sekä muiden suurien muutosten tapahtuessa. (Hyperproof 2024.)

IT-omaisuuden riskienhallinta on elintärkeä osa jokaista tietoturvasuunnitelmaa. Riskienhallinta näyttää yrityksen riskit ja haavoittuvuudet, jonka avulla voidaan tehdä mahdollisia toimia. Uhkia on muitakin kuin huppu päässä istuva hakkeri yrittämässä päästä yrityksen tietoihin käsiksi. Silti stereotypiasta huolimatta yleistä on, että juuri hakkerit hyödyntävät yrityksen palomuurin tai verkkosivujen heikkouksia. Riskien tunnistusvaiheessa pitää olla valmis miettimään monentyyppisiä uhkia. (Hyperproof 2024.)

Uhka voi olla mikä tahansa asia, joka vahingoittaa yritystä. Hakkerin lisäksi mahdollisia uhkia on:

- phishing tai DoS-hyökkäykset
- laitteiston viat
- ihmisen tekemät virheet
- toimitusketjuun kohdistuvat hyökkäykset tai vahingot
- väärin konfiguroidut asetukset
- luonnon katastrofit.

(Sotnikov 2023.)

Riskienhallinta on tärkeää jokaiselle yritykselle. Sen hyötyjä ovat: arvokkaiksi luokiteltujen laitteiden erityinen huomiointi, riskien ymmärtäminen, haavoittuvuuksien tunnistaminen ja ehkäisy, kustannusten vähentäminen, vaatimustenmukaisuus sekä parempi luottamus asiakkailta. (Sotnikov 2023.)

Riskejä voidaan arvioida kolmea kohtaa tarkastelemalla, jotka ovat: olemassa olevat riskit ja yrityksen sen hetkinen tietoturvataso, IT-omaisuuden arvo sekä kuviteltu profiili tietoturvahyökkäyksen tekijästä (WEF & Deloitte 2015). Riskien arviointiin kuuluu kommunikointi eri osastojen välillä. Tietoturvahenkilöiden pitää selvittää jokaiselta työskentelevältä osastolta niiden toiminnasta, siitä miten työntekijät käyttävät eri järjestelmiä sekä miten tiedot liikkuvat eri järjestelmien välillä. Tämä

prosessi parantaa tietoturvahenkilöiden näkemystä siitä, miten yritys toimii ja missä mahdolliset riskit sijaitsevat. (Hyperproof 2024.)

4 KÄYTÖSTÄPOISTO

IT-omaisuuden käytöstäpoisto on keskeinen osa tietotekniikan elinkaarenhallintaa, sillä se auttaa hahmottamaan IT-omaisuuden elinajan päättymistä, hallitsemaan kustannuksia sekä varmistamaan tietoturvan (CDW 2021). Luvussa käsitellään myös elektroniikkajätteen vaikutusta ympäristöön ja ihmisiin.

4.1 Mikä on käytöstäpoisto

Käytöstäpoisto tarkoittaa yrityksen laitteiston hävittämistä ja hävittämisen jälkitoimia. Yleensä laitteet ovat ihan hyvässä kunnossa, joten ne lahjoitetaan tai myydään. Rikkinäiset laitteet kierrätetään sähkö- ja elektroniikkalaiteromuna. Joissakin yrityksissä laitteet vaihdetaan tietyn väliajoin, jotta varmistetaan työn tehokkuus. Laitteita voidaan myös vaihtaa tapauksissa, joissa korjaaminen maksaa liikaa nähden laitteen arvoon. (Indeed 2022.)

Vanhentunut laite poistetaan yrityksestä ja sitä ei voi jälkeenpäin mitenkään yhdistää organisaatioon. Kaikki merkinnät, yhteydet laitehallinnoista ja muut mahdolliset linkitykset poistetaan. Tämä prosessi takaa tietoturvan. Käytöstäpoisto ei ole ainoastaan laitteen hävittämistä, vaan siinä pitää miettiä talouteen, tietoturvaan sekä ympäristöön liittyvät seikat. Tätä varten voidaan kehittää ITAD-suunnitelma, jossa pitäisi keksiä vastaukset seuraaviin kysymyksiin:

- Milloin laitteet korjataan vaihtamisen sijaan?
- Miten laitteet myydään tai annetaan pois (kenelle?)
- Miten laitteet kierrätetään tai uudelleen käytetään?
- Kuinka laitteet poistetaan käytöstä?

(Asset Panda 2024.)

On myös hyvä miettiä, mitä laitteita ITAD-suunnitelma koskee. Meidän tapauksessamme kuulokkeet, hiiret, näppäimistöt ja muut oheislaitteet hajotessaan kierrätetään työntekijän toimesta. Tietoja sisältävät laitteet, kuten kannettavat tietokoneet tai mobiililaitteet tyhjennetään standardien mukaisesti IT-tiimin toimesta.

Täydellinen tietojen poistaminen on tärkeää kaikille yrityksille. Se varmistaa tietoturvan ja tietosuojasäädöksien noudattamisen. Täydellinen käytöstäpoisto on tärkeää, kun otetaan huomioon, että tyypilliset tyhjennysmenetelmät eivät poista tietoja pysyvästi. Poistetut tiedot ovat edelleen palautettavissa joillakin ohjelmistoilla, jonka takia tietovuodot ovat mahdollisia. (Blancco 2017.)

Haasteina itse huomaan logistiikan. Mitä jos vanha laite on Keski-Euroopassa työntekijällä ja meidän toimistomme sijaitsee Oulussa? Etänä tehtävä tyhjennys ei toimi, joten miten laite saadaan järkevästi takaisin? Laite voi sisältää tärkeää dataa ja se voi päätyä vääriin käsiin kuljetuksen aikana. Tämä voitaisiin ratkaista mielestäni tarpeeksi hyvin tekemällä laitteen omista asetuksista alustamisen, jonka jälkeen laite postitettaisiin IT-tiimille ja viimeisenä koulutettu henkilö tekee tietoturvallisen käytöstäpoiston.

Logistiikan haasteita käsittelee niin sanottu Reverse Supply Chain eli suomeksi käänteinen toimitusketju. Käänteinen toimitusketju on sarja toimia, jossa asiakas palauttaa tai hävittää käytetyn tuotteen. Tässä tapauksessa yrityksen täytyy miettiä hävitettävien laitteiden kohdalla sitä, miten laite toimitetaan kierrätykseen, paljonko sen liikuttaminen maksaa ja laitteen arvon alenemista. Kannettavien tietokoneiden arvo laskee koko ajan, jos ne vaan tyhjennetään, mutta niitä ei palauteta tai myydä. (Guide Jr & Van Wassenhove 2002.)

4.2 Ekologinen näkökulma

Tilannetta omin silmin seuranneena uskon, että laitteiden oikeanmukainen lajittelu tekee suuren muutoksen. Olemme kumminkin Suomessa, jossa ekologisuus tuntuu olevan isossa roolissa verrattuna muihin maihin. Tilanne voi olla eri esimerkiksi Yhdysvalloissa, jossa yritykset ovat valtavia ja laitteita sekä ihmisiä on paljon. Miltä näyttäisi tilanne, jossa yritykset heittäisivät jokaisen vanhan laitteen luontoon?

Blanccon mukaan vuonna 2021 heidän työkalujen avulla tyhjennettiin 68,2 miljoonan kilon edestä elektronisia laitteita. Blancolla tyhjennettyjä laitteita voidaan käyttää uudelleen turvallisesti, mikä myös tarkoittaa, että laitteita ei tarvitse valmistaa alusta asti niin paljon. Elektronista jätettä tungetaan tonneittain kehittyviin maihin, vaikka sitä vastaan on olemassa kansainväliset säännökset; tämä vahingoittaa ihmisiä sekä heitä ympäröivää luontoa. Blancco toimii vastuullisesti näiden säännösten mukaan. (Blancco 2022.)

Silti yli 80 % elektronisista laitteista päätyy myrkyllisenä jätteenä kaatopaikoille. Väärin kierrätetyt laitteet vievät tilaa sekä vuotavat muun muassa elohopeaa vesistöihin ja muualle luontoon. Se miten kierrättää, tulisi olla ensisijainen tavoite, eikä korvaus siitä. Kustannukset tai korvaukset ovat mitättömiä verrattuna poliittiseen arvoon tai ekologisuuteen. (Kaestner, 2009.)

5 LAIT JA STANDARDIT

Toimeksiantajan toimesta tähän työhön vaaditaan HIPAA-lain vaatimukset täyttävät tyhjennystyökalut. Tässä luvussa kerron hieman HIPAA-laista sekä NIST SP 800-88 R1 –standardista. Nämä aiheet ovat erittäin laajoja ja komplekseja, mutta pyrin kertomaan niistä vain tärkeät kohdat liittyen opinnäytetyöhön.

5.1 HIPAA-laki

Health Insurance Portability and Accountability Act (HIPAA) on vuonna 1996 asetettu laki, joka sääntelee terveystietojen käytöstä. Se sisältää vaatimukset laitteiden ja datan hävittämisestä. HIPAA on luotu suojelemaan asiakkaiden sensitiivistä dataa. HIPAA ei aseta tiettyjä tietojen puhdistamista koskevia sääntöjä, mutta siinä puhutaan tarpeettomaksi käyneiden tietojen hävittämisen tarpeesta HIPAA-vaatimusten täyttämiseksi. (Blancco 2024a.)

Yritysten vastuulla on kehittää tietoturvallinen tietojen hävittäminen, jotta ne välttävät sakot noudattamattomuudesta. Vuonna 2013 voimaan tullut HIPAA Omnibus -sääntö lisäsi HIPAA-vaatimuksen rikkomisesta aiheutuvan sakon enimmäismääräksi 1,5 miljoonaa Yhdysvaltain dollaria. (Blancco 2024a.)

5.2 NIST SP 800-88 R1 -standardi

NIST SP 800-88 R1 on Yhdysvaltain hallituksen luoma standardi, joka tarjoaa ohjeita tietojen poistamiseen. Nimi tulee sanoista National Institute of Standards and Technology, Special Publication 800–88 Revision 1. Standardin tavoitteena on tyhjentää laitteet tehokkaasti, niin ettei tietoja voida palauttaa. Hallituksen käyttöön otettu standardi on nykyään käytössä monissa yksityisissäkin yrityksissä, sillä se on paras tapa varmistaa, ettei laitteille jää mitään tyhjennyksien jälkeen. Standardi tunnetaan yleisesti kolmesta tekniikasta, jotka ovat Clear, Purge ja Destroy. (NIST SP 800-88 R1, 1–4.)

Clear on loogista suoritustapaa käyttävä sekä yksinkertainen tyhjennystekniikka, joka hyödyntää tietojen ylikirjoittamista tai laitteiden resetointia. Tämä tekniikka on myös näistä kolmesta vähiten

tietoturvallinen, sillä joillakin työkaluilla voidaan hankkia dataa laitteesta tyhjennyksen jälkeenkin. (NIST SP 800-88 R1, 1–4.)

Purge on loogista ja fyysistä suoritustapaa käyttävä tyhjennystekniikka. Datan palauttaminen tehdään mahdottomaksi nykyaikaisilla laboratoriotekniikoilla, kuten ylikirjoittamalla, lohkojen poistamisella sekä salausteknisellä tyhjennyksellä. (NIST SP 800-88 R1, 24.)

Destroy on fyysistä suoritustapaa käyttävä tyhjennystekniikka. Sulattaminen, polttaminen, jauhaminen, silppuaminen ja hajottaminen voidaan luetella tämän alle. Tämä tekniikka muokkaa laitteen fyysistä olemusta, jotta sitä ei voida uudelleenkäyttää. Ainoastaan käytetään, jos Purge tai Clear ei ole mahdollista käyttää, tai jossain muussa harvinaisessa tapauksessa. (NIST SP 800-88 R1, 25.)

6 TYHJENNYSMENETELMÄT

Tässä luvussa käydään läpi Blanccon taustoja sekä toiminnallisessa osuudessa käytettyjä tyhjennysmenetelmiä. Opinnäytetyön kannalta tärkeä tyhjennysmenetelmä on sovelluspohjainen tietojen ylikirjoittaminen.

6.1 Blancco Technology Group

Työkalut valittiin Blancco Technology Group nimiseltä yritykseltä. Yrityksessä työskentelee yli 350 työntekijää eri puolilla maailmaa. Heidän työkalujen avulla tyhjennetään yli 70 000 laitetta päivittäin. Blancco tukee yli 25 eri standardia ja sertifikaattia. (Blancco 2024b.)

Blancco keskittyy käytetyn IT-omaisuuden uudelleenkäyttöön, tietojen tyhjennysmenetelmiin, riskienhallintaan sekä markkinatalouden tukemiseen. Vuositasolla Blanccoa käyttämällä tyhjennetään kymmeniä miljoonia laitteita. Tyhjennyksillä varmistetaan käytöstä poistetun laitteen luvattoman käytön estäminen ja samalla huolehditaan tietoturvasta. (Blancco 2024b.)

6.2 Vaatimukset täyttävät tyhjennysmenetelmät

HIPAA-säädökseen sopivat tyhjennysmenetelmät:

- Salaustekninen tai kryptografinen tyhjennys. Tehokas menetelmä, jos tarvitaan nopea tyhjennys, tai laite on liikkeessä.
- Sovelluspohjainen tietojen ylikirjoittaminen. Tehokas menetelmä lähes jokaiseen tilanteeseen. Käytössä tässä opinnäytetyössä.
- Fyysinen tuhoaminen. Helppo ratkaisu, jos ei tiedä miten toteuttaa muita tietoturvallisia tyhjennysmenetelmiä.

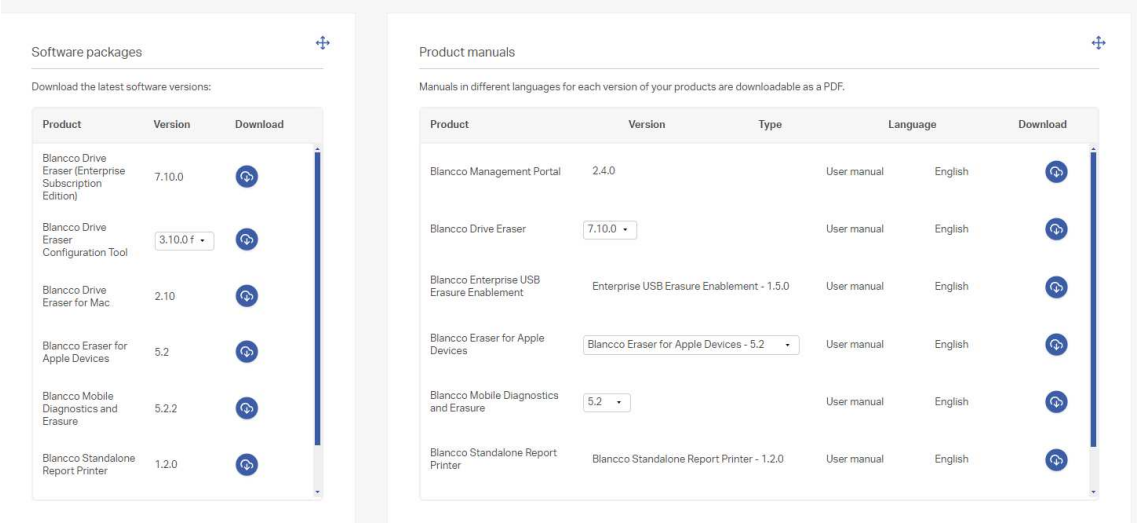
Sovelluspohjainen tietojen poistaminen tai ylikirjoittaminen on tapa korvata vanhat tiedot satunnaisen päällekirjoituksen avulla. Menetelmä toimii siten, että binääriluvuilla yksi ja nolla kirjoitetaan satunnaisesti jokaiseen kiintolevyn sektoriin. Tämä varmistaa, että tiedot ovat pysyvästi palauttamattomia samalla säilyttäen laitteen toimintakyvyn. Tätä käytetään tietokoneisiin, palvelimiin, mobiililaitteisiin sekä ulkoisiin tallennusvälineisiin. (Blancco 2021.)

7 TOTEUTUS

Toteutus-luvussa käsitellään toiminnallista osuutta. Aluksi tutustuin työkaluihin, jonka jälkeen konfiguroin, testasin ja otin ne käyttöön. Luvun lopussa käsittelen lyhyesti dokumentointia ja työkalujen opastusta muille työntekijöille.

7.1 Tutustuminen työkaluihin

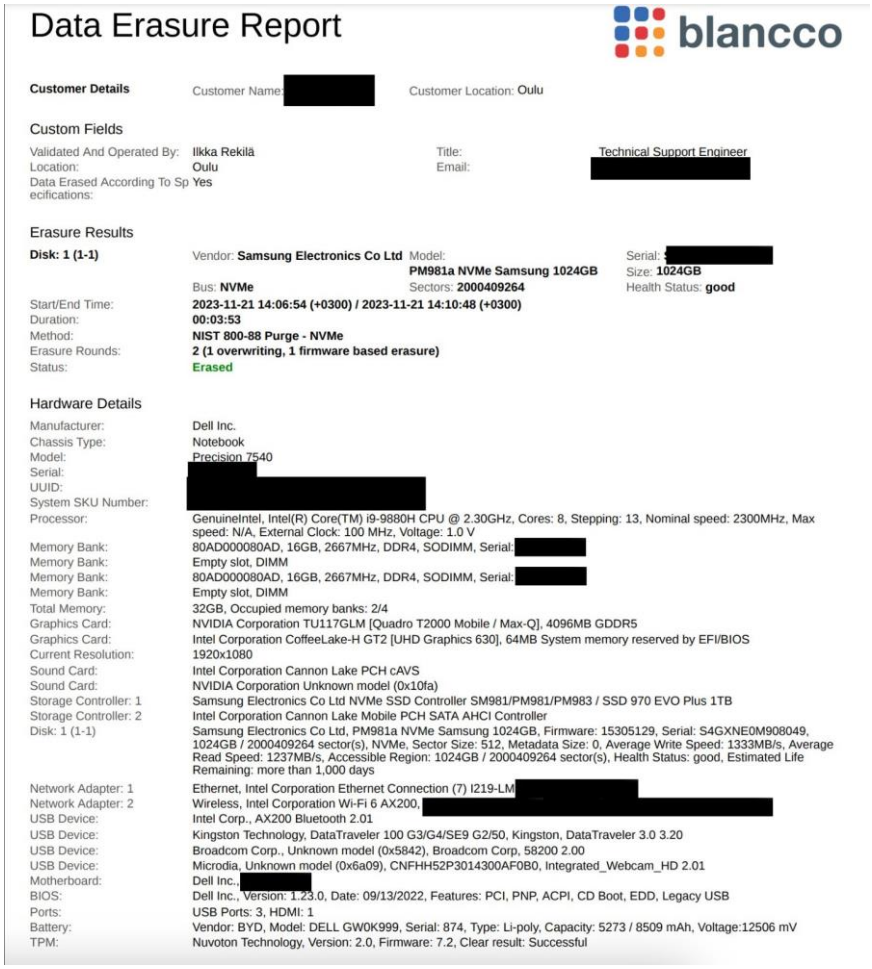
Lähdin tutustumaan työkaluihin Blancco Management Portal -hallintaportaalin kautta. Sieltä löytyvät tukisivun alta yritykselle valikoidut sovellukset, jotka on valittu käyttötarpeiden mukaisesti. Jokaiselle työkalulle on saatavilla hyvin laajasti kirjoitettu ohjekirja. Hallintaportaalissa järjestelmänvalvojat pystyvät kutsumaan uusia käyttäjiä tarpeiden mukaan, analysoimaan ja tutkimaan statistiikkaa sekä lukemaan raportteja tyhjennyksistä. Hallintaportaali tukee täysin kaikkia heidän luomia työkalujaan. (Blancco 2024c.) Kuviosta 2 ilmenee yritykselle sopimuksen mukaan räätälöidyt työkalut ja ohjeet.



KUVIO 2. Blancco Management Portal, Support & help –sivu, jonka alta näkee ladattavissa olevat paketit ja ohjekirjat.

Itse kutsuin kaikki IT-tiimissä työskentelevät henkilöt käyttäjiksi, jotta mahdollisessa tyhjennystilanteessa jokaisella on aktiivinen tili. Tilin sähköpostia ja salasanaa kysytään jokaisen tyhjennyksen aloitusvaiheessa, joiden syöttämisen jälkeen työkalu osaa kaivaa lisenssin portaalista. Valmiista tyhjennyksistä syntyy raportti. Raportit tyhjennyksistä saa ladattua yleisissä tiedostomuodoissa,

kuten XML, PDF ja CSV. Raportit ovat tärkeitä mahdollisissa auditoinneissa, sillä ne sisältävät vaadittavat tiedot tyhjennyksestä. Kuviossa 3 on esimerkkiraportti. (Blancco 2024c.)



Data Erasure Report

blancco

Customer Details Customer Name: [redacted] Customer Location: Oulu

Custom Fields

Validated And Operated By: Ilkka Rekilä Title: Technical Support Engineer
Location: Oulu Email: [redacted]
Data Erased According To Specifications: Yes

Erasure Results

Disk: 1 (1-1) Vendor: **Samsung Electronics Co Ltd** Model: **PM981a NVMe Samsung 1024GB** Serial: [redacted]
Bus: **NVMe** Sectors: **2000409264** Size: **1024GB** Health Status: **good**

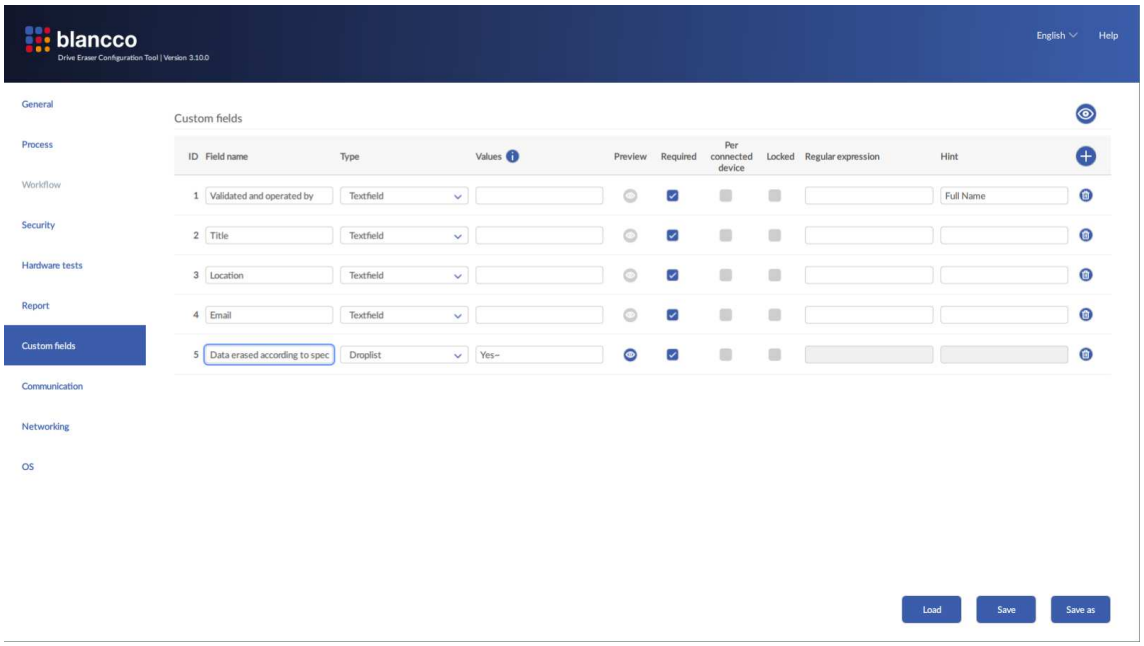
Start/End Time: **2023-11-21 14:06:54 (+0300) / 2023-11-21 14:10:48 (+0300)**
Duration: **00:03:53**
Method: **NIST 800-88 Purge - NVMe**
Erasure Rounds: **2 (1 overwriting, 1 firmware based erasure)**
Status: **Erased**

Hardware Details

Manufacturer: Dell Inc.
Chassis Type: Notebook
Model: Precision 7540
Serial: [redacted]
UUID: [redacted]
System SKU Number:
Processor: GenuineIntel, Intel(R) Core(TM) i9-9880H CPU @ 2.30GHz, Cores: 8, Stepping: 13, Nominal speed: 2300MHz, Max speed: N/A, External Clock: 100 MHz, Voltage: 1.0 V
Memory Bank: 80AD000080AD, 16GB, 2667MHz, DDR4, SODIMM, Serial: [redacted]
Memory Bank: Empty slot, DIMM
Memory Bank: 80AD000080AD, 16GB, 2667MHz, DDR4, SODIMM, Serial: [redacted]
Memory Bank: Empty slot, DIMM
Total Memory: 32GB, Occupied memory banks: 2/4
Graphics Card: NVIDIA Corporation TU117GLM [Quadro T2000 Mobile / Max-Q], 4096MB GDDR5
Graphics Card: Intel Corporation CoffeeLake-H GT2 [UHD Graphics 630], 64MB System memory reserved by EFI/BIOS
Current Resolution: 1920x1080
Sound Card: Intel Corporation Cannon Lake PCH cAVS
Sound Card: NVIDIA Corporation Unknown model (0x10fa)
Storage Controller: 1 Samsung Electronics Co Ltd NVMe SSD Controller SM981/PM981/PM983 / SSD 970 EVO Plus 1TB
Storage Controller: 2 Intel Corporation Cannon Lake Mobile PCH SATA AHCI Controller
Disk: 1 (1-1) Samsung Electronics Co Ltd, PM981a NVMe Samsung 1024GB, Firmware: 15305129, Serial: S4GXNE0M908049, 1024GB / 2000409264 sector(s), NVMe, Sector Size: 512, Metadata Size: 0, Average Write Speed: 1333MB/s, Average Read Speed: 1237MB/s, Accessible Region: 1024GB / 2000409264 sector(s), Health Status: good, Estimated Life Remaining: more than 1,000 days
Network Adapter: 1 Ethernet, Intel Corporation Ethernet Connection (7) I219-LM [redacted]
Network Adapter: 2 Wireless, Intel Corporation Wi-Fi 6 AX200, [redacted]
USB Device: Intel Corp., AX200 Bluetooth 2.01
USB Device: Kingston Technology, DataTraveler 100 G3/G4/SE9 G2/50, Kingston, DataTraveler 3.0 3.20
USB Device: Broadcom Corp., Unknown model (0x5842), Broadcom Corp, 58200 2.00
USB Device: Microdia, Unknown model (0x6a09), CNFHH52P3014300AF0B0, Integrated_Webcam_HD 2.01
Motherboard: Dell Inc., [redacted]
BIOS: Dell Inc., Version: 1.23.0, Date: 09/13/2022, Features: PCI, PNP, ACPI, CD Boot, EDD, Legacy USB
Ports: USB Ports: 3, HDMI: 1
Battery: Vendor: BYD, Model: DELL GW0K999, Serial: 874, Type: Li-poly, Capacity: 5273 / 8509 mAh, Voltage:12506 mV
TPM: Nuvoton Technology, Version: 2.0, Firmware: 7.2, Clear result: Successful

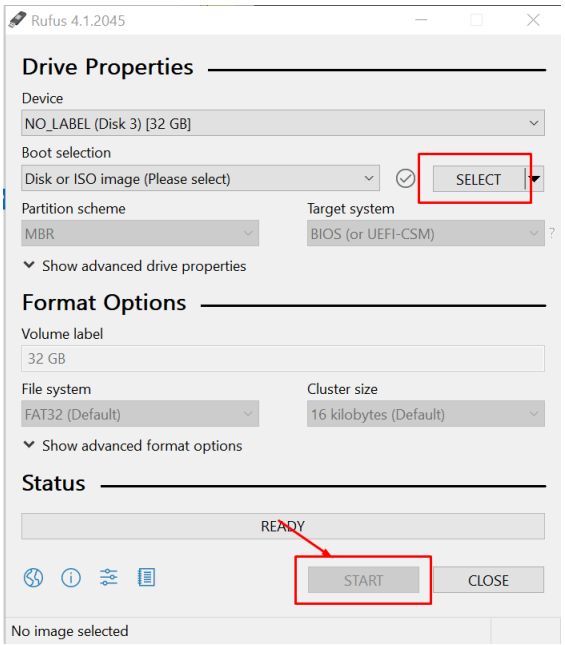
KUVIO 3. Kuvakaappaus esimerkkiraportista. Vihreä väri ja sana "Erased" kertoo selkeästi, että laite on tyhjennetty.

Työkalujen konfiguraatioon käytetään kuviossa 4 näkyvää Blancco Drive Eraser Configuration Tool (DECT) -sovellusta, jonka monipuolisten vaihtoehtojen avulla pystytään muokkaamaan tyhjennys halutulla tavalla. Haluttu ohjelmistoversio ladataan sovellukseen ISO-tiedostona, jonka jälkeen valmiiksi muokattu työkalu asennetaan USB-muistitikulle.



KUVIO 4. DECT – Custom fields kohdat on asetettu vaatimusten mukaisesti

Konfiguroinnin ensimmäinen ongelma tuli vastaan, kun Blancco USB Creator –työkalu ei toiminut, joten jouduin käyttämään Rufusta sen sijaan. Rufus on avoimen lähdekoodin sovellus, jolla voi kätevästi luoda ISO-tiedostoista asennuspaketteja USB-muistitikuille (Rufus 2024). Sovellus oli minulle tuttu jo ennestään, joten en epäröinyt hetkeäkään sen käyttämistä. Alla kuvio Rufuksesta. Kuvio 5 oli osana toimeksiantajalle luomaani dokumentaatiota, jossa punaiset neliöt tarkoittivat tehtäviä työvaiheita.



KUVIO 5. Kuvakaappaus Rufus-sovelluksesta

7.2 Blancco Drive Eraser

Windows-laitteita varten tyhjennykseen käytetään työkalua Blancco Drive Eraser (Blancco 2024d.) BDE-työkalun minimivaatimukset tietokoneelle on:

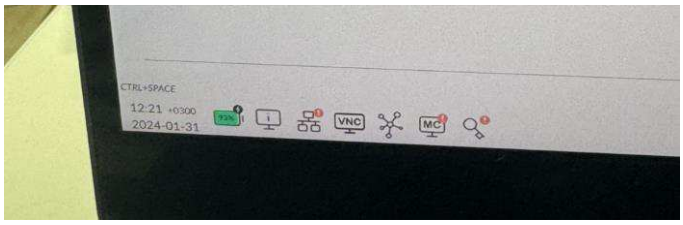
- BIOS:in kello on ajan tasalla.
- Virransäästöasetukset ovat poissa päältä.
- Tietokone käynnistetään AHCI-tilassa.
- On suositeltua, että kannettavat tietokoneet ovat latauksessa tyhjennyksen ajan.

Aluksi tämän työkalun konfiguraatioon meni aikaa, sillä halusin varmistaa, että sitä ei tarvitse jatkossa muokata. Halusin itse kaikki pienetkin hidasteet ja kirjoitusvirheet pois, ettei jatkossa tarvitse samaa virhettä korjata jokaisen tyhjennyksen aikana. Nämä asetukset muokattiin valmiiseen tiedostoon:

- Host name ja portti on asetettu hallintaportaalin kanssa samaksi, joten raportit löytävät tätä reittiä perille.
- NIST 800-88 Purge on valmiiksi valittuna tyhjennystekniikkana. Mahdollisessa virhetilanteessa laite tyhjentyy NIST 800-88 Clear-tekniikan mukaisesti.
- TPM-turvapiirin tyhjentäminen ja päältä pois asettaminen.
- Laite yhdistyy automaattisesti yrityksen verkkoon.
- Kirjautumisikkunassa on valmiiksi käyttäjän loppuosa, joka on kaikilla käyttäjillä sama.

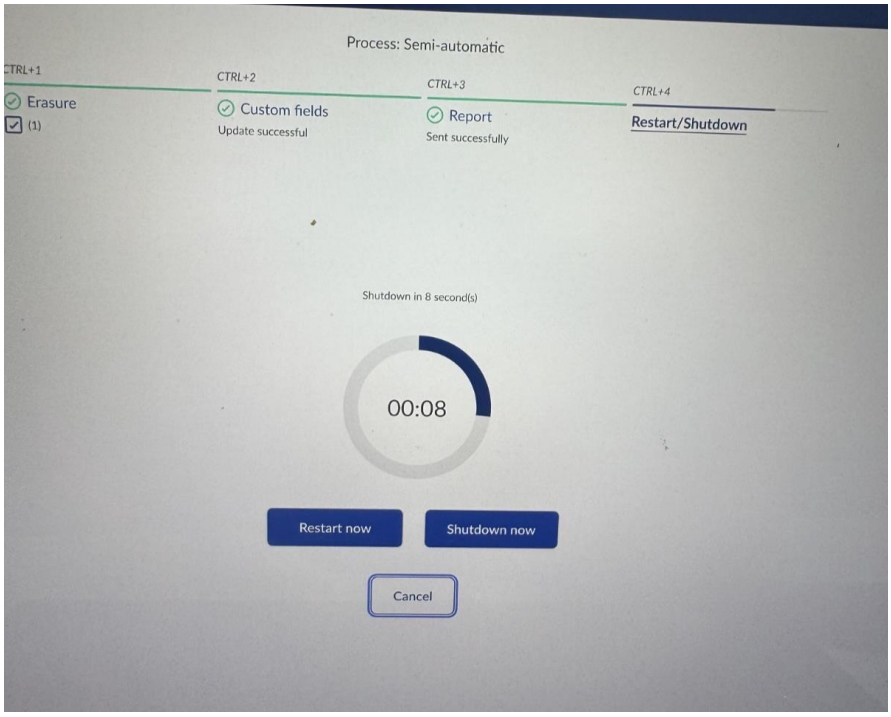
Heti ensimmäisenä työkalun käynnistyessä, se kysyy sähköpostia sekä salasanaa. Tähän käytetään hallintaportaalin kautta luotua tiliä. Seuraavaksi näytöllä näkyy tyhjennettävänä oleva kiintolevy. Jos työkalu on hyvin konfiguroitu, tyhjennys alkaa automaattisesti. Yhdessä tyhjennystilanteessa minulla oli kannettava tietokone, joka ei yhdistynyt automaattisesti yrityksen verkkoon. Tässä tapauksessa tyhjennys pitää aloittaa itse manuaalisesti.

Sovellus kertoo alapalkissa väreillä, jos joku on vialla. Kuviosta 6 näkee, kuinka tässä tapauksessa internetyhteyden sekä lisenssin kohdalla on punainen valo. Tämän virheen korjaamiseksi asetuksista pystyy manuaalisesti vaihtamaan toiseen verkkoon. Verkon valo vaihtuu vihreäksi ja laite saa lisenssin hallintaportaalin kautta. Tämän jälkeen kaikki merkkivalot näyttävät vihreää, joten alapalkin oikeasta reunasta Erase-nappia painamalla tyhjennyksen saa aloitettua. Mahdollisissa ongelmatilanteissa on mahdollista ottaa tukeen yhteyttä tai ilmoittaa virheestä Report issue –nappia painamalla.



KUVIO 6. Alapalkin virhevalot

Kun tyhjennys on valmis, laite on valmiina hävitettäväksi. Tyhjennyksen jälkeen on hyvä tarkistaa, että laite ei löydy enää yrityksen laitehallinnasta. Jos laite löytyy laitehallinnasta, se täytyy poistaa, ettei uudelleenasennuksessa laite rekisteröidy yritykseen. Alla kuvio 7 tyhjennyksen valmistumisesta.



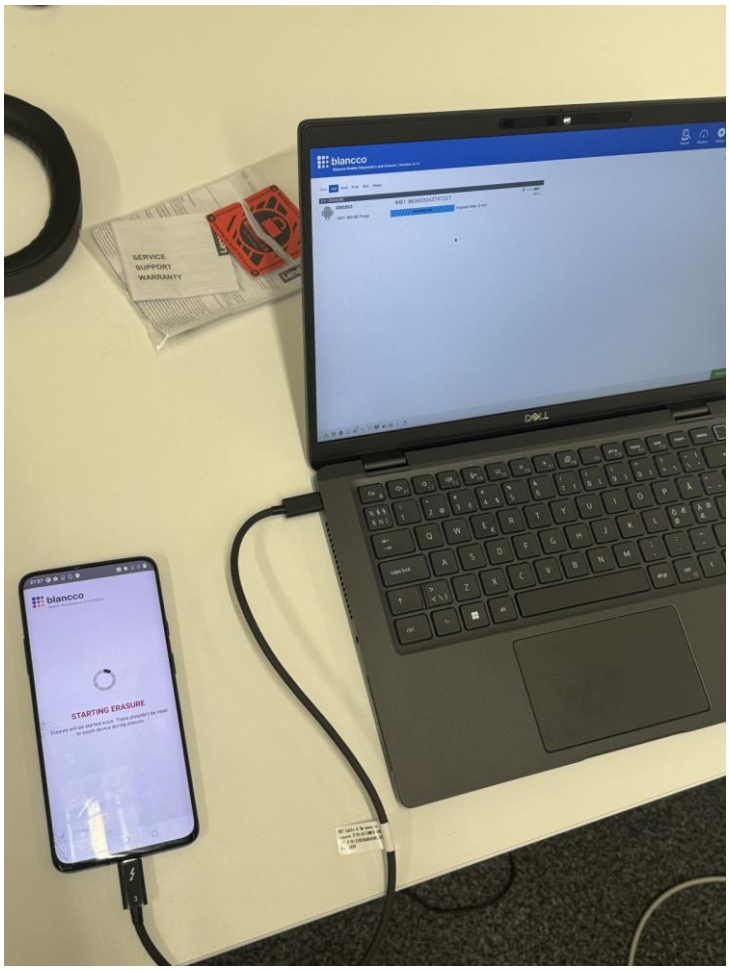
KUVIO 7. Valmis tyhjennys

7.3 Blancco Mobile Diagnostics and Erasure

Mobiililaitteiden tyhjennykseen käytetään työkalua Blancco Mobile Diagnostics and Erasure (Blancco 2024e). Tämä työkalu eroaa Windows-laitteiden tyhjennyksestä paljon, sillä tämä asennetaan yhdelle tietokoneelle ja siitä valmistuu yritykselle mobiililaitteiden tyhjennysasema. Tyhjen-

nysasemaa voidaan käyttää iOS- ja Android-laitteiden tyhjennykseen. Tähän asennukseen piti etsiä yrityksestä poistunut vanha kannettava tietokone, jonka pystyi asentamaan tyhjennysasemaksi. Tällä asemalla pystyy halutessaan tyhjentämään useita puhelimia kerrallaan. Latasin hallintapaneelista BMDE ISO-tiedoston, jonka avasin Rufuksella. Ainoa konfiguraatio mitä itse piti tehdä, oli vaihtaa muistitikku DD-tilaan.

Puhelin yhdistetään USB-kaapelilla tyhjennysasemaan. Tyhjennys vaihtelee paljon riippuen puhelimen merkistä ja mallista. Käytin esimerkkitilanteessa OnePlus 7 Pro –puhelinta. Tyhjennysasema ilmoittaa mitä laitteelle pitää tehdä, jotta se voidaan tyhjentää. Tässä tapauksessa tuli ilmoitus, että puhelimesta pitää laittaa päälle kehittäjäasetukset. Näissä tilanteissa selviää yleensä hakemalla Googlen avulla puhelimen mallin ja virhekoodin. Puhelin alkaa tyhjentymään ja raportista selviää, onko se tyhjentynyt vaatimusten mukaisesti. Kuviossa 8 näkyy tyhjennysasema ensimmäistä kertaa testissä. Testi oli onnistunut ja työkalu otettiin käyttöön.



KUVIO 8. Tyhjennysasema ensimmäisessä testiajossa

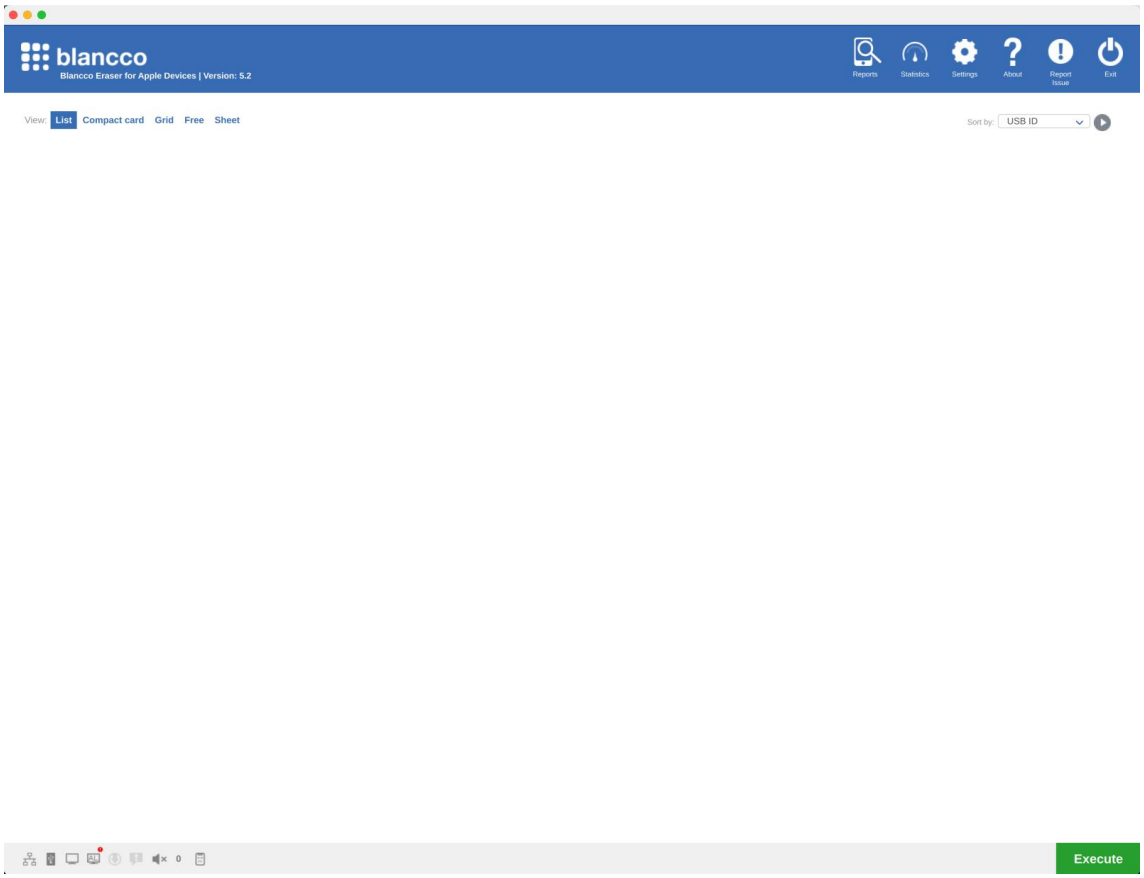
7.4 Blancco Eraser for Apple Devices

Applen laitteiden tyhjennystä varten on työkalu Blancco Eraser for Apple Devices (Blancco 2024f). BEAD vaatii, että käytössä on Applen valmistama tietokone. Otin itse MacBook Pro -kannettavan käyttöön juuri tämän opinnäytetyön aikana, joten pystyin testaamaan sekä Windows- että macOS-ympäristöt.

Tämän työkalun vaatimuksena on:

- Applen valmistama Mac-laite
- USB-C-kaapeli
- MacOS on yhteensopiva Apple Configurator –sovelluksen kanssa. Uusin versio käyttöjärjestelmästä olisi muutenkin hyvä olla asennettuna.
- internetyhteys
- käyttäjä Blancco hallintaportaliin
- lisenssi.

Varmistetaan että Apple Configurator -sovellus löytyy päälaitteelta, eli laitteelta, jolla tyhjennys tehdään. Jos sitä ei löydy, se on ilmaisena ladattavana App storen kautta kaikille Mac-laitteille. Heti kun molemmat sovellukset näkyvät tietokoneella, käynnistetään ne. Luetaan ja hyväksytään käyttöehdot, jonka jälkeen syötetään hallintaportaaliin luotu käyttäjä kirjautumisruutuun. Seuraavaksi luodaan sovellukseen yksi paikallinen tili. Kuviossa 9 näkyy BEAD kirjautumisen jälkeen.



KUVIO 9. BEAD kirjautumisen jälkeen

BEAD:in yksi huono puoli on se, että vain sovelluksen asentanut käyttäjä pystyy sitä käyttämään. Eli meidän tapauksessamme yhdellä yhteiskäyttölaitteella ainoastaan tämän asentanut pystyy käyttämään sovellusta.

Kytketään tyhjennettävä laite USB-C-kaapelilla päälaitteeseen. Tämän jälkeen tyhjennettävä laite täytyy saada Device Firmware Upgrade (DFU) -tilaan. DFU-tilaan pääsemiseksi, laite on sammutettava ja asetettava lataukseen. Seuraavaksi painetaan virtanäppäin pohjaan, jonka jälkeen heti painetaan pohjaan vasemmanpuoleinen Option- ja Control-näppäin sekä oikeanpuoleinen Shift-näppäin. Tyhjennettävällä laitteella ei välttämättä näy mitään merkkiä DFU-tilasta, mutta päälaitteella näkyy Apple Configurator sovelluksessa DFU-logo. (Apple Support 2024.)

Laitteen pitäisi näkyä nyt BEAD-sovelluksen listanäkymässä. Mahdollisessa ongelmatilanteessa laitteen alle ilmenee keltainen kolmio, jonka päälle hiiren viedessä, se kertoo mitä pitää tehdä virheen korjaamiseksi. Laite on nyt mahdollista tyhjentää painamalla Erase device –nappia. Laitteen

tyhjentymisen jälkeen, raportti täytyy lähettää manuaalisesti Reports-sivulta. Alla oleva kuvio näyttää työvaiheet. Ensin laite on yhdistetty, jonka jälkeen aloitetaan tyhjennys ja viimein laite on tyhjennetty. Prosessi on yleensä nopea, omasta kokemuksesta noin 3–10 minuuttia.

7.5 Työkalujen testaus ja käyttöönotto

Työkalut testattiin heti kun se oli mahdollista. Ensimmäisenä otettiin käyttöön BDE, jonka avulla saatiin kaapeista vanhoja tietokoneita pois. BDE aluksi tyhjensi laitteita väärällä standardilla, mutta se oli nopeasti korjattavissa. Aluksi käytössä oli tietokoneen komponenttien tarkistus, mutta huomasin että se vie turhaa aikaa. Testausvaiheissa ei ilmentynyt suurempia ongelmia, joten pystyin ottamaan työkalut käyttöön melko ripeästi.

Onnistuneiden testauksien jälkeen ensimmäinen työkalu otettiin käyttöön heinäkuussa 2023. Tämän jälkeen muut työkalut otettiin käyttöön syksyn aikana. Niitä aluksi käytettiin hitaasti, ettei raportista puutu vaadittavia tietoja tai vaatimuksia. Tällä hetkellä maaliskuussa tätä kirjoittaessa työkalujen avulla on tyhjennetty 175 laitetta, joka tarkoittaa noin 19 laitetta kuukaudessa. Kuvittele tilanne ilman tällaisia työkaluja. Miltä yrityksen IT-huoneen hyllyt näyttäisivät viiden vuoden kuluttua?

7.6 Dokumentointi sekä työkalujen opastus

Kaikki toimenpiteet ja tehdyt muutokset dokumentoitiin yrityksen omaan tietopankkiin. Kuviosta 10 näkee esimerkki dokumentaation BDE-työkalusta. Mahdollisissa uudelleenasennus- tai ongelmatilanteissa näitä dokumentteja pystytään käyttämään apuna. Pyrin tekemään dokumentoinnista aluksi helposti lähestyttävän, jotta prosessi ei tuntuisi monimutkaiselta. Työkalujen käyttöönotossa huomasin dokumentaatiossa aukkoja ja täydensin niitä jälkeenpäin. Dokumentointi IT-alalla on erittäin tärkeää lähes jokaisessa tilanteessa. Jatkossa tulen päivittämään dokumentointia muiden palautteen perusteella tai mahdollisten uusien ongelmatilanteiden takia.

Wiping the device

This is working at least for Dell models; you might need to adapt and Google some things if you are wiping different models.

BIOS

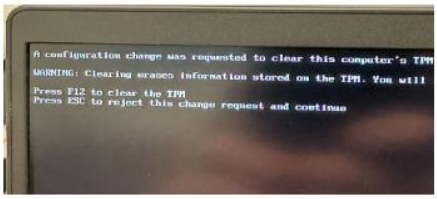
1. Plug the Blancco USB stick into the device you want to wipe.
2. Power up the device. Press F2 simultaneously to get into the BIOS.
3. Go to Boot Configuration, and lift the USB stick to the top of the boot order, and disable Secure Boot
4. Next, go to Storage > AHCI/NVMe if not already on.
5. Apply changes and Exit from the BIOS

Blancco

Make sure you have account in Blancco Management Portal

Power up your laptop and **don't** touch anything. Blancco will open automatically, and it will select the right mode as well. It might freeze a bit.

Press F12 to clear the TPM



It will now open again, and you should see a window where you can type the Blancco username and password

If all of the buttons are green on the bottom left side of the screen, it will start wiping automatically.

Then fill out the custom fields and press update.

KUVIO 10. Esimerkki dokumentaatio Blancco Drive Eraser käyttöönotosta

Opastin omatoimisesti sovelluksen käytöstä pikaisesti muille tiimin jäsenille. Valmiiden konfiguraatioiden ja dokumentoinnin ansiosta käyttöönotto on ollut helpompaa muilla toimistoilla, sillä ne vaativat ainoastaan työkalun asentamisen ilman ylimääräistä säätämistä. Muiden työntekijöiden mielestä tyhjennystyökalut ovat selkeitä ja järkeviä.

8 TULOKSET

Opinnäytetyön tulos on hyvä kokonaisuus, jonka kirjoittaminen opetti minua kirjoittamaan, perehtymään enemmän aiheeseen sekä ymmärtämään tätä kokonaisuutta paremmin. Opinnäytetyö myös vaikuttaa positiivisesti toimeksiantajaan. Työn aikana oli vähän haasteita työmäärään suhteutettuna.

8.1 Haasteet työkalujen käyttöönotossa

Asennuksien ja konfiguraatioiden kanssa oli hieman ongelmia, mutta mitään paljon hidastavaa ei tapahtunut. BDE-työkalun konfiguraatiot vaativat hieman testailua ja dokumentaation lukemista. Mobiililaitteiden tyhjennyssovellus oli hankala saada aluksi toimimaan. Tyhjennysasema pyöritti Blancco-logoa ja näytti siltä, että se lataa jotain. Kuitenkin jopa tunnin odottelun jälkeen se pyöri edelleen. Epähuomiossa en huomannut dokumentoinnissa pientä tekstiä, että työkalu pitää asentaa DD-tilassa. Tämä ratkesi ja tyhjennysasema saatiin käyttöön.

Ainoat tarpeet, joita en saanut toteutettua, olivat etätyhjennys ja raportin automaattinen lähetys toiseen tietokantaan. Etätyhjennys helpottaisi tilanteessa, kun työntekijä ei pysty fyysisesti palauttamaan laitetta tai laitteen lähettäminen tulee olemaan vaikeaa, esimerkiksi ulkomailta etänä työskentelevät henkilöt. Raportin automaattinen lähetys helpottaisi meitä huomattavasti, ja sen avulla voisi poistaa laitteet muista tietokannoista esimerkiksi sarjanumeron perusteella. Nämä todennäköisesti saadaan toteutettua tulevaisuudessa, mutta tärkein eli vanhojen laitteiden paikallinen tyhjennys saatiin tehtyä onnistuneesti.

8.2 Työkalujen vaikutus

Työkalujen käyttöönotto on vaikuttanut toimeksiantajaan positiivisesti. Vanhat, jopa hieman rikkinäiset laitteet on saatu pois hyllyiltä pölyttymästä. Tällaisilla laitteilla ei yritys oikeasti tee mitään, mutta ei niitä suoraan roskiinkaan voi heittää. Tyhjennystyökalujen avulla arvottamaksi luokitellut laitteet saadaan lahjoitettua, kotikäyttöön tai kierrätettyä. On sanomattakin selvää, että yrityksen tietoturva ja vaatimustenmukaisuus voivat tämän avulla paremmin.

Omasta mielestä yksi hienoimmista hetkistä tämän opinnäytetyön aikana oli tilanne, jossa lahjoitettiin Sambiaan kymmenen käytettyä tietokonetta. Vanhat tietokoneet yrityksen perustamisaikakaudelta eli noin kymmenen vuoden takaa, ovat nykypäivänä lähes arvottomia Suomessa. Tilanne on eri monessa Afrikan maassa. Nämä tietokoneet opastavat sambialaisia tietokoneiden käyttöön ja mahdollisesti lisää heidän kiinnostustansa tietokoneisiin ja niihin liittyviin aloihin.

Vanhoja laitteita on lahjoitettu myös esimerkiksi työntekijöiden lapsille opintoja varten, mikä on mahtavaa. Opiskelijoilla ei välttämättä ole rahaa ostaa itse tietokonetta, joten heidän tukemisensa myös itse opiskelijana tuntuu oikealta. Nämä prosessit saattavat tuntua yrityksessä melko pieniltä, mutta niillä on merkittävä vaikutus laitteen uusille omistajille.

9 POHDINTA

Suoritin toiminnallisen osuuden syksyllä 2023. Pyrin tekemään suurimman osan töistä itse, sillä halusin haastaa itseä ja kehittää omia taitojani ilman liiallista tukea työkavereilta.

Opinnäytetyön aihe tuli mieleen vasta, kun työkalut oli jo osittain otettu käyttöön. Tämä hieman vaikeutti opinnäytetyön kirjoittamista, sillä sen olisi voinut suunnitella ja kirjoittaa selkeämmin aiemmin. Vaikka olin aikaisemmin tehnyt dokumentaatiot, jouduin kuitenkin uudelleenasentamaan joitakin työkaluja. Joka tapauksessa tämä osoittautui loppujen lopuksi positiiviseksi asiaksi, koska samalla päivitin dokumentaatioita uudelleen tämän raportoinnin aikana.

Omasta mielestä opinnäytetyön aihe on yksinkertainen, mutta siitä saa huomattavan vaikean riippuen siitä, mihin haluaa perehtyä ja mistä kirjoittaa. Aihe on laaja. Yhtenä ärsyttävimpänä haasteena huomasin IT-alan sanaston kääntämisen suomeksi. Pyrin kääntämään sanaston järkevästi, välillä itsekin pohtien, että mitähän juuri kirjoittamani lause tarkoittaa.

Mielestäni opinnäytetyön kirjoittaminen opetti paljon enemmän, kun itse toiminnallinen osuus. Opinnäytetyön kirjoittamisen aikana piti lueskella erinäisiä lähteitä ja kirjoja. Aiheeseen liittyviä kirjoja oli hieman hankala löytää. Huomasin myös, että nyt minulla on parempi kuva siitä kokonaisuudesta, miksi tätä ylipäätänsä tehdään yrityksissä. Opin paljon tietoturvasta, IT-omaisuudenhallinnasta ja tietojen arkaluontoisuudesta.

Uskon, että tästä opinnäytetyöstä on hyötyä itselle, mutta mahdollisesti myös yrityksille, jotka miettivät näitä asioita. Toimeksiantaja hyötyy myös opinnäytetyöstä, sillä vanhat laitteet saadaan pois, minkä takia mahdollisia tietovuotoja minimoidaan ja hyllyt eivät ole täynnä vanhoja läppäreitä.

LÄHTEET

Andress, Jason 2019. Foundations of Information Security. Hakupäivä 15.2.2024. O'Reilly Media. Vaatii käyttöoikeuden.

Apple Support 2024. Revive or restore a Mac with Apple silicon using Apple Configurator. Hakupäivä 12.2.2024. https://support.apple.com/fi-fi/guide/apple-configurator-mac/apdd5f3c75ad/mac.

Asset Panda 2024. A Comprehensive Guide to IT Asset Disposition. Hakupäivä 12.3.2024. https://www.assetpanda.com/resource-center/blog/a-comprehensive-guide-to-it-asset-disposition/.

Atlassian 2024. What is IT asset management (ITAM)? Hakupäivä 13.3.2024. https://www.atlassian.com/itsm/it-asset-management.

Blancco 2017. What is Data Sanitization? Hakupäivä 26.1.2024. https://www.blancco.com/resources/article-data-sanitization-definition/.

Blancco 2021. What is Data Erasure? Hakupäivä 26.1.2024. https://www.blancco.com/resources/article-what-is-data-erasure/.

Blancco 2022. The Green SIDE of Blancco. Hakupäivä 3.3.2024. https://www.blancco.com/company/sustainability/.

Blancco 2024a. How Does Blancco Help Organizations Achieve HIPAA Compliance? Hakupäivä 25.2.2024. https://www.blancco.com/resources/sb-how-does-blancco-help-organizations-achieve-hipaa-compliance/.

Blancco 2024b. Who Are We? Hakupäivä 30.1.2024. https://www.blancco.com/about-us/.

Blancco 2024c. Blancco Management Portal. Hakupäivä 25.1.2024. https://www.blancco.com/products/blancco-management-portal/.

Blancco 2024d. Blancco Drive Eraser. Hakupäivä 24.1.2024. https://www.blancco.com/products/drive-eraser/.

Blancco 2024e. Diagnostics & Erasure. Hakupäivä 24.1.2024. https://www.blancco.com/use-case/secure-erasure-of-high-mobile-device-volumes/.

Blancco 2024f. Blancco Eraser for Apple Devices. Hakupäivä 25.1.2024. https://www.blancco.com/products/blancco-eraser-for-apple-devices/.

CDW 2021. What is IT Asset Disposition (ITAD)? Hakupäivä 30.1.2024. https://www.cdw.com/content/cdw/en/articles/services/what-is-itad.html.

Coursera 2024. What Is InfoSec? Definition + Career Guide Hakupäivä 13.3.2024. https://www.coursera.org/articles/infosec.

CSC 2024. Definition of Sensitive Data. Hakupäivä 14.3.2024. https://research.csc.fi/definition-of-sensitive-data.

Guide Jr, Dan & Van Wassenhove, Luk 2002. The Reverse Supply Chain. Hakupäivä 3.3.2024. https://hbr.org/2002/02/the-reverse-supply-chain.

Hyperproof 2024. How to Perform a Successful IT Risk Assessment. Hakupäivä 11.3.2024. https://hyperproof.io/resource/it-risk-assessment/.

Indeed 2022. What Is Asset Disposal? Definition, Benefits and Examples. Hakupäivä 14.3.2024. https://www.indeed.com/career-advice/career-development/asset-disposal.

Kaestner, Rich 2009. Computers and the Environment: Minimizing the Carbon Footprint. Hakupäivä 4.3.2024. https://files.eric.ed.gov/fulltext/EJ918586.pdf.

Mantsinen, Jecaterina 2023. Poliisi on selvittänyt kaikkien Vastaamon tietomurron uhrien henkilötiedot – Asianomistajia yli 33 000. Hakupäivä 5.3.2024. https://www.aamulehti.fi/rikos/art-2000009757940.html.

Microsoft 2024. What is information security (InfoSec)? Hakupäivä 5.3.2024. https://www.microsoft.com/en/security/business/security-101/what-is-information-security-infosec.

Myra Security 2024. What is IT compliance? Hakupäivä 13.3.2024. https://www.myrasecurity.com/en/knowledge-hub/it-compliance/.

NIST Special Publication 800–88 Revision 1 2014. Guidelines for Media Sanitization. Hakupäivä 30.1.2024. https://csrc.nist.gov/pubs/sp/800/88/r1/final.

Oura Health Oy 2024. When you go to sleep, Oura goes to work. Hakupäivä 25.1.2024. https://ouraring.com/oura-experience.

Rimpiläinen, Tuomas 2020. Paljastaako pilkutus jotakin Vastaamon kiristäjästä? Miksi hän ei osaa teititellä suomeksi? Tämä tiedetään valtavasta kiristysvyyhdistä. Hakupäivä 5.3.2024. https://yle.fi/a/3-11613667.

Rouse, Margaret 2018. Flash memory. Hakupäivä 26.1.2024. https://www.techopedia.com/definition/24481/flash-memory.

Rufus 2024. Create bootable USB drives the easy way. Hakupäivä 13.3.2024. https://rufus.ie/en/.

Sotnikov, Ilia 2023. The Importance of Security Risk Assessments and How to Conduct Them. Hakupäivä 13.3.2024. https://blog.netwrix.com/2023/08/04/it-risk-assessment/.

Stegon, David 2022. Examples Show The Need for Enterprise Data Erasure. Hakupäivä 3.3.2024. https://www.blancco.com/resources/blog-examples-show-the-need-for-enterprise-data-erasure/.

WEF & Deloitte 2015. Partnering for Cyber Resilience Towards the Quantification of Cyber Threats Hakupäivä 13.3.2024. https://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.