TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kris-Sten Ibrus 205918IAAB

Töökohateenuse andmekandja krüpteerimise juurutamine pilvekeskkonda

Bakalaureusetöö

Juhendaja: Edmund Laugasson
MSc

Tallinn 2024

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Kris-Sten Ibrus

13.05.2024

Annotatsioon

Käesoleva lõputöö eesmärgiks on juurutada ettevõtte töökohateenuste andmekandjate kettakrüpteerimise lahendus pilvekeskkonda.

Töö teoreetilises osas analüüsitakse alternatiive hetkel kasutusel olevale kettakrüpteerimise lahendusele ning kirjeldatakse ära taust praktilise osa mõistmiseks. Lõputöö praktiline osa on jagatud peatükkideks, milles iga peatükk kirjeldab ära ühe etapi lahenduse valmimisel.

Lõputöö tulemusena juurutati Microsoft BitLockeri taastevõtmete kättesaadavus pilvekeskkonda, mis lihtsustas lõppkasutajate ja IT-spetsialistide tööd ning loodi lahendus BitLockeri PIN-koodi sisestamiseks läbi graafilise kasutajaliidese.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti üheksateistkümnel leheküljel, kümmet peatükki ja kaheksat joonist.

Abstract

Deploying Workplace Service Media Encryption to Cloud Environment

The aim of this thesis is to implement a solution for encrypting disk drives of enterprise workplace services in a cloud environment.

The theoretical part of the work analyzes alternatives to the currently used disk encryption solution and describes the background required for understanding the practical part. The practical part of the thesis is divided into chapters, each describing one stage in the completion of the solution.

As a result of the thesis, the availability of Microsoft BitLocker recovery keys in the cloud environment was implemented, simplifying the work of end-users and IT specialists, and a solution for entering the BitLocker PIN code through a graphical user interface was created.

The thesis is written in Estonian and contains text on nineteen pages, with ten chapters and references to eight figures.

Lühendite ja mõistete sõnastik

AD	*Active Directory*, aktiivkataloog
AES	*Advanced Encryption Standard*, täiustatud krüpteerimisstandard
BitLocker	Turvalisuse tööriist andmekandjate krüpteerimiseks
Domain	Domeen, koosneb seadmetest mis tavaliselt on ühes kohtvõrgus
GPO	*Group policy object*, rühmareegel
MBAM	*Microsoft BitLocker Administration and Monitoring*, Microsoft BitLocker'i haldamine ja jälgimine
MDM	*Mobile device management*, mobiilseadmete haldus
Microsoft 365	Microsoftile kuuluv produktiivsustarkvara
Microsoft Entra ID	Pilvepõhine identiteedi- ja juurdepääsuhalduslahendus, endise nimetusega Azure AD
Microsoft Intune	Pilvepõhine teenus rakenduste ja seadmete haldamiseks
SCCM	*System Center Configuration Manager*, süsteemikeskuse konfiguratsioonihaldur
Software Center	Tarkvara keskus, Microsoft Windowsi rakendus tarkvara paigaldamiseks
Symantec Endpoint Encryption	Ketta krüpteerimistarkvara
TPM	*Trusted Platform Module*, usaldusväärse platvormi moodul
Veracrypt	Ketta krüpteerimistarkvara
Microsoft Windows Powershell	Microsofti ülesannete automatiseerimise ja konfigureerimise haldustööriist

Sisukord

Jooniste loetelu

1 Sissejuhatus

Viimastel aastatel on pilvetehnoloogiad muutunud järjest populaarsemaks, mis mõjutab oluliselt nii ärimaailma kui ka tarbijate igapäevaelu. Üha enam ettevõtteid ja organisatsioone liigub traditsioonilistelt serveripõhistelt süsteemidelt pilvekeskkondadesse. See trend on toonud kaasa mitmeid eeliseid, sealhulgas suurema paindlikkuse, parema skaaleeritavuse ja kulude kokkuhoiu [1].

Järgnev lõputöö annab ülevaate, kuidas andmekandja krüpteerimise lahendus juurutatakse pilvekeskkonda. Lõputöö on jagatud kümneks sisupeatükiks, mis hõlmab alternatiivsete lahenduste analüüsi, loodava lahenduse skoobi määratlemist, lahenduse määratlemist, selle kirjeldust ja teostust. Võetakse kokku tulemused, tuuakse välja lahenduse universaalsus ning tulevikuarendused.

2 Taust

Krüpteerimine on teksti või andmete muutmine matemaatilist algoritmi ning krüptovõtit kasutades, viisil, mis lubab edaspidist ligipääsu ainult autoriseeritud osapooltele, näiteks neile, kes omavad võtit või salasõna. [2].

Lõputöö on aktuaalne, kuna Microsoft lõpetab toe MBAM tootele. MBAM põhitugi lõppes juulis 2019 ja hetkel on laiendatud tugi saadaval kuni aprillini 2026. MBAM on Microsofti poolt loodud haldusliides, mis pakub võimalust hallata BitLockeri kettakrüpteerimist [3]. Teema on aktuaalne ka seetõttu, et tehnoloogilised lahendused kolivad pilvekeskkondadesse, samuti ka lõputöös käsitletav MBAM toode, mis kolib Microsoft Intune pilvepõhisele teenusele.

2.1 Hetke olukord

Hetkel on ettevõttes kasutusel Microsoft BitLocker kõvakettakrüpteeringu keskne taastevõtmete haldus. Arvutisse on paigaldatud MBAM agent, mille elu juhitakse läbi GPOde, mis on erinevad sõltuvalt masinate tüübist, funktsioonist jne. MBAM juhib arvutis oleva BitLockeri tööd, mis siis krüpteerib kõvaketta ning MBAM saadab taastevõtme tsentraalsesse serverisse. Kui kasutaja ei mäleta oma PIN-koodi, saab kasutajatugi aidata kõvaketta avada taastevõtme abil.

Teenuse töötamiseks on kasutusel kaks serverit: ühes on MBAM rakendus ning teine server, mis hoiab endas taastevõtmeid. Mõlemaid servereid jälgitakse seiresüsteemi abil ning nendest tehakse varukoopiaid eraldi serverisse.

2.2 Probleem

Kuna Microsoft on otsustanud lõpetada toe MBAM tootele, on ettevõttes vaja leida alternatiivlahendus hetkel kasutusel olevale kettakrüpteerimise lahendusele. MBAM põhitugi lõppes juulis 2019 ja hetkel on laiendatud tugi saadaval kuni 2026 aprillini [3] [4].

Probleemiks on ka see, et tegu on eraldi rakenduse ja riistvaraga, mis võivad ebaõnnestuda. See tähendab, et katastroofijärgse taastamise vaates on rohkem asju, mis võivad nurjuda. Katki võivad minna andmebaasid, mis salvestavad endas taastevõtmeid. Võib kaduda elekter, mis hoiab üleval riistvara, millel antud rakendus töötab.

2.3 Eesmärk

Lõputöö eesmärgiks on juurutada kettakrüpteerimise lahendus, mis asendaks praegust ning ühilduks ettevõttes kasutatavate süsteemide ja pilvekeskkonnaga.

Lahendus peab võimaldama autentimist, mis takistaks operatsioonisüsteemile ligipääsu. Testida uut lahendust, pakkuda see välja lõppkasutajale ja kuu aega pärast avaldamist sulgeda vana lahendus.

3 Loodava lahenduse määratlemine

Järgnevates loeteludes on kirjeldatud loodava lahenduse funktsionaalsed kui ka mittefunktionaalsed nõuded.

3.1 Funktsionaalsed nõuded

Järgnevas loetelus on funktsionaalsete nõuete näol ära kirjeldatud milliseid tegevusi peab olema võimalik antud lahendusega täita.

- Andmekandja krüpteerimise lahendus peab võimaldama terve kettajao krüpteerimist.
- Masinaid peab olema võimalik keskselt hallata kasutades Microsoft Intune'i, et lihtsustada IT-spetsialistide tööd, see hõlmab omas taastevõtmetele ligipääsemist.
- BitLockeri lisamise lahendust peab olema võimalik rakendada keskhalduse kaudu kasutades SCCMi sülearvutitele installimise käigus.
- Lahendus peab toetama arvuti sisese andmekandja krüpteerimist.
- Töötajatel peab olema võimalik iseseisvalt oma andmekandja PIN-koodi läbi kasutajaliidese muuta.

3.2 Mittefunktsionaalsed nõuded

Järgnevas loetelus on mittefunktsionaalsete nõuete näol kirjeldatud loodava lahenduse töökäik ning milliseid omadusi see peaks omama.

- Lahendus peab olema skaleeritav.
- Sülearvutil peab olema usaldusväärse platvormi moodul ehk TPM 1.2 või uuem.
- Krüpteeritavad masinad peavad omama Microsoft Windows 10 või Microsoft Windows 11 operatsioonisüsteemi.
- Krüpteeritavad tööarvutid peavad olema ettevõtte domeeni halduse all.

4 Alternatiivsete lahenduste analüüs

Andmekandja krüpteerimiseks on loodud mitmeid erinevaid lahendusi ning käesolevas peatükis analüüsitakse neid. Analüüsi eesmärk on leida hea alternatiiv hetkel kasutusel olevale MBAM krüpteerimislahendusele. Analüüsitavateks alternatiivseteks lahendusteks valiti Veracrypt, võttes aluseks lehekülje AlternativeTo valimit [5] ning Symantec Endpoint Encryption, võttes aluseks Gartner rühma analüüsi [6], valitud mõlemast üks alternatiiv, et oleks mitmekesisem valim ning andmed erinevatest allikatest.

4.1 BitLocker

BitLocker on Microsofti tasuta tarkvara, mis võimaldab krüpteerida tervet kõvaketast ja kaitsta süsteemi volitamata juurdepääsu eest. BitLocker on integreeritud Microsoft Windowsi operatsioonisüsteemiga, muutes selle kasutamise lihtsaks ja tõhusaks ettevõtete jaoks, kes soovivad oma andmeid tõhusalt kaitsta.

BitLocker kasutab andmete kaitsmiseks täiustatud krüpteerimisstandardit 128-bitiste või 256-bitiste võtmetega. BitLocker kasutab täiustatud krüptograafiat, sealhulgas AESi, et tagada tugev turvalisus [7].

Kui kõvaketas krüpteeritakse BitLockeri abil, ei ole ilma õige salasõnata võimalik kõvakettal olevatele andmetele juurde pääseda. Isegi kui kõvaketas arvutist eemaldada ja teise masina külge ühendada, jääb selle sisu ligipääsmatuks [8]. BitLocker võimaldab kasutada autentimiseks PIN-koodi, mis on salvestatud seadme TPMi [9].

4.2 Veracrypt

Veracrypt on tasuta ja avatud lähtekoodiga ketta krüpteerimistarkvara. See toetab Microsoft Windows operatsioonisüsteemi, samuti macOS ja GNU/Linux operatsioonisüsteeme. Veracrypti peamised omadused on need, et see suudab krüpteerida kogu partitsiooni või kõvaketast, sealhulgas ka partitsiooni või ketta, kuhu on paigaldatud Microsoft Windows operatsioonisüsteem, seega toimib ka eelkäivitusel autentimine [10]. Eelkäivitusel autentimist aitab teha *VeraCrypt Boot Loader*.

Veracrypt pakub kogu süsteemi krüpteerimist, mis tagab kõrgeima turvalisuse ja privaatsuse, kuna kõik failid on püsivalt krüpteeritud [11]. Veracryptiga saab krüpteerimiseks kasutada mitmeid algoritme, üks neist on AES, mida USA valitsus usaldab ka standardina [12].

4.3 Symantec Endpoint Encryption

Symantec Endpoint Encryption on tasuline ja suletud lähtekoodiga ketta krüpteerimistarkvara, mis toetab erinevaid operatsioonisüsteeme nagu Microsoft Windows, macOS ja GNU/Linux [13]. Olemas on ka keskselt hallatav konsool, mis võimaldab tõhusalt juurutada ja jõustada erinevaid krüpteerimisreegleid.

Algse krüpteerimisetapi ajal kasutab Symantec Endpoint Encryption AES krüptograafilist moodulit, et krüpteerida iga ketas sektorite kaupa, tagades, et ükski fail ei jääks krüpteerimata. Lahendus toetab ka usaldusväärse platvormi moodulit ning on võimalik ka sünkroniseerida Active Directory'ga, samuti on lahendus skaleeritav [14].

4.4 Lahenduse väljavalimine

Microsoft BitLocker, Veracrypt ja Symantec Endpoint Encryption on kõik tugevad andmete krüpteerimislahendused Microsoft Windowsi platvormile. Kuna kasutusel oli eelnevalt Microsoft BitLockeri eelkäija MBAM, on BitLocker loogiline valik, sest see on integreeritud Microsoft Windowsi operatsioonisüsteemiga ja võimalik hallata läbi Active Directory ning seadistada läbi rühmareeglite [15].

Veracrypt on avatud lähtekoodiga krüpteerimislahendus, mis pakub paindlikkust ja laia funktsioonide valikut, kuid võib vajada rohkem kohandamist ja haldamist võrreldes BitLockeriga [10]. Symantec Endpoint Encryption on professionaalne krüpteerimislahendus, mis pakub täiendavat funktsionaalsust ja tuge, kuid sõltuvalt organisatsiooni vajadustest võib seda olla kallim ja keerukam hallata.

Lõputöös saab väljavalituks Microsoft BitLocker, kuna eelnevalt on kasutatud MBAMi ning seega on see loogiline valik, sest sellel on hea tugi Microsoft toodetega.

5 Lahenduse kirjeldus

Käesolevas peatükis kirjeldatakse ära teoreetilisem taust, mis lihtsustab arusaamist loodavast lahendusest.

5.1 Krüpteerimine ja võtmed

Kõvaketaste krüpteerimine on protsess, kus andmed muudetakse arusaamatuks ilma õige võtmeta. See tagab, et volitamata isikud ei pääse ligi tundlikele andmetele, isegi kui füüsiline kõvaketas satub nende kätte.

Krüpteerimiseks kasutatakse matemaatilisi algoritme, mis teisendavad andmed krüpteeritud kujule, ja seejärel saab ainult õige võtme abil need uuesti dekrüpteerida. Dekrüpteerimiseks on olemas võti, mis peab olema salajane [2].

5.2 BitLocker PIN

BitLockeri PIN kaitseb füüsilise varguse korral kolmanda isiku ligipääsu andmetele, kuna see takistab edasist ligipääsu BitLockeri PINi küsimise vaatest. PIN-kood on mõeldud selleks, et kõrvalistel isikutel ei oleks võimalik operatsioonisüsteemile ligi pääseda. Microsoft parandab igakuiselt oma operatsioonisüsteemide turvahaavatavusi. See näitab, et operatsioonisüsteem on kompleksne ning avatud erinevatele rünnakutele [16] [17].

5.3 Taastevõtmed BitLockeris

Iga BitLockeriga kaitstud seadme jaoks genereeritakse unikaalne 48-kohaline numbriline taastevõti. Kui kasutaja unustab oma BitLockeri PIN-koodi, saab ta selle numbrilise taastevõtme abil ligipääsu taastada. Taastevõtit võib salvestada ADsse, Microsoft Entrasse. Võimalik on salvestada ka taastevõti tekstifaili, kuid ettevõttes ei ole see mõistlik, kuna ei ole lihtne võtmeid keskselt hallata. [18].

5.4 Microsoft Intune

Microsoft Intune on pilvepõhine teenus, mis võimaldab organisatsioonidel tõhusalt hallata oma seadmeid ja rakendusi. See on osa Microsoft 365 platvormist, mis loob ettevõtetele paindlikuma ja turvalisema töökeskkonna.

Microsoft Intune võimaldab administraatoritel seadistada seadmeid, rakendada turvareegleid, hallata kasutajate ligipääsu andmetele ning jälgida seadmete olekut reaalajas. Lisaks võimaldab see kaugpaigaldada ja uuendada rakendusi, tagada seadmete vastavus organisatsiooni turvastandarditele ning kaugkustutada seadmeid, kui need peaksid kaduma minema.

Microsoft Intune on kujundatud lihtsaks ja tõhusaks lahenduseks, mis toetab kaasaegseid tööviise ja tagab samal ajal organisatsiooni andmete turvalisuse [19].

6 Teostus

Käesolev peatükk kirjeldab lõputöö praktilist sisu ning annab ülevaate, kuidas uus lahendus teostati.

6.1 Valmisoleku hindamine

Kuna ettevõttes on juba varasemalt kasutusel Microsofti tooted, siis eraldi pilvekeskkonna Microsoft Intune'i litsentsi pole tarvis tarnida. Ettevõtte sülearvuteid vahetatakse välja iga 3 aasta tagant ning neid hoitakse riistvaraliselt uuendatuna, seega on kõigil arvutitel TPM versioon 1.2 või uuem. Kõikidel sülearvutitel on kas Microsoft Windows 10 Enterprise versioon 22H2 või Windows 11 Enterprise.

Tuleb veenduda, et kõik masinad oleksid liidestatud Microsoft Entra ID-ga. Eelduseks on, et masinad on varasemalt lisatud kohalikku ADsse [20]. Kontrollimiseks tuleb eksportida Microsoft Entra IDst arvutite nimekiri csv-vormingusse ning võrrelda SCCMist saadud tabeliga.

6.2 Varukoopia kinnitamine

Kui kõik arvutid on Microsoft Entra ID keskkonnas näha, siis tuleb teha MBAM keskkonnas olevatest taastevõtmest varukoopia ja see sünkroniseerida Microsoft Entra IDga. Pärast seda tuleb ajutiselt hakata looma taastevõtmeid mõlemasse keskkonda.

Et teada saada, kas kõikidel masinatel on BitLockeri taastevõtmed üle tulnud ning kättesaadavad ja ajakohased, tuleb teha varukoopia kinnitamine. Tuleb võtta arvutite nimekiri mille sai Microsoft Intune'ist, ning sealt eksportida taastevõtmed csv-vormingusse. Seejärel tuleb filtreerida välja arvutid, millel pole taastevõtit ning kontrollida, miks seda ei ole. Näiteks pole mõni arvuti enam kasutuses.

Kui mõnel arvutil peaks tekkima suuremat sorti probleem, näiteks BitLockerit pole, siis on mõistlik arvuti operatsioonisüsteem taaspaigaldada, et säästa aega. Kui üritada BitLockerit aktiveerida käsitsi, siis tekivad probleemid taastevõtmete salvestamisega, ehk need ei ole keskhalduskeskkonda salvestatud vaid ainult kohalikku arvutisse.

6.3 BitLockeri PINi lisamise funktsionaalsuse vajadus

Kuna MBAMis oli sisseehitatud BitLockeri PIN-koodi lisamine, tuli leida lahendus, kuidas seda teha ilma MBAM kliendita. Eelnevalt oli olemas MBAM klientliidese kasutajaliides, mille kaudu sai BitLockeri PIN-koodi lisada. Uus lahendus saadab Microsoft Entra IDsse ainult taastevõtme. Uuel lahendusel puudub PINi lisamise funktsionaalsus, kuna Microsoft reklaamib PINita varianti [21]: ketas on krüpteeritud, kuid taastevõtit küsitakse alles siis, kui arvuti usaldusväärse platvormi mooduli kiibis olev info tühjendatakse. Muidu arvuti lihtsalt käivitub. Selline lahendus on asendusarvutitel ja esinduste arvutitel ning need on AD rühmas nimega "NoBitlockerPin".

PIN on lisakaitse, mida ettevõte soovib. Tuli leida võimalus selle PIN-koodi lisamiseks. Selleks võiks olla skript, et lihtsustada lõppkasutaja kogemust. Sai valitud skript, millel on olemas kasutajaliides [22]. Tänu kasutajaliidese olemasolule ei ole vaja saata lõppkasutajat kasutama Microsoft Windows Powershelli, kus ta peaks erinevaid käske kirjutama, et BitLockeri PIN-koodi lisada.

6.4 Bitlockeri PINi lisamise funktsionaalsuse ja BitLockeri taastevõtmete salvestamise juurutamine

BitLockeri PIN-koodi lisamise funktsionaalsus sai tehtud kasutades SCCMi. Tuli võtta SCCMis "*Powershell scripts*" ja sealt "*deploy to all*", et tarnida skript kõigile arvutitele. Tuleb tarnida 2 skripti nimedega "*Set BitLocker PIN*" ja "*Bitlocker key to AAD*".

SCCMis rakenduse tarnimiseks, tuleb valida lisa uus rakendus manuaalselt, "*create application*", "*manually*" [23]. Software Center rakendusse lisati PINi lisamise funktsionaalsus. "*BitLocker key to AAD*" skript ei läinud, sest see lisati kõigile arvutitele ning see skript lisab BitLockeri taastevõtmed pilvekeskkonda Microsoft Entra ID. Rakenduse tarnimise tüüp on "*script installer*", sinna tuli siis lisada kasutatav skript "*invokeEscrow.ps1*" [24]. Tuvastusmeetodite all, et mille järgi Software Center saab teada, kas mingi tarkvara on paigaldatud, peab Microsoft Windows Powershellis kindel arv ridu läbi käima. Ehk kui on 0 rida, siis tekitab veateate. Kui on katki, proovib uuesti. "*Bitlocker key to AAD*" puhul, kui on 13 rida olemas, siis on korras. "*Set BitLocker Pin*" on korras siis, kui on olemas 1 rida. Kasutusel on selline lahendus, sest hetkel ei ole

võimalik arvuti siseselt kontrollida, kas taastevõti läks Microsoft Entra IDsse või mitte, kuna sellist funktsionaalsust pole hetkel lisatud. On lihtsam teha manuaalne kontroll, et näha kellel see toimis ja kellel mitte.

BitLockeri PIN-koodi unustamise korral on lisatud funktsionaalsus PINi muutmiseks. Skripti uuesti käivitades, saab panna ka eelnevalt kasutusel olnud PIN-koodi, sest tegu on põhimõtteliselt Microsoft Windows Powershell'i käsuga nimega "*SetBitlockerPin*". Käsu asemel on kasutusel "*setBitlockerPin*" rakendus, mis avab kasutajaliidese salasõna lisamiseks. "*Bitlocker to AAD*" on kasutusel nii Microsoft Intune'is, kui ka SCCMis, aga PIN-kood on ainult SCCM-is. Tekitatud on liiasus, ehk kui peaks tekkima reeglite vahel konflikt, on kasutuses arvutites "*MDM over GPO*", ehk Microsoft Intune reeglid on prioriteetsemad kui lokaalsed reeglid [25]. Kui peaks olema mingi arvuti, kus Microsoft Intune ei mõju, siis lokaalne rühmareegel täidab selle tühja koha.

6.5 Lahenduse testimine

Testrühma kuulus 50 sülearvutit. Rühmas oli erinevate tööülesannetega töötajate arvutid ning paar turvatiimi töötaja arvutit. Kõik testrühmas olevad inimesed olid teadlikud, et nad selles rühmas olid ning kui midagi oleks pidanud juhtuma, teadsid nad, millest see tulenes.

50 sülearvutit 1500-st arvutist on umbkaudu 0.03%, kuid kuna antud valimis ei olnud ainult ühe meeskonna sülearvutid, vaid erinevate meeskondade arvutid, siis neilt tulev tagasiside oli piisav lahenduse valideerimiseks. Vea ilmnemisel oleks saanud sellest teada enne lahenduse juurutamist.

6.6 Juhendi loomine

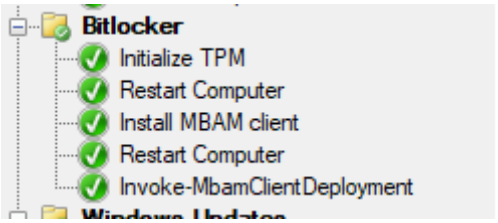
Lõppkasutajatele sai edastatud informatsioon, et antud muudatus on tulemas ja edaspidi saavad lõppkasutajad ise oma BitLockeri PIN-koodi muuta ning ei pea IT-spetsialisti juurde minema. Lõppkasutajate juhend BitLockeri PIN-koodi muutmiseks ja taastevõtmele ligipääsemiseks on nähtav Lisa 2.

IT-spetsialistidele koostatav juhend pidi olema võimalikult detailne, kuid sisaldama ainult vajalikku informatsiooni, et asi ei läheks liiga keeruliseks. Taastevõtmetele ligipääsemiseks oli mõistlik luua IT-spetsialistidele juhend, kuna võtmete leidmine

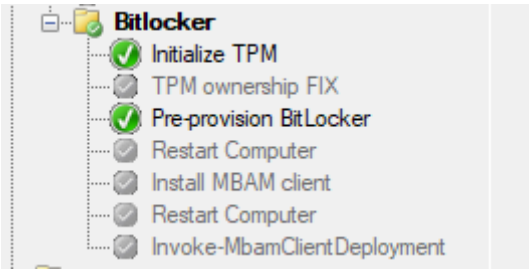
Microsoft Intunest võib esmakordsel kasutamisel segadust tekitada. Lõppkasutajate BitLockeri taastevõtmetele ligipääsemiseks, peavad IT-spetsialistid tellima Microsoft Entra ID administraatori konto ning sellele õigused BitLockeri taastevõtmete nägemiseks Microsoft Intune'i keskkonnas. IT-spetsialistidele mõeldud juhend taastevõtmetele ligipääsemiseks on nähtav Lisa 3.

6.7 Paigaldusülesannete järjestus

Eelnevalt oli paigaldusülesannete lõpus kõik etapid korraga, "*initialize TPM*", "*restart computer*", "*install MBAM client*", "*restart computer*", "*initalize MBAM client deployment*", kujutatud joonisel 1. Uuel lahendusel on paigaldusülesanne kahes osas, alguses toimub "*initialize TPM*" ja "*pre provision*", viidatud joonisel 2, mis siis hakkab kõvaketast krüpteerima ja paigaldusülesannete järjestuse lõpus on BitLockeri sisse lülitamine, viidatud joonisel 3. Viie paigaldusülesande sammu asemel on nüüd kolm.



Joonis 1. Eelnev BitLockeri osa paigaldusülesandes



Joonis 2. Uue BitLockeri aktiveerimise osa paigaldusülesande 1 pooles

Joonis 3. Uue BitLockeri aktiveerimise osa paigaldusülesande 2 pooles

6.8 Arvutite rühmadesse eraldamine

Tegemist on SCCMi rühmadega. On olemas 2 suuremat rühma: üks on "*BitLocker AAD*", selles rühmas on kõik Microsoft Windows operatsioonisüsteemiga arvutid, mida on umbes 1500.

Teine rühm on "*BitLocker Set PIN AAD*", kuhu kuuluvad eelmisest 1500-st masinast ümaralt 1400. Viimasena nimetatud rühmas on veel välistamisrühmad, kuhu kuuluvad näiteks asendusarvutid. Need on arvutid, kus krüpteeritakse kõvaketas, kuid BitLockeri PIN-koodi ei lisata.

6.9 Vana lahenduse sulgemine

Vana lahenduse sulgemiseks tuli lasta arhitektil tellida kasutusest välja võtmise korraldus ning peale seda masin lihtsalt välja lülitada. VMware tiim eemaldas riistvara umbes kuu aega hiljem.

7 Lahenduse analüüs

Lõputöö tulemusena juurutati kettakrüpteerimise lahendus pilvekeskkonda. Selleks hakati looma taastevõtmeid Microsoft Intune'i pilvekeskkonda. Kasutusele sai võetud Microsoft Intune, kuna integreerub Microsofti teenustega hästi ja võimaldab taastevõtmeid keskselt hallata, mis lihtsustab spetsialistide tööd. Pilvekeskkonna kasutuselevõtt taastevõtmete haldamiseks hoiab ära ka vajaduse eraldiseisva riistvara jaoks mis võivad tekitada katastroofijärgse taastamise vaates probleeme [26].

Testperioodi ajal loodi taastevõtmeid endisesse spetsiaalsesse serverisse, mis haldas taastevõtmete hoiustamist. Loodi uus lahendus, mis aitab lõppkasutajal seadistada BitLockeri PIN-koodi. PIN-koodi lisamine on oluline, kuna hoiab ära kolmanda osapoole ligipääsu kõvakettal olevatele andmetele, ilma PINita lahendusel on andmetele ligipääsemine kergesti saavutatav. Kolmandal osapoolel on võimatu ligipääseda kõvakettal olevatele andmetele kui ei kasutata väliseid ründevahendeid. Kuumalt ühendatavad ründevahendid on väljatoodud tulevikuarendusena ning ei kuulu käesoleva lõputöö ulatusse [27].

Testiti BitLockeri PIN-koodi seadistamist ning seejärel pakuti terviklik lahendus välja lõppkasutajale. Vana lahendus suleti. Loodud juhendid lõppkasutajatele, viitatud lisas 2 ning IT-spetsialistidele, viidatud lisas 3.

8 Lahenduse universaalsus

Antud lahendus on teatud määral universaalne. Näiteks tuleks kohandada salasõnareeglid, sest teistes ettevõtetes võivad salasõnareeglid erineda. Lahenduse toimimiseks on vajalikud teatud eeldused: Microsoft Entra ID, Microsoft Intune, sülearvutid peavad olema Microsoft Intune'i keskkonnas nähtavad ning ühishaldamine peab olema võimalik.

Võimalik on ka täielikult kasutada Microsoft Intune'i, aga sel juhul tuleb kõik rühmad luua Microsoft Intune'i kaudu. Hetkel kasutati olemasolevaid SCCM rühmi.

9 Tulevikuarendused

- Ettevõte võiks soetada mõne "*hotplug attack tool*"-i. Tegu on rünnaku tööriistaga, mis töötab süsteemi peatamata ning sellega oleks võimalik katsetada, kas Microsoft BitLocker kettakrüpteerimine kaitseb antud tööriista vastu.

- Läbi viia uuring, et näha statistikat riskidest, mis on realiseerunud. Võtta infoturbe intsidentide statistika ning vaadata, kas nende vastu kettakrüpteerimine aitab.

- Parema ligipääsetavuse tagamiseks luua lahendus, mis võimaldab taastevõtmeid lokaalselt varundada.

10 Kokkuvõte

Käesoleva lõputöö eesmärgiks oli juurutada kettakrüpteerimise lahendus pilvekeskkonda. Lõputöös kirjeldati eelnevat olukorda ning seletati probleemi relevantsust.

Analüüsi käigus nimetati paar alternatiivi, mida oleks saanud kasutada Microsoft BitLockeri asemel. Eelneva lahenduse põhjal sõnastati funktsionaalsed kui ka mittefunktsionaalsed nõuded. Kirjeldati lahenduse tausta, mis lihtsustab lõputöö praktilisest osast arusaamist.

Lõputöö tulemusena juurutati Microsoft BitLockeri taastevõtmete kättesaadavus pilvekeskkonda, mis lihtsustab lõppkasutajate ja IT-spetsialistide tööd ning loodi lahendus BitLockeri PIN-i lisamiseks, mis sisaldab graafilist kasutajaliidest.

Sõnastati edasised arendused, uurimaks Microsoft BitLockeri vajadust, selle haavatavusi ning luua ligipääsetavuse tagamiseks lahendus, mis võimaldaks taastevõtmeid varundada lokaalses keskkonnas lisaks pilvekeskkonnale.

Kasutatud kirjandus

[1] Sonika Choubey; Laurence Goasduff, „Gartner Says Cloud Will Become a Business Necessity by 2028," Gartner, Inc, 29 November 2023. [Võrgumaterjal]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028. [Kasutatud 15 Aprill 2024].

[2] Tartu Ülikooli arvutiteaduse instituut, „Infoturve koolis," [Võrgumaterjal]. Available: https://courses.cs.ut.ee/t/infoturvekoolis/Main/Kr%C3%BCpteerimine. [Kasutatud 15 Aprill 2024].

[3] A. Czechowski, A. Buck, F. Rojas, D. Paunovic, M. Mardahl ja S. Paniagua, „Microsoft BitLocker Administration and Monitoring 2.5," Microsoft, 23 Märts 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/. [Kasutatud 15 Aprill 2024].

[4] J. Lurie, „New extended support dates for MDOP tools," Microsoft, 04 September 2019. [Võrgumaterjal]. Available: https://techcommunity.microsoft.com/t5/windows-it-pro-blog/new-extended-support-dates-for-mdop-tools/ba-p/837312. [Kasutatud 15 Aprill 2024].

[5] „The Best Windows BitLocker Alternatives," AlternativeTo, 07 Veebruar 2024. [Võrgumaterjal]. Available: https://alternativeto.net/software/windows-bitlocker/. [Kasutatud 1 Mai 2024].

[6] „Competitors and Alternatives to Microsoft BitLocker," Gartner, Inc., [Võrgumaterjal]. Available: https://www.gartner.com/reviews/market/mobile-data-protection-solutions/vendor/microsoft/product/microsoft-bit-locker/alternatives?marketSeoName=mobile-data-protection-solutions&vendorSeoName=microsoft&productSeoName=microsoft-bit-locker. [Kasutatud 1 Mai 2024].

[7] K. N. V. P. Paolo Matarazzo, „Device encryption," Microsoft, 07 November 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/#device-encryption. [Kasutatud 19 Aprill 2024].

[8] Chester, „How to Encrypt a Hard Drive in Windows 11/10/8/7/XP," UkeySoft Software Inc, 17 Detsember 2022. [Võrgumaterjal]. Available: https://www.ukeysoft.com/encryption/encrypt-a-hard-drive-in-windows.html. [Kasutatud 15 Aprill 2024].

[9] K. N. V. P. Paolo Matarazzo, „BitLocker and TPM," Microsoft, 07 November 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/#bitlocker-and-tpm. [Kasutatud 18 Aprill 2024].

[10] „Home," Veracrypt, [Võrgumaterjal]. Available: https://veracrypt.eu/en/Home.html. [Kasutatud 15 Aprill 2024].

[11] „System Encryption,“ Veracrypt, [Võrgumaterjal]. Available: https://veracrypt.eu/en/System%20Encryption.html. [Kasutatud 15 Aprill 2024].

[12] „5 Common Encryption Algorithms and the Unbreakables of the Future,“ Arcserve, LLC, 19 September 2023. [Võrgumaterjal]. Available: https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future. [Kasutatud 15 Aprill 2024].

[13] „System requirements for Symantec Endpoint Security,“ Broadcom, 10 Aprill 2024. [Võrgumaterjal]. Available: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Release-Notes/system-requirements-for-v118544952-d4161e11232.html. [Kasutatud 15 Aprill 2024].

[14] „Endpoint Encryption,“ 21 November 2023. [Võrgumaterjal]. Available: https://docs.broadcom.com/docs/endpoint-encryption-en. [Kasutatud 15 Aprill 2024].

[15] P. Matarazzo, „Configure BitLocker,“ Microsoft, 07 November 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/configure?tabs=common. [Kasutatud 15 Aprill 2024].

[16] M. H. Ben Lutkevich, „Patch Tuesday,“ TechTarget, Mai 20222. [Võrgumaterjal]. Available: https://www.techtarget.com/searchsecurity/definition/Patch-Tuesday. [Kasutatud 20 Aprill 2024].

[17] P. Matarazzo, „Preboot authentication,“ Microsoft, 07 November 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/countermeasures#preboot-authentication. [Kasutatud 18 Aprill 2024].

[18] P. Matarazzo, „BitLocker recovery options,“ Microsoft, 07 November 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/recovery-overview#bitlocker-recovery-options. [Kasutatud 18 Aprill 2024].

[19] S. R. A. B. Mandi Ohlinger, „Microsoft Intune securely manages identities, manages apps, and manages devices,“ Microsoft, 05 September 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune. [Kasutatud 18 Aprill 2024].

[20] B. Peppin, „A Beginner’s Guide to Managing BitLocker with Intune,“ Frontside Systems, LLC, 25 Mai 2022. [Võrgumaterjal]. Available: https://brookspeppin.com/2022/05/25/a-beginners-guide-to-managing-bitlocker-with-intune/#?utm_content=cmp-true. [Kasutatud 18 Aprill 2024].

[21] P. Matarazzo, „When should an additional method of authentication be considered?,“ Microsoft, [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/faq#when-should-an-additional-method-of-authentication-be-considered. [Kasutatud 20 Aprill 2024].

[22] O. Kieselbach, „Github,“ 1 Oktoober 2021. [Võrgumaterjal]. Available: https://github.com/okieselbach/Intune/tree/master/Win32/SetBitLockerPin. [Kasutatud 20 Aprill 2024].

[23] A. Marin, „How to deploy PowerShell scripts via Application Model?,“ Advanced

Installer, 22 Märts 2023. [Võrgumaterjal]. Available: https://www.advancedinstaller.com/deploy-powershell-scripts-in-sccm.html. [Kasutatud 20 Aprill 2024].

[24] M. Mardahl, „Github,“ 6 November 2023. [Võrgumaterjal]. Available: https://github.com/mardahl/PSBucket/blob/master/Invoke-EscrowBitlockerToAAD.ps1. [Kasutatud 20 Aprill 2024].

[25] P. M. Vinay Pamnani, „MDMWinsOverGP,“ Microsoft, 18 Jaanuar 2024. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict#mdmwinsovergp. [Kasutatud 20 Aprill 2024].

[26] J. Jarvis, „The Critical Need for Integrating Devices with Intune,“ Quest Software Inc., 21 Veebruar 2024. [Võrgumaterjal]. Available: https://practical365.com/the-critical-need-for-integrating-devices-with-intune/. [Kasutatud 04 Mai 2024].

[27] D. Andzakovic, „ Extracting BitLocker keys from a TPM,“ Pulse Security Ltd. , 13 Märts 2019. [Võrgumaterjal]. Available: https://pulsesecurity.co.nz/articles/TPM-sniffing. [Kasutatud 04 Mai 2024].

[28] K. N. V. P. Paolo Matarazzo, „BitLocker overview,“ Microsoft, 07 November 2023. [Võrgumaterjal]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/. [Kasutatud 18 April 2024].

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[8]

Mina, Kris-Sten Ibrus

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Töökohateenuse andmekandja krüpteerimise juurutamine pilvekeskkonda“, mille juhendaja on Edmund Laugasson
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

13.05.2024

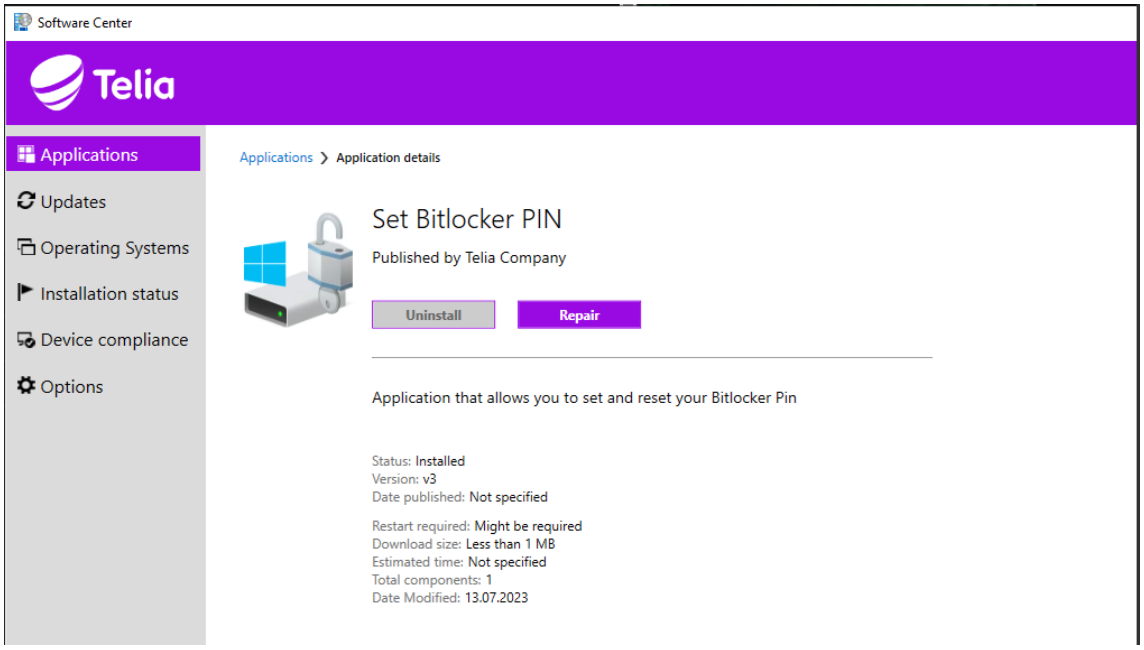
8 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2 – Lahendus lõppkasutaja perspektiivist

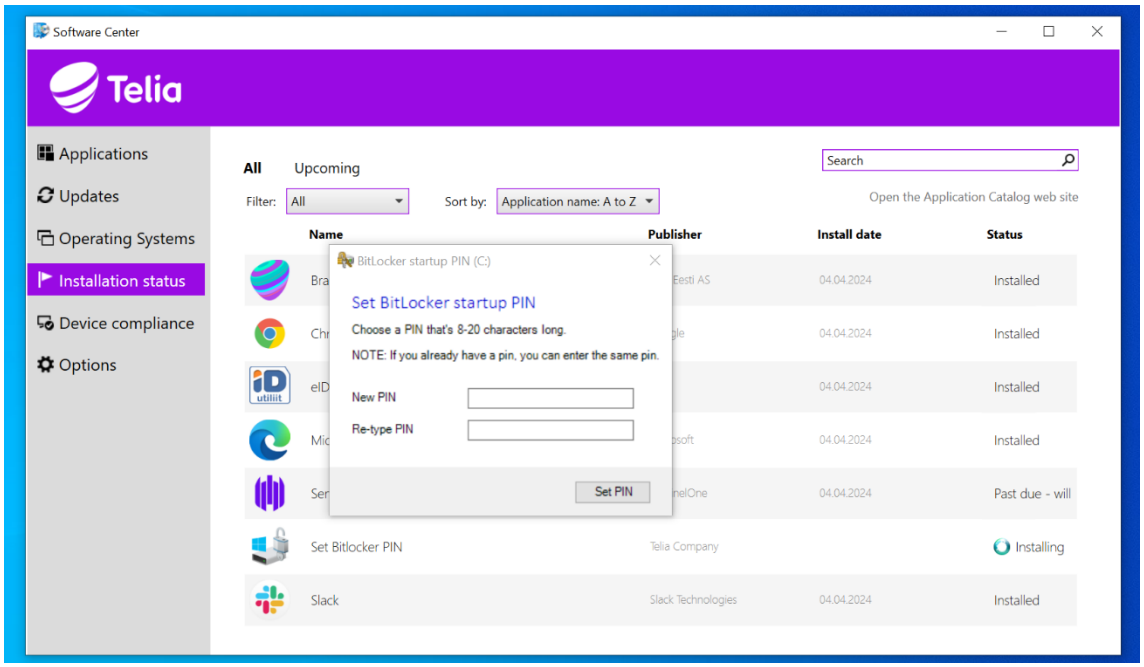
Bitlockeri salasõna lisamiseks ei ole tarvis enda arvuti kettalt sügavalt kaustadest otsida kindlat rakendust, vaid käivitada Software Center rakendus ja sealt valida "*Set BitLocker Pin*", nagu on kujutatud joonisel 4. Siis tekib võimalus lisada BitLockeri salasõna, nagu on kujutatud joonisel 5.

Uues lahenduses on BitLockeri taastevõtmete kättesaamine tehtud lõppkasutajale võimalikult lihtsaks, nagu on kujutatud joonisel 6:

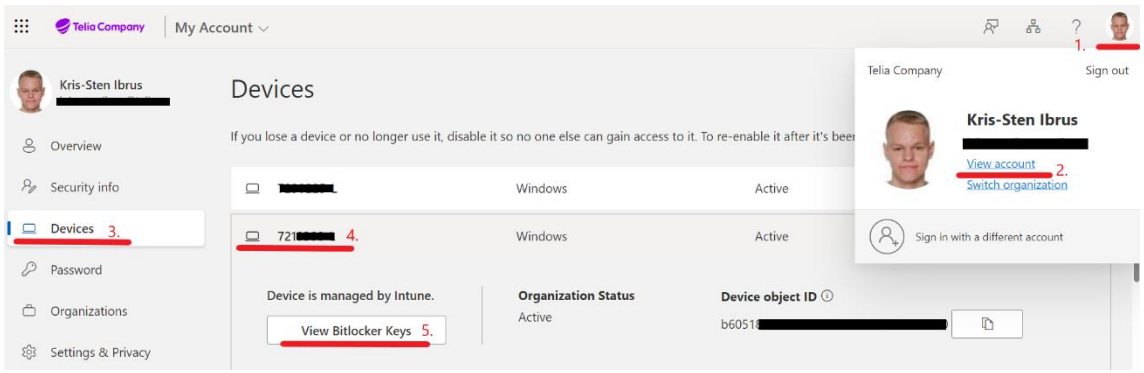
- Logida office.com lehel sisse ettevõtte domeeni andmetega.
- Vajutada paremal kasutaja pildile ja valida "Kuva konto".
- Valida vasakult "Seadmed", otsida nimekirjast üles vajaminev arvuti.
- Valida "Vaata BitLockeri võtmeid".



Joonis 4. BitLockeri PIN lisamise rakendus



Joonis 5. BitLockeri PIN lisamise kast

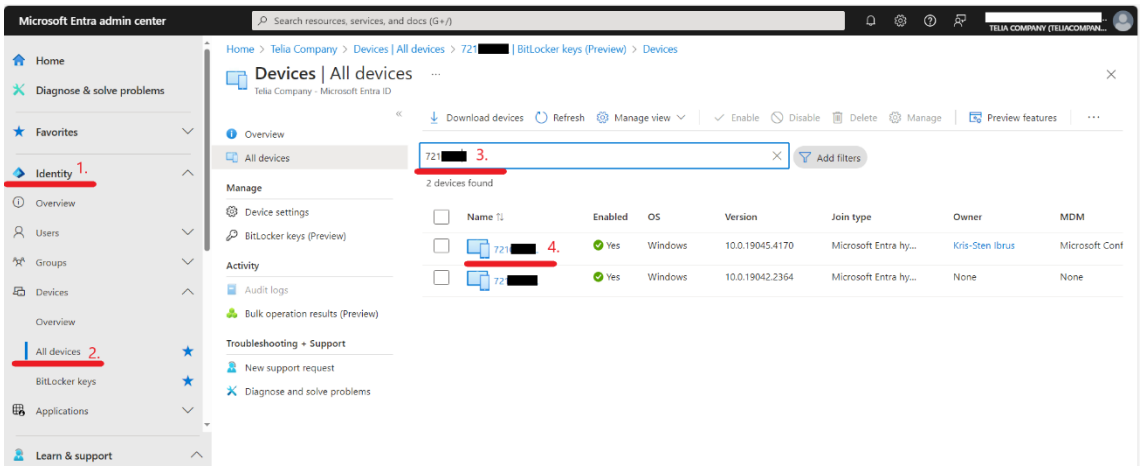


Joonis 6. BitLockeri taastevõtmele ligipääsemine

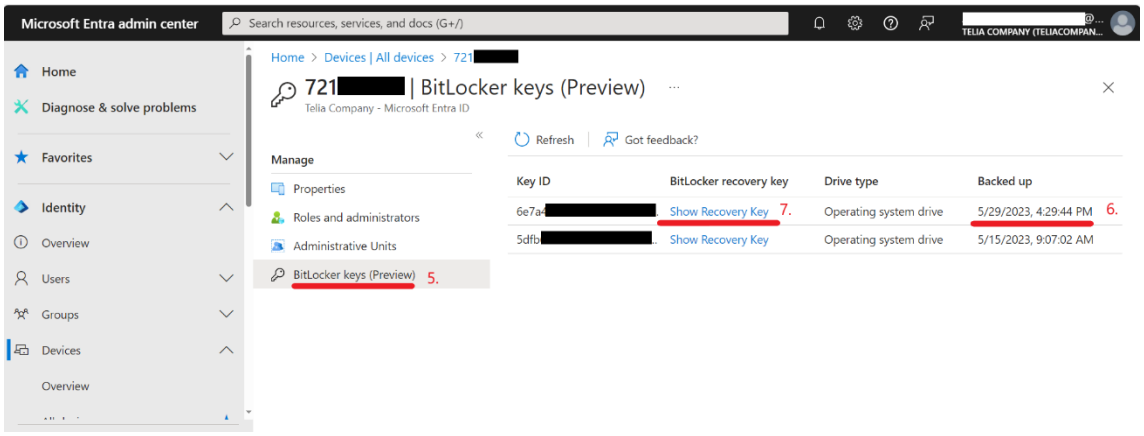
Lisa 3 – Lahendus IT-spetsialistide perspektiivist

IT-spetsialistide perspektiivist muutus taastevõtmele ligipääsemine järgnevaks, kujutatud joonisel 7:

- Avada "*endpoint.microsoft.com*" veebileht ning sisselogida Entra ID administraatori kontoga.
- Valida vasakult tulbast "*Identity*", "*All Devices*" seejärel sisestada otsinguribale arvuti nimi.
- Valida valikust õige arvuti, avaneb uus aken, klikkides "*BitLocker keys (Preview)*" saab ligi taastevõtmetele, millest valida kuupäeva järgi kõige värskem, kujutatud joonisel 8.



Joonis 7. *Microsoft Entra Admin center* vaade taastevõtmetele ligipääsemiseks



Joonis 8. *Microsoft Entra Admin Center* vaates taastevõtmete valik