Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2021

Valtteri Hynnä

LAPS-SALASANARATKAISUN IMPLEMENTOINTI ACTIVE DIRECTORYYN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2021 | 35 sivua

Valtteri Hynnä

LAPS-SALASANARATKAISUN IMPLEMENTOINTI ACTIVE DIRECTORYYN

Kyberhyökkäysten on havaittu yleistyneen aiheuttaen samalla uhkia organisaatioiden tietoturvalle. Organisaatioiden heikot salasanakäytänteet voivat lisätä entisestään tietomurtojen uhkaa. Tämän opinnäytetyön tavoitteena oli tuottaa selkeä ja helposti ymmärrettävä tekstikokonaisuus Active Directory -käyttäjähakemistopalvelun tietoturvaa edistävästä salasanaratkaisusta nimeltä LAPS. LAPS:n kaltaisia hallintatyökaluja on luotu tietoturvallisuuden edistämiseksi ja vahvojen salasanakäytäntöjen turvaamiseksi. LAPS:n tarkoituksena on suojata paikalliset hallintakäyttäjätunnukset ja siten estää hyökkääjän eteneminen kohdeverkossa. Työn tavoitteena oli myös tuottaa selkeä ohjeistus LAPS:n käyttöönotosta.

Työn teoriaosuudessa kuvattujen käsitteiden käsittelyllä pyrittiin luomaan kokonaisvaltainen esitys LAPS-salasanaratkaisusta ja sen lähtökohdista. Teoriaosuudessa käytiin läpi Active Directoryn keskeisimpiä käsitteitä, sen vaatimia ylläpitotoimia sekä työntekijöihin ja salasanakäytäntöihin kohdistuvia uhkia. Teoriaosuudessa kerrottiin myös salasananhallinnasta yleisesti, perehtyen tarkemmin Active Directoryn salasanaratkaisuun LAPS:iin.

Tässä opinnäytetyössä LAPS:n käyttöönotto suoritettiin virtuaalisessa VMWare -testiympäristössä, jonka pohjalta opinnäytetyössä kuvattu ohjeistus laadittiin. Opinnäytetyössä onnistuttiin implementoimaan salasananhallintajärjestelmä osaksi omaa testiympäristöä tavoitteen mukaisesti. Se saatiin myös toimimaan halutulla tavalla. Implementoinnin vaiheet saatiin kuvattua havainnollisesti ja samalla todistettua LAPS:n sujuva käyttöönotto.

Työssä pyrittiin korostamaan salasanojen kokonaisvaltaista merkitystä organisaatioiden tietoturvalle. Johtopäätöksenä todettiin, että LAPS on vain pieni osa kokonaisvaltaista tietoturvaa, mutta voi edistää sitä merkittävästi ja yksinkertaisesti, helpon käyttöönoton ja monipuolisen mukautuvuutensa ansiosta.

ASIASANAT:

tietoturva, salasananhallinta, LAPS, Active Directory

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2021 | 35 pages

Valtteri Hynnä

IMPLEMENTATION OF LAPS TO ACTIVE DIRECTORY

Cyber attacks have been found to generalize and simultaneously cause more threats to organizations. Weak password policies can further increase the risk of data breaches. The objectives of this thesis were to provide clear and comprehensible introduction to a password solution called LAPS. Management tools such as LAPS have been made to enhance the picture of security and improve password policies. The purpose of LAPS is to secure local administrator accounts of Active Directory and thus prevent an attacker moving laterally on internal network. The objective of the thesis were also to provide clear guidelines for the implementation of LAPS.

The theoretical part of this thesis aimed to create a comprehensive insight of LAPS via explaining its concepts and bases. The theoretical part also covered the most important concepts of Active Directory, the maintenance required by it and the most common threats targeted to employees and passwords. The theoretical part also covered password management in general with a closer look at the LAPS.

In this thesis the implementation of LAPS was performed in a VMWare virtualization environment on the basis of which the instructions described in the thesis were prepared. The implementation were successfully done as planned and instructions were illustrated clearly. The simplicity and straightforwardness of deployment were also proved and demonstrated.

This thesis were also made to emphasize the holistic importance of passwords for the security of organizations. In conclusion, LAPS is only a small part of comprehensive information security but can make a significant and simple contribution to it thanks to its easy deployment and versatile adaptability.

KEYWORDS:

cyber security, password management, LAPS, Active Directory

SISÄLTÖ

LYHENTEET JA SANASTO **6**

1 JOHDANTO **7**

2 ACTIVE DIRECTORY -KÄYTTÄJÄHAKEMISTOPALVELU **8**

2.1 Active Directoryn looginen rakenne 8

2.1.1 Toimialue 9

2.1.2 Puut ja metsät 10

2.1.3 Organisaatioyksikkö 10

3 ACTIVE DIRECTORYN HALLINTA **12**

3.1 Käyttäjäryhmät 13

3.2 Ryhmäkäytännöt 14

3.3 Porrastettu hallintamalli 14

4 TIETOTURVAUHAT **16**

4.1 Tietojenkalastelu 16

4.2 Hyökkäysketju 17

5 SALASANAT JA SALASANANHALLINTA **19**

5.1 Salasananhallintajärjestelmät 19

5.2 Salasanat Active Directoryssa 21

6 LAPS-SALASANARATKAISU **23**

6.1 LAPS:n hyödyt ja haitat 24

6.2 Implementointi 25

6.2.1 Valmistelut 25

6.2.2 Asennus 25

6.2.3 Käyttöoikeuksien määritys 27

6.2.4 Käyttöönotto työasemilla 28

6.2.5 Salasanojen kysyminen 29

6.2.6 Auditointi 30

7 POHDINTA JA TULOKSET **32**

LÄHTEET **34**

KUVAT

Kuva 1. Active Directoryn looginen rakenne kuvitettuna. 9
Kuva 2. Objekteihin kohdistuvien asetusmuutosten yleisyys ja niistä aiheutuvat vaikutukset koko hallintaympäristöön (Siddaway 2014, 12). 12
Kuva 3. Porrastetun mallin hallintarajoitukset (Smith 2017 ref. Microsoft). 15
Kuva 4. Tietoturvayhtiö Mandiantin laatima Attack Lifecycle -prosessikaaviomalli (Mandiant 2013, 27). 17
Kuva 5. LastPass-salasanamanagerilla generoitu salasana. 20
Kuva 6. Active Directoryn salasanakäytänteiden oletusasetukset. 21
Kuva 7. Uudelleennimetyn Administrator-tilin turvatunniste. 23
Kuva 8. Asennuksessa valittavat ominaisuudet. 26
Kuva 9. PowerShell-komentotulkilla tehdyt kaavamuutokset. 27
Kuva 10. Lukuoikeuksien määritys Helpdesk-ryhmän käyttäjille. 27
Kuva 11. Listaus käyttäjäryhmistä, joilla on oikeudet lukea LAPS:n tallentamat salasanat. 28
Kuva 12. LAPS:n ryhmäkäytäntöasetukset. 28
Kuva 13. Graafinen LAPS UI -työkalu. 29
Kuva 14. Salasanan tulostaminen PowerShell-komentotulkilla. 30
Kuva 15. Salasanan lukeminen ADUC:n avulla. 30
Kuva 16. Auditoinnin käyttöönotto jokaiselle käyttäjälle. 30
Kuva 17. Salasanan kysymisestä aiheutunut lokitapahtuma. 31

LYHENTEET JA SANASTO

ACL	Access Control List eli käyttäjäoikeuslista. Hyödynnetään erityisesti pääsynhallinnassa.
AD	Active Directory. Microsoftin kehittämä käyttäjähakemistopalvelu.
DC	Domain Controller eli ohjauspalvelin. Palvelin, joka toimii käyttäjähakemiston ytimenä ja hoitaa useita tietokannan tärkeitä tehtäviä.
GPO	Group Policy Object. Käyttäjähakemistossa käytettävä asetusobjekti, jonka avulla määritetään käyttäjien ja laitteiden ominaisuuksia.
LAPS	Local Administrator Password Solution. Microsoftin kehittämä salasananhallintajärjestelmä Active Directoryyn.
OU	Organizational Unit eli organisaatioyksikkö. Active Directoryssa oleva säiliötyyppi, jonka sisälle voi asettaa muita objekteja.
Phishing	Verkkourkintaa eli arkaluonteisen tiedon tavoittelua tekeytymällä toiseksi tahoksi.
PowerShell	Microsoftin komentotulkki Windows-käyttöjärjestelmille.
Salasanamanageri	Sovellus tai ohjelmisto, joka huolehtii käyttäjän salasanojen hallinnasta.

1 JOHDANTO

Organisaatioihin kohdistuvat kyberhyökkäykset ovat kasvava trendi. Usein hyökkääjät pyrkivät hyödyntämään kalasteluviestejä päästäkseen yrityksen verkkoon. Kalasteluviesteissä pyritään vetoamaan kohteiden inhimillisyyteen ja hyödyntämään ajankohtaisia teemoja. Samalla heikot ja piittaamattomat salasanakäytännöt altistavat organisaation uhille. Salasananhallintaohjelmat ovat yleistyneet ja niitä suositellaan käytettävän. Ne tarjoavat mahdollisuuden vahvemman salasanapolitiikan käyttämiselle. Myös AD-hallintaympäristö voi hyötyä salasananhallintaohjelman käyttämisestä.

Hyökkääjät tavoittelevat ensisijaisesti suurten käyttöoikeuksien hallintatilejä ja kohdistavat hyökkäykset usein paikallisiin hallintakäyttäjiin. Osa organisaatioista saattaa käyttää yleistä paikallista hallintatunnusta samalla salasanalla jokaisella laiteella, koska se tunnetaan helpoksi eikä siitä aiheutuvia mahdollisia riskejä tunnisteta. Näin ollen hyökkääjä voi saada murretun paikallisen hallintakäyttäjän avulla koko hallintaympäristön eli organisaation kaikki laitteet haltuunsa vain yhden salasanan avulla. Tästä voi seurata organisaation laajuinen tietomurto.

Monille tuntematon LAPS eli Local Administrator Password Solution tarjoaa helpon tuen käyttäjähakemiston turvaksi. Se suojaa paikallisia hallintakäyttäjätunnuksia määrittämällä organisaation tietokoneille eriävän ja turvallisen salasanan vaihtaen niitä määritetyin väliajoin. LAPS:n hallintatyökalusta on kuitenkin vain vähän materiaalia, etenkin suomen kielellä. Tämän opinnäytetyön tavoitteena on luoda tietoisuutta LAPS-työkalusta ja kuvata sen käyttöönottoa. Opinnäytetyön aihe valikoitui myös omasta kiinnostuksestani aiheeseen ja halusta kehittää omaa tietämystäni Active Directory -ympäristöstä.

Tämä opinnäytetyö etenee johdannon jälkeen käsittelylukuihin 2 ja 3, joissa esitellään Active Directoryn rakennetta, yleisimpiä käsitteitä ja käsitellään sen hallinta- ja ylläpitotehtäviä. Lisäksi kuvataan esimerkki tietoturvaa edistävästä hallintamallista. Luvussa 4 kerrotaan tietojenkalastelusta, joka on tilastojen mukaan suurin orgaanisaatioon kohdistuva uhka. Lisäksi kerrotaan kyberhyökkäyksen etenemisen eri vaiheista. Luku 5 keskittyy salasanojen hallintaan ja luvussa 6 perehdytään LAPS-työkaluun. LAPS:n osalta on kuvattuna sen ydintietoja, hyötyjä sekä haittoja ja sen implementointi. Implementointi on suoritettu VMWare-virtualisointiohjelmistoon luodulla Active Directory -testiympäristöllä.

2 ACTIVE DIRECTORY -KÄYTTÄJÄHAKEMISTOPALVELU

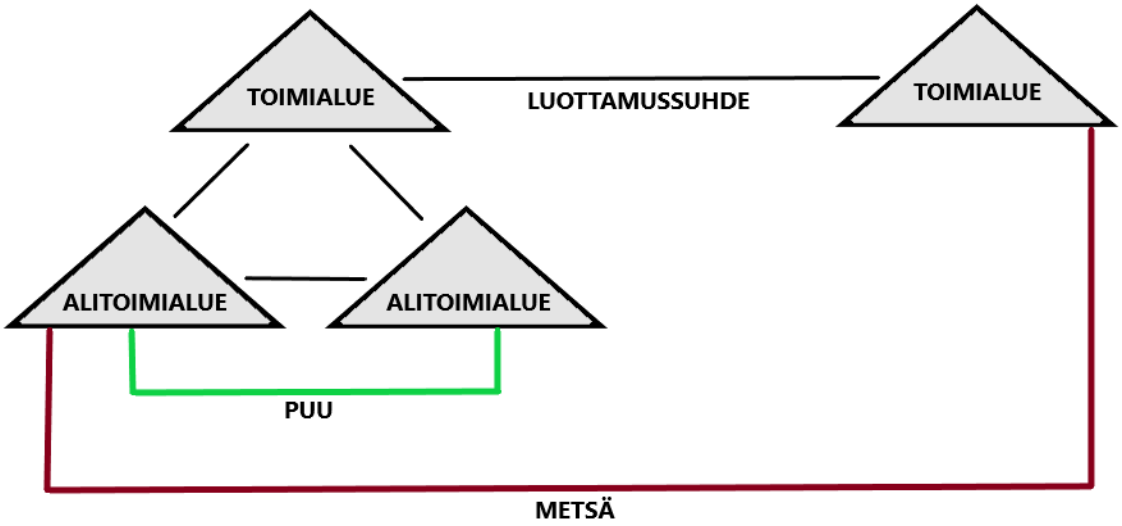
Aktiivihakemisto eli Active Directory on Microsoftin kehittämä käyttäjähakemistopalvelu. Se on julkaistu vuonna 1999 ja se tuli ensimmäisen kerran käyttöön Windows 2000 -käyttöjärjestelmän mukana.

Active Directory on modernin organisaation infrastruktuurin hallinnan peruselementti. Sen avulla hallitaan organisaation käyttäjätilejä, päätelaitteita, palvelimia sekä verkon resursseja. Se on keskitetty palvelukokonaisuus, joka yhdistää toimialueen laitteet ja antaa käyttäjille pääsyn resursseille, mikäli heillä on vaaditut käyttöoikeudet (Siddaway 2014, 4).

2.1 Active Directoryn looginen rakenne

Active Directory on keskitetty tietokanta, joka tuo organisaation resurssit saataville toimialueen käyttäjille mistä päin maailmaa tahansa. Sen sijaan, että ajatellaan tietokannan fyysisiä elementtejä, Active Directoryn loogista rakennemallia hyödyntämällä pystytään hahmottamaan selkeämmin hakemiston kokonaiskuvaa. Samalla se helpottaa toimivan hallintaympäristön suunnittelemista.

Active Directoryn looginen rakenne koostuu tietokannan suurimmista peruselementeistä, joiden avulla rakennetaan koko käyttäjähakemiston perusta. Kuvassa 1 on visualisoitu peruselementit, joita käsitellään seuraavissa alaluvuissa tarkemmin.



Kuva 1. Active Directoryn looginen rakenne kuvitettuna.

Tietokannan perustan ympärille on helppo alkaa rakentamaan toimivaa kokonaisuutta. Hyvin suunniteltu looginen rakenne parantaa parhaimmillaan yrityksen ylläpitokustannuksia, esimerkiksi karsimalla ylimääräistä verkkoresurssien käyttöä. Järjestelmän ylläpitäjien toimivaltaa voidaan selkeämmin kartoittaa vastaamaan välttämättömiä tarpeita ja näin ollen yksinkertaistaa ympäristön hallintaa ja parantaa organisaation kokonaistietoturvaa. (Microsoft 2017a.)

2.1.1 Toimialue

Toimialue (engl. domain) pitää sisällään koko määritetyn organisaatiotoiminnan käyttäjät ja laitteet. Toimialueen rajaa sille määritetty nimiavaruus. Nimiavaruus voi olla määritetty ulkoisen tai sisäisen nimeämisprotokollan mukaisesti. Yritys voi käyttää samaa rekisteröityä nimiavaruutta kuin julkisessa verkossa, jolloin se voi olla esimerkiksi muotoa *example.fi*. Vastaavasti sisäverkon ja julkiverkon nimiavaruudet voidaan pitää erillään, jolloin toimialue voi olla nimetty muotoon *example.local*. Tällöin *.local* on määritetty erilliseksi toimialuetunnukseksi. Sisä- ja ulkoverkon nimiavaruuden nimeäminen eri tavalla saattaa helpottaa verkon hallintaa, sillä päällekkäisiä ylläpitoja ei tällöin tarvita. (Kivimäki 2004, 13–15.)

Pienen organisaation infrastruktuuri on usein mahdollista sisällyttää yhteen toimialueeseen. Suuret ja kompleksit kokonaisuudet voivat hyödyntää useita toimialueita, jolloin

jokaiselle toimialueelle saadaan määritettyä yksilölliset tarpeeseen sopivat turvallisuuskäytännöt.

Toimialuetta ja samalla koko käyttäjähakemistopalvelua ylläpitää yksi tai useampi ohjauspalvelin (engl. domain controller). Ohjauspalvelin toimii koko tietokannan ytimenä ja suorittaa lukuisia eri tehtäviä, esimerkiksi käyttäjien autentikoinnin. (Siddaway 2014, 141.)

2.1.2 Puut ja metsät

Biologisessa ympäristössä metsä on alue, joka koostuu puista. Aktiivihakemistossa metsällä (engl. forest) tarkoitetaan hakemistopalvelun ympäristöä kokonaisuudessaan: se pitää sisällään yhden tai useamman toimialueen eli puun (engl. tree).

Aktiivihakemiston metsän nimi määräytyy ensimmäisen luodun toimialueen eli juuritoimialueen mukaan. Toimialuepuu voi jakaantua useampiin alitoimialueisiin (Kuva 1). Alitoimialueiden välille rakentuu luottamussuhteita (engl. trusts). Luottamussuhteiden avulla voidaan kontrolloida käyttäjien pääsyä ja käyttöoikeuksia eri toimialueiden resursseihin. Alitoimiealueen nimeämispolitiikka määräytyy päätoimialueen mukaan. Mikäli päätoimialueen nimiavaruudeksi on määritetty *example.local*, voi alitoimialue käyttää nimitunnusta *western.example.local.* (Desmond & Richards ym. 2014, 9–11.)

2.1.3 Organisaatioyksikkö

Organisaatioyksiköt (engl. organizational unit) ovat toimialueen aliryhmiä. Ne voidaan kuvitteellisesti rinnastaa vastaamaan kansioita tiedostojärjestelmässä. Organisaatioyksiköt ovat säiliötyyppejä (engl. container). Niiden sisälle voidaan asettaa objekteja eli käyttäjätilejä, konetilejä, ryhmiä ja joissain tapauksissa jopa toisia organisaatioyksiköitä.

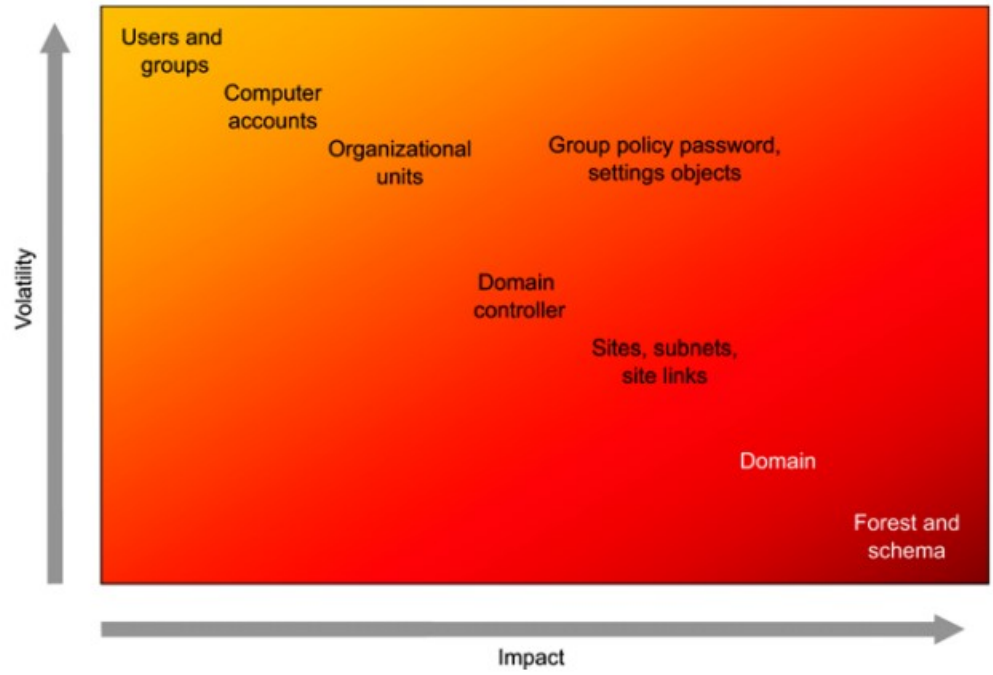
Organisaatioyköiden avulla voidaan rajata hallintakäyttäjien oikeuksia toimialueen sisällä. Mikäli järjestelmänvalvojalle ei haluta antaa hallintaoikeuksia koko toimialueeseen, voidaan toimivalta rajata vain tietyn organisaatioyksikön sisältämiin objekteihin. (Desmond & Richards ym. 2014, 13.)

Organisaatioyksiköitä voidaan käyttää myös apuna ylimääräisten toimialueiden karsimiseen. Mikäli yrityksen toiminta halutaan pitää yhden toimialueen sisällä, voidaan toimialue jakaa useampiin organisaatioyksiköihin. Tämä tekee tietokannan yleisilmeestä selkeämmän ja helpottaa ympäristön ylläpitotehtäviä.

3 ACTIVE DIRECTORYN HALLINTA

Active Directory voi parhaimmillaan kasvaa jopa tuhansista käyttäjistä ja päätelaitteista koostuvaksi tietokannaksi, joten se vaatii myös päivittäisiä hallinta- ja ylläpitotehtäviä. Ylläpitäjät huolehtivat siitä, että hakemistoa päivitetään tarpeiden mukaan ja hakemiston toiminta pysyy käynnissä.

Käyttäjätilit ja -ryhmät sekä ryhmäkäytänteet vaativat eniten toimia kaikista AD:n objekteista. Käyttäjätileihin tehdyillä asetusmuutoksilla on samalla pienin vaikutus koko hallintaympäristöön, lukuun ottamatta suurten oikeuksien hallintatilejä. Metsään tai tietokannan kaavarakenteeseen tehtävät muutokset taas ovat epätavallisia, mutta niistä aiheutuvat vaikutukset ovat myös koko ympäristön kannalta merkittävimmät. (Siddaway 2014, 12.) Tätä kokonaisuutta on visualisoitu kuvassa 2.



Kuva 2. Objekteihin kohdistuvien asetusmuutosten yleisyys ja niistä aiheutuvat vaikutukset koko hallintaympäristöön (Siddaway 2014, 12).

Yleisen tietoturvapolitiikan kannalta ei ole kannattavaa antaa tietylle järjestelmänvalvojalle oikeuksia hallita koko tietokantaa, mikäli vastuualue rajoittuu vain tietyyn käyttäjäryhmään tai osastoon. Delegoimalla hallintatehtäviä voidaan määrittää tarkasti hallintaoikeuksia yksittäiselle käyttäjälle tai käyttäjäryhmälle. Halutulle toimijalle voidaan asettaa

oikeudet tietyn organisaatioyksikön ominaisuuksien hallintaan tai esimerkiksi rajata oikeudet vain tietyn käyttäjäryhmän sisältävien tilien salasanojen nollaamiseen. (Kivimäki 2004, 363.)

Active Directoryssa on useita esiasennettuja työkaluja hallinnointitehtäviä varten. Näistä tunnetuimmat ja yleisimmin käytetyt työkalut ovat ADUC (Active Directory Users and Computers) ja Windows Server 2008 R2:n mukana julkaistu ADAC (Active Directory Administrative Center). Näiden lisäksi perinteinen Windowsin PowerShell-komentotulkki on monipuolinen apuväline, mutta se edellyttää erityistä tietämystä sen käyttämästä komentokielestä. (Desmond & Richards ym. 2014, 33–38).

3.1 Käyttäjäryhmät

Active Directoryssa on oletuksena kolme käyttäjäryhmää korkeimpien oikeuksien hallintatunnuksille. Näiden lisäksi on paikallinen Administrators-ryhmä, joka löytyy myös jokaiselta työasemalta. Administrators-ryhmä takaa rajoittamattomat oikeudet paikallisen laitteen hallintaan. Poikkeuksena ohjauspalvelimen Administrators-ryhmä, joka antaa hallintaoikeudet itse palvelimen lisäksi koko toimialueeseen. Tähän kuuluu automaattesti Domain Admins- sekä Enterprise Admins -ryhmien käyttäjät. (Siddaway 2014, 197.)

Enterprise Admins -ryhmän käyttäjillä on oikeudet koko metsän hallintaan ja on näin ollen tietokannan kriittisin käyttäjäryhmä. Enterprise Admins -oikeuksia tarvitaan esimerkiksi toimialueen luomiseen ja poistamiseen. Domain Admins -käyttäjillä on täydet hallintaoikeudet tiettyyn toimialueeseen ja sen sisältämiin resursseihin. (Siddaway 2014, 197.)

Schema Admins -ryhmän oikeudet vaaditaan tietokannan kaavarakenteen muokkaamiseen. Yleisesti ottaen kaavaan tehtyjä muutoksia pidetään riskialttiina, sillä väärin tai huolimattomasti laaditut konfiguraatiot voivat vahingoittaa koko hallintaympäristöä. Hyvänä esimerkkikäytäntönä on pitää sekä Enterprise Admins- että Schema Admins -ryhmät tyhjinä ja lisätä niihin käyttäjiä ainoastaan tietyn tehtävän suorittamisen ajaksi. (Siddaway 2014, 197.)

3.2 Ryhmäkäytännöt

Ryhmäkäytäntöjen avulla järjestelmänvalvojat voivat kontrolloida päätelaitteiden asetuksia sekä vaikuttaa käyttäjien käyttökokemukseen. Ryhmäkäytännöt ja niihin liittyvät protokollat ovat kokonaisuutena laaja käsite ja merkittävä osa Active Directorya.

Ryhmäkäytäntöjä asetetaan erillisillä ryhmäkäytäntöobjekteilla (engl. group policy object) yksittäisille käyttäjille, päätelaitteille, ryhmille, toimialueille tai organisaatioyksiköille. Ryhmäkäytäntöjen avulla voidaan yksinkertaisimmillaan määrittää esimerkiksi työasemille yhteinen taustakuva tai rajata käyttäjien käyttöoikeuksia Windowsin työkaluihin, kuten PowerShell-komentotulkkiin. Käyttöoikeuksien rajaamista käytetään usein estämään tiettyjen tietokoneen hallintaohjelmistojen tahalliset tai tahattomat väärinkäytöt, joista voisi aiheutua mahdollista vahinkoa hallintaympäristölle. (Desmond & Richards ym. 2014, 283.)

Ryhmäkäytännöillä on niin kutsuttu periytyvä ominaisuus. Mikäli ryhmäkäytäntöobjektin liittää suoraan toimialueeseen, vaikuttavat sille annetut asetukset automaattisesti samalla kaikkiin toimialueen organisaatioyksiköihin ja niiden sisällä oleviin objekteihin (Desmond & Richards ym. 2014, 290). Ryhmäkäytäntöjen avulla voidaan siis aiheuttaa ympäristölle huomaamattomasti tahatonta haittaa, joten niihin tehdyt asetukset tulisi dokumentoida tarkoin.

Ryhmäkäytännöille löytyy oma hallitaohjelma Group Policy Management Console (GPMC), joka tarjoaa työkalut ryhmäkäytäntöjen yleiskuvan havainnointiin, sekä editorin objektien muokkaamiselle (Desmond & Richards ym. 2014, 284).

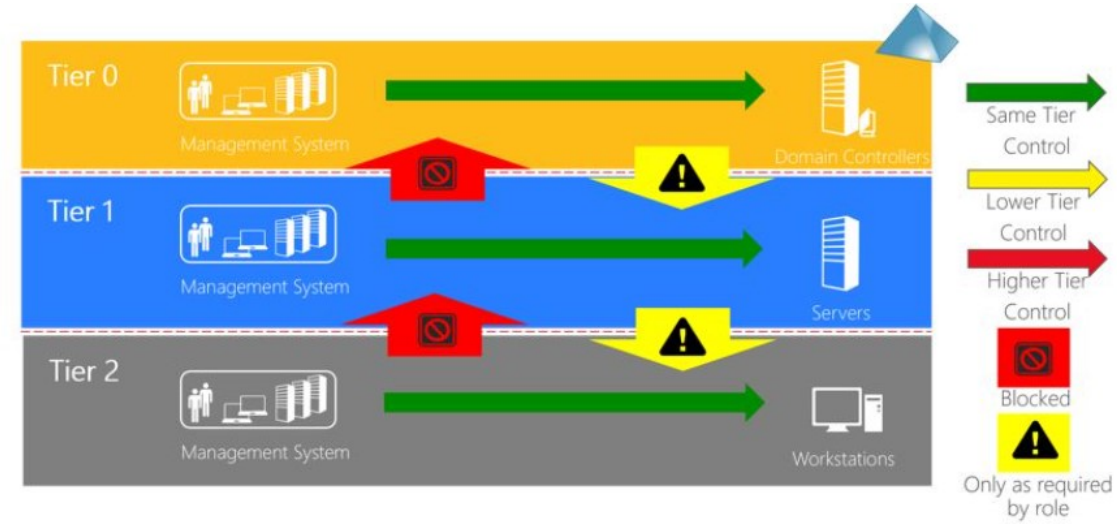
3.3 Porrastettu hallintamalli

Active Directoryn ylläpitoon on suositeltu niin kutsuttua porrastettua hallintamallia, joka edistää erityisesti tietoturvaa. Porrastetussa hallintamallissa koko käyttäjähakemistopalvelu jaetaan osiin näiden kriittisyysasteiden mukaisesti. Jokaisen tason hallintatehtäviin käytetään erillisiä yksilöityjä käyttäjätunnuksia ja mahdollisesti myös erillisiä tietokoneita, jotka tunnetaan yleisesti nimellä Privileged Access Workstation (PAW). (Smith 2017.)

Kriittisimmäksi miellettyyn Tier 0 -portaaseen luetaan kaikki käyttäjätilit, resurssit ja muut objektit, joilla on suora tai epäsuora vaikutus tietokannan hallintaominaisuuksiin. Tällaisia ovat esimerkiksi ohjauspalvelimet, Domain Admins, Enterprise Admins ja Schema Admins -ryhmien käyttäjätilit sekä kaikki päätelaitteet, joille kirjaudutaan edellä mainituilla käyttäjätunnuksilla. (Smith 2017.)

Tier 1 -porras voi pitää sisällään esimerkiksi toimialueen palvelimet ja muut resurssit, joihin tarvitaan erilliset korkeamman tason käyttöoikeudet. Alin ja samalla vähiten potentiaalista vahinkoa aiheuttava Tier 2 -porras koostuu peruskäyttäjien päätelaitteista ja sen hallinta voidaan kohdistaa esimerkiksi helpdesk-osastolle. (Smith 2017.)

Porrastetun hallintamallin keskeisin tarkoitus on käyttää jokaisen tason hallintaan eri käyttäjätunnuksia, ja pitää kriittisimmän tason voimavarat mahdollisimman pienenä (Kuva 3).



Kuva 3. Porrastetun mallin hallintarajoitukset (Smith 2017 ref. Microsoft).

Esimerkkitapauksessa korkeimman tason järjestelmänvalvojalla tulisi siis olla neljä eri käyttätunnusta: kolme jokaisen portaan hallintaan, joita käytetään ainoastaan vaadittuihin ylläpitotehtäviin, sekä yksi yleistunnus ilman hallintaoikeuksia. Kriittisten vomavarojen minimointi pienentää hyökkäyspinta-alaa ja hankaloittaa selvästi mahdollisen ulkopuolisen tunkeutujan pääsyä korkeiden oikeuksien käyttäjätileihin. (Shelbourne 2017.)

4 TIETOTURVAUHAT

Yritysten hyödyntäessä yhä enemmän sähköisiä palveluja ja järjestelmiä, myös rikollisuus on siirtynyt verkkoon. Vaikka rikollisuus on aikojen saatossa muuttanut muotoaan, on päämotivaattori silti sama: raha. Cybersecurity Ventures arvioi globaalin kyberrikollisuuden aiheuttamien kulujen kasvavan vuosittain viidellätoista prosentilla vuoteen 2025 mennessä. Tällöin siitä aiheutuvat vuosittaiset taloudelliset kustannukset saavuttaisivat 10,5 biljoonan dollarin rajapyykin, nousten samalla suurimmaksi rikollisuuden muodoksi. (Morgan 2021, 1.)

Yritykset voivat laatia esimerkillisesti teknisen tietoturvansa ja suojata tärkeät resurssinsa oikeaoppisesti palomuureilla. Samalla voidaan kuitenkin unohtaa, että työntekijät ovat usein ryhmä, johon kohdistuu eniten tietoturvauhkia. On arvioitu, että vuoden 2020 aikana yrityksiin kohdistuneista hyökkäyksistä 95 % on aiheutunut työntekijöihin kohdennettujen kalasteluyritysten kautta (Meharchandani 2020).

4.1 Tietojenkalastelu

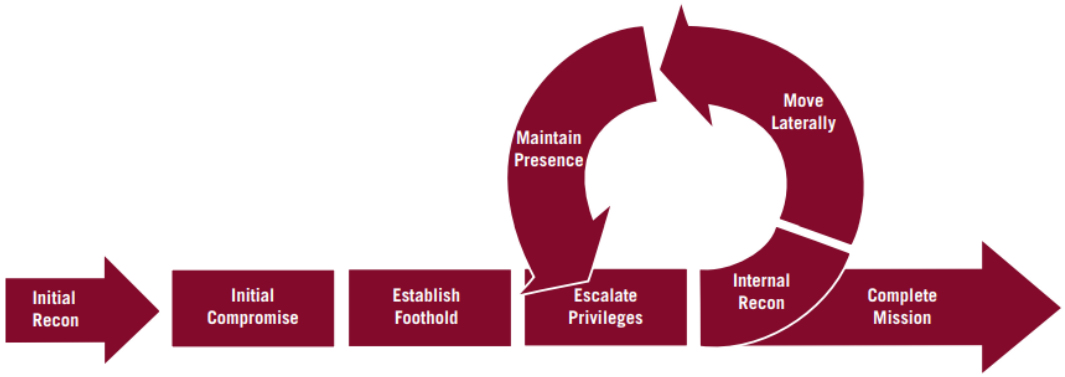
Phishing eli tietojenkalastelu on yleisin sosiaalisen manipuloinnin muoto (Proofpoint 2019). Sen avulla yritetään saada kohde luovuttamaan luottamuksellista tietoa kolmannelle osapuolelle. Kohdennetulla tietojenkalastelulla tarkoitetaan organisaatioon kohdistettua yksilöityä hyökkäystä, joka tapahtuu usein sähköpostiviestein tai sosiaalisen median pikaviestintäpalveluiden kautta. Huijari voi esittää luotettavaa tahoa ja lähettää esimerkiksi manipuloidun kirjautumislinkin uhrille käyttäjätilin vahvistamiseksi tai vanhentuneen salasanan palauttamiseksi. Uhrin avatessa linkin, se voi näyttää ulkoapäin aidolta, mutta syötetyt käyttäjätiedot päätyvätkin suoraan huijarille antaen käyttäjän henkilökohtaisten tietojen lisäksi jalansijan yrityksen verkkoon. Tämä tuo hyökkääjän askeleen lähemmäs laajempaa ja vahingollisempaa hyökkäystä.

F-Securen laatimassa hyökkäystestauksessa asiantuntijat lähettivät eräälle organisaatiolle naamioituja sähköpostiviestejä, joissa pyydettiin avaamaan viestiin liitetty osoitelinkki. Yli puolet kohderyhmästä avasi linkin epäilemättä sen todenperäisyyttä. Toisessa vastaavassa F-Securen testissä, jossa työntekijöitä pyydettiin kirjautumaan huijausportaaliin, 13 prosenttia syötti työtunnuksensa salasanoineen. (F-Secure.) Raportissa ei kuitenkaan mainittu kohderyhmän kokoa.

Kalasteluhyökkäyksissä pyritään usein hyödyntämään uhrien inhimillisyyttä ja käyttämään ajankohtaisia teemoja. Muun muassa koronapandemian tuomia mahdollisuuksia on hyödynnetty kalasteluviesteissä ja poikkeuksellinen maailmantilanne onkin näkynyt huomattavasti kasvaneissa hyökkäystilastoissa. (Kelly 2020.)

4.2 Hyökkäysketju

Hyökkäysketju on alun perin yhdysvaltain armeijalle kehitetty prosessikaavio, joka kuvaa hyökkäyksen eri vaiheita. Se koostuu kuudesta kronologisessa järjestyksessä etenevästä vaiheesta: etsi, tunnista, tarkkaile, kohdista, suorita ja hallitse. Aseteollisuuskonserni Lockheed Martinin tutkijat kehittivät kyseisen kaavion pohjalta visuaalisen havainnollistamismallin myös kyberhyökkäyksille, joka tunnetaan yleisesti nimellä Cyber Kill Chain. Kyseiseen prosessikaavioon perustuvia muunnelmia käytetään edelleen kyberhyökkäyksiä havainnollistaessa ja niiltä suojautuessa. (Korolov & Myers 2018.) Tästä esimerkkinä on Mandiantin näkemys hyökkäyskaaviosta (Kuva 4).



Kuva 4. Tietoturvayhtiö Mandiantin laatima Attack Lifecycle -prosessikaaviomalli (Mandiant 2013, 27).

Hyökkäystä kuvaamaan kehitetyt prosessikaaviot mielletään ketjuiksi erityisesti siksi, että minkä tahansa hyökkäysvaiheen estäminen katkaisee koko hyökkäysprosessin. Ideaalitilanne on katkaista ketju mahdollisimman aikaisessa vaiheessa. Mitä vähemmän hyökkääjä on onnistunut saamaan haltuunsa informaatiota, sitä vaikeampi hyökkäystä on jatkaa myöhemmin saman tai toisen tahon toimesta.

Kyberhyökkäysketju alkaa ulkoisesta tiedusteluvaiheesta, jossa hyökkääjä kerää mahdollisimman paljon informaatiota kohteesta ja laatii hyökkäyssuunnitelman. Julkisista internetlähteistä löytää usein esimerkiksi kohdeorganisaation työntekijöiden yhteystietoja, joita voidaan käyttää hyväksi hyökkäyksessä. (Mandiant 2013, 63.)

Tiedustelua seuraavassa aseistamisvaiheessa hyökkääjä kehittää spesifioidut hyökkäystyökalut, esimerkiksi haitallisen tiedoston tai väärennetyn kirjautumislinkin, joilla tavoitellaan uhrin käyttäjätunnuksia tai suoraa pääsyä tietokoneeseen. Hyökkäystyökalua levitetään kohdennetusti uhreille esimerkiksi sähköpostiviesteillä phishing-menetelmää käyttäen. (Mandiant 2013, 63.)

Uhrin langetessa huijausviestiin, saa hyökkääjä jalansijan yrityksen sisäverkossa ja aloittaa sisäisen tiedustelun. Hyökkääjä pyrkii usein varmistamaan asemansa kohdeverkossa asentamalla takaovia tai etäyhteysohjelmistoja. Sisäverkossa toimiminen tekee haittaohjelmistojen asennuksesta helpompaa, sillä silloin dataliikenteen suunta vaihtuu ja saattaa jäädä heikosti konfiguroidulta palomuurilta huomaamatta. (Mandiant 2013, 63.)

Usein hyökkääjä murtautuu kohdeverkkoon käyttäjätilin kautta, jolla ei ole pääsyoikeuksia haluttuihin resursseihin. Näin ollen hyökkääjä pyrkii etenemään kohdeverkossa poikkisuuntaisesti. Tämä tapahtuu kirjautumalla toimialueen eri laitteille etätyökaluja käyttäen oletustunnuksilla tai heikkoja salasanoja murtamalla. Kohdeverkossa etenemisen tavoitteena on saada haltuun huomaamattomasti suurten käyttöoikeuksien käyttäjätili. Erityisesti Domain Admins -ryhmän käyttäjät, palvelutilit sekä paikalliset hallintatunnukset ovat yleensä hyökkääjän kohteena. (Mandiant 2013, 64.) Toisin sanoen nämä suurten käyttöoikeuksien käyttäjätilit lukeutuvat luvussa 3 mainitun porrastetun hallintamallin Tier 0 -tason tileihin.

Siten varsinaisen tehtävän suorittamisen vaiheessa hyökkääjä on saanut paranneltua jalansijaansa kohdeverkossa poikittaisen etenemisen avulla. Samalla hän on voinut saada täyden hallintaoikeuden toimialueeseen, murretun käyttäjätilin oikeuksista riippuen. Hyökkääjä voi tuhota, varastaa tai lukita halumansa materialiin. Tämän jälkeen hyökkääjä voi poistua kohdeverkosta ja hävittää jäljet mennessään. Joskus hyökkääjä voi myös palata suorittamaan uuden hyökkäysen, hyödyntäen aiemmin luomiaan takaovia. (Mandiant 2013, 64–65.)

5 SALASANAT JA SALASANANHALLINTA

Käyttäjätilejä voidaan pitää kuvitteellisina kulkukortteina yrityksen tietokantaan. Päivän alussa käyttäjä kirjautuu työkoneelleen ja lopulta kirjaa itsensä ulos. Tämän kulkukortin suojana toimii käyttäjätilille määritetty salasana. Heikot tai muuten piittaamattomasti laaditut salasanat mahdollistavat käyttäjätilien varastamisen ja ulkopuolisen tahon pääsyn yrityksen sisäverkkoon.

Yhä useammat verkossa toimivat palvelut vaativat käyttäjätilin luomisen. Tavallisella käyttäjällä voi olla kymmeniä salasanan vaativaa käyttäjätiliä eri palveluissa ja määrä kasvaa vuosittain. Yhdellä internet-käyttäjällä on keskimäärin noin 38 salasanan vaativaa käyttäjätiliä eri palveluissa (LogMeIn 2020, 4). Tämän vuoksi vahvan salasanapolitiikan noudattaminen saattaa olla hankalaa ja voidaan turvautua käyttämään heikkoja helposti muistettavia salasanoja tai peräti samaa salasanaa useassa palvelussa.

Esimerkiksi Googlen ja Harris Poll -markkinointitutkimusorganisaation yhteistyönä laaditusta tietoturvakyselystä ilmeni, että yli puolet kolmesta tuhannesta vastanneesta käyttää samaa salasanaa useassa eri palvelussa ja 13 % käyttää samaa salasanaa jokaisessa käyttämässään palvelussa, mukaan lukien työpaikan käyttäjätilit (Google & Harris Poll 2019). Se tarkoittaa käytännössä sitä, että yhden tilin joutuminen tietomurron kohteeksi vaarantaa samalla myös muut samaa salasanaa käyttävät tilit.

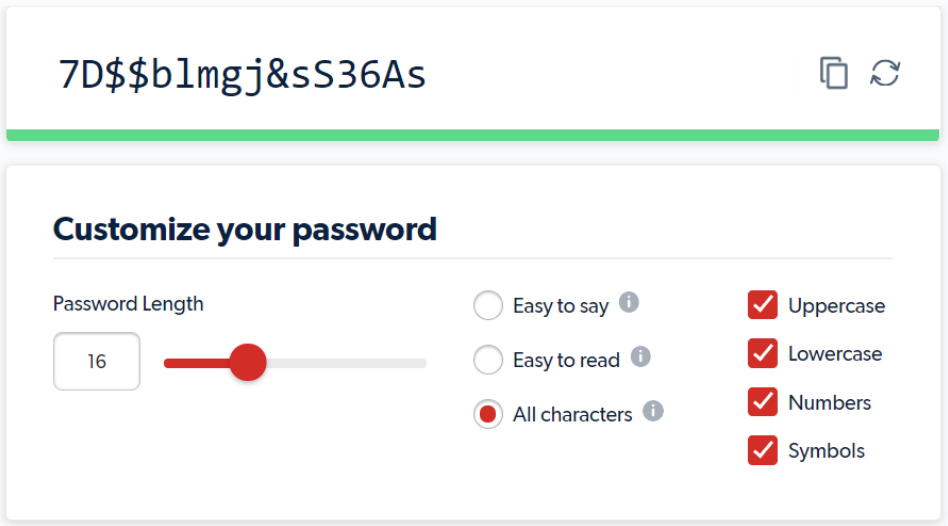
Vahvan salasanapolitiikan noudattaminen on varmin ja samalla helpoin tapa välttyä tietomurroilta, ja parantaa ohella edustamansa yrityksen tietoturvaa. Tärkeimpänä ohjeena on käyttää jokaisessa palvelussa eri salasanaa, eikä niitä tule missään tilanteessa jakaa muille. Lisäksi monivaihetunnistautumista tulisi käyttää aina sen ollessa mahdollista. Salasanan tulisi olla mahdollisimman pitkä ja sen tulisi sisältää isoja kirjaimia sekä erikoismerkkejä. Tunnettujen sanojen käyttämistä on hyvä välttää, sillä modernit sanalistat, joita salasanojen murtamiseen käytettävät hyökkäystyökalut käyttävät, sisältävät yleisimmät käytössä olevat sanat ja niistä muodostetut johdannaiset. (Traficom 2020a.)

5.1 Salasananhallintajärjestelmät

Vahvan salasanapolitiikan saavuttamiseksi useat tietoturvan parissa toimivat organisaatiot, kuten viestintävirasto Traficom, suosittelevat salasananhallintajärjestelmän käyttöä.

Salasananhallintajärjestelmä, toiselta nimeltään salasanamanageri, on erillinen salattu tietokanta, joka säilöö ja hallinnoi käyttäjän eri palveluissa käytettyjä salasanoja. Salasanamanagerin käyttöön vaaditaan yksi pääsalasana, jolla kirjaudutaan itse palveluun ja saadaan käyttöön sen tarjoamat ominaisuudet. Vahvan pääsalasanan määrittäminen on erityisen tärkeää, sillä se toimii samalla kaikkien muiden manageriin tallennettujen salasanojen suojana. (Traficom 2020b.)

Peruskäyttäjille on saatavilla useita eri salasananhallintajärjestelmiä. Sopivaa valittaessa on syytä vertailla niiden ominaisuuksia. Tärkeänä ominaisuutena voidaan pitää esimerkiksi monivaihetunnistautumista. Se tuo lisäkerroksia hallintajärjestelmän tietoturvaan ja mahdollistaa samalla pääsalasanan palauttamisen, mikäli se unohtuu. Salasanamanagerit tarjoavat lisäksi automatisoitua työkalua vahvojen salasanojen luomiseen. Nämä niin kutsutut salasanageneraattorit luovat kymmenien merkkien pituisia satunnaisista kirjaimista ja erikoismerkeistä koostuvia salasanoja (Kuva 5). Koska salasanamanageria käytetään yhden pääsalasanan avulla, ei muiden sinne tallennettujen käyttäjätilien salasanoja tarvitse muistaa. Tämän ominaisuuden vuoksi voidaankin käyttää pitkiä ja komplekseja salasanoja eri tileissä. Osa salasanamanagereista auttaa suojautumaan myös mahdollisilta kalasteluyrityksiltä. Mikäli käyttäjä on esimerkiksi avannut sähköpostin mukana tulleen kirjautumislinkin, mutta salasanamanageri ei tunnista sitä, on aiheellista epäillä verkkosivun todenperäisyyttä. (Traficom 2020b.)



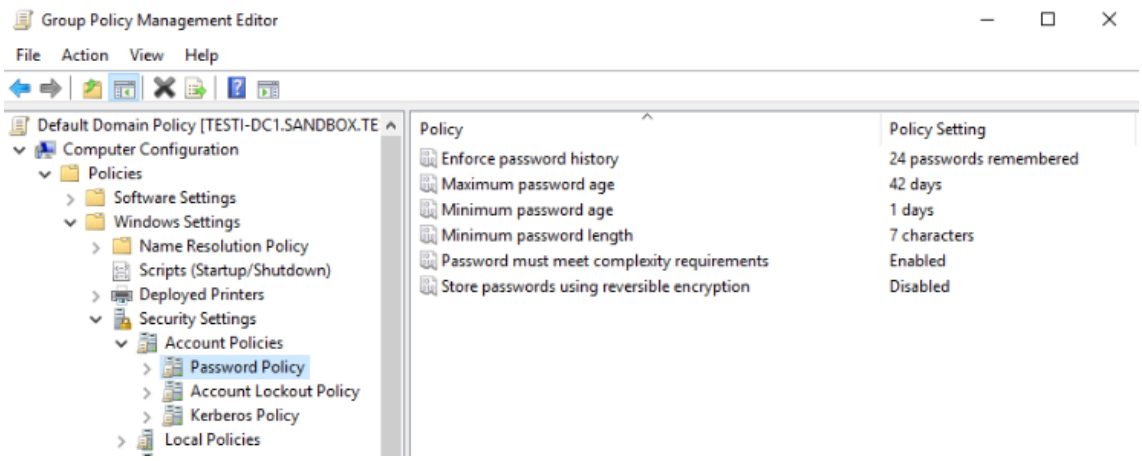
Kuva 5. LastPass-salasanamanagerilla generoitu salasana.

Yleisimmät salasanamanagerit toimivat verkkoselaimeen lisättävinä laajennustyökaluina, erillisinä ohjelmistoina tai mobiililaitteisiin ladattuina sovelluksina. Salasanamangerit tarjoavat usein mahdollisuutta myös tilien synkronoimiselle tietokoneen ja mobiililaitteiden välillä. Tunnettuja yksityiskäyttäjille sunnattuja salasanamanagereita ovat muun muassa 1Password, Dashlane ja LastPass.

5.2 Salasanat Active Directoryssa

Active Directoryssa salasanakäytänteet määritetään salasanaobjektien avulla. Windows Server 2008:n mukana tulleet uudistukset mahdollistivat ensi kertaa useiden salasanakäytäntöjen luomisen yhden toimialueen sisälle. Nykyään salasanaobjektit voidaan kohdentaa tietylle käyttäjäryhmälle tai organisaatioyksikölle normaalin objektikäytännön mukaisesti käyttämällä salasanojen hienosäätömahdollisuutta (engl. fine-grained password policy). Esimerkiksi hallintakäyttäjille voidaan asettaa erilaiset salasanakäytänteet kuin peruskäyttäjille. (Siddaway 2014, 125–126.)

Salasanaobjekti sijaitsee oletuksena suoraan juuritoimialueeseen liitettynä, joten se vaikuttaa kaikkiin toimialueen käyttäjiin. Kuvassa 6 on nähtävissä salasanaobjektin oletusasetukset.



Kuva 6. Active Directoryn salasanakäytänteiden oletusasetukset.

Näitä oletusasetuksia voidaan pitää yleisesti ottaen heikkoina ja esimerkisi salasanan vaadittua vähimmäismerkkipituutta tulisi nostaa. Vaikka salasanan säännöllinen vaihtaminen on suositeltavaa, myös sen alkuperäisesti asetettua 42 päivän vaihtoväliä olisi suotavaa pidentää. Lyhyin aikavälein vaihdettu salasana saattaa unohtua helposti ja

kuormittaa ylläpitäjiä turhilla hallintatomilla. Valtaosan käyttäjistä on todettu myös vaihtavan salasanaa muokkaamalla vanhaa käytössä olevaa salasanaa, mikä ei todellisuudessa paranna sen vahvuutta ja luotettavuutta (Balbix 2020, 6).

Myös Active Directoryssä on mahdollista hyödyntää salasananhallintajärjestelmää. Hallintajärjestelmän integraatio laajaan käyttäjähakemistopalveluun tuottaa kuitenkin tiettyjä peruskäytöstä poikkeavia ongelmia, sillä käyttäjätilien ja salasanojen hallinnan tulee olla keskitettyä. Salasananhallintajärjestelmät ovat lähes aina kolmannen osapuolen tarjoamia palveluita, eikä yritykset välttämättä halua ulkopuolista palveluntarjoajaa osaksi tietojärjestelmäänsä. Tämä siis saattaa kasvattaa kynnystä tietokantaan liittämiselle. Poikkeuksena tälle on Microsoftin oma Active Directoryyn kehitetty salasanaratkaisu LAPS, joka tarjoaa suojaa paikallisille hallintakäyttäjätunnuksille.

6 LAPS-SALASANARATKAISU

Valitettavan usein organisaation kaikkiin työasemiin on mahdollista kirjautua yhtä ja samaa salasanaa käyttävällä paikallisella hallintakäyttäjätunnuksella. Tämä hallintatunnus on usein Windowsin natiivi Administrator-tili. Administrator-tili on ainoa käyttöjärjestelmän mukana tuleva tili, jolla on rajoittamattomat hallintaoikeudet laitteeseen. Administrator-tilillä on laitteesta huolimatta aina sama turvatunniste (SID), joka on muotoa *S-1-5-21-domain-500*. Turvatunniste ei muutu, vaikka tilin nimeäisi uudelleen (Kuva 7). Tästä syystä se on helposti identifioitavissa ja usein hyökkääjien ensimmäinen kohde. Paikallisen hallintatunnuksen tarpeetonta käyttöä tulisi välttää ja siihen tulisi turvautua ainoastaan äärimmäisissä tilanteissa esimerkiksi silloin, kun toimialuekäyttäjällä kirjautuminen ei ole mahdollista. (Metcalf 2015.)

```
User Name          SID
================== ============================================
pc-01\frasiercrane S-1-5-21-2969175712-2931743174-2502246324-500
```

Kuva 7. Uudelleennimetyn Administrator-tilin turvatunniste.

Samaa salasanaa usealla laitteella käyttävä hallintatunnus mahdollistaa hyökkääjälle helpon etenemisen kohdeympäristössä eri laitteiden välillä. LAPS eli Local Administrator Password Solution on Microsoftin kehittämä, vuonna 2015 julkaistu ilmainen salasanahallintatyökalu Active Directoryyn. Sen tarkoituksena on tuoda lisäturvaa koko hallintaympäristölle suojaamalla paikalliset hallintakäyttäjätunnukset. LAPS automatisoi paikallisen hallintakäyttäjätilin ylläpidon generoimalla jokaiselle määritetylle tietokoneelle eriävän, vahvan salasanan ja vaihtaa niitä automaattisesti halutuin väliajoin. (Microsoft 2017b.)

Paikallisen hallintatunnuksen käyttämisestä on useita eri näkemyksiä. Joidenkin mielestä natiivia Administrator-tili tulisi pitää käytössä, koska silloin Administrators-ryhmän käyttäjämäärä pysyisi mahdollisimman pienenä. Toisaalta joidenkin mielestä se pitäisi lukita ja korvata se ryhmäkäytäntöjen avulla luodulla paikallisella hallintakäyttäjällä. Administrator-tiliä ei kuitenkaan ole mahdollista poistaa, mutta lukitseminen onnistuu.

Koska LAPS:lla on mahdollista hallinnoida vain yhtä tiliä, Microsoft on suunnitellut sen alun perin natiivin Administrator-tilin hallinnoimiseen. LAPS:ia voidaan käyttää myös itse

luodulla paikallisella käyttäjällä. Yleisesti ottaen on kuitenkin suositeltavaa pyrkiä pitämään Administrators-ryhmän käyttäjämäärä mahdollisen pinenenä. (Metcalf 2015).

LAPS:n asettamat salasanat tallentuvat selkokielisenä Active Directoryn tietokantaan ja ne ovat suojattu ACL:n eli käyttäjäoikeuslistan avulla. Käyttäjäoikeuslistalla voidaan määrittää yksityiskohtaisesti käyttäjät tai käyttäjäryhmät, joilla on oikeus lukea salasanat tietokannan muistista. Vaikka salasanat tallentuvat selkokielisinä, ne eivät ole nähtävissä ohjauspalvelimen auditointilokeista, eivätkä ne replikoidu Read-Only-ohjauspalvelimille. Salasanojen turvana toimii myös Kerberos-protokollaan perustuva salausmenetelmä. (Microsoft 2015.)

6.1 LAPS:n hyödyt ja haitat

LAPS:ssa, kuten muissakin hallintajärjestelmissä on sekä hyötyjä että haittoja. LAPS:ssa hyötyjen suhde on kuitenkin huomattavasti suurempi, jonka vuoksi sen käyttöönotto on suositeltavaa. LAPS:n ylläpitoon ei tarvita ylimääräisiä palvelimia tai muita fyysisiä resursseja, sillä se on itsenäinen ryhmäkäytäntöobjektien liitännäinen (engl. group policy client-side extension). LAPS lataa koneen välimuistiin pienen DLL-tiedoston, joka aktivoituu aina ryhmäkäytäntöjen päivittyessä, toisin sanoen käyttäjätilille kirjautuessa tai tietokoneen käynnistyessä. Se ei siis ole erillinen ohjelma, eikä näin ollen vaikuta tietokoneen toimintakykyyn. LAPS automatisoi täysin paikallisten hallintatilien salasanojen hallinnan määritettyjen asetusten mukaisesti, eikä vaadi ylläpitäjiltä erillisiä toimenpiteitä. LAPS:n etuina voidaan pitää myös sen riippumattomuutta kolmannesta osapuolesta ja helppoa integraatiota hallintaympäristöön. (Stacey 2018.)

LAPS:sta aiheutuvat haitat johtuvat usein käyttäjän tekemistä virhekonfiguraatioista tai muusta huolimattomasta toiminnasta. LAPS voi hallinnoida vain yhtä tiliä kerrallaan, joten se voi altistaa Administrator-tilin turhalle käytölle, mikäli riskejä ei tiedosteta. Koska salasanat tallentuvat selkotekstinä tietokantaan, huolimattomasti määritetty ACL saattaa mahdollistaa väärien henkilöiden pääsyn salasanoihin. Luku- tai muokkausoikeudet saaneet henkilöt pääsevät milloin tahansa näkemään salasanat. LAPS:n käyttöliikennettä on kuitenkin mahdollista auditoida, mutta auditointimääritykset on konfiguroitava erikseen. Keskitetty salasananhallinta aiheuttaa sen, että mikäli ulkopuolinen taho pääsee käsiksi ohjauspalvelimeen, vaarantuu samalla myös kaikki LAPS:n hallinnoimat salasanat. Resurssina ohjauspalvelin itsessään on kuitenkin huomattavasti kriittisempi, joten sen vaarantuessa ongelmat ovat lähtökohtaisesti suurempia. (Metcalf 2015).

6.2 Implementointi

Tässä opinnäytetyössä implementointi suoritetaan VMWare-virtualisointiohjelmistoon luodulla Active Directory -testiympäristöllä. Toimialueeksi on määritetty SANDBOX.test. Implementoinnin vaiheina ovat muun muassa asennus, käyttöoikeuksien määritys, salasanojen hakeminen ja auditoinnin käyttöönotto.

6.2.1 Valmistelut

Ennen LAPS:n käyttöönottoa on hyvä tarkistaa organisaation toimintatavat paikallisille hallintakäyttäjätileille ja niiden käyttämälle salasanapolitiikalle. Sen perusteella tulee tehdä arvio siitä, tarvitaanko LAPS:n kaltaista salasananhallintaa. Tämän jälkeen tulee suorittaa toimialueen kartoitus ja määrittää laitteet, joihin LAPS halutaan asentaa. Erityisen tärkeää on samalla suunnitella tarkoin listat käyttäjistä, jotka pääsevät lukemaan LAPS:n tallentamat salasanat tietokannasta sekä käyttäjät, joilla on täydet hallintaoikeudet työkalun ominaisuuksiin. Salasanaratkaisun käyttäminen edellyttää yhtenäistä sitoutumista ja ymmärrystä siitä, että käytäntöjen laiminlyöminen mitätöi niiden alkuperäisen tarkoituksen.

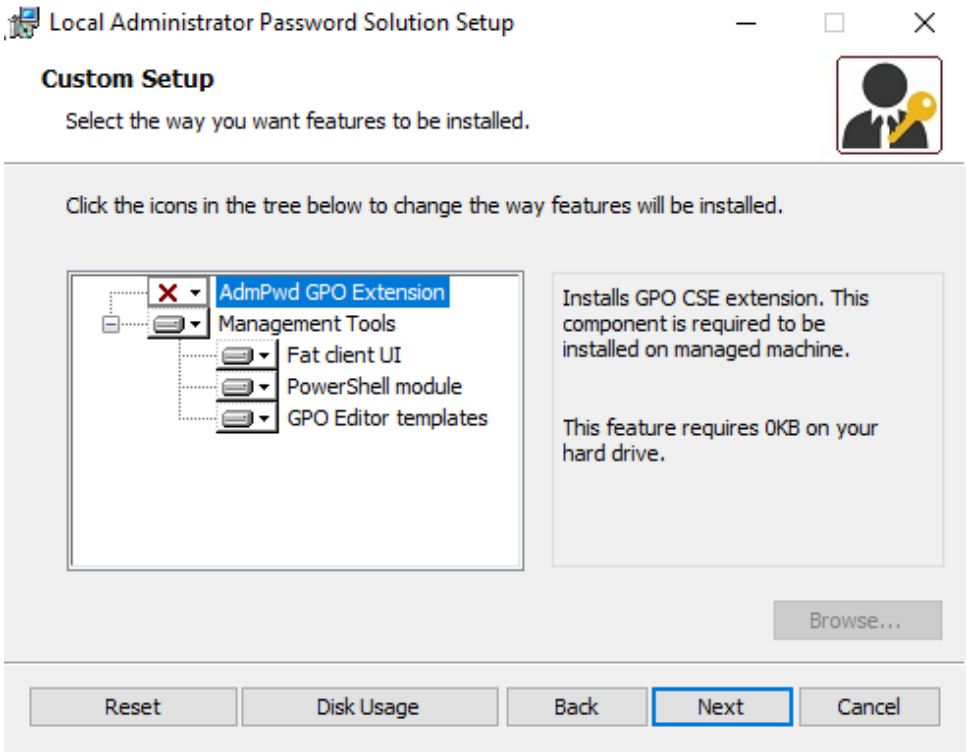
6.2.2 Asennus

LAPS:n asennus on suoritettava Schema Admins -ryhmään kuuluvalla käyttäjällä, sillä tietokannan kaavarakenteeseen on tehtävä pieniä attribuuttimuutoksia. Tietokanta on suositeltavaa varmuuskopioida ennen asennusta.

LAPS:n asennustiedosto on saatavilla Microsoftin omilta verkkosivuilta. Asennus voidaan suorittaa millä tahansa toimialueeseen liitetyllä tietokoneella tai palvelimella. Ohjauspalvelimen käyttäminen ei kuitenkaan ole suositeltavaa, sillä tietoturvan edistämiseksi ohjauspalvelinta ei tulisi käyttää ylimääräisiin toimenpiteisiin (Microsoft 2017c). Hallintatyökalut on kuitenkin halutessa mahdollista asentaa myös ohjauspalvelimelle esimerkiksi ryhmäkäytäntöjen tai verkkojaon kautta.

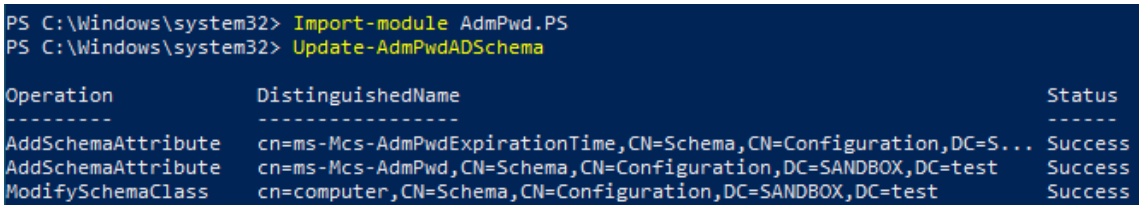
Laitteelle, jolla ensiasennus suoritetaan, määritetään työkalun hallintaominaisuudet. Asennuksessa valitaan siis Management Tools -hallintatyökalut (Kuva 8). AdmPwd GPO

Extension -lisäosa on tarkoitettu asennettavaksi laitteelle, joita LAPS:n halutaan hallinnoivan. Tässä esimerkkitapauksessa hallintalaitteelle ei haluta LAPS-ominaisuutta käyttöön, joten se jätetään valitsematta. Mikäli liitännäinen asennetaan ohjauspalvelimelle, se hallinnoi automaattisesti ohjauspalvelimen Administrator-tiliä. Tämä on huomionarvoista siitä syystä, että ohjauspalvelimen Administrator-tili ei ole poikkeuksellisesti laitekohtainen vaan sillä on koko toimialueen laajuiset oikeudet, kuten luvussa 3.1 on mainittu.



Kuva 8. Asennuksessa valittavat ominaisuudet.

Asennustiedoston ladattua voidaan tehdä tietokannan kaavaan tarvittavat muutokset, kuten kuvassa 9 on kuvattu. Attribuuttimuutokset tehdään syöttämällä PowerShell -komentotulkkiin komento `Import-module AdmPwd.PS`. Komennolla `Update-AdmPwdADSchema` otetaan muutokset käyttöön. Komento lisää tietokantaan kaksi uutta attribuuttia. Attribuutti ms-Mcs-AdmPwd tallentaa salasanan selkokielisenä ja estää muun muassa replikoinnin Read-Only-ohjauspalvelimelle. Toinen lisätty attribuutti ms-Mcs-AdmPwdExpirationTime tallentaa salasanan vanhentumisajan. (Metcalf 2015.)



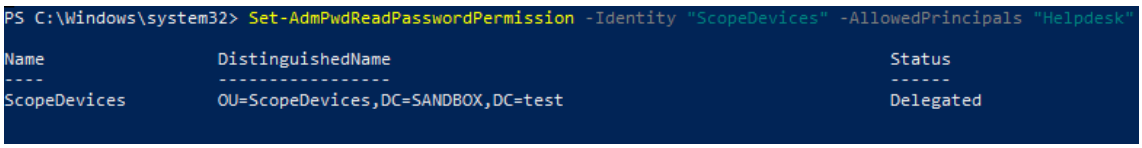
Kuva 9. PowerShell-komentotulkilla tehdyt kaavamuutokset.

Kaavamuutosten onnistuminen voidaan varmistaa komentotulkin Status-sarakkeesta, jossa tulisi lukea ”Success” kuvan 9 mukaisesti.

6.2.3 Käyttöoikeuksien määritys

PowerShell-komentotulkin komennolla `Set-AdmPwdComputerSelfPermission -OrgUnit ”OU”` annetaan halutun organisaatioyksikön laitteiden päivittää paikallisen hallintakäyttäjän salasanan attribuuttia ms-Mcs-AdmPwd. Tämä tulee tehdä laitteille, joille halutaan ottaa käyttöön LAPS-ominaisuus.

LAPS-työkaluun on mahdollista määrittää kaksi käyttäjäluokkaa: toinen salasanojen lukemista varten, toinen nollaamista varten. Lukuoikeudet voidaan määrittää esimerkiksi helpdesk-osastolle (Kuva 10). Lukuoikeuksien määritys tapahtuu komennolla `Set-AdmPwdReadPasswordPermission -Identity ”OU” -AllowedPrincipals ”Group”`. Oikeudet salasanojen nollaamiselle annetaan komennolla `Set-AdmPwdResetPasswordPermission -Identity ”OU” -AllowedPrincipals ”Group”`.



Kuva 10. Lukuoikeuksien määritys Helpdesk-ryhmän käyttäjille.

Komennolla `Find-AdmPwdExtendedRights -Identity ”OU”` saadaan listattua käyttäjäryhmät, joilla on oikeudet lukea LAPS:n tallentamat salasanat (Kuva 11). Komennon avulla on hyvä tarkistaa mahdollisten väärien ryhmien oikeudet.

```
PS C:\Windows\system32> Find-AdmPwdExtendedRights -Identity ScopeDevices |
>> Format-Table ExtendedRightHolders

ExtendedRightHolders
--------------------
{NT AUTHORITY\SYSTEM, SANDBOX\Domain Admins, SANDBOX\Helpdesk}
{NT AUTHORITY\SYSTEM, SANDBOX\Domain Admins}
{NT AUTHORITY\SYSTEM, SANDBOX\Domain Admins}
```

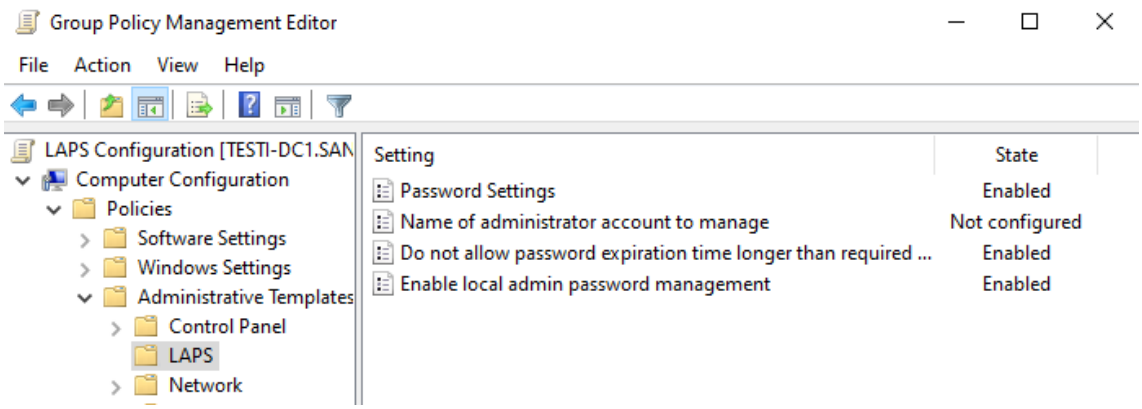
Kuva 11. Listaus käyttäjäryhmistä, joilla on oikeudet lukea LAPS:n tallentamat salasanat.

Halutun ryhmän käyttöoikeudet voidaan muuttaa ADUC-työkalun avulla poistamalla All extended rights -ominaisuus käytöstä. Lähtökohtaisesti LAPS:n käyttöoikeudet on suositeltavaa rajata mahdollisimman pienelle määrälle käyttäjiä. Domain Admins -ryhmä kuuluu oletuksena LAPS:n hallintakäyttäjiin.

6.2.4 Käyttöönotto työasemilla

LAPS-liitännäisen jakaminen halutuille työasemille on mahdollista suorittaa eri tavoin. Aikaisemmin ladattu tiedosto voidaan esimerkiksi jakaa paikallisverkkojaon kautta toimialueen käyttäjille ja asentaa liitännäinen manuaalisesti yksittäisille laitteille. Suuressa ympäristössä voidaan hyödyntää SCCM-työkalua, jonka avulla asennus voidaan tehdä keskitetysti usealle laitteelle samanaikaisesti.

LAPS:n käyttöä varten luodaan erillinen ryhmäkäytäntöobjekti, joka liitetään haluttuun organisaatioyksikköön. 6.2.2 esitellyssä asennuksessa ryhmäkäytäntöeditoriin lisättiin automaattisesti LAPS-välilehti, joka koostuu neljästä konfiguroitavasta asetuksesta (Kuva 12).

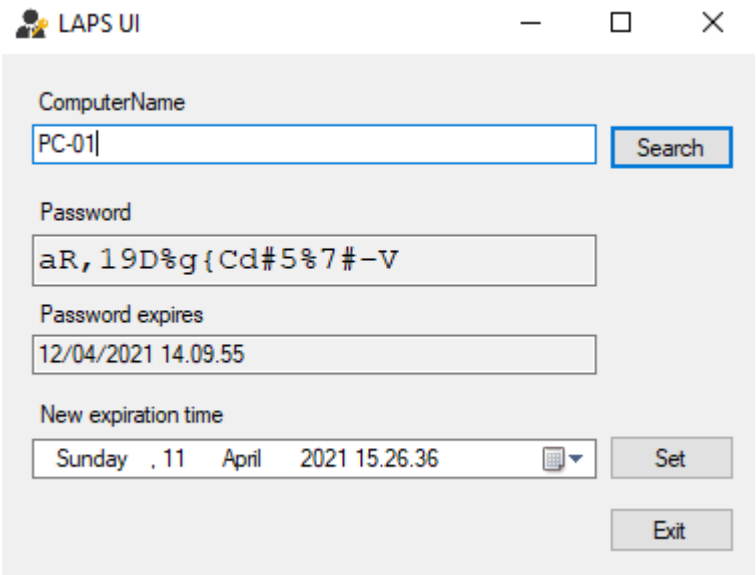


Kuva 12. LAPS:n ryhmäkäytäntöasetukset.

”Password Settings” -asetuksen avulla määritetään LAPS:n tuottamien salasanojen pituus, käytettyjen erikoismerkkien monipuolisuus sekä salasanan automatisoitu vaihtoväli. Mikäli organisaatiossa käytetään erillistä paikallista hallintatunnusta, tulee se syöttää ”Name of administrator account to manage” -editoriin. Muussa tapauksessa se jätetään konfiguroimatta, sillä LAPS hallitsee automaattisesti SID 500 -tunnusta, vaikka tilin nimi olisi vaihdettu. ”Enable local admin password management” -asetus aktivoi työkalun. Ryhmäkäytäntöä määrittäessä on tärkeä huomioida, että juuriyksikköön liitetty ryhmäkäytäntöobjekti vaikuttaa kaikkiin sen sisällä oleviin resursseihin. Uudet ryhmäkäytännöt voidaan varmistaa käyttöönotettaviksi ajamalla PowerShell-komento `gpupdate /force`.

6.2.5 Salasanojen kysyminen

Luvussa 6.2.3 määritetyt käyttäjät voivat lukea LAPS:n tallentamia salasanoja eri tavoin. Mikäli laitteelle on asennettu LAPS:n hallintatyökalut, voidaan käyttää kuvassa 13 esitettyä LAPS UI -ominaisuutta. Työkaluun syötetään halutun laitteen nimi ja se tulostaa laitteessa sillä hetkellä käytössä olevan salasanan ja sen vanhentumisajan. Työkalulla on mahdollista pyytää myös uutta vanhentumisaikaa.



Kuva 13. Graafinen LAPS UI -työkalu.

PowerShell-komentotulkin avulla voidaan hakea halutun laitteen salasanaa komennolla `Get-AdmPwdPassword -ComputerName <computername>` kuvan 14 mukaisesti. Käyttäjät, joilla on ResetPasswordPermission-oikeudet voivat pyytää tilille välittömästi uutta salasanaa komennolla `Reset-AdmPwdPassword -ComputerName <computername>`.

```
PS C:\Windows\system32> Get-AdmPwdPassword -ComputerName PC-01

ComputerName         DistinguishedName                          Password          ExpirationTimestamp
------------         -----------------                          --------          -------------------
PC-01                CN=PC-01,OU=Workstations,OU=ScopeDevices,D... aR,19D%g{Cd#5%7#-V 4/12/2021 2:09:55 PM
```

Kuva 14. Salasanan tulostaminen PowerShell-komentotulkilla.

Salasanat voidaan lukea myös ADUC-hallintatyökalun avulla halutun laitteen attribuuttieditorista (Kuva 15).

Kuva 15. Salasanan lukeminen ADUC:n avulla.

6.2.6 Auditointi

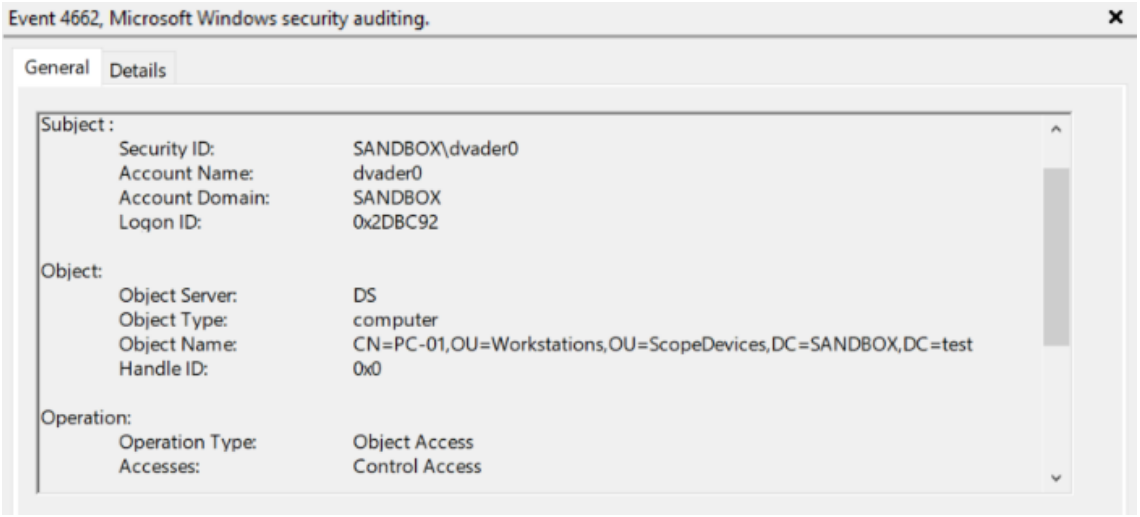
Luvussa 6.2.5 esiteltyjen salasanojen hakemiseen tarkoitettujen työkalujen käyttäminen on rajoittamatonta. Tämän vuoksi niihin saattaa kohdistua tarpeetonta käyttöä. LAPS ei auditoi työkalun käyttöliikennettä oletuksena. LAPS tarjoaa kuitenkin mahdollisuuden auditoinnin käytölle. Auditointi on mahdollista määrittää koskemaan vain tiettyjä käyttäjäryhmiä tai kaikkia mahdollisia käyttäjiä, kuten kuvassa 16 on esitetty. Auditointi voidaan ottaa käyttöön komennolla `Set-AdmPwdAuditing -Identity ”OU” -AuditedPrincipals ”Group”`.

```
PS C:\Windows\system32> Set-AdmPwdAuditing -Identity "ScopeDevices" -AuditedPrincipals Everyone

Name                 DistinguishedName                                  Status
----                 -----------------                                  ------
ScopeDevices         OU=ScopeDevices,DC=SANDBOX,DC=test                 Delegated
```

Kuva 16. Auditoinnin käyttöönotto jokaiselle käyttäjälle.

Kun auditointi on aktivoitu ms-Mcs-AdmPwd -attribuutin käyttäminen aiheuttaa Windows Security -lokitapahtuman, jonka yksilöity tapahtumatunnus on 4662 (Kuva 17).



Kuva 17. Salasanan kysymisestä aiheutunut lokitapahtuma.

Lokitapahtumasta nähdään esimerkiksi tapahtuman aikaleima ja käyttäjä, jonka toimesta LAPS:ia on käytetty sekä laite jonka salasanaa on kysytty.

7 POHDINTA JA TULOKSET

Tämän opinnäytetyön tavoitteena oli käsitellä LAPS-salasanaratkaisua ja luoda sen käytöönotosta ohjeistus. Opinnäytetyön alussa käsiteltiin LAPS:n kannalta olennaisia lähikäsitteitä, kuten Active Directorya ja sen ylläpitoa. Samalla työssä kuvattiin heikoista salasanoista aiheutuvia mahdollisia seurauksia ja kalasteluviestejä yhtenä hyökkäysmuotona. Lähikäsitteiden ja olennaisten aihealueiden kuvaamisen tarkoituksena oli luoda kokonaisvaltainen kuvaus LAPS-salasanaratkaisusta, sen lähtökohdista ja merkityksestä organisaatioiden tietoturvan näkökulmasta tarkasteltuna.

Työssä suoritettu LAPS:n implementointi on kuvattu vaihe vaiheelta, koska sen käyttöönottoa on pyritty havainnollistamaan ohjeistuksessa. Implementointi sujui helposti ja toimi virtuaaliympäristössä odotetun kaltaisesti. Tekemäni tarkastelun perusteella voi myös todeta, että LAPS:iin liittyvää tietoa ei juurikaan ole tarjolla suomeksi, jonka puutteeseen tässä työssä on pyritty vastaamaan. Lähteenä on käytetty pitkälti ajankohtaista verkosta löytyvää vieraskielistä materiaalia, esimerkiksi tietoturva-alan asiantuntijoiden artikkeleita sekä blogikirjoituksia.

Kyberhyökkäyksistä aiheutuvat kasvavat kokonaiskustannukset ja esimerkiksi ajankohtaisen koronavirusepidemian myötä kasvaneet hyökkäystilastot osoittavat, että LAPS:n kaltaisille ratkaisuille on tarvetta. Ne voivat turvata organisaatioiden tietoturvaa mahdollistamalla vahvan salasanapolitiikan käytön. Tämänkaltaisella pienellä asialla, kuten turvallisella salasanalla voi olla suuri vaikutus. Hyökkäysketjun osoittamalla tavalla parhain ratkaisu on katkaista hyökkäys aikaisessa vaiheessa. Kyberhyökkäysten kohdalla LAPS:n kaltainen työkalu voi estää sen, etteivät hyökkääjät pääse levittäytymään koko hallintaympäristöön.

Tekemäni tarkastelun mukaan LAPS:n käyttö osana käyttäjähakemistoa yhdessä porrastetun hallintamallin kanssa voi parantaa organisaatioiden tietoturvaa merkittävästi. LAPS:n käyttöönotto on myös helposti toteuttavissa ja se mukautuu erilaisiin käyttöympäristöihin. Se on siis yksinkertainen tapa parantaa organisaatioiden tietoturvaa.

Käytännössä LAPS on kuitenkin vain pieni osa kokonaisvaltaista tietoturvaa. Samalla organisaatioiden sisäisten salasananhallintajärjestelmien käyttö tarvitsee yhtenäisen linjauksen. Teknisen tietoturvan lisäksi henkilöstön proaktiivinen valistaminen tietoturvasta sekä ajankohtaisista uhkatekijöistä on tärkeää.

Tämä opinnäytetyö kehitti omaa tietämystäni Active Directorysta ja sen hallintatoimista. Jatkossa aion perehtyä syvemmin AD:n ominaisuuksiin, sen tietoturvaa parantaviin ratkaisuihin sekä eri kyberhyökkäysmenetelmiin ja niiden havainnointiin. Koska LAPS:n kaltaiset työkalut voivat tehokkaasti ehkäistä tietomurtoja ja siten kasvavia kyberhyökkäyksistä aiheutuvia kustannuksia, aion perehtyä myös muihin vastaaviin työkaluihin.

LÄHTEET

Balbix 2020. Passwords In The Enterprise - State of Password Use Report.

Desmond, B. & Richards, J. & Allen, Robbie & A Lowe-Norris, A.G. 2013. Active Directory: Designing, Deploying, and Running Active Directory 5th Edition, 2013.

F-Secure. Tutkimukset & raportit, yritysten turvallisuus. F-Secure: Luottamus teknologiaan luo yrityksissä väärää turvallisuudentunnetta – yli puolet työntekijöistä klikkasi huijausviestin linkkiä. Viitattu 16.2.2021. https://www.f-secure.com/fi/press/p/f-secure-luottamus-teknologiaan-luo-yrityksissa-vaaraa-turvallisuudentunnetta-yli-puolet-tyontekijoista-klikkasi-huijausviestin-linkkia

Google & Harris Poll 2019. Online Security Survey. https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Kelly, T. 2020. How hackers are using COVID-19 to find new phishing victims. Security Magazine. Viitattu 17.4.2021. https://www.securitymagazine.com/articles/92666-how-hackers-are-using-covid-19-to-find-new-phishing-victims

Korolov, M. & Myers, L. 2018. What is the cyber kill chain? Why it's not always the right approach to cyber attacks. Viitattu 17.2.2021. https://www.csoonline.com/article/2134037/strategic-planning-erm-the-practicality-of-the-cyber-kill-chain-approach-to-security.html

LogMeIn 2020. Psychology of Passwords: The Online Behavior That's Putting You At Risk. https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-B2C-Assets-Ebook.pdf

Mandiant 2013. APT1 – Exposing One of China's Cyber Espionage Units. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Meharchandani, D. Staggering Phishing Statistics in 2020. Security Boulevard. Viitattu 12.2.2021. https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/

Metcalf, S. 2015. Microsoft Local Administrator Password Solution (LAPS). Viitattu 27.3.2021. https://adsecurity.org/?p=1790

Microsoft 2015. LAPS and password storage in clear text in AD. Viitattu 23.3.2021. https://docs.microsoft.com/fi-fi/archive/blogs/laps/laps-and-password-storage-in-clear-text-in-ad

Microsoft 2017a. The logical structure of active directory. Viitattu 4.2.2021. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)?redirectedfrom=MSDN/

Microsoft 2017b. Local Administrator Password Solution. Viitattu 8.3.2021. https://docs.microsoft.com/en-us/previous-versions/mt227395(v=msdn.10)?redirectedfrom=MSDN/

Microsoft 2017c. Securing Domain Controllers Against Attack. Viitattu 29.3.2021. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack/

Morgan, S. 2021. Cybercrime Facts And Statistics. 2021 Report: Cyberwarfare In The C-Suite. Cybersecurity Ventures. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

Proofpoint 2019. Human Factor Report. https://derschenner.at/files/dokumente/studien/gtd-pfpt-us-tr-human-factor-2019.pdf

Siddaway, R. 2014. Learn Active Directory Management in a Month of Lunches.

Stacey, M. 2018. Why aren't you using Microsoft's Local Administrator Password Solution (LAPS) yet?. Viitattu 9.3.2021. https://medium.com/@mestacey/why-arent-you-using-microsoft-s-local-administrator-password-solution-laps-yet-66a8a2987a65/

Shelbourne, C. 2017. Securing Privileged Access for the Ad Admin – Part 1. Viitattu 8.2.2021. https://argonsys.com/microsoft-cloud/library/securing-privileged-access-for-the-ad-admin-part-1/

Traficom 2020a. Pidempi parempi – Näin teet hyvän salasanan. Viitattu 23.2.2021 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan/

Traficom 2020b. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Viitattu 27.2.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon?toggle=Huomioitavia%20ominaisuuksia/