



Osaamista  
ja oivallusta  
tulevaisuuden  
tekemiseen

Joonas Vermeulen

# Hallintatunnusten hallinta

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

11.12.2018

Tekijä Otsikko	Joonas Vermeulen Hallintatunnusten hallinta
Sivumäärä Aika	33 sivua 11.12.2018
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tietotekniikka
Ammatillinen pääaine	Ohjelmointi
Ohjaajat	Osaamisaluepäällikkö Janne Salonen Vice President Mika Käck Service Manager Karita Suvanto
<p>Tässä insinööriyössä tutustuttiin hallintatunnusten hallinnoinnin hyviin käytäntöihin ja automaattisiin hallintajärjestelmiin. Lisäksi selvitettiin, mitä hallintatunnuksia identiteetinhallintakonsulttiyrityksellä on viidelle eri asiakkaalleen ja miten niitä tällä hetkellä hallitaan. Kartoituksen perusteella tehtiin suosituksia ja yhteiset parhaat käytännöt. Samalla tutkittiin, onko yrityksen puolesta mahdollista automatisoida hallintatunnusten hallinnointi.</p> <p>Hallintatunnukset ovat suurin yksittäinen tietomurtojen kohde ja suurin osa tietomurroista on toteutettu läpäisemällä hallintatunnus. Hallintatunnuksilla on usein suuret valtuudet sensitiiviseen dataan, joten niiden tietoturvan tulisi olla hyvin korkea. Yritykset eivät kuitenkaan usein tiedä, kuinka paljon hallintatunnuksia niillä on, ja käyttäjillä on tarpeisiinsa nähden liikaa oikeuksia.</p> <p>Hallintatunnusten hallintaan on kehitetty erilaisia automaattisia ratkaisuja, jotka auttavat hallitsemaan tunnuksia ja niiden oikeuksia. Automaattisilla hallintatunnusten hallintajärjestelmillä voidaan mm. seurata, mitä oikeuksia tunnuksilla on, kenellä on tunnuksiin oikeudet, mitä tunnuksilla on tehty ja vaihtaa tunnusten salasanoja automaattisesti.</p> <p>Hallintatunnuskartoituksessa yritykselle selvisi, että useimpien asiakkaiden hallintatunnusten hallinta on ylläpitäjien omien käytäntöjen varassa. Tästä on syntynyt huonoja käytäntöjä, kuten yhteiskäytössä olevia jaettuja tunnuksia, joiden salasanat ovat heikot ja joita ei ole monitoroitu erityisen hyvin. Henkilökohtaisten tunnusten käyttöönotto vaatii kuitenkin asiakkaiden hyväksyntää ja työtunteja, joihin osa asiakkaista ei välttämättä ole valmiita investoimaan. Jaetut hallintatunnukset tulee kuitenkin tallentaa salasanapankkiin ja heikot salasanat vaihtaa vahvempiin.</p> <p>Automaattista hallintajärjestelmää ei ole mahdollista ottaa käyttöön yritykselle. Automaattisia järjestelmiä voidaan kuitenkin suositella asiakkaille ja sitä kautta ottaa käyttöön myös yrityksen hallitsemissa järjestelmissä.</p>	
Avainsanat	Identiteetin hallinta, pääsynhallinta, hallintatunnus, hallintatunnusten hallinta, tietoturva

Author Title	Joonas Vermeulen Privileged Account Management
Number of Pages Date	33 pages 11 December 2018
Degree	Bachelor of Engineering
Degree Programme	Software Engineering
Professional Major	Name of the professional major
Instructors	Janne Salonen, Head of Department Mika Käck, Vice President Karita Suvanto, Service Manager
<p>The purpose of this thesis project was getting to know privileged account management best practices and automated solutions. And analyze what privileged accounts an identity consultant firm has for five of their customers and how they are managed currently. Recommendations and best practices were done based on the privileged account inventory. The purpose was also to investigate would an automated management solution be viable for the firm.</p> <p>Privileged accounts are the single biggest threat in hacking attempts. Most hackings are done by gaining access to a privileged account. Privileged accounts often have elevated access to sensitive data and therefore should be well protected. However, companies often don't know how many privileged accounts they have, and users have too many privileges for their needs.</p> <p>Automatic Privileged Access Management (PAM) solutions provide tools to manage privileged accounts. PAM solutions can for example manage privileged account access rights, users, provide monitoring, and automatic password management.</p> <p>During the privileged account analyze it became clear that many of the privileged accounts of the investigated customers were managed by the administrators themselves. This has caused a number of bad practices, such as shared administrator accounts with weak passwords that are not well monitored. Using personal administrator accounts would require customer approval and some investments which many customers are not willing to do. Shared accounts should nevertheless be saved in a password vault and weak passwords changed.</p> <p>PAM solution for the firm is not recommendable. However, PAM solution can be recommended for customers and that way use PAM in the systems controlled by the firm as well.</p>	
Keywords	Identity management, access management, privileged account, Privileged Access Management, PAM, cyber security

## Sisällys

### Lyhenteet

1	Johdanto	1
2	Hallintatunnus	2
2.1	Hallintatunnuksen määritelmä	2
2.2	Käyttäjätunnusten hallinta ja tietoturva	3
2.3	Hallintatunnusten riskejä	6
2.4	Hallintatunnusten hallinta	8
3	Hallintatunnusten hallinnoinnin, PAM, parhaat käytännöt	9
3.1	Tunnuskartoitus	10
3.2	Hallintatunnusten käyttö ja oikeudet	11
3.3	Hallintatunnusten monitorointi ja valvonta	13
3.4	Tunnusten hakuprosessi	14
3.5	Käytännön esimerkki PAM-järjestelmän toiminnasta	16
4	Hallintatunnuskartoitus yrityksessämme	18
4.1	Asiakas A	19
4.2	Asiakas B	20
4.3	Asiakas C	20
4.4	Asiakas D	21
4.5	Asiakas E	22
5	Suosituksset tunnusten hallintaan	23
5.1	Asiakas A	23
5.2	Asiakas B	24
5.3	Asiakas C	25
5.4	Asiakas D	25
5.5	Asiakas E	26
5.6	Yhteiset käytännöt	26
5.7	Automaattinen hallinnointi	28



## Lyhenteet

AD	Active Directory. Microsoftin Windows-palvelimien tietokanta käyttäjistä, laitteista ja verkon resursseista.
IdM	Identity Management. Identiteetinhallinta. Identiteetin, auktorisoinnin, roolien ja käyttövaltuuksien hallinta.
PAM	Privileged Access Management. Hallintatunnusten hallinnointi.
VPN	Virtual Private Network. Virtuaalinen erillisverkko.

## 1 Johdanto

Tämän insinööriyön tarkoitus on tutustua hallintatunnusten hallintaan ja automaattisiin hallintajärjestelmiin. Hallintatunnus on käyttäjätunnus, jolla on tavallista tunnusta enemmän oikeuksia ja pääsy arkaluontoiseen tietoon, jolla voi aiheuttaa haittaa henkilölle tai organisaatiolle. Lisäksi tarkoitus on tehdä hallintatunnuskartoitus yritykselle, jossa tutustutaan asiakasympäristöjen hallintatunnuksiin ja niiden hallintaan. Tietoturvaystävistä yrityksen tai asiakkaiden nimiä ei ole mainittu.

Hallintatunnuskartoituksen tarkoituksena on selvittää, mitä hallintatunnuksia yrityksellä on viiden eri asiakkaan järjestelmissä, miten niitä tällä hetkellä hallitaan ja onko nykyistä tilannetta tarvetta tai mahdollista kehittää. Tarkoituksena on luoda yhtenäiset parhaat menettelytavat, joita voidaan soveltaa mahdollisuuksien mukaan eri asiakkaisiin. Samalla selvitetään mahdollisuudet automatisoida hallintatunnusten hallinto.

Yritys toimii konsulttina identiteetin- ja pääsynhallinnassa enimmäkseen suurille suomalaisille yrityksille ja työn luonteen takia tietoturva on hyvin tärkeässä asemassa. Identiteetin- ja pääsynhallinta ovat yleiskäsitteitä prosessille, joilla hallitaan tietojärjestelmissä identiteettejä, oikeuksia ja käyttövaltuuksia. Identiteetin- ja pääsynhallintajärjestelmien kautta voi hallita esimerkiksi käyttäjien henkilötietoja, aloitus- ja lopetuspäivämääriä, rooleja ja pääsyjä eri järjestelmiin.

Yrityksellä on pääsy asiakkaiden sensitiiviseen henkilödataan, joten tietoturva on meille tärkeää. Yrityksellä olevat pääsyoikeudet ovat asiakkaille suuri riski, koska työn luonteen takia konsulteilla on laajat oikeudet henkilötietoihin. Yrityksen konsulttien hallintatunnuksilla pääsee käsiksi mm. asiakkaiden henkilökunnan henkilökohtaisiin tietoihin ja identiteetinhallintajärjestelmiin.

Tällä hetkellä hallintatunnusten hallintaan ei ole yrityksessä yhtenäistä prosessia, vaan konsultit ovat itse saaneet luoda ja käyttää niitä osittain asiakkaan ohjeiden mukaan, toisinaan ilman mitään ohjeistusta. Tästä on seurannut eri asiakasympäristöihin erilaisia käytäntöjä ja mahdollisia tietoturvaongelmia. Yhtenäisellä ohjeistuksella on tarkoitus parantaa tietoturvaa, käytettävyyttä ja ammattitasoa asiakkaiden suuntaan.

Tässä työssä käydään läpi hallintatunnusten määritelmä ja hallintaan liittyviä riskejä. Tämän jälkeen selvitetään hallintatunnusten hallinnoinnin parhaat käytännöt ja automaattinen hallinta. Sitten on tarkoitus selvittää, mitä hallintatunnuksia yrityksellä on asiakkaille, miten niitä nyt hallitaan ja antaa suosituksia tunnusten hallintaan. Lopuksi hallintatunnuskartoituksen perusteella selvitetään, onko automaattinen tunnusten hallinnointi mahdollista toteuttaa yritykselle.

## 2 Hallintatunnus

### 2.1 Hallintatunnuksen määritelmä

Hallintatunnusta, engl. privileged account, ei ole yksiselitteisesti määritelty, vaan organisaatio määrittelee itse, minkä tyyppiset tunnukset ovat hallintatunnuksia. Hallintatunnuksia ovat käytännössä tunnukset, joilla on tavallisia tunnuksia suuremmat oikeudet ja pääsy tuloutettavaan tai sensitiiviseen dataan.

Tuloutettava data on mitä tahansa organisaation tietoa, jota voidaan käyttää rahallisen hyödyn saamiseksi. Tyypillisesti tällaista dataa voi olla esimerkiksi sosiaaliturvatunnukset, luottokorttitiedot ja organisaation taloustiedot.

Sensitiivistä dataa voi olla organisaation henkilötiedot tai muu tieto, josta ei välttämättä ole rahallista hyötyä, mutta jolla voidaan aiheuttaa harmia tai haittaa henkilölle tai organisaatiolle. Sensitiivistä dataa voi olla esimerkiksi organisaation sisäinen raportti henkilöstön työkyvyistä tai palkoista.

Organisaatio määrittelee itse, mikä tieto tulisi pitää salassa. Esimerkiksi tuloutettava data ei ole yksiselitteisesti määritelty, vaan se voi vaihdella organisaatiosta toiseen, siitä riippuen, mitä dataa organisaatio käsittelee ja pitää tärkeänä. Yhdelle organisaatiolle tuloutettavaa dataa voi olla asiakastiedot, jolloin tiedon pitää olla salaista, kun taas toiselle se voi olla vain sensitiivistä ja kolmannelle julkista tietoa.

Käytännössä hallintatunnus voi olla esimerkiksi:

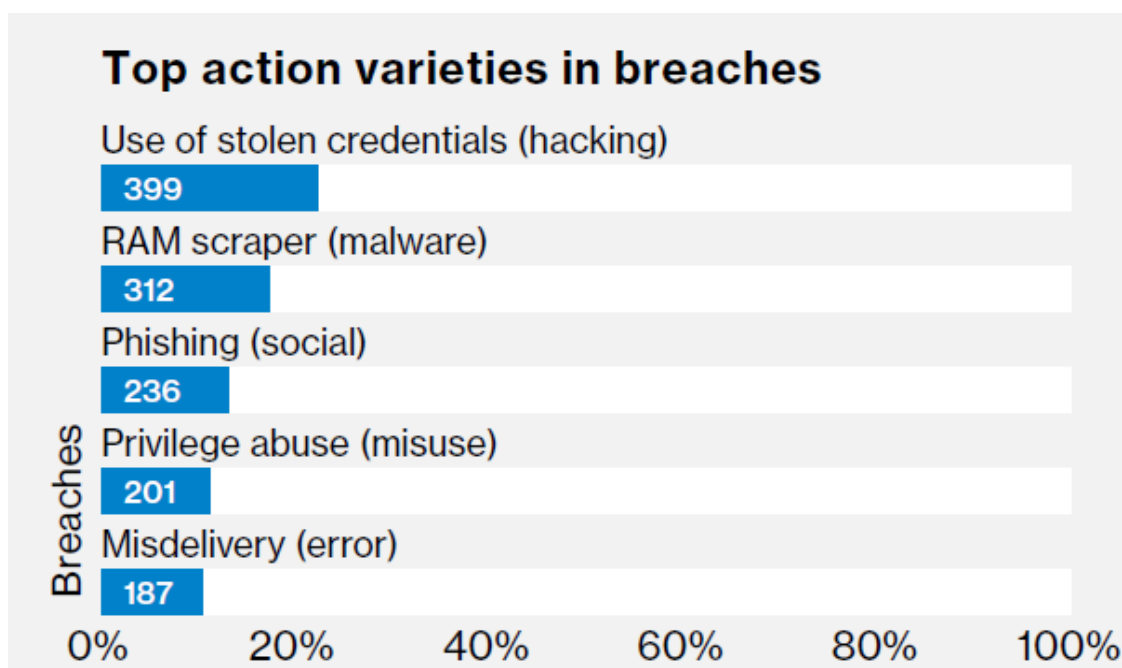


- Paikallinen järjestelmänvalvojan tunnus, jolla on pääsy tiettyyn organisaation paikalliseen järjestelmään, esimerkiksi reitittimeen tai tulostimeen.
- Yleinen järjestelmänvalvojan tunnus, jolla on pääsy organisaation yhteen tai useampaan järjestelmään etänä verkon yli. Käytetään järjestelmän yleiseen hallintaan.
- Palvelun tai palvelimen käyttämä tunnus toisen palvelun tietokantaan, vaikka kukaan ihminen ei käyttäisi tunnusta.
- Tunnus, jolla on pääsy sensitiiviseen dataan, esimerkiksi organisaation henkilöstötietoihin.

Hallintatunnus voi olla henkilökohtainen, jolloin vain yhdellä henkilöllä on pääsy tunnukseen, tai yhteinen jaettu tunnus, jolloin useampi henkilö voi käyttää tunnusta. Tunnusta, jolla ei ole hallintapääsyä, ei luokitella hallintatunnukseksi.

## 2.2 Käyttäjätunnusten hallinta ja tietoturva

Käyttäjätunnukset ovat yleensä keskeisessä roolissa yrityksen joutuessa tietoturvamurron uhriksi. Verizonin 2018 Data Breach Investigations -raportin mukaan viidestä suurimmasta tekijästä tietoturvamurroissa neljä ovat käyttäjäkeskeisiä (kuva 1) [1]. Suurin yksittäinen tietomurtojen tekijä on varastetut tunnukset. Tunnusten suojeleminen pitäisi olla yritysten tärkeimpiä tietoturvakohteita, mutta näin ei usein ole. Monissa yrityksissä hallintatunnuksia on liikaa, niitä ei valvota, identiteettejä ei varmisteta riittävän vahvasti ja liian monilla käyttäjillä on liian suuret oikeudet.

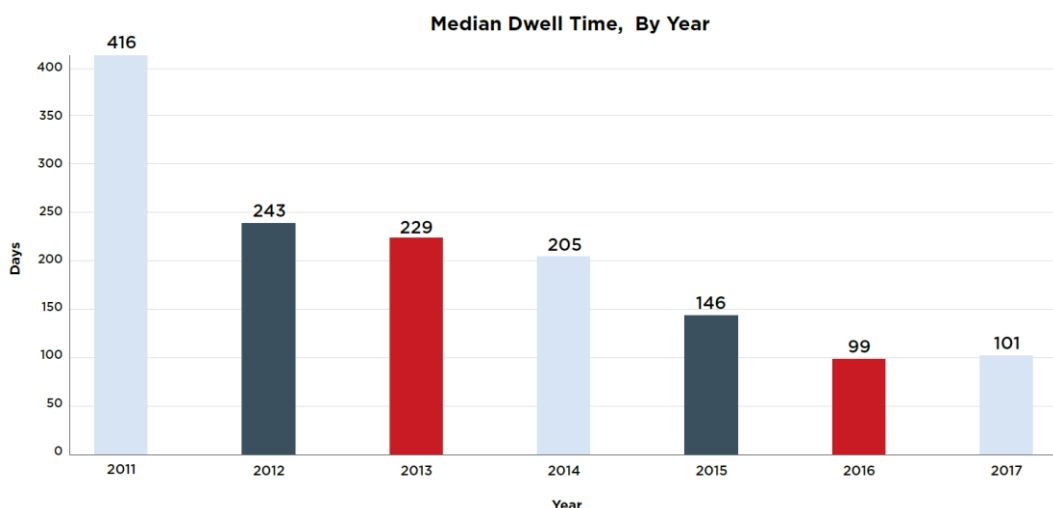


Kuva 1. Verizonin raportin mukaan 2018 tietoturvamurtojen viisi suurinta tekijää [1]. (n=1799)

Forrester-tutkimusyhtiön analyysien mukaan kaikista tietoturvamurroista 80 %:iin liittyy tunnuksen salasanan murtaminen [2]. Osassa tietoturvamurroista hyökkääjät pääsevät sisään alemman tason huonosti suojatulla käyttäjätunnuksella, jonka jälkeen he järjestelmällisesti etsivät yhä korkeamman tason tunnuksia, kunnes saavat haltuunsa riittävillä oikeuksilla olevan hallintatunnuksen.

Hallintatunnusten ollessa ilman valvontaa voi kestää kauan ennen kuin yritys huomaa, että ulkopuolinen taho on päässyt käsiksi niiden järjestelmiin ja dataan. Ilman hyvää valvontaa ei välttämättä voida heti nähdä, mihin kaikkeen hyökkääjät ovat päässeet käsiksi ja mitä muuta vahinkoa järjestelmälle on tehty.

Mandiant M-Trends 2018 -raportin mukaan maailmanlaajuisesti yritykset huomasivat luvattoman pääsyn järjestelmiin vuonna 2017 keskimäärin 101 päivän kuluttua [3]. Edellisenä vuonna luku oli 99 päivää, mutta vielä viisi vuotta sitten tilanne oli huomattavasti huonompi: keskimäärin 243 päivää (kuva 2). Hyökkäyksiä on viimeisten vuosien aikana huomattu enemmän ja niihin on reagoitu nopeammin, mikä johtuu lisääntyneistä tietoturvakäytännöistä. Yhä useampi yritys käyttää erilaisia tietoturvaohjelmia ja hallintavälineitä. Yritykset huomasivat tietoturvamurron useammin itse kuin ulkopuolisen tahon ilmoittamana: 62 % tietomurroista huomattiin sisäisesti.



Kuva 2. Luvattoman pääsyn huomaamiseen kulunut aika per vuosi [3].

Tutkimusten mukaan monet yritykset eivät tiedä, mitkä tunnuksista ovat hallintatunnuksia, kuinka paljon hallintatunnuksia on ja miten laajat oikeudet niillä on. Tunnuksilla voi lisäksi olla tarpeettoman suuria oikeuksia sekä pääsyjä tietoon tai palveluihin, joita tunnuksen käyttäjät eivät tarvitse, käytä tai saisi päästä näkemään. Tietoturvayhtiö CyberArk arvioi, että yrityksillä on kolme kertaa enemmän hallintatunnuksia kuin työntekijöitä [4] ja 30 %:lla käyttäjistä on liikaa oikeuksia [5].

BeyondTrust-tietoturvayhtiön raportin mukaan salasanojen väärinkäyttö on yksi suurin tietoturvariski yrityksissä [6]. 500 haastatellun IT-ammattilaisen mielestä tunnuksiin liittyviä suurimpia riskejä organisaatioissa ovat:

- salasanojen jakaminen työntekijöiden kesken (79 %)
- oletussalasanoja ei vaihdeta (76 %)
- heikon salasanan käyttö (75 %).

Huolimatta siitä, että organisaation IT-henkilöstö on usein tietoinen riskeistä ja huonoista käytännöistä, henkilöstön kouluttamiseen ja tunnusten hallinnoinnin automatisointiin ei usein haluta investoida. Tietoturvajärjestelmien toimiessa oikein loppukäyttäjä ei edes tiedosta niitä, jolloin käytännön hyötyjä voi olla vaikea nähdä lyhyellä aikavälillä.

Yhdellä hallintatunnuksella voi olla useita eri käyttäjiä, jolloin puhutaan jaetuista hallintatunnuksista. Ne ovat usein huonosti ylläpidettyjä ja valvottuja, koska kukaan ei varsinaisesti ole vastuussa tunnuksesta. Tunnus voi tällöin olla hyvin vanha, sen salasanaa ei ole vaihdettu koskaan - edes tunnuksen tietäneen työntekijän lähtiessä organisaatiosta - ja/tai samalla tunnuksella hallitaan useita eri järjestelmiä. Ongelmia muodostuu, kun esimerkiksi salasanaa vaihdettaessa jokaisen tunnusta tarvitsevan pitäisi saada uusi salasana, ja salasanan vaihtaminen aiheuttaa katkoksia palveluihin – on helpompi jättää salasana entiselleen.

Tietoturva ja tietosuoja ovat laissa eri tavalla määritelty. Tietoturva kattaa tietojen saatavuuden, oikeellisuuden ja tiedon suojelemisen ulkopuolisilta. Tietosuoja kattaa ihmisten henkilötietojen keräämisen ja käsittelyn. Tietosuoja on henkilön yksityisyyden suojamista. Tässä työssä tietoturvasta puhuttaessa se kattaa myös tietosuojan.

### 2.3 Hallintatunnusten riskejä

Hallintatunnusten luonteen takia niihin liittyy erilaisia riskejä. Riskit voivat tulla ulkopuolelta. Esimerkiksi tunnuksen joutuessa väärin käsiin hyökkääjä voi ladata tai muokata organisaation sensitiivistä dataa, kiertää olemassa olevat turvatoimet, poistaa tapahtumien lokeja tai levittää haittaohjelmia. Kaikki riskit eivät kuitenkaan ole ulkopuolisia, esimerkiksi mikäli koko järjestelmään on vain yksi jaettu hallintatunnus, jonka salasanan vaihtaa esimerkiksi irtisanottu työntekijä kertomatta siitä kenellekään, voi koko järjestelmän joutua asentamaan uudestaan. Ilman monitorointia ei voida välttämättä edes todistaa, kuka salasanan on vaihtanut.

Ilman tunnusten järjestelmällistä hallintaa organisaatioon voi kertyä turhia hallintatunnuksia, kun vanhoja tunnuksia ei poisteta ja uusia luodaan uusiin tarpeisiin. Lisäksi monilla tunnuksilla saattaa olla tarpeisiin nähden liikaa oikeuksia. Yhteisille hallintatunnuksille kertyy myös usein käyttäjiä, joiden oikeuksia ei poisteta, vaikka henkilö ei enää tarvitse niitä. Nämä kaikki synnyttävät tietoturvariskejä, hankaloittavat järjestelmän ylläpitoa ja aiheuttavat ylimääräisiä kuluja.

Tietoturvamurto ei siis aina tule yrityksen ulkopuolelta, vaan yrityksen omat työntekijät voivat tahallaan tai tahattomasti aiheuttaa vahinkoa hallintatunnuksilla. Työntekijä saattaa tietämättään tehdä yritykselle vahingon, koska hänellä on pääsy tietoon tai palveluun, jota ei tarvitse tai osaa käyttää. Työntekijän päästessä tietoon, johon hänellä ei pitäisi olla oikeutta, voi yritykselle aiheutua vain kiusallisia tilanteita tai suuria taloudellisia vahinkoja. Esimerkiksi työntekijän nähdessä kollegoidensa palkkatietoja voi siitä syntyä harmia työntekijöiden välillä, tai työntekijän käyttäessä saamaansa tietoa haitallisiin tarkoituksiin, voi siitä syntyä suuria rahallisia vahinkoja.

Hallintatunnusten hallinta ja valvonta sekä sisäisiltä että ulkoisilta uhilta on tärkeää yrityksen luotettavuuden, maineen ja taloudellisten syiden takia. Tietomurrot ovat nykyään valitettavan yleisiä ja aiheuttavat suuria haittoja organisaatioille.

Esimerkkejä organisaatioille koituneista haitoista tietomurroissa:

- Sony Pictures Entertainment 2015: tietomurto, joka maksoi yritykselle pelkästään 2015 vuoden aikana \$15 miljoonaa ja arvioiden mukaan lopulliset menetykset voivat olla sata miljoonaa [7].
- Amerikan Office of Personnel Management 2015: tietomurrossa, jossa 21,5 miljoonan henkilön sensitiivistä tietoa varastettiin, mikä aiheuttaa valtion turvallisuuskriisin [8].
- Edward Snowdenin 2013 vuotamat tiedot, jotka paljastivat lukuisia eri maiden hallitusten johtamia vakoiluohjelmia sekä omien kansalaisten että muiden maiden vakoiluun. Mm. amerikkalaiset teleoperaattorit ovat joutuneet antamaan hallitukselle puhelin- ja tekstiviestitietoja [9].
- Englantilainen TalkTalk -operaattorin 2015 tietomurto, jossa hyökkääjät pääsivät käsiksi 150 000 käyttäjän tietoihin. Yhtiön osakearvo putosi kolmanneksen ja 100 000 asiakasta lopetti sopimuksensa [10].
- Canadian Pacific Railwayltä 2015 erimielisyyksien takia lähtenyt työntekijä poisti tärkeitä tiedostoja ja salasanoja verkkojärjestelmästä aiheuttaen katkoksia ja vahinkoa yhtiön toimintaan. Entinen työntekijä tuomittiin 366 päiväksi vankilaan hyökkäyksestä [11].

Käyttäjätunnuksiin liittyviä tietoturvariskejä voidaan vähentää varmistamalla, että yhdelläkään yksittäisellä henkilöllä ei ole liikaa valtuuksia tai oikeuksia. Tehtävien eriyttämisellä (engl. Separation of Duties) varmistetaan, että yksittäisellä henkilöllä ei ole mahdollisuutta tehdä suurta vahinkoa organisaatiolle. Esimerkiksi alkuperäinen kehittäjä ei

voi tehdä suurta järjestelmämuutosta ennen hyväksyntää toiselta taholta. Erityisen sensitiiviseen dataan pääsy voidaan toteuttaa jakamalla vastuu useamman henkilön välille niin, että yksittäinen henkilö ei pääse dataan käsiksi yksin.

## 2.4 Hallintatunnusten hallinta

Hallintatunnusten hallinta vastaa osittain tietoturvan lisäämisen tarpeeseen verkottuneessa dataympäristössämme. Hallintatunnusten hallinnalla ja johtamisella pyritään määrittelemään, millä hallintatunnuksilla on mitään oikeuksia, kenellä on näihin tunnuksiin oikeudet, minkä takia ja kuka on oikeudet myöntänyt. Hallintatunnusten hallintaan kuuluu tunnusten elinkaaren ja käytön valvonta: miten ja miksi tunnuksia luodaan, mihin ja milloin tunnusta käytetään, kuka tunnusta käyttää ja kuka on hyväksynyt tunnuksen käytön ja miksi. Jäljitettävyyden kannalta hallintatunnusten hallinnointiin kuuluu valvonta ja monitorointi. On tärkeää tietää tunnuksen käyttäjän lisäksi myös, mitä tunnuksella on tehty ja milloin.

Hallintatunnusten hallinnan tarkoitus on minimoida riskejä. Kaikkien työntekijöiden jatkuva valvonta ei ole mahdollista, kustannustehokasta tai järkevää. Tämä ei kuitenkaan tarkoita, että mitään käyttäjien toimintaa ei tarvitse tai kannata valvoa. Parhaat tulokset saadaan kohdistamalla valvonta riskialttiisiin kohteisiin. Näin voidaan vähimmällä vaivalla kattaa suurin osa riskeistä.

Tunnusten hallinta voidaan toteuttaa monella tavalla, yksinkertaisimmillaan paperilla tai Excelillä. Nämä menetelmät kuitenkin luottavat käyttäjän omaan luotettavuuteen ja viiteliäisyyteen. Nykyään hallintaan on kehitetty prosesseja ja työkaluja, joilla on seuraavia ominaisuuksia:

- Tunnistavat hallintatunnukset automaattisesti.
- Ottavat haltuun uudet hallintatunnukset, esimerkiksi vaihtamalla salasanan tai lukitsemalla tunnuksen ennen kuin se on hyväksytty käyttöön.
- Estävät tunnuksen luvattoman käytön.
- Estävät tunnuksen käytön ilman valvontaa.
- Varmistavat kuka on vastuussa tehdyistä muutoksista.
- Hallitsevat tunnusten salasanoja.

- Poistavat tarpeen kovakoodatuille tunnuksille ja salasanoille
- Monitoroivat hallintatunnuksia automaattisesti esimerkiksi keräämällä lokeja tunnuksella tehdyistä muutoksista ja nauhoittamalla sessiot.
- Hallitsevat kohdejärjestelmien lokeja.
- Ilmoittavat riskialttiista tai oudosta käytöstä automaattisesti.

Privileged Access Management (PAM) on yleisnimitys prosesseille ja työkaluille, joilla hallitaan hallintatunnuksia. PAM-työkaluilla voi varmistaa käyttäjän identiteetin, hallita tunnusten salasanoja ja valvoa tunnusten käyttöä. PAM on tunnuksen käyttäjän ja kohdejärjestelmän välissä varmistamassa, että vain luotettu taho pääsee käyttämään kohdejärjestelmää.

Seuraavassa luvussa analysoidaan PAM-prosessien ja -työkalujen parhaita käytäntöjä.

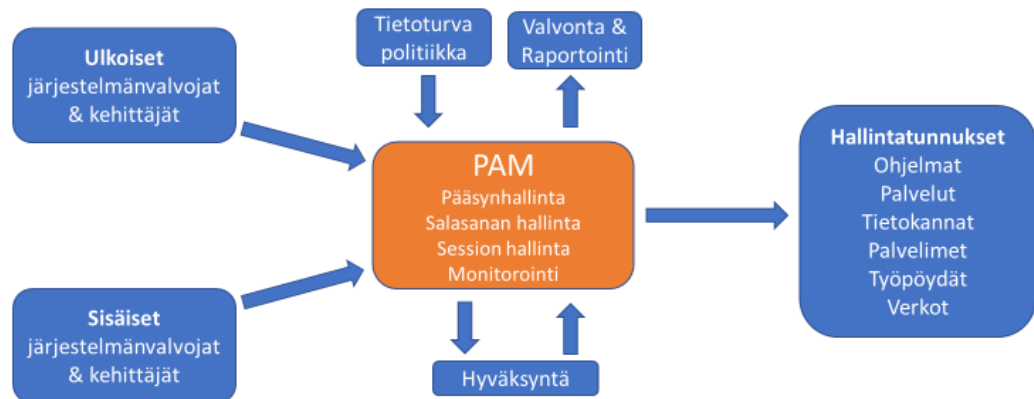
### 3 Hallintatunnusten hallinnoinnin, PAM, parhaat käytännöt

Perinteisesti hallintatunnusten ongelmana on, että samalla tunnuksella voi sekä hallita järjestelmää että peittää käytön jäljet. Käyttäjän saatua oikeudet tietoon ja järjestelmiin on vain luotettu, että hän ei tee mitään pahaa oikeuksilla. Hallintatunnuksia voi yrittää hallita rajoittamalla käyttöoikeuksia ja valvoa keskittämällä lokien hallintaa, mutta nämä toiminnot voi usein edelleen kiertää helposti.

Hallintatunnusten hallinnoinnin paras tapa on automatisoida koko hallinnointi käyttämällä PAM-järjestelmää. PAM-järjestelmä toimii hallitsemalla hallintatunnusten järjestelmiin pääsyä estämällä kaiken muun pääsyn paitsi PAM:n hyväksymän käytön. PAM estää hallintatunnuksen luvattoman käytön ja uusien tunnusten luomisen, joita ei tehdä PAM-järjestelmän kautta. Lisäksi PAM:n kautta voi monitoroida kaikkia hallintatunnuksia.

PAM-järjestelmä toimii käyttäjän ja loppujärjestelmän välissä (kuva 3). PAM varmistaa käyttäjän identiteetin ja antaa tarvittavat oikeudet kohdejärjestelmään hyväksymisprosessin jälkeen. Koko tapahtuma on monitoroitu ja tallennettu.

## Privileged Access Management



Kuva 3. PAM:n toimintatapa.

Usein tietoturvaratkaisujen käytön ongelmana on käytettävyyden heikkeneminen. Käyttäjät kokevat esimerkiksi virustorjuntaohjelmat hankaliksi ja ärsyttäviksi. Organisaatiot vuorostaan näkevät tietoturvaratkaisut kalliina ja tuottavuutta heikentävinä. PAM-järjestelmä oikein toteutettuna kuitenkin parantaa käytettävyyttä ja lisää käyttäjätyytyväisyyttä. PAM-järjestelmästä voi esimerkiksi avata kohdejärjestelmän hallintapaneelin suoraan ja hoitaa sisäänkirjautumisen ilman, että käyttäjän tarvitsee välittää salasanaa. Näin PAM-järjestelmä minimoi riskejä ja säästää rahaa.

### 3.1 Tunnuskartoitus

Ensimmäinen askel kohti hallintatunnusten hallinnointia on selvittää ja löytää kaikki organisaation tunnukset, joilla on hallintaoikeuksia. Uusia hallintatunnuksia tulee etsiä säännöllisesti järjestelmistä. Tunnukset tulee kerätä turvalliseen paikkaan, esimerkiksi salasatatyökaluun. Tunnuksia ja varsinkin salasanoja ei saa säilyttää tekstimuodossa missään.



Useimmat PAM-järjestelmät tarjoavat automaattisen hallintatunnusten haun ja jatkuvan uusien tunnusten skannauksen. Uuden tunnuksen löydyttyä PAM ottaa sen haltuun, esimerkiksi vaihtamalla salasanan niin, että sitä ei voi käyttää kuin PAM:n kautta. Näin järjestelmään ei voi luoda hyväksymättömiä tunnuksia valvonnan kiertämiseksi.

Hallintatunnusten löydyttyä niille tulee asettaa omistaja. Tunnuksella tulee aina olla omistaja. Omistajan ei tule olla henkilö, vaan tulee käyttää *roolia*, joka määritellään yhdelle tai useammalle henkilölle. Näin pyritään vähentämään riskiä, että tunnus jää ilman omistajaa. Rooli voidaan myös väliaikaisesti määritellä toiselle henkilölle, esimerkiksi lomien ajaksi. Omistajuuden asettaminen tunnukselle on tärkeää, jotta voidaan selvittää, kenen vastuulla tunnuksella tehdyt muutokset ovat.

Hallintatunnuskartoituksessa tulee selvittää, mitä oikeuksia hallintatunnuksilla on missäkin järjestelmissä, mitkä tunnuksista ovat oikeasti tarpeellisia ja onko tunnuksilla oikeat oikeudet. Hallintatunnuksilla tulee olla oikeudet ainoastaan siihen, mihin tunnusta on tarkoitus käyttää. Eri käyttötarkoituksiin on hyvä tehdä eri tunnus ja näin rajoittaa yhden tunnuksen oikeuksia järjestelmään. Tunnusten määrää tulisi kuitenkin rajoittaa pienempään mahdolliseen. Näin mahdollisia hyökkäys- ja hallintakohteita on vähiten.

### 3.2 Hallintatunnusten käyttö ja oikeudet

Hallintatunnukset tulee erotella tavallisista tunnuksista. Tavallisilla tunnuksilla tulee tehdä normaalit päivittäiset asiat, eikä niillä saa olla oikeuksia hallinnointiin tai sensitiiviin tietoon. Tämä käytäntö pyrkii vähentämään käyttäjän virheitä ja vahinkoja rajoittamalla tavallisten tunnusten oikeuksia. Hallintatunnuksella on tarkoitus ainoastaan hallita sitä järjestelmää tai tietoa, mihin se on tarkoitettu. Hallintatunnuksia voidaan valvoa tiukemmin, kun taas käyttäjien henkilökohtaisia tunnuksia voidaan seurata vähemmän tarkasti yksityisyyden säilyttämiseksi.

Organisaation tietokoneet voidaan tarvittaessa myös jakaa tavallisiin ja hallintatietokoneisiin. Tavallisilla koneilla tulee hoitaa normaalit päivittäiset asiat ja erillisillä koneilla ainoastaan käyttää hallintatunnuksia. Näin pyritään vähentämään haittaohjelmien aiheuttamia riskejä. Esimerkiksi organisaation laskuja voidaan maksaa ainoastaan sille tarkoitettulta koneelta, jota ei käytetä mihinkään muuhun tarkoitukseen.

Hallintatunnuksella tulee olla vain juuri sen verran oikeuksia, kuin tunnuksella tarkoitetun tehtävän tekemiseen tarvitaan. Yhdelle hallintatunnukselle ei tarvitse antaa kaikkia valtuuksia, vaan oikeudet voi jakaa tunnusten ja henkilöiden välillä. Erittäin sensitiiviseen tietoon voidaan vaatia useamman henkilön hyväksyntä ja näin varmistaa, että yhden tunnuksen murtaminen ei vaaranna kaikkein tärkeintä tietoa.

Järjestelmien omia sisäänrakennettuja hallintatunnuksia ei tulisi käyttää lainkaan. Nämä tunnukset ovat järjestelmän oletustunnuksia järjestelmän asennusta varten. Järjestelmän asennuksen jälkeen näiden tunnusten salasanat tulee vaihtaa hyvin vahvoihin tai tunnukset poistaa käytöstä kokonaan, mikäli mahdollista. Sisäänrakennetut tunnukset ovat yleinen tietoturvamurtojen kohde, koska tunnuksen nimi on yleisessä tiedossa.

PAM-järjestelmän ollessa käytössä henkilökohtaiset, nimetyt hallintatunnukset tulee poistaa ja käyttää ainoastaan PAM:n hallitsemissa hallintatunnuksia. Näin hallintatunnusten määrää voidaan vähentää huomattavasti. Tunnuksille kirjautuminen tapahtuu aina PAM:n kautta niin, että yhteisten hallintatunnusten salasanojen ei tule olla kenenkään tiedossa. PAM:lla valvotaan tunnuksen käyttöä, seurataan, kuka tunnusta käyttää ja kuka on myöntänyt käyttöoikeuden.

Yhteisiä hallintatunnuksia tulisi kuitenkin välttää niin kauan kuin PAM-järjestelmää ei ole käytössä. Ilman PAM:n tarjoamaa valvontaa ei voida tietää kuka yhteistä tunnusta on käyttänyt ja mitä tunnuksella on tehty. Yksittäinen käyttäjä voi muuttaa yhteisen tunnuksen salasanan, mikä on mahdollinen riski. Henkilökohtaiset hallintatunnukset ovat tässä tapauksessa turvallisempi vaihtoehto, koska tunnuksesta näkee suoraan käyttäjän ja sille voidaan myöntää vain tarvittavat oikeudet.

PAM-järjestelmä huolehtii automaattisesti hallintatunnusten salasanoista ja identiteetin varmistamisesta. PAM-järjestelmä voi esimerkiksi avata ja sulkea tunnuksen tarpeen mukaan tai luoda jokaista käyttökertaa varten uuden salasanan. Näin edes salasanan joutuminen väärin käsiin ei vaaranna järjestelmää, koska se on jo vaihtunut. PAM myös estää salasanan vaihtamisen käyttäjän toimesta. Näin esimerkiksi työntekijä ei voi tehdä vahinkoa salasanoja vaihtamalla.

PAM-järjestelmään kirjauduttaessa autentikointimenetelmän tulee olla erityisen vahva ja salasana vaihtaa säännöllisesti. Käytössä tulee olla kaksivaiheinen tunnistautuminen.

Kaksivaiheisessa tunnistautumisessa varmistetaan käyttäjän identiteetti kahdella eri tavalla: esimerkiksi salasanalla ja älypuhelimeen lähetettävällä koodilla. Näin varmistetaan, että edes salasanan joutuminen väärin käsiin ei vielä vaaranna koko järjestelmää. Toisen tunnistautumistavan estäminen estää koko järjestelmään pääsyn ja näin estää järjestelmän käytön.

Ilman PAM-järjestelmää kaksivaiheista tunnistautumista tulisi käyttää suoraan hallintatunnuksissa, mikäli mahdollista. Tällä voidaan varmistaa, että salasanan murtaminen ei vielä vaaranna tunnusta. Kaksivaiheinen tunnistautuminen helpottaa myös tilanteissa, joissa salasanaa ei voida vaihtaa, mutta tunnukseen pitää estää pääsy esimerkiksi työntekijän lähtiessä organisaatiosta.

### 3.3 Hallintatunnusten monitorointi ja valvonta

Hallintatunnusten hallinnointiin kuuluu tietää, mitä tunnuksella on tehty. PAM-järjestelmät kykenevät monitoroimaan tunnuksen käyttöä usealla eri tavalla. Valvonta voi olla epäsuoraa järjestelmien lokien keruuta ja niiden valvontaa tai suoraan session nauhoittamista. Näin voidaan varmistaa, mitä tunnuksella on tehty ja mihin aikaan.

Ilman PAM:ia useampaa järjestelmää hallittaessa voi tulla ongelmaksi lokien hajaus ja säilytys. PAM-järjestelmään kuuluu myös kohdejärjestelmien omien lokien keskitetty säilytys ja hallinta. Lokien keruu yhteen järjestelmään helpottaa hallintaa ja parantaa tietoturvaa. Lokeja ei myöskään voi poistaa tai muokata samalla hallintatunnuksella kuin järjestelmää hallitaan, mikä estää tunnusten väärinkäytön peittelemisen.

Lokitietoja ei tule vain kerätä pahan päivän varalle, vaan säännöllinen sessioiden ja lokitietojen katsaus on hyödyllistä. Näin voidaan kitkeä pois huonoja käytäntöjä ja oppia hyviä tapoja siitä, miten tunnuksia käytännössä käytetään. Tallennettuja sessioita voidaan käyttää myös opetustarkoituksiin uusille ylläpitäjille.

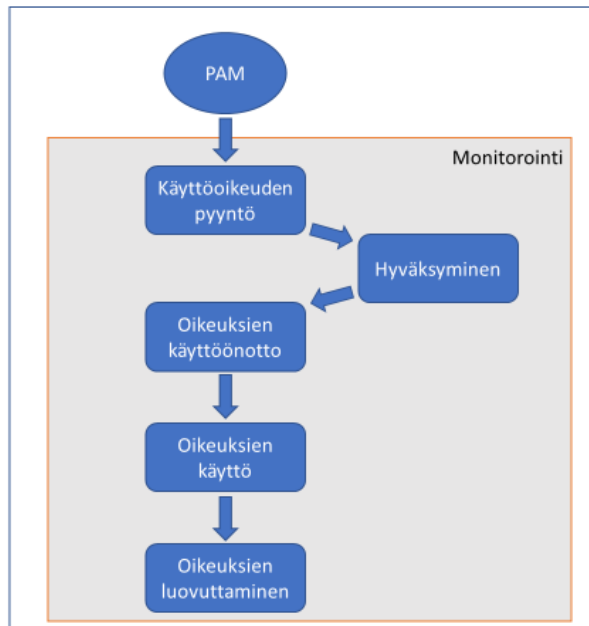
PAM-järjestelmät tukevat tunnuksen suoraa monitorointia kuvankaappauksilla tai jopa suoraan jatkuvaa videokuvaa, riippuen miten järjestelmä on toteutettu. Näin voidaan tunnuksen käyttöä valvoa jopa reaaliajassa ja tarvittaessa estää tunnuksen käyttö heti epäilyttävää käytöstä ilmetessä.

PAM-järjestelmiin on viime aikoina kehitetty koneoppimista, jolla voidaan arvioida riskejä ja seurata käyttäjää tarkemmin, jos hän tekee jotain tavoistaan poikkeavaa tai jos tunnuksella yritetään päästä dataan, johon sillä ei ole oikeuksia. Jos järjestelmä huomaa, että käyttäjä tekee jotain tavoistaan poikkeavaa, voidaan siitä hälyttää, tiukentaa valvontaa, esimerkiksi nauhoittamalla koko sessio, tai jopa katkaisemalla yhteys kokonaan, kunnes tilanne on varmistettu. Näin ihmisten ei tarvitse valvoa kaikkea, vaan ainoastaan tarkistaa mahdolliset riskialttiit kohteet.

### 3.4 Tunnusten hakuprosessi

Hallintatunnuksia ei saa jakaa vapaasti kaikille, jotka saattavat joskus niitä tarvita. Hallintatunnuksen käyttöoikeus tulee jakaa vain sitä tarvitseville. Tunnusten saantiin tarvitaan prosessi, josta ilmenee mihin hallittavaan järjestelmään tai tietoon tarvitsee pääsyä, mitä varten ja kuinka pitkäksi aikaa. Näin voidaan varmistaa, että oikeat henkilöt saavat tarvittavat oikeudet tarvitsemaansa aikaan ja että oikeudet poistuvat, kun niitä ei enää tarvita.

PAM-järjestelmissä käyttöoikeuksia voidaan hakea joka kerta erikseen. Tämän ei kuitenkaan tarvitse olla pitkä ja hankala prosessi, vaan automatisoitu ja nopea. Prosessin tarkoitus on varmistaa, että jokaisesta tapahtumasta on selkeä jälki ja jokaiselle käyttötapaaukselle on selkeä syy. Seuraavana on esitetty esimerkki PAM-järjestelmän oikeuksien hakuprosessista (kuva 4).



Kuva 4. Oikeuksien hakuprosessi.

1. Käyttöoikeuden pyyntö. Riippuen tunnuksen oikeuksista ja organisaation tarpeista, oikeuksia pyydetessä voidaan vaatia selitys oikeuksien käyttöön tietyn ajan välein tai joka käyttökerralla. Tukipyyntöä ratkaistaessa PAM-järjestelmä voi esimerkiksi vaatia tukipyynnön tunnusnumeron ja verrata sitä tukipalvelun järjestelmään, jotta tunnusta voi käyttää.
2. Hyväksyminen. Hyväksyntä voi olla usein käytetyille hallintatunnuksille automaattinen hyväksytyllä syyllä ja kaikkein tärkeimmille tunnuksille vaatia henkilön hyväksynnän.
3. Oikeuksien käyttöönotto. Riippuen järjestelmästä ja tunnuksen oikeuksista, tunnus voidaan ottaa käyttöön usealla eri tavalla: tunnus voidaan aktivoida automaattisesti tai manuaalisesti, PAM-järjestelmä voi generoida uuden salasanan tai salasanan saanti voi vaatia kahden ihmisen valvontaa.
4. Oikeuksien käyttö. Oikeudet saanut henkilö käyttää hallintatunnusta session ajan.

5. Oikeuksien luovuttaminen. Hallintatunnukselta tulee kirjautua ulos välittömästi, kun tunnusta ei enää tarvita session aikana. Session jälkeen PAM muuttaa tunnuksen salasanan tai ottaa tunnuksen kokonaan pois käytöstä.
6. Monitorointi. Koko prosessi on valvottu ja tallennettu.

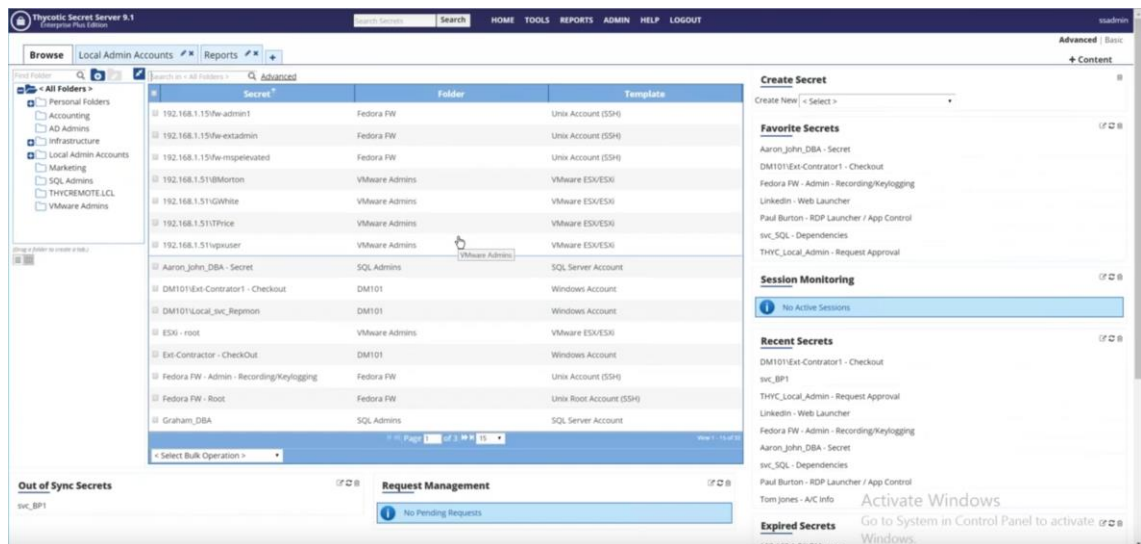
### 3.5 Käytännön esimerkki PAM-järjestelmän toiminnasta

Tässä luvussa käydään läpi esimerkin kautta, millä tavalla PAM auttaa hallintatunnusten hallinnoinnissa käytännössä verrattuna manuaaliseen prosessiin. Esimerkki perustuu todellisiin tapauksiin, mutta tietoturvasyistä organisaatiota tai henkilöitä ei voida nimetä [12].

Organisaatiossa pitkään työskennellyt IT-ylläpitäjä lähti tyytymättömänä organisaatiosta uhaten kostotoimenpiteillä. Hänelle oli vuosien saatossa kertynyt useita hallintatunnusten salasanoja. Organisaation IT-osasto ei edes tiennyt, mihin kaikkiin tunnuksiin henkilöllä oli ollut pääsy tai mitä salasanoja hän oli saattanut nähdä. Organisaatio käyttää jaettuja hallintatunnuksia, joista osan salasanoja ei ole vaihdettu koskaan.

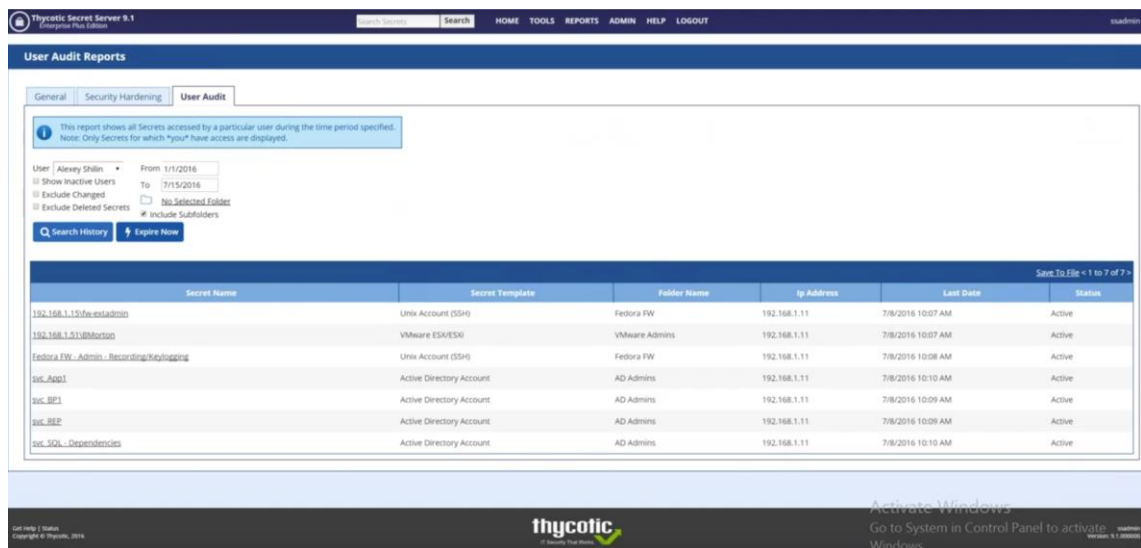
Organisaation IT-osastoa pyydettiin manuaalisesti etsimään kaikki mahdolliset hallintatunnukset, joihin henkilöllä oli saattanut olla pääsy ja vaihtamaan näiden salasanat. Tämä aiheutti suuria ongelmia järjestelmissä: järjestelmät kaatuivat ja yhteydet katkesivat. Neljän hengen tiimi joutui työskentelemään 10 päivää vuoroissa löytääkseen manuaalisesti kaikki hallintatunnusten yhteydet ja päivittääkseen kaikkiin järjestelmiin uudet salasanat. Lähtenyt työntekijä ei koskaan toteuttanut uhkauksiaan hyökätä organisaatiota vastaan, mutta hänen uhkailustaan aiheutui suurta haittaa.

Kaikki tämä oltaisiin voitu välttää käyttämällä PAM-järjestelmää. PAM-järjestelmät tunnistavat hallintatunnukset automaattisesti ja tallentavat tunnuksen turvallisesti holviin. Yksi johtavista ja käytetyimmistä PAM-järjestelmätuottajista on Thycotic. Thycotic kutsuu salasanaholviaan Thycotic Secret Serveriksi (kuva 5). Järjestelmä tunnistaa, missä kaikkialla tunnus on käytössä ja osaa samanaikaisesti vaihtaa salasanan kaikkialla.



Kuva 5. Thycotic Secret Serveriin tallennetaan järjestelmien hallintatunnukset.

Secret Serverissä voi helposti nähdä, mitä hallintatunnuksia käyttäjä on koskaan käyttänyt ja yhdellä painikkeella vaihtaa kaikki salasanat automaattisesti kaikkiin järjestelmiin (kuva 6). Näin voidaan olla varmoja, että kaikki tunnukset, joita käyttäjä koskaan käytti, ovat turvallisia ja kaikkien palvelujen yhteydet toimivat edelleen salasanan vaihdoin jälkeenkin.



Kuva 6. Käyttäjän käyttämien tunnusten historia.

## 4 Hallintatunnuskartoitus yrityksessämme

Tässä kappaleessa kartoitetaan yrityksemme viiden eri asiakkaan hallintatunnuksia. Tietoturvasyistä yritystämme tai asiakkaita ei ole nimetty. Tarkoitus on selvittää, millaisia hallintatunnuksia yrityksellämme on näille asiakkaille mihinkin järjestelmiin ja miten niitä tällä hetkellä hallitaan.

Yrityksemme tarjoaa identiteetinhallintaratkaisuja (Identity Management, IdM). IdM-järjestelmällä automatisoidaan käyttäjätunnusten ja pääsyn hallinta. Identiteetinhallinta on muun muassa käyttäjien elinkaaren hallintaa. Esimerkiksi uuden käyttäjän tunnusten luonti ja lähtevän käyttäjän tunnusten sulkeminen tehdään automaattisesti IdM-järjestelmässä aloitus- ja lopetuspäivämäärän mukaan.

IdM-ratkaisuja on erilaisia, mutta kaikki tämän kartoituksen järjestelmät toimivat samoilla periaatteilla: Linux- tai Windows-palvelimelle asennettu IdM-järjestelmä. Yrityksemme ylläpitää IdM-järjestelmää ja asiakas vastaa palvelimien ylläpidosta, mutta konsulteilamme on usein tunnuksia myös suoraan palvelimille IdM-järjestelmän ylläpitoa varten. Kaikilla asiakkailla on myös käytössä Microsoft Active Directory -järjestelmä (AD), jota yrityksemme ei ylläpidä, mutta hallintatunnukset usein löytyvät. Osalle asiakkaista yrityksemme on alun perin asentanut IdM-järjestelmän ja osalla on valmiiksi muun tahon asentama järjestelmä, jota yrityksemme hallinnoi.

Asiakkaiden järjestelmiin ei ole pääsyä suoraan ulkoverkosta, vaan saadaksemme yhteyden tarvitaan virtuaalinen erillisverkko (Virtual Private Network, VPN) -yhteys, joka luo yhteyden ulkoverkosta asiakkaan sisäverkkoon. Tämä estää ulkopuolisia pääsemästä asiakkaiden järjestelmiin ulkoverkosta, vaikka he pääsisivät käsiksi järjestelmän tunnuksiin jollain tavalla. VPN-tunnukset ovat aina henkilökohtaiset, mutta eivät varsinaisesti ole hallintatunnuksia. Useimmat asiakkaat käyttävät kaksivaiheista tunnistautumista VPN-yhteyksissä. Tutkituista viidestä asiakkaasta kaikki käyttävät VPN-ratkaisua, mutta osalla muista asiakkaista on muitakin ratkaisuja, esimerkiksi etäyhteysohjelma tai erilliset tietokoneet.

Kukin IdM-järjestelmä pystyy keräämään lokitietoja kirjautumisista ja tehdyistä muutoksista. Palvelimet osaavat myös kerätä omia lokejaan. Eri asiakkailla lokien hallinta on



toteutettu eri tavalla. IdM-lokitiedot ovat asiakkaiden hallitsemilla palvelimilla ja niitä hallitaan samoilla hallintatunnuksilla kuin IdM-järjestelmääkin.

Seuraavissa luvussa on käyty tapauskohtaisesti läpi kunkin asiakkaan hallintatunnukset.

#### 4.1 Asiakas A

Yrityksellämme on hallintatunnuksia asiakas A:lle kolmeen eri IdM-ympäristöön: kehitys, testaus ja tuotanto, joissa kussakin on useita eri Linux-palvelimia. Myös Linux-palvelimille on hallintatunnuksia IdM-järjestelmien ylläpitoa varten. Lisäksi asiakkaan AD-järjestelmään on hallintatunnus. Asiakas A vastaa itse palvelimien ylläpidosta ja määrittelee millaiset oikeudet yrityksellämme on järjestelmiin. Asiakas A:lla on myös omat tunnukset kaikkiin järjestelmiin.

Asiakas A:lla on yleisesti tietoturvaso hyvin korkea ja myös hallintatunnukset on otettu huomioon hyvin. Tuotanto- ja testausympäristöissä on käytössä sekä henkilökohtaiset tunnukset että henkilökohtaiset hallintatunnukset. Jaettuja tunnuksia käytetään IdM-järjestelmässä ainoastaan kehitysympäristössä, josta ei ole pääsyä muihin järjestelmiin. Linux-palvelimille on käytössä henkilökohtaiset hallintatunnukset, joilla on järjestelmänvalvojan oikeudet. AD-järjestelmässä on joillain ylläpitäjillä henkilökohtainen paikallinen tunnus, ja osa käyttää yhteistä järjestelmänvalvojan tunnusta.

Asiakas A:lla on palvelimillaan kattava keskitetty lokien hallinta, joka tallentaa kaiken, mitä eri tunnuksilla tehdään. Lokit on hallittu hyvin ja niitä säilytetään pitkään. IdM-järjestelmän lokeihin pääsee kuitenkin käsiksi samoilla hallintatunnuksilla. Tämä on tarpeen järjestelmän ylläpitoa varten, koska lokeja käytetään usein ongelmatilanteiden ratkomiin.

Tunnuksia haetaan automatisoidun prosessin kautta itse. Esimiehen tulee hyväksyä tunnukset, jonka jälkeen tunnuksen saa sähköpostiin ja salasana lähetetään tekstiviestillä. Salasana pyydetään vaihtamaan ensimmäisellä kirjautumiskerralla ja säännöllisesti tämän jälkeen. Ainoastaan testiympäristön jaettut tunnukset ja AD-tunnus jaetaan sisäisesti tarvittaessa.

## 4.2 Asiakas B

Yrityksellämme on hallintatunnuksia asiakas B:lle kahteen eri IdM-järjestelmään: testaus ja tuotanto. Hallintatunnuksia on myös IdM-järjestelmän Windows- ja Linux-palvelimille sekä AD-järjestelmään. Asiakas vastaa palvelimista ja yrityksemme IdM:n ylläpidosta.

Asiakas B:n kaikki hallintatunnukset ovat jaettuja hallintatunnuksia. Konsulteillamme on asiakas B:lle henkilökohtaiset tunnukset, mutta niillä ei ole mitään oikeuksia järjestelmissä ja ne ovat hyvin vähän käytettyjä. Linux-palvelimella on käytössä järjestelmän oletushallintatunnus. Ainoastaan IdM-käyttöliittymän puolella henkilökohtaiset tunnukset ovat jonkin verran käytössä konsulttien omien mieltymysten mukaan, mutta oikeuksien antaminen henkilökohtaiselle tunnukselle tapahtuu edelleen yhteisellä hallintatunnuksella itse.

Jaettujen hallintatunnusten salasanat ovat kauttaaltaan varsin heikkoja. Osin tämä johtuu asiakkaan omista tavoista tunnuksia yrityksellemme tehdessään ja osin peruja järjestelmän alkuperäiseltä asentajalta. Salasanoja ei kuitenkaan ole koskaan pyydetty vaihtamaan, eikä niille ole asiakkaan puolelta minkäänlaisia vaatimuksia vahvuudesta tai vanhenemisesta.

Eri järjestelmät keräävät omia lokeja omien asetusten mukaan. IdM-järjestelmien lokeissa on asetettu kokorajoitus, jonka ylittyessä järjestelmä poistaa vanhan lokin. Joissain tapauksissa tämä tapahtuu hyvinkin nopeasti. Lokeja ei kerätä keskitetysti minnekään vaan lokin poistuessa se poistuu kokonaan.

Henkilökohtaiset tunnukset haetaan asiakkaalta suoraan sähköpostilla esimiesten hyväksynnällä ja jaetut hallintatunnukset jaetaan yrityksemme sisällä niitä tarvitseville. VPN-tunnuksissa ei ole käytössä kaksivaiheista tunnistautumista.

## 4.3 Asiakas C

Yrityksellämme on hallintatunnuksia asiakas C:lle kolmeen IdM-järjestelmään: kehitys, testaus ja tuotanto sekä niiden Linux-palvelimiin. Lisäksi hallintatunnuksia on AD-järjes-

telmään. Asiakas C on muihin asiakkaisiin verrattuna erilainen tapaus, koska yrityksemme on vastuussa identiteetinhallintajärjestelmän ylläpidosta ja hallinnasta ilman, että asiakkaalla on hallintapääsyä koko järjestelmään.

IdM-järjestelmiin on henkilökohtaiset tilit, mutta niillä ei suurimmaksi osin ole riittäviä oikeuksia. Suurin osa ylläpitäjistä käyttää jaettuja hallintatunnuksia. Osa ylläpitäjistä on asettanut henkilökohtaisille tileilleen joitain oikeuksia, jotta heidän ei tarvitse aina käyttää jaettuja hallintatunnuksia. Käytäntötavat riippuvat kuitenkin ylläpitäjästä, eikä tunnuksia ole jaettu erikseen tavalliseen henkilökohtaiseen tunnukseen ja henkilökohtaiseen hallintatunnukseen. Henkilökohtaisilla tunnuksilla on hallintaoikeuksia AD-järjestelmään ja Linux- ja Windows-palvelimille.

Järjestelmässä on salasanasäännöt henkilökohtaisia tilejä varten, mutta jaetut hallintatunnukset on tehty ennen sääntöjen toteutusta, jolloin niiden salasanat ovat heikot eikä niitä ole vaihdettu pitkään aikaan. Henkilökohtaiset hallintatunnukset ovat kuitenkin tämän salasanapolitiikan piirissä.

Eri järjestelmät keräävät omia lokeja omien asetusten mukaan. Lokeja ei kerätä keskitysti minnekään, vaan lokin poistuessa se katoaa kokonaan. IdM-järjestelmien lokeissa on asetettu kokorajoitus, jonka ylittyessä järjestelmä poistaa vanhan lokin, joissain tapauksissa hyvinkin nopeasti.

Henkilökohtaiset tunnuksot haetaan asiakkaalta heidän prosessinsa mukaisesti, mutta jaetut hallintatunnukset annetaan tarpeen mukaan suoraan niitä tarvitseville.

#### 4.4 Asiakas D

Asiakas D:n IdM-järjestelmä on alun perin yrityksemme asentama. Hallintatunnuksia IdM-järjestelmään on kehitys-, testaus- ja tuotantoympäristöihin ja niiden Linux-palvelimille. Lisäksi AD-järjestelmään on tunnuksot.

IdM-järjestelmässä käytetään yhteisiä hallintatunnuksia. Henkilökohtaiset tunnuksot ovat olemassa, mutta niillä ei ole oikeuksia ylläpitää järjestelmää eikä niitä juuri käytetä. AD:ssa on käytössä henkilökohtaiset tunnuksot ja henkilökohtaiset hallintatunnukset.

IdM-järjestelmä kerää omia lokejaan, mutta lokien hallintaa ei ole keskitetty. Lokeja ei kuitenkaan poisteta koskaan järjestelmän toimesta.

Henkilökohtaiset tunnukset haetaan asiakkaalta heidän prosessinsa mukaan. Jaetut tunnukset annetaan tarpeen mukaan sisäisesti. Jaettuja tunnuksia varten käytössä on yhteinen salasanojen hallintatyökalu, jossa salasanat säilytetään ja luodaan. Näin salasanat ovat hyvin vahvoja.

#### 4.5 Asiakas E

Asiakas E:lle on hallintatunnuksia IdM-järjestelmien kehitys-, testaus- ja tuotantoympäristöihin, niiden Linux- ja Windows-palvelimille sekä AD-järjestelmään. Asiakas E:tä on pitkään ollut ylläpitämässä vain yksi henkilö ja tällä hetkellä ylläpitäjiä on kaksi.

Kaikki hallintatunnukset ovat yhteisiä. Henkilökohtaiset tunnukset ovat olemassa, mutta niillä ei ole mitään oikeuksia järjestelmien hallintaan. Yhteiset hallintatunnukset ovat myös käytössä palveluiden välillä, mikä vaikeuttaa niiden käytöstä poistoa, koska hallintatunnukset pitäisi korvata jokaiseen järjestelmään erikseen.

Henkilökohtaisille tunnuksille on salasanapolitiikka, mutta jaetut hallintatunnukset ovat politiikan ulkopuolella. Ylläpitäjät ovat kuitenkin käyttäneen salasanatyökalun luomia salanoja, jolloin ne ovat hyvin vahvoja.

IdM-järjestelmät keräävät omia lokeja ja kierrättävät niitä automaattisesti, ettei niiden koko kasva liian isoksi. IdM-lokeja pääsee lukemaan ainoastaan IdM-järjestelmän kautta. Muut järjestelmät keräävät omia lokeja. Lokien hallintaa ei ole kuitenkaan keskitetty mitenkään.

Henkilökohtaiset tunnukset tilataan asiakkaalta ja yhteiset tunnukset jaetaan yhteisellä salasanojen hallintatyökalulla.

## 5 Suositukset tunnusten hallintaan

Asiakasympäristöt ovat olleet tähän mennessä asiakkaiden omien vaatimusten sekä konsulttiemme omien käytäntöjen varassa. Tässä luvussa on tarkoitus kerätä kehitysehdotukset, hyvät käytännöt ja toimintatavat yhteen ja näin kehittää yhteinen toimintamalli, joka on yrityksemme toteutettavissa. Asiakkaiden omat vaatimukset menevät toki aina omien käytäntöjemme edelle, mutta yhtenäiset käytännöt helpottavat asiakkuuksien välillä työskentelyä.

Suurin osa hallintatunnusten hallinnoinnin parannuksista vaatii asiakkaan hyväksyntää ja resursseja muutosten toteutuksiin. Tämä saattaa vaatia investointeja ilman, että asiakas kokee suoraa hyötyä itselleen. Toki tietoturva paranee yleisesti, mutta asiakkaan on ehkä vaikea sitä kokea.

Yrityksemme otti lokakuussa 2018 käyttöön LastPass-salasananhallintatyökalun. LastPassiin voi tallentaa tunnuksia ja salasanoja, generoida uusia salasanoja ja jakaa tunnuksia ja salasanoja ylläpitäjien välillä. LastPass pitää jaetut tunnukset ajan tasalla jokaiselle käyttäjälle. LastPass tukee omien tunnusten tallentamista sekä useampaa eri jaettua tunnuslistaa, niin että yhdellä käyttäjällä voi olla omien tunnusten lisäksi useamman eri asiakkaan jaetut tunnukset tallessa. LastPass helpottaa tunnusten hallintaa, kun salasanoja ei tarvitse muistaa, tai edes osata, ja yhteiset tunnukset ovat kaikki samassa paikassa helposti saatavilla.

### 5.1 Asiakas A

Asiakas A:lla on tietoturva yleisesti hyvin korkealla ja myös hallintatunnukset on hyvin hoidettu. Ainoastaan kehitysympäristössä on käytössä yhteinen tunnus. Kehitysympäristöstä ei kuitenkaan ole pääsyä muihin ympäristöihin, joten tämä ei sinällään ole ongelma, eikä henkilökohtaisille tunnuksille ole tarvetta.

Ainoat pienet parannukset olisi tuoda kehitysympäristön jaetut tunnukset LastPassin jaettuun salasananholviin. Ylläpitäjille tulisi ottaa käyttöön AD-järjestelmään IdM:n hallitsemat henkilökohtaiset hallintatunnukset ja yhteisestä hallintatunnuksesta luopua. AD-järjestelmässä on paikallisia hallintatunnuksia, joiden tarpeellisuus tulisi tutkia ja yhdistää

tarvittaessa. Tämä on kuitenkin jo asiakaan tiedossa ja tähän on mahdollisesti tulossa muutoksia. Asiakas on myös harkinnut kaksivaiheisen tunnistuksen käyttöönottoa IdM-järjestelmissä.

## 5.2 Asiakas B

Asiakas B:n IdM-järjestelmä on varsin vanha ja peruja toiselta yritykseltä. Tästä johtuen järjestelmässä on monia huonoja käytäntöjä hallintatunnusten suhteen.

Asiakas B:llä on monia jaettuja tunnuksia, joiden salasanat ovat varsin heikkoja ja ne on tallennettu wikiimme tekstimuodossa. Nämä kaikki salasanat tulisi tallentaa jaettuun LastPassin salasananholviin ja vaihtaa vahvempiin. Näin vain asiakkuuden ylläpitäjillä on pääsy salasanoihin.

Pidemmällä aikavälillä asiakas B:n ylläpitäjille tulisi tehdä henkilökohtaiset hallintatunnukset IdM:ään ja Linux- ja Windows-palvelimelle. Mikäli Linux-palvelimelle ei voida tehdä henkilökohtaisia hallintatunnuksia, voidaan vähintään tehdä yhteinen hallintatunnus nykyisen järjestelmän oletushallintatunnuksen sijaan. Näin yhteisiä tunnuksia voidaan käyttää vain hätätilanteissa, salasanat vaihtaa ja jakaa vain niitä tarvitseville. Tämä parantaa tietoturvaa jo huomattavasti, kun kaikki ei ole jaettujen tunnuksen varassa.

IdM-järjestelmän lokit eivät tällä hetkellä säily pitkään, koska järjestelmä poistaa vanhan lokin kokorajan ylittyessä. Tähän auttaa kokorajan nostaminen, mikä vie tietysti enemmän kovalevytilaa. Lokitiedostot voi myös kopioida talteen muualle. Lokien kopiointi talteen onnistuu automaattisesti varsin helposti, mutta vaatii toki logiikan rakentamista ja palvelimelta kovalevytilaa, mikä taas vaatii investointeja asiakkaan puolelta.

Tietoturvaa parantaisi ottamalla käyttöön VPN-tunnuksiin kaksivaiheisen salasanan, vaikka VPN-tunnus ei ole varsinaisesti hallintatunnus. Kaksivaiheinen tunnistautuminen kuitenkin varmistaisi, ettei pelkällä VPN-tunnuksella pääsisi sisäverkkoon.

### 5.3 Asiakas C

Asiakas C:n kohdalla yrityksellämme on vastuu järjestelmästä, jolloin myös tietoturvan parantamisesta on suoraan hyötyä yrityksellemme.

Asiakas C:llä on monia jaettuja tunnuksia, joiden salasanat ovat heikkoja ja niitä ei ole vaihdettu koskaan. Nämä kaikki tunnukset voidaan jakaa LastPassilla ylläpitäjien välillä ja niiden salasanat vaihtaa keskitetysti vahvempiin.

Ylläpitäjille tulisi tehdä omat henkilökohtaiset hallintatunnukset tai vähintään antaa oikeudet olemassa oleville henkilökohtaisille tunnuksille ylläpitää järjestelmää. Tämän jälkeen jaettujen hallintatunnusten salasanat voidaan vaihtaa eikä niitä tarvitse enää käyttää kuin hätätilanteissa.

IdM-järjestelmän lokit eivät tällä hetkellä säily pitkään, koska järjestelmä poistaa vanhan lokin kokorajan ylittyessä. Tällä hetkellä rajoitettu kovalevytila on estänyt lokien säilyttämistä pidempään. IdM-järjestelmää ollaan juuri päivittämässä, minkä yhteydessä on pyydetty enemmän kovalevytilaa palvelimille.

Lokitiedostot voi myös kopioida muualle parempaan talteen. Lokien kopiointi talteen onnistuu automaattisesti varsin helposti, mutta vaatii toki logiikan rakentamista ja palvelimilta kovalevytilaa.

### 5.4 Asiakas D

Asiakas D:n ylläpitäjät ovat käyttäneet itsenäisesti toista salasananhallintatyökalua. LastPassin käyttöönoton myötä salasanat tulisi kuitenkin siirtää LastPassiin ja toisen työkalun käyttö lopettaa. Yrityksemme politiikan mukaan muita salasananhallintatyökaluja ei saa käyttää.

IdM-järjestelmien ylläpitoon on mahdollista käyttää AD:n henkilökohtaisia hallintatunnuksia, kunhan niille asetettaisiin oikeat oikeudet. Asiakas itse ei kuitenkaan ole nähnyt tälle

tarvetta. Henkilökohtaisten hallintatunnusten käyttöönottoa voisi kuitenkin ehdottaa asiakkaalle tietoturvan parantamiseksi. Samalla voidaan ehdottaa järjestelmien keskitettyä lokienhallintaa.

## 5.5 Asiakas E

Ylläpitäjät ovat itsenäisesti käyttäneet toista salasanan työkalua, mutta LastPassin käyttöönoton myötä salasanat voidaan siirtää LastPassiin yrityksemme politiikan mukaan. Jaettujen tunnusten salasanoja ei kuitenkaan voida helposti muuttaa, koska tunnukset ovat käytössä järjestelmien välillä, mikä tekee tunnuksen käytön lopetuksesta ja salasanan vaihdosta vaikeaa.

Järjestelmissä ei ole estettä henkilökohtaisille hallintatunnuksille, mutta ylläpitäjien vähäisyyden ja kätevyyden takia niitä ei ole otettu käyttöön. Mahdollisuuksien mukaan henkilökohtaiset hallintatunnukset voidaan ottaa käyttöön ja järjestelmien välille tehdä omat tunnukset, jotka ovat vain siihen käyttöön. Näin niiden salasanoja voidaan tarvittaessa ylläpitää paremmin eikä samaa tunnusta tarvitse käyttää ylläpitoon. Ainakin henkilökohtaiset hallintatunnukset saadaan salasanapolitiikan piiriin. Tämä vaatii kuitenkin jonkin verran työtä, josta asiakas ei suoraan näe hyötyjä heti.

Keskitettyä lokien hallintaa on hankala rakentaa, koska IdM-lokeja hallitaan suoraan IdM-käyttöliittymän kautta. IdM-lokit ja muiden järjestelmien lokit voidaan kuitenkin keskitetysti kerätä ja hallita erikseen. Tämä kuitenkin vaatii asiakkaalta erillisiä resursseja ja investointeja.

## 5.6 Yhteiset käytännöt

Monilla asiakkaistamme ilmeni samankaltaisia puutteita hallintatunnusten hallinnoinnissa. Monet kehityskohteet kuitenkin vaativat asiakkaan hyväksyntää ja jopa investointeja. Tässä luvussa on koottu tärkeimmät kehityskohteet sekä uusille asiakkaille hyviä käytäntöjä.



Yrityksemme otettua käyttöön LastPass-salasanatyökalun voidaan kaikki jaetut tunnukset tuoda keskitetysti yhteen holviin ja jakaa asiakaskohtaisesti niitä tarvitseville. Osalla ylläpitäjistä on käytössä toinen salasanatyökalu tai salasanat ovat tekstinä. Näistä huonoista käytännöistä päästään eroon helposti ottamalla käyttöön LastPass kaikille. Lisäksi uuden ylläpitäjän aloittaessa hänen ei tarvitse enää metsästää eri tunnuksia eri lähteistä, vaan kaikki jaetut tunnukset ovat yhdessä ja samassa paikassa.

LastPassin käyttöönoton myötä kaikki heikot salasanat voidaan vaihtaa ohjelman generoimiin vahvoihin salasanoihin. Salasanoja voidaan myös vaihtaa säännöllisesti ilman, että siitä syntyy suuria ongelmia ylläpitäjille, koska LastPass synkronoi salasanat automaattisesti ylläpitäjien välillä.

Asiakaskohtaisesti voidaan nimetä henkilö, jonka tehtävä on kerätä kaikki tunnukset LastPassiin, jakaa ylläpitäjille ja ylläpitää salasanoja vaihtamalla niitä säännöllisesti. Osa tunnuksista on järjestelmien välillä käytössä, jolloin salasanan vaihtaminen rikkoo yhteyden. Tunnuksen käytössä olevat palvelut tulee dokumentoida ja tunnuksen salasanaa päivittäessä se tulee vaihtaa palveluihin manuaalisesti. Salasanojen vaihto täytyy siis edelleen tehdä manuaalisesti, mutta ainakin tiedetään, mihin salasana täytyy vaihtaa, ja ylläpitäjät saavat uuden salasanan helposti LastPassin kautta.

Monilla asiakkaista on käytössä jaettuja hallintatunnuksia. Myös järjestelmän oletushallintatunnus on joillain asiakkaista edelleen käytössä. Asiakkaiden hyväksynnällä voidaan vanhoille henkilökohtaisille tunnuksille antaa suuremmat oikeudet tai luoda uudet henkilökohtaiset hallintatunnukset ja lopettaa hallinta järjestelmien oletustunnuksilla. Uuden IdM-järjestelmän asennuksen yhteydessä henkilökohtaiset hallintatunnukset tulee ottaa käyttöön heti asennuksen jälkeen.

Monilla asiakkailla IdM-järjestelmän lokien hallinta jättää toivomisen varaa. Lokeja ei hallita keskitetysti ja ne poistetaan nopeasti. Järjestelmiin on mahdollista rakentaa keskitetty lokien hallinta, joka kopioi lokit talteen asiakkaan omille palvelimille ennen kuin ne poistetaan. Tämä vaatii investointeja ja monissa tapauksissa lisää kovalevytilaa. Yhteinen keskitetty valvontajärjestelmä yrityksemme puolesta kaikille eri asiakkaille ei kuitenkaan ole mahdollista toteuttaa tietoturvan ja asiakkaiden omien politiikkojen takia.

Tunnusten saantiprosessiin asiakkaan puolesta ei todennäköisesti voi tehdä juuri muutoksia, mutta yhteisten tunnusten jakoa ylläpitäjien välillä voi kehittää. Uuden ylläpitäjän aloittaessa asiakkaan ympäristössä jaettuja tunnuksia ei tule jakaa sisäisesti ennen kuin asiakas on hyväksynyt ylläpitäjän ja tehnyt hänelle VPN-tunnukset tai muun yhteystavan. Näin vältetään jaettujen tunnusten salasanojen vaihdolta, jos ylläpitäjää ei hyväksytä asiakkaan puolesta. Mikäli ylläpitäjä tarvitsee työssään pääsyn vain osaan järjestelmästä, ei kaikkia tunnuksia tule jakaa, vaan vain tarvittavat tunnukset.

Henkilökohtaiset hallintatunnukset auttavat esimerkiksi ylläpitäjän lopettaessa asiakkaan ylläpitäjänä, jolloin vain hänen tunnuksensa voidaan lopettaa, eikä tarvitse huolehtia jaettujen tunnusten salasanojen vaihdosta. Niissä tapauksissa, joissa jaettuja tunnuksia edelleen käytetään, tulee tunnuksen salasana vaihtaa huolimatta siitä, että VPN-tunnus on lopetettu. Myös heidän LastPass-pääsynsä kyseiseen asiakkuuteen tulee poistaa.

## 5.7 Automaattinen hallinnointi

Osana tämän työn tarkoitusta oli kartoittaa, onko valmiin PAM-ratkaisun käyttöönotto mahdollista yrityksessämme. Hallintatunnuskartoituksen ja PAM-ratkaisuihin tutustumisen jälkeen näyttää siltä, että valmiin PAM-ratkaisun rakentaminen yrityksemme puolesta on lähes mahdotonta järjestelmien monimutkaisuuden ja monen eri järjestelmän erilaisten tarpeiden takia.

Jokainen asiakkaamme käyttää jonkinlaista menetelmää estääkseen järjestelmien käytön ulkoverkosta. Suurin osa asiakkaista käyttää VPN-yhteyttä; osalla on virtuaalityöpöytäohjelma, jonka kautta pääsee järjestelmiin; osa vaatii heidän omien tietokoneidensa käyttöä tai erillistä sertifikaatin asentamista tietokoneen todentamista varten. PAM-järjestelmää varten pitäisi jokaiselle asiakkaalle rakentaa erillinen yhteys heidän sisäverkkoonsa ennen kuin PAM pääsisi edes käsiksi hallintatunnuksiin.

Eri IdM-ratkaisut tuottavat myös omat ongelmansa, kun jokaista eri järjestelmää varten joutuisi PAM-järjestelmään rakentamaan erikseen erillisen kustomoidun liittymän järjestelmiin. Tämä vaatisi hyvin paljon sisäistä kehitystä, eikä olisi taloudellisesti kannattavaa.

Lisäksi IdM-järjestelmien palvelimien hallinta on asiakkaan vastuulla tai osa on ulkoistanut sen eteenpäin. PAM:n toiminan kannalta on tärkeää, että kaikki järjestelmän hallintatunnukset toimivat PAM:n kautta, jotta PAM:n valvontaa ei voi kiertää PAM:n ulkopuolisilla hallintatunnuksilla.

Tämän lisäksi tunnusten monitorointi toisi omat haasteensa. Tunnuksen käyttöönoton jälkeen kaikki monitorointi tapahtuu asiakkaiden järjestelmissä, mikä vaatii asiakkaan hyväksyntää. Järjestelmien lokitiedostojen siirtäminen asiakkaiden järjestelmistä pois ei välttämättä sovi asiakkaille. Tunnusten valvonta nauhoittamalla voi myös olla hankalaa, jos asiakas ei anna lupaa.

Parempi tapa ottaa käyttöön PAM-järjestelmä olisi auttaa asiakkaita ottamaan PAM käyttöön kaikissa heidän järjestelmissään ja sitä kautta käyttää heidän PAM-järjestelmäänsä. Tämä tietysti vaatisi investointeja asiakkailta. Yhä useampi yritys on kuitenkin tutkinut PAM:n käyttöönottoa.

## 6 Yhteenveto

Tässä insinööriyössä oli tarkoitus tutustua hallintatunnusten hallinnan parhaisiin käytäntöihin ja tehdä yritykselle hallintatunnuskartoitus, jossa selvitetään, mitä hallintatunnuksia yrityksellä on viidelle eri asiakkaalle ja miten niitä hallitaan. Yritys toimii konsulttina identiteetinhallinnassa ja työn luonteen takia konsulteilla on pääsy suureen määrään sensitiivistä tietoa. Identiteetin hallinta on mm. käyttäjien elinkaaren- ja pääsynhallintaa. Tästä seuraa tietoturvariskejä, koska konsulteilla on järjestelmänvalvojan oikeudet yritysten henkilötietohallintajärjestelmiin.

Hallintatunnuskartoituksen ja hallintatunnusten hallinnan parhaiden käytäntöjen perusteella kehitettiin suosituksia asiakaskohtaisesti ja parhaat yhteiset käytännöt hallintatunnusten hallintaan. Tällä pyrittiin parantamaan käytettävyyttä ja lisäämään tietoturvaa. Osana kartoitusta oli tarkoitus tutustua automaattisiin hallintatunnusten hallintajärjestelmiin ja selvittää, onko automaattinen järjestelmä mahdollista ottaa käyttöön yrityksessä.

Hallintatunnus on tunnus, jolla on pääsy sensitiiviseen dataan. Hallintatunnuksia ovat esimerkiksi järjestelmänvalvojan oikeuksilla olevat tunnuksset. Hallintatunnukset ovat

usein tietomurtojen kohteena ja riskialttiita väärinkäytölle. Monet yritykset eivät tiedä, kuinka paljon hallintatunnuksia niillä on eikä tunnuksia ole valvottu. Ilman valvontaa tietomurtojen havaitsemiseen saattaa mennä pitkään.

Työssä esiteltiin hallintatunnusten parhaita hallintatapoja sekä manuaalisesti että automaattisesti Privileged Access Management (PAM) -järjestelmillä. Hallintatunnukset tulee erotella tavallisista tunnuksista ja varmistaa, että hallintatunnuksilla on vain ne oikeudet, jotka ovat välttämättömiä tunnuksen käyttöön. Ilman automaattista hallintaa on tietoturvan kannalta suositeltavampaa käyttää henkilökohtaisia hallintatunnuksia identiteetin varmistamisen ja monitoroinnin takia, kun taas PAM-järjestelmissä käytetään jaettuja hallintatunnusta hyökkäyskohteiden minimoimiseksi. PAM:ssa identiteetin varmistus ei tapahdu tunnuksen kautta vaan PAM:n kautta.

PAM-järjestelmä toimii käyttäjän ja kohdejärjestelmän välissä, mikä estää kohdejärjestelmän hallinnoinnin PAM:n ulkopuolelta. PAM-järjestelmät varmistavat käyttäjän identiteetin, oikeudet tunnuksiin ja monitoroivat, mitä hallintatunnuksilla tehdään. PAM-järjestelmät myös hallitsevat hallintatunnusten salasanoja automaattisesti ja estävät PAM:n ulkopuolisten hallintatunnusten käytön, jotta valvontaa ei voi kiertää.

Hallintatunnuskartoituksen yhteydessä tuli esiin, että jaetut hallintatunnukset ovat laajalti käytössä monilla asiakkailla niiden aiheuttamasta tietoturvariskistä huolimatta. Joissain tapauksissa jaettujen tunnusten salasana on heikko eikä sitä ole vaihdettu koskaan. Jaetuista hallintatunnuksista ei todennäköisesti päästä kokonaan eroon asiakkaiden omien käytäntöjen ja tunnusten roolin takia palveluiden välisissä yhteyksissä. Jaetut hallintatunnukset tulisi kuitenkin asiakaskohtaisesti kerätä LastPass-salasanatyökaluun ja heikot salasanat vaihtaa vahvempiin. Mahdollisuuksien mukaan tulisi ottaa käyttöön henkilökohtaiset hallintatunnukset.

Monien asiakkaiden järjestelmien lokien hallintaa ei ole keskitetty ja lokit saatetaan kiertää hyvinkin nopeasti. Lokien hallintaa voitaisiin tehostaa keskitetyllä lokien keruu- ja hallintajärjestelmällä. Suurin osa kehitysmahdollisuuksista kuitenkin vaatii asiakkaan hyväksyntää ja investointeja.

Yksi työn tavoitteista oli selvittää, onko mahdollista automatisoida hallintatunnusten hallinnointi PAM-järjestelmällä. Selvityksen tuloksena on, että PAM:n käyttöönotto yritykselle ei olisi kannattavaa. Järjestelmän käyttöönotto vaatisi todella suuria investointeja; jokainen asiakas vaatisi erilaisten VPN-yhteyksien tai muiden tunnistautumistapojen takia erillisen yhteyden luomisen, ja jokainen IdM-järjestelmä vaatisi oman räätälöidyn erillisen PAM-liitännän rakentamisen. Koko järjestelmää ei ole myöskään mahdollista saada PAM:n haltuun ulkoverkosta.

Oman PAM-järjestelmän sijaan suositeltavampi tapa on auttaa asiakkaita itse ottamaan käyttöön PAM-järjestelmä heidän koko IT-järjestelmälleen ja sen yhteydessä tuoda IdM-järjestelmien hallintatunnukset PAM-järjestelmään. Näin vältetään hankalilta yhteysohjelmit ja kalliilta investoinneilta.

Hallintatunnusten parhaiden käytäntöjen perusteella voidaan tehdä hallintatunnuksille politiikka, jota uusien asiakkaiden uusissa järjestelmissä pyritään seuraamaan alusta lähtien. Vanhat asiakkaat pyritään tuomaan mahdollisuuksien mukaan politiikan piiriin. Asiakkaiden omat vaatimukset toki menevät aina edelle, mutta monilla asiakkailla ei ole itsellään kovin tarkkoja säädöksiä, jolloin voidaan esitellä heille yrityksen politiikka ja pyrkiä käyttämään sitä alusta lähtien.

## Lähteet

- 1 Verizon. 2018. 2018 Data Breach Investigations Report. Verkkoaineisto. Verizon. <<https://enterprise.verizon.com/resources/reports/dbir/>>. Päivitetty 2018. Luettu 24.10.2018.
- 2 Cser, Andras. 2016. The Forrester Wave™: Privileged Identity Management, Q3 2016. Verkkoaineisto. Forrester. <<https://www.forrester.com/report/The+Forrester+Wave+Privileged+Identity+Management+Q3+2016/-/E-RES123903#>>. Päivitetty 6.8.2016. Luettu 25.10.2018.
- 3 Mandiant M-Trends 2018 Report. Verkkoaineisto. FireEye. <<https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf>>. Päivitetty 04.04.2018. Luettu 28.05.2018.
- 4 2016. What is a Privileged Account?. Verkkoaineisto. Youtube. <<https://www.youtube.com/watch?v=mjJELLKV0sE>>. Päivitetty 24.05.2016. Luettu 28.05.2018.
- 5 2016. Building the Business Case for Privileged Account Security. Verkkoaineisto. Youtube. <[https://www.youtube.com/watch?v=NR4kfT6\\_Vqs](https://www.youtube.com/watch?v=NR4kfT6_Vqs)>. Päivitetty 04.10.2016. Luettu 28.05.2018.
- 6 BeyondTrust. 2017. BeyondTrust Survey Reveals the “5 Deadly Sins” That Increase the Risks of a Data Breach <<https://www.beyondtrust.com/resources/press-release/beyondtrust-survey-reveals-the-5-deadly-sins-that-increase-the-risks-of-a-data-breach/>>. Päivitetty 20.9.2017. Luettu 25.10.2018.
- 7 Kang, Cecilia. 2015. Sony Pictures hack cost the movie studio at least \$15 million. Verkkoaineisto. The Washington post <<https://www.washingtonpost.com/news/business/wp/2015/02/04/sony-pictures-hack-cost-the-movie-studio-at-least-15-million/>>. Päivitetty 4.2.2015. Luettu 1.10.2018.
- 8 Hirschfeld Davis, Julie. 2015. Hacking of Government Computers Exposed 21.5 Million People. Verkkoaineisto. The New Your Times. <<https://www.ny-times.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html>>. Päivitetty 9.7.2015. Luettu 1.10.2018.
- 9 Fitzpatrick, Alex. 2013. NSA Secretly Collecting Millions of Verizon Subscribers' Records: Report. Verkkoaineisto. Mashable. <<https://mashable.com/2013/06/05/verizon-nsa-phone-records/>>. Päivitetty 6.6.2013. Luettu 11.10.2018.

- 10 Spanier, Gideon. 2016. Protecting brand reputation in the wake of a cyber attack. Verkkoaineisto. Racounter. <<https://www.raconteur.net/risk-management/protecting-brand-reputation-in-the-wake-of-a-cyber-attack>>. Päivitetty 8.3.2016. Luettu 1.10.2018.
- 11 Raiter, Stepanie. 2018. Former IT Administrator Sentenced to Prison for Hacking Canadian Pacific Railway Network. Verkkoaineisto. Crowelldatalaw. <<https://www.crowelldatalaw.com/2018/02/former-it-administrator-sentenced-to-prison-for-hacking-canadian-pacific-railway-network/>>. Päivitetty 16.2.2018. Luettu 1.2018.
- 12 2016. ISSA presentation: Thycotic Secret Server Demo. Verkkoaineisto. YouTube. <<https://www.youtube.com/watch?v=OUTDjHRppp0>>. Päivitetty 2.8.2016. Luettu 25.10.2018.