LAUREA AMMATTIKORKEAKOULU Uuden edellä

Sähköisen tietoturvaoppaan suunnittelu

Jurvanen, Petri

2014 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Sähköisen tietoturvaoppaan suunnittelu

Petri Jurvanen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2014

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Petri Jurvanen

Sähköisen tietoturvaoppaan suunnittelu

Vuosi 2014 Sivumäärä 34

Tämän toiminnallisen opinnäytetyön tarkoituksena oli tuottaa OS X-käyttöjärjestelmää käsittelevä tietoturvaopas Tekninen toimisto Tektor oy:n asiakkaille. Oppaan pääasiallinen tarkoitus oli kertoa asiakkaalle käyttöjärjestelmään sisäänrakennetuista tietoturvaan liittyvistä komponenteista sekä olla asiakkaan luettavissa kaikilla hänen laitteillaan.

Tietoturvaoppaan suunnittelussa pääpaino oli sisällön tuottamisessa. Oppaan suunnitteluprosessista rajattiin pois visuaalinen suunnittelu jonka lopullisesta toteuttaa Tectorin visuaalisesta ilmeestä vastaava henkilö. Sisällön suunnitteluprosessin alkuvaiheessa annettiin tuotteen loppukäyttäjille eli asiakkaille mahdollisuus omien näkemyksien esille tuontiin sisältöön liittyen.

Oppaan suunnittelun alussa määriteltiin millainen on hyvä ohjeistus. Suunnittelussa otettiin huomioon lukijan lukemista helpottavia asioita kuten: info-laatikot joista näkee aiheen ydinasian yhdellä silmäyksellä. Oppaan alustaksi määrittyi iBooks-muodossa oleva e-kirja juuri sen helpon muokattavuuden ansiosta.

Ydinasia eli tietoturvaoppaan sisältö suunniteltiin OS X-käyttöjärjestelmän sisäänrakennettujen työkalujen ympärille. Millä toimenpiteillä tietokoneesta saa turvallisen ja kuinka turvallisuutta ylläpidetään. Oppaassa otettiin huomioon myös tietoturvan yleistä teoriaa CIA-triadin eli tiedon luottamuksellisuuden, saatavuuden sekä eheyden muodossa. Tietoturvaoppaan sisällön kehitys on jatkuvaa ja tämä otettiin suunnitteluprosessissa huomioon.

Opinnäytetyön lopputuloksena syntyi tietoturvaopas joka vastaa käytettävyydeltään sekä sisällöltään Tectorin vaatimuksia. Opasta tullaan käyttämään liiketoimintaan kuuluvien kurssien oheismateriaalina sekä se on asiakkaiden saatavilla erikseen pyydettäessä. Opasta tullaan kehittämään yrityksen toimesta eteenpäin tulevaisuudessa asiakkaiden toiveiden sekä uusien järjestelmäversioiden mukaisesti.

Asiasanat Tietoturvaopas, e-kirja, CIA-triadi

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Degree in Business Information Technology

Petri Jurvanen

Designing an electronic information security guide

Year 2014 Pages 34

The purpose of this thesis was to create a guidebook about information security in the OS X operating system for customers of Tekninen toimisto Tektor. The main objective of this guide was to inform the customer about built-in features, which can improve the level of security. The customer must also have the option to read this particular guide with any Apple device. Another important aspect was to make the guidebook readable on any Apple device.

In the process the main focus was on the content of the guidebook. The main point was to create content for this information security guide. Visual design was excluded from this project; this was due to the fact that Tector has a visual designer. Customers had a chance to impact on the content design in the beginning of this project.

Before starting on the main content, it was defined what makes a good guidebook. When a guidebook is well produced, it is easy to read and the main idea is easy to adopt at once. It was decided that an e-book platform was needed, since it makes editing possible.

The main content for this guidebook is based on the built in-tools of the OS X operating system; what operations customers need to build a safe environment and how to maintain it. The guidebook also focuses on the CIA triad that stands for confidentiality, integrity and availability. The constantly developing information security was taken into consideration during the project, and therefore the content of the guidebook will change over time.

The outcome of this thesis is an electronic guidebook that corresponds to Tector's requirements. Tector will be using this guidebook as side material on their courses for their customers. The guidebook will also be distributed to their customers, when needed. After the release Tector will develop the guidebook further according to customers' needs and the ever-changing operating system.

Keywords Infromation security guide, e-book, CIA-triad

Sisällys

1 Johdanto

Tämän opinnäytetyön tarkoituksena on suunnitella sisältö sekä toteuttaa sähköinen tietoturvaopas Tekninen toimisto Tektorin asiakkaille. Tietoturvaopas keskittyy OS X –käyttöjärjestelmän sisäänrakennettuihin komponentteihin joiden oikeanalaisella käytöllä asiakas voi helposti luoda tietoturvallisen toimintaympäristön. Tutkimus aloitettiin perehtymällä asiakkaiden tietotaitoon sekä tietoturvaohjeistukseen tarpeisiin.

Tutkimusstrategiaksi valittiin konstruktiivinen tutkimus ja tiedonhankintamenetelmiksi kvalitatiiviset menetelmät. (Järvinen & Järvinen, 2011, 74) Kvalitatiivisiksi menetelmiksi valittiin teemahaastattelu ja havainnointi. Tutkimusongelma pyrittiin ratkaisemaan konstruktiivisella tutkimusotteella. Konstruktiivinen tutkimus on yksi tapa luoda uusia toimintamalleja ja –tapoja. (Järvinen & Järvinen 2011, 103)

Aineiston analysoinnin jälkeen lähdetään kehittämään konstruktiota eli tässä tapauksessa kehittämään kirjallista opasta asiakkaille jotta tiedon saatavuus, eheys ja luottamuksellisuus voidaan turvata. Oppaassa keskitytään OS X-käyttöjärjestelmän sisäänrakennettuihin työkaluihin ja ominaisuuksiin sekä niiden oikeanlaiseen käyttöön. Näiden toimintatapojen tulee yhdessä sisäänrakennettujen työkalujen kanssa olla helppoja ja vaivattomia jokapäiväisessä käytössä.

Työn toisessa luvussa kuvataan tutkimuksessa käytettyjä menetelmiä ja tutkimukselle asetettuja tavoitteita. Kolmannessa luvussa perehdytään ohjeistuksen laatimiseen ja miksi e-kirja on tässä tapauksessa paras formaatti työlle. Neljännessä luvussa perehdytään tietoturvallisuuden teoriaan ja CIA-triadiin yleisellä tasolla. Viidennessä luvussa perehdytään OS X -käyttöjärjestelmän sisäänrakennettuihin tietoturvakomponentteihin ja niiden jokapäiväiseen käyttöön. Kuudennessa luvussa arvioidaan työn lopputulos ja sitä, kuinka opas toimii jokapäiväisessä käytössä.

2 Tutkimusenetelmä ja -tavoite

Tämän opinnäytetyön tutkimusongelmana on selvittää, millainen tietoturvaohjeistuksen tulisi olla jotta se palvelisi Tectorin asiakkaita mahdollisimman tehokkaasti. Työn tarkoituksena luoda työn kohteelle eli Tekninen toimisto Tektorin asiakkaille tietoturvaohjeistusta, jonka avulla asiakkaat voivat tarkastaa toimintamuotojaan tietoturvallisuuden parantamiseksi. Perustutkimuksen osana on selvitetty, millaisia tarpeita ja toiveita asiakkailla on tällaista ohjeistusta varten. Opinnäytetyössä keskityn tietoturvaohjeen suunnittelu- ja toteutusprosessiin.

Asiakkaan kohdalla aineiston kasaamiseksi valitsin laadulliseksi menetelmiksi teemahaastattelun koska tässä tutkimuksessa keskityttiin uuden innovaation eli asiakkaille suunnatun tietoturvaoppaan luomiseen. Teemahaastattelu sisältää keskustelua valitusta aiheesta keskittyen tutkimusongelmaan ja toivottuun tavoitetilaan (Kurkela). Haastateltavaksi valittiin joukko Tectorin asiakkaita kaikista asiakasryhmistä. Haastatellut asiakkaat edustivat Tectorin tyypillisiä asiakkaita (pk-yrityksiä, yksityishenkilöitä), joilla kaikilla oli erilaiset taustat ja tarpeet tietoturvallisuuden varmistamiseen. Asiakkaita haastatellessa tavoitteena oli saada kuva asiakkaiden tarpeista ja mahdollisuuksista käyttää ohjeistusta. Koska haastattelujen jälkeen selvisi, ettei asiakkailla ollut selkeää ja yhtenevää näkemystä tarpeellisesta ohjeistuksesta tai sen formaatista, otettiin tietoturvaoppaan sisällön ja formaatin suunnittelussa huomioon myös kollegoiden näkemys ja mielipide. Alla olevassa kuvassa (Kuva 1) on kuvattuna ohjeistuksen laatimisprosessini.

Kuva 1: Ohjeistuksen laatimisprosessi

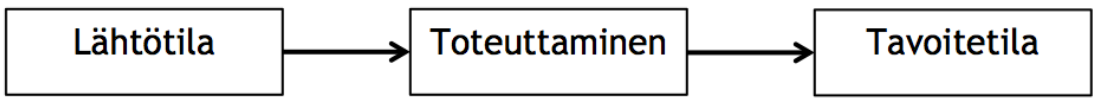
Opinnäytetyön tutkimuksen empiirisessä osuudessa tutkimusongelman ratkaisemiseksi päädyttiin konstruktiiviseen tutkimukseen. Konstruktiivinen tutkimuksen tarkoitus on luoda pohjaa suunnittelua ja sen toteutusta varten tai vaihtoehtoisesti parantaa nykyisten toimintojen suorituskykyä. Jos tutkimusongelman peruskysymys sisältää esimerkiksi seuraavanlaisia sanoja: rakentaa, muuttaa, parantaa, vahvistaa, huoltaa laajentaa, korjata, sovittaa, laatia kuuluu tutkimus suurella todennäköisyydellä suunnittelutieteen piiriin. (Järvinen & Järvinen, 2011, 103)

Konstruktiivisen tutkimuksen onnistumisen kannalta on erityisen tärkeää, että tutkija ja käytännön työntekijät tekevät läheistä yhteistyötä yhteisenä tavoitteenaan saavuttaa aikaisempaan kokemukseen pohjautuvaa oppimista. Tutkimuksen konstruktiivisessa osuudessa suurin apu kokonaisuuden hahmottamisessa oli juuri kollegoilla, jotka työskentelevät asiakasrajapinnassa. Konstruktiivinen tutkimus on sidottava myös teoriaan ja heijastaa sieltä havaitut uudet löydökset takaisin käytäntöön jotta uusi innovaatio syntyy. (Henttonen, Kaakkuri-Knuuttila & Rolin 2006, 112-113)

Koska tietoturvassa erityyppiset riskit ja uhkatilanteet vaativat omanlaisensa toiminnan on konstruktiivinen tutkimusote tässä tapauksessa selkein tapa ratkaista tutkimusongelma sekä luoda ja toteuttaa asiakasta tyydyttävä kokonaisuus. Koska tietty uhka voi esittäytyä erilaisissa tilanteissa on varauduttava asiakkaan kannalta kaikkein kriittisimpiin kohteisiin. Selkein esimerkki tällaisesta voisi olla: ”Jos haluat saavuttaa Y:n tilanteessa Z, niin jokin sellainen toimenpide kuin X saattaisi auttaa.” (Järvinen 2011, 104)

Alla olevassa kuvassa lähtötilalla tarkoitetaan tämän tutkimuksen kohdalla asiakkaan toimintatavoissa ja toiminnoissa nyt vallitseva tilanne. Koska Tectorilla ei tällä hetkellä ole tarjottavana asiakkaille vastaavaa ohjeistusta käyttöjärjestelmän turvallisuuden varmistamisesta on tämän tyyppiselle työlle käyttöä Tectorin asiakaskunnassa. Työn tavoitetilalla tarkoitetaan lopputulosta siitä, kun idea ja innovaatio on realisoitu. Toteuttaminen käsittää metodin jolla saadaan lopullisesti aikaan muutos lähtötilanteesta lopulliseen tavoitetilaan (Järvinen 2011, 108).

Järvinen & Järvinen kuvaavat toteuttamisprosessin karkeasti seuraavalla tavalla:



Kuva 2: Toteuttamisprosessi (Järvinen & Järvinen, 2011, 108)

3 Ohjeistuksen laatiminen

Teknisiä ja vaativia tietoturvaohjeistuksia kirjoittavat yleensä aiheeseen perusteellisesti perehtyneet asiantuntijat. Yleisesti tekniset ohjeistukset ovat kattava kuvaus koko järjestelmästä ja sisältävät asioita jotka ovat loppukäyttäjälle usein tarpeettomia. Hankalan luettavuuden takia tällaiset dokumentit voivat olla huomattavan puutteellisia, epäloogisia sekä sisältää loppukäyttäjälle vieraita termejä. Koska loppukäyttäjät ovat kaikkein haastavin mahdollinen lukijakunta, onkin tärkeää tehdä oppaasta selkeä ja mielenkiintoinen luettava, jotta tarvittava informaatio saavuttaa loppukäyttäjän. (Alasilta 1999, 59-69.)

Ohjeistusta kirjoitettaessa on hyvä muistaa ainakin seuraavat asiat:

- Pidä yllä kärsimättömimmänkin lukijan mielenkiinto.
- Esitä asia kirkkaasti.
- Selitä täsmällisesti kaikki, mitä lukijan tarvitsee tietää kyetäkseen etenemään vaiheesta toiseen.
- Opasta lukijaa nopeasti ja vaivatta oikean asiakohdan äärellä.
- Huomaa, että lukija ymmärtää monimutkaiset asiat helpommin jokapäiväisen esimerkin kautta.

Olennaisinta on tehdä lukijalle selväksi miksi ohjeen lukeminen on tärkeää. Ihmisillä on usein taipumus tarttua toimeen välittömästi ja jättää ohjeet lukematta. Ohjeisiin tartutaan usein vasta virheen sattuessa. Ohjeen tärkein tehtävä on siis saada loppukäyttäjä lukemaan sekä ymmärtämään se ennen minkäänlaisia toimenpiteitä. (Kauppinen, Nummi & Savola 2006, 102)

3.1 Ohjeistuksen tehokkuus ja käytettävyys

Tehokkaan ja toimivan ohjeistuksen perusvaatimuksia ovat silmäiltävyys, luettavuus ja käytettävyys. Hyvin laadittu ohjeistus antaa jo ensisilmäyksellä innoittavan vaikutelman ja saa lukijan kiinnostumaan itsestään. Silmäiltävyys on ensiarvoisen tärkeää ensivaikutelman kannalta, tekstin yleinen luettavuus ja sen käytettävyys takaavat viestinnän ja ymmärtämisen tehon. Ennen varsinaisen tekstin lukemista lukija yleensä silmäilee kokonaisuutta. Lukijan katse kiertää kehää myötäpäivään alkaen keskipisteen vasemmalta ja sen yläpuolelta. (Alasilta 1999, 59-69)

Kaikki lukijat eivät välttämättä osaa eritellä miksi lukevat tekstistä vain osan ja jättävät osia siitä kokonaan lukematta. Hyvässä luettavuudessa on kysymys siitä, kuinka nopeasti lukija pystyy tekstin lukemaan ja kuinka helposti hän omaksuu tekstin sisällön. Tekstin luettavuuteen vaikuttavat tekstin ulkoasu, kielellinen ymmärrettävyys sekä tietenkin lukijan motivaatio aihetta kohtaan (Alasilta 1999, 59-69.).

Alasilta (1999, 82) listaa käytettävyyden syntymiseen liittyviä tekijöitä:

- silmäiltävyys
- luettavuus
- juonellisuus
- lukemisen ohjaus
- jäsentely ja rakenne
- motivointi

Kaikkien yllä mainittujen ominaisuuksien tulee olla tasapainossa. (Kuva 3)

Kuva 3: Käytettävyyden tasapaino viestinnässä

3.2 E-kirja tietoturvaoppaana

Ohjeistuksen käytettävyyteen voidaan vaikuttaa sillä, miten tiedot on esitetty ja millainen teoksen ulkoasu on. Lisäksi käytettävyyteen vaikuttaa näiden ohella ohjeistuksen saatavuus. Sähköinen ohjeistus kulkee asiakkaan mukana kaikissa hänen laitteissaan. Applen ekosysteemissä ohjeistus on luettavissa ja ladattavissa asiakkaan tietokoneeseen, iPadiin sekä esimerkiksi iPodiin. Perinteisesti erilaiset käyttöohjeistukset ovat olleet painettuja pieniä ohjelappuja tai isoja ohjekirjoja. Vasta viimevuosina sähköiset ohjekirjat ovat yleistyneet maailmalla osana yritysten ympäristöohjelmia, joiden tarkoitus on minimoida ympäristön kuormitusta. (Apple and the environment)

Asiakkaiden toiveiden mukaisesti ohjeistuksen jakelu tapahtuu ilmaisena teoksena Applen iBookstore-kirjakaupan kautta sekä sähköisesti yrityksen omia jakelukanavia pitkin. Kirjan formaatin valinnassa kohderyhmän perusteella päädyttiin Applen omaan e-kirja formaattiin. Applen iBooks Author-ohjelmassa käyttämä e-kirjaformaatti ei ole yhteensopiva yleisen EPUB-standardin kanssa. Tämä rajoite estää oppaan käytön kilpailevissa mobiilialustoissa ja näin vaikeuttaa oppaan käyttöä asiakkailla, joilla mac-koneen ohella ei ole muita Applen ekosysteemiin kuuluvia laitteita. (Hakkarainen 2012)

3.3 Kirjan kokoaminen ja julkaiseminen iBooks storessa

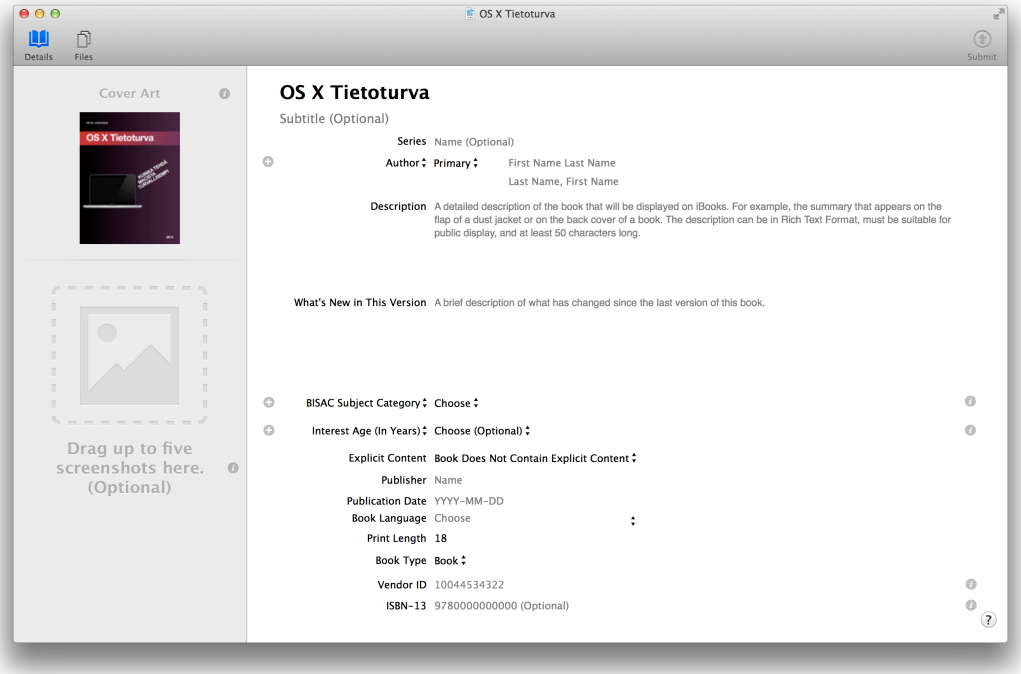
Ohjeistus laatimiseen ja kasaamiseen valittiin halutun alustan pohjalta Apple iBooks-Author ohjelma, jonka avulla opas voidaan toteuttaa ja julkaista. Ohjelmassa luotavaan kirjaan voidaan tuoda valmiita tekstikappaleita suoraan tekstinkäsittelyohjelmasta ja muotoilla ne kirjaan sopivaan muotoon. Kuvien lisääminen tapahtuu samalla tavalla.

Tällä hetkellä Applen iBooks Authorilla tehdyt e-kirjajulkaisut toimivat ainoastaan mac-tietokoneiden ohella vain iPad-laitteissa. Tätä kyseistä opasta on mahdollista käyttää myös esimerkiksi Applen iPhonessa tai iPod Touchissa, tällöin opas on konvertoitava PDF-muotoon

ja synkronoitava iBooks-sovelluksen kanssa. PDF-muoto mahdollistaa oppaan jakamisen asiakkaille esimerkiksi sähköpostin liitetiedostona tai ladattavana versiona yrityksen kotisivuilta. PDF-muodossa oleva tietoturvaopasta voidaan käyttää myös muissa käyttöjärjestelmäympäristöissä.

Kirjan julkaisua varten käyttäjällä on oltava voimassa oleva Apple-ID tili ja tämä tulee liittää erilliseen iTunes Connect-tiliin joista käyttäjällä on valittavissa kaksi vaihtoehtoa. Ilmainen tili mahdollistaa ilmaisten kirjojen jakelun iBooks storessa ja kirja on tällöin ladattavissa kaikiis 51 iBooks storessa. Maksullinen palvelu mahdollistaa kirjojen myymisen ja sallii rajata kirjan jakelualueen. iTunes Connect palvelusta ladataan iTunes Producer-sovelluspaketti joka liittyy osaksi iBooks Author ohjelmaa, tämän lisäosan avulla kirjan lopullinen julkaisu tapahtuu. (iBooks Author-ohje) Oppaan päivittäminen on mahdollista vielä julkaisun jälkeen ja tuolloin asiakas saa ilmoituksen uudesta versiosta ja hänen on mahdollista päivittää vanha versio uudeksi yhdellä napin painalluksella. (iBooks Author: Julkaistun kirjan päivittäminen iBooks Storessa)

Kirjan julkaisuprosessi alkaa iBooks Authorissa valitsemalla julkaise-painiketta. Valmis kirja siirtyy tämän jälkeen iTunes Produceriin (Kuva 4) jossa täytetään kirjan lisätiedot sekä luodaan kirjasta esikatseluversio. Kun tarvittavat tiedot on täytetty lähetetään kirja Applelle hyväksyttäväksi, tämä hyväksymisprosessi kestää yleensä noin 48 tuntia. (iBooks Autor: Kirjan julkaiseminen iBooks Storessa)



Kuva 4: iTunes Producer

4 CIA-Triadi tietoturvassa

CIA-triadin lyhenne tulee sanoista: Confidentiality, availability ja integrity, jotka suomeksi tarkoittavat tiedon luottamuksellisuutta, saatavuutta ja eheyttä. Loppukäyttäjän tietoturvallisuuden varmistamiseksi on määriteltävä millaisia suojaustoimenpiteitä voidaan suorittaa erilaisia tietoturvauhkia vastaan, jotta CIA-triadin osa-alueet toteutuvat. On hyvä huomata, että yksittäinen pienikin tietoturvauhka saattaa kohdistua yhden tukipilarin sijaan kaikkiin CIA-triadin tukipilareihin. Hyvin suunniteltu tietoturvaratkaisu sen sijaan torjuu useampaan, kuin yhteen CIA-triadin tukipilariin kohdistuvat uhat ja loukkaukset. CIA-triadi liittyy olennaisesti tietoturvallisuuteen sen jaottelun myötä ja on tässä työssä näkökulmana erilaisten tietoturvallisuuteen vaikuttavien toimenpiteiden suorittamisessa.

Tässä opinnäytetyössä CIA-triadi toimii runkona jonka kautta perehdytään erilaisten komponenttien hyödyntämiseen tietoturvallisuuden ylläpidossa OS X –käyttöjärjestelmässä. Ohjeistuksen loppukäyttäjän on helppo hahmottaa CIA-triadin kautta mihin osa-alueeseen tietty toimenpide liittyy ja miksi näin tehdään. Koska CIA-triadi on loppukäyttäjälle lähtökohtaisesti vieras termi on sille varattava oma osio opaskirjan alkupuoliskolta, jotta loppukäyttäjällä on käytössään opaskirjan koko potentiaali.

4.1 Luottamuksellisuus

Luottamuksellisuudessa olennaista on määritellä ja rajata pääsyoikeudet yrityksen tietoihin sekä dataan jotka liittyvät sen liiketoimintaan, asiakkaisiin ja työntekijöihin. Jos luottamuksellisuutta ei voida toteuttaa vaaditulla tavalla voi suojattavaa tietoa sisältävä kohde olla sellaisten henkilöiden ulottuvilla, joilla ei ole kohteen käsittelyyn vaadittavia oikeuksia. Tietojen jakamista ja käyttöä voidaan rajata luomalla käyttöjärjestelmään riittävän vahvalla salasanalla sekä yksilöllisillä käyttöoikeuksilla suojattuja käyttäjätilejä. Pääsynvalvonta voidaan jakaa kolmeen osa-alueeseen: Käyttäjän tunnistamiseen, jossa määritellään käyttäjä annetun käyttäjänimen perusteella. Käyttäjän todennukseen, jossa annettu käyttäjätunnus varmistetaan annetulla salasanalla. Oikeutukseen, jolla määritellään käyttäjälle oikeanlaiset ja hänen työkuvaansa vastaavat käyttäjäoikeudet. Oikeanlaisella pääsynvalvonnalla voidaan tietojen luottamuksellisuutta suojata niin sisäisiltä, kuin ulkoisiltakin uhilta. (Paananen 2005, 398)

Tiedon luottamuksellisuuden takaamiseksi käyttäjäprofiilien, -tunnusten ja vahvojen salasanojen ohella voidaan esimerkiksi käyttää tietojen rajoittamista vain tiettyihin verkkoihin ja tietokoneisiin, sekä fyysisiä pääsynrajoituksia kuten suljettuja laite- ja työskentelytiloja. Koska mikään yksittäinen suoja ei ole täydellinen, rakentavat järjestelmien ylläpitäjät usein mo-

nia suojauskerroksia väärinkäytösten havaitsemiseksi sekä niiltä suojautumiseksi. (Jordan & Silcock 2006, 166)

Mahdollisia uhkakuvia tiedon luottamuksellisuuteen liittyen voivat esimerkiksi olla seuraavia:

- Rikollinen mieli – Jos henkilö pääsee käsiksi yrityksen toimitusaikatauluihin tai asiakastietokantaan on ne mahdollista esimerkiksi myydä kilpailijoille sivutulon saamiseksi.
- Kilpailijan mieli – Jos samoissa toimitiloissa työskentelevä kilpailija löytää yhteisistä toimitiloista valmiiksi sisäänkirjautuneen tietokoneen.
- Työntekijä – Kuka tahansa työntekijä voi olla kiinnostunut esimerkiksi esimiehensä palkasta tai hänestä itsestään kirjatusta arvioinnista. Ennen pitkään työntekijä tulee lähes varmuudella etsimään töitä muualta, joten on mahdollista, että hän pohjustaa uuteen yritykseen siirtymistään esimerkiksi: Asiakaslistauksella, sisäisellä hinnastolla tai uuden tuotteen julkaisusuunnitelmalla.
- Haktivistit – Kenellä tahansa internetin käyttäjällä voi olla ”missio” jolla yritystä halutaan mustamaalata paljastamalla ”totuus” keskustelupalstoilla. Pohjana ja motiivina tällaisille iskuille voi olla esimerkiksi tietovuoto yrityksen sisältä. (Jordan & Silcock 2006, 165-166)

4.2 Eheys

Millä toimenpiteillä loppukäyttäjä voi varmistaa, että sen omistama tieto-omaisuus ei ole korruptoitunut tahallisesti tai tahattomasti? Tieto-omaisuuden turmeleminen tai sen osan hävittäminen voi olla keino häivyttää jäljet luvattomasta käynnistä yrityksen tietovarastolla. Esimerkkinä henkilökohtaisesta hyödystä tiedon vääristämisestä ovat esimerkiksi omien palkkatietojen muuttelu yrityksen tietokantaan josta palkat maksetaan tai opiskelijan arvosanatietojen väärentäminen. Tietojen tahaton häviäminen on yleensä seuraus seuraavista asioista:

- Laitteistoviat, esimerkiksi kiintolevyn rikkoutuminen tai tietoliikenneviat.
- Ohjelmistoviat
- Infrastruktuuria kohdanneet häiriöt, esimerkiksi sähkökatkokset.
- Käyttäjää ohjaavien viestien, esimerkiksi ”Tätä toimintoa ei voi keskeyttää” tai ”varmuuskopioi ennen kuin jatkat” tottelematta jättäminen.

Tyypillisiä toimenpiteitä tieto-omaisuuden eheyden varmistamiskeksi ovat esimerkiksi hyvin vikasietoiset järjestelmät ja etenkin niiden peilatut levyt, järjestelmän lokitiedostot, varmuuskopiot, tiedon tarkistussummat, kirjausketjut sekä palautuksen testaus. Luvattoman käytön ja tunkeutumisen havaitseminen on toinen erittäin tärkeä osa

eheyden varmistuksessa. Tietojen oikeellisuuden palautus voi muodostua erittäin kalliiksi operaatioksi tiedon eheyden menetyksen jälkeen. (Jordan & Silcock 2006, 167)

4.3 Saatavuus

Yrityksen tietojen saatavuus liittyy olennaisesta tiedostojärjestelmän turvaamiseen. Laitteiden, järjestelmien ja verkkoyhteyksien tulee toimia juuri silloin, kun tietoa ja laitteita halutaan käyttää. Toimistojärjestelmien kohdalla tämä tarkoittaa käytännössä riittävää toimivuutta toimistotyöaikoina, yöaikaan ja viikonloppuisin voidaan suorittaa tiedostojen varmistaminen. (Järvinen 2002, 24)

Tietokoneista ei ole yritykselle paljoakaan hyötyä elleivät myös niiden sisältämät tiedot ole käytettävissä niitä tarvittaessa. Tiedostojen varmuuskopiointi onkin yrityksen elintärkein toimenpide saatavuuden varmistamisessa toimintaa turvaavan tekniikan ohella, kuten esimerkiksi UPS-laitteiden käyttö sähkökatkojen varalta. Tietojen saatavuus voi aiheuttaa yritykselle yllättäviäkin ongelmia. Yritys saattaa tarvita tiedostoja jotka on luotu esimerkiksi 10 vuotta sitten. Vaikka kyseiset tiedostot on varmistettu asianmukaisesti saattaa ongelmaksi muodostua tiedostojen avaaminen ja hyödyntäminen. Yhteensopivia sovelluksia ei välttämättä enää ole tallessa tai saatavilla tai ne eivät enää toimi uusissa laitteissa. (Järvinen 2002, 24)

Yrityksillä on hyvä olla käytössään strategia ja palautumissuunnitelmia erilaisia palvelunkatkos skenaarioita varten. Tärkeää on kattaa yrityksen kannalta kaikki tärkeimmät uhkakuvat jokaisen mahdollisen uhkakuva sijaan ja laaditaan selkeä suunnitelma millä tavoin ja millä aikaikkunalla toimintaa voidaan jatkaa ilman turhia riskejä. Palautumiskykyä kehitetään osaltaan huolellisella laitteiston valinnalla ja vahvistamisella, vaikkakin niiden toiminnallinen ulottuvuus on vähintäänkin yhtä tärkeä. Erilaisilla testiskenaarioilla voidaan käydä henkilöstön kanssa läpi mahdollisia riskitilanteita ja rakentaa varteenotettava kyky reagoida kriisitilanteisiin mahdollisimman lyhyellä viiveellä. Kahdennetut resurssit, toimintakykyinen varalaitteisto sekä vahvistetut järjestelmät ovat lähestymistapoja yrityksen infrastruktuurin vahvistamisessa, valinta näiden toimenpiteiden väliltä tehdään kulujen ja riskien mukaan. Pelkistä teknisistä toimenpiteistä ja varmistuksista ei tosin ole hyötyä jos henkilökuntaa ei harjoiteta ja testata säännöllisesti. (Jordan & Silcock 2006,136)

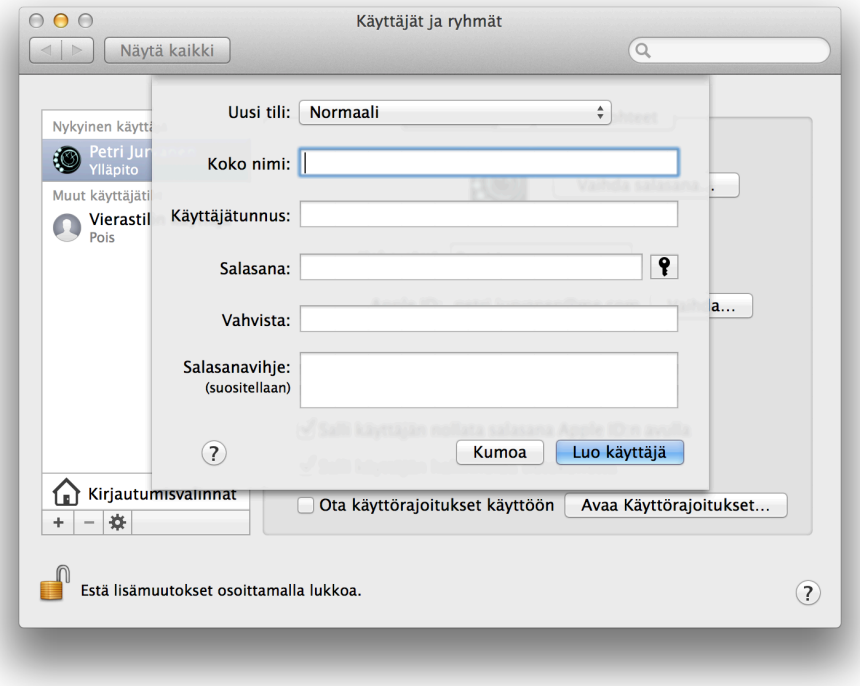
5 Tietoturva OS X:ssä

Käyttäjälle OS X -käyttöjärjestelmässä on tarjolla useita tietoturvaratkaisuja, joiden hyödyntämiseen tässä luvussa keskitytään. Perusteellista virustorjuntaa lukuun ottamatta kaikki näistä ratkaisuista ovat käyttöjärjestelmään sisäänrakennettuja ja toiminnaltaan käyttäjälle pääosin näkymättömiä mutta tarpeellisia. Jotta näistä ominaisuuksista olisi käyttäjälle ja hänen

tiedoilleen hyötyä on niiden oikeanlainen käyttö ja konfigurointi avainasemassa. Lisäksi käyttäjän tulee pitää huolta järjestelmän päivityksistä, sillä mikään tietoturvaratkaisu ei ole turvallinen jos järjestelmäpäivityksiin ei ole kiinnitetty tarvittavaa huomiota.

5.1 Käyttäjätilit ja oikeudet

OS X:ssä käyttäjätilien tyypit jakaa kuuteen erilaiseen kategoriaan, jotka ovat: ylläpitäjä, normaali, käyttörajoitusten alainen, vieras, vain jako ja juurikäyttäjä eli root joka on oletuksena poistettu käytöstä. Näistä edellä mainituista käyttörajoitusten alainen, vieras ja vain jako ovat normaali-tilityypin alakategorioita rajoitetummilla käyttöoikeuksilla ja -mahdollisuuksilla. (Kissell 2009, 62.) Käyttäjätilienhallinta ja uusien käyttäjien lisääminen järjestelmään tapahtuu järjestelmäasetuksista ”Käyttäjät ja ryhmät”- valinnan kautta. (Kuva 5)



Kuva 5: Uuden käyttäjätilin luominen

Ylläpitäjä eli Administrator on käyttäjä joka pitää huolen järjestelmän toiminnasta sekä ylläpidosta. Ylläpitäjällä on oikeudet muuttaa lähes kaikkia järjestelmän asetuksia, sekä määritellä muiden käyttäjien käyttöoikeuksia. OS X on Unix-pohjainen käyttöjärjestelmä ja siksi jokaisella koneella on oltava vähintään yksi ylläpitäjätili ja tämä luodaan jo koneen käyttöönottovaiheessa automaattisesti ensimmäisenä käyttäjänä.
Ylläpitäjätilillä on seuraavanlaisia käyttöoikeuksia:

- Asettaa itselleen juurikäyttäjän oikeudet.
- Hallinoidan kaikkien käyttäjien ohjelmia.

- Muuttaa järjestelmäasetuksia jotka koskevat koko järjestelmää ja kaikkia käyttäjiä.
- Hallinnoida käyttäjätilejä. (Kissell, 2009, 62-63)

Koska OS X:n ensimmäinen oletuksena luotu tili on ylläpitäjätili on ylläpitäjän luotava normaalikäyttäjän tili erikseen. Normaalitilin käyttöoikeuksilla voi tehdä lähes samoja asioita, kuin ylläpitäjätilillläkin, mutta muutokset järjestelmän asetuksiin koskevat ainoastaan omaa käyttäjätiliä.
Normaalitilin käyttäjä voi siis

- Avata, muokata ja poistaa omia tiedostojaan.
- Asentaa ohjelmia vain omalle käyttäjätililleen.
- Mukauttaa asetuksia omaa käyttöä varten. (OS X Mountain Lion: Create a new user account)

Käyttörajoitettu tili eli Managed account on rajoitetuilla oikeuksilla varustettu käyttäjätili. Rajoituksien hyöty korostuu esimerkiksi lapsiperheissä ja yrityskäytössä. Ylläpitäjä pystyy esimerkiksi määrittämään hyvinkin tarkasti käyttäjälle sallitut tai kielletyt sovellukset, internetin käyttöä voidaan rajoittaa joko aikarajoitteisesti tai tietyt sivustot voidaan suodattaa kokonaan käyttäjän ulottumattomiin. Lisäksi Mail-ohjelman sähköpostiviestintä voidaan sallia vain tiettyihin osoitteistoihin. Lisäksi käyttäjän yleistä tietokoneen käyttöä voidaan rajoittaa tiettyyn kokonaistuntimäärään erikseen viikonlopuille ja arkipäiville. Ylläpitäjällä on mahdollisuus valvoa käyttörajoitetun tilin käyttöä lokitiedoista joista ilmenee tiedot vierailluista verkkosivuista, yrityksistä vierailla kielletyillä sivustoilla sekä mitä sovelluksia käyttäjä on avannut. (Kissell 2009, 66)

Vierastili on tarkoitettu satunnaisia käyttäjiä varten joille ei ole tarvetta antaa pysyvää kirjautumisoikeutta tietokoneelle. Vierastilille voidaan asettaa samalla tavalla rajoituksia, kuin käyttörajoitetulle tilille ja käyttöä voidaan valvoa samoilla työkaluilla. Vierastilille kirjautumiseen ei tarvita käyttäjätunnusta eikä salasanaa. Kaikki vierastilille tallennetut tiedot poistetaan automaattisesti uloskirjautumisen yhteydessä. (OS X Mountain Lion: Set ups guest users)

Vain jako-tilin avulla voidaan päästä käsiksi tietokoneen jaettuihin resursseihin. Tällaisia resursseja ovat: Näytön jakaminen, tiedostonjako, etäkirjautuminen, Apple remote desktop-etähallintajärjestelmä sekä Apple Event-etäkomennot. Edellä mainittuja resursseja voidaan hallinnoida järjestelmäasetuksissa ”Jako”-valinnan kautta. Vain jako-tilin avulla voidaan kohdetietokoneelle kirjautua ainoastaan verkon kautta. (Kissell 2009, 66)

Kuudes ja viimeinen tilityyppi on root eli juurikäyttäjä. Juurikäyttäjän oikeudet ovat ylläpitäjän kanssa identtiset mutta muutamalla lisäominaisuudella vahvistettuna. OS X-käyttöjärjestelmä sisältää muutamia ylläpitäjiäkin koskevia turvamekanismeja, joiden avulla voidaan estää väärinkäytöksiä jos esimerkiksi ylläpitäjätili joutuu vääriin käsiin. Tiettyjä järjestelmäasetuksia muutettaessa tai uusia ohjelmia asennettaessa järjestelmä pyytää ylläpitäjää automaattisesti tunnistautumaan tilin salasanalla. Juurikäyttäjä ohittaa nämä mekanismit ja pystyy näin vapaasti muuttamaan asetuksia ja muokkaamaan tiedostoja koko järjestelmässä. Näillä rajoittamattomilla oikeuksilla juurikäyttäjä pystyy vahingoittamaan järjestelmää joko tahallisesti tai tahattomasti poistamalla esimerkiksi järjestelmän toiminnan kannalta kriittisiä kohteita. Tästä tietoturvariskistä johtuen juurikäyttäjä on oletuksena kytketty pois päältä. Normaalikäytössä juurikäyttäjää ei tarvitse koskaan kytkeä päälle sillä sen käyttäminen aiheuttaa merkittäviä tietoturvariskejä. (Enabling and using the ”root” user in Mac OS X)

Jokaisella järjestelmään luodulla käyttäjällä on oma kotikansio tietokoneen kiintolevyllä. Kotikansio sisältää tallennustilan käyttäjän henkilökohtaisille tiedostoille ja asetuksille. Kotikansiot ovat yksityisiä, käyttäjän ohella vain root-käyttäjä pystyy tarkastelemaan kansion sisältöä.

OS X- käyttöjärjestelmässä jokaisella tiedostolla tai kansiolla on omistaja jolla on tietynlaiset käyttöoikeudet kohteeseen. Järjestelmässä on käyttössä POSIX-standardin mukaiset käyttöoikeudet. POSIX-standardissa käyttäjälle on mahdollista antaa tiettyyn tiedostoon tai kansioon kolme erilaista käyttöoikeutta; read eli luku, write eli kirjoitus ja execute eli suoritus. Nämä toiminnot lyhennetään kirjaimin ”r”, ”w” ja ”x”. ”r” eli read- oikeus tarkoittaa, että käyttäjä voi avata kansion tai tiedoston ja tarkastella sen sisältöä. ”w” eli Write- toiminto antaa oikeuden muokata tai poistaa tiedoston tai kansion. ”x” eli Execute- toiminto antaa oikeuden sovelluksen käynnistämiseen ja suorittamiseen sekä uuden kansion luomiseen. (OS X Mountain Lion: Set permissions)

Käyttäjän oikeudet merkitään aina kolmen merkin joukkona ja kirjainten paikat ovat aina samat. Esimerkkinä, jos käyttäjällä on kansioon luku-, kirjoitus- ja suoritusoikeudet, merkitään käyttöoikeudet muodossa ”rwx”. Jos jonkin merkin paikalla on ”-”-merkki ei käyttäjällä ole oikeuksia kyseiseen toimenpiteeseen. (OS X Mountain Lion: Set permissions)

Kansion ja tiedoston kokonaiset käyttöoikeudet koostuvat kolmesta kolmen merkin jonosta. Edellisessä kappaleessa mainitut ”r”, ”w” ja ”x” – toiminnot ovat edelleen voimassa mutta kokonaisessa oikeusmerkinnässä ne viittaavat myös muihin käyttäjiin ja heidän oikeuksiin (Kuva 6). Ensimmäinen kolmen merkin ryhmä koskee tiedoston tai kansion omistajaa, toinen

kohteen omistavaa ryhmää ja kolmas muita käyttäjiä. Ryhmien luominen on helppo tapa antaa muille käyttäjille pääsy tiettyihin tiedostoihin. (Kissell, 2009, 53)

```
Last login: Mon Jan  6 17:05:41 on ttys000
Petri-MacBook-Pro:~ petrijurvanen$ ls -l
total 0
drwxr-xr-x   7 petrijurvanen  staff   238  8 Jou  2012 ACSP
drwxr-xr-x   4 petrijurvanen  staff   136  8 Jou 14:55 Applications
drwxr-xr-x@  8 petrijurvanen  staff   272 29 Jou 22:55 DOS
drwx------+ 26 petrijurvanen  staff   884  6 Tam 17:01 Desktop
drwx------+ 19 petrijurvanen  staff   646  6 Tam 17:08 Documents
drwx------+ 28 petrijurvanen  staff   952  4 Tam 18:18 Downloads
drwx------@ 17 petrijurvanen  staff   578  6 Tam 10:54 Dropbox
drwxr-xr-x   9 petrijurvanen  staff   306  2 Jou 19:27 Hakemus
drwxrwxrwx  15 petrijurvanen  staff   510 10 Kes  2013 Koulu
drwx------@ 66 petrijurvanen  staff  2244  2 Mar 19:43 Library
drwx------+ 10 petrijurvanen  staff   340  6 Tam 17:07 Movies
drwx------+  9 petrijurvanen  staff   306 23 Lok 08:53 Music
drwxrwxrwx  19 petrijurvanen  staff   646  6 Tam 17:01 Oppari
```

Kuva 6: Kotikansion käyttöoikeuksien tarkastaminen päätteen avulla

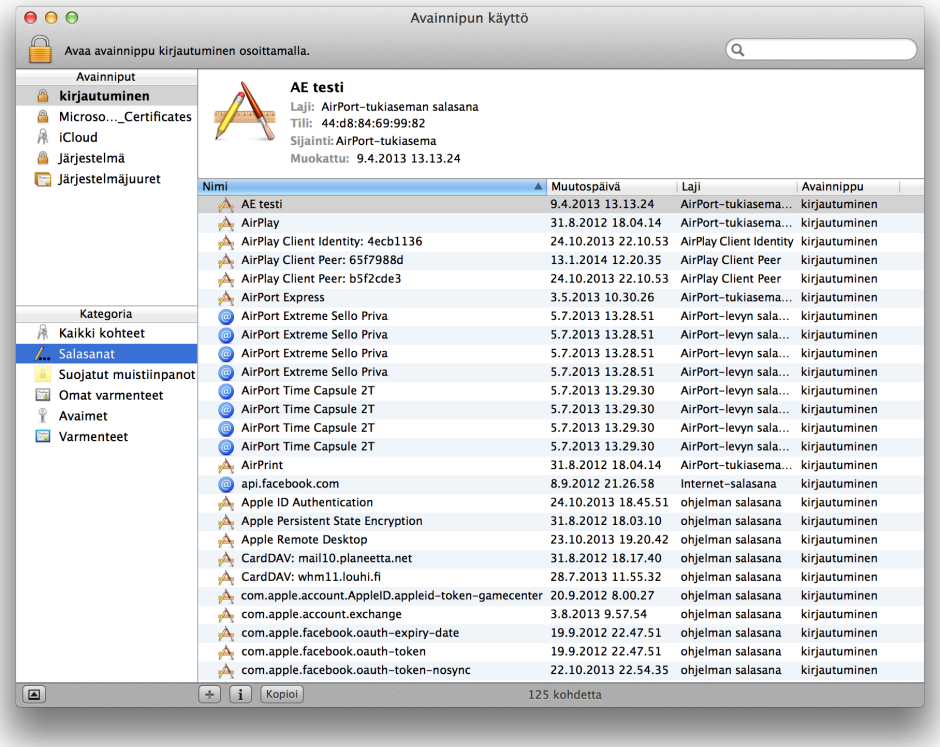
5.2 Salasanojen hallinta

Tietokoneen käyttäjälle tiedon saatavuuden ja luottamuksellisuuden varmistaminen voi olla vaikeaa. Helpoin esimerkki käyttäjälle tästä ovat esimerkiksi salasanat. Normaalilla käyttäjällä voi olla käytössään yhtäaikaisesti useita erilaisia salasanoilla suojattuja kohteita, kuten esimerkiksi: verkkopankki, tietokoneen sähköposti sekä tietokoneen käyttäjätili. Saman salasanan käyttöä samanaikaisesti kaikissa käyttäjän palveluissa ei voida pitää suositeltuna, koska tällöin ei voida turvata tietojen luottamuksellisuutta vaikka tietojen saatavuus säilyisi hyväksyttävällä tasolla. Toisaalta käytettäessä uniikkeja salasanoja on luottamuksellisuus turvattu mutta tietojen saatavuus saattaa vaarantua vaikeasti muistettavien salasanojen takia. Tätä ongelmaa voidaan helpottaa käyttämällä erillistä sovellusta salasanojen hallinnointia varten, käyttäjän salasanat tallentuvat tällaiseen ohjelmaan automaattisesti.

OS X- käyttöjärjestelmässä salasanojen hallinnointiin ja ylläpitoon voidaan käyttää sisäänrakennettu avainnippua (Kuva 7). Avainnippuun voidaan tallentaa salasanojen ohella sertifikaatteja, salausavaimia ja lomaketietoja automaattista täyttöä varten (Apple Inc. OS X Mountain Lion: About certificates). Avainnippu itsessään salataan ja suojataan salasanalla. Avainnippu mahdollistaa sen, että käyttäjän ei tarvitse muistaa kaikkia käytössään olevia salasanoja vaan ainoastaan avainnipun salasanan, jonka avulla hänellä on tarvittaessa pääsy tietyn salasanan luo. Avainnipun pääsalasanaan kannattaa kiinnittää huomiota, sillä nipun sisältämät salasanat ovat heikon pääsalasanan takana aivan yhtä haavoittuvia.

Avainnippu ei oletusasetuksilla käytettynä ole kovinkaan turvallinen. Oletuksena käyttäjän salasanat tallennetaan automaattisesti avainnippuun, joka tarkoittaa, että järjestelmään kirjautumisen jälkeen nippuun tallennetut salasanat syötetään automaattisesti niihin kuuluviin kenttiin. Tällöin avainnippu on ”auki”. Jo käyttöönottovaiheessa käyttäjän kannattaa ”Lisäohjelmat” – kansiossa sijaitsevan avainnipun hallintapaneelin kautta luoda käyttöönsä oma erillinen riittävän turvallisella eli vähintään kahdeksan merkkisellä salasanalla suojattu avainnippu ja asettaa se oletusavainnipuksi. Lisäksi asetuksista kannattaa kytkeä päälle ominaisuudet ”Lukitse 5 minuutin käyttämättömyyden jälkeen” ja ”Lukitse nukkuessa”, näin estetään ulkopuolisen pääsy avainnippuun sen ollessa auki. (White 2012, 99)

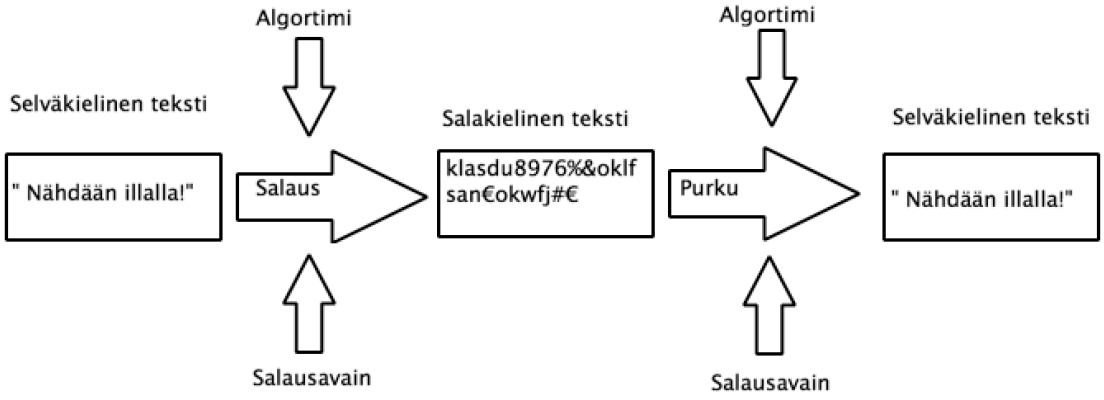
Avainnipun käyttäminen ei ole käyttäjälle pakollista, mutta oikein käytettynä avainnippu parantaa tietojen saatavuutta ilman luottamuksellisuuden vaarantumista. Avainnipun avulla kaikki käyttäjän salasanat voidaan pitää uniikkeina ja vahvoina, koska käyttäjällä on niihin vapaa ja helppo pääsy yhdellä erikseen asetetulla pääsalasanalla. Avainnippu integroituu jokapäiväiseen käyttöön huomaamattomasti ja toimiikin parhaiten Applen Safari-selaimella. (White 2012, 99)



Kuva 7: Avainnipun hallintapaneeli

5.3 Tietojen salaaminen

Edellisissä luvuissa kuvattu pääsynvalvonta on merkityksetöntä jos järjestelmä asennetaan tietokoneelle uudelleen. (Paananen 2005, 398) Tällöin käyttäjän tulee turvata kiintolevyn sisältämät tiedot salauksella eli kryptauksella. OS X-järjestelmä käyttää salauksessaan symmetristä AES-algortimia. Salauksessa selväkielinen tieto muutetaan salausalgoritmin sisältämän matemaattisen kaavan avulla sekä salausavaimella salakieliseksi tekstiksi. Salaus puretaan vastaavalla mutta käänteisellä prosessilla. Symmetrisessä salauksessa sekä viestin salaaminen, että purkaminen tapahtuu samalla salausavaimella. (Kuva 8) (Kissell 2009, 424-425)



Kuva 8: Symmetrinen salaus ja salauksen purku

OS X-järjestelmässä käyttäjän tärkeimmät tiedostot sijaitsevat käyttäjän omassa kotikansiossa. Jos käyttäjällä on käytössään kannettava tietokone ja kotikansio sisältää luottamuksellista tai salassa pidettävää tietoa on käyttäjän syytä salata kotikansion sisältö sisäänrakennetulla FileVault 2 - ominaisuudella. FileVault-ominaisuuden ollessa päällä salataan kotikansio AES-algoritmilla sekä kirjautumissalasanalla. Salauksen purku tapahtuu ilman toimenpiteitä automaattisesti tietoja käytettäessä. Kun käyttäjä on kirjautunut ulos järjestelmästä on tietoihin pääsy mahdotonta ilman kirjautumissalasanaa.

FileVaultin käyttöönottovaiheessa käyttäjän on hyvä tehdä muutamia toimenpiteitä alkuvalmisteluina. Koska kiintolevyllä olevat tiedot ovat suojattuina vain silloin, kun käyttäjä on uloskirjautuneena on käyttäjäprofiilin asetuksiin syytä tehdä muutoksia. Filevault käyttöönottopaneeli (Kuva 9) joka löytyy järjestelmäasetuksien ”Suojaus ja yksityisyys” –valikosta. Samasta valikosta kannattaa aktivoida valinnat ”Estä automaattinen sisäänkirjautuminen” sekä ”Vaadi salasana välittömästi heräämisen jälkeen tai näytönsäästäjän käynnistyttyä”. (Kissell 2009, 446) Jälkimmäisen viivettä voidaan säätää valinnasta välittömästi aina neljään tuntiin asti.

Salauksen käyttöönottovaiheessa järjestelmä luo palautusavaimen joka käyttäjän kannattaa tallettaa varmaan paikkaan tietokoneen ulkopuolelle. Palautusavainta käytetään levyn avaa-

miseen jos käyttäjä unohtaa tai hukkaa salasanansa. Jos sekä palautusavain, että salasana ovat kadonneet on levyn tiedot menetetty. Seuraavassa vaiheessa käyttöönottoavustaja tarjoaa vielä mahdollisuutta tallettaa palautusavain Applelle jolloin pääsyavain salataan ja turvataan kolmella turvakysymyksellä sekä Apple-tilin salasanalla. Edellä mainitun tiedon korruptoitumisen varalta käyttäjän on hyvä varmuuskopioida järjestelmä ennen salauksen käyttöönottoa. (OS X: About FileVault 2)

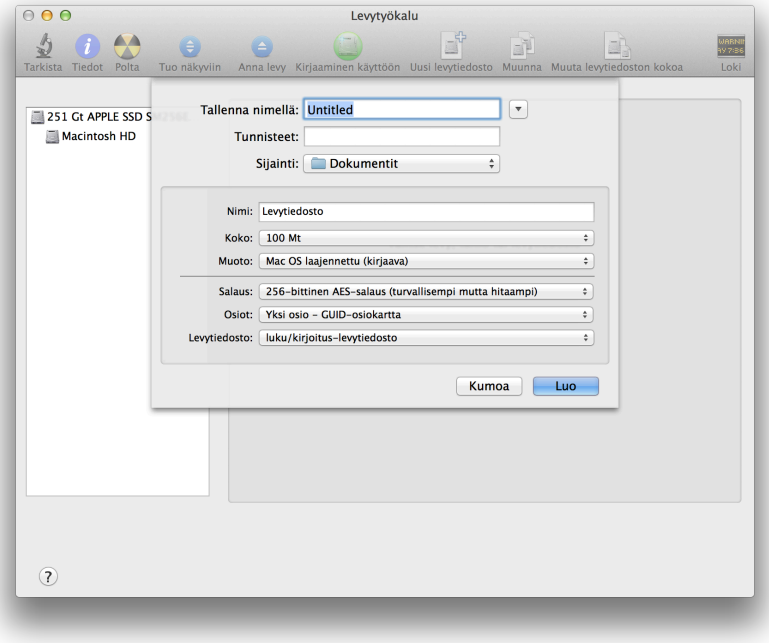
FileVaultin käyttöönotossa järjestelmä luo salatun kopion kotikansiosta ja tähän prosessiin saattaakin kulua paljon aikaa etenkin jos kotikansio sisältää paljon dataa. Prosessin alussa käyttäjän kannattaa valita suojattu poisto jolloin käyttöönottoprosessin päätyttyä järjestelmä poistaa automaattisesti alkuperäisen salaamattoman kotikansion. FileVaultilla salatun kotikansion tunnistaa helposti kassakaappikuvakkeesta. Käyttöönoton jälkeen käyttäjä ei juurikaan huomaa salauksen olemassaoloa, hidastelua saattaa esiintyä käsiteltäessä suuria tiedostoja. FileVaultissa käytettävä 128 bittinen AES-algortimi on varmuudella luotettava, kokonaisuuden suurin haittapuoli tietoturvallisuutta ajatellen on sisäänkirjautumissalasanan käyttö salausavaimena. Turvallisinta olisi käyttää kirjautumissalasanan sijaan erillistä monimutkaista salasanaa salausavaimena. Lisäksi huonona puolena on sovelluksen heikko yhteensopivuus sisäänrakennetun Time Machine- varmuuskopioinnin kanssa. Automaattiset Time Machine-varmuuskopiot voidaan ajaa ainoastaan käyttäjän ollessa uloskirjautuneena eikä käyttäjän kotikansion yksittäisiä tiedostoja voida palauttaa graafisen käyttöliittymän avulla. (OS X: About FileVault 2)

Kuva 9: FileVault käyttöönottopaneeli

Kaikille käyttäjille kotikansion salaaminen ei ole tarpeellista, mutta esimerkiksi USB-muistitikun tai yksittäisen kansion salaaminen saattaa tulla ajankohtaiseksi esimerkiksi henkilökohtaisten tietojen liikuttelussa tai työasioiden työstämisessä omalla kotikoneella. Nämä voidaan toteuttaa helposti sisäänrakennetulla levytyökalu-ohjelmalla jolla voidaan luoda salattuja levykuvia eli imageja tai alustaa USB-muistitikku salattuun muotoon.

Levytyökalu sijaitsee ohjelmakansion lisäohjelmat-kansiossa. Valitsemalla ”uusi levytiedosto” päästän ikkunaan (Kuva 10) jossa uusi levykuva voidaan nimetä sekä määrittää levykuvan koko, tallennuspaikka, muoto ja salauksen taso. Käyttäjän kannalta paras valinta levymuodoksi on harva levytiedosto, joka kasvaa sitä mukaa kun tiedostoja lisätään aina käyttäjän määrittelemään maksimiin asti. (Kissell 2009, 434) Muita muotoja ovat Applen HFS+ sekä Windowsin tukema FAT. Salaukseksi voidaan valita joko 128-bittinen tai 256-bittinen AES algortimi. Poiketen FileVaultista käyttäjä voi itse päättää salausavaimen. (How to create a password protected (encrypted) disk image)

Levykuvan luonnin jälkeen voi käyttäjä kopioida sinne valitsemiaan tiedostoja tai kansioita. Levykuva tulee avatessa näkyviin työpöydälle sekä Finderin sivupalkkiin. Kun valitut tiedostot on siirretty voi käyttäjä poistaa levykuvan näkyvistä jolloin tiedot ovat turvassa levykuvan sisällä salasanan takana. Mikäli käyttäjä säilyttää levykuvaa tietokoneen kiintolevyllä on muistettava, että sinne siirretyt tiedot ovat kopioita alkuperäisistä ja alkuperäiset kohteet on poistettava salaamattomalta levyltä jotta tiedon luottamuksellisuus säilyy.



Kuva 10: Uuden levykuvan luominen

5.4 Virustorjunta ja haittaohjelmat

Yleisimpiä tiedon eheyteen vaikuttavia uhkia käyttäjälle ovat haittaohjelmat. Haittaohjelma vaarantaa tietokoneen sisältämän tiedon eheyden saastuttaessaan kiintolevyn. Haittaohjelmia ovat sovellukset tai ohjelmat jonka tarkoituksena on tunkeutua tietojärjestelmiin ja aiheuttaa niissä vahinkoa (Barker 2010, 213). Haittaohjelma on yleisnimitys joka pitää sisällään virukset, madot, troijalaiset sekä erilaiset järjestelmien takaovet. (Paananen 2005, 387, 410-411)

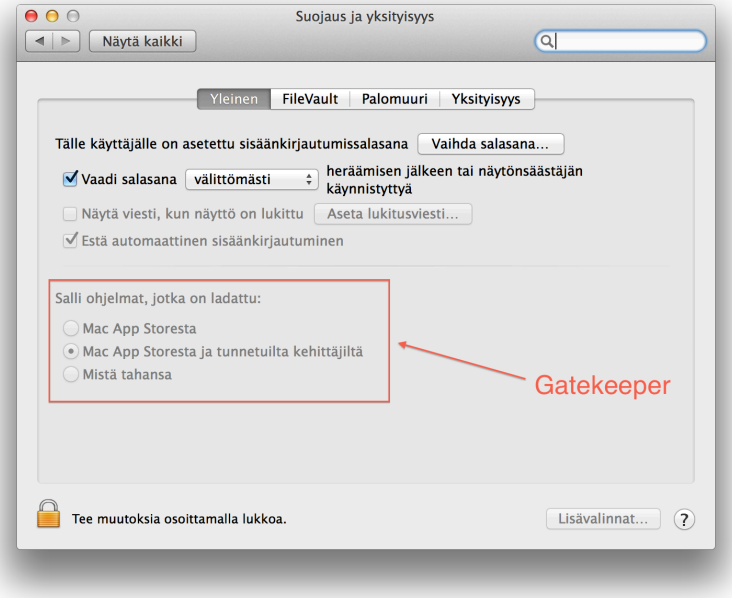
OS X –käyttöjärjestelmälle uhan aiheuttavien haittaohjelmien lukumäärä on tunnetusti pienempi, kuin kilpailevilla alustoilla. Haittaohjelmien tarkkaa lukumäärää on mahdotonta sanoa. Tietoturvatuotteita kehittävä Kaspersky kertoo verkkosivuillaan, että vuosien 2011 ja 2012 välisenä aikana tartuntahavaintojen määrä mac-tietokoneissa kasvoi 30% joista valtaosa on tarkoitettu vanhojen järjestelmäversioiden haavoittuvuuksia varten. (Mac Internet security Threats, 2014) Myös Windows-ympäristöistä tutut haittaohjelmat ovat omana riskinä OS X-järjestelmässä. Vaikka haittaohjelma ei osaisikaan aiheuttaa uhkaa OS X-käyttäjälle voi käyttäjä tietämättään levittää haittaohjelmaa eteenpäin sähköpostin tai ulkoisen tallennusmedian kautta.

OS X-järjestelmällä varustetulle tietokoneelle suurimman potentiaalisen uhan muodostavat haittaohjelmista troijalaiset. Ohjelma joka saattaa vaikuttaa harmittomalta ja jollain tasolla jopa käyttäjälle hyödylliseltä sisältääkin todellisuudessa haitallista ohjelmakoodia joka vahingoittaa järjestelmää tavalla tai toisella. (Kissell 2009, 465) Tähän mennessä merkittävin OS X-järjestelmälle suunnattu haittaohjelma on Flashback-troijalainen joka vuonna 2012 saastutti lyhyessä ajassa 600 000 mac-tietokonetta. Flashback-troijalainen käyttää hyväkseen Java-haavoittuvuutta ja valjastaa tietokoneen osaksi bottiverkostoa. (Symantec. OSX.Flashback Rises On Java Vulnerability, 2014) Toinen merkittävä ja pitkäikäinen troijalainen tunnetaan nimellä MacKeeper. Kyseinen haittaohjelma naamioituu virustorjuntaohjelmaksi ja lupaa käyttäjälle tietokoneen puhdistuksen olemattomista haittaohjelmista edullisella hinnalla. Todellisuudessa ohjelma kerää käyttäjän luottokorttitiedot ja jää kiintolevylle tekemättä yhtään mitään. Ohjelman tekijät edesauttavat ohjelman leviämistä tehokkaan hakukoneoptimoinnin avulla jolla kyseinen ohjelma saadaan hakukonetuloksissa kärkipaikalle. Verkkosivuilla vierailtaessa ohjelma latautuu käyttäjän tietokoneelle automaattisesti, mutta ei aiheuta vahinko ilman käyttäjän suorittamaa manuaalista asennusta. Kyseinen ohjelma tunnettiin aiemmin nimellä MacDefender. (The Safe Mac. Beware MacKeeper, 2014)

Paras ja samalla varmin tapa ehkäistä haittaohjelmatartuntoja on tunnetun virustorjuntaohjelmiston asentaminen tietokoneelle. Vaikka ohjelmien yleisesti puhutaan virustorjuntaohjelmistoista, pystyvät ne havaitsemaan järjestelmästä myös kaikki muut haittaohjelmat kuten troijalaiset, madot ja takaovet. Jokainen haittaohjelma on yksilöllinen sekä omaa omanlaisen tavan toimia. Virustorjuntaohjelmisto pyrkii reaaliaikaisesti tarkkailemaan tällaisia poikkeamia tietokoneen kiintolevyltä sekä saapuvasta verkkoliikenteestä. Ohjelmien virustietokanta päivittyy yleensä automaattisesti mikä tuo käyttäjälle jatkuvaa turvaa. (Kissell 2009, 471-472)

OS X -käyttöjärjestelmästä löytyy muutama alkeellinen virustorjuntaratkaisu sisäänrakennettuna. Näiden avulla voidaan tehokkaasti estää monien haitallisten ohjelmien suorittaminen. Käyttäjän ladatessa internetistä sovelluspaketin kirjoitetaan paketin metatietoihin automaattisesti tiedot lataussivusta, ajankohdasta sekä ohjelmasta jota lataukseen käytettiin. Sovelluspaketin ensimmäisellä avauskerralla järjestelmä näyttää käyttäjälle kyseiset metatiedot varoitusikkunassa, jotta käyttäjä tiedostaa onko ohjelma latautunut hänen huomaamattaan. Jos ohjelma on ladattu muualta, kuin App Storesta eikä sovellus ole Applen kehittäjälle antamaa sertifikaattia ei järjestelmä oletuksena suostu avaamaan pakettia. Tätä ominaisuutta kutsutaan nimellä Gatekeeper. (Kuva 11) (OS X: About Gatekeeper, 2014)

OS X -järjestelmä kykenee itsenäisesti tunnistamaan suppeahkon määrän haittaohjelmia suppean virustietokannan avulla. Jos järjestelmä havaitsee ajettavassa sovelluksessa haitallista ohjelmakoodia, pyytää se automaattisesti käyttäjää siirtämään tiedoston roskakoriin. (Kissell 2009, 336-337)



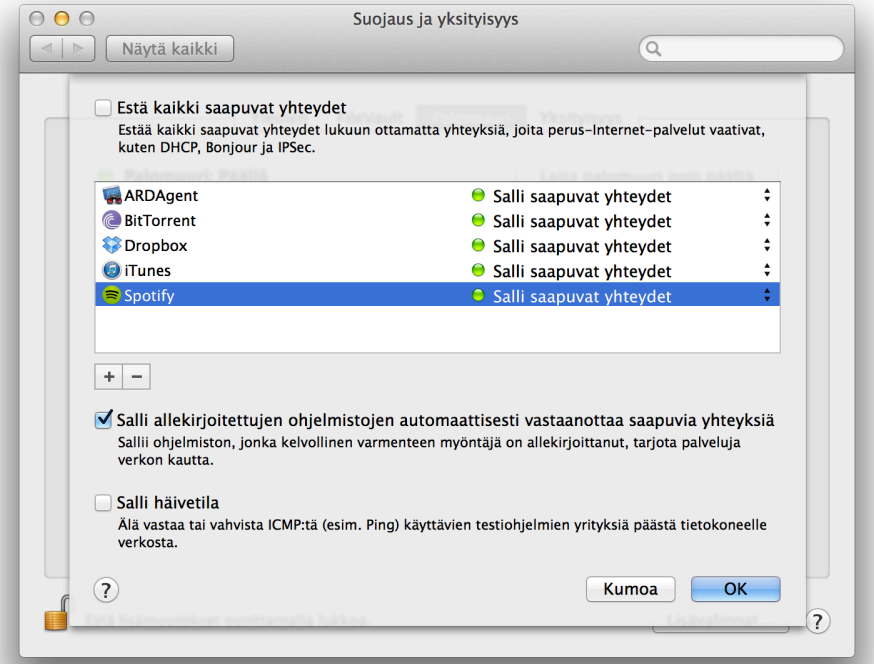
Kuva 11: Gatekeeper

5.5 Palomuuri

OS X –käyttöjärjestelmän eheyttä voidaan parantaa palomuurilla, joka valvoo tietokoneen verkkoliikennettä sekä rajoittaa sitä tarvittaessa tarkasti määriteltyjen sääntöjen mukaan. Hyvän palomuurin avulla voidaan estää erilaisten haittaohjelmien yritykset avata yhteydet haitalliselle palvelimelle. Palomuurit ovat tämän lisäksi tehokas keino tietomurtojen estämisessä. Tietojärjestelmään murtautuessaan hakkeri rikkoo välittömästi tietojärjestelmän eheyden. (Paananen 2005, 388, 403-404) Jotta turvallisuus olisi kokonaisvaltaista on palomuuri välttämätön komponentti, sillä laitteisto- tai ohjelmapohjainen palomuuri kykenee torjumaan kaikki CIA-triadin tukipilareihin kohdistuvat uhat. Eheyden ohella järjestelmään murtautunut hakkeri vaarantaa myös tietojärjestelmän sisältämien tietojen luottamukselliuuden. Palomuurin avulla voidaan näiden lisäksi estää palvelunestohyökkäykset jotka uhkaavat tietojen saatavuutta.

Käyttöjärjestelmä sisältää kaksi palomuuriratkaisua jotka poikkeavat toisistaan toimintatavaltaan sekä käytettävyydeltään. Järjestelmäasetuksien ”Suojaus ja yksityisyys” valinnan kautta hallittava sovelluskohtainen palomuuri on ominaisuuksiltaan suppea mutta käyttäjäystävällinen ja helppokäyttöinen palomuuriratkaisu. (Kuva 13) Palomuuri valvoo vain sovellustason saapuvaa verkkoliikennettä sekä sallii ja rajoittaa sitä käyttäjän määrittelemän listan mukaisesti. Oletusasetuksille asetettu palomuuri hyväksyy vain allekirjoitettujen ja luotettujen sovellusten verkkoliikenteen. Luotettuja sovelluksia ovat Applen sovellusten ohella Applen virallisesti hyväksymien kehittäjien tuottamat sovellukset. (Kissell 2009, 553) Näiden luotettujen sovellusten automaattinen salliminen voidaan tarvittaessa poistaa käytöstä. Allekirjoittamattoman sovelluksen muodostaessa yhteyttä kysytään käyttäjältä lupa yhteyden sallimiselle.

Palomuuri voidaan asettaa estämään kaikki saapuvat yhteydet jolloin saavutetaan korkein mahdollinen tietoturvallisuuden taso. Tällaisessa tilanteessa palomuuri sallii vain tärkeimmät internetpalvelut kuten DHCP-protokollan joka vastaa IP-osoitteiden jakamisesta. Samalla kytkeytyy niin sanottu häivetila eli Stealth-mode joka tekee tietokoneesta muulle verkolle näkymättömän eikä esimerkiksi vastaa toisesta tietokoneesta lähetettyyn ping-käskyyn. Häivetilalla ei ole vaikutusta saapuvan verkkoliikenteen sääntöihin joten sitä voidaan käyttää myös ilman ”Estä kaikki saapuvat yhteydet”-valintaa.



Kuva 12: Palomuurin hallintaikkuna

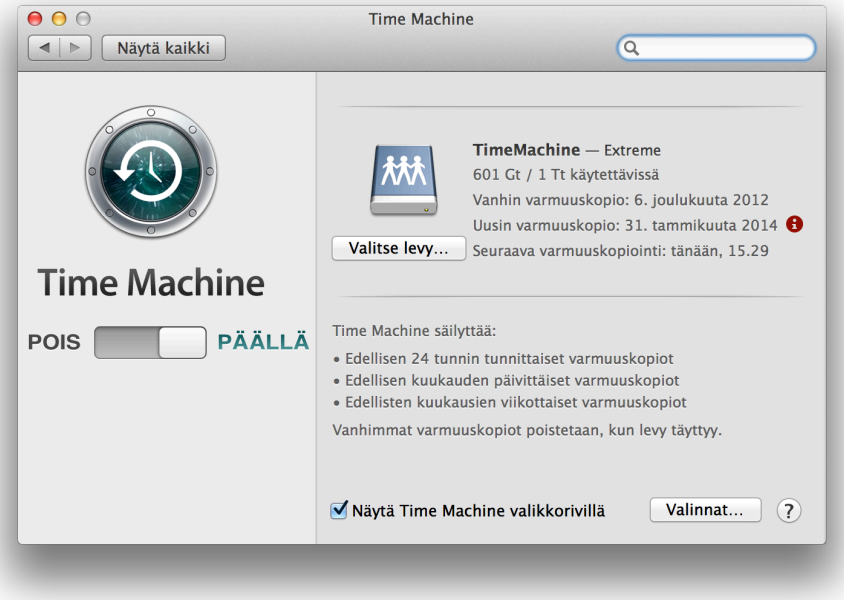
Sovelluskohtaisen palomuurin haittapuolena on sen yksinkertaisuus sekä mahdollisuus valvoa ulospäin suuntautuvaa verkkoliikennettä. Sovelluskohtainen palomuuri ei myöskään kykene seuraamaan verkkoliikennettä porttikohtaisesti. Näihin puutteisiin ratkaisuna on Unix-perinteisiin pohjutuva IPFW-palomuuri joka on oletuksena kytketty pois päältä. (Kissell 2009, 557) IPFW-palomuuria hallinnoidaan komentoriviltä, mikä tekeekin palomuurin konfiguroinnista haastavaa perehtymättömälle käyttäjälle.

5.6 Varmuuskopiointi

Tiedon saatavuuteen kohdistuva uhka voi toteutuessaan tuhota kiintolevylle tallennetun tiedon tai vaihtoehtoisesti pääsy siihen voi estyä joko hetkellisesti tai pysyvästi. Vakavimmat OS X- järjestelmän tiedon saatavuuteen liittyvät uhkia ovat fyysiset laiteviat tai varkaudet. Varkauksien todennäköisyys Mac-tietokoneelle on erityisen suuri johtuen laitteiden korkeahkosta arvosta ja tämän hetkisestä trendikkyydestä. Tästä johtuen ennaltaehkäisevät suojaustoimenpiteet ovat aina kaikkein parhaimpia vaihtoehtoja tietoturvallisuuden kannalta. Varkaustapauksien ennaltaehkäisyssä laitteen säilytyspaikkaan on kiinnitettävä erityistä huomiota. Laitevikoja voidaan estää huomioimalla ylläpitävät huoltotoimenpiteet sekä seuraamalla laitteen toimintaa käytön aikana. (Valtiovarainministeriö 2003, 46) Tässä opinnäytetyössä ei kuitenkaan ole tarkoituksena keskittyä tämän enempää tietokoneen fyysiseen turvallisuuteen tai laitteiden suojaustoimenpiteisiin.

Ainoastaan ennaltaehkäisevät toimenpiteet eivät ole riittäviä tiedon saatavuuden varmistamiseksi. Uhkakuvan toteutuessa on otettava käyttöön tietoa turvaavat toimenpiteet joista yleisin on tietojen varmuuskopiointi. Yksinkertaisesti kuvattuna varmuuskopiointi tarkoittaa tietojen kahdentamista eli kopioimista esimerkiksi ulkoiselle kiintolevylle, muistitikulle, verkkolevylle tai muulle liikuteltavalle tallennusmedialle. Alkuperäisen tiedon kadotessa tai korruptoituessa voidaan menetetty tieto helposti palauttaa varmuuskopiosta jonka jälkeen tiedon käsittely sekä työskentely voi jatkua normaalisti. Varmuuskopiointi ei välttämättä ole käyttäjälle hyödyllinen jos sitä ei ole suoritettu säännöllisesti. (Paananen 2005, 398) Lisäksi varmuuskopioinnissa on huolehdittava tallennuskohteen riittävästä tallennuskapasiteetista jottei se pääse loppumaan varmuuskopioinnin yhteydessä.

OS X -käyttöjärjestelmässä on sisäänrakennettu automaattinen varmuuskopiointitoiminto Time Machine. Käyttöönoton jälkeen Time Machine osaa suorittaa varmuuskopioinnin automaattisesti yhteensopivalle kiinto- tai verkkolevylle automaattisesti eikä näin ollen vaadi käyttäjältä minkäänlaisia lisätoimenpiteitä. Varmuuskopiointiin käytettävä levy on ennen käyttöönottoa alustettava Applen HFS+ tiedostojärjestelmämuotoon. Time Machine otetaan käyttöön järjestelmäasetuksista löytyvän hallintaikkunan avulla (Kuva 13). Hallintaikkunassa käyttäjän on mahdollista valita varmuuskopion tallennuskohde sekä kansiot joita ei haluta sisällyttää varmuuskopioon. Hallintaikkuna ilmoittaa myös mahdollisista poikkeamista automaattisesta varmuuskopiointiaikataulusta.



Kuva 13: Time Machine hallintaikkuna

Käyttöönotossa Time Machine varmuuskopio ensimmäisellä varmuuskopiokerralla koko järjestelmän ja seuraavilla kerroilla vain edellisestä varmuuskopiosta muuttuneet kohteet. Varmuuskopiointi suoritetaan kerran tunnissa ja ohjelma säilyttää kopiot kuluneelta 24 tunnilta, päivän ensimmäiset kopiot kuluneelta kuukaudelta sekä viikoittain tehtävät kopiot menneiltä kuukausilta. Tallennuslevyn täyttyessä kirjoittaa ohjelma automaattisesti uusimmat kopiot vanhimpien päälle.

Tietojen palautus tapahtuu erillisellä Time Machine-käyttöliittymällä johon pääsee siirtymään joko Time Machine kuvakkeesta joka sijaitsee Dock-palkissa tai valikkoriviltä. Käyttöliittymä tietojen palautuksessa toimii aikakoneen tavoin näyttäen tietokoneen sisällön tiettyinä ajankohtina. Sivussa olevan aikajanan avulla käyttäjän on helppo liikkua eri ajankohtien välillä. Käyttöliittymällä on mahdollista palauttaa yksittäisiä kohteita jotka on helposti löydettävissä ikkunan oikean yläkulman hakukentän avulla. Uutta konetta käyttöönotettaessa on vanhan koneen tiedot helppo siirtää uuteen Mac-tietokoneeseen Time Machine varmuuskopiosta avulla kokonaisuudessaan. (Mac Basics: Time Machine backs up your mac)

Time Machine-varmuuskopiointisovellus on suunniteltu kotikäyttäjän tarpeita ajatellen. Helpon käyttöönoton jälkeen sovellus toimii automaattisesti taustalla eikä käyttäjä juurikaan huomaa sen olemassaoloa. Käytännössä kerran tunnissa suoritettava varmuuskopio käyttäjän kotikansiosta ei vie muutamaa minuuttia kauempaa eikä näin ollen syö koneen resursseja käyttäjää häiritsevästi. Juuri ohjelman yksinkertaisuus ja helppokäyttöisyys on seurausta edistyneempien varmuuskopiointitoimintojen puutteesta. Yrityskäytössä Time Machine ei yksistään ole riittävä varmuuskopiointiratkaisu mutta toimiva yhtenä osana tiedon saatavuuden varmistamisessa. Suositeltavaa on, että Järjestelmälevystä tehdään Time Machine-varmuuskopion ohella klooni eli identtinen kopio ulkoiselle medialle säännöllisin väliajoin jotta tiedon varmistus olisi kahdessa erillisessä paikassa ja kahdella erilaisella tavalla toteutettuna.

6 Työn arviointi

Konstruktiivisen tutkimuksen teorian kehittämisen mahdollisuudet ovat joko uuden teorian ja toimintatavan kehittäminen, olemassa olevan teorian kehittäminen, testaus ja havainnollistaminen. Teorian jalostaminen on konstruktiivisen tuktkimuksen tyypillisin teoreettinen saavutus. Jos konstruktio havaitaan toimivaksi alkuperäisessä ympäristössään, tuottaa se lisäarvoa aiempaan teoriaan verrattuna. Konstruktioon tulisi asennoitua uutena ja käytännöllisenä keinona tietyn päämäärän saavuttamisessa. (Henttonen ym. 2006, 118-119.)

Tämän opinnäytetyön tarkoituksena oli toteuttaa tietoturvaopas Tekninen toimisto Tektorin asiakkaille. Vaikka tietoturvaopas on suunnattu Mac-käyttäjille oli yritykselle tärkeää, että se

on luettavissa myös muilla Applen laitteilla. Edellä mainituista syistä ohjeistuksen formaatin valinnassa päädyttiin sähköiseen iBooks-versioon, tämä mahdollistaa oppaan jakamisen asiakkaille myös PDF-muodossa sähköpostin liitteenä.

Oppaan sisältöä kartoitettaessa käytettiin yhtenä tiedonhankintametodina valituille asiakkaille toteutettua teemahaastattelua. Näitä haastatteluja arvioitaessa kävi ilmi etteivät asiakkaat suoranaisesti tienneet millaisia asioita haluaisivat tämäntyyppisessä oppaassa käsiteltävän ja millä tavalla. Tarve oppaalla silti oli ja asiakkailta tuli toive sen pikaisesta valmistumisesta. Oppaan sisältöä suunniteltaessa paras näkökulma tuli kollegoilta jotka työskentelevät asiakasrajapinnassa päivittäin. Nämä sisältöä koskevat näkemykset syntyivät vapaissa ryhmäkeskusteluissa.

Kehitetyn konstruktion sisältö on pyritty suunnittelemaan asiakkaalle mahdollisimman helppolukuiseksi ja jokaisen osa-alueen alussa on info-laatikko josta asiakkaan on helppo saada selkeä kuva aiheesta jota kyseisessä luvussa käsitellään. Käytännön esimerkit henkilökohtaistavat näiden lukujen sisältöä jolloin asiakkaan on helppo samaistua tilanteeseen ja samalla omaksua käsiteltävä aihealue.

Tekninen toimisto Tektor on lanseerannut maaliskuun alussa kurssipaketteja joissa asiakkaille on tarjolla koulutusta niin ryhmässä, kuin yksityisestikin. Tässä opinnäytetyössä suunniteltu opas tulee olemaan kyseisillä kursseilla oheismateriaalina sekä osana uusien työntekijöiden koulutusprosessia.

Tietoturvaopasta tullaan tulevaisuudessa personoimaan yrityksen näköiseksi. Sähköinen opas on helppo pitää ajan tasalla uusien järjestelmäpäivitysten yhteydessä sekä mahdollistaa oppaan jatkokehityksen asiakkaiden toiveiden perusteella helposti. Yritykselle ei myöskään pääse syntymään turhia paino- eikä varastointikuluja uusien versioiden yhteydessä.

Opas on tässä muodossaan kerännyt asiakkailta kehuja ja sitä on testattu uuden kurssituotteen pilotoinnin yhteydessä maaliskuussa 2014. Kehitysehdotuksia on oppaaseen liittyen tullut sekä asiakkailta, että kollegoilta ja oppaan jatkokehitystä varten laaditaan kehityssuunnitelma kevään 2014 aikana.

Lähteet

Alasilta, A. 1999. Näin kirjoitat tehokkaasti. Viestintäopas työelämän kirjoittajille. Tampere: Tammer-Paino.

Apple and the environment. Apple inc. viitattu 06.01.2014.
http://www.apple.com/environment/

How to create a password protected (encrypted) disk image. Apple Inc. Viitattu 22.02.2104
http://support.apple.com/kb/HT1578

Enabling and using the ”root” user in Mac OS X. Apple Inc. Viitattu 20.3.2014
http://support.apple.com/kb/HT1528

iBooks Author-ohje. Apple inc. Viitattu 06.01.2014
http://help.apple.com/ibooksauthor/mac/?lang=fi

iBooks Author: Julkaistun kirjan päivittäminen iBooks Storessa. Apple Inc. Viitattu 11.3.2014
http://support.apple.com/kb/HT5213?viewlocale=fi_FI

iBooks Autor: Kirjan julkaiseminen iBooks Storessa. Apple Inc. Viitattu 12.3.2014
http://support.apple.com/kb/PH12101?viewlocale=fi_FI

Mac Basics: Time Machine backs up your mac. Apple Inc. Viitattu 24.2.2014
http://support.apple.com/kb/HT1427?viewlocale=en_US

OS X: About Gatekeeper. Apple Inc. Viitattu 23.2.2014
http://support.apple.com/kb/ht5290

OS X: About FileVault 2. Apple inc. Viitattu 22.2.2014
http://support.apple.com/kb/ht4790

OS X Mountain Lion: About certificates. Apple Inc. Viitattu 24.2.2014
http://support.apple.com/kb/PH10967

OS X Mountain Lion: Create a new user account. Apple Inc. Viitattu 20.3.2014
http://support.apple.com/kb/PH11468

OS X Mountain Lion: Set permissions. Apple Inc. Viitattu 20.3.2014
http://support.apple.com/kb/PH10669

OS X Mountain Lion: Set up guest users. Apple Inc. Viitattu 20.3.2014
http://support.apple.com/kb/PH11321

White, K. 2012. Apple Pro Training Series: OS X Lion Support Essentials. Peachpit Press

Barker, W., Edge, C., Hunter, B. & Sullivan, G. 2010. Enterprise Mac Security: Mac OS X Snow Leopard. New York: Apress.

Hakkarainen, A: Applen uusi e-kirjajärjestelmä vaikuttaa loistavalta, mutta kätkee sisälleen synkkiä yksityiskohtia. 2012. Viitattu 06.01.2014
http://www.klaava.fi/Kirjat/Applen_uusi_e_kirjaj_rjestelm_vaikuttaa_loistavalta_mutta_k_tkee_sis_lleen_synkki_yksityiskohti

Henttonen, E. Kaakkuri-Knuuttila, M-L. Rolin, K. 2006. Soveltava yhteiskuntatiede ja filosofia. Hakapaino Oy. Helsinki

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. 15. painos, 2009. Tammi. Helsinki.

Jordan, E & Silcock, L. 2006. Strateginen IT-riskien hallinta. Helsinki: Edita.

Järvinen, P. 2002. Tietoturva & yksityisyys. 2.painos, Jyväskylä: Docendo.

Järvinen, P. & Järvinen, A. 2011. Tutkimustyön metodeista. Opinpajan kirja.

Kaspersky Lab. Mac Internet security Threats. Viitattu 23.2.2014
http://usa.kaspersky.com/internet-security-center/threats/mac

Kauppinen, A. Nummi, J. & Savola, T. 2006. Tekniikan viestintä. Kirjoittamisen ja puhumisen käsikirja. Helsinki: Edita Prima.

Kissell, J. 2009. Mac Security Bible. Indianapolis: Wiley.

Kurkela, R. Tilastollinen tiedonkeruu. Tilastokeskus. Viitattu 15.11.2013
http://www.stat.fi/virsta/tkeruu/04/03/

Paananen, J. 2005. Tietotekniikan peruskirja. 1.painos, Jyväskylä: Docendo.

The Safe Mac. Beware MacKeeper. Viitattu 23.2.2014
http://www.reedcorner.net/?p=245

Symantec. OSX.Flashback Rises On Java Vulnerability. Viitattu 23.2.2014
http://www.symantec.com/connect/blogs/osxflashback-rises-java-vulnerability

Valtiovarainministeriö. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. 2003. Viitattu 24.2.2014
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf

Kuvat

Liitteet

Liite 1: OS X tietoturva-opas

PETRI JURVANEN

OS X Tietoturva

KUINKA TEHDÄ MACISTA TURVALLISEMPI

2014

OS X Tietoturva

OS X -käyttöjärjestelmässä on tarjolla useita tietoturvaratkaisuja, joiden hyödyntämiseen tässä oppaassa keskitytään. Perusteellista virustorjuntaa lukuun ottamatta kaikki näistä ratkaisuista ovat käyttöjärjestelmään sisäänrakennettuja ja toiminnaltaan käyttäjälle pääosin näkymättömiä mutta tarpeellisia.

CIA-Triadi

CIA-triadi = Confidentiality, Integrity, Availability (luottamuksellisuus, eheys sekä saatavuus)

- Tietoturvallisuudessa tiedonkäsittelyn perusjaottelu
- Luottamuksellisuus liittyy oikeuksiin tiedon käsittelyssä
- Eheys liitty tiedon paikkansapitävyyteen
- Saatavuus liittyy tiedon mahdolliseen palauttamiseen ongelmatilanteissa

Luottamuksellisuus

Luottamuksellisuudessa olennaista on määritellä ja rajata pääsyoikeudet yrityksen tietoihin sekä dataan jotka liittyvät sen liiketoimintaan, asiakkaisiin ja työntekijöihin. Jos luottamuksellisuutta ei voida toteuttaa vaaditulla tavalla voi suojattavaa tietoa sisältävä kohde olla sellaisten henkilöiden ulottuvilla, joilla ei ole kohteen käsittelyyn vaadittavia oikeuksia. Tietojen jakamista ja käyttöä voidaan rajata luomalla käyttöjärjestelmään riittävän vahvalla salasanalla sekä yksilöllisillä käyttöoikeuksilla suojattuja käyttäjätilejä.

Tiedon luottamuksellisuuden takaamiseksi käyttäjäprofiilien, -tunnusten ja vahvojen salasanojen ohella voidaan esimerkiksi käyttää tietojen rajoittamista vain tiettyihin verkkoihin ja tietokoneisiin, sekä fyysisiä pääsynrajoituksia kuten suljettuja laite- ja työskentelytiloja. Koska mikään yksittäinen suoja ei ole täydellinen, rakentavat järjestelmien ylläpitäjät usein monia suojauskerroksia väärinkäytösten havaitsemiseksi sekä niiltä suojautumiseksi.

Eheys

Millä toimenpiteillä loppukäyttäjä voi varmistaa, että sen omistama tieto-omaisuus ei ole korruptoitunut tahallisesti tai tahattomasti? Tieto-omaisuuden turmeleminen tai sen osan hävittäminen voi olla keino häivyttää jäljet luvattomasta käynnistä yrityksen tietovarastolla. Esimerkkinä henkilökohtaisesta hyödystä tiedon

vääristämisestä ovat esimerkiksi omien palkkatietojen muuttelu yrityksen tietokantaan josta palkat maksetaan tai opiskelijan arvosanatietojen väärentäminen. Tietojen tahaton häviäminen on yleensä seuraus seuraavista asioista:

- Laiteviat esimerkiksi kiintolevyn rikkoutuminen tai tietoliikenneviat
- Ohjelmistoviat
- Infrastruktuuria kohdanneet häiriöt, esimerkiksi sähkökatkokset
- Käyttäjää ohjaavat viestit, esimerkiksi ”Tätä toimintoa ei voi keskeyttää” tai ”varmuuskopioi ennen kuin jatkat”

Tyypillisiä toimenpiteitä tieto-omaisuuden eheyden varmistamiskeksi ovat esimerkiksi hyvin vikasietoiset järjestelmät ja etenkin niiden peilatut levyt, järjestelmän lokitiedostot, varmuuskopiot, tiedon tarkistussummat, kirjausketjut sekä palautuksen testaus. Luvattoman käytön ja tunkeutumisen havaitseminen on toinen erittäin tärkeä osa eheyden varmistuksessa. Tietojen oikeellisuuden palautus voi muodostua erittäin kalliiksi operaatioksi tiedon eheyden menetyksen jälkeen.

Saatavuus

Tietokoneista ei ole käyttäjälle paljoakaan hyötyä elleivät myös niiden sisältämät tiedot ole käytettävissä niitä tarvittaessa. Tiedostojen varmuuskopiointi onkin käyttäjän elintärkein toimenpide saatavuuden varmistamisessa toimintaa turvaavan tekniikan ohella, kuten esimerkiksi UPS-laite sähkökatkojen varalta. Tietojen saatavuus voi aiheuttaa käyttäjälle yllättäviäkin ongelmia. käyttäjä saattaa tarvita tiedostoja tai valokuvia jotka on luotu esimerkiksi 10 vuotta sitten. Vaikka itse tiedostot on asianmukaisesti varmistettu saattaa ongelmaksi muodostua tiedostojen avaaminen ja hyödyntäminen. Yhteensopivia sovelluksia ei välttämättä enää ole tallessa tai saatavilla tai ne eivät enää toimi uusissa laitteissa.

Käyttäjätilit ja oikeudet

Oikeat käyttöoikeudet jokaiseen tarpeeseen

- Tietokoneen pääkäyttäjälle sopivin käyttäjätilityyppi on Ylläpitäjä (Administrator)
- Tietokoneen muille käyttäjille useimmiten sopivin valinta on Normaalikäyttäjä
- Lapsille on mahdollista asettaa Rajoitettu-käyttäjätili jossa voidaan rajoittaa tietokoneen käyttöä ajan-, verkkosivujen tai sovellusten mukaan
- Satunnaisia vieraita varten on mahdollista tehdä Vierastili jonka sisältämät tiedot poistetaan automaattisesti uloskirjautumisen yhteydessä

OS X:ssä käyttäjätilien tyypit voidaan jakaa kuuteen erilaiseen kategoriaan, jotka ovat: ylläpitäjä, normaali, käyttörajoitusten alainen, vieras, vain jako ja juurikäyttäjä eli root joka on oletuksena poistettu käytöstä. Näistä edellä mainituista käyttörajoitusten alainen, vieras ja vain jako ovat normaali-tilityypin alakategorioita rajoitetummilla käyttöoikeuksilla ja –mahdollisuuksilla. Käyttäjätilienhallinta ja uusien käyttäjien lisääminen järjestelmään tapahtuu järjestelmäasetuksista ”Käyttäjät ja ryhmät”- valinnan kautta.

Ylläpitäjä eli Administrator on käyttäjä joka pitää huolen järjestelmän toiminnasta. Ylläpitäjällä on oikeus muuttaa lähes kaikkia järjestelmän asetuksia, sekä määritellä muiden käyttäjien käyttöoikeuksia. OS X on Unix-pohjainen käyttöjärjestelmä ja siksi jokaisella koneella on oltava vähintään yksi ylläpitäjätili ja tämä luodaan jo koneen käyttöönottovaiheessa automaattisesti ensimmäisenä käyttäjänä. Ylläpitäjätilillä on seuraavanlaisia käyttöoikeuksia:

- Asettaa itselleen juurikäyttäjän oikeudet
- Hallinoidan kaikkien käyttäjien ohjelmia
- Muuttaa järjestelmäasetuksia jotka koskevat koko järjestelmää ja kaikkia käyttäjiä
- Hallinnoida käyttäjätilejä

Koska OS X:n ensimmäinen oletuksena luotu tili on ylläpitäjätili on ylläpitäjän luotava normaalikäyttäjän tili erikseen. Normaalitilin käyttöoikeuksilla voi tehdä lähes samoja asioita, kuin ylläpitäjätilillläkin, mutta järjestelmän muutosoikeudet koskevat ainoastaan omaa tiliä.

Normaalitilin käyttäjä voi siis

- Avata, muokata ja poistaa omia tiedostojaan
- Asentaa ohjelmia vain omalle käyttäjätililleen
- Mukauttaa asetuksia omaa käyttöä varten

Käyttörajoitettu tili eli Managed account on nimensä mukaisesta rajoitetuilla oikeuksilla asetettu käyttäjätili. Rajoituksien hyöty konkretisoituu esimerkiksi lapsiperheissä ja yrityksissä. Ylläpitäjä pystyy esimerkiksi määrittämään käyttäjälle sallitut ja kielletyt sovellukset, internetin käyttöä voidaan rajoittaa joko aikarajoitteisesti tai tietyt sivustot voidaan suodattaa kokonaan käyttäjän ulottumattomiin. Lisäksi Mail-ohjelman sähköpostiviestintä voidaan sallia vain tiettyihin osoitteistoihin. Lisäksi käyttäjän yleistä tietokoneen käyttöä voidaan rajoittaa tiettyyn kokonaistuntimäärään erikseen viikonlopuille ja arkipäiville. Ylläpitäjällä on mahdollisuus valvoa käyttörajoitetun tilin käyttöä lokitiedoista joista ilmenee tiedot vierailluista verkkosivuista, yrityksistä vierailla kielletyillä sivustoilla sekä mitä sovelluksia käyttäjä on avannut.

Vierastili on tarkoitettu satunnaisia käyttäjiä varten joille ei ole tarvetta antaa pysyvää kirjautumisoikeutta tietokoneelle. Vierastilille voidaan asettaa samalla tavalla rajoituksia, kuin käyttörajoitetulle tilille ja käyttöä voidaan valvoa samoilla työkaluilla. Vierastilille kirjautumiseen ei tarvita käyttäjätunnusta eikä salasanaa. Kaikki vierastilille tallennetut tiedot poistetaan automaattisesti uloskirjautumisen yhteydessä.

Vain jako-tilin avulla voidaan päästä käsiksi tietokoneen jaettuihin resursseihin. Tällaisia resursseja ovat: Näytön jakaminen, tiedostonjako, etäkirjautuminen, Apple remote desktop-etähallintajärjestelmä sekä Apple Event-etäkomennot. Edellä mainittuja resursseja sekä niihin oikeutettuja käyttäjiä voidaan hallinnoida järjestelmäasetuksissa ”Jako”-valinnan kautta. Vain jako-tilin avulla voidaan kohdetietokoneelle kirjautua ainoastaan verkon kautta etänä.

Kuudes ja viimeinen tilityyppi on root eli juurikäyttäjä. Juurikäyttäjän oikeudet ovat ylläpitäjän kanssa identtiset mutta muutamalla lisäominaisuudella vahvistettuna. OS X-käyttöjärjestelmä sisältää muutamia ylläpitäjiäkin koskevia turvamekanismeja, joiden avulla voidaan estää väärinkäytöksiä jos esimerkiksi ylläpitäjätili joutuu vääriin käsiin. Tiettyjä järjestelmäasetuksia muutettaessa tai uusia ohjelmia asennettaessa järjestelmä pyytää ylläpitäjää automaattisesti tunnistautumaan tilin salasanalla. Juurikäyttäjä ohittaa nämä mekanismit ja pystyy näin vapaasti muuttamaan asetuksia ja

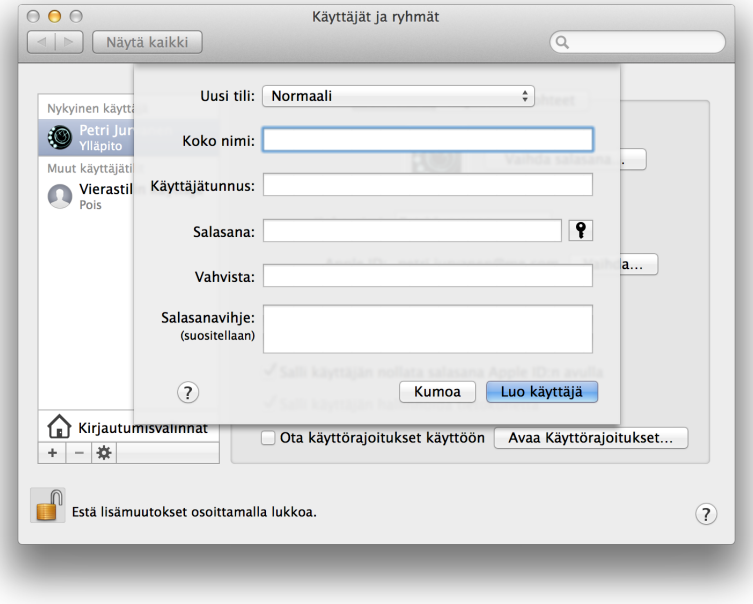
muokkaamaan tiedostoja koko järjestelmässä. Näillä rajoittamattomilla oikeuksilla juurikäyttäjä pystyy vahingoittamaan järjestelmää tahallisesti tai tahattomasti poistamalla esimerkiksi järjestelmän toiminnan kannalta kriittisiä tiedostoja. Tästä tietoturvariskistä johtuen juurikäyttäjä on oletuksena kytketty pois päältä. Normaalikäytössä juurikäyttäjää ei tarvitse koskaan kytkeä päälle sillä sen käyttäminen aiheuttaa huomattavia tietoturvariskejä.

Jokaisella järjestelmään käyttäjätilin tehneellä on oma kotikansio tietokoneen kiintolevyllä. Kotikansio sisältää tallennustilan käyttäjän henkilökohtaisille tiedostoille ja asetuksille. Kotikansiot ovat pääosin yksityisiä ja vain root-käyttäjä pystyy tarkastelemaan kansioiden sisältöä käyttäjän ohella.

OS X- käyttöjärjestelmässä jokaisella tiedostolla ja kansiolla on omistaja ja tietynlaiset käyttöoikeudet yksityiskohtaisesti. Järjestelmä seuraa POSIX-standardin mukaisia käyttöoikeuksia. POSIX-standardissa käyttäjälle voidaan tiettyyn tiedostoon tai kansioon antaa kolme erilaista käyttöoikeutta; read eli luku, write eli kirjoitus ja execute eli suoritus. Nämä toiminnot lyhennetään kirjaimin ”r”, ”w” ja ”x”. Read- oikeus tarkoittaa, että käyttäjä voi avata kansion tai tiedoston ja tarkastella sen sisältöä. Write- toiminto antaa oikeuden muokata tai poistaa tiedoston tai kansion. Execute- toiminto antaa oikeuden sovelluksen käynnistämiseen ja suorittamiseen sekä uuden kansion luomiseen.

Käyttäjän oikeudet merkitään aina kolmen merkin joukkona ja kirjainten paikat ovat aina samat. Esimerkkinä, jos käyttäjällä on kansioon luku-, kirjoitus- ja suoritusoikeudet, merkitään käyttöoikeudet muodossa ”rwx”. Jos jonkin merkin paikalla on ”-”-merkki ei käyttäjällä ole oikeuksia kyseiseen toimenpiteeseen.

Kansion ja tiedoston kokonaiset käyttöoikeudet koostuvat kolmesta kolmen merkin joukosta. Edellisessä kappaleessa mainitut ”r”, ”w” ja ”x” – toiminnot ovat edelleen voimassa mutta kokonaisessa oikeusmerkinnässä ne viittaavat myös muihin käyttäjiin ja heidän oikeuksiin. Ensimmäinen kolmen merkin ryhmä koskee tiedoston tai kansion omistajaa, toinen tiedoston tai kansion omistavaa ryhmää ja kolmas kaikkia muita käyttäjiä. Ryhmien luominen on kätevä tapa antaa tietyille henkilöille pääsy tiettyihin tiedostoihin.



Salasanojen hallinta

Avainnippu salasanojen suojana

- Kaikki käyttäjän salasanat turvassa salatussa avainnipussa
- Helppo pääsy yhdella salasanalla
- mahdollistaa jokaiseen verkko- tai sähköpostipalveluun uniikin ja monimutkaisen salasanan
- Automaattinen integraatio verkkoselaimen kanssa
- Ei riitä ainoaksi säilytyspaikaksi salasanoille

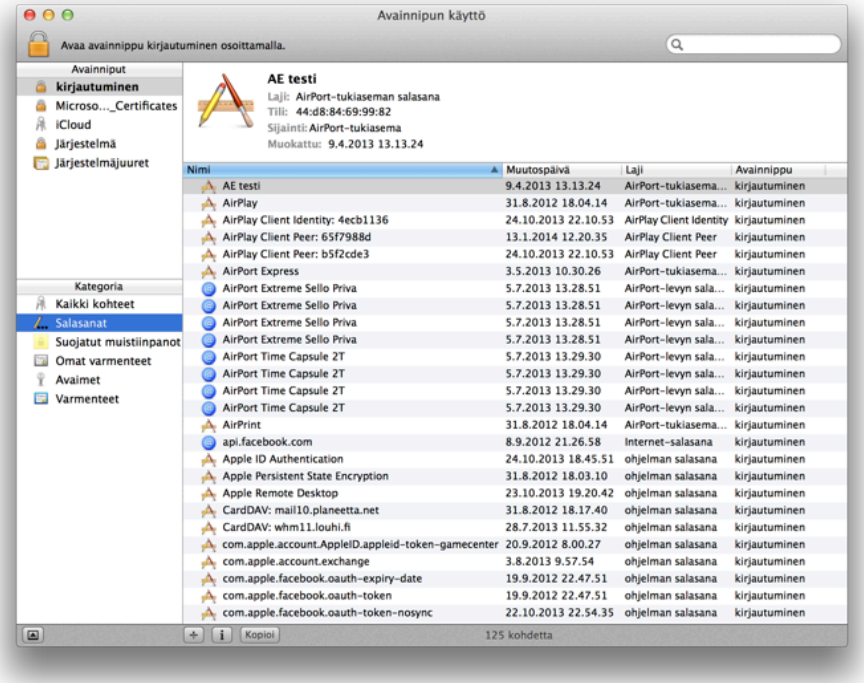
Kotikäyttäjälle tietojen saatavuuden ja luottamuksellisuuden varmistaminen voi olla vaikeaa. Konkreettisin esimerkki tästä ovat esimerkiksi salasanat. Normaalilla kotikäyttäjällä voi olla käytössä useita salasanoilla suojattuja kohteita, kuten esimerkiksi: käyttäjätili, erilaiset verkkopalvelut ja sähköposti. Saman salasanan käyttöä kaikissa palveluissa ei voida pitää suositeltuna, koska tällöin ei voida turvata tietojen luottamuksellisuutta vaikka tietojen saatavuus säilyisi hyvällä tasolla. Toisaalta käytettäessä uniikkeja salasanoja on luottamuksellisuus turvattu mutta tietojen saatavuus saattaa vaarantua vaikeasti muistettavien salasanojen takia. Tätä ongelmaa voidaan helpottaa käyttämällä salasanojenhallintaan keskittyvää ohjelmaa jonne salasanat tallentuvat automaattisesti.

OS X- käyttöjärjestelmässä salasanojen hallinnointiin ja ylläpitoon voidaan käyttää sisäänrakennettu avainnippua. Avainnippuun voidaan tallentaa salasanojen ohella sertifikaatteja, salausavaimia ja lomaketietoja. Avainnippu itsessään salataan ja suojataan salasanalla. Tämä mahdollistaa sen, että käyttäjän ei tarvitse muistaa kaikkia käyttämiään salasanoja vaan ainoastaan avainnipun salasanan, jonka avulla hänellä on tarvittaessa pääsy tietyn salasanan luo. Avainnipun pääsalasanaan kannattaa kiinnittää huomiota, sillä nipun sisältämät salasanat heikoin pääsalasanan alla aivan yhtä heikkoja.

Avainnippu ei oletusasetuksilla käytettynä ole kovinkaan turvallinen. Oletuksena käyttäjän salasanat tallennetaan automaattisesti avainnippuun, joka tarkoittaa, että

järjestelmään kirjautumisen jälkeen nippuun tallennetut salasanat syötetään automaattisesti niihin kuuluviin kenttiin. Tällöin avainnippu on niin sanotusti auki. Jo käyttöönottovaiheessa käyttäjän kannattaa ”Lisäohjelmat” – nimisessä kansiossa sijaitsevan avainnipun hallintapaneelin kautta luoda käyttöönsä oma erillinen riittävän turvallisella eli vähintään kahdeksan merkkisellä salasanalla varustettu avainnippu ja asettaa se oletusavainnipuksi. Lisäksi asetuksista kannattaa kytkeä päälle ominaisuudet ”Lukitse 5 minuutin käyttämättömyyden jälkeen” ja ”Lukitse nukkuessa”, näin estetään riski jolloin avainnipun ollessa auki on nipun salasanoihin vapaa pääsy.

Avainnipun käyttäminen ei ole käyttäjälle pakollista, mutta oikein käytettynä ja konfiguroituna parantaa avainnippu tietojen saatavuutta ilman luottamuksellisuuden vaarantumista. Avainnipun avulla kaikki käyttäjän salasanat voidaan pitää uniikkeina ja vahvoina, koska käyttäjällä on niihin vapaa ja helppo pääsy yhdellä pääsalasanalla. Avainnippu integroituu jokapäiväiseen käyttöön huomaamattomasti ja toimiikin parhaiten Applen Safari-selaimella.



Tietojen salaaminen

Tietojen salaamisen edut ja haitat

- Turvaa henkilökohtaiset tietosi laitteen kadotessa
- Estää laitteen käytön varkaustapauksissa
- Levykuvan luonnilla voidaan salata vain tietyt kansiot tai tiedostot
- Unohdettu salasana estää käyttäjää pääsemästä tietoihinsa käsiksi
- Kiintolevyn rikkoutuessa riski tietojen menetyksestä kasvaa

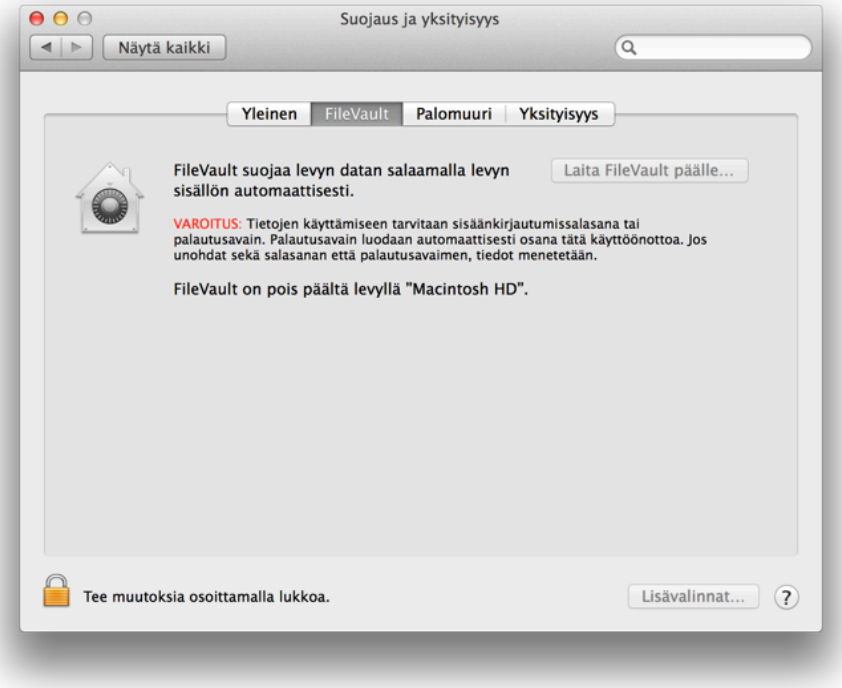
OS X-järjestelmä käyttää salauksessaan pääasiassa symmetristä salaus AES-algortimia. Salauksessa selväkielinen tieto muutetaan salausalgoritmin sisältämän matemaattisen kaavan avulla sekä salausavaimella salakieliseksi tekstiksi. Salaus puretaan vastaavalla mutta käänteisellä prosessilla. Symmetrisessä salauksessa sekä tiedon salaus, että purku tapahtuu käyttäen samaa salausavainta .

Järjestelmän käyttäjän tärkeimmät tiedostot sijaitsevat käyttäjän kotikansiossa. Jos käyttäjällä on käytössään kannettava tietokone ja kotikansio sisältää luottamuksellista tietoa on käyttäjän syytä harkita kotikansion salaamista sisäänrakennetun FileVault 2 ominaisuuden avulla. FileVault-ominaisuuden ollessa päällä salataan kotikansio AES-algoritmilla sekä kirjautumissalasanalla. Salauksen purku tapahtuu ilman toimenpiteitä automaattisesti tietoja käytettäessä. Kun käyttäjä on kirjautunut ulos järjestelmästä on tietoihin pääsy mahdotonta ilman kirjautumissalasanaa.

FileVaultin käyttöönottovaiheessa käyttäjän on hyvä tehdä muutamia toimenpiteitä alkuvalmisteluina. Kiintolevyllä olevat tiedot ovat suojattuna vain silloin, kun käyttäjä on uloskirjautuneena on käyttäjäprofiilin asetuksiin syytä tehdä muutoksia. Järjestelmäasetuksien ”Suojaus ja yksityisyys” –valikon kautta kannattaa aktivoida ”Estä automaattinen sisäänkirjautuminen” ja ”Vaadi salasana välittömästi heräämisen jälkeen tai näytönsäästäjän käynnistyttyä”. Jälkimmäisen viivettä voidaan säätää valinnasta välittömästi aina neljään tuntiin asti.

Salauksen käyttöönottovaiheessa järjestelmä luo palautusavaimen joka käyttäjän kannattaa tallettaa varmaan paikkaan tietokoneen ulkopuolelle. Palautusavainta käytetään levyn avaamiseen jos käyttäjä unohtaa tai hukkaa salasanansa. Jos sekä palautusavain, että salasana ovat kadonneet on levyn tiedot menetetty. Seuraavassa vaiheessa käyttöönottoavustaja tarjoaa vielä mahdollisuutta tallettaa palautusavain Applelle jolloin pääsy avain salataan ja turvataan kolmella turvakysymyksellä sekä Apple-tilin salasanalla. Edellä mainitun tiedon korruptoitumisen varalta käyttäjän on hyvä varmuuskopioida järjestelmä ennen salauksen käyttöönottoa.

FileVaultin käyttöönotossa järjestelmä luo salatun kopion kotikansiosta ja tähän prosessiin saattaakin kulua paljon aikaa etenkin jos kotikansio sisältää paljon dataa. Prosessin alussa käyttäjän kannattaa valita suojattu poisto jolloin käyttöönottoprosessin päätyttyä järjestelmä poistaa automaattisesti alkuperäisen salaamattoman kotikansion. FileVaultilla salatun kotikansion tunnistaa helposti kassakaappi-kuvakkeesta. Käyttöönoton jälkeen käyttäjä ei juurikaan huomaa salauksen olemassaoloa, hidastelua saattaa esiintyä käsiteltäessä suuria tiedostoja. FileVaultissa käytettävä 128-bittinen AES-algortimi on varmuudella luotettava, kokonaisuuden suurin haittapuoli on sisäänkirjautumissalasanan käyttö salausavaimena. Turvallisinta olisi käyttää erillistä monimutkaista salasanaa salausavaimena. Lisäksi huonona puolen on heikko yhteensopivuus sisäänrakennetun Time Machine-varmuuskopioinnin kanssa. Automaattiset Time Machine-varmuuskopiot voidaan ajaa ainoastaan käyttäjän ollessa uloskirjautuneena eikä yksittäisiä kotikansion sisältämiä tiedostoja voida palauttaa graafisen käyttöliittymän kautta.

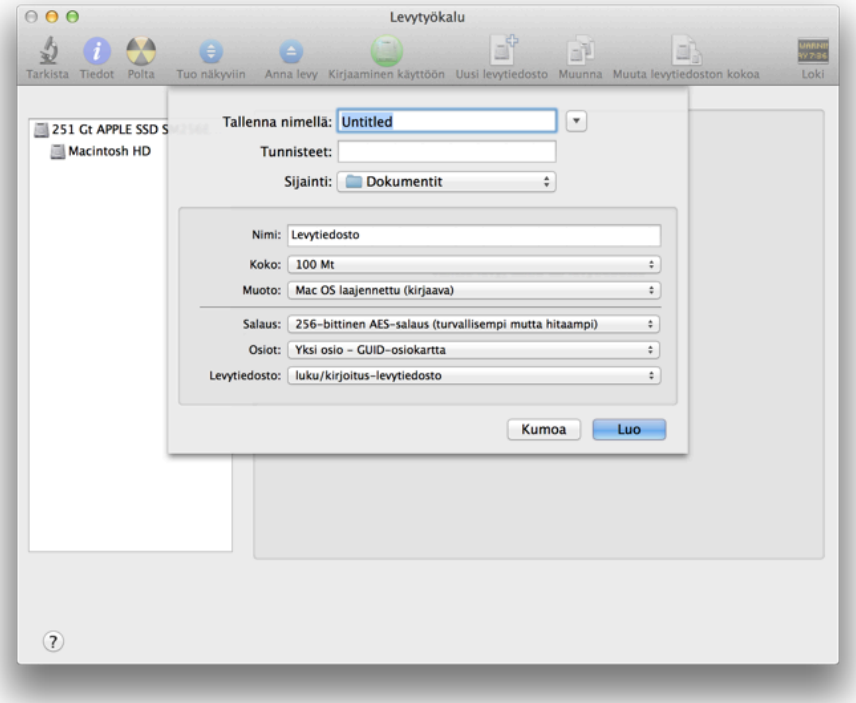


Kaikille käyttäjille kotikansion salaaminen ei ole tarpeellinen toimenpide, mutta esimerkiksi USB-muistitikun tai yksittäisen kansion salaaminen saattaa tulla ajankohtaiseksi esimerkiksi henkilökohtaisten tietojen liikuttelussa tai työasioiden työstämisessä omalla kotikoneella. Nämä voidaan toteuttaa helposti sisäänrakennetulla levytyökalu-ohjelmalla jolla voidaan

luoda erikokoisia salattuja levykuvia eli imageja tai alustaa USB-muistitikku salattuun muotoon.

Levytyökalu sijaitsee ohjelmakansion lisäohjelmat-kansiossa. Valitsemalla ”uusi levytiedosto” päästän ikkunaan jossa uusi levykuva voidaan nimetä sekä määrittää levykuvan koko, tallennuspaikka, muoto ja salauksen taso. Käyttäjän kannalta paras valinta levymuodoksi on harva levytiedosto, jonka koko kasvaa kiintolevyllä kohti maksimia sitä mukaa kun tiedostoja lisätään. Muita muotoja ovat Applen HFS+ sekä Windowsin tukema FAT. Salaukseksi voidaan valita joko 128-bittinen tai 256-bittinen AES algortimi. Poiketen FileVaultista käyttäjä voi itse päättää salausavaimen.

Levykuvan luonnin jälkeen voi käyttäjä kopioida sinne tiedostoja tai kansioita hiirellä raahaamalla. Levykuva tulee näkyviin työpöydälle sekä Finderin sivupalkkiin. Kun valitut tiedostot on siirretty levykuvan sisään voi käyttäjä poistaa levykuvan näkyvistä jolloin tiedot ovat turvassa levykuvan sisällä salasanan takana. Mikäli käyttäjä säilyttää levykuvaa tietokoneen kiintolevyllä on muistettava, että siinne siirretyt tiedot ovat kopioida ja alkuperäiset kohteet on poistettava salaamattomalta levyltä luottamuksellisuuden varmistamiseksi.



Virustorjunta ja haittaohjelmat

Macin suojaaminen haittaohjelmilta

- Käyttöjärjestelmän päivitykset ajan tasalla
- GateKeeper kytketty vähintään oletusasetuksille
- Virustorjuntaohjelmiston asentaminen

Virustorjuntaohjelmia:

- F-Secure (maksullinen)
- Kaspersky AntiVirus for Mac (maksullinen)
- Norton Anti-Virus for Mac (maksullinen)
- Sophos Anti-Virus for Mac (maksullinen)
- ClamXav (ilmainen)
- avast free antivirus for mac (ilmainen)

Yleisimpiä tiedon eheyteen vaikuttavia uhkia ovat erilaiset haittaohjelmat. Tietokoneen kiintolevyn saastuessa haittaohjelmalla vaarantuu samalla tietojen eheys. Haittaohjelmia ovat sovellukset tai ohjelmat jonka tarkoituksena on tunkeutua tietojärjestelmiin ja aiheuttaa niissä vahinkoa. Haittaohjelma on yleisnimitys joka pitää sisällään virukset, madot, troijalaiset sekä erilaiset järjestelmät takaovet.

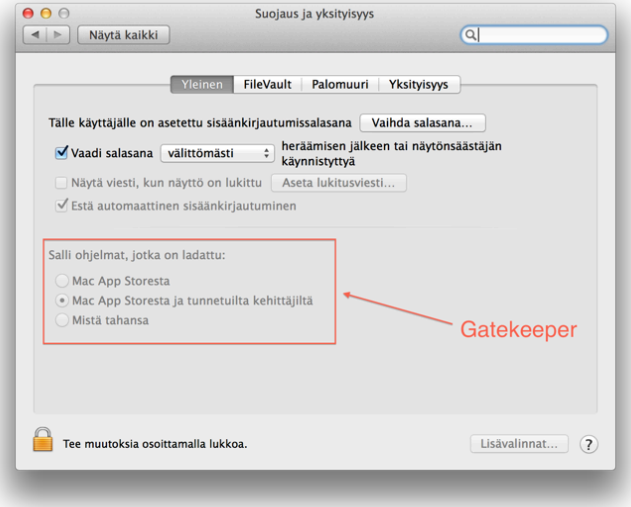
OS X –käyttöjärjestelmää uhkaavien haittaohjelmien lukumäärä on tunnetusti pieni. Tarkkaa määrää on mahdotonta sanoa. Tietoturvatuotteita kehittävä Kaspersky kertoo verkkosivuillaan, että vuosien 2011 ja 2012 välisenä aikana tartuntahavaintojen määrä kasvoi 30% joista valtaosa on tarkoitettu vanhojen järjestelmäversioiden haavoittuvuuksia varten. Myös Windows-ympäristöistä tutut haittaohjelmat ovat omana riskinä OS X-järjestelmässä. Vaikka haittaohjelma ei osaisikaan aiheuttaa uhkaa OS X-käyttäjälle voi käyttäjä tietämättään levittää haittaohjelmaa eteenpäin sähköpostin tai ulkoisen tallennusmedian kautta.

OS X-järjestelmällä varustetulle tietokoneelle suurimman potentiaalisen uhan muodostavat haittaohjelmista troijalaiset. Ohjelma joka saattaa vaikuttaa harmittomalta ja jollain tasolla hyödylliseltä sisältääkin todellisuudessa haitallista koodia joka vahingoittaa järjestelmää tavalla tai toisella. Tähän mennessä merkittävin OS X-järjestelmälle suunnattu haittaohjelma on Flashback-troijalainen joka vuonna 2012 saastutti lyhyessä ajassa 600 000 mac-tietokonetta. Flashback-

troijalainen käyttää hyväkseen Java-haavoittuvuutta ja valjastaa tietokoneen osaksi bottiverkostoa. Toinen merkittävä ja pitkäikäinen troijalainen tunnetaan nimellä MacKeeper. Kyseinen haittaohjelma naamioituu virustorjuntaohjelmaksi ja lupaa käyttäjälle tietokoneen puhdistuksen olemattomista haittaohjelmista edullisella hinnalla. Todellisuudessa ohjelma kerää käyttäjän luottokorttitiedot ja jää kiintolevylle tekemättä yhtään mitään. Ohjelman tekijät edesauttavat ohjelman leviämistä tehokkaan hakukoneoptimoinnin avulla jolla kyseinen ohjelma saadaan hakukonetuloksissa kärkipaikalle. Verkkosivuilla vierailtaessa ohjelma latautuu käyttäjän tietokoneelle automaattisesti, mutta ei aiheuta vahinko ilman käyttäjän suorittamaa manuaalista asennusta. Kyseinen ohjelma tunnettiin aiemmin nimellä MacDefender.

Paras ja samalla varmin tapa ehkäistä haittaohjelmatartuntoja on virustorjuntaohjelmiston asentaminen tietokoneelle. Vaikka ohjelmien yleisnimitys on virustorjuntaohjelmista, pystyvät ne havaitsemaan myös muunlaiset haittaohjelmat kuten troijalaiset, madot ja takaovet. Jokaisella haittaohjelmalla on yksilöllinen piirre ja tapa toimia joita virustorjuntaohjelmisto pyrkii reaaliaikaisesti tarkkailemaan tietokoneen kiintolevyltä sekä saapuvasta verkkoliikenteestä. Ohjelmien virustietokanta päivittyy yleensä automaattisesti mikä tuo käyttäjälle reaaliaikaista turvaa.

OS X –käyttöjärjestelmästä löytyy muutama alkeellinen virustorjuntaratkaisu sisäänrakennettuna, joiden avulla voidaan estää monien haitallisten ohjelmien suorittaminen järjestelmässä. Käyttäjän ladatessa internetistä sovelluspaketin lisätään niihin automaattisesti metatietoja jotka sisältävät tiedot lataussivusta, ajankohdasta sekä ohjelmasta jota lataukseen käytettiin. Sovelluspakettia avattaessa ensimmäisen kerran näyttää järjestelmä kyseiset metatiedot varoitusikkunassa, jotta käyttäjä tiedostaa onko ohjelma ladattu hänen huomaamattaan. Jos ohjelma on ladattu muualta, kuin App Storesta eikä sovelluksessa ole yleisesti tunnetun kehittäjän allekirjoitusta metatiedoissa ei järjestelmä oletuksena suostu avaamaan pakettia. Tätä ominaisuutta kutsutaan nimellä Gatekeeper. OS X –järjestelmä kykenee itsekseen tunnistamaan suppeahkon määrän haittaohjelmia suppean virustietokannan avulla. Jos ajettava ohjelma sisältää haitallista ohjelmakoodia, pyydetään käyttäjää automaattisesti siirtämään tiedosto roskakoriin.



Palomuuri

Mikä on palomuuri ?

- Palomuuri valvoo tietokoneen verkkoliikennettä
- Palomuuri voi olla laite- tai sovelluspohjainen.
- Jokaiselle verkkoa käyttävälle sovellukselle on mahdollista asettaa omat säännöt (salli/estä).
- Palomuuri ei yksistään ole riittävä suoja tietokoneelle.

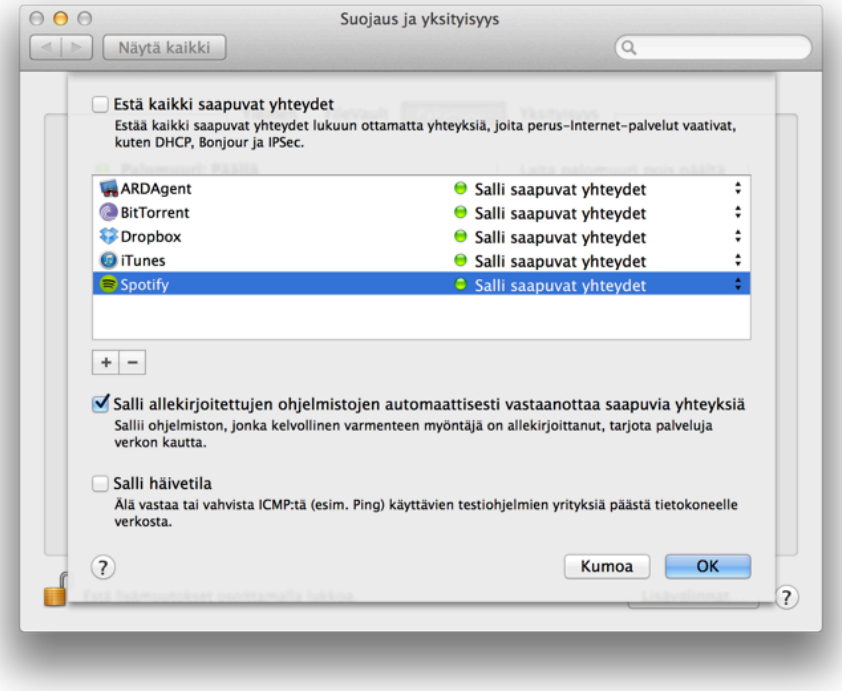
OS X –käyttöjärjestelmän eheyttä voidaan parantaa palomuurilla, joka valvoo ja tarvittaessa rajoittaa tietokoneen saapuvaa ja lähtevää verkkoliikennettä määriteltyjen sääntöjen mukaan. Palomuurin avulla voidaan estää erilaisten haittaohjelmien yritykset avata yhteydet isäntäpalvelimeensa. Palomuurit ovat tämän lisäksi tehokas keino tietomurtojen estämisessä. Murtautuessaan sisään tietojärjestelmään rikkoo hakkeri välittömästi tietojärjestelmän eheyden. Jotta turvallisuudesta kokonaisvaltainen on palomuuri välttämätön komponentti. Eheyden ohella järjestelmään murtautunut hakkeri vaarantaa myös tietojärjestelmän sisältämien tietojen luottamuksellisuuden. Palomuurin avulla voidaan näiden ohella estää palvelunestohyökkäykset jotka uhkaavat tietojen saatavuutta.

Käyttöjärjestelmä sisältää kai palomuuriratkaisua jotka poikkeavat toisistaan toimintatavaltaan sekä käytettävyydeltään. Järjestelmäasetuksien ”Suojaus ja yksityisyys” valinnan kautta hallittava sovelluskohtainen palomuuri on ominaisuuksiltaan niukka mutta helppokäyttöinen palomuuriratkaisu. Palomuuri valvoo vain sovelluksien saapuvaa verkkoliikennettä sekä sallii ja rajoittaa sitä käyttäjän valitseman listan mukaisesti. Palomuuri hyväksyy oletusasetuksilla vain allekirjoitettujen ja luotettujen sovellusten verkkoliikenteen. Luotettuja sovelluksia ovat esimerkiksi kaikki Applen valmistamat sovellukset sekä Applen hyväksymien kehittäjien tuottamat sovellukset. Näiden luotettujen sovellusten automaattinen

salliminen voidaan kytkeä pois päältä. Allekirjoittamattoman sovelluksen muodostaessa yhteyttä kysytään käyttäjältä lupa yhteyden sallimiselle. Käyttäjän vastauksesta riippuen lisätään sovellus palomuurin listalle joko sallittuna tai estettynä. Sovellusten lisääminen listalle on mahdollista myös manuaalisesti hallintaikkunassa.

Jotta käyttäjän tietoturva pysyy mahdollisimman korkeatasoisena voidaan palomuuri asettaa estämään kaikki saapuvat yhteydet. Tämän valinnan ollessa aktiivinen järjestelmä sallii vain tärkeimmät internetpalvelut kuten DHCP-protokolla joka vastaa IP-osoitteiden jakamisesta. Samalla aktivoituu häivetila (Stealth-mode) joka tekee tietokoneen löytämisen verkosta vaikeaksi eikä esimerkiksi vastaa toisesta tietokoneesta lähetettyyn ping-käskyyn. Häivetilan käyttö ei vaikuta sovellusten saapuvan verkkoliikenteen rajoittamiseen tai sallimiseen joten sitä voidaan käyttää myös ”Estä kaikki saapuvat yhteydet”-valinnan ollessa poissa käytöstä.

Sovelluskohtaisen palomuurin haittapuolena on sen kykenemättömyys valvoa ulospäin suuntautuvaa verkkoliikennettä. Sovelluskohtainen palomuuri ei myöskään kykene seuraamaan verkkoliikennettä porttikohtaisesti. Näihin puutteisiin ratkaisun tuo sisäänrakennettu Unix-perinteisiin perustuva IPFW-palomuuri joka on oletuksen kytketty pois päältä. IPFW-palomuuria hallinnoidaan komentoriviltä käsin erilaisilla käskyillä, mikä tekee palomuurin konfiguroinnista haastavaa perehtymättömälle käyttäjälle. Käytön helpottamiseksi internetistä on onneksi saatavilla IPFW-palomuuriin liitettäviä graafisia käyttöliittymiä. Näitä ovat esimerkiksi WaterRoof ja NoobProof.



Varmuuskopiointi

Miksi pitäisi varmuuskopioida?

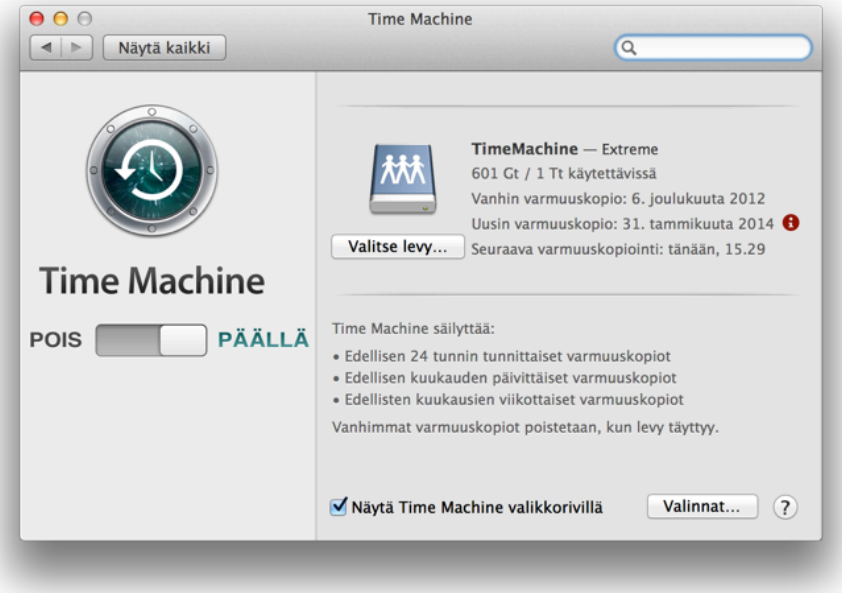
- Tietokoneen päälle kaatunut vesilasi aiheuttaa helposti kiintolevyn vaurioitumisen.
- Tietokoneen käyttöjärjestelmä ei toimi kuten ennen ja järjestelmä joudutaan asentamaan uudestaan.
- Tietokoneelta on vahingossa poistettu tärkeä kansio, tiedosto tai kuvakirjasto.
- Jos varmuuskopiota ei ole on tietojen palautus tehtävä erikoisliikkeessä joka on erittäin kallista ja aikaa vievää.
- Asianmukaiselta varmuuskopiolta tietojen palautus käy kaikissa yllä mainituissa tapauksissa helposti ja vaivattomasti.

Tiedon saatavuuteen kohdistuva uhka voi toteutuessaan tuhota kiintolevylle tallennetun tiedon tai vaihtoehtoisesti pääsy siihen voi estyä joko hetkellisesti tai pysyvästi. Vakavimmat OS X- järjestelmän tiedon saatavuuteen liittyvät uhat ovat laiteviat tai varkaudet. Varkauksien todennäköisyys Mac-tietokoneelle on erityisen suuri johtuen laitteen rahallisesta arvosta sekä trendikkyydestä. Tämän takia tietoturvallisuuden ylläpitämiseksi ennaltaehkäisevät suojaustoimenpiteet ovat aina kaikkein parhaimpia vaihtoehtoja. Varkaustapauksia ennaltaehkäistessä on laitteen säilytyspaikkaan kiinnitettävä huomiota. Laitevikoja voidaan estää kiinnittämällä huomiota ja seuraamalla niiden toimintaa ja käyttäytymistä käytön aikana.

Ennaltaehkäisevät toimenpiteet eivät yksistään riitä tiedon saatavuuden varmistamiseksi. Uhan toteutuessa on otettava käyttöön turvaavat menetelmät joista yleisin on tietojen varmuuskopiointi. Yksinkertaisesti kuvattuna varmuuskopiointi tarkoittaa tietojen kahdentamista eli kopioimista esimerkiksi ulkoiselle kiintolevylle, muistitikulle, varmuuskopiointipalvelimelle tai muulle liikuteltavalle tallennusmedialle. Alkuperäisen tiedon kadotessa tai korruptoituessa voidaan menetetty tieto helposti palauttaa varmuuskopiosta jonka jälkeen työskentely voi jatkua normaalisti. Varmuuskopio ei välttämättä ole käyttäjälle hyödyllinen jos sitä ei ole suoritettu säännöllisesti. Lisäksi varmuuskopioinnissa on huolehdittava tallennuskohteen riittävän isosta kapasiteetista jottei se pääse loppumaan varmuuskopioinnin yhteydessä.

OS X –käyttöjärjestelmässä on sisäänrakennettu automaattinen varmuuskopiointitoiminto Time Machine. Käyttöönoton jälkeen Time Machine osaa suorittaa varmuuskopioinnin automaattisesti yhteensopivalle kiinto- tai verkkolevylle automaattisesti eikä näin ollen vaadi käyttäjältä minkäänlaisia lisätoimenpiteitä. Varmuuskopiointiin käytettävä levy on ennen käyttöönottoa alustettava Applen HFS+ tiedostojärjestelmämuotoon. Time Machine otetaan käyttöön järjestelmäasetuksista löytyvän hallintaikkunan kautta. Hallintaikkunassa käyttäjän on mahdollista valita varmuuskopion tallennuspaikka sekä kansiot joita ei haluta sisällyttää varmuuskopioon. Hallinta ikkuna ilmoittaa myös mahdollisista poikkeamista automaattisesta varmuuskopiointiaikataulusta.

Käyttöönotossa Time Machine varmuuskopio ensimmäisellä varmuuskopiokerralla koko järjestelmän ja seuraavilla kerroilla vain edellisestä varmuuskopiosta muuttuneet kohteet. Varmuuskopiointi suoritetaan kerran tunnissa ja ohjelma säilyttää kopiot kuluneelta 24 tunnilta, päivän ensimmäiset kopiot kuluneelta kuukaudelta sekä viikoittain tehtävät kopiot menneiltä kuukausilta. Tallennuslevyn täyttyessä kirjoittaa ohjelma automaattisesti uusimmat kopiot vanhimpien päälle.



Tietojen palautus tapahtuu erillisellä Time Machine-käyttöliittymällä johon pääsee siirtymään joko napsauttamalla Time Machine kuvaketta Dock-palkissa tai valikkoriviltä. Käyttöliittymä tietojen palautuksessa toimii aikakoneen tavoin näyttäen tietokoneen sisällön tiettyinä ajankohtina. Sivussa olevan aikajanan avulla käyttäjän on helppo liikkua eri ajankohtien välillä. Käyttöliittymällä on mahdollista palauttaa yksittäisiä kohteita jotka on helposti löydettävissä ikkunan oikean yläkulman hakukentän avulla. Uutta konetta käyttöönotettaessa on vanhan koneen tiedot helppo siirtää uuteen Mac-tietokoneeseen Time Machine varmuuskopiosta avulla kokonaisuudessaan.

Time Machine-varmuuskopiointisovellus on suunniteltu kotikäyttäjän tarpeita ajatellen. Yksinkertaisen alkuvalmistelun jälkeen sovellus toimii automaattisesti taustalla eikä käyttäjä juurikaan huomaa sen olemassaoloa. Käytännössä kerran tunnissa suoritettava varmuuskopio käyttäjän kotikansiosta ei vie muutamaa minuuttia kauempaa eikä näin ollen syö koneen resursseja käyttäjää häiritsevästi. Juuri ohjelman yksinkertaisuus ja helppokäyttöisyys on seurausta edistyneempien varmuuskopiointitoimintojen puutteesta. Yrityskäytössä Time Machine ei yksistään ole riittävä mutta toimiva yhtenä osana tiedon saatavuuden varmistamisessa. Suositeltavaa on tehdä Time Machinen ohella Käytettävästä kiintolevystä klooni ulkoiselle medialle tasaisin väliajoin jotta tiedon varmistus olisi kahdessa erillisessä paikassa ja kahdella erilaisella tavalla toteutettuna.