Marko Lehkonen

KODIN SÄHKÖISEN ASIOINNIN JA TIETOTURVAN KEHITTÄMINEN KOKONAISARKKITEHTUURIN NÄKÖKULMASTA

Opinnäytetyö
Sähköisen asioinnin ja arkistoinnin koulutusohjelma

Toukokuu 2014

MAMK
University of Applied Sciences

KUVAILULEHTI

MAMK University of Applied Sciences	**Opinnäytetyön päivämäärä** 17.5.2014
Tekijä(t) Marko Lehkonen	**Koulutusohjelma ja suuntautuminen** Sähköinen asiointi ja arkistointi

Nimeke

Kodin sähköisen asioinnin ja tietoturvan kehittäminen kokonaisarkkitehtuurin näkökulmasta

Tiivistelmä

Yhä suurempi osa sähköisestä asioinnista hoidetaan nykyään kotoa käsin. Sitä mukaa kuin asiointi on muuttunut sähköiseksi ja siirtynyt koteihin, kodin tietoverkoiltakin vaaditaan enemmän, sillä asioinnin aikana käsitellään yksityisiä tietoja. Sähköisesti asioidaan niin viranomaisten kuin yritystenkin kanssa, joten siihen liittyy usein myös taloudellisia etuja.

Tutkimuksessa perehdytään julkishallinnon kokonaisarkkitehtuurista antamiin suosituksiin. Opinnäytetyössä tutkitaan sitä, kuinka julkishallinnon suositukset soveltuvat sekä kodin sähköisen asioinnin, että sen tietoturvan kehittämiseen. Tutkimusmateriaali on kerätty havainnoimalla erään perheen tietokoneen käyttöä ja kodin sähköistä asiointia.

Opinnäytetyössä kodin nykytila on kuvattu kokonaisarkkitehtuurin neljän näkökulman avulla. Kuvauksessa on otettu huomioon toiminta-arkkitehtuuri, tietoarkkitehtuuri, tietojärjestelmäarkkitehtuuri ja teknologia-arkkitehtuuri. Eri arkkitehtuurien perusteella havaittiin ja valittiin ne kohteet, joita kodin tietoturvassa ja sähköisessä asioinnissa tulisi kehittää. Tämän jälkeen voitiin kuvata kodin tavoitetila.

Tutkimus osoitti, että julkishallinnon suosituksia voidaan käyttää myös kodin tietoteknisen ympäristön kehittämiseen. Vaikka suositusten yleisiä periaatteita voidaan soveltaa hyvin myös kodeissa, niitä ei kuitenkaan kannata käyttää sellaisinaan. Suositusten monimutkaisuuden ja kotien vähäisten resurssien vuoksi on haastavaa noudattaa suosituksia tarkasti.

Asiasanat (avainsanat)
sähköinen asiointi, koti, julkishallinnon suositus, tietoturva

Sivumäärä	**Kieli**	**URN**
59 + 1 liite	Suomi	

Huomautus (huomautukset liitteistä)

Ohjaavan opettajan nimi	**Opinnäytetyön toimeksiantaja**
Jukka Selin	

DESCRIPTION

MAMK University of Applied Sciences	**Date of the master's thesis** 17 May 2014
Author(s) Marko Lehkonen	**Degree programme and option** eServices and Digital Archiving

Name of the master's thesis

Development of household e-services from the viewpoint of enterprise architecture

Abstract

The requirements of home network security have increased, because more and more of e-services including the transfer of important information take place in the home network. Due to conducting business with public authorities as well as private companies also financial interests are often linked to the e-services that are used at home.

This study focused on the recommendations given for the public authorities called JHS recommendations of the enterprise architecture. The thesis examined, if the JHS recommendations could be applicable in developing e-services and data security in the households. The research method applied in this study was observation, which was a practical method to examine how the e-services were used at home.

In this thesis the present state of a home was defined by using the enterprise architecture description methods. The four aspects of the architecture included operating architecture, data architecture, information architecture and technology architecture. The aim of this study was to identify, by utilizing the above mentioned architectural aspects, the areas of the example household that needed to be developed. As a result of defining the current state and development areas, a target state for the home enterprise architecture was created.

This study showed that the general principles of the JHS recommendations could well be used to develop the home information technology environment. However, the complexity of the JHS recommendations and the minor resources available at home pose great challenges to applying these recommendations to the letter.

Subject headings, (keywords)

e-services, households, JHS recommendation, security

Pages	**Language**	**URN**
59 + 1 appendix	Finnish	

Remarks, notes on appendices

Tutor	**Master's thesis assigned by**
Jukka Selin	

SISÄLTÖ

1 JOHDANTO

Asiointi viranomaisten, pankkien, yritysten ja muidenkin toimijoiden kanssa tapahtuu nykyisin yhä enenevissä määrin sähköisenä tietoverkoissa. Myös kotikäytössä olevat paikallisverkot ovat viime vuosina kasvaneet ja monimutkaistuneet. Samalla niiden tietoturvan ylläpito on kuitenkin jäänyt vähemmälle huomiolle. Kodin tietokoneissa on ehkä virustorjunta asennettuna ja käyttöjärjestelmän tarjoamat automaattipäivitykset asennetaan automaattisesti. Usein ajatellaan, että nämä toimenpiteet riittävät. Kotiverkkoon on kuitenkin kytkettyinä tiedosto- ja mediapalvelimia, verkkotulostimia, puhelimia, tabletteja, valvontakameroita, älytelevisioita ja muita laitteita. Näissä laitteissa voi olla haavoittuvuuksia, jotka voivat olla uhkana kodin tietoturvalle. Kotiverkoissa säilytetään myös yksittäisille henkilöille hyvin tärkeitä tietoja, joiden tuhoutuminen voi aiheuttaa suurta vahinkoa yksittäiselle kansalaiselle. Sähköinen asiointi on jo arkipäivää joka kodissa. Sähköiseen asiointiin liittyviä tietoturvauhkia ei kuitenkaan usein tarkkaan selvitetä eikä niihin varauduta.

Opinnäytetyön tarkoituksena on tutkia sähköisien palveluiden käyttöä. Tarkoituksena on tunnistaa omaan kotiverkkooni liittyviä parantamiskohteita, jotta kotiverkkoni tietoturva olisi riittävällä tasolla uhkien varalta. Tutkin myös sitä, miltä osin julkishallinnon suosituksia kokonaisarkkitehtuurista voidaan käyttää apuna kotiverkon kehittämisessä. Erityisesti tarkastelen Julkishallinnon suositusta 179 ICT palveluiden kehittämisestä ja suositusta 152 prosessien kuvaaminen.

Tarkoitus on etsiä vastauksia seuraaviin kysymyksiin: Mitä ja miten sähköisiä palveluita käytetään kotona? Millaisia tietoturvauhkia palveluiden käyttö sisältää ja erityisesti kuinka niiltä suojaudutaan? Kuinka teen kodistani tietoturvallisen? Mitä vaatimuksia sähköinen asiointi asettaa kotiverkon tietoturvallisuudelle? Mistä lähden liikkeelle, jotta kodistani tulee tietoturvallinen? Yhä tärkeämmäksi on myös muodostunut ohjelmistohaavoittuvuuksien hallinta. Kuinka tämä toteutetaan kotiverkossa? Voidaanko julkishallinnon suosituksia, joissa käsitellään kokonaisarkkitehtuuria, käyttää apuna kodin sähköisen asioinnin kehittämisessä? Mitkä osat julkishallinnon suosituksista on hyödynnettävissä kehittäessä kodin sähköistä asiointia ja sen tietoturvaa?

Keskityn opinnäytetyössä aihealueisiin, jotka ovat kotiverkossa ja kotikäyttäjille merkityksellisiä. Opinnäytetyöni ei sisällä sellaisia tietoturvan osa-alueita, jotka ovat yrityksen tietoturvan kannalta oleellisia, mutta joilla ei ole kotikäyttäjille merkitystä.

2 OPINNÄYTETYÖN TAVOITTEET JA TUTKIMUSMENETELMÄT

Opinnäytetyön aihe, sähköisen kodin sähköisen asioinnin ja sen tietoturvan kehittämisestä, syntyi henkilökohtaisesta tarpeesta varmistaa kotini tietoverkon turvallisuus. Kodissani on kymmeniä laitteita, jotka ovat yhteydessä internetiin. Kodin tietoverkon ylläpito tapahtuu vapaa-ajalla eikä kaikkien laitteiden ylläpitoon ja päivittämiseen aina riitä aikaa. Kodin tietoverkoissa käsitellään kuitenkin verkko-ostoksia, raha-, pankki- ja vakuutusasioita sekä muuten luottamuksellisia tietoja. Näiden tietojen väärinkäytön uhka on nykyaikana todellinen. Tutkimuksen tavoitteena on saada todellinen kuva kotini tietoverkosta, sen turvallisuudesta sekä suunnitella ja tehdä siihen käytettävissä olevien resurssien puitteissa parannuksia.

2.1 Tavoitteet

Opinnäytetyön tavoitteena on kehittää kodin sähköistä asiointia ja kodin tietoturvaa. Kehittäminen toteutetaan käyttäen hyväksi julkishallinnon suosituksia kokonaisarkkitehtuurin kehittämisetä. Tavoitteena on kuvata nykytila, havaita kehittämiskohteita, valita kehittämiskohteet, tehdä kehittämissuunnitelma sekä laatia lyhyt ohjeistus kodin tietoturvan kehittämiseksi.

Nykytilan kuvauksessa kuvaan kodissa käytössäni olevat sähköisen asioinnin prosessit. Kuvauksissa käytän kuvauksissa apuna julkishallinnon suosituksia. Lisäksi teen kodin riskianalyysin, jolla pyrin selvittämään kotini tietoturvaan liittyvät riskit. Tuloksena nykytilan kuvauksessa syntyy seuraavat dokumentit: sidosryhmä analyysi, tietoarkkitehtuurin kuvaus, tietojärjestelmäarkkitehtuurin kuvaus, teknologiaarkkitehtuurin kuvaus sekä riskianalyysi ja luettelo alustavista kehittämiskohteista.

Tavoitetilan ja toimeenpanon suunnittelussa selvitetään: Voisiko kodilla olla strategisia linjauksia sähköiseen asiointiin ja kuvaan Lehkosten perheen strategian. Alustavien kehittämiskohteiden, strategisten linjausten sekä käytettävissä olevien resurssien

perusteella tehdään valinta kehitettävistä kohteista, vaatimusmäärittely sekä kuvataan kodin kokonaisarkkitehtuurin tavoitetila. Kuvauksessa käytetään niitä arkkitehtuurin kuvauksen näkökulmia, joita halutaan kehitettävän. Esimerkiksi mikäli halutaan kehittää tietoturvaan liittyvää teknistä yksityiskohtaa, tehdään tavoitetilan kuvaus ainakin teknologia arkkitehtuurin kuvaus. Tarvittaessa kuvataan myös esimerkiksi toiminta-arkkitehtuuri, mikäli muutos vaikuttaa myös toimintaan. Tuloksena tavoitetilan ja toimeenpanon suunnittelussa syntyvät kodin strategia, kehittämiskohteiden rajaus, vaatimusmäärittely, tavoitetilan arkkitehtuurikuvaukset ja toimeenpanon suunnitelma.

Opinnäytetyön tavoitteena on myös laatia kodin sähköisen asioinnin ja tietoturvan kehittämisen toimenpidelista, johon on koottu yhdelle tai kahdelle sivulle keskeisimmät vaiheet ja tarkistettavat asiat kodin tietoturvan ja sähköisen asioinnin kehittämiseksi.

2.2 Opinnäytetyön rajaus

Tutustuttuani julkishallinnon suosituksiin 152, 171, 172, 173 ja 179 ja niiden laajuuteen päätin rajata opinnäytetyötäni seuraavasti: Kuvaan kotini sähköisen asioinnin kokonaisarkkitehtuurin nykytilan JHS 179 mukaisesti jaoteltuna toiminta-arkkitehtuuri, tietoarkkitehtuuri, tietojärjestelmäarkkitehtuuri ja teknologia arkkitehtuuri kuvauksiin. Nykytilan kuvaamisessa syntyneiden kehittämisehdotusten pohjalta kuvaan kodin kokonaisarkkitehtuurin tavoitetilan. Kehittämistoimenpiteet tehdään huomioiden ajalliset ja taloudelliset resurssit.

Rajaan lisäksi kehittämisen koskemaan mielestäni sähköisen asioinnin kannalta keskeisiin prosesseihin. Prosessit kuvaan JHS152 mukaisesti. Tällaisia voisi olla esimerkiksi laskujen maksaminen verkkopankissa, ostosten tekeminen verkkokaupassa sekä asiointi julkishallinnon palvelussa. En käsittele opinnäytetyöni sosiaalista mediaa, pelaamista, valvontakameroita yms. elleivät kyseiset asiat tule sähköistä asiointia tutkittaessa muuten esille.

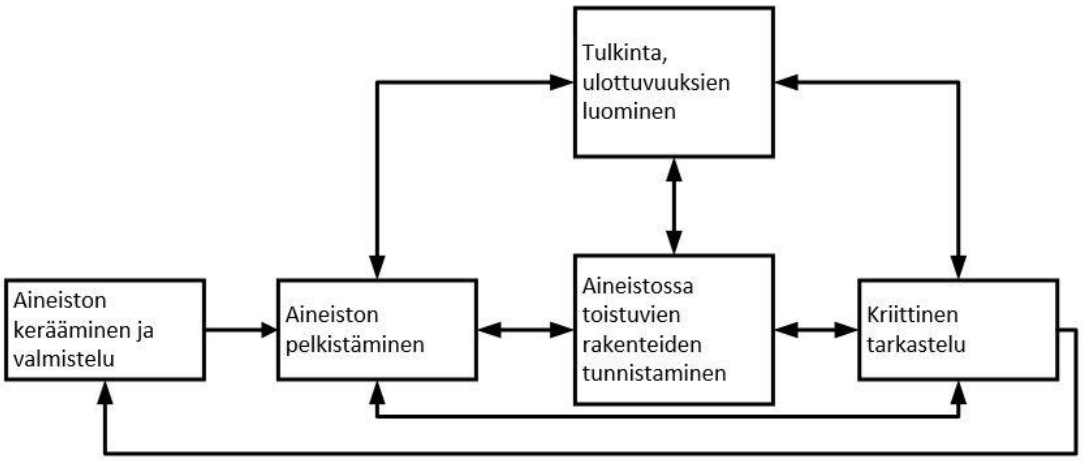
2.3 Tutkimusmenetelmät

Kehittämistyö tehdään toimintatutkimuksena. Toimintatutkimuksessa ongelman ratkaisu perustuu osallistuvaan tutkimukseen, jossa kehitettävään toimintaan osallistuvat

ihmiset otetaan mukaan aktiivisesti kehittämään toimintaa. Toimintatutkimuksessa ei vain pyritä kuvaamaan nykyistä toimintaa vaan myös kehittämään toimintaa ja myös kuvaamaan sitä millaista toiminnan pitäisi olla. (Ojasalo ym. 2009, 58.)

Kehittämistyössä käytetään havainnointia. Havainnointi on järjestelmällistä toimintaa joka kohdistuu ennalta määrättyyn kohteeseen. Havainnoinnin tulokset voidaan kerätä esimerkiksi havainnointilomakkeella, johon havainnoinnin tulokset kirjataan heti ylös. Osallistuvassa havainnoinnissa havainnoija osallistuu itse tapahtumaan esimerkiksi asiakkaana. (Ojasalo ym. 2009, 104–105.)

Havainnoinnin tuloksena syntyneeseen havaintoaineiston analysointiin voidaan käyttää sisältöanalyysia. Ojasalo ym. esittelee kirjassaan laadullisen tutkimuksen yleisen mallin (Kuva 1), joka kuvaa hyvin myös dokumenttianalyysin vaiheet.



KUVA 1. Laadullisen tutkimuksen yleinen malli (Ojasalo ym. 2009, 123)

Havainnoinnin analysointi jakautuu tavallisesti pelkistämis- ja tulkintavaiheeksi. Pelkistämisvaiheessa havainnot yhdistetään, jotta tieto voidaan luokitella tai ryhmitellä. Luokittelun jälkeen voidaan etsiä tyypillisiä tai keskivertoilmiöitä. (Ojasalo ym. 2009, 106–107.)

Tulkintavaiheessa pyritään löytämään jotakin uutta ja tekemään aineiston perusteella johtopäätöksiä. Tulkinta voi perustua aiempaan teoriaan tai tutkimukseen. Tulkinta ei ole kuitenkaan yksittäinen vaihe tutkimuksessa vaan usein on mukana koko tutkimuksen ajan. (Ojasalo ym. 2009, 128–129.)

Havainnoinnin kaikissa vaiheissa tehdään myös kriittistä tarkastelua, jonka tarkoituksena on löytää virheitä ja vääristymiä. Havainnointi soveltuu hyvin tutkimukselliseen kehittämistoimintaan. Havainnoinnilla saadaan selville miten ihmiset käyttäytyvät luonnollisessa ympäristössä. Havainnoinnilla voidaan esimerkiksi selvittää, kuinka esinettä käytetään ja mitä esinettä käytettäessä tapahtuu. (Ojasalo ym. 2009, 103, 123.)

3 KOTI JA SEN TOIMINNOT

Koti on MOT kielitoimiston sanakirjan (2012) mukaan ”yhden tai useamman ihmisen, varsinkin perheen vakinainen asunto”. Tilastokeskuksen mukaan (2014) kotitalous koostuu kaikista niistä henkiköistä, jotka asuvat ja ruokailevat yhdessä tai käyttävät yhdessä tulojaan. Kuluttajaviraston mukaan kotitalouden toiminnot ovat inhimillistä toimintaa, jota harjoitetaan kodiksi sanotussa tilassa ja jota tuo toiminta edellyttää ja aiheuttaa. Kodin arkitoimintoihin kuuluvat arjenhallinnalle välttämättömät toiminnot, joita ovat ruoan valmistus ja ateriointi, vaatteiden huolto, siivoaminen, kodin laitteiden ylläpito ja korjaus sekä hoivatyöt. Lisäksi kodissa levätään ja nukutaan, vietetään vapaa-aikaa, opiskellaan ja tehdään myös työtä. Kodin toimintoja on myös kotitalouden hallinto, kodin resurssien jakaminen, seuranta ja kirjanpito, asiointi, hankinnat, tiedonhankinta sekä median käyttö ja viestintä. Osa toiminnoista tehdään itse, mutta niitä voidaan ostaa myös palveluna. (Kuluttajavirasto 2010, 4.)

Kodin perinteisten toimintojen kodin sisällä tehtäviin toimintoihin on nykyaikana sisältynyt toimintoja, jotka aiemmin tehtiin kodin ulkopuolella. Tällaisia töitä ovat pankki- ja sopimusasiat, ostosten tekeminen, sosiaalinen yhdessäolo. Koti on kytketty tietoverkkojen avulla ulkomaailmaan sekä myös kodin sisällä toisiinsa niin, että ne muodostavat älykkään toimintaympäristön. (Kuluttajavirasto 2010, 3.)

Kodille välttämättömiksi toiminnoksi voidaan mielestäni katsoa myös kodin tietojärjestelmien asentaminen ja ylläpito. Kun tietoteknisen laitteen hankkii, ei yleensä riitä että laite vain kytketään tieto- ja sähköverkkoon ja käynnistetään. Laitteiden käyttöönotto vaatii erilaisten asetusten määrittämistä sekä tuntemusta ympäristöstä johon laite kytketään. Yrityksissä tietojärjestelmien ylläpitoon on oma henkilöstönsä, mutta kotona tällaista henkilöstöä ei ole. Kodin teknistyessä ylläpito vaatii yhä enemmän aikaa ja muita resursseja. Mikäli osaamista ei omasta kodista löydy, turvaudutaan tut-

tujen ja sukulaisten apuun. Ylläpitoa voi ostaa myös palvelun ja näiden palveluiden käyttö onkin viime vuosina yleistynyt.

3.1 Sähköinen asiointi

Sanastokeskus TSK:n Tietotekniikan termitalkoot sanaston mukaisesti sähköinen asiointi on asioiden hoitamista tietoverkon palveluiden avulla. Asiointi pitää sisällään esimerkiksi tietoverkon välityksellä suoritettua viranomaisasiointia, asiointia verkkopankissa sekä verkko-ostosten suorittamista. Sähköisestä asioinnista voidaan käyttää myös termiä verkkoasiointi. (Tietotekniikan termitalkoot 2008.)

Väestön tieto- ja viestintätekniikan käyttö tilaston mukaan 16 – 74-vuotiasta Internetiä käytti 92 prosenttia suomalaisista. Yleisimmin Internetiä käytetään pankkiasioiden hoitoon, viestintään, tiedonetsintään sekä sähköisten medioiden seurantaan. Verkkopankkia oli käyttänyt viimeisen 3 kuukauden aikana 84 prosenttia ja ostoksia verkon kautta 49 prosenttia. 45 prosenttia suomalaisista oli lähettänyt viranomaiselle lomakkeen. Vanhojen tavaroiden kauppa oli myös yleistä. Käytettyjä tavaroita osti 26 prosenttia 16 – 74-vuotiaista ja 17 prosenttia oli myynyt omia tavaroitaan. (Tilastokeskus 2013.)

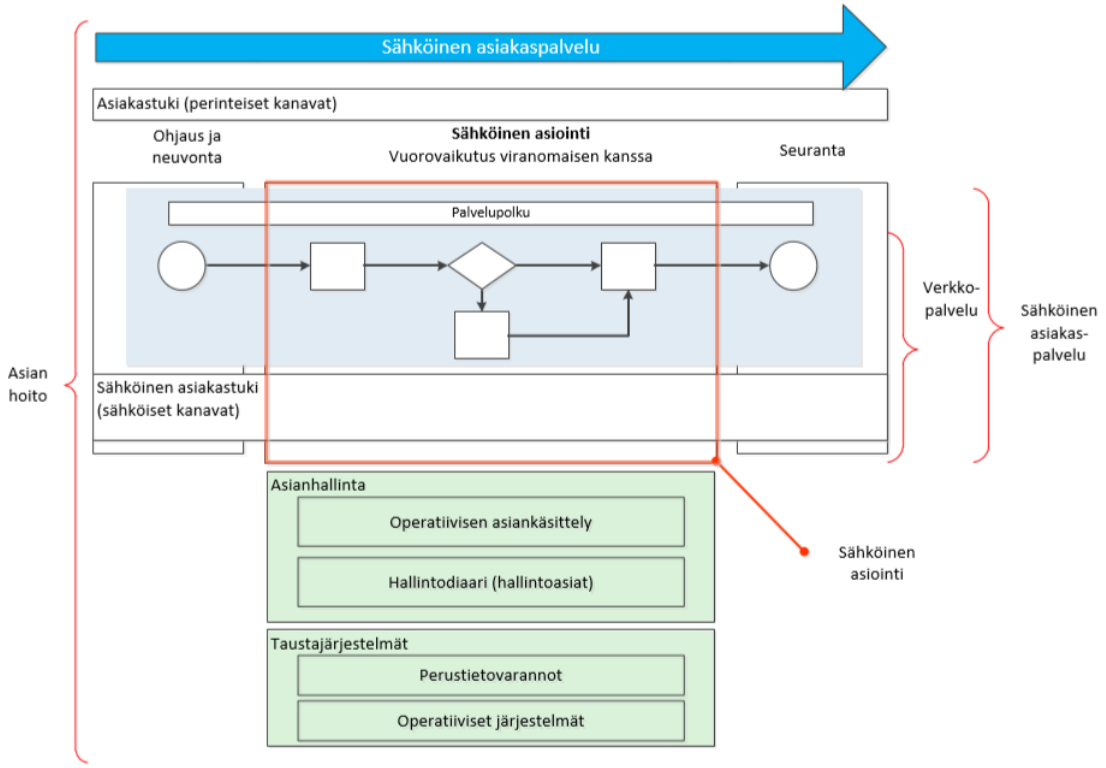
TAULUKKO 1. Internetin käytön ja eräiden käyttötapojen yleisyys 2013 (Tilastokeskus 2013)

	Käyttänyt internetiä viimeisten 3 kk aikana	Käyttää internetiä yleensä useita kertoja päivässä	Käyttänyt verkkopankkia viimeisten 3 kk aikana	Ostanut tai tilannut jotain verkon kautta viimeisten 3 kk aikana	Seurannut jotain yhteisöpalvelua viimeisten 3 kk aikana	Lähettänyt täytetyn lomakkeen viranomaisille tai julkiselle palvelun tuottajalle viim 3 kk aikana	Katsonut televisioyhtiöiden netti-tv-palveluita viimeisten 3 kk aikana	Älypuhelin käytössä
	%-osuus väestöstä							
16-24	100	76	78	55	87	42	75	80
25-34	100	88	98	70	78	62	81	81
35-44	99	80	98	69	67	63	75	74
45-54	97	67	92	52	41	44	64	59
55-64	85	52	80	29	26	34	51	45
65-74	65	33	55	16	13	21	37	25
75-89	27	8	22	3	3	5	12	5
Miehet	88	65	80	45	44	43	60	60
Naiset	83	57	77	44	49	40	58	51
Yhteensä 16–89	85	61	79	44	47	41	59	56
Yhteensä 16–74	92	66	84	49	51	45	64	61

Käsiteltäessä kodin sähköistä asiointia koti ei ole välttämättä tietty yksittäinen paikka, jossa sähköinen asiointi tapahtuu. Kodin sähköinen asiointi voidaan ymmärtää tapahtuvan Internetissä, joka voidaan käsittää Virven (2006, 15) esittämän ajatuksen mukaan fyysisen paikan kaltaisena. Tällöin ajatus siitä että kodin sähköinen asiointi pitäisi tapahtua kotona menettää merkityksensä. Merkityksellisempää on, että silloin kun sähköisessä asioinnissa käsitellään kotitalouteen liittyviä asioita, paikasta riippumatta, voidaan toiminta käsittää kodin sähköiseksi asioinniksi.

Valtiovarainministeriön julkaiseman sähköisen asioinnin viitearkkitehtuurin mukaan sähköinen asioinnin asiakkaita ovat kansalaiset, yritykset yhteisöt ja viranomaiset. Sähköinen asiointi on tapahtuma, jossa vuorovaikutuksessa julkisen palvelun tuottajan kanssa, asiakas hoitaa asiaansa tietoverkon avulla. Sähköinen asiointi on kokonaisuus ja voi sisältää myös ei sähköisiä osia, esimerkiksi asiakaskäyntejä tai asiointia puhelimella sekä palvelu voi siirtyä palvelun tuottajalta toiselle. Palvelun tuottamiseen liittyvät taustaprosessit eivät sisälly sähköiseen asiointiin. (Valtiovarainministeriö 2013, 43.)

Sähköisen asiakaspalvelun käsitteissä (Kuva 2) on kuvattu, mikä osa sähköisestä asiakaspalvelusta on sähköistä asiointia.



KUVA 2. Sähköisen asiakaspalvelun keskeiset käsitteet (Valtiovarainministeriö 2013, 6.)

Sähköinen asiointi täytyy järjestää siten että kansalaisen yksityisyys, joka on perusoikeus, ei vaarannu. Web-asioinnissa tiedonsiirtoväylän pitää olla luotettava, toimijoiden täytyy tunnistaa toisensa riittävän luotettavasti ja mikäli käsitellään asiakastietoa, liikenteen täytyy olla salakirjoitettua. (Andreasson ym. 2013, 199.)

Sähköinen tunnistaminen voidaan toteuttaa monella tavalla. Ratkaisuja on useita, toiset ovat heikompia kuin toiset. Palvelun tietosisällön tulisi määrittää tunnistamismenetelmä. Palvelulla ei saavuteta tavoiteltuja hyötyjä, mikäli tunnistamisratkaisu ei ole toimiva ja haittaa palvelun käyttöä. Vahvaa tunnistamista tulisi käyttää silloin kun se on perusteltua. (Andreasson ym. 2013, 200.)

Verkkopalveluissa on käytössä erilaisia tunnistamisen vaihtoehtoja. esimerkiksi käyttäjätunnus ja salasana, mobiilivarmenne, toimikortti, tupas jne. Vielä nykyisinkin suu-

ressa osassa julkishallinnon palveluista ei käytetä vahvaa tunnistusta, vaikka julkishallinnon palveluissa suositellaan käytettäväksi vahvan tunnistamisen tarjoajia kuten VETUMA. (Andreasson ym. 2013, 182–183.)

VETUMA

VETUMA on kansalaisille tarkoitettu sähköisen tunnistamisen ja maksamisen palvelu, jonka omistaa valtio ja vastaa Valtion IT-palvelukeskus (VIP). Palvelun on tarkoitus tuottaa koko julkiselle hallinnolle yhteinen verkkomaksamisen ja tunnistamisen alusta. VETUMASSA on tarkoituksena tarjota yhtenäinen tapa tunnistaa käyttäjä riippumatta siitä, millainen ratkaisu taustalla on. VETUMASSA voidaan tunnistautua käyttämällä Tupas–tunnistamista, Mobiilivarmennetta tai sähköisellä henkilökortilla olevalla kansalaisvarmenteella. Tällä hetkellä käyttäjinä on jo yli 100 julkishallinnon toimijaa. (Andreasson ym. 2013, 183–184.)

Tupas

Tupas on suomalaisten pankkien käyttämä tapa tunnistaa verkkopalvelun käyttäjä. Palvelun on määrittänyt Finanssialan keskusliitto (FK). Palvelussa pankki tunnistaa kolmannen osapuolen asiointipalvelua käyttävän kansalaisen palveluntuottajan puolesta. Tunnistus tapahtuu siten, että tunnistamista varten asiakas ohjautuu oman pankin tunnistamissivulle, jossa syötetään tunnistamisessa tarvittavat kyseiseen pankkiin tunnistamiseen tarvittavat tiedot. Tunnistamisen jälkeen pankki lähettää palveluntarjoajalle tiedon siitä kuka henkilö on. (Andreasson ym. 2013, 184–185.)

Mobiilivarmenne

Mobiilivarmenne on teleoperaattoreiden tarjoama palvelu vahvaan tunnistamiseen, jossa matkapuhelimen sim-korttiin liitetään tietopaketti henkilötiedoista. Mobiilivarmenteen käyttöön vaaditaan varmennetoiminnallisuutta tukeva sim-kortti, tunnusluku sekä sopimuksen operaattorin kanssa. Mobiilivarmenteella voidaan allekirjoittaa sopimuksia verkossa ja puhelimessa. Mobiilivarmenteella tehdyt sopimukset ovat juridisesti sitovia. Mobiilivarmenne on yksi VETUMA-tunnistamispalveluiden tunnistusvaihtoehto. (Andreasson 2013, 185.)

Operaattori vastaa viestintäverkkonsa tietoturvasta ja tarjoamistaan tietoturvapalveluista. Muuten vastuu palvelunkäytöstä laitteiden ja ohjelmistojen tietoturvasta on käyttäjällä. (Elisa 2011)

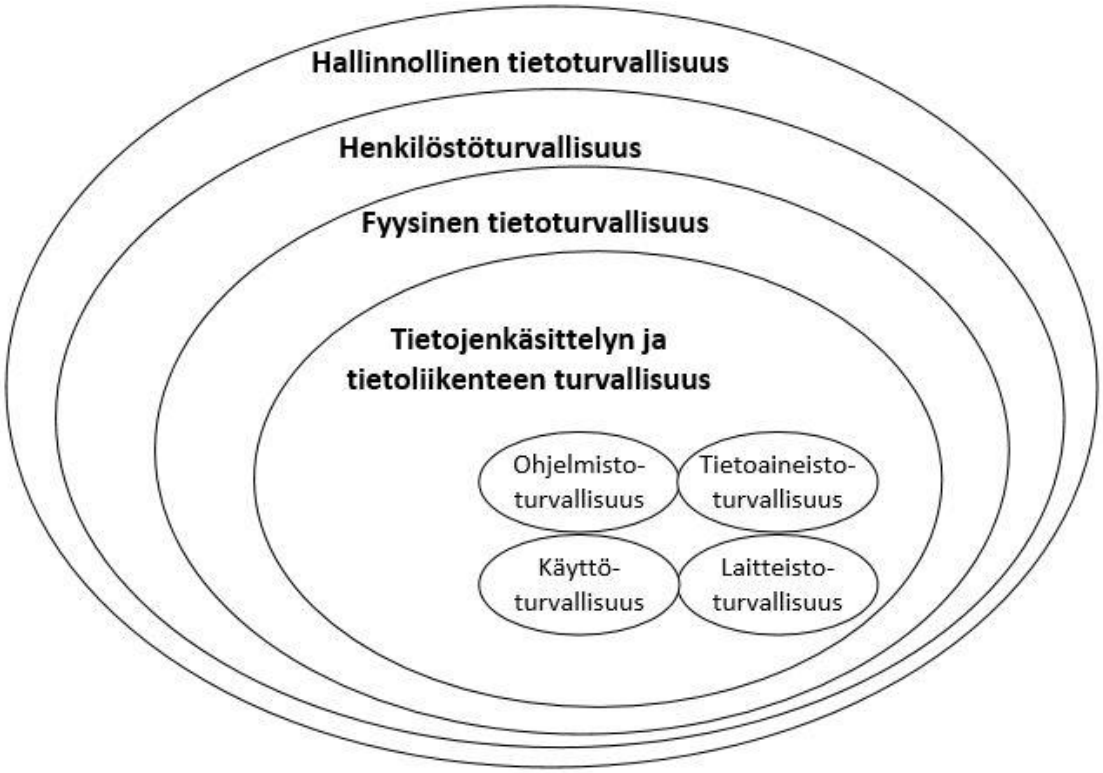
Kansalaisen asiointitili

Kansalaisen asiointitili on tarkoitettu viranomaisen ja kanasalaisen väliseen sähköiseen viestintään paperipostin sijasta. Palvelussa voi seurata asian käsittelyn etenemistä ja tarvittaessa toimittaa lisätietoja tai täydennyksiä hakemuksiin sekä saada päätösasiakirjat tiedoksi. (Valtiokonttori 2012)

3.2 Tietoturva

Perinteisesti tietoturvallisuuden tavoitteiden katsotaan koostuvan kolmesta osatekijästä. Tavoitteena on tiedon luottamuksellisuus, tiedon käytettävyys sekä tiedon eheys. Luottamuksellisuudella tarkoitetaan sitä, että tieto on vain sellaisten henkilöiden käytettävissä, jotka ovat niihin oikeutettuja. Käytettävyydellä tarkoitetaan sitä, että tieto on saatavissa, oikeassa muodossa ja riittävän nopeasti. Eheys tarkoittaa sitä, että tiedot eivät sisällä virheitä eli tiedot pitävät paikkansa. (Hakala ym. 2006, 4.) Näiden kolmen osa-alueen lisäksi tietoturvan osatekijöiksi luetaan usein myös todennus, vastuullisuus ja kiistämättömyys. Todennuksella tarkoitetaan sitä, että osapuolet ja käyttäjät ovat luetetusti tunnistettu. Vastuullisuudella tarkoitetaan tietojen jäljitettävyyttä. Jäljitettävyys on sitä, että voidaan jälkikäteen todentaa kuka tietoa on käyttänyt tai muuttanut. Kiistämättömyydellä tarkoitetaan todisteiden luomista tietojenkäsittelytapahtumista niin, etteivät osapuolet voi jälkikäteen kiistää osuuttaan tietojenkäsittelyyn. (Pitkänen ym. 2013, 216.) Näitten tietoturvan tavoitteiden voidaan katsoa olevan myös tietoturvallisen kodin tavoitteena.

Tietoturvan katsotaan perinteisesti kostuvan seuraavista osa-alueista: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen tietoturvallisuus sekä tietojenkäsittelyn ja tietoliikenteen turvallisuus, joka jakautuu ohjelmisto-, tietoaineisto, käyttö- ja laitteistoturvallisuuteen (Kuva 3).



KUVA 3. Tietoturvan klassinen sipulimalli

Kodissa hallinnollinen tietoturvallisuus voi olla vaikeasti hahmotettava kokonaisuus, mutta mielestäni se voidaan käsittää yhteisesti sovittuina käytäntöinä. Niitä ei ole useasti kirjattuna tai dokumentoituna. Näitä yhteisesti sovittuja käytäntöjä voisi olla esimerkiksi tieto siitä, kuka on vastuussa tietokoneiden päivittämisestä.

Henkilöstöturvallisuudeksi kodissa voidaan ajatella sisältävän esimerkiksi lasten opastamisen turvalliseen verkkokäyttäytymiseen sekä käyttöoikeuksien rajaamisen niin, ettei lapsilla ja nuorilla ole mahdollisuutta tehdä sellaisia asennuksia, jotka vaarantavat kodin tietoturvan. Fyysinen turvallisuus kodissa ei poikkea yritysten vastaavasta, muuten kuin ympäristön koossa. Myös koti pitäisi suojata fyysisiltä uhkilta, kuten varkauksilta, tulipaloilta ja muilta tahallisilta tai tahattomilta vahingoilta. Myös tietojenkäsittelyn ja tietoliikenteen turvallisuuden ongelmat ja ratkaisut ovat samat kuin yritysmaailmassa. Laitteiden, ohjelmistojen ja tietoverkkojen täytyy toimia oikein, luotettavasti, turvallisesti niin, että tiedot on tallennettu ja varmuuskopioitu asianmukaisesti.

Tietoturvaopas sähköisen palvelun tarjoajalle (Luoti 2006, 9.) mukaan sähköinen palvelu on turvallista silloin, kun

- sen on tuottanut luotettavat taho

- sen sisältö ja toiminta on luotettavaa
- se on saatavilla sovittujen ehtojen mukaisesti
- maksaminen palvelussa on luotettavaa
- käyttäjien henkilökohtaisten tietojen on säilyttävä luottamuksellisena
- palvelun käyttäminen onnistuu ainoastaan oikeudet omaavalta henkilöltä
- ulkopuolisen tekemän käyttäjän harhaanjohtamisen tulisi olla hankalaa.

Kodissa sähköisen palvelun turvallisuuden ja luotettavuuden arviointi voi olla haastavaa, varsinkin mikäli palvelun tarjoaja on ulkomainen toimija. Luotettavuutta pyritään arvioimaan verkkosivuja arvioimalla sekä etsimällä muiden asiakkaiden kokemuksia kyseisestä toimijasta. Lisäksi on olemassa yksityisille henkilöille palveluita, jotka tekevät sivujen luotettavuuden arviointia automaattisesti. Tällainen on esimerkiksi suomalainen Web of Trust (WOT). (Kuluttajaliitto 2014)

3.3 Ydintieto ja pilvipalvelut

Ydintieto on liiketoiminnan kannalta kriittistä tietoa. Kriittistä tietoa yrityksissä on esimerkiksi asiakas- ja tuotetiedot. Ydintieto on usein pysyvää ja sitä on tallennettu useisiin tietojärjestelmiin ja myös eri organisaatioihin. On tärkeää, että ydintiedon hallintaan on selkeät prosessit. Tiedon elinkaarenhallinta on myös huomioitava. (Andreasson ym. 2013, 213.)

Ydintietojen hallinnalla tavoitellaan luotettavaa ja hyvälaatuista tietoa, jonka on oltava nopeasti saatavilla. Toiminta-arkkitehtuurissa kuvataan ydintiedon hallintamalli, jolla määritetään organisaatio, roolit ydintiedon hallintaan sekä tiedon hallinnan prosessit. Tietoarkkitehtuurissa määritetään käsite- ja tietomallit. Teknologia arkkitehtuuri luo teknisiä edellytyksiä ydintiedon hallintaan ja tietojärjestelmäarkkitehtuurin näkökulmasta katsottuna ydintietoja käsitellään kuten muitakin tietojärjestelmiä. (Andreasson ym. 2013, 222–224.)

Onko kodissa ydintietoa? Edellä mainittuun viitaten, mielestäni kodissa on paljon sellaista tietoja, joka on kodin toimintojen kannalta kriittistä ja jonka eheys, käytettävyys ja luottamuksellisuus on varmistettava. Kriittistä tietoa kodissa ovat esimerkiksi käyttäjätunnukset ja salasanat, valokuvat, sopimukset, takuutodistukset, koulutodistukset, passit, yhdistystoimintaan liittyvät asiakirjat, sukututkimusmateriaalit, opiskeluun

liittyviä tiedostot jne. Ydintieto voi kodissa olla tallennettuna moneen eri muotoon ja paikkaan. Ydintieto voi olla paperisena tai sähköisenä, se voi olla tallennettuna kodin sisälle tai se voi olla tallennettuna esimerkiksi pilvipalveluun.

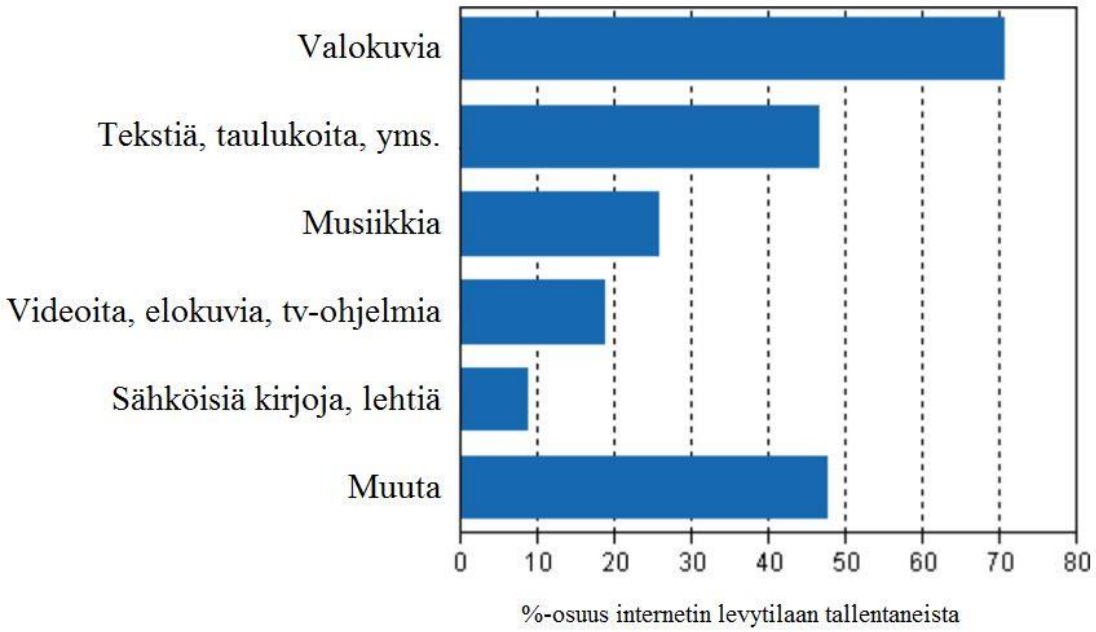
Pilvipalvelut ovat internetissä olevia, organisaation omia palveluita täydentäviä tai korvaavia palveluita. Pilvipalvelut voivat pitää sisällään ohjelmistoja, palveluita, levykapasiteettia tai laskentatehoa. Pilvipalvelut ovat yleistymässä merkittävästi, mutta palveluiden käyttöönottoon liittyy useita tietoturvakysymyksiä, jotka organisaation on mietittävä ennen palveluiden käyttöönottoa.

- missä tiedot sijaitsevat
- kuinka tiedot suojataan
- kuka pääsee käsittelemään tietoa ja kuinka käyttöä valvotaan?
- vastaako palvelujen tietoturva asiakkaan vaatimuksia?
- onko riskianalyysit tehty?
- onko tietoturva-asiat huomioitu riittävä tarkasti sopimuksissa vai onko menty tarjoajan "standardisopimuksen" mukaan?
- mitä ovat käytännön mahdollisuudet siirtyä pois käyttöön otetusta palvelusta.

(Andreasson ym. 2013, 26.)

Pilvipalveluiden käyttöönotto on helppoa ja tiedon tallentaminen niihin on vaivatonta. Pilvipalveluiden huonona puolena on, että ei voida olla täysin varmoja siitä, että tallennettuihin tietoihin ei olisi pääsyä muilla kun tiedon tallentajalla. Mikäli halutaan varmistaa tietojen yksityisyys, voidaan tiedot suojata salaamalla ne ennen tietojen tallentamista pilvipalveluun.

Pilvipalveluita käytti vuonna 2013 viidesosa 16 – 89-vuotiaista suomalaisista (Tilastokeskus 2013). Pilvipalveluihin tallennettiin valokuvia, tekstiä ja taulukukoita, musiikkia, videoita, elokuvia, tv-ohjelmia, sähköisiä kirjoja tai lehtiä. (Kuva 4).



KUVA 4. Viimeisten kolmen kuukauden aikana internetin levytilaan tallennettu aineisto 2013 (Tilastokeskus 2013).

Kun harkitaan kodin ydintiedolle tallennuspaikkaa pilvipalveluna, on tärkeää miettiä vastauksia seuraaviin kysymyksiin. Onko järkevää sijoittaa kodille tärkeää tietoa pilvipalveluihin? Useat pilvipalveluista sijaitsevat ulkomailla, eikä voida olla aivan varmoja siitä ketkä tietoja pääsevät katsomaan. Tärkeitä kysymyksiä on myös, kuinka käyttöönotetuista palveluista voidaan siirtyä pois ja ovatko tiedot siirrettävissä takaisin omaan hallintaan?

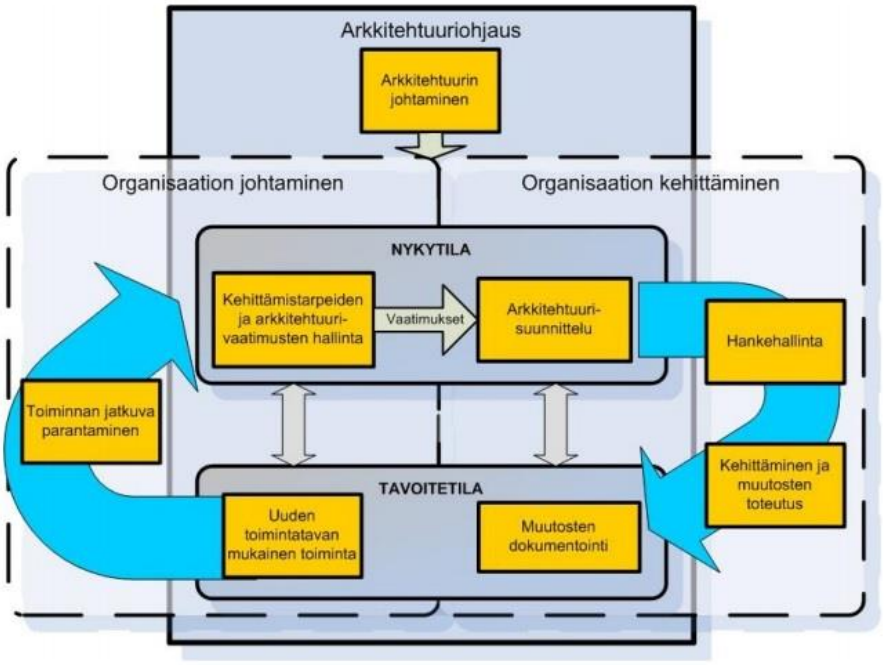
4 KOKONAISARKKITEHTUURI

Kokonaisarkkitehtuuri on väline, joka on tarkoitettu kehittämisen johtamiseen. Kokonaisarkkitehtuuri on suunnittelumenetelmä sekä suunnittelun dokumentointimenetelmä. Kokonaisarkkitehtuurilähtöinen kehittäminen tapahtuu prosessimallin mukaisesti, jossa varmistetaan, että järjestelmät ovat yhteensopivia niin sisäisesti kuin myös sidosryhmien järjestelmiin. Kokonaisarkkitehtuuri varmistaa, että hankittava ratkaisu on tarpeellinen, tarkoituksenmukainen eikä vastaavaa ratkaisua ole jo käytössä muualla organisaatiossa ja tämä kaikki tehdään ennen kuin uuden ratkaisun tai mallin kehittäminen on alkanut. (Andreasson ym. 2013, 220–221.)

4.1 Kokonaisarkkitehtuuri

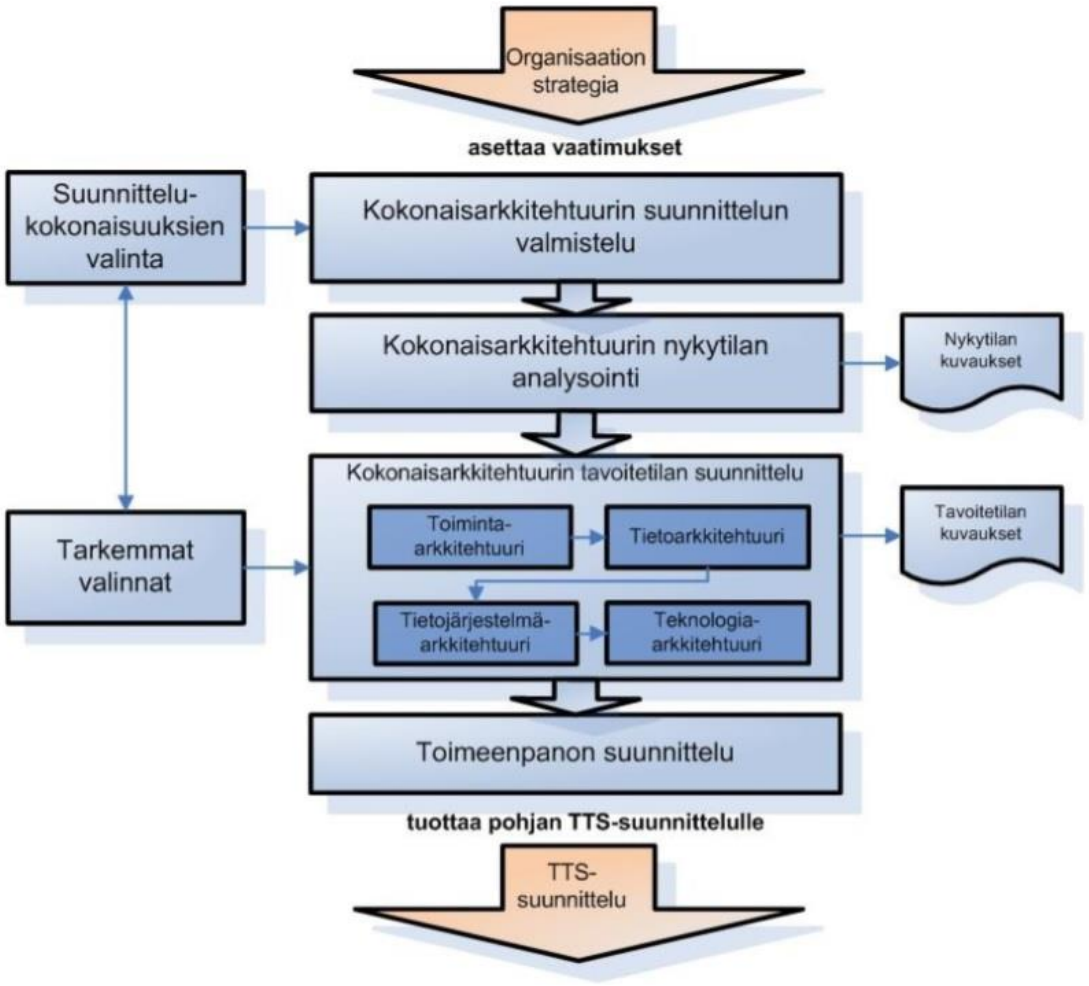
Julkishallinnon suosituksessa JHS179 (ICT-palveluiden kehittäminen: kokonaisarkkitehtuurin kehittäminen) määritetään se, millaista menetelmää julkishallinnon tulisi käyttää kokonaisarkkitehtuurin suunnittelussa. Suositus antaa suunnittelumenetelmän, viitekehyksen, kuvaustavat, mallit kokonaisarkkitehtuurin kuvaamiselle. JHS179 suositus on tarkoitettu lähinnä julkishallinnolle, mutta siitä on hyötyä myös yksityiselle sektorille. (Andreasson ym. 2013, 220–221.)

Julkisen hallinnon neuvottelukunnan laatiman JHS:n suosituksen 179 liitteen 1 mukaan kokonaisarkkitehtuurilähtöinen kehittäminen on normaalia kehittämistoimintaa, jota ohjataan kokonaisarkkitehtuurin välinein ja menetelmin. Kehittäminen on jatkuvaa toimintaa, jossa aiempien kehittämistoimenpiteiden arviointi antaa pohjan uudelle kehittämiskierrokselle (Kuva 5).



KUVA 5. Arkkitehtuuriohjaus organisaation kehittämisen syklissä

Kokonaisarkkitehtuurin suunnittelu voidaan jakaa neljään vaiheeseen, kokonaisarkkitehtuurin suunnittelun valmistelu, kokonaisarkkitehtuurin nykytilan analysointi, kokonaisarkkitehtuurin tavoitetilan suunnittelu sekä toimeenpanon suunnittelu. (Kuva 6)



KUVA 6. Kokonaisarkkitehtuurin suunnitteluprosessi (JHS 179)

JHS:n suosituksen 179 liite 4. mukaan (nykytilan ja tavoitetilan kuvaus) nykytilan kuvaaminen kannattaa aloittaa fyysisestä tasosta, loogisen tason kautta, kohti käsitteellistä tasoa. Konkreettisten osien kuvaaminen on helpompaa kuin suunnitteluperusteet, joilla nykytilaan on tultu. Nykytilan kuvaaminen on suositeltavaa aloittaa toiminnan kuvaamisesta ja edetä tieto- ja tietojärjestelmäarkkitehtuurin kautta teknologia-arkkitehtuurin kuvaamiseen. Tavoitetilan kuvaaminen tehdään päinvastaisessa järjestyksessä kuin nykytilan kuvaus. Suunnittelussa edetään periaatteellisista linjauksista, kuten strategiat kohti konkreettisia linjauksia. Näin varmistetaan, että tehdyt linjaukset toteutuvat myös muilla suunnittelun tasoilla.

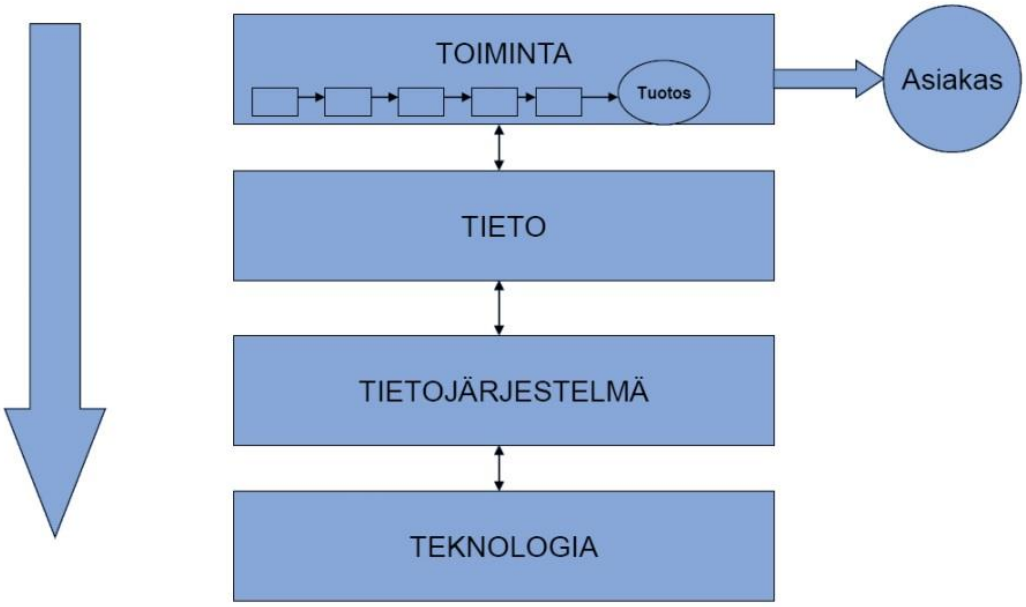
Toimeenpanon suunnittelussa laaditaan ylätason toimeenpanosuunnitelma, jolla tavoitetilaan päästään. Toimeenpanosuunnitelmaa käytetään toiminnan ja talouden suunnittelussa, jossa sovitut kehittämisalueet tarkennetaan kehittämishankkeiksi ja kehittämisprojekteiksi. (JHS 179)

4.2 Kodin kokonaisarkkitehtuuri

Alle 55-vuotiaista lähes kaikki käyttävät Internetiä. Älypuhelin on 56 prosentilla väestöstä. 80 prosenttia suomalaisista 16 – 74-vuotiaista oli internetissä päivittäin ja 89 prosentilla heistä oli jokin tietokone ja internet-yhteys kotonaan. 80 prosenttia laskuista maksetaan internetissä. Vuonna 2013 verkkokaupan arvo oli 7 miljardia euroa. (Tilastokeskus 2013).

Kodeissa on siis käytössä suuri määrä tietoteknisiä laitteita, mutta vain rajallinen määrä resursseja kehittämiseen. Perheenjäsenten kiinnostus ja kyky kehittää kodin tietojärjestelmiä vaihtelee suuresti. Kuitenkin jokaisen täytyisi olla kiinnostunut siitä, että asiointi, jota nykyisin lähes jokaisessa kodissa tehdään, olisi turvallista.

Kodin tietojenkäsittely-ympäristöä voidaan tarkastella myös kokonaisarkkitehtuuri näkökulmasta (Kuva 7). Mielestäni kuitenkin paljon suppeammassa merkityksessä kun julkishallinnossa ja yrityksissä kokonaisarkkitehtuurilla ymmärretään.



KUVA 7. Kokonaisarkkitehtuuri (Nenonen, 2012)

Kodin kokonaisarkkitehtuuriin voidaan ymmärtää sisältävän kaikki kokonaisarkkitehtuurin näkökulmat eli toiminta, tieto, tietojärjestelmät ja teknologia. Suppeampaa näkökulmaa voidaan perustella sillä, että kokonaisarkkitehtuurin kuvaaminen JHS 179 mukaisesti sisältää osia, kuten arkkitehtuuriperiaatteet, tietojärjestelmäsalkku sekä

integraatioratkaisut, eikä tällaisia kodeissa ole. Julkishallinnon suositusten perusajatus on kuitenkin hyvin sovellettavissa myös kodeissa. Ajatuksena on, että ensi kuvataan nykytila, johon saadaan eri selvitysten ja kuvausten kautta muutostoiveita. Näiden perusteella priorisoidaan ja päätetään toteutettavat muutokset, jotka kuvataan tavoitetilan kuvauksessa. Tavoitetilan kuvauksen tekemisen jälkeen siirrytään toteuttamisvaiheeseen, jolloin tehdään tarvittavat muutokset, jotta päästäisiin kuvattuun tavoitetilaan. Tämän jälkeen palataan kierroksen alkuun, jossa jälleen kuvataan nykytila.

5 KODIN SÄHKÖISEN ASIOINNIN TIETOTURVAN KEHITTÄMINEN

Tietoturvallisen kodin lähtökohtana täytyisi olla ajatus siitä, että on olemassa tärkeää tietoa tai omaisuutta, joka täytyy jotenkin suojata. Käsitykseni mukaan, perustuen perheessäni suoritettuun havainnointiin, yksi suurimmista kodin tietoturvaan liittyvistä uhista liittyy ohjelmistojen päivittämättömyyteen sekä tiedon varastointiin. Useinkaan tietoturvapäivityksiä ei ole asennettu, tiedon varastointia ei ole suunniteltu eikä tietoa ei ole suunnitelmallisesti varmuuskopioitu. Usein ei ole myöskään tietoa siitä, mitä kaikkea tietoa on varastoitu ja mihin.

Hyvänä esimerkkinä edellä mainitusta ovat valokuvat. Niitä on tallennettuna mm. erilaisille muistikorteille, tietokoneiden kiintolevyille, usb-kiintolevyille. Mielestäni suurena uhkana on, että suuri osa nykyaika otettavista valokuvista häviää muistivälineiden tuhoutumisen vuoksi. Mikäli valokuvia kuitenkin säilyy jälkipolville, niistä ei tiedetä missä ne on otettu, keitä kuva esittää jne. Jotta mahdollisilta uhkilta pystytään suojautumaan ja kodin sähköistä asiointia kehittämään, täytyy ensimmäisenä olla käsitys siitä, kuinka tällä hetkellä toimitaan sekä mikä tieto on tärkeää ja suojaamisen arvoista. Kodissa tyypillisiä suojattavia asioita voisivat olla esimerkiksi pankkiyhteydet, valokuvat, musiikki, käyttäjätunnukset ja salasanat sekä opiskeluun, työhön liittyvät tiedot ja tiedostot.

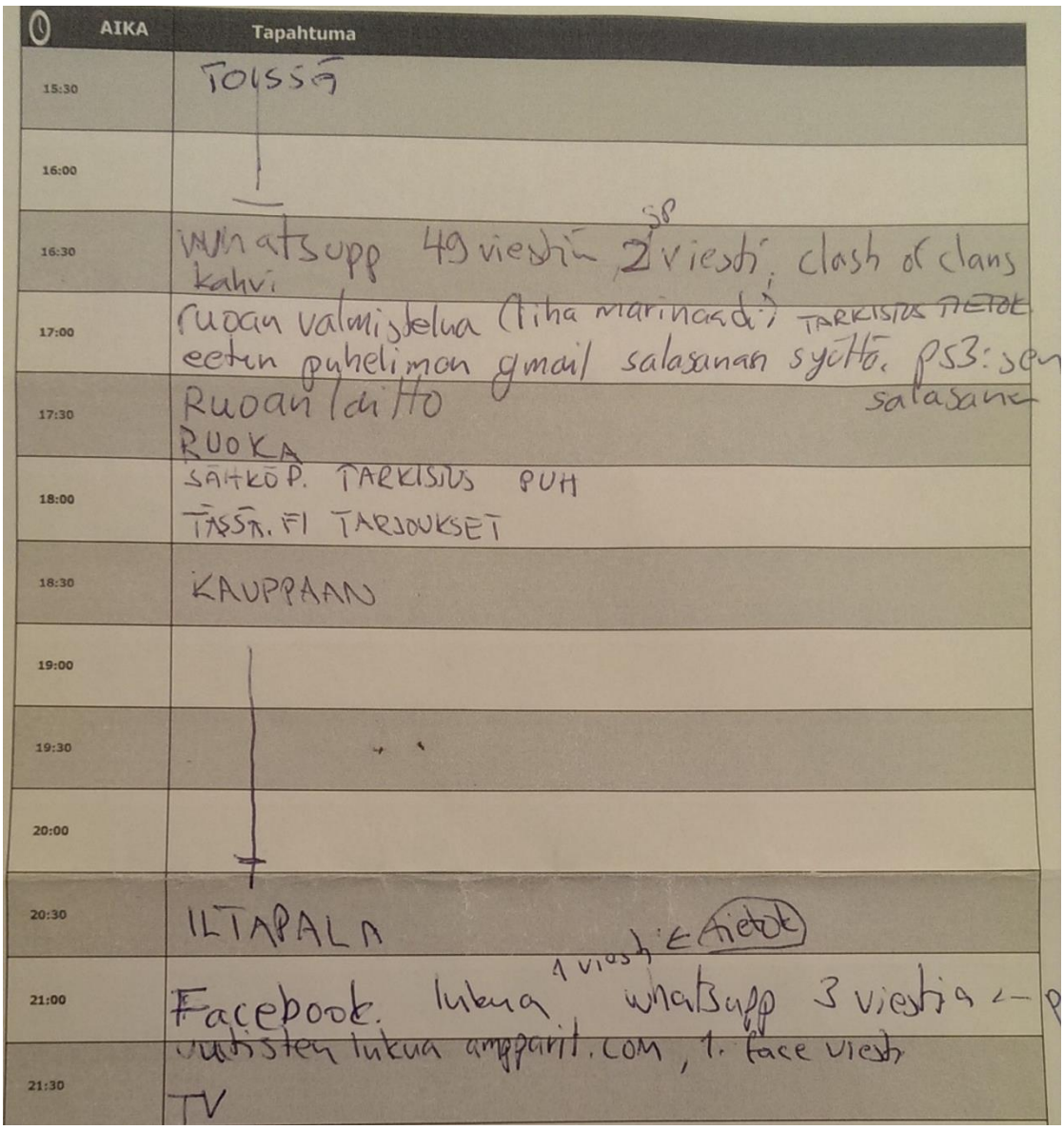
5.1 Nykytilan kuvaus

Nykytilan kuvauksessa esitetään kodin sähköisen asioinnin nykytila käyttämällä kokonaisarkkitehtuurin kuvausmenetelmiä. Nykytilasta ei ole ennen opinnäytetyötä olemassa minkäänlaista kirjallista kuvausta. Nykytilan kuvauksessa tarvittavan tiedon

kerääminen toteutetaan havainnoimalla kodin toimintaa. Havainnointia suoritetaan keräämällä tietoa lomakkeella ja analysoimalla lomakkeella kerättyä tietoa. Tämän lisäksi tietoa kerätään kodin laitteista ja ohjelmista niiltä osin kun se on tarpeen nykytilanteen kartoittamiseksi.

5.1.1 Havainnointi

Havainnoitavaan perheeseen kuuluu kaksi vanhempaa, yksi toisella paikkakunnalla opiskeleva aikuinen tytär ja 11 ja 14 vuotiaat pojat. Havainnointi toteutettiin kahdessa jaksossa 13.12.2013 ja 23.12.2013 ja kesti yhteensä 48 tuntia. Havainnoinnin ajankohdat valittiin perheen vanhempien palkkapäivien perusteella. Palkkapäivä valikoitui sen olettamuksen perusteella, että palkkapäivänä sähköisten palveluiden käyttö on todennäköisempää kuin muina päivinä. Ensimmäiseen havainnointijaksoon osallistui 4 henkilöä ja toiseen 5 henkilöä. Havainnointi toteutettiin jakamalla perheenjäsenille havainnointilomake (Kuva 8), johon perheenjäsenet merkitsivät päivän tapahtumat. Tavoitteena oli saada tietoa siitä millaisia sähköisiä palveluita perhe käyttää ja kuinka usein.



KUVA 8. Lehkosen perheen havainnointilomake

Havainnointijakson jälkeen lomakkeet kerättiin ja niistä poimittiin sähköiseen asiointiin liittyvät tapahtumat.

Tulosten pelkistäminen

Havainnoinnin tuloksia pyrin vertaamaan tilastokeskuksen ajankäyttötutkimuksen tuloksiin. Ongelmaksi muodostui se, ettei tilastokeskuksen ajankäyttötutkimuksen jaottelussa ole eritelty sähköisten palveluiden käyttöön käytettävää aikaa. Verkko-ostokset esimerkiksi täytyi sijoittaa ostokset kohtaan, jossa olivat normaalitkin ostokset. Lisäksi nykyisin hyvinkin yleistä Internetissä tapahtuvaa suoratoisto palveluiden

katsomista oli hyvin vaikeaa sijoittaa jaotteluun. Suoratoistopalveluiden katsominen olisi sopinut ainakin seuraaviin kohtiin elokuvat, tv:n katselu ja atk-harrastus.

Toteutinkin havainnoinnin pelkistämisen tekemällä jaottelun, jossa eri sähköiset palvelut on kerätty taulukon 2 mukaisesti. Sähköisen palvelun käytöksi katsottiin internetissä olevan palvelun käyttö tietokoneella, tabletilla, puhelimella tai pelikoneella. Taulukkoon on kerätty asiointikerrat.

Tulkinta

Havainnoinnin perusteella perheessä aikaa käytetään nuorten osalta lähinnä pelaamiseen, suoratoistopalveluihin sekä musiikin kuunteluun. Aikuisilla käyttö on monipuolisempaa ja mukana on myös raha-asioiden hoitoa, ostoksia, sosiaalisen median käyttöä ja uutisten seuraamista.

TAULUKKO 2. Lehkosten kodin sähköisten palveluiden käyttö

	Ajankäyttö prosentteina	Yhteensä kertaa	Hlö 1	Hlö 2	Hlö 3	Hlö 4	Hlö 1	Hlö 2	Hlö 3	Hlö 4	Hlö 5
			ajankäyttö 15.12.2013				ajankäyttö 23.12.2013				
01 Suoratoistopalvelut	14,8	9			2			1	3	2	1
02 Pelaaminen	21,3	13	1			3	2		3	4	
03 Sosiaalinen media	9,8	6	2				2				2
04 Ostokset verkossa	3,3	2	2								
05 Raha-asioiden hoito	4,9	3	1	1				1			
06 Sähköinen asiointi	1,6	1	1								
07 Sähköposti	14,8	9	5	1			3				
08 Pikaviestipalvelut	13,1	8	2				5				1
09 Musiikin kuuntelu	4,9	3							1	1	1
10 Uutiset	3,3	2	1				1				
11 Muu nettikäyttö	8,2	5					3		1		1
	100	61	15	2	2	3	16	2	8	7	6

Laitteet toimintoihin valittiin satunnaisesti sen mukaan, millä kyseisen toiminnan pystyi tekemään ja mikä laite oli sillä hetkellä vapaana. Esimerkiksi suoratoistopalveluita katsottiin kannettavalla tietokoneella, puhelimella, pelikoneella sekä myös tabletilla. Pankkipalveluita ja sähköistä asiointia käytettiin pääasiassa kannettavalla tietokoneella tai puhelimella. Sähköpostia luetaan puhelimella, tabletilla ja kannettavalla tietokoneella

Kehitysehdotukset

Kodissa käytetään laitteita lähinnä sen mukaan, mitä sillä pystytään tekemään. Laitteen valintaa ei vaikuta se, kuinka turvallista laitteen käyttö on ja onko laitteen ohjelmistot päivitetty. Mikäli sähköiseen asiointiin valitaan laite, jota ei ole vähään aikaan käytetty ja on näin ollen päivittämättä, saattaa sen käyttöön liittyä tietoturvariskejä. Kehitysehdotuksena on, että viralliseen asiointiin käytetään vain päivitettyjä tietoturvallisia laitteita.

Kodissa voidaankin ajatella olevan kahden eri turvaluokan toimintoja ja laitteita. Ensimmäisen turvaluokan toimintoja olisivat pankkiasioiden hoito, viranomaispalveluiden käyttö eli yleensä kaikki toiminnot, jossa vaaditaan vahvaa tunnistamista. Kodissa voitaisiin määritellä ensimmäisen turvaluokan laitteet, joilla näitä toimintoja tehtäisiin. Nämä laitteet pidettäisiin päivitettyinä ja tietoturvallisina. Kodin verkon voisi myös jakaa turvaluokkiin. Ensimmäisen turvaluokan verkkoon voisi kytkeytyä vain ko. luokan koneilla. Sovellusten ajantasaisuuden varmistamiseksi, voitaisiin ottaa käyttöön jokin sopiva työkalu ohjelmistojen ajantasaisuuden varmistamiseksi. Tällainen ohjelmisto voisi olla esimerkiksi Secunia PCI.

Perustelut

Ohjelmistojen päivittäminen on tärkeää, koska päivittämättömät ohjelmat sisältävät ohjelmistohaavoittuvuuksia, joita rikolliset ja haittaohjelmat käyttävät asentaakseen haitallisia ohjelmia.

Ohjelmistoihin jää aina väistämättä virheitä. Osa virheistä tulee ilmi ohjelmistoja kehitettäessä ja joistakin virheistä raportoivat ohjelmistojen käyttäjät. Nämä virheet ovat

tunnettuja virheitä. Ohjelmistojen toimittajat eivät aina kuitenkaan aina julkaise virheitä ja virheitä korjataankin usein vasta ohjelman julkaisun jälkeen. Ohjelmistoihin jää kuitenkin myös virheitä, joita ei löydetä. Näiden virheiden määrä on tuntematon. Tunnetut ohjelmistovirheet johtavat ohjelmistohaavoittuvuuksiin joita rikolliset tahot käyttävät hyväkseen. (Saleh, 2009, 6–7.).

Manzuikin ym. (2007, 2) mukaan ohjelmistohaavoittuvuus voi ohjelmiston virheen lisäksi koskea myös ohjelmiston väärin konfigurointia. Ohjelman ei siis välttämättä tarvitse olla päivittämätön tai sisältää ohjelmointivirhettä. Riittää että jonkin ohjelmistossa oleva asetus on virheellinen.

Secunia PCI on ohjelma, jolla voi tarkistaa tietokoneen ohjelmistojen ajantasaisuuden. Ohjelmisto tarkistaa onko tietokoneessa haavoittuvuuksia, jotka altistavat tietokoneen hyökkäyksille. Ohjelma sisältää myös mahdollisuuden ohjelmistojen päivittämisen Secunian avulla. Ohjelma ei korvaa virustarkistusta, vaan täydentää sitä. Ohjelma on yksityiskäyttäjille ilmainen. Ohjelmasta on myös Android versio, jolla voi tarkistaa puhelimessa olevat haavoittuvuudet ja päivittää ne. (Secunia 2014)

5.1.2 Arkkitehtuurinkuvaukset

Arkkitehtuurikuvauksissa on kuvattu Lehkosen perheen toiminta-arkkitehtuuri, tieto-arkkitehtuuri, tietojärjestelmäarkkitehtuuri ja teknologia-arkkitehtuuri. Kuvaukset perustuvat kodissa suoritettuun havainnointiin sekä kodin tietojärjestelmistä kerättyyn tietoaan.

Toiminta-arkkitehtuuri

Toiminta-arkkitehtuuri kuvaa organisaation toiminnan rakenteet kuten sidosryhmät, palvelut, tuotteet, prosessit ja organisaatiot. Toiminta-arkkitehtuuriin sisältyvät myös visiot ja strategiat, mikäli niitä on. Toiminta-arkkitehtuurin kuvauksiin sisältyvät loogisella tasolla prosessien kuvaaminen sekä käsitteellisellä tasolla sidosryhmät, niiden vaatimukset ja tavoitteet sekä palvelusalkku. (JHS 179)

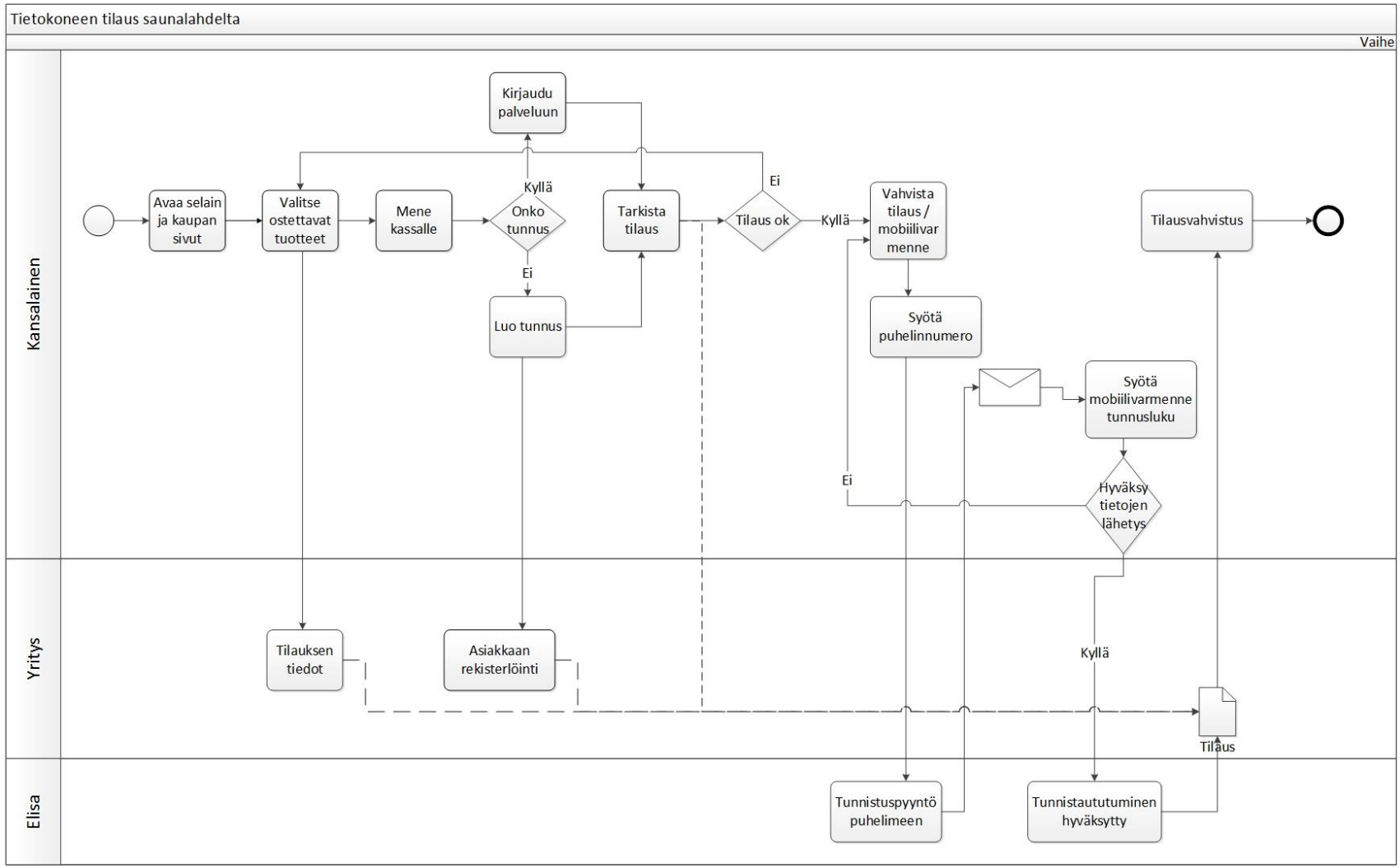
Toimintakuvauksessa kuvattiin Lehkosen perheen sidosryhmät (Taulukko 3) sekä prosessikuvauksella kuinka sähköisiä palveluita käytetään. Kuvattaviksi sähköisiksi palveluiksi valikoitui tilaus verkkokaupasta (Kuva 9) sekä laskujen maksun prosessi.

TAULUKKO 3. Lehkosen perheen sidosryhmät

Lehkosen perheen sidosryhmät
Päivväys 9.2.2014'
Versio 1.0

Sidosryhmä		Kuvaus
Sidosryhmätyyppi	Nimi	kuvaus sidosryhmästä
Liittymätoimittja	**MPY**	ADSL-toimittaja, MPY-viihde toimittaja
Liittymätoimittja	**Saunalahti**	Matkapuhelinliittymätoimittaja
Liittymätoimittja	**Elisa**	Matkapuhelinliittymätoimittaja
Pankki	**Nordea**	Pääasiallinen paknkki
Pankki	**S-pankki**	Toissijainen pankki
Pankki	**Sampo-pankki**	Omaishoitaja pankki
Vakuutusyhtiö	**Tapiola**	Perheen vakuutusyhtiö
Luottokorttiyhtiö	**Luottokunta (Mastercard)**	Korttiluottoyhtiö
Luottokorttiyhtiö	**Visa**	Korttiluottoyhtiö
Puhelinvalmistaja	**Samsung**	Puhelinvalmistaja
Puhelinvalmistaja	**Htc**	Puhelinvalmistaja
Puhelinvalmistaja	**LG**	Puhelinvalmistaja
Ohjelmatoimittaja	**F-Secure**	Virustorjunnan toimittaja
Ohjelmatoimittaja	**Microsoft**	Käyttöjärjestelmän toimittaja
Ohjelmatoimittaja	**Google**	Käyttöjärjestelmän toimittaja
Vedonlyöntiyhtiö	**Veikkaus**	Vedonlyöntiyhtiö
Kaupan kanta-asiakas	**K-plussa**	Kauppa
Kaupan kanta-asiakas	**S-Bonus**	Kauppa
Julkinen palvelu	**Verottaja**	Verottaja
Julkinen palvelu	**Kela**	Lapsilisät ym tuet
Verkkokauppa	**Ebay**	verkkokauppa
Suoratoistopalvelu	**Netflix**	elokuvien suoratoistopalvelu
Suoratoistopalvelu	**Viaplay**	elokuvien suoratoistopalvelu
Nettimaksu	**Paypal**	sähköinen maksu
Verkkokauppa	**Verkkokauppa.com**	verkkokauppa
Taltioni palvelu	**Taltioni osuuskunta**	Terveystietojen tallenus
Musiikin suoratoisto	**Spotify**	Musiikki
Sähköinen tallennuspaikka	**Elisa**	Elektroninen kirja
Sähköinen tallennuspaikka	**Google music**	Levyjen talllennus / toistopalvelu
Sähköinen tallennuspaikka	**Google drive**	pilvitallennus
Sähköinen tallennuspaikka	**Microsoft skydrive**	pilvitallennus
Sähköinen tallennuspaikka	**dropbox**	pilvitallennus
Sähköinen tallennuspaikka	**younited**	pilvitallennus

Tunnistaminen sähköisiin palveluihin Lehkosten perheessä tapahtuu joko mobiilivarmenteella tai Tupas tunnistamisella. Mikäli vahvaa tunnistamista ei tueta, tunnistaminen tapahtuu käyttämällä käyttäjätunnus/salasana yhdistelmää. Maksaminen sähköisessä asioinnissa tapahtuu ensisijaisesti Paypal-maksulla tai luottokortilla. Mikäli kyseiset maksutavat eivät ole mahdollisia, voidaan käyttää myös laskua tai muuta luotettavaa maksutapaa.



KUVA 9. Tietokoneen tilaus Saunalahdelta

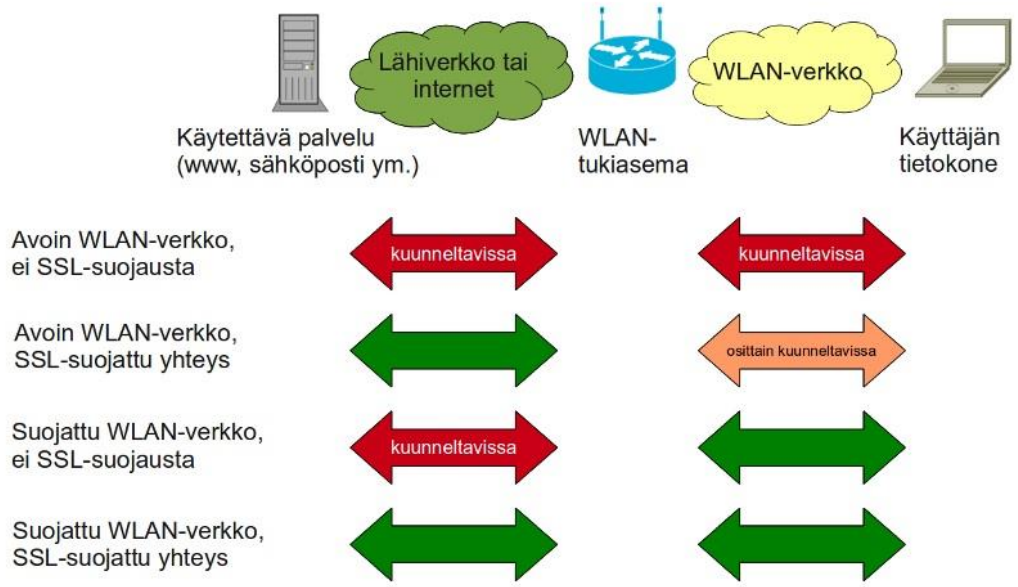
Toiminta sähköisessä asioinnissa on määritetty palveluntarjoajan toimesta, eikä siihen pääse yksittäinen käyttäjä tai asiakas helposti vaikuttamaan. Kodissa voidaan kuitenkin vaikuttaa siihen että käytettävät laitteet ja ohjelmat ovat turvallisia. Sähköisessä palveluissa käytettävien ja syntyvien tietojen säilytykseen ja käyttöön voidaan myös jossakin määrin vaikuttaa.

Kehitysehdotukset

Kehitysehdotuksena on, että määritetään sähköiseen asiointiin käytettävät koneet ja selainohjelmistot. Selainohjelmien asetukset käydään läpi, jotta niiden käyttö on turvallista. Sähköisessä asioinnissa käytettävien ja syntyvien tietojen säilytyksestä ja käsittelystä tehdään turvallista. Turvallisuudella tarkoitetaan sitä, että esimerkiksi tunnukset ja salasanat on säilytetty turvallisesti ja että palveluissa syntyvät asiakirjat on tallennettu turvallisesti ja että niiden hävitys on hoidettu asianmukaisesti. Sähköisessä asioinnissa ja asioinnissa joka tapahtuu kodin ulkopuolella, käytetään SSL suojattuja palveluita.

Perustelut

Mikäli käytetään kodin ulkopuolisia langattomia verkkoja, kuten esimerkiksi kahviloiden avoimia verkkoja, niitä voidaan helposti salakuulla. Salakuuntelulta voi tällöin välttyä käyttämällä vain sellaisia palveluita, jotka käyttävät SSL-suojattua yhteyttä. Myös SSL-suojatut sivut voivat sisältää salaamattomia osia. (Viestintävirasto 2011b)



KUVA 10. Langattoman verkon turvallisuus (Viestintävirasto 2011)

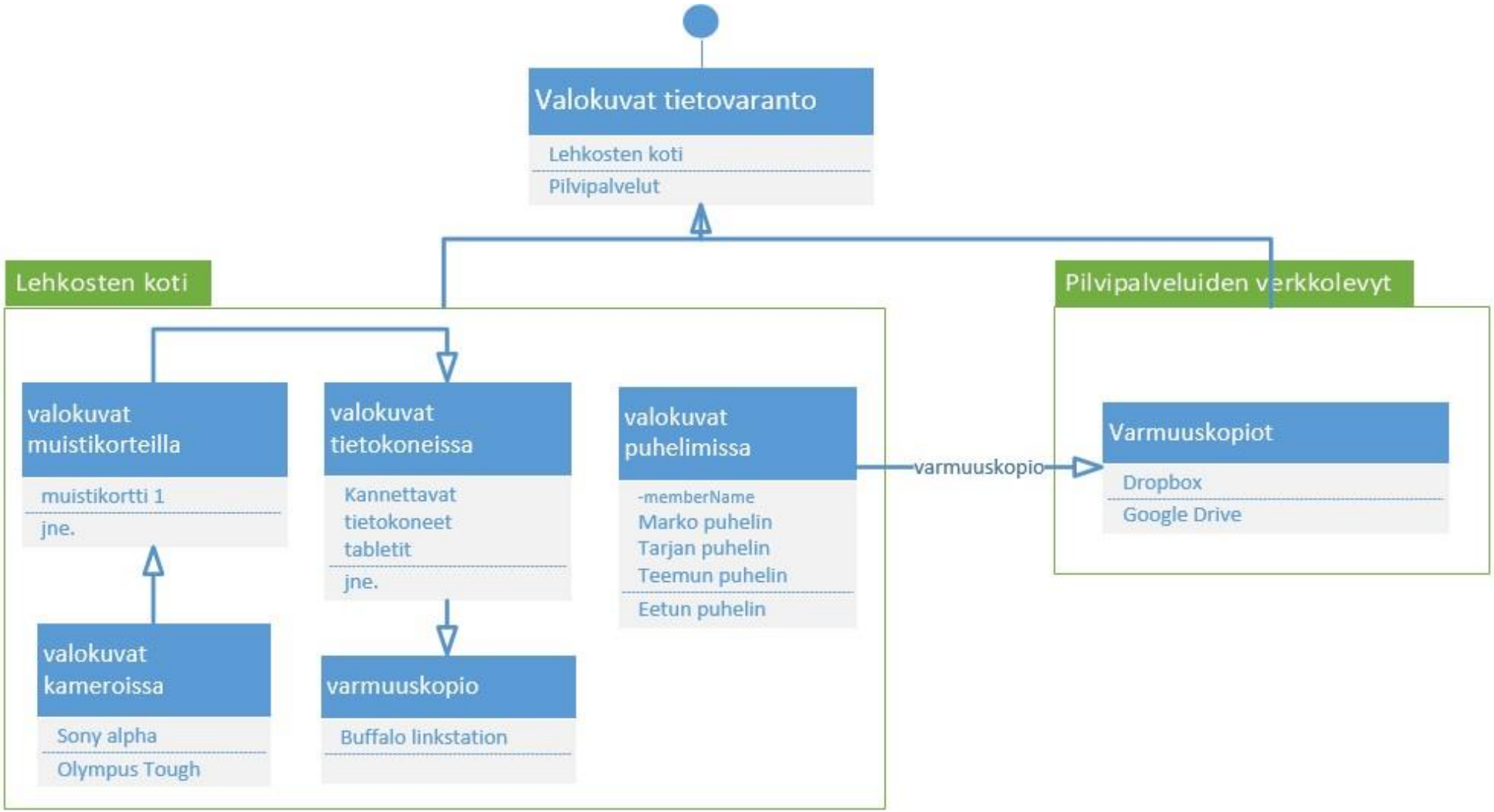
Sähköisiä palveluita pitäisi käyttää vain sivustoilla, joiden yhteyden aikainen liikenne salataan. Tällaisen yhteyden tunnistaa siitä, että sivuston osoite on muotoa https eikä http. Salatun yhteyden merkiksi selaimen tilarivilillä on lukon kuva. Liikenne on tällöin suojattu SSL-suojauksella ja sivustot käytävät hyväkseen varmenteita. Varmenteen ja sivun osoitteen pitäisi vastata toisiaan. (Viestintävirasto 2011a)

Tietoarkkitehtuuri

Tietoarkkitehtuuri tarkoituksena on selvittää organisaation ydin- ja palveluprosessien käytössä oleva keskeinen tietopääoma sekä kuvata tiedon rakenne ja tietojen väliset suhteet. Tavoitteena on tiedon löytymisen, välittämisen ja hallinnan helpottaminen. Tietoarkkitehtuurin suunnittelussa pyritään tietojen ja niiden rakenteiden vakiointiin sekä mahdollistamaan tiedon uudelleenkäyttöä. Tietoarkkitehtuurin kuvaukseen kuuluvat fyysisellä tasolla sanastot, loogisella tasolla loogiset tietovarannot, tietovirtakuvaus sekä päätietoryhmien kuvaus. Käsitteellisellä tasolla kuvataan käsitemalli. (JHS 179).

Tietoarkkitehtuurin kuvaamisella pyritään JHS:n suositusten mukaan kuvaamaan mikä on tärkeää tietoa ja missä se sijaitsee. Tämän vuoksi valitsin tietoarkkitehtuurin kuvaustavaksi tietovarantojen kuvaaminen. Tietovarantojen kuvaamisella saadaan mielestäni riittävästi tietoa siitä, mikä on Lehkosten perheessä keskeistä tietopääomaa ja

missä se sijaitsee. Tietovarantojen kuvaamisessa on lisäksi yhdistetty loogisten ja fyysisten tietovarantojen kuvaaminen. Esimerkki tietovarannon kuvaamisesta on kuvassa 11.



KUVA 11. Lehkosten perheen valokuvien tietovarannon kuvaus

Havainnointiin ja tietovarantojen kuvaamiseen perustuen tärkeäksi eli ydintiedoksi Lehkosten kodissa määritettiin valokuvat, musiikki, ostoksiin ja laskujenmaksuun liittyvät tiedot, salasanat, yhteystiedot sekä asennuskoodit. Valokuvat ovat tärkeitä siksi, että niissä säilytetään tietoa tuleville sukupolville. Musiikki ja asennuskoodit ovat tärkeitä niihin käytetyn rahan vuoksi. Yhteystietojen tärkeys perustuu siihen, että niiden uudelleenkerääminen on työlästä. Salasanat ovat tärkeitä siksi, että niiden häviäminen estää pääsyn sähköisiin palveluihin ja niiden joutuminen väärien henkilöiden haltuun voi aiheuttaa paljon vahinkoa. Pankkitunnusten varkaus voi johtaa rahalliseen menetykseen. Sähköpostin tai sosiaalisen median tunnusten varkaus voi johtaa identiteettivarkauden kohteeksi. Verkkokauppojen salasanojen varkaus mahdollistaa verkko-ostokset salasanavarkaille. Salasanat on muodostettu vaihtelevan käytännön mukaisesti ja salasanojen pituus vaihteli riippuen palvelusta, neljästä merkistä aina kahteentoista merkkiin. Osassa salasanoista on käytetty myös erikoismerkkejä ja numeroita, mutta ei kaikissa. Salasanojen säilytys oli toteutettu tallentamalla ne salasanalla suojattuun tiedostoon, paperille tai henkilön muistiin.

Kehitysehdotukset

Tiedot on tallennettuina moneen paikkaan ja moneen kertaan. Esimerkkinä valokuvat. Valokuvat eivät ole tallennettuna yhteen paikkaan, eikä niitä ole mitenkään järjestelty. Kehitysehdotus on tallennettujen tietojen läpikäynti ja yhteisen tallennuspaikan löytäminen. Lisäksi on sovittava, kuinka tiedot tähän yhteiseen tallennuspaikkaan viedään ja kenen vastuulla tietojen vienti, ylläpito on. Tämä yhteinen tallennuspaikka varmistetaan siten, että tiedot ovat palautettavissa mikäli ne jostakin syystä tuhoutuvat.

Salasanat muutetaan suositusten mukaisiksi. Salasanojen säilytykseen suositellaan käyttämään joko salasanapalvelua tai siirtämään salasanat turvalliseen ja varmistettuun säilytykseen. esimerkiksi (paperi/muistitikku).

Perustelut

Vahva tunnistaminen on vähentänyt käyttäjätunnusten ja salasanojen tarvetta. Tästä huolimatta moneen palveluun täytyy kirjautua käyttämällä käyttäjätun-

nus/salasanaparia. Salasanojen laatuun olisikin tärkeä kiinnittää riittävästi huomiota, jotta niiden käyttäminen olisi mahdollisimman helppoa ja turvallista.

Millainen on turvallinen salasana? Hyvän salasanan laatimiseen löytyy moniakin ohjeita. Yksi on esimerkiksi Cert.fi (2011) palvelun tiedote: Vaihda salasanasi vahvempiin, jossa hyvän salasanan tunnusmerkkejä ovat:

- hyvä salasana ei löydy sanakirjoista eikä se ole kenenkään nimi
- huono salasana ei muutu hyväksi lisäämällä sen jatkoksi numeroita
- hyvä salasana on riittävän pitkä (8 merkkiä on aivan liian vähän, 15 merkkiä on sopiva lähtökohta)
- hyvää salasanaa ei ole kierrätetty eri palveluissa.

Useissa ohjeissa, kuten esimerkiksi valtiovarainministeriön henkilöstön tietoturvaohjeessa, hyvän salasanan tunnusmerkeiksi nimetään myös että salasanan täytyy sisältää isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä. (Vahtiohje 4 2013, 13.)

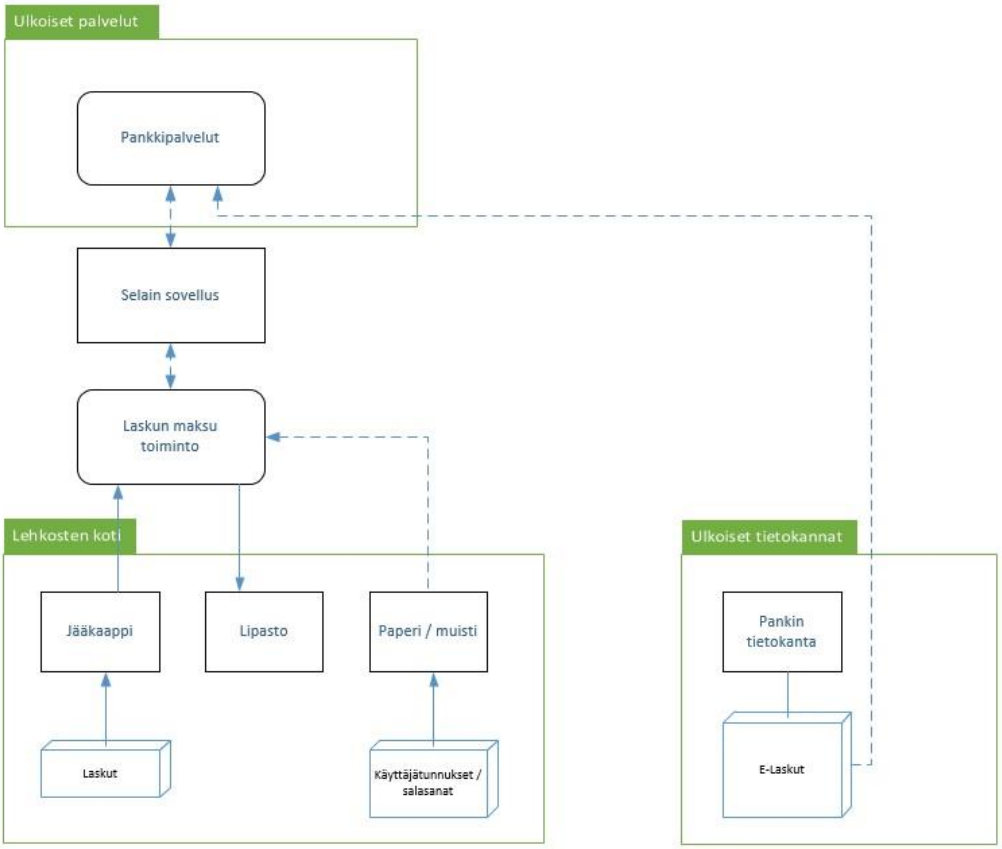
Mikäli salasanoja kertyy suuria määriä, kuten aktiiviselle internet käyttäjälle, suosittelee Cert.fi sivusto (2011) tallentamaan salasanan rekisteröintivaiheessa seuraavat palveluun syötetyt tiedot talteen.

- palvelun osoite
- käyttäjätunnus
- salasana (muista suojata hyvin, älä talleta koneen kiintolevylle ainakaan salaamattomana)
- rekisteröinnissä käyttämäsi sähköpostiosoite (jos mahdollista, käytä kuhunkin palveluun yksilöllistä osoitetta)
- tieto siitä, että onko palveluun syötetty luottokorttitietoja (verkkokaupat).

Tietojärjestelmäarkkitehtuuri

Tavoitteena tietojärjestelmäarkkitehtuurin suunnittelussa on suunnitella tietojärjestelmät niin, että ne tukevat organisaation tavoitteita mahdollisimman hyvin. Tietojärjestelmäarkkitehtuuri kuvaa keskeiset tietojärjestelmät, niiden väliset suhteet ja ominaisuustiedot. Tietojärjestelmäarkkitehtuuri sisältää rakenteellista suunnittelua, elinkaarisuunnittelua sekä optimointia. (JHS 179)

Havainnointiin perustuen kodissa Lehkosten kodissa ei ole laajoja tietojärjestelmäkokonaisuuksia, mutta erilaisten sähköisten palveluiden käyttöön tarvittavia yhteyksiä, tietoja, laitteita ja sovelluksia sekä niiden välisiä riippuvuussuhteita voidaan hyvin kuvata tietojärjestelmäarkkitehtuurin menetelmin. Esimerkkinä Lehkosten kodin pankkipalveluiden tietojärjestelmäarkkitehtuuri (Kuva 12).



KUVA 12. Lehkosten perheen pankkipalveluiden tietojärjestelmäarkkitehtuuri

Esimerkissä lasku voi olla paperisena tai E-laskuna. Maksamatonta paperista laskua säilytetään jääkaapin ovessa ja maksettua laskua lipaston laatikossa. E-laskut on tallennettuna pankin tietokantaan. Pankkipalveluihin tarvittavat käyttäjätunnukset, salasanat ja avainlukulistat ovat tallennettuina osittain paperisena sekä käyttäjien muistiin.

Teknologia-arkkitehtuuri

Teknologia arkkitehtuurin kuvaus vastaa kysymyksiin miten ja millä. Teknologia arkkitehtuuri sisältää millaisia teknologisia ratkaisuja on käytetty. Teknologia arkkitehtuurin suunnittelun ratkaisuvaihtoehtojen on tuettava organisaation tavoitteita. Teknologia-arkkitehtuurin kuvaukseen kuuluvat fyysisellä tasolla verkkokaavio, sijoituskaa-

vio, fyysiset tietovarannot sekä teknologiasalkku. Loogisella tasolla kuvataan teknologiakomponentit ja käsitteellisellä tasolla teknologiapalvelut. (JHS 179)

Kotiverkossa teknologia-arkkitehtuurin kuvaamisessa mielestäni keskeisimmät osa-alueet ovat käytettävien ohjelmien (teknologiasalkku) ja laitteiden kuvaaminen (fyysiset tietovarannot) sekä verkko-infrastruktuurin kuvaaminen (verkkokaavio).

5.1.3 Laitteet ja ohjelmistot

Toiminnan kehittämiseksi täytyy tietää, mitä laitteita järjestelmä pitää sisällään ja kuinka nämä laitteet kommunikoivat keskenään. Teknologia arkkitehtuurin kuvaus aloitettiin listaamalla käytössä olevat laitteet taulukkoon. Laitteita löytyi noin 30 kappaletta. Laiteluettelo esimerkki on esitetty taulukossa 4.

TAULUKKO 4. Lehkosten perheen laiteluettelo

Kannettavat tietokoneet

Nimi	Nimi verkossa	malli	sarjanro	käyttöjärjestelmä
HP pavilion	HPLehkonen	15-b114eo	5CD3281D3Y	Windows 8.1 64 bit
HP pavilion g series		g6-1104eo	CNF-1273TS6	Windows 7 home premium
Acer Extensa 5630EZ	Extensa-lappari	MS2231	? Tarra kulunut	Windows home premiuim 7 32 bit
Acer Aspire 3100	marko-laptop	BL51	? Tarra kulunut	Ubuntu 10.04
Acer aspire	Miniläppäri	ZG5	LUS080B0678430(	Windows XP Home edition sp3
Asus Eee PC	marko-901	EEEPC901-BK034	8COAAQ034431	Ubuntu 12.04 LTS 32 bit

Pöytätietokone

Nimi	Nimi verkossa	malli	sarjanro	käyttöjärjestelmä
HP Compaq				Windows xp

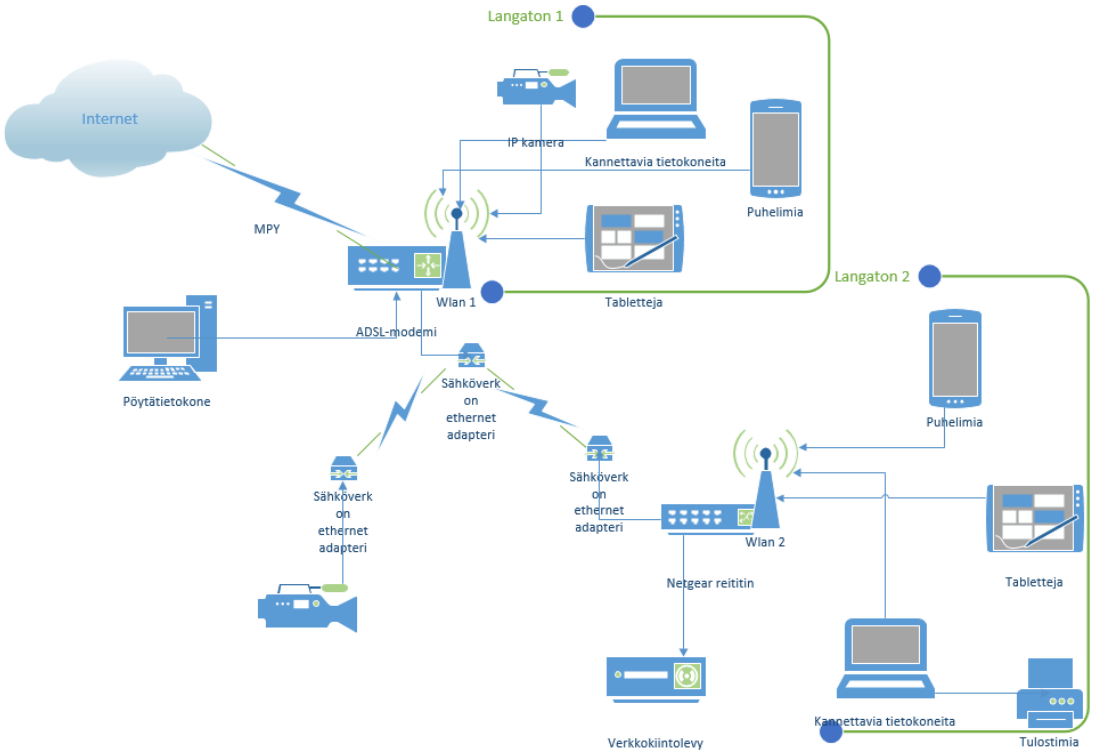
Tabletit

Nimi	Nimi verkossa	malli	sarjanro	käyttöjärjestelmä
Microsoft Surface RT		RT		Windows RT
Asus Transformer prime		TF201		Android 4.1.1
ICOO iCou D70pro II				Android 4.1
ICOO iCou D70pro II				Android 4.1

Puhelimet

Nimi	Nimi verkossa	malli	sarjanro	käyttöjärjestelmä
Htc one				Anroid 4.3.3
LG				Anroid
Sony Ericsson				Anroid
Samsung				Anroid
Samsung				Anroid
Nokia E71				Symbian v 9.2

Kotiverkon verkkokuvalla kuvataan sitä, millaisia laitteita verkkoon on kytketty ja millaisia tietoverkkoja koti sisältää. Lisäksi verkkokuvasta ilmenee, kuinka laitteet on kytketty internetiin ja miten laitteet kommunikoivat keskenään.



KUVA 13. Lehkosen kotiverkon verkkokuva

Lehkosen kotiverkko (Kuva 13) on jaettu kahteen erilliseen verkkoalueeseen ja langattomaan verkkoon. Toinen verkkoalue kattaa talon pohjoispäädyn ja toinen eteläpäädyn. Verkot on yhdistetty toisiinsa sähköverkkoon kytkettävillä Ethernet-adaptereilla. Laitteet kytketään verkkoalueeseen sen perusteella, missä päin taloa laitetta pääasiassa käytetään. Lehkosen kotiverkon internet-yhteyden palveluntarjoaja on Mikkelin puhelinyhdistys.

Havainnointi

Reitittimen ja langattoman reitittimen salasanat on vaihdettu, Langattomien verkkojen salauksessa on käytetty WPA2-PSK salausta. Verkon SID-tunnuksia ei ole piilotettu. Langattomien verkkojen käyttö perustuu sijaintiin. Langatonta verkkoa 1 käytetään talon toisessa päädyssä ja langatonta verkkoa 2 toisessa. Laitteet on kytketty langattomiin verkkoihin sen mukaisesti, millä puolella taloa niitä pääasiassa käytetään.

Kehittämisehdotukset

Tietoturvan lisäämiseksi langattomat verkot voitaisiin jakaa kahteen osaan sen mukaisesti millaista tietoa verkossa käsitellään. Tämä sen vuoksi, että havainnoinnin perusteella kaikkien laitteiden tietoturvasta ei pystytä käytettävissä olevin resurssein huolehtimaan riittävällä tavalla. Tietoturvan ylläpidossa keskitytään korkeamman turvaluokan ylläpitoon niin, että sen laitteet ja ohjelmistot ovat päivitettynä ajan tasalle.

Langaton verkko 1 olisi tietoturvaluokan 1 verkko, jonka laitteiden ja ohjelmistojen turvallisuudesta pidettäisiin erityisen tarkkaa huolta. Verkkoon pääsy sallittaisiin vain määritetyillä MAC osoitteella. Verkkoon kytkeytyvillä laitteilla voitaisiin käsitellä sähköistä asiointia ja kodin muuta tärkeää tietoa.

Langaton verkko 2 olisi tietoturvaluokan 2 verkko, jota voidaan käyttää vähemmän tärkeisiin toimintoihin kuten pelaamiseen, suoratoistopalveluiden katsomiseen jne.

Perustelut

ADSL-modeemin suojaamisessa on oleellista että modeemin ohjelmisto on ajan tasalla, oletussalasanat on vaihdettu sekä että laitetta pääsee hallinnoimaan vain sisäverkosta käsin. (Viestintävirasto 2013)

Langattoman verkon suojaukseen täytyy kiinnittää enemmän huomiota. Sen salakuuntelu on helpompaa kuin kiinteissä yhteyksissä. Suojaamattoman langattoman verkon liikenteen salakuuntelu on helppoa. Viestintäviraston suositus langattoman verkon suojaamiseksi on käyttää WPA2-salausta. Verkon nimen (SSID) mainostamisen estämistä tulisi myös harkita, vaikka se ei estäkään langattoman verkon löytymistä. Muita suojaustoimenpiteitä ovat esimerkiksi oletussalasanojen vaihtaminen, verkon pääsyn rajoittaminen MAC-osoitteilla, tukiasemien hallinnan mahdollistaminen vain kaapeliyhteyden avulla sekä lokitietojen kerääminen. (Viestintävirasto 2011)

Ohjelmistolista kodissa käytössä olevista ohjelmista

Ydintiedon käsittelyyn ja hallintaan sekä sähköiseen asiointiin käytetään Lehkosten perheessä tietokoneita, tabletteja sekä puhelimia. Ohjelmaluetteloon (Taulukko 5) on koottu toimintoihin käytettävät ohjelmat.

TAULUKKO 5. Lehkosen perheen ohjelmaluettelo

Ohjelmalista		**27.1.2014**
Ohjelma	Alusta	Käyttötarkoitus
Google Chrome	Windows 8 kannettava	Pankkiasiointi, Verkko-ostokset, Viranomais asiointi, sähköposti
Internet Explorer	Windows 8 kannettava	Pankkiasiointi, Verkko-ostokset, Viranomais asiointi, sähköposti
eBay sovellus	Android puhelin	Verkko-ostokset,/maksaminen
Nordea mobiilipankki	Android puhelin	Pankkiasiat
S-Mobiilipankki	Android puhelin	Pankkiasiat
Google Authenticator	Android puhelin	Googlen kaksivaiheisen kirjautumisen sovellus
Photo+	Android puhelin	Arkkeo dokumenttien arkistointisovellus
Taltioni	Android puhelin	Terveystietojen tallennus
MobilePay	Android puhelin	Kännykkäraha
Microsoft Word	Windows 8 kannettava	Salasanojen käsittely
Dropbox	Pilvi	Puhelimen valokuvien varmuuskopiointi
Googe Drive	Pilvi	Opiskeluun liittyvät tiedot
Microsoft Skydrive	Pilvi	Sekalaista materiaalia
Paint	Windows 8 kannettava	Kuvankäsittely
Google Music	Android puhelin	Levyjen kuuntelu
Gmail	Android puhelin	Sähköposti
Elisa Kirja	Android puhelin, tabletti	Kirja sovellus
Netflix	Android puhelin, tabletti, windows 8 kannettava	Elokuvien / tv-sarjojen suoratoistopalvelu
Viaplay	Android puhelin, tabletti, windows 8 kannettava	Elokuvien / tv-sarjojen suoratoistopalvelu
Posti sovellus	Android puhelin	Pakettien seuranta
Spotify	Android puhelin, tabletti	Musiikin suoratoisto
Veikkaus	Android puhelin	Veikkauksen palveluiden käyttö

Pilvipalveluihin tallennetaan tietoa useilla laitteilla. Dropbox-palvelua käytetään puhelimeen tallennettujen kuvien varmuuskopiointiin. Google Drive palvelua puolestaan käytetään opiskeluun liittyvien tietojen tallennuspaikkana.

Havainnointi

Haittaohjelmien torjuntaan käytetään kannettavissa tietokoneissa, joissa on asennettuna Windows-käyttöjärjestelmä, F-Securen tuotetta. Puhelimissa, Android-tableteissa ja Linux-käyttöjärjestelmällä varustetuissa kannettavissa tietokoneissa, ei haittaohjelmien torjuntaohjelmaa ollut asennettuna.

Käyttöjärjestelmät hakevat päivitykset automaattisesti ja ne ovat ajan tasalla. Android-puhelinten ja tablettien sovellukset päivitetään manuaalisesti mutta säännöllisesti. Windows-sovellusten ajantasaisuuden seuraamiseen ja päivittäminen ei ole säännöllistä, eikä siihen ei ole olemassa prosessia ja työkalua.

Toimenpide-ehdotukset

Haittaohjelmien torjuntaohjelma tulisi olla asennettuna kaikkiin niihin laitteisiin, myös puhelimiin, joilla sähköistä asiointia suoritetaan. Windows sovellukset olisi pidettävä ajan tasalla käyttämällä jotakin siihen soveltuvaa ohjelmistoa. Android-laitteiden päivitykset olisi asennettava automaattisesti, mikäli se on mahdollista.

Perustelut

Tähän päivään asti haittaohjelmat ovat koskeneet tietokoneita ja niissäkin lähinnä Microsoftin käyttöjärjestelmiä. Tosin myös muihin ympäristöihin tulee jatkuvasti enemmän haittaohjelmia eikä esim. Macintosh käyttäjätkään ole enää turvassa haittaohjelmilta. (F-Secure 2013)

Mobiililaitteiden yleistyessä haittaohjelmien kirjoittajatkin ovat siirtymässä näihin uusiin ympäristöihin. F-Securen (2013, 8) mukaan vuoden 2013 ensimmäisellä neljänneksellä oli 149 puhelimiin kohdistuvaa uhkaa. Näistä 136 kohdistui Android-järjestelmään ja 13 Symbian-käyttöjärjestelmään.

Haittaohjelmat voivat saastuttaa myös verkon aktiivilaitteita, kuten laajakaistamodeemeja ja digitv-virittimiä. Näitä verkon aktiivilaitekin voidaan liittää osaksi hyökkääjän bottiverkkoa. (Cert-fi 2013)

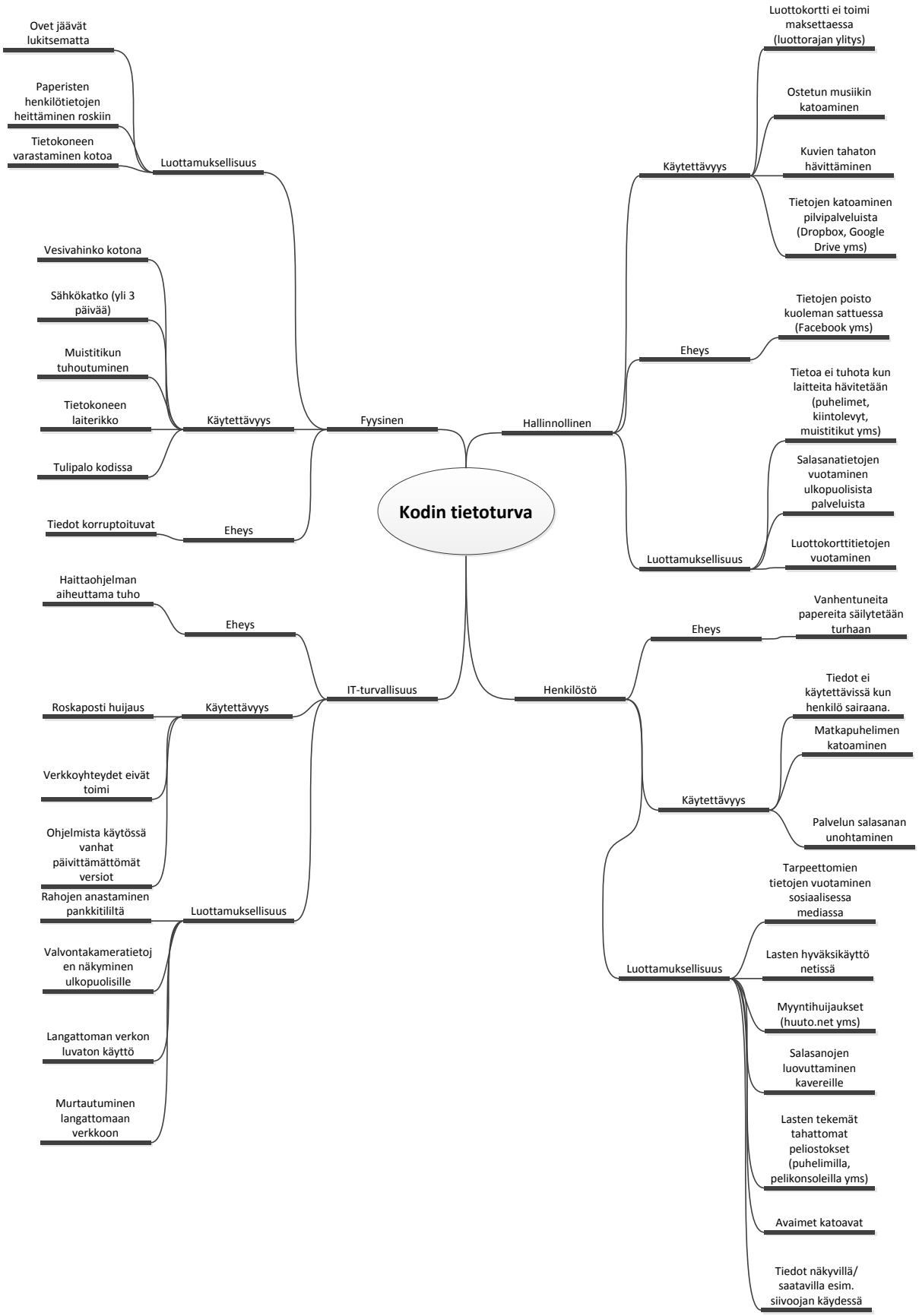
Aikaisemmin haittaohjelmia tekivät ns. ”nörtit”, joilla ei ollut muuta tavoitetta kuin näyttää osaamisensa. Nykyisin haittaohjelmien tekeminen on ammattimaista ja pääasiallisena tarkoituksena on rahallisen tai muun hyödyn tavoittelu. Esimerkiksi puhelimiin kohdistuvista haittaohjelmista 76,5 prosenttia oli tehty puhtaasti ansaintatarkoituksessa (F-Secure 2013, 9.).

Matkapuhelimien käyttäminen sähköisessä asioinnissa on yleistynyt ja myös niiden tietoturvaan pitäisi kansalaisten kiinnittää enemmän huomiota. Tietoturvauhkiin ei ole varauduttu eikä tietoturvaa mietitty matkapuhelinta käytettäessä. Ongelmana ovat erityisesti haittaohjelmat, joita ei aina ymmärretä myös matkapuhelimien ongelmaksi. Perusasioita ovatkin pin- ja suojakoodikyselyiden päällä pitäminen ja haittaohjelmilta suojautuminen. (Andreasson ym. 2013, 203.)

5.1.4 Riskianalyysi

Julkishallinnon suosituksen 171 mukaan nykytilauksen kuvausten lisäksi suositellaan käytettäväksi jotakin ongelmanratkaisu tai määrittelymenetelmiä. Suositus mainitsee keinoinen SWOT-analyysin, toiminnan ja prosessien simulaation, miellekartta tekniikan, riskianalyysin, kustannus-/hyötyanalyysin sekä tietoturvallisuuden kartoituksen. Lehkosen perheen menetelmäksi valittiin riskianalyysi.

Lehkosten kodin riskien kartoittaminen on tehty luetteloimalla kodin riskit ja luokittelemalla ne miellekarttatekniikan avulla tietoturvan sipulimallin mukaisesti. Riskit on luokiteltu hallinnolliseen tietoturvaan, henkilöstöturvallisuuteen, fyysiseen tietoturvaan sekä tietojenkäsittelyn ja tietoliikenteen turvallisuuteen. Tämän jälkeen tiedot on vielä luokiteltu tietoturvallisuuden tavoitteiden mukaisesti luottamuksellisuuden, käytettävyyden ja eheyden mukaan. Tämän kartoituksen tuloksena on syntynyt seuraava miellekartta (Kuva 14).



KUVA 14. Lehkosten perheen tietoturvariskit

Miellekartan avulla voidaan varmistua siitä, että riskit on kartoitettu tarpeeksi kattavasti. Mikäli jollekin tietoturvan osa-alueelle ei löydy riittävästi riskejä, on syytä varmistua siitä, että riskit on kartoitettu riittävän kattavasti.

Riskien luokittelu ja arviointi

Riskien kartoittamista jatkoin tekemällä riskeistä Excel-taulukon, johon myös luokittelin riskit sipulimallin sekä tietoturvallisuuden tavoitteiden mukaisesti. Jatkoin riskien arvioinnilla, jossa arvioin riskien todennäköisyyden ja vaikuttavuuden. Nämä kaksi lukua kertomalla keskenään tulokseksi tulee riskin odotusarvo. Riskit voidaan tämän jälkeen lajitella odotusarvon mukaan tärkeysjärjestykseen. Riskikartoituksen perusteella Lehkosten perheen 8 suurinta tietoturvariskiä on lueteltu oheisessa taulukossa (Taulukko 6).

TAULUKKO 6. Lehkosten perheen tietoturvariskit

Riski	Reakointitapa	Miten
Muistitikun tuhoutuminen	Pienentäminen	Varmuuskopiointi
Tietoa ei tuhota kun laitteita hävitetään (puhelimet, kiintolevyt, muistitikut yms)	Pienentäminen	Ohjeistus
Tietokoneen laiterikko	Pienentäminen	Varmuuskopiointi
Salasanatietojen vuotaminen ulkopuolisista palveluista	Pienentäminen	Salasanakäytännön luominen, ei käytössä samoja salasanoja
Matkapuhelimen katoaminen	Pienentäminen	Etäsulkemisen käyttöönotto, laitteen salaus
Ohjelmista käytössä vanhat päivittämättömät versiot	Pienentäminen	Ohjelmistojen päivityskäytännön luominen
Haittaohjelman aiheuttama tuho	Pienentäminen	Torjuntaohjelmien käyttöönotto (puhelimet ml)
Tietojen katoaminen pilvipalveluista (Dropbox, Google Drive yms)	Pienentäminen	Kopiot myös paikallisella medialla

Riskianalyysin perusteella havaitut merkittävimmät tietoturvariskit otetaan mukaan alustaviin kehittämiskohteisiin.

5.1.5 Alustavat kehittämiskohteet

Kokonaisarkkitehtuurin periaatteiden mukaisesti kehittämiseen liittyy alustavien kehittämiskohteiden tunnistaminen. Julkishallinnon suosituksen 179 liitteen 8 kokonaisarkkitehtuurin kuvauspohja on taulukko, jota voidaan hyödyntää kehittämiskohteiden luetteloinnissa ja arvioinnissa. Nykytilan kuvauksen ja riskianalyysin perusteella alustaviksi kehittämiskohteiksi löytyivät seuraavan asiat.

- laitteiden tietoturvatasojen määrittäminen
- kodin tietoverkon jakaminen kahteen turvaluokkaan
- sovellusten ajantasaisuuden seuraaminen (tietoturvapäivitykset)
- sähköiseen asiointiin käytettävien laitteiden ja ohjelmistojen määrittäminen
- selainten asetusten läpikäynti tietoturvallisiksi

- käyttäjätunnusten ja salasanojen turvallinen säilytys
- asioinnissa syntyvät asiakirjat säilytetty turvallisesti (sähköisenä)
- asioinnissa syntyvät asiakirjat hävitetty turvallisesti (sähköisenä)
- sähköisessä asioinnissa kodin ulkopuolella on käytettävä suojattua yhteyttä (SSL)
- kodin tietojen tallentaminen yhteen keskitettyyn paikkaan, Tietovarastoon (valokuvat, musiikki jne.)
- tietovaraston vastuiden määrittely (ylläpitäjä)
- tietovaraston varmuuskopiointi / palautus
- salasanojen muuttaminen määritysten mukaisiksi
- salasanojen tallettaminen turvalliseen sijaintiin
- salasanojen varmuuskopiointi
- haittaohjelmien torjuntaohjelmien asentaminen kaikkiin laitteisiin joissa sähköistä asiointia suoritetaan (esim. puhelimet)
- puhelimien päivitykset asetetaan asentumaan automaattisesti
- muistitikun tuhoutumiseen varautuminen (varmuuskopiointi)
- tietoa ei tuhota kun laitteita hävitetään (muistitikku, puhelimet, kiintolevyt ym.)
- tietokoneen laiterikkoon varautuminen (varmuuskopiointi)
- salasanatietojen vuotamiseen ulkopuolisista palveluista varautuminen (salasanakäytäntö, ei samoja salasanoja)
- matkapuhelimen katoaminen (etäsulkeminen, salaus)
- ohjelmista käytössä vanhat päivittämättömät versiot
- haittaohjelmien aiheuttamien tuhojen estäminen (torjuntaohjelman asentaminen)
- tietojen katoamisen estäminen pilvipalveluista (dropbox, microsoft skydrive, google drive, younited), varmuuskopiointi,

Alustavia kehittämiskohteita ei ole tässä vaiheessa vielä ryhmitelty tai laitettu tärkeysjärjestykseen. Kehittämiskohteen strategianmukaisuutta ei ole tässä vaiheessa arvioitu.

5.2 Tavoitetilan ja toimeenpanon suunnittelu

Tavoitetilan kuvauksessa otetaan huomioon tai tehdään strategiset linjaukset sekä kuvataan kodin kokonaisarkkitehtuurin tavoitetila. Kuvauksessa käytetään samoja arkki-

tehtuurin kuvauksen välineitä, joita on käytetty nykytilankuvauksessa. Esimerkiksi, mikäli halutaan kehittää jotakin tietoturvaan liittyvää teknistä yksityiskohtaa, tehdään tavoitetilan kuvaus ainakin teknologia arkkitehtuurin näkökulmasta katsottuna. Tarvittaessa kuvataan myös esimerkiksi toiminta-arkkitehtuuri, mikäli muutos vaikuttaa myös toimintaan jne.

Julkishallinnon suosituksessa 171 kuvattu prosessi tavoitetilan kuvaukseen on aivan liian jäykkä ja monimutkainen kodin sähköisen asioinnin kehittämiseen. Kodin sähköisen asioinnin kehittämisessä oli mielestäni järkevää yhdistää tavoitetilan kuvaus, tavoiteratkaisun kuvaus ja toimeenpanon suunnittelu yhdeksi kokonaisuudeksi. Tavoitetilan suunnittelun vaiheet voisivat olla esimerkiksi seuraavat.

- strategian määrittäminen
- kehittämiskohteiden rajaus
- budjetin laatiminen, mikäli muutokset aiheuttavat merkittäviä kustannuksia
- kuvataan tavoitetilan ratkaisut niin toiminnalliselta kuin tekniseltäkin näkökulmalta
- selvitetään mihin olemassa oleviin palveluihin muutokset vaikuttavat
- toimeenpanon suunnittelu.

Tavoitetilan suunnittelua helpottaa, että on olemassa käsitys siitä, mitkä ovat kodin yleiset tavoitteet. Näitä tavoitteita voisi kutsua kodin strategiaksi.

5.2.1 Kodin strategia

JHS 179 mukaan johdon asettama strategia on merkittävin syöte kokonaisarkkitehtuurin suunnittelussa. Visioista ja strategioista johdetaan kehittämisen tavoitteet ja vaatimukset. (JHS 179) Kotiverkossa ja kotona strategia voitaisiin ymmärtää yhteisesti sovittuina tavoitteina ja käytäntöinä, jossa kaikki perheenjäsenet ovat sitoutuneet käyttämään samoja toimintatapoja. Yleensä näitä linjauksia ei kuitenkaan kirjata mihinkään ylös, vaan niitä tehdään tilanteen niin vaatiessa, ilman sen suurempaa suunnittelua. Tällaisia strategisia linjauksia voisivat olla esimerkiksi pankin ja vakuutusyhtiön valinta, käytettävät sähkö-, vesi- ja viestintäalan toimijat, tietojen tallennuspaikat sekä yhteisesti tehty päätös käyttää jonkin määritetyn toimittajan tuotteita (Apple, Microsoft tms.) jne. Nämä päätetyt linjaukset vaikuttavat millaisessa sähköisen asioinnin

ympäristössä toimitaan. Esimerkiksi valittu pankki vaikuttaa siihen, kuinka kodissa pankkiasioita hoidetaan.

Mielestäni olisi kuitenkin aiheellista miettiä jo pankkia valittaessa, kuinka se mahdollisesti vaikuttaa toimintaan. Onko kaikki entiset sähköiset palvelut saatavilla uudessa pankissa? Kodissakin olisi mahdollista tehdä jonkinlainen suunnitelma siitä, millaisia palveluita halutaan hoitaa sähköisesti ja kuinka tähän tavoitetilaan päästään. Olisi myös hyvä linjata jonkinlaisia taloudellisia realiteetteja kehittämiselle eli kuinka paljon rahaa on käytettävissä kehittämiseen.

Mikäli tällainen kodin strategia on olemassa, kodin tietoturvallisena pitäminen huomattavasti helpompaa. Esimerkiksi mikäli tiedot ovat tallennettuna yhteisesti sovittuun paikkaan ja muotoon, on niiden varmuuskopiointi ja ylläpito huomattavasti helpompaa kuin jos tiedot olisi hajautettuna useaan eri laitteeseen ja paikkaan. Kodin strategia voi olla esimerkiksi seuraava.

Lehkosen kodin Strategia

Tämä kodin strategia koskee sähköisessä muodossa olevaa tietoa, ellei toisin mainita. Strategialla määritellään mihin suuntaan Lehkosten kodin sähköisten tietojen käsittelyä kehitetään. Lehkosten kodin strategiana on turvata kodille tärkeä sähköisessä muodossa olevan tiedon eheys, luottamuksellisuus ja käytettävyys.

Tärkeäksi tiedoksi Lehkosten kodissa on määritetty raha-asioihin, asumiseen, sopimuksiin, ostoksiin ja opiskeluun liittyvät tiedot sekä valokuva- ja musiikki tiedostot. Tavoitteena on myös siirtää tärkeitä paperisia asiakirjoja sähköiseen muotoon niin, että ne ovat muunnettuna sähköiseen muotoon, mikäli alkuperäiset asiakirjat jostakin syystä katoavat tai tuhoutuvat. Tällaisia asiakirjoja ovat ainakin koulu- ja työtodistukset sekä taloon- ja tonttiin liittyvät viralliset asiakirjat.

Strategiana on varmistaa tärkeiden sähköisten toimenpiteiden turvallisuus ja toimivuus eriyttämällä tärkeiden tietojen käsittely vähemmän tärkeistä. Tärkeiden tietojen käsittelyyn tarkoitetut laitteet on pidettävä eriytettynä muista laitteista ja niiden tietoturva on pidettävä ajantasaisina.

Strategiana on myös varautua poikkeuksellisiin tapahtumiin varmistamalla yhteyksien toimivuus myös silloin kun pääyhteys ei ole toiminnassa. Laitteiden elinkaarenhallinta on suunniteltava. Tuotevalinnoissa suositaan suomalaisia tuotteita ja palveluita, mikäli ne täyttävät tekniset ja taloudelliset vaatimukset.

Tuote- ja toimittajavalinnat

Sähköiset tallennus yms. palvelut toteutetaan, mikäli mahdollista, ilmaisia palveluita hyödyntäen. Kannettavien tietokoneiden käyttöjärjestelmävalinnat ovat Windows ja Linux. Tablettien käyttöjärjestelmät ovat Android tai Windows. Puhelimien käyttöjärjestelmä on Android. Haittaohjelmien torjuntaohjelmistona käytetään F-Securen tuotteita. Pankkipalveluiden toimittajia ovat Nordea ja S-pankki. Vakuutusyhtiönä on Tapiola. Tunnistuspalveluina käytetään, mikäli mahdollista pankkitunnistusta tai mobiilivarmennetta.

5.2.2 Kehittämiskohteen valinta

Nykytilan kuvauksella ja riskianalyysin perusteella Lehkosen perheen keittämistarpeet koottiin taulukkoon (Taulukko 7). Kehittämiskohteista muodostettiin kehittämiskokonaisuuksia. Kehittämiskokonaisuusiksi tunnistettiin seuraavat.

1. Tietoverkot ja laitteet eriytetään kahdeksi eri turvaluokan verkoksi.
2. Ydintiedolle luodaan keskitetty ja varmistettu tallennuspaikka.
3. Ulkoisille medioille ja palveluihin tallennetulle tiedolle luodaan turvalliset säilytys, hävitys ja hallinnointimenetelmät (muistitikut, puhelimet, pilvipalvelut)
4. Salasanojen hallinta turvalliseksi.

Kehittämisehdotukset priorisoitiin kehittämisehdotuksen tärkeyden mukaan kolmeen luokkaan, välttämättömiin, hyödyllisiin ja toivottuihin. Kehittämisehdotuksista ja niiden tärkeysluokituksesta laskettiin kullekin kehittämiskokonaisuudelle vaikutusluku. Vaikutusluku kertoo, kuinka suuri vaikutus kehittämiskokonaisuudella on Lehkosten perheen sähköisen asioinnin turvallisuuteen.

TAULUKKO 7. Lehkosen perheen kehittämisehdotusten luokittelu ja priorisointi

Lehkosten perheen kehittämisvaatimukset ja tavoitteet

15.2.2014
Versio 1.0

Prioriteetti: 3=välttämätön, 2=hyödyllinen, 1= toivottu
Tyyppi= toiminnallinen, luotettavuus, käytettävyys, tehokkuus, ylläpidettävyys, siirrettävyys, tietoturvallisuus

Kokonaisuus
1. Tietoverkot ja laitteet eritetään kahdeksi eri turvaluokan verkoksi.
2. Ydintiedolle luodaan keskitetty ja varmistettu tallennuspaikka.
3. Ulkoisille medioille ja palveluihin tallennetulle tiedolle luodaan turvalliset säilytys, hävitys ja hallinnointimenetelmät (muistitikut, puhelimet, pilvipalvelut)
4. Salasanojen hallinta turvalliseksi

Vaatimuksen/ kehitystarpeen kuvaus	Vaatimuksen alkuperä/ esittäjä	Vaatimuksen tyyppi	Edellytys	Tavoitetila	Mittari	Tavoitetaso	Prioriteetti	Kokonaisuus	1	2	3	4
Laitteiden tietoturvatasojen määrittäminen	Havainnonti, teknologia-arkkitehtuuri	tietoturvallisuus	Laitteiden käyttötarkoitus päätetty	Turvatasot määritttty	Toteutettu K/E	K	3	1	3			
Kodin tietoverkon jakaminen kahteen turvaluokkaan	Havainnonti, teknologia-arkkitehtuuri	tietoturvallisuus	Suunnitelma tietoverkon jakamisesta	Tietoverkko jaettu turvaluokkiin	Toteutettu K/E	K	3	1	3			
Sovellusten ajantasaisuuden seuraaminen	Havainnonti	ylläpidettävyys, tietoturvallisuus	Päätös käytettävästä sovelluksesta tehty	Ohjelma(t) asennettu ja käytössä	Toteutettu K/E	K	3	1	3			
Määritetään sähköiseen asiointiin käytettävät laitteet ja ohjelmistot	Toimintakuvaus	Käytettävyys, tietoturvallisuus	Tieto siitä mitä sovelluksia asioinnissa voidaan käyttää	Laitteet / ohjelmat määritetty	Toteutettu K/E	K	3	1	3			
Selaiten asetusten läpikäynti tietoturvallisiksi	Toimintakuvaus	tietoturvallisuus	Päätös käytettävistä selainohjelmista	Asetukset tehty turvallisiksi	Toteutettu K/E	K	2	1	2			
Käyttäjätunnukset ja salasanat säilytetty turvallisesti	Toimintakuvaus	tietoturvallisuus	Käytäntö määritetty	Salasanat säilytetty asianmukaisesti	Toteutettu K/E	K	3	4				3
Asioinnissa syntyvät asiakirjat säilytetty turvallisesti (sähköisenä)	Toimintakuvaus	tietoturvallisuus	Päätetty säilytystapa	Asiakirjojen säilytys järjestetty	Toteutettu K/E	K	2	2		2		
Asioinnissa syntyvät asiakirjat hävitetty turvallisesti (sähköisenä)	Toimintakuvaus	tietoturvallisuus	Päätetty tuohoamistapa	Hävitys järjestetty	Toimitatapa käytössä K/E	K	2	2		2		
Sähköisessä asioinnissa kodin ulkopuolella käyttään suojattua yhteyttä (SSL)	Toimintakuvaus	tietoturvallisuus	Opastettu käyttäjiä	Toimintatapa käytössä	Käytetään yhteyttä K/E	K	1	1	1			
Kodin tietojen tallentaminen yhteen keskitettyyn paikkaan, Tietovarastoon (valokuvat, musiikki jne)	Tietoarkkitehtuuri	tietoturvallisuus, käytettävyys, ylläpidettävyys, siirrettävyys	Tallennuspaikka päätetty, olemassa ja opastettu käyttäjät	Tallennuspaikka päätetty, olemassa ja opastettu käyttäjät	Käytetään tallennuspaikkaa K/E	K	3	3			3	
Tietovaraston vastuiden määrittely (ylläpitäjä)	Tietoarkkitehtuuri	tietoturvallisuus	tietovarasto olemassa	asia päätetty	määritetty K/E	K	3	3			3	
Tietovaraston varmuuskopiointi / palautus	Tietoarkkitehtuuri	tietoturvallisuus	varmuuskopiointipaikka olemassa	Varmuuskopiot tehty	K/E	K	3	3			3	
Salasanojen muuttaminen määritysten mukaisiksi	Tietoarkkitehtuuri	tietoturvallisuus	titu-määritykset päätetty	salasanat turvallisia	K/E	K	3	4				3
Salasanojen tallettaminen turvalliseen sijaintiin	Tietoarkkitehtuuri	tietoturvallisuus, käytettävyys, ylläpidettävyys	Sijainti päätetty, olemassa	Salasanat talletettu turvallisesti	K/E	K	3	4				3
Salasanojen varmuuskopiointi	Tietoarkkitehtuuri	tietoturvallisuus, käytettävyys, ylläpidettävyys	Sijainti päätetty, olemassa	Salasanat varmuuskopioitu	K/E	K	2	4			2	2
Haittaohjelmien torjuntaohjelmien asentaminen kaikkiin laitteisiin joissa sähköistä asiointia suoritetaan (ml. Puhelimet)	Teknologia-arkkitehtuuri	tietoturvallisuus	Käytettävä ohjelma valittu ja hankittu	Ohjelma asennettu käyttöön	K/E	K	3	1	3			
Puhelimien päivitykset asetetaan asentumaan automaattisesti	Teknologia-arkkitehtuuri	ylläpidettävyys, tietoturvallisuus		Asetukset tehty	K/E	K	1	1	1			
Muistitikun tuhoutumiseen varautuminen (varmuuskopiointi)	riskianalyysi	tietoturvallisuus	varmuuskopiointipaikka olemassa, opastettu	Varmuuskopiot tehty	K/E	K	3	2		3		
Tietoa ei tuhota kun laitteita hävitetään (muistitikku, puhelimet, kiintolevyt ym)	riskianalyysi	tietoturvallisuus	Opastettu käyttäjiä	Tiedot tuhotaan kun laitetta hävitetään	K/E	K	2	2		2		
Tietokoneen laiterikkoon varautuminen (varmuuskopiointi)	riskianalyysi	tietoturvallisuus	varmuuskopiointipaikka olemassa, opastettu	Varmuuskopiot tehty	K/E	K	3					
Salasanatietojen vuotamiseen ulkopuolisista palveluista varautuminen (salasanakäytäntö, ei samoja salasanoja)	riskianalyysi	tietoturvallisuus	titu-määritykset päätetty	salasanat turvallisia	K/E	K	3	4				3
Matkapuhelimen katoaminen (etäsulkeminen, salaus)	riskianalyysi	tietoturvallisuus	tarvittavien asetusten / ohjelmien asentminen	Ohjelmat asennettu ja käytössä	K/E	K	1	2		1		
Ohjelmista käytössä vanhat päivittämättömät versiot	riskianalyysi	tietoturvallisuus	Tieto käytössä olevista ohjelmista ja niiden päivitystarpeesta	Käytössä ohjelma päivitysten havaitsemiseksi ja asentamiseksi	K/E	K	3	1	3			
Haittaohjelmien aiheuttamien tuhojen estäminen (torjuntaohjelman asentaminen)	riskianalyysi	tietoturvallisuus	Ohjelma hankittu	Ohjelma käytössä	K/E	K	3	1	3			
Tietojen katoamisen estäminen palveluista (Dropbox ym), varmuuskopiointi	riskianalyysi	tietoturvallisuus	varmuuskopiointipaikka olemassa, opastettu	Varmuuskopiot tehty	K/E	K	3	2		3		
									25	13	11	14

Kehittämiskokonaisuuksista muodostettiin yhteenveto taulukko toteutettavien kehittämiskohteiden valitsemiseksi. Kehittämiskohteiden valitsemiskriteeriksi otettiin mukaan vielä kehittämiskokonaisuuden toteuttamiseksi vaadittava taloudellinen ja ajallinen panos (Taulukko 8).

TAULUKKO 8. Kehitysehdotusten valinta

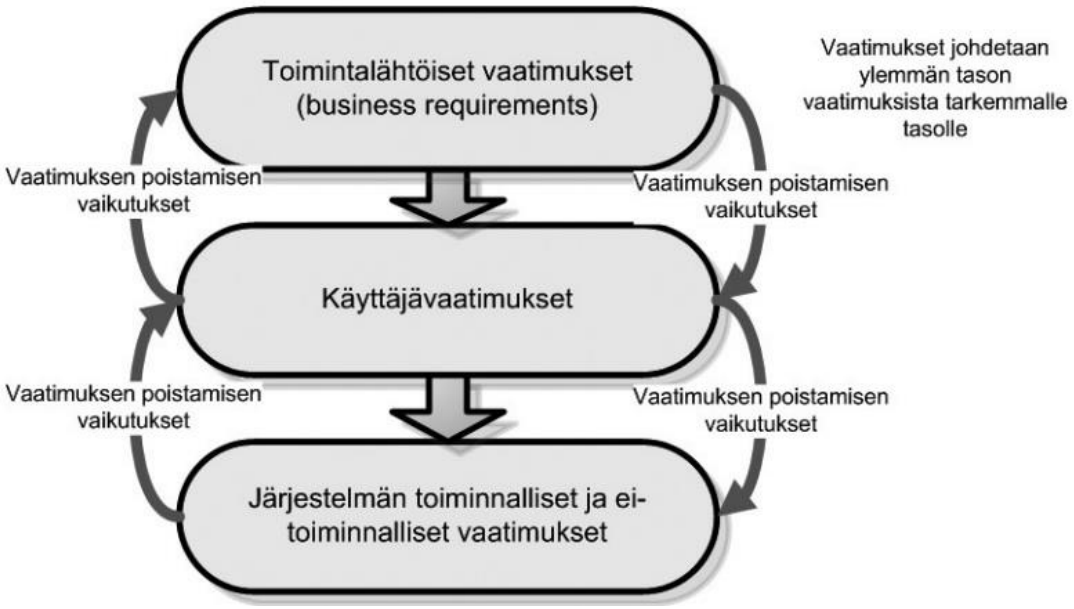
Kehittämisehdotus	Vaikutus	Talous	Aika	Yhteensä
1. Tietoverkot ja laitteet eriytetään kahdeksi eri turvaluokan verkoksi.	25	14	8	47
2. Ydintiedolle luodaan keskitetty ja varmistettu tallennuspaikka.	13	10	12	35
3. Ulkoisille medioille ja palveluihin tallennetulle tiedolle luodaan turvalliset säilytys, hävitys ja hallinnointimenetelmät (muistitikut, puhelimet, pilvipalvelut)	11	15	10	36
4. Salasanojen hallinta turvalliseksi	14	13	12	39

Vaikutus	= moneenko kehittämisehdotukseen kehittämiskokonaisuus vaikuttaa (prioriteetilla painotettuna)
Talous	= käytettävä rahallinen panos 0= panostettava merkittävästi 15 = ei tarvitse rahallista panosta
Aika	= käytettävä ajallinen panos, 0 = panostettava merkittävästi 15 = ei tarvitse ajallista panosta

Kehittämiskokonaisuuksien toteutusjärjestys on saatu laskemalla yhteen vaikutus, talous ja aikasarakkeiden luvut. Kehittämiskohteeksi valittiin edellä mainituilla perusteilla kehittämiskokonaisuuksien kohta 1, tietoverkon ja laitteiden eriyttäminen kahteen turvaluokkaan.

5.2.3 Kehittämiskohteen vaatimusten määrittely

Vaatimusmäärittely on osa vaatimustenhallintaa ja sitä tehdään läpi koko kehittämisen. Vaatimuksia asetetaan nykytilan kuvauksesta aina kilpailutukseen saakka. Vaatimukset saattavat muuttua ja tarkentua, kun kehittämisessä edetään. Vaatimustenhallintaan kuuluu mm kehittämistarpeiden kerääminen nykytilan kuvauksessa ja myöhemmin niiden tarkentaminen sekä toteutuksen jälkeen arviointi, kuinka vaatimukset ovat toteutuneet. Varsinainen vaatimusmäärittely tehdään ennen hankintaa, kilpailutusta ja toteutusta. Vaatimuksia voi olla toimintalähtöisiä vaatimuksia, käyttäjävaatimuksia sekä järjestelmän toiminnallisia ja ei toiminnallisia vaatimuksia (Kuva 15). (JHS 173).



KUVA 15. Vaatimusryhmät ja niiden hierarkia (JHS 173)

Kodin sähköisen asioinnin kehittämisessä saattaa olla toimintalähtöisiä vaatimuksia, joita tulee kodin strategista, esimerkiksi yksilöidyn käyttöjärjestelmän tai selaimen käyttövaatimus sähköisessä asioinnissa tai vaatimus siitä kuinka palveluihin tunnistaminen hoidetaan. Käyttäjävaatimuksia puolestaan voisi olla esimerkiksi verkkopankkien käyttövaatimus, joka asettaa vaatimuksia esimerkiksi Javan käytölle. Toiminnallisia vaatimuksia sähköiseen asiointiin sinänsä voi olla hankala asettaa, koska asiointi tapahtuu pääsääntöisesti palveluntarjoajan ympäristössä. Toiminnallisia vaatimuksia voidaan kuitenkin asettaa mm. kodin laitteille, esimerkiksi varmuuskopioinnille voidaan asettaa vaatimus raid1 peilauksesta. Ei-toiminnallisia vaatimuksia voidaan asettaa kodissa aivan samoin kuin muuallakin, mutta ei ehkä niin tiukkoja vaatimuksia. Voidaan asetta vaatimuksia esimerkiksi varayhteyksille tai tietoturvalle.

Kodin sähköisen asioinnin vaatimusmäärittelyssä kootaan yhteen aiemmissa vaiheissa esiin tulleet vaatimukset ja tehdään niistä tavoitetilaa vastaava yhteinen vaatimusmäärittely. Tässä vaiheessa voidaan vielä kehittämiskohteita priorisoida, jolla määritetään eri kehittämiskohteiden toteuttamisjärjestystä. Lehkosen perheen tietoverkon ja laitteiden eriyttäminen kahteen turvaluokkaan vaatimusmäärittely on koottu taulukkoon 9.

TAULUKKO 9. Vaatimusmäärittely: Tietoverkon ja laitteiden eriyttäminen kahteen turvaluokkaan

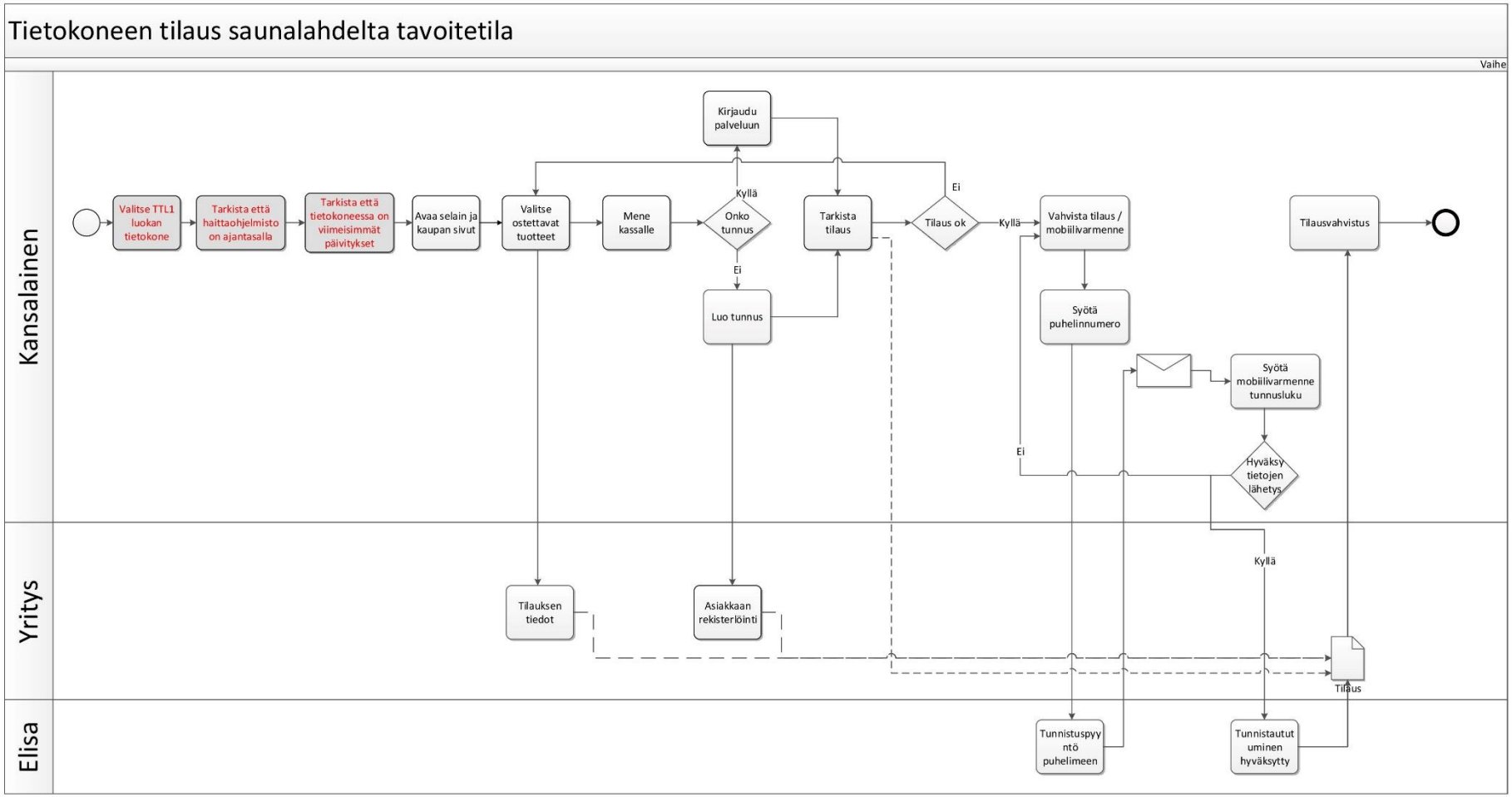
Vaatimusmäärittely	
Tietoverkon ja laitteiden eriyttäminen kahteen turvaluokkaan	
versio 1.0	
Tunnus (ID)	**Vaatimus**
1	Lehkosen kodin tietoverkko on jaettava kahteen turvaluokkaan (I turvaluokka on tarkoitettu turvalliseen sähköiseen asiointiin, II turvaluokka muuhun toimintaan.
2	I Turvaluokan langaton verkko ei saa olla näkyvillä
3	Langattomien verkkojen salauksessa on käytettäva WPA2-PSK salausta
4	Käytettävät laitteet on jaettava kahteen turvaluokkaan.
5	II turvaluokan koneilla ei voi kytkeytä I turvaluokan verkkoon.
6	I turvaluokan koneet ovat päivitetty ajantasalle viikon kuluessa ohjelmistopäivityksen julkaisusta.
7	I turvaluokan koneet on määritettävä ja merkittävä selkeästi.
8	I turvaluokan tietokoneissa käytettävät selaimet määritettävä sekä niiden asetukset tehtävä turvalliseksi.
9	I turvaluokan koneiden ohjelmistojen ajantasaisuus on pystyttävä todentamaan.
10	Ennen sähköisen asioinnin aloittamista ohjelmistojen ajantasaisuus on pystyttävä todentamaan.
11	I turvaluokan koneet on merkittävä niin että koneen turvaluokka voidaan todentaa ilman koneen käynnistämistä.
12	I turvaluokan yhteydelle on luotava varayhteys
13	I ja II turvaluokan windows koneille on asennettava virustarkistusohjelma.
14	XP käyttöjärjestelmät on päivitettävä tuettuun versioon (lunux tai windows)
15	Käyttäjät on opastettava I ja II turvaluokain koneiden käyttöön

Vaatimuksia tietoverkkojen ja laiteiden eriyttämiseen kahteen turvaluokkaan muodostui yhteensä 15 kappaletta. Näiden vaatimusten perusteella tehdään tavoitetilan kuvaukset.

5.2.4 Lehkosen perheen tavoitetilan kuvaukset

Tavoitetilan kuvauksissa on kuvattu ne arkkitehtuurinäkökulmat, jotka ovat muuttuvat kehittämistoimenpiteiden seurauksena. Tällaisia ovat toiminta- ja teknologia-

arkkitehtuurin kuvaukset. Toiminta-arkkitehtuurin kuvauksessa (Kuva 16) on punaisella merkitty muuttuvat toiminnot.

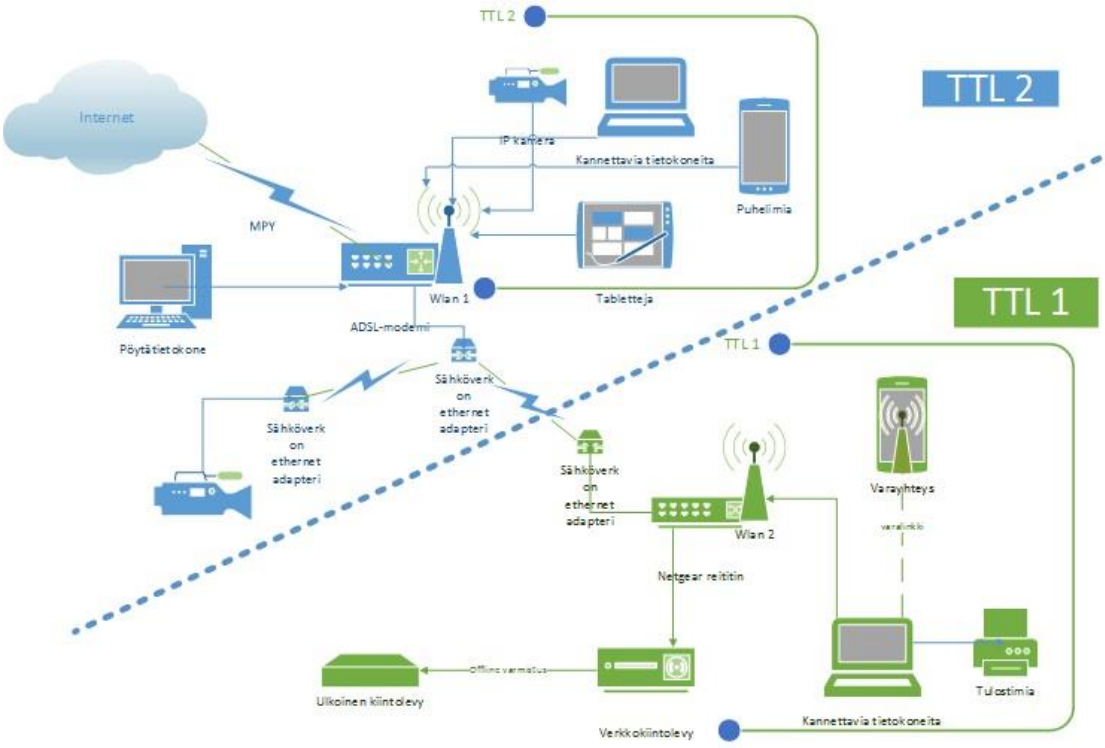


KUVA 16. Toiminta-arkkitehtuurin tavoitetila

Toiminta muuttuu siten, että konetta valittaessa käyttöön otetaan tietoturvaluokka I:sen työasema. Ennen sähköisen asioinnin aloitusta täytyy lisäksi tarkistaa, että tietokoneen päivitykset ja virustorjunta ovat ajan tasalla. Muilta osin toiminta säilyy ennallaan.

Teknologia-arkkitehtuuri

Teknologia-arkkitehtuurin kuvauksessa (Kuva 17) verkko on jaettu kahteen turvaluokkaan. Sinisellä värillä on merkitty 2 turvaluokan verkko ja vihreällä värillä 1 turvaluokan verkko.



KUVA 17. Lehkosten perheen teknologia-arkkitehtuurin tavoitetila

Lehkosen perheessä on käytössä käyttöjärjestelmiä, joiden tuki on loppumassa tai on jo loppunut (Taulukko 10). Kehittämistoimenpiteenä päivitetään käyttöjärjestelmät tuettuun versioon oheisen taulukon mukaisesti. Korvaavana käyttöjärjestelmänä käytetään Linux Ubuntu jakelua.

TAULUKKO 10. Lehkosten perheen käyttöjärjestelmien elinkaari

Käyttöjärjestelmien elinkaari	Tuki loppuu	Korvaava tuote
Windows XP	8.4.2014	Ubuntu 12
Windows 7	14.1.2020	
Windows 8	10.1.2023	
Windows 8 RT	10.1.2023	
Ubuntu 10	9.5.2013	Ubuntu 12
Ubuntu 12	5/2017	

Laiteluettelon tavoitetilassa (Taulukko 11) kuvataan laitteiden tietoturvatasoa ja elinkaarenhallintaa. Tietoturvaluokka on merkitty taulukkoon TTL sarakkeeseen merkinnällä I tai II. Laitteen käyttöjärjestelmän tuen päättymisen merkkinä taulukossa on P, jolloin laitteen käyttöjärjestelmä on päivitettävä. P kirjain taulukossa tarkoittaa että laite on tullut elinkaarensa loppuun ja se on poistettava käytöstä.

TAULUKKO 11. Lehkosen perheen laitteiden tavoitetila

Laiteluettelo tavoitetila

TTL I = I tietoturvaluokka, II= II tietoturvaluokka, X=poistettava, P=päivitettävä

Kannettavat tietokoneet

TTL	Nimi	Nimi verkossa	malli	sarjanro	käyttöjärjestelmä	Kiintolevyn koko
I	HP pavilion	HPLehkonen	15-b114eo	5CD3281D3Y	Windows 8.1 64 bit	450 GT
I	Packard bell	PB-Lehkoset	Easynote TE69KB	NXC2CED0393440A	Windows 8.1 64 bit	500 GT
X	HP pavilion g series		g6-1104eo	CNF-1273TS6	Windows 7 home premiun	450 GT
II	Acer Extensa 5630EZ	Extensa-lappari	MS2231	? Tarra kulunut	Windows 7 home premiui	120 Gt
P	Acer Aspire 3100	marko-laptop	BL51	? Tarra kulunut	Ubuntu 10.04	60 Gt
P	Acer aspire	Miniläppäri	ZG5	LUS080B067843068	Windows XP Home editior	140 GT
II	Asus Eee PC	marko-901	EEEPC901-BK034X	8COAAQ034431	Ubuntu 12.04 LTS 32 bit	10 Gt ssd

Laitteen elinkaarenhallinta on myös suunnittelu taulukon TTL sarakkeessa. Mikäli laitteen elinkaari on loppumassa ja laite tulisi hävittää, on sarakkeeseen merkitty X merkillä. Merkintä P merkitsee että laitteen käyttöjärjestelmän tuki on päättymässä ja käyttöjärjestelmä on vaihdettava.

5.2.5 Toimeenpanon suunnittelu

Toimeenpanon suunnittelussa suunnitellaan ne toimenpiteet, jotka aiotaan toteuttaa tavoitetilaan pääsemiseksi sekä arvioidaan toimenpiteiden hyödyt ja riskit sekä priorisoidaan toimenpiteet. Välttämättä kaikkia toimenpiteitä ei toteuteta vaan vain tärkeimmät.

Lähiverkon jakaminen kahteen turvaluokkaan

- muuta Tietoturvaluokka 1:sen SID (Lehkoverkko1)

- piilota Lehkoverkko1:sen SID
- muuta Tietoturvaluokka 2:sen SID (Lehkoverkko2)
- kytke Lehkoverkko1:seen MAC suodatus päälle
- määrittele ja testaa Lehkoverkko1:sen mobiili varayhteys.

Ohjelmistojen päivittäminen

- päivitä käyttöjärjestelmät tuettuun version
- asenna virustarkistusohjelma (F-secure) kaikkiin Windows tietokoneisiin ja suorita virustarkistus
- asenna EMET ja Secunia PCI ohjelmistot tietoturvaluokka 1:sen tietokoneisiin
- tarkista että tietoturvaluokan koneissa on uusimmat ohjelma versiot.

Koneiden jakaminen kahteen turvaluokkaan

- kytke TTL1 koneet Lehkoverkko1:seen
- merkitse TTL1:n koneet
- kytke muut tietokoneet Lehkoverkko2:seen.

Opinnäytetyöni ei sisällä varsinaista toimeenpanoa, mutta kehittämistoimenpiteiden toteuttamisen jälkeen kehittämisprosessi aloitettaisiin alusta nykytilan kuvauksella.

6 PÄÄTELMÄT

Julkishallinnon suositukset on tarkoitettu isoihin julkishallinnon organisaatioihin ja suurien järjestelmien kehittämiseen. Suositusten mukaisesti tehtynä organisaation ICT-palveluiden kehittäminen vaatii paljon aikaa ja resursseja. Julkishallinnon suositukset ICT-palveluiden kehittämisestä ovat mielestäni sekava ja vaikeasti hahmotettava kokonaisuus, jossa paljon jää organisaation itsensä päätettäväksi. Tästä huolimatta suosituksista löytyy useitakin hyödynnettäviä kohtia kodin sähköisen asioinnin kehittämiseen.

Koteihin on tulossa yhä enemmän tietotekniikkaa. Puettava elektroniikka on jo tulossa koteihin. Älykellot, aktiivisuusmittarit, älylasit alkavat olla jo nykypäivänä kuluttajien arkipäivää. Tulossa ovat myös älykkäät kodinkoneet. Kaikki nämä halutaan yhdistää kodin tietoverkkoon. Tämä uusi tietotekniikan osa-alue tuo paljon mahdollisuuksia,

mutta myös uhkakuvia. Pitäisikö ja onko yleensä mahdollista asentaa älytelevisioon esimerkiksi virustorjunta ohjelma? Tämä älytelevisio on kuitenkin kytketty kodin tietoverkkoon ja siihen voidaan murtautua kuten perinteisiin tietokoneisiinkin.

Samalla kun kodin tietoteknisiä laitteita käytetään sähköiseen asiointiin yhä enemmän, niiden ylläpidon resurssit eivät ole lainkaan kasvaneet. Isä tai äiti tekee tätä ylläpitoa vapaa-ajallaan. Tästä huolimatta sähköisen asioinnin turvallisuudesta täytyisi huolehtia. Kokonaisarkkitehtuuri antaa hyvän kokonaiskuvan ja lähtökohdan sille, kuinka kodin sähköistä asiointia ja tietoturvaa tulisi kehittää, joskin samaan lopputulokseen voisi päästä yksinkertaisemmallakin kehittämismenetelmällä.

Mielestäni tärkeä osa kodin sähköisen asioinnin ja tietoturvan keittämisessä on strategia. Luultavasti monessakaan kodissa ei ole mietitty mihin suuntaan kotia, sen tietotekniikkaa ja sähköisten palveluiden käyttöä halutaan kehitettävän. Kodissa on kuitenkin rajalliset voimavarat ylläpitää kodin laitteita ja sen vuoksi ylläpidossa olisi tärkeää keskittyä niihin laitteisiin, joissa käsitellään kodille tärkeää ydintietoa. Strategia voisi olla hyvä keino vähentää ylläpidon tarvetta ja vapauttaa resursseja sellaisten asioiden tekemiseen, joilla turvataan kodille tärkeitä asioita.

Kodin mahdollisuudet vaikuttaa siihen, miten sähköistä asiointia hoidetaan, ovat rajalliset. Palvelun käyttötapaan ja sisältöön pystyy vaikuttamaan vain hyvin rajallisesti. Suurin palveluiden käyttötapaan vaikuttava päätös tehdään palveluntarjoajaa valittaessa. Palveluntarjoajan valintavaiheessa tulisikin kiinnittää enemmän huomiota palveluiden ominaisuuksiin ja käytettävyyteen, eikä pelkästään siihen mitä palvelu maksaa. Palveluiden tarjoajan valinnan lisäksi kodissa valintoja voidaan tehdä lähinnä siinä miten Internetiin kytkeydytään, mitä koneita ja ohjelmistoja palveluiden käyttämiseen valitaan. Näillä valinnoilla on kuitenkin merkittävä vaikutus siihen, kuinka turvallista palvelun käyttö on. Tietoturvan parantaminen ei kuitenkaan välttämättä merkitse sitä että siihen olisi rahallisesti panostettava merkittävästi. Toimintatapoja muuttamalla ja käyttäjiä opastamalla saadaan usein parannettua tietoturvaa.

Käyttämällä kokonaisarkkitehtuurin kuvausmenetelmiä kehittämisestä saadaan järjestelmällistä ja dokumentoitua. Dokumentointi on mielestäni myös kodissa tärkeää, vaikka kodissa ylläpitäjät vaihtuvat harvemmin.

Moni voi kokea että tarvetta kodin tietojärjestelmien kehittämiseen ei ole, mutta tarve kehittämiselle kasvaa sen myötä kun laitteiden määrä kodissa kasvaa. Tulevaisuudessa kun verkkoyhteyden sisältäviä laitteita on kodeissa useita kymmeniä, ylläpitoon käytettävät resurssit on kohdennettava ydintiedon turvaamiseen.

Kiteytettynä kodin sähköisen asioinnin ja sen tietoturvan kehittäminen: Täytyy olla tieto siitä, millainen on kodin nykyinen ympäristö ja kuinka sitä käytetään eli on tunnettava nykytila. Lisäksi on päätettävä, mikä tieto kodissa on tärkeää suojaamisen arvoista ydintietoa ja millaisia muutoksia ympäristöön halutaan eli millainen on tavoitetila. Vasta tämän jälkeen muutokset voidaan suunnitella ja toteuttaa. Liitteessä 1 on lueteltu toimenpiteet, joiden katson olevan tärkeitä kehitettäessä kodin tietoteknistä ympäristöä.

LÄHTEET

Andreasson Ari, Koivisto Juha 2013. Tietoturvaa toteuttamassa. Helsinki:Tietosanoma Oy.

Cert-fi 2013. Suomessakin Carna-bottiverkon saastuttamia laitteita, WWW-dokumentti. http://www.cert.fi/tietoturvanyt/2013/05/ttn201305291605.html. Luettu 30.5.2013.

Cert-fi 2011, WWW-dokumentti, https://www.cert.fi/tietoturvanyt/2011/11/ttn201111141503.html, Luettu 13.1.2014.

Elisa 2011. Elisa mobiilivarmenne -palvelun yleiset sopimusehdot. WWW-dokumentti. https://mobile-id.elisa.fi/rekisterointi/generalterms. Luettu 20.9.2013.

F-Secure 2013. News from the lab – Mac spyware found at Oslo Freedom Foorum. WWW-dokumentti. http://www.f-secure.com/weblog/archives/00002554.html. Luettu 25.5.2013.

F-secure 2013. Mobile threat report January-march 2013. pdf-dokumentti. http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2013.pdf. Luettu 25.5.2013.

Hakala Mika, Vainio Mika, Vuorinen Olli 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

JHS 171 2012. ICT-palveluiden kehittäminen. Kehittämiskohteiden tunnistaminen. WWW-dokumentti. http://docs.jhs-suositukset.fi/jhs-suositukset/JHS171/JHS171.pdf. Luettu 8.2.2014.

JHS 173 2012. ICT-palveluiden kehittäminen. Vaatimusmäärittely. WWW-dokumentti. http://docs.jhs-suositukset.fi/jhs-suositukset/JHS173/JHS173.pdf. Luettu 22.2.2014.

JHS 179 2011. ICT-palveluiden kehittäminen. Kokonaisarkkitehtuurin kehittäminen. WWW-dokumentti. http://docs.jhs-suositukset.fi/jhs-suositukset/JHS179/JHS179.pdf. Luettu 13.1.2014.

Kuluttajaliitto 2014. Valppaana verkkokaupassa. WWW-dokumentti. http://www.kuluttajaliitto.fi/teemat/kuluttajan_talous/hankkeet_ja_materiaalit/ostospuntari/valppaana_verkkokaupassa. Luettu 8.3.2014

Luoti 8/2006, Liikenne ja viestintäministeriö 2006. Tietoturvaopas sähköisen palvelun tarjoajalle (Luoti 8/2006). WWW-dokumentti. http://www.lvm.fi/fileserver/8_2006.pdf. Luettu 13.1.2014.

Manzuik Steve, Gold André, Gatford Chris 2007. Security Assessment from vulnerability to patch. Rockland:Syngress Publishing inc.

MOT Kielitoimiston sanakirja 2012. Kotimaisten kielten keskus ja Kielikone Oy

Mäntylä ,Taina 2010. Nuorten aikuisten koti, kulutus ja ajankäyttö. Kuluttajaviraston julkaisusarja 3/2010.

Nenonen, Markku 2012. Kokonaisarkkitehtuuri. Mikkelin ylemmän amk:n sähköisen asioinnin ja arkistoinnin luennot 2012-2013.

Saleh, Kassem A 2009. Software Engineering. Fort Lauderdale:J. Ross Publishing inc.

Sanastokeskus TSK ry 2008. Tietotekniikan termitalkoot. WWW-dokumentti, http://www.tsk.fi/tsk/termitalkoot/. Luettu 2.3.2014

Ojasalo Katri, Moilanen Teemu, Ritalahti Jarmo 2009.
Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Porvoo, WSOYpro.

Pitkänen Olli, Tiilikka Päivi, Warma Eija 2013. Henkilötietojen suoja. Vantaa, Hansaprint.

Tilastokeskus 2013. Väestön tieto- ja viestintätekniikan käyttö 2013. WWW-dokumentti. http://www.stat.fi/til/sutivi/2013/sutivi_2013_2013-11-07_fi.pdf. Luettu 2.3.2014.

Tilastokeskus 2014. Käsitteet ja määritelmät. WWW-dokumentti. http://www.stat.fi/meta/kas/index.html. Luettu 25.1.2014.

Secunia 2014. Secunia personal software inspector (PSI). WWW-dokumentti. Secunia.com. Luettu 25.1.2014.

Valtiokonttori 2012. Kansalaisen asiointitili - viranomaisten päätökset sähköisesti kansalaisille. WWW-dokumentti, http://www.valtiokonttori.fi/fi-FI/Kansalaisille_ja_yhteisoille/Sahkoisen_asioinnin_palvelut/Kansalaisen_asiointitili/Kansalaisen_asiointitili__viranomaisten_(44474), Luettu 20.1.2014.

Valtiovarainministeriö 2013. Sähköisen asioinnin viitearkkitehtuuri. pdf-dokumentti. https://www.yhteentoimivuus.fi/view/Asset/downloadAsset.xhtml?releaseId=1519&id=60126. Luettu 8.1.2014

Vahtiohje 4 2013. Henkilöstön tietoturvaohje. pdf-dokumentti. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20131122Henkil/Vahti_4_2013_A5.pdf. Luettu 13.1.2014

Viestintävirasto 2011a. Palveluiden turvallinen käyttö. WWW-dokumentti, http://www.tietoturvaopas.fi/internetinpalvelut/palveluidenturvallinenkaytto.html. Luettu 25.1.2014.

Viestintävirasto 2011b. Ohje 2/2011 Langattomien verkkojen tietoturvasta. WWW-dokumentti. https://www.cert.fi/ohjeet/2011_23/ohje-2011-02.html. Luettu 13.1.2014.

Viestintävirasto 2013. ADSL-modemin suojaaminen. WWW-dokumentti. https://www.viestintavirasto.fi/tietoturva/laitteenturvallinenkaytto/adsl-modeemi.html. Luettu 13.1.2014.

Virve Petteri 2006. Mediaksi kotiin, Tutkimus teknologioiden kotouttamisesta. Tampere, Tampereen yliopistopaino Oy – Juvenes Print.

LIITE 1(1).

Kodin sähköisen asioinnin ja tietoturvan kehittämisen vaiheet

1. päätä mitkä ovat kodissasi tärkeitä ja suojattavia asioita (ydintietoa)
    - tiedostot
    - asiakirjat
    - salasanat
    - tärkeät yhteydet

2. kartoita nykytila
    - mitä palveluita käytät ja miten?
    - mihin ydintieto on tallennettu?
    - miten ydintieto on varmistettu?
    - millainen kotisi sisäverkko on?
    - mitä laitteita kotisi verkkoon on kytketty?
    - mitä ohjelmia käytät?
    - mitä haittaohjelmien torjuntaohjelmistoja käytät?
    - miten havaitset päivittämättömät ohjelmat ja kuinka päivität ohjelmat?
    - dokumentoi nykytila
    - havainnoi kehittämiskohteita

3. laadi kehittämissuunnitelma
    - laadi strategia eli mitkä ovat kehittämisen tavoitteet?
    - pohjana ovat nykytilan kartoituksessa esille tulleet kehittämisehdotukset
    - laadi budjetti
    - rajaa kehittämiskohteet resurssien mukaan.

4. laadi vaatimusmäärittely
    - helpottamaan hankintoja

5. toteuta kehittämiskohteet resurssien puitteissa
    - kaikkea ei tarvitse tehdä kerralla

6. tee kehittämisestä jatkuvaa toimintaa
    - eli palaa kohtaan 1.

Lisäksi seuraa jatkuvasti tietoturvauhka tilannetta

- cert-fi:n haavoittuvuustiedotteet
- mediassa esillä olevat tietoturvauhat
- reagoi havaittuihin tietoturvauhkiin.