VALTIOVARAINMINISTERIÖ

Pääte-laitteiden tieto-turva-ohje

5/2013 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Päätelaitteiden tietoturvaohje

Valtionhallinnon tietoturvallisuuden johtoryhmä 5/2013 VAHTI

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila/VM-julkaisutiimi
Kuvitus: Grafiant / Antti Laitinen

ISSN 1455-2566 (nid.)
ISBN 978-952-251-519-3 (nid.)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-520-9 (PDF)

Juvenes Print - Suomen Yliopistopaino Oy, 2013

VALTIOVARAINMINISTERIÖ

Ohje VM/2723/00.00.00/2013

5.12.2013

Ministeriöille, virastoille ja laitoksille

Päätelaitteiden tietoturvaohje

Oheisen valtiovarainministeriön antaman päätelaitteiden tietoturvaohjeen (VAHTI 5/2013) tarkoituksena on toimeenpanna tietoturvallisuusasetuksen vaatimuksia valtionhallinnon päätelaitteissa sekä yhdenmukaistaa päätelaitteiden suojauskäytäntöjä tietojen käsittelyssä. Ohje antaa linjauksia päätelaitteiden käytön suunnittelulle ja ohjeistamiselle sekä olemassa olevien päätelaitteiden ja palveluiden käyttämiseen liittyvien riskien arvioimiselle ja hallinnalle.

Ohje tukee organisaatioita valtion tietoturvallisuutta koskevan valtioneuvoston periaatepäätöksen (26.11.2009) ja Suomen kyberturvallisuusstrategian 2013 täytäntöönpanossa. Ohje on valmisteltu valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) toimesta.

Ohjeessa kuvataan nykyaikaisten päätelaitteiden ja niihin liittyvien palveluiden tyypillisiä uhkia sekä annetaan suuntaviivoja ja hyviä käytäntöjä riskien arvioimisen tueksi, turvallisen käytön mahdollistamiseksi sekä salassa pidettävien ja muiden tietojen turvaamiseksi.

Ohje tukee ja täydentää olemassa olevia VAHTI-ohjeita. Ohjetta suositellaan hyödynnettäväksi koko julkisessa hallinnossa. Ohje korvaa Älypuhelimien tietoturvallisuus - hyvät käytännöt VAHTI-ohjeen (VAHTI 2/2007) sekä täsmentää Sisäverkko-ohjeen lukua 13 (VAHTI 3/2010) ja Teknisen ICT-ympäristöjen tietoturvataso-ohjeen (VAHTI 3/2012) vaatimuksia päätelaitteiden osalta.

Tätä ohjetta voidaan käyttää sellaisenaan tai organisaatioiden omien ohjeiden tukena. Ohje julkaistaan VAHTIn internet-sivuilla. Lisätietoja antavat valtiovarainministeriön tietoturvallisuusasiantuntija Aku Hilve, erityisasiantuntija Aarne Hummelholm, erityisasiantuntija Kimmo Janhunen ja neuvotteleva virkamies Tuomo Pigg (etunimi.sukunimi@vm.fi).

Hallinto- ja kuntaministeri — Henna Virkkunen

Yksikön päällikkö — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite — Päätelaitteiden tietoturvaohje (VAHTI 5/2013)

Tiedoksi — Kunnat

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

Lyhyesti VAHTI:sta

Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tieto- ja kyberturvallisuuden linjaukset ja niiden tietoturvatoimenpiteiden ohjausasiat. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTI:n tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTI edistää hallitusohjelman, Yhteiskunnan turvallisuusstrategian (YTS), Julkisen hallinnon ICT-strategian, valtioneuvoston huoltovarmuuspäätöksen, valtioneuvoston periaatepäätöksen valtion tietoturvallisuuden kehittämisestä ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä valtion tietoturvallisuutta ja siihen liittyvää yhteistyötä.

Valtioneuvosto teki 26.11.2009 periaatepäätöksen valtionhallinnon tietoturvallisuuden kehittämisestä. Periaatepäätös korostaa VAHTI:n asemaa ja tehtäviä hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elimenä. Periaatepäätöksen mukaisesti hallinnonalat kohdistavat varoja ja resursseja tietoturvallisuuden kehittämiseen ja VAHTI:ssa koordinoitavaan yhteistyöhön.

VAHTI:n toiminnalla parannetaan valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on kansainvälisestikin verrattuna merkittäväksi katsottava yleinen tietoturvallisuusohjeisto (www.vm.fi/vahti ja www.vahtiohje.fi).

Tiivistelmä

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) edellyttää tietoturvallisuuden perustason saavuttamista kaikilta valtionhallinnon virastoilta ja laitoksilta. Mikäli organisaatio on tehnyt tietojen luokittelupäätöksen, asetus edellyttää myös tietoturvallisuuden korotetun ja korkean tason tietojenkäsittelyn suojaustoimia ja menettelyitä silloin kun käsitellään suojaustasojen I, II tai III tietoja. Tämän VAHTI-ohjeen näkökulmana on eri tietoturvatasojen hallinnan sekä salassa pidettävien tietojen vaatimusten toimeenpanon tukeminen päätelaitekäytössä.

Ohjetta laadittaessa on huomioitu VAHTI:n vuonna 2012 julkaisema Teknisten ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012), jonka sisältöä tämä ohje täydentää sekä täsmentää vaatimuksia päätelaitteiden vaatimusten osalta. Tämä ohje korvaa Älypuhelimien tietoturvallisuus - hyvät käytännöt -ohjeen (VAHTI 2/2007) sekä täsmentää Sisäverkko-ohjeen luvun 13 (VAHTI 3/2010), sen vaatimukset 13.1-13.12 ja Teknisen ICT-ympäristöjen tietoturvataso-ohjeen (VAHTI 3/2012) vaatimuksia päätelaitteiden osalta.

Osa valtionhallinnon organisaatioista on ottanut käyttöön uusia työskentelytapoja, päätelaitteita sekä niihin liittyviä palveluita. Tämän ohjeen avulla valtionhallinnon organisaatiot voivat niitä käyttäessään ja käyttöä suunnitellessaan arvioida ja ottaa huomioon salassa pidettävien tietojen käsittelyn turvallisuuden erilaisissa käyttötapauksissa. Salassa pidettävän tiedon siirtyessä valtionhallinnon organisaatiolta toiselle, yhteisillä turvallisuusvaatimuksilla varmistetaan tiedon turvallisuuden pysyminen sillä tasolla, minkä tiedon omistaja on sille asettanut. Valtionhallinnon organisaation tulee huomioida näiden turvallisuusvaatimusten varmistaminen myös yhteistyökumppaneidensa ja asiakkaidensa kanssa tapahtuvassa salassa pidettävien tietojen käsittelyssä ja vaihdossa.

On suositeltavaa, että tämän ohjeen sisältämät linjaukset otetaan käyttöön hallinnonaloja ja virastoja koskevissa soveltamisohjeissa sekä organisaatioiden

suunnitellessa uusien päätelaitteiden ja niihin liittyvien palveluiden käyttöönottoja. Eri suojaustason tietojen käsittely edellyttää kyseiselle suojaustasolle asetettujen vaatimusten varmistamista myös päätelaitteilla ja niihin liittyvissä palveluissa tapahtuvassa tietojen käsittelyssä. Joissain tapauksissa tietojärjestelmän tai palvelun teknisillä ratkaisuilla voidaan kompensoida tiettyjen päätelaitteiden tietojen suojauksen tai hallinnan puutteita, tai rajata salassa pidettävien tietojen käsittelyä päätelaitteilla. Näin pienentyneiden riskien ansiosta voidaan tarvittaessa mahdollistaa tiettyjen käyttötapausten salliminen valituille päätelaitteille. Tämä tehdään aina riskien arvioinnin kautta, jossa on huomioitava muun muassa kohderyhmän (loppukäyttäjien, pääkäyttäjien, yhteistyökumppaneiden ja asiakkaiden) kannalta tarpeelliset käyttötapaukset sekä näissä muodostuva rajattu tietojenkäsittely-ympäristö, joka sisältää päätelaitteiden ja palveluiden lisäksi tarvittavat tietojärjestelmät, verkot sekä tilat.
Ohje on laadittu VAHTI:n alaisessa hankeryhmässä, jonka jäseninä ovat toimineet:

- Kimmo Janhunen, valtiovarainministeriö
  (Oikeusrekisterikeskus 31.10.2013 saakka), ryhmän puheenjohtaja
- Aku Hilve, valtiovarainministeriö, ryhmän varapuheenjohtaja
- Tuomo Pigg, valtiovarainministeriö
- Tommi Simula, Valtiokonttori
- Teemu Kuparinen, Valtiokonttori
- Tommi Welling, Valtiokonttori
- Sauli Pahlman, Viestintävirasto
- Jyrki Kokkinen, Aalto yliopisto
- Aarne Koutaniemi, tasavallan presidentin kanslia
- Pekka Vähämäki, Maanmittauslaitos
- Jussi Salminen, Tullihallitus.

Ohjeen laadintaan osallistuivat konsultteina KPMG:n asiantuntijat Matti Järvinen ja Antti Alestalo.

Ohjeen luonnos oli laajalla lausuntokierroksella 16.9.2013 – 2.10.2013. Saadut lausunnot käsiteltiin työryhmän kokouksessa 9.10.2013 ja huomioitiin ohjeen lopullisessa versiossa.

VAHTI päätti ohjeen julkistamisesta lokakuussa 2013 pidetyssä kokouksessaan.

Sisältö

1 Johdanto

1.1 Ohjeen tausta, tarkoitus ja tavoite

Ohje on laadittu tukemaan valtionhallinnon toimijoita päätelaitteilla tai niiden välityksellä tapahtuvan tietojen käsittelyn turvaamista. Päätelaitteita koskevien linjausten, vaatimusten ja erilaisten toteutustapojen tavoitteina on osaltaan varmistaa salassa pidettävien tietojen ja tietojärjestelmien turvallisuus ja saatavuus tarvittavissa käyttötilanteissa. Ohjeen tavoitteena on myös jakaa hyviä käytäntöjä ja yhtenäistää menettelytapoja, joita tarvitaan salassa pidettävien tietojen käsittelyn turvaamiseksi päätelaitteilla ja niihin liittyvissä palveluissa. Tässä ohjeessa keskitytään päätelaitteilla tai pääteistunnoissa tapahtuvan tietojen käsittelyyn täydentäen ja täsmentäen aiemmin annettuja VAHTI-ohjeita.

Ohjetta laadittaessa on huomioitu päätelaitteiden tarkoituksenmukainen käytettävyys, kustannustehokkuus sekä vakioitujen toimintamallien ja menettelyiden kautta toivottavasti saavutettavat säästöt eri tietoturvatasojen tietojenkäsittely-ympäristöjen hallinnassa. Päätelaitteella on keskeinen rooli salassa pidettävän tiedon käsittelyn turvaamisessa, etenkin jos tietojärjestelmässä tai palvelussa on tietoturvapuutteita tai jos järjestelmä tai palvelu ei pysty päätelaitteella tapahtuvaa salassa pidettävien tietojen käsittelyä rajaamaan. Puutteita voi olla esimerkiksi päätelaitteen, loppukäyttäjän tai pääkäyttäjän vahvassa tunnistamisessa. Puutteen vaikutus tai sen merkittävyys voi muuttua käsiteltäessä eri suojaustasojen tietoja, riippuen tarvittavista käyttötavoista ja tietojenkäsittely-ympäristöistä.

Tässä ohjeessa esitetään nykyaikaisiin päätelaitteisiin sekä niiden palveluihin, sovelluksiin ja käyttöympäristöihin liittyviä yleisimpiä uhkia. Lisäksi liitteessä 1 esitetään päätelaitteille ja niihin liittyville palveluille täydentäviä ja täsmennettyjä vaatimuksia Teknisen ICT-ympäristön tietoturvataso-ohjeen (VAHTI 3/2012) liitteeseen 3. Ohjeessa keskitytään suojaustasojen IV ja III tietojen päätelaitekäsittelyn suojaamiseen. Lisäksi käsitellään suojaustason II tietojen käsittelyä päätelaitteilla sekä niihin liittyvien palveluiden (esim. hallinta-, valvonta- ja tukipalvelut) järjestämistä sisäverkosta, sisäverkon palveluista ja muista päätelaitteista irrallaan olevissa turvatyöasemissa (stand-alone -käyttö).

1.2 Yleistä päätelaitteista

Päätelaitteella tarkoitetaan laitetta, jolla käytetään organisaation tietoja, jotka ovat päätelaitteella, sähköisissä tietojärjestelmissä tai muissa palveluissa. Tässä ohjeessa päätelaitteen käsite on laaja; pöytätyöasemien ja kannettavien tietokoneiden lisäksi päätelaitteita ovat mm. puhelimet, älypuhelimet, päätteet ja taulutietokoneet (tabletit). Päätelaitteen tietojenkäsittely voi tapahtua itse laitteella ja siihen kiinteästi asennetulla ohjelmistolla tai käyttöympäristö voidaan käynnistää ulkoiselta vaihdettavalta muistilta, esimerkiksi USB-muistilta (Universal Serial Bus). Päätelaitteenomainen käyttöympäristö (pääteistunto) voidaan suorittaa myös verkkoyhteyden kautta, esimerkiksi etätyöpöydältä. Tällöin joissain tapauksissa samalla fyysisellä laitteella voidaan ajaa eri suojaustasojen tietojen käsittelyn mahdollistavia tietojenkäsittely-ympäristöjä tai eri käyttöjärjestelmiä.

Eri suojaustasojen tietojen käsittelyn mahdollistaminen yhdellä päätelaitteella on kuitenkin monimutkaista tai joskus jopa mahdotonta. Tästä syystä suojattavien kohteet on tunnistettava (tilat, päätelaitteet, palvelut, tietojärjestelmät, rekisterit sekä verkot) ja niissä käsiteltävien tietojen suojaustasot sekä muut suojaustarpeet tulee arvioida ja määritellä VAHTI-ohjeiden mukaisesti. Kussakin käyttötapauksessa päätelaitteille voidaan määrittää tietojenkäsittely-ympäristön, tietojen käsittelyn ja toiminnan asettamat vaatimukset.

2 Normit ja muu viitekehys

Tässä luvussa kuvataan lyhyesti keskeisimmät säädökset, normit ja suositukset, joille tämän ohjeen ohjaava sisältö perustuu.

2.1 Lait

Laki viranomaisten toiminnan julkisuudesta (621/1999) määrittelee yleisellä tasolla, millaiset viranomaisten tiedot ovat salassa pidettäviä, valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) määrittelee miten näitä tietoja tulee käsitellä.

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) edellyttää, että Suomi valtiona kunnioittaa kaikessa toiminnassaan kansainvälisen yhteistyön turvallisuusvelvoitteita. Velvoitepohjana kansainvälisessä kanssakäymisessä tyypillisesti toimivat joko tietoturvallisuutta koskevat valtiosopimukset tai Suomen muuten hyväksymät kansainväliset turvallisuussäännöstöt.

Edellä mainittujen lisäksi muun muassa perustuslaki (731/1999), henkilötietolaki (523/1999), sähköisen viestinnän tietosuojalaki (516/2004) ja laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) asettavat tietoturva- ja tietosuojavaatimuksia, jotka on huomioitava viranomaistehtävien hoitamisessa. Jos viranomaistehtävien hoitamiseen käytetään valtionhallinnon ulkopuolisia organisaatioita, on huomioitava erityisesti tietosuojaan ja varautumiseen liittyvät sijaintirajoitteet. Lisäksi viranomaisen on varmistettava riittävä tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa.

2.2 Tietoturvallisuusasetus

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) antaa määritelmän asiakirjan käsittelylle (3§), normittaa tietoturvallisuuden perusteita (4§) sekä asettaa vaatimukset tietoturvallisuuden perustasolle (5§).

Julkisuuslain 24 §:ssä on määritelty, mitkä asiakokonaisuudet ovat salassa pidettäviä. Tietoturvallisuusasetuksen 8 §:ssä on säännökset salassa pidettävien asiakirjojen ja tietojen luokituksen perusteista. Suojaustasoluokittelun perusteet on esitetty 9 §:ssä ja turvallisuusluokittelun perusteet 11 §:ssä.

Tietoturvallisuusasetuksen pykälät 13-21 asettavat luokitellun asiakirjan käsittelylle vaatimukset elinkaaren eri vaiheissa.

2.3 Ohje tietoturvallisuusasetuksen täytäntöönpanosta (VAHTI 2/2010)

Tietoturvallisuusasetuksen toimeenpanoa edesauttava VAHTI-ohje 2/2010 (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta) linjaa tietojen käsittelyssä tiedon elinkaaressa huomioitavat asiat ja menettelyt tietoturvallisuusasetusta tarkemmin. Ohjeessa asetetaan vaatimuksia salassa pidettävien tietojen käsittelylle sekä määritellään tietoturvatasot ja niihin liittyvät tietoturvavaatimukset. Ohjetta on täydennetty muilla VAHTI-ohjeilla. Tässä ohjeessa erityisesti sisäverkko-ohjeen (VAHTI 3/2010) sekä Teknisen ICT-ympäristön tietoturvataso-ohjeen (VAHTI 3/2012) tiettyjä vaatimuksia on täsmennetty huomioimaan päätelaitteet aiempaa laajemmin (muutokset on kuvattu kappaleen 2.4. taulukossa).

2.4 Sisäverkko-ohje (VAHTI 3/2010)

Sisäverkko-ohje kuvaa sisäverkkojen turvaamisen periaatteita ja antaa linjauksia salassa pidettävien tietojen suojaamiseksi eri tietoturvatasoilla. Sisäverkko-ohje kuvasi luvussa 13 myös päätelaitteiden hallinnan yleisiä vaatimuksia. Tämä ohje korvaa kyseisen luvun 13 ja sen vaatimukset 13.1-13.12. Täsmennetyt vaatimukset on kirjattu päivitettyyn Teknisen ICT-ympäristön tietoturvataso-ohjeen (VAHTI 3/2012) tietojärjestelmien tietoturvatasovaatimuksia kuvaavaan liitteeseen 3, joka on päivitettynä tämän ohjeen liitteenä 1. Päivitykset on kuvattu seuraavassa taulukossa:

Aiempi Viite	Aiempi VAHTI 3/2010 vaatimus	Täsmennetty vaatimus	Uusi viite päivitetyssä VAHTI 3/2012 liitteessä 3
13.1	Internet-palveluiden käyttö on sallittu ainoastaan organisaation sisäverkosta tai etäyhteyden (VPN) kautta.	Päätelaitteilla voidaan käyttää ei-luotettujen verkkojen (ml. Internet) palveluita vain • luotetusta sisäverkosta • etäyhteydellä (VPN) organisaation sisäverkon kautta.	2.5.1 (uusi tarkennus vaatimukseen)
13.2	Kullakin päätelaitteella on yksilöity tunnus. Identtiset laitekoonpanot erotetaan em. tunnuksen perusteella.	Organisaatiossa on luettelot organisaation omistamista, hallitsemista ja käyttämistä fyysisistä tai virtuaalisista laitteista, tietojärjestelmistä, palveluista sekä ohjelmistoista ja lisensseistä.	2.2.3 (vanha liitteen vaatimus tarkennuksineen kattaa VAHTI 3/2010 -vaatimuksen)
13.3	Käyttäjille on laadittu lyhyet, selkeät ohjeet päätelaitteiden turvallisesta verkkokäytöstä - kullekin päätelaitetyypille omansa.	Käyttäjille laaditaan lyhyet, selkeät ohjeet päätelaitteiden turvallisesta käytöstä	2.3.1 (uusi tarkennus vaatimukseen)
13.4	Tuntemattomien päätelaitteiden pääsy verkkoon on estetty kytkinporttien asetuksilla.	Tietoverkkoihin saadaan liittää vain verkon omistajan hyväksymiä laitteita.	2.5.8 (vanha liitteen vaatimus tarkennuksineen kattaa VAHTI 3/2010 -vaatimuksen)
13.5	Työasemilta avatuissa etäyhteyksissä on automaattinen aikakatkaisu.	Päätelaitteilta avatuissa etäyhteyksissä on automaattinen aikakatkaisu.	2.5.9 (uusi tarkennus vaatimukseen)
13.6	Päätelaitteissa on soveltuvilta osin käytössä laitekohtainen palomuuri.	Päätelaitteissa estetään niiden palveluiden näkyminen verkkoon, joita ei ole erikseen hyväksytty.	2.5.1 (uusi tarkennus vaatimukseen)
13.7	Päätelaitteille suoritetaan automaattinen terveystarkastus ennen niiden liittämistä sisäverkkoon.	Päätelaitteelle tehdään tarkastus ennen kuin se päästetään käsiksi verkkoihin, joista on pääsy salassa pidettäviin tietoihin.	2.5.8 (uusi tarkennus vaatimukseen)
13.8	Työasema- ja muu päätelaitekanta on yhtenäistetty.	Vaatimus on poistettu.	
13.9	Mobiililaiteiden loppukäyttäjiä on ohjeistettu niiden turvalliseen käyttöön, esimerkiksi käyttäen pohjana ja muokaten Älypuhelinten turvallinen käyttö –ohjetta (VAHTI 2/2007, muokattava liite)	Käyttäjille laaditaan lyhyet, selkeät ohjeet päätelaitteiden turvallisesta käytöstä (Vaatimus 13.9 yhdistetty vaatimuksen 13.3. kanssa)	2.3.1 (uusi tarkennus vaatimukseen)
13.10	Työasemissa on käytössä työasemakohtainen palomuuri.	Päätelaitteissa estetään niiden palveluiden näkyminen verkkoon, joita ei ole erikseen hyväksytty. (Vaatimus 13.10 yhdistetty vaatimuksen 13.6 kanssa)	2.5.1 (uusi tarkennus vaatimukseen)
13.11	Kannettavien työasemien kiintolevyt on salattu	Päätelaitteilla olevat salassa pidettävät tiedot tai massamuistit kokonaisuudessaan on salattu	2.3.3 (uusi tarkennus vaatimukseen)

Aiempi Viite	Aiempi VAHTI 3/2010 vaatimus	Täsmennetty vaatimus	Uusi viite päivitetyssä VAHTI 3/2012 liitteessä 3
13.12	Pöytätyöasemien kiintolevyt on salattu	Päätelaitteilla olevat salassa pidettävät tiedot tai massamuistit kokonaisuudessaan on salattu. (Vaatimus 13.12 yhdistetty vaatimuksen 13.11 kanssa)	2.3.3 (uusi tarkennus vaatimukseen)

2.5 Teknisen ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012)

Teknisen ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012) auttaa tietoturvallisuusasetuksen toimeenpanoa teknisemmissä palvelu- ja tietojärjestelmäympäristöissä. Ohjeen luku 4 kuvaa vaatimuksia tekniselle tietotekniikkaympäristölle ja siten osaltaan myös päätelaitteille. Ohjeen liitettä 3 on täsmennetty päätelaitteiden osalta luvun 2.4 taulukon mukaisesti.

2.6 Toimitilojen tietoturvaohje (VAHTI 2/2013)

Päätelaitteiden tietoturvallisuuden kannalta on tärkeää, että niiden käyttö tapahtuu fyysisesti riittävällä tavalla suojatussa ympäristössä. Erityishuomiota tulee kiinnittää ja tarvittaessa päivittää ohjeistusta niiden päätelaitteiden turvallisessa käytössä, joita käyttäjät siirtävät tai joita käytetään julkisissa tiloissa. VAHTI 2/2013 kuvaa toimitilojen turvallisuusvaatimukset käsiteltäessä salassa pidettäviä tietoaineistoja eri turvallisuusvyöhykkeillä. Ohjeessa on päivitetty myös laitetilojen turvallisuusvaatimukset. Ohjetta tulee hyödyntää erityisesti toimitilojen muutostilanteissa.

2.7 Kansallinen turvallisuusauditointikriteeristö (2011)

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on laadittu ensisijaisesti tapauksiin, joissa auditoinnin avulla todennetaan elinkeinonharjoittajan valmius täyttää kansainvälisen turvaluokitellun aineiston käsittelykriteerit. Sen kriteerejä voidaan käyttää myös julkishallinnon oman turvallisuustason määrittämisessä ja tarkastuksissa.

KATAKRIn I-sarjan (tietoturvallisuus) osioissa on esitetty kriteerit tietoliikenneturvallisuudelle, tietojärjestelmäturvallisuudelle ja käyttöturvallisuudelle. Osa näistä kriteereistä koskee päätelaitteiden käyttöä, koventamista ja hallintaa. Kriteerit pohjautuvat suomalaisten viranomaisten sisäisiin vaatimuksiin, VAHTI-suosituksiin, ulkomaisten viranomaisten ja tietoturvatoimijoiden julkaisuihin sekä kansainvälisiin turvallisuussäännöstöihin ja standardeihin.

2.8 Muu tausta-aineisto

Muuna tausta-aineistona on käytetty päätelaitealustojen, käyttöjärjestelmien, tietojärjestelmien ja palveluiden kovennusohjeita. Koventaminen tarkoittaa menetelmiä ja toimenpiteitä joilla turvallisuuteen liittyviä ominaisuuksia, toimintoja ja asetuksia muutetaan tai niiden käyttö estetään siten, että teknisen tietoturvallisuuden taso paranee.

Tarkempia kovennusohjeita kaipaava organisaatio voi arvioiden käydä läpi ja soveltuvin osin hyödyntää kansainvälisiä ohjeita, joita julkaisevat esimerkiksi NIST (National Institute of Standards and Technology) ja CIS (Center for Internet Security). Myös tuotteiden valmistajat julkaisevat ohjeita ja suosituksia tuotteidensa turvalliseen käyttöön (esimerkiksi security guide- ja hardening-dokumentit). Lisätietoja näiden hyödyntämisestä voi tiedustella Valtion IT palvelukeskukselta ja Viestintävirastolta.

3 Tyypillisiä uhkia ja tärkeitä huomioitavia asioita

Tässä luvussa kuvataan uhkia joita salassa pidettävien tietojen käsittelyyn erilaisilla päätelaitteilla kohdistuu.

3.1 Tietoturvallisuus päätelaitteilla

Päätelaitteen turvaominaisuuksien ja turvaohjelmistojen tehtävänä on muun muassa:

- Eriyttää eri ohjelmat ja niiden suorittaminen toisistaan
- Eriyttää eri ohjelmien käsittelemät tiedot toisistaan
- Salata päätelaitteelle tallennetut tiedot (tai päätelaitteen massamuistit)
- Havaita mikäli tietoja on yritetty käsitellä tai käsitelty oikeudettomasti
- Rajoittaa käyttäjien toimia järjestelmässä, kuten ohjelmien asennuksia ja turva-asetusten muutoksia
- Rajoittaa pääkäyttäjien toimia järjestelmässä
- Havaita tai estää haittaohjelmien toimintaa, esimerkiksi käyttäjältä vaadittavien vahvistuksien avulla
- Estää tai havaita väärinkäyttö tai tietojen oikeudeton käyttö, esimerkiksi lokitusten tai turva-asetusten avulla.

Päätelaitetta vastaan voidaan hyökätä esimerkiksi:

- Houkuttelemalla käyttäjä asentamaan haitallisia ohjelmistoja tai muodostamaan takaportti päätelaitteelle.

- Houkuttelemalla käyttäjä kytkemään päätelaitteeseen toinen laite (esimerkiksi oheislaite, vaihdettava apumuisti, älypuhelin tai muu laite), ja sen avulla suorittamalla haittaohjelmia tai varastamalla tai muokkaamalla laitteen sisältämiä tai sen kautta käsiteltäviä tietoja.
- Tartuttamalla haittaohjelma käyttäjän vieraillessa sivustolla, jossa on haittaohjelma (drive-by-download).
- Kuuntelemalla päätelaitteen tietoliikennettä tai esiintymällä yhdyskäytävänä tai muuna päätelaitteen tarvitsemana palveluna.
- Lähettämällä käyttäjälle haittaohjelman sisältävä tiedosto esimerkiksi sähköpostin, pikaviestiohjelman tai sosiaalisen median palvelun kautta. Kun käyttäjä avaa tiedoston, haittaohjelma asentuu päätelaitteeseen.
- Kalastelemalla tietoja (phishing) esimerkiksi sähköpostin, pikaviestiohjelman tai sosiaalisen median palvelun avulla. Hyökkääjä voi pyrkiä saamaan käsiinsä esim. uhrin salasanan tai organisaation salassa pidettäviä tietoja.
- Ottamalla laitteeseen etäyhteys esimerkiksi varastettujen ylläpitotunnusten, haavoittuvuuden tai (laitteisto tai ohjelmisto) takaportin avulla.
- Kohdistetulla hyökkäyksellä, jossa hyökkääjällä on tietoa organisaation IT-ympäristöstä ja henkilöistä. Tällöin voidaan käyttää esimerkiksi haavoittuvuuksia, joihin ei ole julkaistu päivityksiä eikä päätelaitteen haittaohjelmien torjuntaohjelma vielä tunnista hyökkäystä. Tällaista hyökkäystä vastaan on erittäin vaikea puolustautua pelkästään päätelaitteella, vaan se vaatii hyökkäyksen tunnistamiskykyä laajemmin koko tietojenkäsittelyympäristöltä.

Eri päätelaitealustat eroavat toisistaan merkittävästi ominaisuuksiltaan sekä uhkien ja hyökkäysten torjumiskyvyltään. Organisaation tulee mahdollistaa tietojenkäsittely eri tyyppisillä päätelaitteilla ja niihin liittyvissä palveluissa (esim. hallinta-, valvonta- ja tukipalvelut sekä mahdolliset laite- ja ohjelmistovalmistajien pilvi-, tunnistus-, tallennus- ja sosiaalisen median palvelut) vasta riskiarvioinnin jälkeen. Sen perusteella voidaan määrittää tarkoituksenmukaiset turva-asetukset ja kovennukset eri käyttötapauksille, päätelaitteille ja niihin liittyviin palveluihin sekä päättää, miten ja minkä suojaustason tietoja eri päätelaitteella ja niihin liittyvissä palveluissa voidaan käsitellä. On huomioitavaa, että tietyissä käyttötilanteissa salassa pidettävien tietojen käsittelyyn tarkoitettu verkko, tietojärjestelmä ja palvelu asettavat vaatimuksia tietojen päätelaitekäytölle.

Päätelaitteen tietoturvallisuutta voidaan heikentää merkittävästi käyttäjän tahallisilla tai tahattomilla toimilla, esimerkiksi nostamalla käyttäjän oikeuksia haavoittuvuuden avulla. Korotetuilla oikeuksilla käyttäjän on mahdollista esimerkiksi asentaa sovelluksia muistakin kuin virallisista lähteistä (esim. Applen iOS-alustalla niin kutsutun jailbreakin tavoite on usein nimenomaan uusien ohjelmien asentaminen). Tietoturvallisuus saattaa samalla heiketä myös muilla tavoin, esimerkiksi mahdollistamalla uusia verkkoa kuuntelevia tai verkkoon tietoja lähettäviä palveluita.

Päätelaitteissa saattaa olla myös valmistajasta, operaattorista tai muusta kolmannesta osapuolesta johtuvia tietoturvallisuutta heikentäviä ominaisuuksia kuten avoimia palveluita tai haavoittuvuuksia. Näitä voi olla esimerkiksi hallinta-, valvonta- ja tukipalveluissa sekä mahdollisissa laite- ja ohjelmistovalmistajien pilvi-, tunnistus-, tallennus- ja sosiaalisen median palveluissa. Päätelaitteen ja niihin liittyvien palveluiden käyttöön liittyvät riskit on hyvä kartoittaa auditoinneilla. Sosiaalisen median palveluiden ohjeistuksessa ja käytössä tulee huomioida Sosiaalisen median tietoturvaohje (VAHTI 4/2010) sekä organisaation omat sosiaalisen median käytön linjaukset.

Päätelaitteen turvallisuutta arvioitaessa on hyvä ottaa huomioon tietojen suojattavat ominaisuudet, eli luottamuksellisuus, eheys ja saatavuus. Päätelaitteiden tietoturvallisuuden heikentyminen voi vaikuttaa myös niillä käytettävien palveluiden luottamuksellisuuteen, eheyteen ja saatavuuteen sekä johtaa pahimmassa tapauksessa organisaation maineen menetykseen.

3.2 Päätelaitteelle tallentuvat tiedot

Paikallisesti tallennettavat tiedot usein nopeuttavat erilaisten palveluiden käyttöä, mutta lisäävät tietojen eheyteen kohdistuvia ja hyökkäyspinta-alan kasvun aiheuttamia tietoturvariskejä. Tietyissä palveluissa ja järjestelmissä voidaan käyttömukavuuden parantamiseksi tallentaa päätelaitteelle rajatusti suojaustason IV tietoja. Jos käsitellään usein suojaustason III tai II tietoja, niiden käsittelyä, tallennusta ja suojaamista päätelaitteella sekä käsittelyn rajauksia pitää arvioida tarkemmin.

Päätelaitteelle tallennettavia tietoja tulee tarkastella laajasti ja ainakin seuraavat tiedot on hyvä ottaa huomioon:

- Käyttäjien itse tallentamat ja siirtämät tiedostot
- Väliaikaistiedostot
- Varmuuskopiot
- Eri sovelluksissa ja järjestelmissä tallennettavat tiedot
  - kirjautumisen mahdollistavat tiedot (kuten pitkäaikaiset evästeet)
  - päätelaitteen tai sen selaimen ominaisuuksien (kuten näytön tai multimedian käsittelykyvyn) tunniste- ja sijaintitiedot
  - päätelaitteen ja sen sovellusten asetustiedot
  - sovelluksista päätelaitteelle ja sovelluksiin tallennettavat tiedot.

Edellisessä luvussa lueteltujen lisäksi tyypillinen uhka on päätelaitteen katoaminen tai varastaminen. Tällöin ei ole tiedossa, ovatko päätelaitteessa olleet tiedot joutuneet ulkopuolisten käsiin. Mikäli päätelaitteen saanut henkilö pyrkii hankkimaan tietoja, hän saattaa saada haltuunsa kaikki päätelaitteella olevat tiedot ja mahdollisesti päästä käsittelemään myös verkkopalveluiden sisältämiä tietoja, mikäli päätelaitteelle on tallennettu niiden kirjautumistietoja. Ulkopuolinen voi myös päästä muokkaamaan päätelaitetta, jolloin se tekee organisaatiolle haitallisia toimia, kuten lähettää tietoja ulkopuoliselle, häiritsee tai yrittää murtautua muihin laitteisiin ja palveluihin. Näiden tapausten varalle päätelaitteiden hallintaan on suositeltavaa harkita mobiililaitteiden hallintaohjelmiston (MDM – Mobile Device Management) hankintaa.

3.3 Päätelaitteen tietoliikenne

Päätelaitteet mahdollistavat tietoliikenneyhteyden muodostamisen monella eri tavalla, kuten GSM (2G), WCDMA (3G), LTE (4G), Ethernet, WLAN, bluetooth, NFC ja RFID. Osa tavoista, kuten NFC, ovat lähtökohtaisesti turvattomia ja toiset, kuten WLAN, ovat oikein asennettuna ja suojattuna soveltuvia salassa pidettävien suojaustason IV tietojen käsittelyyn langattomassa yhteydessä. Sisäverkko-ohje sisältää langattomien verkkojen vaatimukset, joita voidaan soveltaa myös muihin langattomiin yhteyksiin. Otettaessa käyttöön erilaisia yhteystapoja on hyvä ensin tutkia, onko niissä käytetyissä yhteyksien

salauksen toteutuksissa (kryptografisissa ratkaisuissa) mahdollisesti tunnistettuja heikkouksia. Lähtökohtana on, että kaikki tietoliikennetavat suljetaan aluksi pois ja sallitaan vain ne, joille on työtehtävissä tarvetta ja jotka voidaan asianmukaisesti turvata.

Jotkut päätelaitteet voidaan asentaa siten, että ne tunnistavat milloin ne ovat yhteydessä organisaation sisäverkkoon. Päätelaite voidaan asentaa siten, että se sallii liikennöinnin vapaammin sisäverkossa kuin muissa verkoissa. Voidaan tehdä myös päätelaitteen tarkastus ennen kuin sen sallitaan liikennöidä sisäverkkoon. Siinä voidaan varmistaa esimerkiksi laitekohtaisen palomuurin ja haittaohjelmien torjuntaohjelmiston päälläolo ja päivitysten ajantasaisuus sekä muita tietoturvallisuuteen vaikuttavia asioita.

Edellisissä luvuissa mainittujen lisäksi muita erityisesti tietoliikenteeseen liittyviä uhkia ovat esimerkiksi seuraavat:

- Hyökkääjä pystyy kuuntelemaan ja mahdollisesti muokkaamaan tietoliikennettä turvattoman liikennöintitavan kautta. Tällöin hyökkääjä voi kuunnella salassa pidettäviä tietoja ja mahdollisesti muokata liikennettä tai palveluissa tallennettavia tietoja.
- Eri valmistajien tietoliikennetoteutuksista saattaa löytyä haavoittuvuuksia, joita käyttäen hyökkääjä voi pystyä murtautumaan päätelaitteelle.

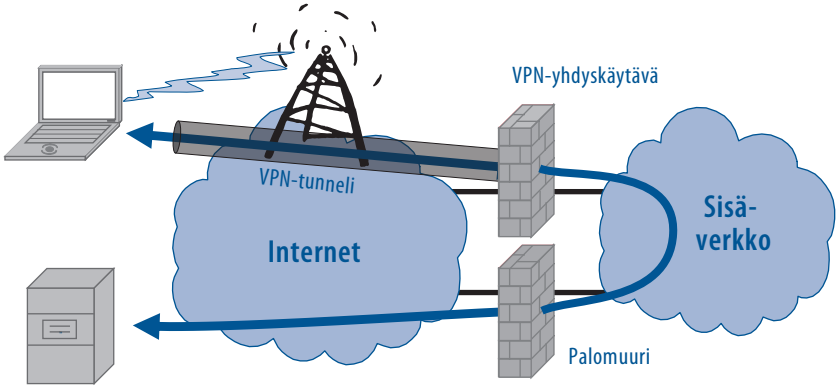
Sisäverkko-ohje sisältää laajemmin tietoa tietoliikenteeseen liittyvistä uhkista ja niiden hallitsemisesta.

3.4 Etätyön ja liikkuvan työn uhkat

Etätyön ja liikkuvan työn merkittävimmät uhkat johtuvat siitä, että päätelaite ei ole enää fyysisesti tunnetussa eikä suojatussa tilassa, ja palveluihin pitää liittyä tyypillisesti Internetin tai muun ei-luotetun verkon ylitse. Käytetyistä yhteyksistä ja tiloista johtuen on syytä ottaa huomioon tietojen salakuuntelun ja -katselun mahdollisuus sekä ohjeistaa käyttäjiä minimoimaan tarpeettomia riskejä.

Pysyvässä etätyössä on mahdollisesti järjestettävä toisin mm. ylläpito- ja päivitysprosessit mahdollisesti etäyhteyksien (VPN) kautta tai tarvittaessa fyysisesti päätelaitteella tehtävät huoltotoimenpiteet. Tiedon luottamuksellisuuden suojaamisen lisäksi palveluiden ja tietojen saatavuus ja eheys ovat tärkeitä, kun

päätelaitteilla pitää monissa käyttötapauksissa päästä käsiksi samoihin palveluihin ja tietoihin kuin organisaation sisäverkosta. Teknisen ICT-ympäristön tietoturvataso-ohje ja sen liite 7 sisältävät etäkäytön tekniset linjaukset, suositukset ja vaatimukset.



Salassa pidettävien tietojen käsittely on sallittua ainoastaan käyttäen ratkaisuja, joissa voidaan tehokkaasti salata tietoliikenne päätelaitteelta organisaation sisäverkkoon asti. Eräiden päätelaitteiden, kuten tablettien ja puhelinten, osalta tilanne saattaa olla sellainen, että ne eivät milloinkaan ota yhteyttä organisaation sisäverkkoon. Tällöin on hyvä miettiä tarkasti, miten turvallisuuteen vaikuttavat toimenpiteet, kuten päivitykset, turva-asetukset ja ohjelmistoasennukset on tarkoituksenmukaista tehdä, ja voidaanko kyseisille päätelaitteille tarjota joitakin organisaation rajattuja palveluja. Merkittävänä riskinä on hallitsematon, päivittämätön ja haavoittuva päätelaite, joka uhkaa tietojen luottamuksellisuutta, eheyttä ja saatavuutta. Tällaisten päätelaitteiden kautta tapahtuvaa tietojenkäsittelyä voi olla välttämätöntä rajata sekä teknisesti suojata palveluja ja muuta tietojen käsittelyä.

Matkustettaessa ulkomaille saattaa tulla vastaan tilanteita, joissa esimerkiksi rajavirkailija vaatii päätelaitteen tarkastettavakseen ja voi uhata käännyttämisellä, mikäli vaatimukseen ei suostuta. Virkailija voi myös sallia maahanpääsyn sillä ehdolla, että laite annetaan tarkastukseen määräajaksi. Tällöin saatetaan vaatia myös päätelaitteen salasanoja. Päätelaitteella olevat tiedot voivat silloin päätyä ulkopuolisen haltuun. Lisäksi esimerkiksi hotellien, kokoustilojen tai konferenssien tiloissa saattaa esiintyä langattomia tukiasemia tai verkkoja sekä tietojärjestelmiä (mm. ilmoittautumis-, ohjelma- ja esityksien julkaisujärjes-

telmät), joista osa voi pyrkiä keräämään ja hyödyntämään tietoja niitä käyttäneistä päätelaitteista sekä niiden käytöstä. Organisaation onkin syytä ohjeistaa päätelaitteiden sekä sisäisten sekä ulkoisten tietojärjestelmien käyttämisestä ulkomailla. Lisäksi on huomioitava myös päätelaitteiden sijaintitietojen käyttö. Nämä ovat tarpeen myös mahdollisista tietoliikenneyhteyksistä syntyvien kustannusten hallitsemiseksi.

3.5 USB-muistille asennettava käyttöympäristö

Päätelaitteelle saattaa olla tarpeen asentaa erilaisia käyttöjärjestelmiä eri käyttötapauksiin. Joissain käyttötapauksissa voidaan sallia päätelaitteen käyttö tiettyyn tarkoitukseen, jos voidaan toteuttaa sellainen ympäristö, jota käyttäjä ei pysty muokkaamaan. Monet nykyaikaisista käyttöjärjestelmistä voidaan asentaa esimerkiksi USB-muistille, jolloin päätelaitteen kiintolevyllä olevaa järjestelmää ei käytetä eikä käyttäjä pääse siihen käsiksi. Lähtökohtaisesti USB-muistilta käynnistys tulisi olla päätelaitteilla estettynä ja sallittu vain käyttötapauksen vaatimille päätelaitteille. Tällöin käyttäjille pitää antaa mahdollisuus valita käyttöjärjestelmä päätelaitteen käynnistymisen yhteydessä. Tätä ei kuitenkaan tule tehdä poistamalla käytöstä päätelaitteen BIOS-salasanaa (Basic Input-Output System, päätelaitteen käynnistyksessä käytetty ohjelmisto), vaan esimerkiksi mahdollistamalla käynnistettävän järjestelmän valinta ilman BIOS-salasanaa tai kertomalla käyttäjälle BIOS salasana.

Tällaisessa toteutuksessa tulee ottaa huomioon ainakin seuraavia asioita:

- USB-muistilta suoritettavat käyttöympäristöt on monesti tehty joustaviksi esimerkiksi siten, että ne hyväksyvät monia erilaisia laitteita. Osa käyttöympäristön oletuksena hyväksymistä laitteista voi olla tietoturvallisuuden kannalta kuitenkin haitallisia.
- Käytetäänkö käyttöympäristössä vain paikallisesti tallennettuja tietoja vai käytetäänkö käyttöympäristöä suorittavan päätelaitteen tarjoamia verkkoratkaisuja. Tuleekin ratkaista se, miten erilaisia verkkoja ja niiden palveluita voidaan käyttää turvallisesti. Tästä riippuen edellisestä, tulee myös ratkaista mm. käyttöympäristön muutoshallinnan ja päivitysten järjestäminen sekä niiden turvallinen toteutus.

- Käyttöympäristössä voi olla kaksi eri ympäristöä: päätelaitteelle asennettu käyttöympäristö ja esim. USB –muistilta ajettava käyttöympäristö. Tällöin tulee erityisesti ottaa huomioon onko tarvetta suojata näitä kahta käyttöympäristöä toisiltaan esim. siten, että ne eivät pääse käsiksi eivätkä pysty tuhoamaan toistensa tietoja. Tuhoamisen estäminen voi olla helpointa toteuttaa hyvillä varmistuskäytännöillä.

3.6 Muita huomioitavia asioita

Päätelaitekanta on viime vuosina monipuolistunut ja yhdellä käyttäjällä saattaa olla käytössään useampia päätelaitteita. Eri päätelaitteiden ominaisuudet, turva-asetukset ja ohjelmistot mahdollistavat hyvinkin erilaiset ratkaisut tietoturvallisuuden, turva-asetusten ja päätelaitteiden hallintaan ja valvontaan. Eri päätelaitteet eivät välttämättä mahdollista tietoturvallisuuden hallintaa samalla tasolla. Tietoaineistojen luokitteluun ja käsittelyohjeistukseen, muihin ohjeistuksiin sekä koulutuksiin on hyvä panostaa entistä enemmän, jotta käyttäjät tuntevat ne ja voivat toimia oikein työtehtävissään. Tällöin käyttäjä tietävät missä, miten ja mihin eri päätelaitteita saa käyttää, mitä tietoja, palveluita ja tietojärjestelmiä niille on sallittu, millä edellytyksillä ja miksi käyttöä on mahdollisesti rajattu. Näin he voivat toimia oikein käsitellessään salassa pidettäviä tietoja.

Organisaatioissa käytetään usein muiden osapuolten tuottamia palveluita. Niitä saatetaan hankkia valtionhallinnon sisältä tai ulkopuolisilta tahoilta. Valtionhallinnon organisaatioissa tulee olla toteutettuna tietoturvallisuuden perustaso. Valtionhallinnon organisaatioiden tulee toteuttaa käyttöympäristöt joissa palveluiden ja niitä käyttävien päätelaitteiden tulee pystyä turvaamaan vähintään salassa pidettävien suojaustason IV tietojen käsittely. Tämä osaltaan helpottaa suojaustason IV tietojen käsittelyn palveluiden käyttöä ja tiedon vaihtoa valtionhallinnon eri organisaatioiden välillä. Lisäksi valtionhallinnon yhteisten ratkaisujen, palveluiden ja sisäverkkojen kautta valtionhallinnon tiedon vaihtoa voidaan kehittää keskitetysti sekä periaatteessa suunnitella ja mahdollistaa myös liikkuvuuden ja tilankäytön joustavampia ratkaisuja.

4 Tietoturvatasojen soveltaminen erilaisiin päätelaitteisiin

Tässä luvussa kuvataan, miten eri tietoturvatasoja voidaan soveltaa erilaisille päätelaitteille ja mitä tietyissä esimerkkitapauksissa tulee ottaa huomioon.

4.1 Eri tietoaineistot ja suojaustasot

Salassa pidettävää tietoa säilytetään ja käsitellään organisaatiossa tyypillisesti hyvin erilaisissa paikoissa sekä monilla eri laitteilla. Tietoa on sähköisesti muun muassa päätelaitteilla ja niiden lisälaitteilla, palvelimilla, palveluissa, tietojärjestelmissä, rekistereissä, varmistusnauhoilla sekä myös fyysisesti esimerkiksi kuvina ja paperisina asiakirjoina. Sovellettaessa tietoturvatasoja päätelaitteisiin tulee päätelaitteen ja tietojen suojaustason lisäksi ottavat huomioon myös mahdolliset rajoitukset tietojen käsittelyn eri vaiheissa, käyttötapauksissa, tietojärjestelmissä, tietoverkoissa ja tiloissa. Jotkin järjestelmät, kuten sähköposti, sisältävät useampia erilaisia palveluita ja sovelluksia, joiden avulla voidaan esimerkiksi välittää usean eri omistajan tietoja. Käytettäessä tällaisia järjestelmiä eri päätelaitteilla, tulee varmistua siitä, että päätelaitteella tai niihin liittyvissä palveluissa ei käsitellä korkeamman suojaustason tietoja kuin minkä käsittelyyn päätelaite ja siihen liittyvät palvelut (esim. hallinta-, valvonta- ja tukipalvelut sekä mahdolliset laite- ja ohjelmistovalmistajien pilvi-, tunnistus-, tallennus- ja sosiaalisen median palvelut) on organisaatiossa tai valtionhallinnon palvelukeskuksessa hyväksytty, ja joiden käyttö on ohjeistettu. Erityisesti tulee muistaa, että vaikka suojaustason IV tietojen käsittely olisi sallittu organisaation ja valtionhallinnon sisäverkkojen välityksellä tapahtuvassa tiedon vaihdossa salaamattomana, ei suojaustason IV tietoja saa välittää niiden ulkopuolisille tahoille salaamattomana.

Tietojenkäsittely-ympäristöä tulee käsitellä käyttötapauksiin rajattuna kokonaisuutena. Kokonaisuutta on pystyttävä suojaamaan eri tavoin eri suojaustason tietojen käsittelyssä kaikissa käsittelyvaiheissa. Riskiarvioinnin keinoin voidaan hyväksyä korvaavia menettelyjä, mikäli tietojenkäsittely-ympäristö tai sen osa jossain käyttötapauksessa suojaa salassa pidettäviä tietoja varsinaisesta vaatimuksesta poikkeavalla tavalla, kontrollilla tai menetelmällä. Korvaava menettely on toteutettava siten, että sen avulla alkuperäisen kontrollin tavoite täyttyy riittävällä tavalla toteutettuna ja korvaavasta menettelystä aiheutuvat riskit on pienennetty hyväksyttävälle tasolle. Esimerkiksi suojaustason III tietojen käsittelyssä vaatimukseen etäyhteyksissä käytettävästä vahvasta tunnistautumisesta (VAHTI 3/2010, vaatimus 15.3 ja VAHTI 3/2012 liite 7, etäkäytön tekniset vaatimukset) voidaan tapauskohtaisesti riskiarvioinnin jälkeen hyväksyä korvaava menettely, jos päätelaite esimerkiksi sijaitsee aina luotetussa tilassa ja teknisillä menetelmillä pystytään rajoittamaan pääsyä tilaan, palveluun, tietoon tai pystytään huolehtimaan riittävän kattavista käytön lokitiedoista.

4.2 Päätelaitteiden käyttö eri tietoturvatasoilla

Jokaisen valtionhallinnon viranomaisen tulee täyttää vähintään tietoturvallisuuden perustaso. Toiminnoissa, joissa viranomaisilta edellytetään korotetun tai korkean tietoturvallisuustason toimintaympäristöä (toimintaa, tietojärjestelmiä ja tietoverkkoja) ja joissa käsiteltävät asiakirjat viranomainen on luokitellut, tulee toteuttaa vaatimukset viiden vuoden kuluessa siitä, kun luokitus on otettu käyttöön. Viranomainen voi riskienarvioinnin perusteella toteuttaa korkeampien tietoturvatasojen vaatimukset kyseisten toimintojen mahdollisesti hyvinkin rajattuihin toimintaympäristöihin ja käyttötapauksiin.

Organisaation tulee selvittää ja tarvittaessa rajata, mitkä ovat tietojenkäsittely-ympäristöt ja niiden tietoturvatasot sen eri toiminnoissa[1]. Päätöksien tulee perustua riskiarviointiin, kyseisessä tietojenkäsittely-ympäristössä käsiteltävien salassa pidettävien tietojen luokitukseen, saatavuusvaatimuksiin sekä muihin tietojen käsittelyn ja toiminnan vaatimuksiin. Päätös eri tietoturvatason tietojenkäsittely-ympäristöistä ja niihin kuuluvista palveluista vaikuttaa merkittävästi siihen, mitä tietoja, järjestelmiä ja palveluita (esimerkiksi sähköposti) päätelaitteilla voidaan käsitellä, miten laitteita tulee hallita, missä kohdin tarvitaan salausta tai muita suojauksia, tai tietojen käsittelyn rajaamista tai sen estämistä.

[1] Kts. VAHTI 3/2012

Kun organisaatio on hyväksynyt päätelaitteen ja niihin liittyvät palvelut (esim. hallinta-, valvonta- ja tukipalvelut sekä mahdolliset laite- ja ohjelmistovalmistajien pilvi-, tunnistus-, tallennus- ja sosiaalisen median palvelut) jollekin tietoturvatasolle, voidaan siinä tietoturvallisuusasetuksen mukaisesti käsitellä selväkielisenä kyseiselle tasolle hyväksytyn tai alempien suojaustasojen tietoja, kunhan samalla huolehditaan myös muista tietojen käsittelyn vaatimuksista. Tietoa ei lähtökohtaisesti tule tallentaa tai siirtää tietoverkoissa selväkielisenä. Mikäli päätelaite hyväksytään esimerkiksi korotetun tietoturvatason ympäristöön, voidaan sillä käsitellä selväkielisenä suojaustason III tietojen lisäksi suojaustason IV ja julkisia tietoja. Mikäli korkeamman tietoturvatason päätelaitteella halutaan käyttää alemman tietoturvatason järjestelmiä, tulee käytön riskejä arvioida, ja käyttö tapahtua yhdyskäytäväratkaisun kautta. (vertaa KATAKRI, ks. erityisesti I 401.0).

Päätelaitteen hyväksyntä tietylle tietoturvatasolle voidaan tehdä esimerkiksi auditoinnilla, jossa päätelaitteiden ja niihin liittyvien palveluiden (esim. hallinta-, valvonta- ja tukipalvelut sekä mahdolliset laite- ja ohjelmistovalmistajien pilvi-, tunnistus-, tallennus- ja sosiaalisen median palvelut) ominaisuuksia ja niiden hallintaa verrataan halutun tietoturvatason vaatimuksiin. Kun päätelaitteen soveltuvuus haluttuun käyttöön, asetukset ja kovennukset halutun mukaiselle päätelaitteen tietoturvallisuuden hallinnalle on varmistettu, voidaan päätelaite hyväksyä käyttöön. Jokaisen valtionhallinnon organisaation ei kannata erikseen auditoida erilaisia päätelaitteita, vaan on hyvä selvittää onko jokin muu organisaatio (esimerkiksi valtionhallinnon palvelukeskus tai Viestintävirasto) jo selvittänyt halutun päätelaitteen soveltuvuuden vastaavaan käyttötarkoitukseen. On kuitenkin huomioitava kyseisen käyttötarkoituksen ja käytettyjen tietojärjestelmien mahdollisesti hyvinkin rajoitettu käyttäminen sekä rajoitetun tietojenkäsittely-ympäristön vaikutukset väärinkäsitysten välttämiseksi. Edellä mainitut vaihtelevat eri toteutuksissa ja käyttötapauksissa, eivätkä siksi ole sellaisenaan suoraan vertailukelpoisia.

Organisaatio määrittelee esimerkiksi tietoaineistojen käsittelyohjeessaan, miten eri suojaustasojen tietoa voidaan käsitellä eri palveluissa, tietojärjestelmissä, rekistereissä ja päätelaitteissa. On syytä määritellä ja ohjeistaa myös ne tietojenkäsittely-ympäristöt ja käyttötavat, joilla tietoa voidaan käsitellä eri päätelaitteilla halutuissa käyttötapauksissa.

Organisaatiossa voi olla useamman eri tietoturvatason päätelaitteita, voidaan esimerkiksi hyväksyä työasemat korotetulle ja älypuhelimet tietoturvallisuuden perustasolle. Tässä esimerkissä eri päätelaitteilta voi käyttää erilaisia

palveluita tai käyttää niitä rajoitetusti: kaikilta laitteilta voidaan käyttää tietoturvallisuuden perustason järjestelmiä, mutta vain työasemilta korotetun tietoturvatason järjestelmiä. Joitakin korotetun tietoturvatason järjestelmiä ja niissä käsiteltäviä salassa pidettäviä tietoja voidaan kuitenkin mahdollisesti riittävästi rajata ja hyväksyä niiden tarkasti rajattu käyttö hyvin hallituilla älypuhelimilla.

Käytetyt järjestelmät ja niiden sisältämät salassa pidettävät tiedot ovat pohjana päätöksenteolle, mutta siihen voi vaikuttaa myös se, mitä työvälineitä, palveluita, sovelluksia, tietojärjestelmiä ja rekistereitä eri päätelaitteella halutaan käyttää. Organisaatio voi olla aiemmin käyttänyt sähköpostia suojaustason III tietojen sisäiseen käsittelyyn salaamattomana ja haluaa käyttää sähköpostia myös älypuhelimilla. Jos organisaation käyttämät älypuhelimet saadaan teknisesti kovennettua vain suojaustason IV käsittelykykyiseksi, voi organisaatio päättää rajoittaa sähköpostilla sisäisesti käsittelyn vain suojaustason IV tietoihin. Uusi menettely tulee ohjeistaa sähköpostin käyttäjille sekä ohjeistaa tarkasti miten suojaustason III tietoja käsitellään sisäisesti sekä miten suojaustason IV ja III tietoja voidaan turvallisesti välittää ulkopuolisille. Tulee myös ottaa huomioon miten käsitellään aiempia viestejä ja niiden sisältämiä tietoja. Suojaustason III tietojen välittäminen ulkopuolisille voidaan toteuttaa rajatusti esimerkiksi salatulla sähköpostilla tai liitetiedostoilla, joiden avaaminen tai joihin pääsy voidaan teknisesti estää hyväksymättömiltä päätelaitteilta. Menettely pitää ohjeistaa sekä huomioida tietosuoja ja toiminnan muut vaatimukset. Välitettäessä ulkopuolisille suojaustason IV tietoja sähköpostilla tulee ottaa huomioon tietojen asianmukainen suojaus, ja käyttää salattua sähköpostia tai salattua liitetiedostoa.

Tiedon käyttöä eritasoisissa päätelaiteympäristöissä voidaan rajoittaa myös siten, että tietoaineisto merkitään DRM-leimalla (Digital Rights Management) tai metatiedoilla, jotka kertovat vähintäänkin tietoaineiston suojaustason. Järjestelmät voidaan konfiguroida siten, että ne eivät salli pääsyä sellaisilta päätelaitteilta tai tiedon välitystä sellaisiin päätelaitteisiin tai palveluihin, joita ei ole erikseen hyväksytty kyseiselle suojaustasolle. Tällaisissa järjestelmissä voidaan mahdollisesti myös teknisesti huomata ja estää tietojen luokittelut vahingossa väärälle suojaustasolle, jolloin kyseisen tietoaineiston käsittely voi estyä virheluokituksen perusteella.

Lähtökohtana on, että salassa pidettäviä tietoja käsitellään vain hyväksytyillä päätelaitteilla ja käyttötapauksilla. Käytännön syistä on kuitenkin joihinkin rajattuihin käyttötapauksiin tarvetta käyttää päätelaitteita, joiden saattaminen halutulle tietoturvatasolle kaikilta osin on teknisesti hankalaa tai mahdotonta.

Tällöin tulee tehdä tapauskohtainen riskiarvio ja päättää voidaanko kyseisiä käyttää korvaavan menettelyn avulla, vaikka ne eivät kaikilta osin vaatimuksia täyttäisikään. Tietojärjestelmän tai palvelun teknisillä ratkaisuilla voidaan osaltaan kompensoida päätelaitteiden suojauksen puutteita tai rajata salassa pidettävien tietojen käsittelyä. Riskejä pienentämällä voidaan tarvittaessa harkita tiettyjen käyttötapausten mahdollistamista valituille päätelaitteille. Riskiarviointiin voidaan hyödyntää mm. Valtion IT-palvelukeskuksen tietoturvallisuuden työkalupakin riskiarviointivälineettä tai VAHTI 7/2003 ”Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa” -ohjetta. Riskiarvioinnissa on huomioitava käyttötapauksessa tarvittava rajoitettu tietojenkäsittely-ympäristö eikä vain päätelaitetta.

Tietojen omistaja määrittelee salassa pidettävän tiedon suojaustason, jonka perusteella vaatimukset tietojen käsittelyyn määräytyvät. Tietojen omistajan ja tietoturvavastaavan on myös hyväksyttävä mahdolliset poikkeukset turvatoimenpiteisiin. Tietojen omistaja voi myös määritellä tietojen käytölle ja käsittelylle reunaehtoja, kuten

- Rajallinen aika – päätelaitetta, joka ei täytä vaatimuksia kaikilta osin, voidaan käyttää rajattu aika, jonka jälkeen tulee siirtyä käyttämään vaatimukset täyttäviä päätelaitteita ja menettelyitä
- Rajallinen käyttäjäjoukko – salassa pidettävään tietoon pääsyä ei anneta yhtä suurelle käyttäjäjoukolle kuin siinä tapauksessa, että päätelaitteet ovat kaikilta osin vaatimusten mukaisia
- Poikkeava ja rajattu käyttötapa – toteutetaan jokin menetelmä, jolla tietoaineistosta pystytään esim. hakemaan vain pieniä osia, kun vaatimusten mukaisilla päätelaitteilla pääsy voitaisiin myöntää isompiin tietokokonaisuuksiin, tai esim. pääsy pystytään rajaamaan teknisesti ja hallinnollisesti vain suojaustason IV ja julkisiin tietoihin.

Tietoja käsitellään useimmiten erilaisten palveluiden, sovellusten, tietojärjestelmien tai rekisterien kautta. Samaa tietoa voidaan käsitellä useissa eri palveluissa tai tietojärjestelmissä eri käyttötapauksin. Tiedon omistajan on syytä huolehtia siitä, että eri tavoilla tietoja käsiteltäessä kokonaisriskitaso ei nouse liian suureksi.

Korvaavia menettelyitä arvioitaessa on hyvä kiinnittää huomiota mm. seuraaviin päätelaitteita koskeviin asioihin:

- Kuka hallinnoi ja hallitsee päätelaitteita – voidaanko omilla hallintamenettelyillä esim. (1) tyhjentää päätelaitteen sisältö, jos huomataan, että päätelaite on kadonnut tai varastettu, (2) muokata helposti tietoturvallisuuteen vaikuttavia turva-asetuksia, (3) pakottaa halutut turva-asetukset käyttöön tai (4) valvoa päätelaitteiden käyttöä (huomioitava mahdolliset YT-menettelyt ja tietosuojan varmistaminen)
- Kuinka paljon hyötyä poikkeuksen hyväksymisestä on
- Onko kyseisessä rajatussa tietojenkäsittely-ympäristössä käytössä muita korvaavia menettelyjä ja aiheutuuko niistä lisäriskejä.

5 Palveluiden ja sovellusten käyttäminen päätelaitteella

Tässä luvussa kuvataan päätelaitteiden palveluiden ja sovellusten käyttämiseksi tarvittavia organisaatiotason päätöksiä sekä niiden huomioimista tietojen ja palveluiden käytössä.

5.1 Tehtävät päätökset

Tärkeimmät valtionhallinnon organisaation päätelaitteisiin ja näiden käyttöön liittyvät päätökset ovat (1) tietojen luokittelupäätös, (2) päätökset valittujen päätelaitteiden sijoittumisesta eri tietoturvatasoille sekä (3) päätökset palveluiden, tietojärjestelmien ja rekistereiden sijoittumisesta eri tietoturvatasoille.[2] Näitä päätöksiä ohjaavat osaltaan palveluiden, järjestelmien ja rekistereiden tärkeys- ja kriittisyysluokitus, niiden mahdollisesti eriytetyt tekniset tietojenkäsittely-ympäristöt (tuotanto-, kehitys-, koulutus- ja testiympäristöt tai niiden osat), palveluiden ja järjestelmien elinkaari, niiden suojausmahdollisuudet sekä toiminnan tavoitteet ja niihin liittyvät uhat. Valtionhallinnon toimijan tulee tehdä riskianalyysi ennen merkittäviä päätelaitteisiin liittyviä päätöksiä ja toimenpiteitä. Riskianalyysissä voidaan hyödyntää esim. luvussa 4.2 mainittuja tapoja.

Organisaation päätelaitteilla käsitellään tyypillisesti julkista tietoa, ja silloin kun on tarvetta käsitellä salassa pidettäviä tietoja, ne ovat tyypillisesti suojaustasoilla IV ja III. Organisaation tulee kartoittaa, onko joissakin toiminnoissa ja joillain päätelaitteilla tarvetta käsitellä suojaustasojen II tai I tietoja. Niitä varten

[2] Palveluiden luokittelua ja vaadittavia kontrolleja eri tietoturvatasoille on kuvattu VAHTI 3/2012 –ohjeessa ja sen liitteissä.

tulee tehdä erillisratkaisuja tai kehittää olemassa olevia päätelaitteita vaatimusten mukaiselle tasolle. Lisäksi tulee kartoittaa se, missä määrin toiminnoissa on tarvetta suojaustason III tietojen käsittelyyn, ja voidaanko niiden käsittely järkevästi rajata tiettyihin käyttötapauksiin, käyttäjäryhmiin/-rooleihin, palveluihin ja järjestelmiin.

Organisaation tulee päättää myös rajoitetaanko käyttäjän mahdollisuutta asentaa ja suorittaa ohjelmia päätelaitteilla. Riippuen päätelaitteesta, voidaan käyttää ainakin seuraavia asentamisen ja suorittamisen malleja (turvallisimmasta turvattomimpaan):

- Estetään ohjelmien asentaminen ja suorittaminen: teknisesti estetään käyttäjiltä (ja haittaohjelmilta) kokonaan mahdollisuus ohjelmien asentamiseen ja mahdollistetaan ainoastaan haluttujen ohjelmien suorittaminen
- Whitelist: mahdollistetaan ainoastaan haluttujen ohjelmien asentaminen ja suorittaminen sekä estetään muiden ohjelmien asentaminen ja suorittaminen
- Kielletään ohjelmien asentaminen: teknisesti ei estetä ohjelmien asentamista, mutta päätelaitepolitiikassa ja käyttöohjeistuksessa kielletään käyttäjien itse tekemät ohjelmien asennukset
- Blacklist: estetään joidenkin haitalliseksi havaittujen ohjelmien asentaminen ja suorittaminen
- Sallitaan kaikkien ohjelmien asentaminen: teknisesti ei estetä ohjelmien asentamista eikä myöskään kielletä sitä.

Mikäli ohjelmien asentamista ei estetä teknisesti, voidaan päätelaitetta käyttää riskiarvioinnin jälkeen korkeintaan suojaustason IV tietojen käsittelyyn rajoitetusti. Tällöin on erityinen syy ohjeistaa käyttäjille, miten he voivat itse havaita haitallisia ohjelmia ja miten he voivat käsitellä tietoja. Käytännössä organisaation tulee tällöinkin harkita ainakin käyttäjien asentamien ohjelmien seurantaa eri päätelaitteilla (ja niiden alustaversioilla). Lisäksi tulee muistaa, että päätelaiteille on saatavilla myös paljon ohjelmia, jotka eivät vaadi varsinaista asentamista (pääkäyttäjäoikeuksin), vaan ne voidaan suorittaa lataamalla ohjelmatiedosto internetistä tai siirrettävältä apumuistilta (esim. USB-muisti).

Organisaation ei-julkisia palveluita voi olla tarve käyttää myös muilla kuin organisaation omistuksessa ja hallinnassa olevilla päätelaitteilla. Näitä voivat olla esimerkiksi

- Käyttäjien omat päätelaitteet:
  - Mobiililaitteet (ns. BYOD-laite, Bring Your Own Device)
  - Kotikoneet
- Yhteistyökumppaneiden päätelaitteet
  - Toiset valtionhallinnon organisaatiot
  - Palvelutoimittajat
- Yleisessä käytössä olevat päätelaitteet, esim. Internet-kahvilat.

Organisaation tulee tehdä päätös, sallitaanko tällaisten päätelaitteiden käyttö ja mikäli sallitaan, miten ja mihin niitä on luvallista käyttää. Lähtökohtaisesti niiltä ei pidä sallia pääsyä organisaation sisäverkkoon, jossa omat päätelaitteet ovat. Lisäksi tulee päättää, miten tällaisia laitteita hallitaan ja valvotaan sekä voidaanko päätelaitteita edes joiltain osin koventaa ja mahdollisesti sallia rajattu pääsy. Tässä yhteydessä on huomioitava seuraavat asiat:

- Jokaiselle edellä mainitun kaltaiselle päätelaitteelle sallitulle palvelulle tulee tehdä riskiarvio ja päättää voidaanko palvelun käyttö sallia kyseisille päätelaitteille ja millä tavoin
- Lähtökohtaisesti käyttäjien omia päätelaitteita ei saa käyttää salassa pidettävien tietojen käsittelyyn. Vain suojaustason IV rajattu käyttö voidaan sallia riskiarvioin jälkeen, kun huomioidaan vähintäänkin tässä ohjeessa kuvatut uhat ja niiden pienentämiseksi tehdyt rajaukset ja muut toimet.
- Suojaustasojen I, II tai III –tietojen käsittely käyttäjien omilla päätelaiteilla on kielletty.

Pääsy organisaation palveluihin voidaan mahdollistaa esimerkiksi eriyttämällä tietyt päätelaitteet tai palvelun osat muusta tietojenkäsittely-ympäristöstä, virtualisoimalla tai pääteistunnoilla. Mikäli päätelaitteiden käyttöä ei kontrolloida riittävällä tavalla, riskeinä ovat ainakin:

- salassa pidettävää tietoa päätyy organisaation ulkopuolisille laitteille, jotka eivät välttämättä vastaa tietojen käsittelyn vaatimuksia. Tietojen oikeudeton käyttö on mahdollista eikä käyttöä välttämättä havaita.

- salassa pidettävää tietoa päätyy käyttäjän omien laitteiden kautta kaupallisten yritysten palveluihin ja tietojärjestelmiin, jotka eivät välttämättä vastaa tietojen käsittelyn vaatimuksia. Oikeudeton käyttö on mahdollista eikä käyttöä välttämättä havaita. Palveluita, joihin tietoa voi päätyä, ovat esimerkiksi hallinta-, valvonta- ja tukipalvelut sekä mahdolliset laite- tai ohjelmistovalmistajien pilvi-, tunnistus-, tallennus- ja sosiaalisen median palvelut.
- henkilötietoja päätyy EU-alueen ulkopuolelle, jossa lait saattavat mahdollistaa henkilötietojen laajemman hyväksikäytön. Tietosuoja ja tietoturvallisuus vaarantuvat.
- päätelaitteiden kautta saattaa tarttua erilaisia haittaohjelmia organisaation sisäverkossa oleviin päätelaitteisiin tai tietojärjestelmiin
- salassa pidettäviä tietoja saattaa vuotaa ulkopuolisille ja oikeudeton käyttö mahdollistuu eikä sitä välttämättä havainta
- tietojen käsittelystä ei jää lokia tai muuta jälkeä, jolloin korkeampien suojaustasojen tietojen käsittelyn vaatimuksia ei voida täyttää. Esimerkiksi rikollisen tai muutoin haitallisen toiminnan jälkiselvittely voi hankaloitua merkittävästi tai olla mahdotonta.

Monissa päätelaitteissa voidaan eristää haluttuja sovelluksia muusta ympäristöstä esimerkiksi erilaisilla virtualisointiratkaisuilla. Valtionhallinnon organisaation tulee päättää, mitkä ovat sellaisia olennaisia palveluja (jos sellaisia on), jotka tulee eriyttää päätelaitteessa muusta käsittely-ympäristöstä. Näin voidaan esimerkiksi toteuttaa sellainen rajattu käsittely-ympäristö, jossa vain yksittäisen palvelun tiedot on salattu. Jos päätelaite katoaa, niin voidaan poistaa tämän yksittäisen palvelun tiedot. Haittapuolena tällaisissa ratkaisuissa on se, että ne yleensä hankaloittavat päätelaitteen käyttöä jonkin verran.

Virtualisoidun päätelaitteella suoritettavan käyttöympäristön[3] (kuten VMware workstation, Virtualbox tai muu vastaava) suunnittelussa ja käytössä tulee ottaa huomioon myös virtualisoidun ympäristön hallinta sekä salassa pidettävien tietoaineistojen käsittelyyn ja toimintaan liittyvät vaatimukset. Lisäksi tulee ottaa huomioon, että suoritettavassa virtuaaliympäristössä ei voida käsitellä korkeamman suojaustason tietoa kuin minkä käsittelyyn päätelaitealusta on hyväksytty.

Sovellusten eriyttämisen lisäksi palveluita voidaan tarjota myös pääteistuntojen kautta, jolloin päätelaitteille ei tallennu mitään tietoja, eikä haittaohjelmilla ei ole niin helppoa murtautua käytettävään sovellukseen tai salassa pidettäviin

[3] Tässä tarkoitetaan tyypin 2 hypervisor-ratkaisuja

tietoihin. Tällaisia ratkaisuja voidaan käyttää esimerkiksi silloin, kun itse päätelaitetta ei saada kaikilta osin kovennettua halutulle tietoturvatasolle. Tulee kuitenkin arvioida se, täyttyykö haluttu tietoturvataso pääteistunnon suojauksen kautta. Pääteistunnoissakin riskeinä ovat mm.

- näppäinpainallusten tallentaminen (ns. keyloggerit)
- järjestelmään mahdollisesti tallentuvien pääteistunnon mahdollistavien käyttäjätunnusten ja salasanojen paljastuminen
- mikrofonin tai kameran kaappaus, jolloin murtautuja voi saada tietoonsa käyttäjän fyysisessä ympäristössä tapahtuvia asioita, kuten salassa pidettäviä tietoja keskusteluista
- kuvankaappauksia näytöstä, jolloin murtautuja voi saada tietoonsa pääteistunnon avulla järjestelmässä käsiteltäviä salassa pidettäviä tietoja.

Monia päätelaitteita voidaan käyttää tunnistautumiseen tai maksamiseen erilaisissa verkko- tai muissa palveluissa. Loppukäyttäjien toimia ne saattavat helpottaa merkittävästi, mutta ne saattavat tuoda mukanaan vastuukysymyksiä, esimerkiksi jos päätelaitteita vaihdetaan henkilöltä toiselle tai ulkopuolinen (tai haittaohjelma) pääsee käsiksi maksamisessa käytettäviin tietoihin. Nämä asiat tulee huomioida organisaation toiminnassa, erityisesti päätelaitepolitiikassa ja käytön ohjeistuksessa, joita on kuvattu tarkemmin luvussa 8.2.

Monia päätelaitteilla käytettäviä palveluita ja järjestelmiä voidaan hankkia myös pilvipalveluna, tai käyttäjät saattavat omatoimisesti haluta käyttää erilaisia pilvipalveluita. Lähtökohtaisesti pilvipalveluiden käyttö ei ole sallittua salassa pidettävien tietojen käsittelyyn. Organisaation tulee päättää, mitä pilvipalveluita voidaan käyttää rajatusti työtehtäviin ja miten niissä käsiteltävien tietojen turvallisuudesta huolehditaan. Lisäksi organisaation tulee tarvittaessa tarkentaa tietoaineistojen käsittelyohjeistusta siten, että loppukäyttäjät tietävät mitä pilvi-, tunnistus-, tallennus- tai sosiaalisen median palveluita saa käyttää ja mihin tarkoitukseen. Päätelaitteita hyväksyttäessä tulee ottaa huomioon, että monissa laitteissa on jo valmiiksi asennettuna erilaisia pilvipalveluja (hallinta-, valvonta- ja tukipalvelut sekä mahdolliset laite- ja ohjelmistovalmistajien pilvi-, tunnistus-, tallennus- ja sosiaalisen median palvelut). Lisäksi saatetaan tarvita tunnukset päätelaitteen tai ohjelmiston valmistajan palveluun, sekä mahdollisesti maksuvalmius (esim. luottokorttimaksamisen tiedot). Monesti nämä valmiiksi asennetut palvelut ovat kiinteä osa päätelaitteen käyttökokemusta. Ne saattavat myös oletuksena synkronoida jotkut tai kaikki päätelaitteelle tallentuvat tiedot. Organisaation tulee päättää, sallitaanko pilvipalveluiden käyttö ja

jos sallitaan, niin miten niiden käyttöä työtehtävissä ja palveluissa tulisi muutoin rajoittaa, tai muutoin suojata salassa pidettäviä tietoja tai turvata sisäverkon palveluita ja tietojärjestelmiä. Mikäli riskiarviointia pilvipalvelujen käytöstä ei voida tehdä, tulee pilvipalvelujen käyttö kieltää.

5.2 Tietojen ja sovellusten käyttö

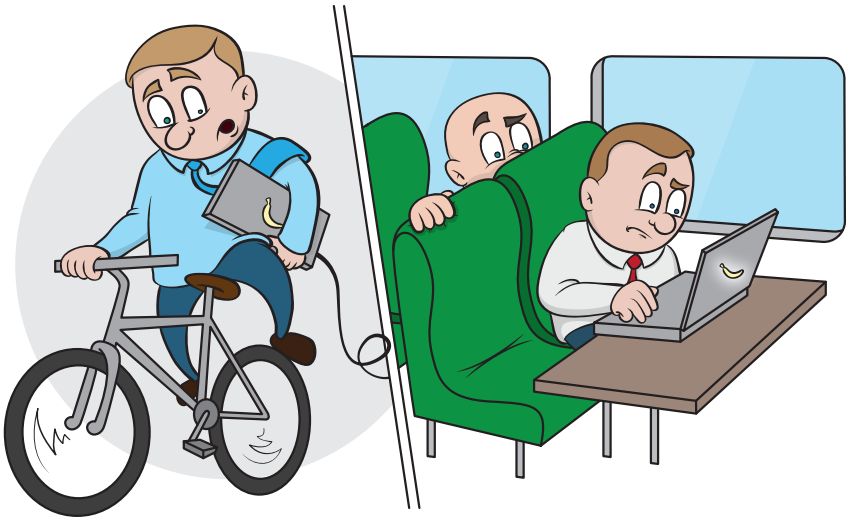
Pääperiaatteena erilaisten tietojen ja sovellusten käytölle on edellä kuvattu malli siitä, että päätelaitteella käsitellään vain hyväksytyn suojaustason käsittelykyvyn tietojärjestelmissä olevia tietoja (ja alemman suojaustason käsittelykyvyn järjestelmissä olevia tietoja yhdyskäytäväratkaisujen avulla). Monia päätelaitteita, erityisesti tablettilaitteita ja älypuhelimia, ei kuitenkaan saada kovennettua kustannustehokkaasti halutulle käsittelykyvylle tai se vaatisi useita eri tukipalveluita niiden toteuttamiseksi riittävän turvallisesti. Tällöin voidaan toteuttaa korvaavia menettelyjä yksittäisten tai korkeintaan muutamien vaatimusten osalta. Korvaava menettely tarkoittaa, että varsinaisen vaatimuksen kontrollin tilalle rakennetaan jokin toinen kontrolli, joka riittävällä tavalla toteuttaa alkuperäisen kontrollin tavoitteen ja jonka käytön riskit pienennetään hyväksyttävälle tasolle. Jos päätelaitteelle ei esimerkiksi pystytä asettamaan organisaation salasanapolitiikan mukaista huonolaatuisten salasanojen estoa, voidaan hyväksyä heikommat salasanavaatimukset ja toteuttaa laitteen tyhjentäminen, mikäli salasana syötetään väärin useita kertoja. Tarkempi ohjeistus korvaavien menettelyjen käytölle löytyy VAHTI 2/2010-ohjeen liitteestä 6.

Riskiarviointia tehtäessä tulee ottaa huomioon edellisessä luvussa kuvatut päätökset. Mitä paremmin tietoturvallisuus on huomioitu päätöksissä ja päätelaitteen käyttötapauksissa, sitä paremmin voidaan hyväksyä poikkeavia menettelyitä. Mikäli organisaatio rajoittaa teknisesti ohjelmien asentamista tai suorittamista päätelaitteella, sitä pienempi on haittaohjelmariski koska niiden hyökkäyspinta-ala kaventuu.

Mikäli organisaatio päätyy päätelaitteiden käytössä joissakin käyttötapauksissa yllä kuvattuihin korvaaviin menettelyihin ja alkaa käyttää näillä päätelaitteilla jonkin toisen valtionhallinnon toimijan tarjoamia palveluita, tulee organisaation varmistua siitä, että korvaava menettely ei vaaranna niiden tietoja ja järjestelmiä. Korvaavista menettelyistä tulee kertoa palvelua tarjoavalle organisaatiolle silloin kun palveluiden käyttöönottoa suunnitellaan.

Päätelaitteen turva-asetuksissa ja kovennuksessa sekä palveluiden ja sovellusten käytössä voidaan erottaa käyttö organisaation sisäverkossa (organisaation sisäverkko tai valtionhallinnon sisäverkot) ja ei-luotetuissa verkoissa (ml. Internet). Mikäli päätelaitteiden suojaamisessa turvaudutaan korvaaviin menettelyihin, tulee käyttötapausten käsittely-ympäristö ottaa huomioon riskiarvioinnissa.

Mikäli päätelaitteella käytetään organisaation ulkopuolisia palveluita, tulee niiden käyttöehdot lukea tarkasti. Niissä saatetaan rajoittaa palvelun tarjoajan vastuuta tietoturvallisuudesta esimerkiksi tiedon luottamuksellisuuden, eheyden, saatavuuden, varmistuksien tai mahdollisesti palvelun kautta tarttuneiden haittaohjelmien osalta. Käyttöehdoissa voidaan myös vaatia käyttäjiltä joitakin toimia tietoturvallisuudesta huolehtimiseen liittyen tai estää käyttö laiminlyönnistä.



Etätyössä ja liikkuvassa työssä voidaan käyttää samoja suojaustason IV tietoja ja sovelluksia kuin organisaation sisäverkossa ja tiloissa työskenneltäessä. Seuraavat seikat tulee kuitenkin ottaa huomioon:

- Päätelaitteen säilytys; kun päätelaitetta ei valvota, sen tulee olla lukittu (esim. suojakoodi), sitä tulee säilyttää fyysisesti suojatussa tilassa, esimerkiksi lukitussa kaapissa, ja sille tallennetut salassa pidettävät tiedot tai kaikki massamuistit kokonaisuudessaan ovat salattuja.
- Yhteydet käytettäviin palveluihin; tietoliikenneyhteys tulee salata kokonaan erilaisilla VPN-ratkaisuilla tai sovelluskohtaisesti esimerkiksi TLS-salauksella.
- Fyysinen turvallisuus; käytettäessä päätelaitetta julkisissa tiloissa tulee varmistua siitä, että kukaan ei näe laitteen näytöltä siinä käsiteltävää salassa pidettävää tietoa, tai kuule jos niistä olisi tarpeen puhua. Loppukäyttäjille voidaan hankkia näyttösuojia, joilla näyttöjen näkyvyyttä rajataan, sekä ohjeistaa käyttäjiä huomioimaan sekä salakatselu että salakuuntelu.

6 Päätelaitteiden hallinta

Päätelaitteiden hallinnassa on tärkeää, että organisaatiolla on tiedossa millä päätelaitteilla sen palveluita ja tietoja käytetään, ja että organisaatio on määritellyt miten erilaiset päätelaitteet tulee koventaa sekä miten niitä hallitaan ennen kuin niillä voidaan päästä käsiksi salassa pidettäviin tietoihin. Teknisessä tietoturvallisuudessa kovennusten lisäksi on olennaista seurata valmistajien julkaisemia tietoturvapäivityksiä ja asentaa ne hallitusti mahdollisimman nopeasti, sekä seurata julkaistuja haavoittuvuuksia ja tarvittaessa muuttaa turva-asetuksia tai rajoittaa päätelaitteiden tai sovellusten käyttöä.

Teknisten tietoturvatoimenpiteiden lisäksi on tärkeää ohjeistaa loppukäyttäjiä ja pääkäyttäjiä päätelaitteiden käytöstä ja turvallisuudesta. Luvussa 8 on kuvattu tarkemmin suositukset päätelaitepolitiikan ja käyttöohjeistuksen sisällöksi.

Pääkäyttäjän ohjeistuksessa on hyvä käsitellä ainakin seuraavia asioita, tarvittaessa laajemmin jos kyseessä on esimerkiksi ulkoisen palvelutoimittajan henkilö:

- Pääkäyttäjän vastuut, oikeudet ja mahdolliset seuraamukset
- Mitä palveluita ja tietoja päätelaitteella (tai sen kautta hallittavilla päätelaitteilla) saa käsitellä
  - pääkäyttäjäoikeuksin
  - loppukäyttäjäoikeuksin
- Ylätason kuvaus siitä, miten päätelaitteen turvallisuudesta on huolehdittu ja miten käyttöä valvotaan
- Käyttö oman organisaation sisäverkon tai tilojen ulkopuolella
  - pääkäyttäjäoikeuksin
  - loppukäyttäjäoikeuksin

- Käyttö muun valtionhallinnon organisaation tiloissa
  - pääkäyttäjäoikeuksin
  - loppukäyttäjäoikeuksin
- Päätelaitteiden siirtäminen ja säilytys
- Kenelle ja miten ilmoitetaan tietoturvapoikkeamatapauksista tai niiden epäilystä.

6.1 Päätelaitteiden koventaminen ja hallintaohjelmistot

Ennen kuin päätelaitteella voidaan käsitellä salassa pidettävää tietoa, tulee varmistua siitä, että se täyttää halutun suojaustason tietojen mukaisen käsittelyn vaatimukset. Tämä voidaan tehdä esimerkiksi seuraavasti:

- Asettamalla ja lukitsemalla päätelaitteen turva-asetukset paikallisesti halutuiksi
- Ottamalla päätelaite keskitettyyn hallintaan, jonka kautta laitteet voidaan koventaa sekä käyttöä valvoa (YT-menettelyn mukaisesti ja tietosuoja varmistaen).

On olennaista varmistaa, että loppukäyttäjät tai haittaohjelmat eivät pääse muuttamaan päätelaitteen turva-asetuksia.

Mikäli päätelaitteita hallitaan keskitetysti, tulee varmistua, että myös käytetyt hallintapalvelimet ja hallintaan käytettävät päätelaitteet ovat riittävän turvallisia, halutun suojaustason käsittelykyvyn mukaisesti hallittuja ja teknisesti kovennettuja. Nämä seikat tulee varmistaa riippumatta siitä, ovatko ne organisaation omassa tai esimerkiksi palvelutoimittajan hallinnassa.

Tietoturvaominaisuuksia voidaan toteuttaa päätelaitteiden omilla tai päätelaitevalmistajan muilla ohjelmistoilla, niiden ominaisuuksilla tai erillisillä turva-ohjelmistoilla.

Päätelaitteiden kovennuksessa tulee toteuttaa suojaustason IV käsittelemiseksi ainakin:

- Estää niiden päätelaitteiden palveluiden/toiminnallisuuksien näkyminen verkkoon, jotka eivät ole erikseen hyväksytty
- Salassa pidettävien tietojen tai kaikkien massamuistien salaus
- Haittaohjelmien torjunta
- Päätelaitteen hallinnan yksilöivät tunnisteet (kuten päätelaiteen laitetili/-id).

Päätelaitteiden kovennuksessa pitää edellisten lisäksi toteuttaa suojaustason III käsittelemiseksi ainakin:

- Rajata Internetin käyttö sisäverkosta käsin vain yhdyskäytävän (esim. välityspalvelin) kautta
- Rajata Internetin käyttö organisaation verkon ulkopuolelta tapahtuvaksi vain VPN-yhteyden kautta
- Estää muiden kuin hyväksyttyjen ohjelmien asentaminen ja suorittaminen (whitelist).
- Estää päätelaitteen ja sen sovellusten turva-asetuksien muutokset.

Päätelaitteiden kovennuksessa pitää edellisten lisäksi toteuttaa suojaustason II käsittelemiseksi verkotetulla päätelaitteella ainakin:

- Etäyhteyksien automaattinen aikakatkaisu
- Huomioida erityiset tila-vaatimukset mukaan lukien Tempest-suojaus (sähkömagneettisesta hajasäteilystä syntyvän uhan) tilalle tai päätelaitteille (oheislaitteineen)
- Huomioida suojaustason II tietojen käsittelyn lokitusvaatimukset
- Huomioida kyseisen verkon, tietojärjestelmien ja palveluiden muut vaatimukset.

Päätelaitteiden kovennuksessa pitää edellisten lisäksi toteuttaa suojaustason II käsittelemiseksi verkottomalla päätelaitteella ainakin:

- Estää verkkoyhteyksien käyttö
- Huomioida erityiset tila-vaatimukset mukaan lukien Tempest-suojaus (sähkömagneettisesta hajasäteilystä syntyvän uhan) -suojaus tilalle tai päätelaitteille (oheislaitteineen)
- Hallita paikallisesti käyttöoikeudet ja –valtuudet sekä dokumentoita ja varmistaa ne kyseisen ympäristön ulkopuolelle
- Huomioida suojaustason II tietojen käsittelyn lokitusvaatimukset
- Testata tarvittavat päivitykset säännöllisesti ja suunnitellusti
- Asentaa tarvittavat päivitykset paikallisesti säännöllisesti ja suunnitellusti
- Hallita paikallisesti suojaustason II tietojen säännöllinen varmuuskopiointi, suojakopiointi ja palauttaminen sekä näiden testaus suunnitelmien mukaisesti.

Päätelaitteen tietoturvallisuuden hallinnassa ja päätelaitteen kovennuksessa voidaan toteuttaa myös:

- Virtualisoitu tai ns. hiekkalaatikko-ympäristö, jossa salassa pidettävä tieto rajoitetaan virtuaalisen 'kuplan' sisään
- Paikallisen päätelaitteen tietojen varmuuskopiointi, mikäli käyttäjien sallitaan tallentaa tietoja paikallisesti
- Päätelaitteen tyhjennys katoamis- ja varkaustapauksissa etäyhteydellä, esim. mobiililaitteiden hallintaohjelmiston avulla
- Päätelaitteen tarkastus ennen verkkoon pääsyä. Tarkastuksessa voidaan varmistaa esimerkiksi laitekohtaisen palomuurin tai haittaohjelmien torjuntaohjelmiston päällä olo, päivitysten ajantasaisuus sekä muita tietoturvallisuuteen vaikuttavia asioita. Mikäli edellytykset eivät täyty, voidaan päätelaite päästää verkkosegmenttiin, josta ei ole pääsyä organisaation salassa pidettäviin tietoihin.

Katso myös KATAKRI, erityisesti I-osa-alue (tietoturvallisuus).

Yllä listattujen kovennustoimien lisäksi on suositeltavaa, että organisaatio tai valtionhallinnon palvelukeskus määrittelee tarkemmalla tasolla ne tekniset kovennustoimenpiteet, joita eri tasoilla sekä mahdollisesti eri ympäristöissä ja käyttötapauksissa käytetään. Tarkempia kovennusohjeita kaipaava organisaatio voi arvioiden käydä läpi ja soveltuvin osin hyödyntää kansainvälisesti tunnettuja kovennusohjeita, joita julkaisevat esimerkiksi NIST (National Institute of Standards and Technology) ja CIS (Center for Internet Security). Myös tuotteiden valmistajat julkaisevat tarkempia ohjeita ja suosituksia tuotteiden turvalliseen käyttöön (esimerkiksi security guide ja hardening-dokumentit). Kovennuksessa tulee erityisesti ottaa huomioon Teknisen ICT-ympäristön tietoturvataso-ohjeen (VAHTI 3/2012) päivitetty liite 3, tietojärjestelmien tietoturvatasovaatimukset, joka on tämän ohjeen liitteenä 1. Etäyhteyksien osalta organisaation tulee varmistaa ja huomioida myös saman ohjeen liite 7, etäkäytön tekniset vaatimukset. Lisätietoja ohjeiden hyödyntämisestä voi tiedustella Valtion IT palvelukeskukselta ja Viestintävirastolta.

Monia päätelaitteita, erityisesti kuluttajakäyttöön suunniteltuja älypuhelimia ja tabletteja sekä niihin liittyviä palveluita ei ole teknisesti helppoa saattaa suojaustason IV käsittelykyvyn edellyttämälle tasolle, mutta saattaa olla mahdollisesta rajoittaa suojaustason IV käsittelyä päätelaitteella tai tietojärjestelmästä käsin. Organisaation tulee riskiarvioinnin avulla päättää, voidaanko niillä rajatusti käsitellä tai tallentaa salassa pidettävää suojaustason IV tietoa.

Korvaavat menettelyt tulee dokumentoida ja hyväksyttää sekä selvittää säännöllisin väliajoin, mahdollistaako päätelaitteiden nopea kehittyminen uusia suojaavia menetelmiä, jotka eivät jossakin vanhemmassa tuotteessa tai versiossa ole olleet mahdollisia.

Esimerkkinä hallitusta tavasta ottaa käyttöön sähköposti ja kalenteri päätelaitteella, jossa ei pystytä kaikkia suojaustason IV rajatun käsittelyn vaatimuksia toteuttamaan, on seuraava:

- Selvitetään, miten tieto tulee päätelaitteelle, jolloin havaitaan seuraavat asiat:
  - sähköpostit ja kalenterimerkinnät sisältävät vain poikkeustapauksissa salassa pidettäviä suojaustason IV tietoja
  - salassa pidettävät suojaustason IV tiedot ovat yleensä liitteessä, eivät sähköpostin tai kalenterimerkinnän varsinaisessa tekstissä
- Selvitetään, miten päätelaitetta ja niissä tarvittuja palveluja voidaan koventaa, jolloin havaitaan seuraavat asiat:
  - päätelaitteessa voidaan määritellä, että sähköposteja säilytetään siinä vain lyhyen aikaa (esim. 7 päivää tai vähemmän) ja kalenterimerkintöjenkin näkymiseen voidaan asettaa ajalliset rajoitteet
  - päätelaitteessa voidaan määritellä, että liitteiden nouto tapahtuu vain erikseen pyydettäessä, ja se tulee tehdä sähköposti- ja kalenterimerkintäkohtaisesti tai se voidaan estää palvelussa tai palvelimelta
- Otetaan käyttöön edellä mainitut asetukset
- Lisätään päätelaitteen käyttöohjeistukseen tietoturvalliset käyttötapauksien menettelytavat ja muut käytössä huomioitavat asiat, sekä erityisesti maininnat:
  - mikäli käyttäjä epäilee liitteen sisältävän salassa pidettävää tietoa, tulee se avata vain vaatimusten mukaisella päätelaitteella
  - ohjeistaa ilmoitusmenettelyt ja muut mahdolliset toimenpiteet katoamis- ja varkaustapauksissa.
- Toteutetaan korvaava menettely. Dokumentoidaan korvattava vaatimus, järjestelystä aiheutunut riski ja tehdyt toimenpiteet riskin pienentämiseksi hyväksyttävälle tasolle sekä seurataan säännöllisesti, onko mahdollista teknisesti koventaa päätelaite tai rajata palvelu paremmin, jolloin korvaavaa menettelyä ei enää tarvita.

6.2 Päätelaitteiden omistajuus ja yhteiskäyttö

On suositeltavaa, että organisaatio lähtökohtaisesti hankkii työvälineet salassa pidettävien tietojen käsittelyyn siten, että kullakin käyttäjällä on oma päätelaite. Nykyään on jonkin verran yleistynyt malli, jossa käyttäjä käyttää organisaation palveluita itse hankkimallaan päätelaitteella (BYOD, Bring Your Own Device). BYOD-laitteiden työkäyttö salassa pidettävien tietojen käsittelyssä on lähtökohtaisesti kielletty, ellei niitä ole erikseen organisaation tai valtion palvelukeskuksessa riskiarvioinnin kautta hyväksytty tiettyyn käyttötapaukseen ja rajattuun käyttöön. Päätelaitteella voi olla myös joissakin rajatuissa tapauksissa tai rajatuissa palveluissa useita käyttäjiä, esimerkiksi organisaation yhteiskäyttöiset päätelaitteet, kotikonekäyttö tai Internet-kahvilakäyttö.

Kuten aiemmissa luvuissa on todettu, on olennaista, että organisaatio sallii salassa pidettävien tietojen käsittelyn vain kyseisessä käyttötapauksessa hyväksytyillä ja dokumentoiduilla päätelaitteilla. Myös käyttäjän omien laitteiden tulee olla organisaation hyväksymiä ja tietoturvallisuuden perustasolle kovennettuja, jos niillä halutaan sallia rajattua suojaustason IV tietojen käsittelyä.

Käyttäjien omien laitteiden käytön riskiarvioinnissa tulee käsitellä ainakin seuraavia asioita:

- Mitä päätelaitteita käyttäjillä on, miten hyvin ne voidaan koventaa ja ottaa keskitettyyn hallintaan
- Mitä palveluita käyttäjien omille päätelaitteille sallitaan
- Mitä salassa pidettäviä tietoja laitteilla käsiteltäisiin ja mihin suojaustasoon tiedot kuuluvat
- Miten käyttöohjeistuksia on päivitettävä ja mikä on arvio käyttäjien sitoutumisesta niiden noudattamiseen
- Voidaanko käyttäjät sitouttaa siihen, että organisaatio hallitsee heidän omia laitteitaan
- Voidaanko käyttäjät sitouttaa siihen, että organisaatio voi tarvittaessa ottaa haltuun heidän omat laitteensa väärinkäytöstilanteiden tutkimiseksi tai etätyhjentää ne
- Miten paljon käyttäjien omien päätelaitteiden hyväksyminen helpottaa organisaation toimintaa
- Miten paljon organisaatio tukee erilaisia päätelaitetyyppejä
- Miten kustannukset mahdollisesti jaetaan käyttäjän ja organisaation kesken

- Mitkä asiat on hyväksytettävä työntekijällä, esim. YT-menettelyllä tai luovutussopimuksella.

Sen lisäksi, että palveluita käytetään päätelaitteilta, jotka eivät ole organisaation hankkimia tai hallinnoimia, voidaan palveluita käyttää päätelaitteelta, jonka kaikki käyttäjät eivät ole organisaation sisäisiä. Esimerkiksi organisaatio saattaa hyväksyä tiettyjen rajattujen palveluiden käytön kotikoneilta, joita käyttävät myös muut perheenjäsenet. Tällöin riskejä tulee pohtia samantyyppisistä näkökulmista kuin käyttäjän omien päätelaitteiden tapauksessa.

Erityishuomiota jaetuissa laitteissa tulee kiinnittää eri käyttäjien tietojen erottamiseen toisistaan; voidaanko päätelaitteessa esim. toteuttaa useita käyttäjätilejä, profiileja tai istuntoja, jotka eivät mitenkään pääse käsiksi toistensa tietoihin. Tämä voidaan toteuttaa esim.

- Salaamalla kiintolevy ja siirrettävät apumuistit tai käyttäjähakemistot sekä vaatimalla, että organisaation tietoja käsitellään vain yhdellä käyttäjätunnuksella, jota käyttää vain nimetty henkilö
- Käyttämällä rajattuja palveluita pääteistuntoratkaisun kautta, esim. verkkoprofiilin tai pääteistunnon, jossa on estetty tietojen tallentaminen kyseisestä ympäristöstä käytettävälle päätelaitteelle.

6.3 Laitteen ja käyttäjän tunnistaminen

Tulee erottaa toisistaan käyttäjän tunnistaminen laitteelle ja käyttäjän tai laitteen tunnistaminen käytettävälle palvelulle. Jo laitteelle tunnistautuminen voi antaa pääsyn niihin organisaation tietoihin, jotka on tallennettu päätelaitteelle, tai mahdollisen kertakirjautumisen kautta organisaation palveluihin, järjestelmiin ja tietoihin.

Suojaustason IV käsittelykykyisissä järjestelmissä käyttäjä voidaan tunnistaa salasanalla tai vastaavalla menetelmällä. Päätelaitteita ei ole täysin välttämätöntä tunnistaa rajatuissa järjestelmissä ja palveluissa, joissa rajataan tietojen käsittelyä ja käsitellään korkeintaan suojaustason IV tietoja. Päätelaitteissa voidaan käyttää salasanan sijaan myös erilaisia kuvioihin perustuvia tunnistamismenetelmiä, mikäli organisaatio tai valtionhallinnon palvelukeskus on ensin varmistanut, että kuvion käyttö on yhtä turvallista kuin salasanan käyttö.

Käytettäessä suojaustason III järjestelmiä etäyhteyksillä, tulee käyttää vahvaa tunnistamista. Lisäksi päätelaite tulee tunnistaa käyttämällä organisaation hyväksymää varmennetta tai vastaavaa menettelyä. Lisäksi tulee ottaa huomioon suojaustason muut vaatimukset, tietojen käsittelyn vaatimukset sekä toiminnan asettamat vaatimukset.

7 Päätelaitteiden elinkaari

Tyypillisesti organisaatiossa on käytössä useita erilaisia, eri aikoina valittuja ja hankittuja päätelaitteita. Eri päätelaitteita hyväksyttäessä tulee ottaa huomioon niiden koko elinkaaren aikana tehtävät toimet ja tietoturvallisuuden varmistaminen niissä. Elinkaaren voi jakaa seuraaviin päävaiheisiin:

- Esikartoitus
- Hankinta
- Käyttöönotto
- Käyttö ja ylläpito
- Uudelleenkäyttöönotto
- Käytöstä poisto.

Kaikki eri vaiheissa kuvatut toimenpiteet tai tehtävät eivät välttämättä ole mahdollisia tai mielekkäitä tietyn tyyppiseen, esimerkiksi rajattuun käyttöön tarkoitettujen päätelaitteiden hallinnassa.

7.1 Esikartoitus

Esikartoituksessa tietoturvallisuuden kannalta tärkeimmät tehtävät ovat päätelaitekartoitus sekä päätös tarvittavasta tietoturvatasosta. Siihen vaikuttavat käsiteltävien tietojen suojaustaso, millaiseen ympäristöön tai palveluihin on tarve kytkeytyä ja millaisilla käyttötapauksilla, sekä muut toiminnan ja tietojen käsittelyn vaatimukset. Tarkoituksena on varmistaa, että markkinoilla on saatavilla tuotteita, jotka täyttävät halutut ominaisuudet, käyttötarpeet ja vaatimukset.

7.2 Hankinta

Hankintavaiheessa kilpailutuksen yhteydessä tulee listata ne tietoturvavaatimukset, jotka hankittavan tai vuokrattavan päätelaitteen ja niihin liittyvien palveluiden (esim. hallinta-, valvonta- ja tukipalvelut) tulee toteuttaa, jotta halutun suojaustason tietoa voidaan käsitellä turvallisesti. Tietoturvallisuudessa tulee ottaa huomioon valitun tietoturvatason ja tämän ohjeen vaatimusten ja ohjeistuksen lisäksi lainsäädäntö ja muu regulaatio, sekä muut organisaation toiminnan ja palveluiden kautta tulevat vaatimukset päätelaitteille ja niihin liittyville palveluille.

Päätelaitteiden hallintavälineet (esim. ohjelmistot ja pääkäyttäjän päätelaitteet) ovat tietoturvallisuuden näkökulmasta avainasemassa, ja niiden tuleekin noudattaa vähintään samaa tietoturvatasoa kuin niillä hallittavien päätelaitteiden. Mikäli kaikkia asetettuja vaatimuksia ei pystytä noudattamaan, tulee riskiarvioinnissa ottaa huomioon, että hallintavälineet ovat erityisen tärkeässä roolissa ja varmistua, että niiden osalta ei tehdä tietoturvallisuuden kannalta merkittäviä heikennyksiä. Erityisen tärkeitä ovat niin sanotut hyppykoneet ja keskitetyt järjestelmät, joiden kautta voidaan päästä hallinnoimaan organisaation päätelaitteita ja määrittämään niihin asennettuja ohjelmistoja ja turva-asetuksia.

Mikäli jokin osa päätelaitteiden hallinnasta hankitaan ulkoiselta palveluntuottajalta, tulee hankinnassa varmistua, että päätelaitteisiin ja niiden hallintaan liittyvät tiedot säilyvät oman organisaation omistuksessa, ja että palveluntuottaja käyttää hallintaan vain asiakkaan erikseen hyväksymiä henkilöitä, päätelaitteita, hallintavälineitä, tiloja ja prosesseja palvelua tuottaessaan. Erityisesti hallinnan lokien jäljitettävyyteen, etäkäyttöön ja etätyöhön hallintatyötehtävissä on otettava kantaa, jos hallittavilla päätelaitteilla on pääsy salassa pidettäviin tietoihin tai tietojärjestelmiin. Nykyään esimerkiksi hallintavälineitä voidaan julkaista etäkäyttöisesti käytettäväksi tai käyttää pääkäyttäjän omia välineitä hallintatyöhön, jos käyttöä ei teknisesti ja sopimusteitse estetä sekä toimintaa seurata (mm. lokitietojen kattavuus ja katselmoinnit).

7.3 Käyttöönotto

Käyttöönottoon liittyvien tehtävien lisäksi tässä vaiheessa tulee suunnitella seuraavien vaiheiden tietoturvatehtävien toteuttaminen. Käyttöönottovaiheessa päätelaitteet, niiden ohjelmistot ja lisenssit lisätään rekisteriin tai vastaaviin luetteloihin.

Käyttöönotossa tyypillisesti tehdään levykuva (image) tai jokin muu järjestely, jonka avulla kaikki tarvittavat asennukset ja asetukset tehdään. On tärkeää varmistua järjestelyn eheydestä, jotta siihen ei tule hallitsemattomia muutoksia esimerkiksi haittaohjelmien tekemänä. Levykuvalle tai sen mukaiselle päätelaitteelle on hyvä tehdä myös tietoturva- ja murtotestaus.

Mikäli päätelaitteen massamuistit salataan, tulee järjestely olla sellainen, että salaus tehdään ennen kuin päätelaitteelle syötetään salassa pidettäviä tietoja. Lisäksi salauksen tulee olla sellainen, että se avataan vasta, kun salausavaimen purkava salasana, toimikortti, TPM-siru (Trusted Platform Module) tai vastaava on annettu tai käytössä.

Mikäli ohjelmistojen asennus tapahtuu ohjelmistopaketointia käyttäen, tulee viimeistään käyttöönottovaiheessa käydä läpi paketointiin liittyvät tekniset yksityiskohdat, kuten pakettien allekirjoitukset, jakelun prosessi ja varmistua, että siinä käytettävät järjestelmät ja menetelmät täyttävät halutun tietoturvatason ja muut toiminnan vaatimukset.

7.4 Käyttö ja ylläpito

Käytön yhteydessä tulee usein tarvetta tehdä erilaisia ylläpitotoimenpiteitä tai lisähankintoja laitteisiin, lisälaitteisiin ja ohjelmistoihin. Mikäli huollon tai ylläpidon hoitaa palvelutoimittaja tai muu ulkopuolinen taho, tulee huolehtia siitä, että päätelaitteella ei ole salassa pidettävää tietoa salaamattomana. Vaihtoehtoisesti tiedon salassapito voidaan turvata esimerkiksi turvallisuussopimuksilla ja taustatarkastuksilla.

Päätelaitteiden muutoshallintaprosessissa tulee varmistaa laitteistojen, ohjelmistoasennusten ja -poistojen päivittäminen rekisteriin. Lisäksi tulee ottaa huomioon muutosten testaaminen sekä niiden mukanaan tuomat riskit.

Käytön aikana päivityksiä tulee ainakin päätelaitteen käyttöjärjestelmään ja sovelluksiin sekä niiden turva-asetuksiin. Mahdollisesti myös muihin osa-alueisiin, kuten laitteisiin, lisälaitteisiin, laitteisto-ohjelmistoihin (firmware) ja ajureihin tulee muutoksia. Organisaation tulee varmistaa, että kaikki tietoturvallisuuden kannalta olennaiset päivitykset (ml. käyttöjärjestelmä, sovellukset, laitteisto-ohjelmisto ja ajurit) asennetaan. Joko käyttäjät itse tai ylläpitohenkilöt voivat tehdä asennuksia. Organisaation tulee seurata, että ainakin olennaiset päivitykset on tehty riittävän nopeasti niiden julkaisun jälkeen. Mikäli päivityksiä ei pystytä asentamaan, tulee riskiarvioinnin kautta toteuttaa kompensoivia kontrolleja esimerkiksi verkkoteknisin keinoin tai turva-asetuksin.

Mikäli päätelaite katoaa ja se saadaan takaisin, tulee sen käyttöön palauttamisesta tehdä riskiarvio. On mahdollista, että päätelaitteelle on asennettu ylimääräinen laitekomponentti, massamuisti, haitta-, vakoilu- tai takaporttiohjelma, jonka avulla hyökkääjä pääsee käsiksi laitteeseen ja mahdollisesti sitä kautta järjestelmiin, kun se kytketään takaisin verkkoon. Katoamisen jälkeen takaisin saatujen päätelaitteiden kohdalla vaihtoehtoina ovat käytön jatkaminen, uudelleenkäyttöönotto tai käytöstä poisto.

7.5 Uudelleenkäyttöönotto

Päätelaitteen elinkaaren aikana voi tulla eteen tilanteita, joissa laitteelle on tarpeen tehdä käyttöönotto uudelleen. Voi olla esimerkiksi tarve siirtää päätelaite toiselle käyttäjälle tai puhdistaa se mahdollisista haittaohjelmista. Mikäli päätelaitteen kaikkia massamuisteja ei ole salattu, tulee ne tyhjentää kuten käytöstä poiston yhteydessä. Mikäli massamuistit ovat salattuja, ei toimenpide ole kaikissa tapauksissa välttämätön. Tämän jälkeen päätelaitteelle tehdään samat toimenpiteet kuin käyttöönoton yhteydessä. Mikäli tietojen tallennus päätelaitteelle on sallittu, tulee muistaa niiden varmuuskopiointi ennen tyhjennystä.

Mikäli päätelaite otetaan uudelleen käyttöön haittaohjelmatartunnan vuoksi, on syytä selvittää sen toimintatapa. Mikäli haittaohjelma on niin kehittynyt, että se saastuttaa muitakin osia kuin kiintolevyn tavallisen tallennustilan, tulee tehdä riskiarvio ja harkita tuleeko laite poistaa kokonaan käytöstä. Haittaohjelma voi olla tarttunut esimerkiksi BIOS- tai laitteisto-ohjelmistoon (firmware).

7.6 Käytöstä poisto

Käytöstä poiston yhteydessä tulee varmistua, että päätelaitteella olevat toiminnan kannalta olennaiset tiedot on tallennettu siten, että ne ovat käytettävissä myös poiston jälkeen.

Tulee varmistua myös siitä, että salassa pidettävät tiedot on poistettu päätelaitteelta ennen kuin se toimitetaan organisaation ulkopuolelle. Viestintäviraston sivuilta on saatavilla ohje kiintolevyn ylikirjoitukselle (https://www.viestintavirasto.fi/attachments/Ylikirjoitusohje.pdf). Ylikirjoituksessa on sallittua käyttää myös muita kuin sertifioituja ohjelmia. Myös puhelimille ja tableteille

on saatavilla ohjelmistoja, joilla ne voidaan tyhjentää. Mikäli ylikirjoittamista ei jostain syystä voida tehdä, tulee suojaustason III tietoja sisältävät massamuistit tuhota fyysisesti. Suojaustason II ja I tietoja sisältävät massamuistit tulee aina tuhota fyysisesti. On huomioitava, että tehdasasetusten palauttaminen ei ole sama asia kuin tietojen ylikirjoitus. Ylikirjoitus-, tyhjennys- tai käytöstä poiston prosessin toimivuus tulee testata huolellisesti. Siinä tulee ottaa huomioon, ettei ylikirjoitus tai tyhjennys välttämättä tuhoa tietoja riittävällä varmuudella kaikille suojaustasoille sekä se, että SSD- ja yhdistelmälevyjen (SSD-massamuisti, Solid-state Drive) ylikirjoitusta ei tällä hetkellä pidetä riittävän turvallisena, joten toistaiseksi suositellaan näiden levyjen fyysistä tuhoamista.

8 Toimeenpano ja tarkempi ohjeistaminen

Tähän lukuun on koottu asioita, jotka tulee huomioida tämän ohjeen toimeenpanossa, päätelaitteiden käytön riskien arvioimisessa sekä päätelaitepolitiikan ja käyttöohjeistuksen päivittämisessä. Osa asioista on kertausta, osa on esitetty esimerkkien tai tarkistuslistojen muodossa.

8.1 Tietoturvatasojen toteutus päätelaitteiden osalta

Mikäli päätelaitteella käsitellään salassa pidettäviä tietoja, tulee päätelaitteita hallita ja niillä salassa pidettäviä tietoja käsitellä vaatimusten mukaisesti. Teknisen ICT-ympäristön tietoturvataso-ohjeen (VAHTI 3/2012) liite 3, tietojärjestelmien tietoturvatasovaatimukset, on päivitettynä tämän ohjeen liitteessä 1. Siinä on listattu vaatimukset tietojärjestelmien tietoturvallisuuden hallinnalle mukaan lukien luvun 2.4 mukaisesti täsmennetyt ja tarkennetut vaatimukset päätelaitteille.

Vaatimusten toteuttamiseksi on yleensä helpointa hallita päätelaitteita keskitetysti, jolloin vaatimustenmukaisuus on helpompi toteuttaa ja varmistaa. Eräillä päätelaitteilla (kuten tabletit ja puhelimet), varsinkin BYOD-laitteilla, keskitetyn hallinnan toteuttaminen saattaa olla haastavampaa. Silloin ylläpidollisia tehtäviä, kuten päivitysten asentaminen, voidaan jättää loppukäyttäjille aiemmin kuvatuin edellytyksin ja sallia vain rajoitetusti suojaustason IV tietojen käsittely. Näillä laitteilla käsiteltävien tietojen määrää tai palvelua on syytä rajoittaa, valvoa toimintaa tarkemmin, kouluttaa käyttäjät hyvin sekä arvioida tästä toimintamallista aiheutuvia riskejä määräajoin. Organisaation ulkopuolisia päätelaitteita, kuten BYOD-laitteita ja yhteistyökumppanien päätelaitteita,

ei saa kytkeä organisaation sisäverkkoon, mikäli organisaatio tai sen päätelaiteympäristön palvelutoimittaja ei hallitse niitä halutun suojaustason käsittelykyvyn, toiminnan ja tietojen käsittelyn vaatimusten mukaisesti. Käytännössä organisaation palveluiden käyttö ulkopuolisilla päätelaitteilla on usein helpointa toteuttaa erilaisilla pääteistuntoratkaisuilla tai sallia pääsy vain hyvin rajattuihin palveluihin.

8.2 Päätelaitepolitiikka, päätelaitekäytön ohjeistus ja vaatimukset

Päätelaitteisiin liittyvä tietoturva-ohjeistus voidaan toteuttaa erillisenä, mutta suositeltavampaa on, että se sisällytetään loppukäyttäjien ja pääkäyttäjien yleiseen päätelaitteiden käyttöohjeistukseen. Organisaatio voi halutessaan laatia päätelaitepolitiikan ohjeistuksen lisäksi ja tueksi.

Päätelaitepolitiikka on ylätason kuvaus siitä, mitä tietoa ollaan suojaamassa, mitä turvallisuus periaatteita ja kontrolleja tiedon suojaamiseen käytetään ja kuka on vastuussa tiedon suojaamisesta. Se on yleensä lyhyt sivun tai kahden mittainen dokumentti jossa siinä viitataan tarkempaan ohjeistukseen. Käytön ohjeistuksessa kuvataan käytännön keinoja esimerkiksi tietoturvapolitiikan ja päätelaitepolitiikan toteuttamiseen sekä tiedon turvaamiseen. Päätelaitekäytön ohjeistus voi koskea päätelaitteita yleensä tai se voidaan tehdä erikseen erityyppisille päätelaitteille huomioiden niiden ominaisuudet ja käyttötapaukset.

Päätelaitepolitiikan ja käyttöohjeistuksen pääasiallinen ero on siinä, että politiikka asettaa vaatimuksia, periaatteita ja linjauksia päätelaitteiden turvalliselle käytölle ja käyttäjille, ohjeistus puolestaan auttaa käyttäjiä tekemään asioita oikealla, tarkoituksenmukaisella ja turvallisella tavalla. Päätelaitepolitiikassa voidaan esimerkiksi linjata, että salassa pidettäviä tietoja ei koskaan välitetä eiluotettujen verkkojen (ml. Internetin) kautta salaamattomana ja ohjeistuksessa käsitellään sitä kuinka sähköposti tai liitetiedostot käytännössä voidaan salata viestittäessä ulkopuolisten yhteistyökumppaneiden tai asiakkaiden kanssa.

Päätelaitepolitiikassa asioita tulee käsitellä ytimekkäästi kuvaten vaatimuksia ja yleisiä linjauksia. Päätelaitteiden käyttöohjeistuksessa tulee käsitellä esim. tietoturvapolitiikasta ja päätelaitepolitiikasta johdettujen periaatteiden, linjausten ja vaatimusten toteuttamista eri käyttötapauksissa. Käyttöohjeistuksessa voidaan myös kuvata tarkemmin eri käyttötapauksia sekä salassa pidettävien

tietojen käsittelemistä niissä turvallisesti sallituilla päätelaitteilla. Organisaatio voi halutessaan yhdistää päätelaitepolitiikan ja käyttöohjeistuksen laatimalla riittävän kattavan käyttöohjeistuksen. Käyttöohjeistus voidaan myös sisällyttää tai linkittää käyttäjän muuhun ohjeistukseen.

Seuraavassa taulukossa on listattu asiat, jotka tulisi linjata päätelaitepolitiikassa ja käsitellä tarkemmin käyttöohjeistuksessa. Taulukosta ilmenee myös, kummassa dokumentissa kyseisen asian esilletuominen on suositeltavaa. Kohta ’Päätelaitteiden käyttö’ sisältyy pääasiassa ohjeistukseen, mutta siitä voidaan sisällyttää haluttuja asioita myös päätelaitepolitiikkaan, mikäli organisaatiossa erityisesti halutaan painottaa jonkin asian toteuttamista.

	Päätelaitepolitiikka	Ohjeistus
Yleiset asiat		
Dokumentin kohderyhmä (organisaation loppukäyttäjät, pääkäyttäjät, yhteistyökumppanit vai myös esim. palvelutoimittajan pääkäyttäjät)	X (ylätasolla, esim. kaikki organisaation salassa pidettäviä tietoja tai tiedon käsittelyyn liittyviä järjestelyitä ylläpitävät)	X (tarkempi kohdemäärittely)
Vaatimusympäristö, joihin organisaation päätelaitteiden tietoturvavaatimukset perustuvat (esim. luvussa 2 listatut)	X	
Missä ympäristössä politiikkaa / ohjetta tulee käyttää (esim. erilaiset päätelaitteet, tuotanto-/kehitys-/testiympäristö, fyysiset tilat, organisaation/käyttäjän päätelaitteet, laitteiden yhteystavat)	X (ylätasolla, esim. koskeeko politiikka vain päätelaitteiden käyttöä vai myös tiloja)	X (tarkempi määrittely kyseisille ympäristöille, päätelaitteille, tiloille ja yhteyksille)
Kohderyhmän oikeudet ja vastuut päätelaitteiden käytössä sekä mitä seuraamuksia niiden noudattamatta jättämisellä on	X (määritellään, että ohjetta tulee noudattaa)	X (tarkempi määrittely)
Ylätason kuvaus siitä, miten päätelaitteen turvallisuudesta on huolehdittu	X	
Vaatimus tietoturvapoikkeamista tai niiden epäilystä ilmoittamisesta	X (vaatimuksena)	X (vaatimuksena, ohjeistus miten havaitaan sekä miten ja kenelle ilmoitetaan)
Viittaus muuhun ohjeistukseen, esim. tietoturvapolitiikkaan, päätelaitepolitiikkaan, päätelaiteen käyttöohjeistukseen, palveluiden käyttöohjeistuksiin, tiedon luokitteluun ja tietoaineistojen käsittelyohjeistukseen	X (voidaan viitata esim. päätelaiteohjeistuksen, josta viittaukset muuhun ohjeistukseen löytyvät)	X

	Päätelaitepolitiikka	Ohjeistus
Päätelaitteiden käyttö		
Päätelaitteen käsittely erilaisissa fyysisissä tiloissa		
Erilaisia tiloja ovat esimerkiksi • Organisaation omissa tai muun valtionhallinnon organisaation tiloissa ja sisäverkossa (esim. eri tilojen turvallisuusvyöhykkeet, eri verkot ja verkkosegmentit) • Organisaation tai muun valtionhallinnon toimijan tilojen ja sisäverkon ulkopuolella • Etätyön sallimissa tiloissa (käyttäjän kotona tai vastaavassa tilassa) • Julkisissa tiloissa		
Asioita, jotka tulee linjata ja ohjeistaa • Mitä salassa pidettäviä tietoja, palveluita ja tietojärjestelmiä tilassa voidaan käsitellä • Näyttösuojan käyttäminen • Salakuuntelun ja salakatselun huomiointi		X
Päätelaitteen siirtäminen • Turvattomissa tiloissa päätelaitteen pitäminen koko ajan näkyvissä • Päätelaitteen vienti ulkomaille		X
Omien ohjelmien asentaminen ja ohjelmien suorittaminen		X
Turvallisuuteen vaikuttavien asetusten muuttaminen		X
Kuka saa käyttää laitetta		X
Salasanojen käsittely ja tunnistautuminen	X (jos salasanapolitiikkaa ei ole määritelty ylätasolla)	X
Tiedon tallennuspaikka ja varmuuskopiointi		X
Päätelaitteen lukitseminen, kun sen äärestä poistutaan tai sitä ei käytetä vähään aikaan		X

	Päätelaitepolitiikka	Ohjeistus
Päätelaitteen katoamisesta tai varastamisesta ilmoittaminen • miten ja kenelle ilmoitetaan • päätelaiteen poisto sallittujen päätelaitteiden listalta ja mahdollinen etätyhjennys		X
Toimenpiteet käyttäjän esim. virka-/työ-/sopimussuhteen päättyessä		X (mm. mahdollisesti tarvittavien tietojen siirto, päätelaitteen luovutus tai esim. BYOD-laitteen tyhjennys)
Sähköpostin ja Internetin turvallinen käyttö		X
Erilaisten ei-luotettujen verkkojen käyttö, erityisesti avoimet WLANit ja mobiiliverkot		X

BYOD-laitteiden työkäyttö salassa pidettävien tietojen käsittelyssä on lähtökohtaisesti kielletty ellei niitä ole erikseen organisaation tai valtion palvelukeskuksen riskiarvioinnin kautta hyväksytty tiettyyn käyttötapaukseen ja rajattuun käyttöön. On suositeltavaa, että organisaatio hankkii kaikki salassa pidettävien tietojen käsittelyyn käytettävät työvälineet. Mikäli organisaatio kuitenkin päätyy riskiarvioinnin jälkeen ottamaan BYOD-laitteita rajattuun työkäyttöön, tulee varmistaa, että päätelaitepolitiikassa ja ohjeistuksessa asiat on kirjattu siten, että BYOD-laitteiden työkäyttö on rajattu vain sallittuihin käyttötapauksiin. Lisäksi tulee linjata ja ohjeistaa seuraavat asiat:

1) Käyttöjärjestelmän päivitys
2) Ohjelmistojen päivitys
3) Haittaohjelmien torjuntaohjelmiston asentaminen
4) Salassa pidettävien tietojen tai kaikkien massamuistien salaus
5) Palomuurin asentaminen
6) Mitä palveluita laitteella saa käyttää (esim. sähköpostilla suojaustason IV tietoja rajatusti).

Käyttäjille tulee järjestää koulutusta päätelaitteisiin ja muihin työvälineisiin liittyvistä tietoturva-asioista, esimerkiksi osana yleistä tietoturvatietoisuuskoulutusta tai päätelaitteiden ja työvälineiden käyttökoulutusta. Mikäli käytössä BYOD-laitteita tai monimutkainen päätelaiteympäristö useine käyt-

tötapauksineen, tulee kiinnittää erityistä huomiota käyttäjien tietoturvakoulutukseen ja katselmoida ohjeistuksia säännöllisesti. Koulutuksessa voidaan käsitellä ohjeistukseen kirjattuja asioita ja salassa pidettävien tietojen käsittelyä eri käyttötapauksissa sekä mahdollisia muutoksia. Yleisellä tasolla tietoturvatietoisuuden kehittämiseksi on materiaalia saatavilla esimerkiksi Valtion IT -palvelukeskuksen sivuilla[4] .

BYOD-laitteiden käyttäjiltä tulee vaatia allekirjoitettu suostumuslomake ennen kuin laitteilla voidaan käsitellä rajatusti suojaustason IV tietoja. Suostumuslomakkeen tulee käsitellä ainakin seuraavat asiat:

- Mitä tietoja, palveluja ja tietojärjestelmiä päätelaitteella saa käyttää ja miten tiedot päätelaitteelle siirretään
- Päätelaitteen katoamisen yhteydessä tehtävät toimenpiteet
- Mahdollinen etätyhjennys esim. mobiililaitteiden hallintaohjelmistolla (MDM – Mobile Device Management)
- Päätelaitteen mahdollinen poistaminen sallittujen päätelaitteiden listalta
- Päätelaitteen tietojen varmuuskopiointi
- Ohjelmistopäivitysten asentaminen
- Organisaation lisenssien mahdollinen hyödyntäminen BYOD-laitteella
- Ohjelmien asentaminen päätelaitteelle
- Ohjelmien ostaminen. Valtionhallinnon organisaation luottokorttitietojen syöttäminen BYOD-päätelaitteelle ei ole sallittua.
- Päätelaitteen haittaohjelmasuojaus
- Päätelaitteen käyttäjänhallinta ja tunnistaminen
- Päätelaitteen automaattilukitus ja suojaus, esim. suojakoodi
- Mahdollisen verkkoyhteyden mahdollistavan laitteen (esim. SIM-kortti) käyttäminen ulkomailla
- Pilvipalveluiden käyttö (hallinta-, valvonta- ja tukipalvelut sekä mahdolliset laite- tai ohjelmistovalmistajien pilvi-, tunnistus-, tallennus- ja sosiaalisen median palvelut).

[4] http://www.valtiokonttori.fi/fi-FI/Virastoille_ja_laitoksille/Yhteiset_ICTpalvelut/Tietoturvapalvelut/Tietoturvasarjakuvat/Tietoturvasarjakuvat_ja_julisteet(44190)

8.3 Tarkistuslista riskianalyysiin

Mikäli päädytään tilanteeseen, jossa tiettyjä päätelaitteita ei voida tai haluta koventaa vaatimustenmukaiseksi, voidaan riskiarvioinnin tukena tapauskohtaisen arvioinnin lisäksi käyttää seuraavaa tarkistuslistaa:

1) Mitä vaikutuksia poikkeamilla on tiedon saatavuuteen?
2) Mitä vaikutuksia poikkeamilla on tiedon eheyteen?
3) Mitä vaikutuksia poikkeamilla on tiedon luottamuksellisuuteen?
4) Mikä tietoturvatavoite niillä vaatimuksilla on, joita ei noudateta? Voidaanko rakentaa muita tietoturvaratkaisuja tai käyttää muita suojaustapoja, joilla tavoite saavutetaan?
5) Kuinka turvallisia ja millaisia turva-ominaisuuksia on palveluissa, joita päätelaitteilla on tarkoitus käyttää? Voidaanko tukeutua palveluiden tietoturvallisuuteen ja turva-ominaisuuksiin, ja saavuttaa haluttu tietoturvallisuuden taso tai riittävästi rajata riskejä?
6) Voidaanko manuaalisilla menetelmillä tai ohjeistuksella saavuttaa samoja tavoitteita kuin teknisillä ratkaisuilla?
7) Miten paljon hyötyä riskien hyväksymisellä saadaan?
8) Mahdollistaako poikkeama omien ohjelmien asentamisen päätelaitteille ei-luotetuista verkoista?
9) Mahdollistaako poikkeama toimintaa, jossa käyttäjä saa päätelaitteeseen pääkäyttäjän oikeudet (niin sanottu roottaus)?
10) Mikäli poikkeaman aiheuttama riski realisoituu, vaarantuvatko tiedot vain päätelaitteella vai aiheutuuko siitä samalla pääsy organisaation palveluihin? Voidaanko riskiä rajata?
11) Miten poikkeama vaikuttaa tilanteessa, jossa päätelaite katoaa tai se varastetaan?
12) Miten poikkeama vaikuttaa tilanteessa, jossa päätelaite poistetaan käytöstä?
13) Lisääkö poikkeama hyökkääjän mahdollisuuksia houkutella käyttäjä hyökkääjän tarjoamaan www-sivustolle tai langattomaan verkkoon?

Mikäli riskiarvioinnin tuloksena päädytään tilanteeseen, jossa kaikkia tietoturvavaatimuksia ei täysin täytetä, vaatimuksille on luotava korvaavat menettelyt. Lisäksi on syytä aikatauluttaa uudelleenarviointi, jossa selvitetään, voidaanko vaatimuksia noudattaa tai onko riskeissä tapahtunut muutoksia.

8.4 Esimerkkejä

Tässä kappaleessa on kuvattu esimerkkejä, miten kuvitteellisissa organisaatioissa on toteutettu tietojen käsittelyn vaatimusten toteuttamista eri suojaustason käsittely-ympäristöissä ja käyttötapauksissa. Ratkaisuissa valittaessa tulee harkita niiden sopivuutta omaan ympäristöön ja tiettyihin käyttötapauksiin. Joissakin ympäristöissä voidaan tarvita tiukempia tietoturvaratkaisuja tai tietojen käsittelyyn kohdistuu muita vaatimuksia. Nämä esimerkit eivät kuvaa kattavasti koko ympäristöä, vaan ainoastaan päätason ratkaisuja.

Suojaustason IV käsittelyyn tabletti-päätelaite

Organisaatiossa haluttiin ottaa käyttöön tablettilaitteita työnteon tehostamiseksi. Vaihtoehtona BYOD-käytölle organisaatio päätti hankkia päätelaitteet käyttöönoton tehostamiseksi ja siksi, että organisaation omistamaa laitetta voidaan paremmin hallita ja valvoa YT-menettelyn mukaisesti.

Projekti aloitettiin selvittämällä kyseisiin päätelaitteeseen kohdistuvat tietoturvavaatimukset sekä käytettävät sovellukset ja tiedot, joita päätelaitteilla halutaan käyttää. Tietoturvavaatimukset saatiin arvioimalla VAHTI-ohjeiden vaatimuksia sekä muita organisaation toiminnan ja tietojen käsittelyn asettamia vaatimuksia. Organisaatiossa päädyttiin käyttämään ainakin tässä vaiheessa päätelaitteita vain sähköpostin käsittelyyn sekä yksittäiseen www-pohjaiseen sovellukseen, joissa käsitellään korkeintaan suojaustason IV tietoja.

Vaatimusten määrittelyn jälkeen organisaatio selvitti, miten markkinoilla olevat laitteet vastaavat vaatimuksia ja tarpeita. Tässä vaiheessa selvisi, että kaikkia vaatimuksia ei pystytä toteuttamaan, joten puutteiden aiheuttamia riskejä kartoitettiin ja etsittiin keinoja pienentää niiden vaikutusta.

Tablettilaitteissa on vaikeaa rajoittaa käyttäjän toimia, kuten sovellusten asentamista, yhtä helposti kuin kannettavissa tietokoneissa, joten päädyttiin mobiililaitteiden hallintaohjelmiston (MDM – Mobile Device Management) hankintaan. Sen kautta voidaan muun muassa muokata laitteiden asetuksia, päivittää järjestelmää, valvoa käyttäjien toimia ja hoitaa laitteen etätyhjennys katoamis- tai varkaustapauksissa.

Tablettilaitteelle ei pystytä helposti asettamaan salasanapolitiikan mukaista suojausta, joten niille asetettiin 5-numeroinen suojakoodi. Puutteesta aiheutunutta riskiä pystyttiin pienentämään merkittävästi konfiguroimalla päätelaite siten, että käyttäjän syöttäessä suojakoodin väärin viisi kertaa, tyhjennetään

päätelaitteesta kaikki tiedot. Suojakeino ei välttämättä olisi riittävä, jos päätelaitteelle tallennettaisiin paljon salassa pidettäviä suojaustason IV tietoja.

Laitteen suunnitellun käytön mukaisesti sillä voi käsitellä suojaustason IV tietoja kahdesta palvelusta, joiden turvallisuus varmistettiin seuraavasti:

- Sähköposti: Varmistettiin muun muassa, että organisaation ohjeistuksen mukaan sähköpostilla voi käsitellä korkeintaan suojaustason IV tietoja, tietoliikenneyhteys on riittävän hyvin suojattu ja yli 10 päivää vanhemmat sähköpostit poistetaan automaattisesti päätelaitteesta.
- WWW-pohjainen sovellus: otettiin yhteyttä sovelluksen omistajaan ja varmistettiin, että palvelun käyttö on sallittua, vaikka päätelaite ei täytäkään kaikkia vaatimuksia. Samalla varmistettiin, että sovellus ei istunnon jälkeen jätä laitteeseen suojaustason IV tietoja ja että sovellus vaatii käyttäjältä asianmukaisen tunnistautumisen.

Koska toteutettavan päätelaitteen tietoturvallisuuden taso oli lopulta teknisesti heikompi kuin aiemmin käytössä olleissa kannettavissa työasemissa, päätettiin käyttäjille järjestää tietoturvakoulutus, jossa ohjeistettiin uuden päätelaitteen rajattu käyttö sekä kerrottiin periaatteet, linjaukset, pelisäännöt ja tarkemmat ohjeet uuden päätelaitteen turvalliseen käyttöön. Päätettiin myös, että organisaation intranetissä julkaistaan säännöllisesti jokin lyhyt neuvo tablettilaitteen turvalliseen käyttöön.

BYOD -laite

Organisaatiossa päätettiin sallia omien laitteiden työkäyttö rajatusti tableteilla ja kotikoneilla. Projekti aloitettiin kartoittamalla ne työtarpeiden mukaiset sovellukset, joita käyttäjät haluaisivat käyttää omilla laitteillaan. Kartoituksen tuloksena oli, että pääasiassa laitteilla haluttiin käyttää sähköpostia, kalenteria ja dokumenttien hallintajärjestelmää.

Kartoituksen jälkeen todettiin, että käyttäjien laitteita ei saada helposti organisaation keskitetyn hallinnan piiriin, joten käytännössä niille ei saada toteutettua kaikkia vaatimuksia. Organisaatiossa ei ollut selkeää ohjeistusta sille, mitä tietoa saadaan välittää sähköpostilla tai mitä tietoa saa laittaa kalenteriin. Organisaatiossa oli toteutettu tiedon luokittelu ja määritelty luokitus tehtäväksi dokumenttikohtaisesti metatietoihin.

Organisaatiossa tehtiin riskiarviointi ja päätelaitteiden turvattomuuden vuoksi päädyttiin ratkaisuun, jossa organisaation dokumentit ovat käytettävissä erillisen pääteistuntoratkaisun avulla. Ratkaisussa päätelaitteelle ei tallenneta mitään tietoa, vaan niille välitetään vain kuva etätyöpöydästä ja vastaavasti laitteelta välitetään vain hiiren ja näppäimistön tiedot. Kyseistä pääteistuntoa voidaan käyttää sekä tableteilta että kotikoneilta, jolloin sama ratkaisu on käytettävissä molemmista halutuissa käyttötapauksissa. Tämä oli helpompi ratkaisu myös dokumenttien muokkaukseen käytettävien ohjelmistojen lisenssien kannalta. Päätelaitealustan turvattomuuden vuoksi dokumenttien hallintajärjestelmä konfiguroitiin siten, että pääteistunnolla voitiin käsitellä julkisia tai rajatusti vain suojaustason IV tietoja. Pääteistuntoratkaisun käyttö edellytti päätelaitteelle asennettua ohjelmistoa sekä päätelaitekohtaista sertifikaattia. Myös sähköpostin ja kalenterin käyttö mahdollistettiin pääteistunnon kautta.

Organisaatiossa linjattiin lisäksi, että sähköpostissa ja kalenterissa saadaan käsitellä julkaista tietoa tai rajatusti vain suojaustason IV tietoja. Samalla ohjeistettiin käyttämään salattua sähköpostia tai liitetiedostoa suojaustason IV tietojen välittämiseen ulkopuolisille yhteistyökumppaneille tai asiakkaille. BYOD-laitteiden käyttäjiä vaadittiin allekirjoittamaan suostumuslomake, jossa vaadittiin luvun 8.2 mukaisia asioita. Lisäksi organisaation säännöllisessä tietoturvakoulutuksessa sekä intranetissä käsiteltiin BYOD -laitteisiin liittyviä hyviä käytäntöjä.

Suojaustason III käsittelyyn päätelaite

Organisaatiossa päätettiin tehdä päätelaitteille versiopäivitys tuotantoympäristössä, jolloin päätettiin myös varmistaa niiden käytön turvallisuus ja vaatimustenmukaisuus. Korotetun tietoturvatason päätelaiteympäristö päätettiin toteuttaa perinteisillä ja kannettavilla työasemilla, sillä markkinoilta ei löytynyt käytännöllistä ja kustannustehokasta tapaa toteuttaa tietoturvallista käyttöä puhelimilla tai tableteilla.

Projekti aloitettiin selvittämällä ympäristöön kohdistuvat tietoturvavaatimukset. Tietoturvavaatimukset saatiin arvioimalla VAHTI-ohjeiden vaatimuksia sekä muita organisaation toiminnan ja tietojen käsittelyn asettamia vaatimuksista. Organisaatiossa päätettiin, että päätelaitteilla tullaan tuotantoympäristössä käyttämään mahdollisesti hyvin laajaa joukkoa eri sovelluksia, eikä siten ole mahdollista ottaa yhteyttä kaikkien käsiteltävien tietojen omistajiin. Näin ollen, päätelaitteen tulee täyttää kaikki asetetut vaatimukset.

Päätelaitteet päätettiin ottaa keskitettyyn hallintaan, jolloin muun muassa turva-asetukset voidaan määrittää ja hallita sekä päivitykset voidaan asentaa nopeasti ja luotettavasti. Myös käyttäjien hallinta päätettiin hoitaa keskitetysti ja antaa loppukäyttäjille vain käyttäjätasoisia käyttäjätunnuksia, sekä pitää henkilökohtaiset ylläpitotunnukset IT-organisaation sisällä. Kaikki päätelaitteiden käyttöön ja sen hallintaan liittyvät käyttäjätunnukset tehtiin henkilökohtaisiksi, samoin tietojärjestelmien ylläpitotunnukset.

Käyttöönottoprojektin yhteydessä laadittiin dokumentti, joka kuvaa tunnistetut vaatimukset ja käytettävät turva-asetukset. Se liitettiin muutoshallintaprosessiin siten, että tulevat muutokset tulevat päivitettyä dokumenttiin.

Projektissa myös määriteltiin vastuutahot säännöllisille tietoturvatehtäville. Näitä ovat muun muassa päivitysten asentaminen sekä palomuurisääntöjen ja käyttövaltuuksien ajantasaisuuden varmistaminen.

Päätelaitteiden massamuistit päätettiin salata kokonaisuudessaan, jolloin katoamistapauksissa tieto on paremmin suojattu. Päätelaitteella otettiin käyttöön myös haittaohjelmien torjuntaohjelmisto ja palomuuri, joiden hälytykset liitettiin organisaation poikkeamien seurantajärjestelmään. Samalla päivitettiin päätelaitepolitiikka ja käyttöohjeistus luvun 8.2 mukaisiksi sekä pidettiin tarvittavat koulutukset.

Liiteluettelo

Liite 1: Teknisen ICT-ympäristön tietoturvataso-ohjeen (VAHTI 3/2012) päivitetty liite 3 (TTT – Tietojärjestelmien hallinnan vaatimukset).

Liite 1 erillisenä tiedostona.

Liite 2: Voimassa olevat VAHTI-julkaisut

VAHTI 5/2013	Päätelaitteiden tietoturvaohje
VAHTI 4/2013	Henkilöstön tietoturvaohje
VAHTI 3/2013	VAHTIn toimintakertomus vuodelta 2012
VAHTI 2/2013	Toimitilojen tietoturvaohje
VAHTI 1/2013	Sovelluskehityksen tietoturvaohje
VAHTI 3/2012	Teknisen ICT-ympäristön tietoturvataso-ohje
VAHTI 2/2012	ICT-varautumisen vaatimukset
VAHTI 3/2011	Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011	Johdon tietoturvaopas
VAHTI 4/2010	Sosiaalisen median tietoturvaohje
VAHTI 3/2010	Sisäverkko-ohje
VAHTI 2/2010	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 7/2009	Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009	Kohdistetut hyökkäykset
VAHTI 3/2009	Lokiohje
VAHTI 2/2009	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin
VAHTI 9/2008	Hankkeen tietoturvaohje
VAHTI 8/2008	Valtionhallinnon tietoturvasanasto
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen
VAHTI 3/2008	Valtionhallinnon salauskäytäntöjen tietoturvaohje
VAHTI 2/2008	Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007	Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 1/2007	Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006	Tietoturvakouluttajan opas
VAHTI 9/2006	Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006	Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006	Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi

VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 2/2006	Electronic-mail Handling Instruction for State Government
VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 3/2003	Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002	Valtionhallinnon etätyön tietoturvaohje
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

Uudistuva ja täydentyvä ohjeisto löytyy VAHTIn Internet-sivuilta (www.vm.fi/vahti) sekä www.vahtiohje.fi

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 16001
Telefaksi 09 160 33123
www.vm.fi

5/2013
VAHTI
Joulukuu 2013

ISSN 1455-7606 (nid.)
ISBN 978-952-251-519-3 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-520-9 (pdf)