VALTIOVARAINMINISTERIÖ

Päätelaitteiden tietoturvaohje

LUONNOS xx.xx.2013

Valtionhallinnon tietoturvallisuuden johtoryhmä

x/2013

VALTIOVARAINMINISTERIÖ

VM/ /00.00.00/2013

OHJE

Julkisen hallinnon ICT-toiminto . .2013

Ministeriöille, virastoille ja laitoksille

PÄÄTELAITTEIDEN TIETOTURVAOHJE

Valtionhallinnon päätelaitteiden tietoturvaohjeen (VAHTI X/2013) tarkoituksena on edesauttaa valtionhallinnon ja tarvittaessa myös muun julkishallinnon päätelaitteiden saattamista valtionhallinnon tietoturvallisuusasetuksen edellyttämille tietoturvatasoille sekä yhdenmukaistaa valtionhallinnon päätelaitteiden suojauskäytäntöjä salassa pidettävien tietojen käsittelyssä.

Ohje antaa suuntaviivoja päätelaitteiden käytön suunnittelulle, käytön ohjeistamiselle sekä olemassa olevien päätelaitteiden ja palveluiden käyttämiseen liittyvien riskien arvioimiseen. Ohje tukee organisaatioita valtion tietoturvallisuutta koskevan valtioneuvoston periaatepäätöksen (26.11.2009) ja asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010) toimeenpanossa ja erilaisilla päätelaitteilla tapahtuvan tietojen käsittelyn turvaamista. Ohjeessa kuvataan nykyaikaisten päätelaitteiden ja niihin liittyvien palveluiden tyypillisiä uhkia ja annetaan suuntaviivoja ja käytäntöjä uhkien arvioimisen tueksi, turvallisen käytön mahdollistamiseksi sekä salassa pidettävien tietojen turvaamiseksi.

Ohje on valmisteltu valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) toimesta. Ohje tukee ja täydentää olemassa olevia VAHTI-ohjeita ja julkisen hallinnon tietohallinnon JHS-suosituksia. Ohje kumoaa VAHTI –ohjeen 2/2007, ”Älypuhelimien tietoturvallisuus - hyvät käytännöt”, sisäverkko-ohjeen luvun 13 (VAHTI 3/2010) sekä täsmentää VAHTI 3/2012 vaatimuksia päätelaitteiden osalta.

Hallinto- ja kuntaministeri Henna Virkkunen

Yksikön päällikkö Mikael Kiviniemi

Liite: *Päätelaitteiden tietoturvaohje (VAHTI X/2013)*

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

Puh 09 160 01 tai 09 578 11 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

Lyhyesti VAHTI:sta

Valtiovarainministeriö ohjaa ja yhteen sovittaa 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 tietoturvallisuuden linjaukset ja 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 toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

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. Asetus edellyttää lisäksi tietoturvallisuuden korotetun ja korkean tason tietojenkäsittelyltä suojaustoimia sekä menettelyitä jos se käsittelee suojaustasojen I, II tai III tietoja, mikäli organisaatio on tehnyt tietojen luokittelupäätöksen. Tämän VAHTI -ohjeen näkökulmana on kyseisten eri tietoturvatasojen vaatimusten toimeenpanon tukeminen valtionhallinnossa.

Ohjetta laadittaessa on huomioitu VAHTI:n vuonna 2012 julkaisema Teknisten ICT-ympäristöjen tietoturvataso-ohje, jonka sisältöä tämä ohje täydentää täsmentämällä sen vaatimuksia päätelaitteiden näkökulmasta. Tämä ohje kumoaa VAHTI –ohjeen 2/2007, ”Älypuhelimien tietoturvallisuus - hyvät käytännöt”, sisäverkko-ohjeen luvun 13 (VAHTI 3/2010) ja vaatimukset 13.1-13.12 sekä täsmentää VAHTI 3/2012 vaatimuksia päätelaitteiden osalta. Osa valtionhallinnon toimijoista on ottanut käyttöön uusia työskentelytapoja, päätelaitteita sekä palveluita. Tämän ohjeen avulla valtionhallinnon toimijat voivat arvioida ja huomioida uusia työskentelytapoja, päätelaitteita ja palveluita mahdollistaessaan ja ottaessaan käyttöön tarvittavissa käyttötapauksissa salassa pidettävien tietojen käsittelyn turvallisuuden. Salassa pidettävän tiedon siirtyessä valtionhallinnon toimijalta toiselle varmistetaan yhteisillä turvallisuusvaatimuksilla tiedon turvallisuuden pysyminen sillä tasolla, jonka tiedon omistaja on sille asettanut. Valtionhallinnon toimijan tulee huomioida näiden turvallisuusvaatimusten varmistaminen myös yhteistyökumppaneidensa toimesta mahdollisesti tapahtuvassa salassa pidettävien tietojen käsittelyssä.

Tämän ohjeen sisältämät linjaukset on suositeltavaa ottaa käyttöön hallinnonaloja ja virastoja koskevina soveltamisohjeina sekä suunniteltaessa uusien päätelaitteiden ja niihin liittyvien palveluiden käyttöönottoja. Halutun suojaustason tiedon käsittelyn edellytys on vastaavan tietoturvatason toteuttaminen myös päätelaitteissa ja niihin liittyvissä palveluissa. Tietyissä tapauksissa tietojärjestelmän tai palvelun teknisillä ratkaisuilla voidaan osaltaan kompensoida tiettyjen päätelaitteiden tietojen käsittelyn suojauksen puutteita kyseiselle tietoturvatasolle tai rajata salassa pidettävien tietojen käsittelyä. Näin pienentyneiden riskien kautta voidaan tarvittaessa arvioida tiettyjen käyttötapausten mahdollistamista tietyille päätelaitteille. Tämä tehdään riskiarvioinnin kautta. Riskiarvioinnissa on huomioitava muun muassa kyseisen kohderyhmän (loppukäyttäjien, pääkäyttäjien ja yhteistyökumppaneiden) työnteon kannalta tarpeelliset eri käyttötapaukset ja näissä käyttötapauksissa muodostuva rajattu tietojenkäsittely-ympäristö huomioiden käyttötapauksissa tarvittavien päätelaitteiden ja palveluiden lisäksi tarvittavat tietojärjestelmät, verkot sekä tilat.

Ohje on laadittu VAHTI:n alaisessa hankeryhmässä, jonka jäseninä ovat toimineet:

- Kimmo Janhunen, Oikeusrekisterikeskus, 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 konsultteina osallistuivat KPMG:n asiantuntijat Matti Järvinen ja Antti Alestalo.

Sisältö

1 Johdanto

1.1 Ohjeen tausta, tarkoitus ja tavoite

Ohje on laadittu tukemaan valtionhallinnon toimijoita päätelaitteilla tai niiden välityksellä tapahtuvan tietojen käsittelyn turvaamiseksi. Päätelaitteita koskevien linjauksien, vaatimuksien ja mahdollisten eri toteutustapojen tavoitteina on osaltaan varmistaa salassa pidettävien tietojen turvallisuus tarvittavissa käyttötapauksissa. Ohjeen tavoitteena on myös jakaa hyviä käytäntöjä ja yhtenäistää menettelytapoja päätelaitteiden ja niihin liittyvien palveluiden osalta salassa pidettävien tietojen käsittelyn turvaamiseksi. Tässä ohjeessa keskitytään päätelaitteilla tai pääteistunnoissa tapahtuvan tietojen käsittelyn turvaamiseen täydentäen ja täsmentäen aiemmin annettuja VAHTI-ohjeita ja -vaatimuksia.

Ohjetta laadittaessa on huomioitu päätelaitteiden tarkoituksen mukainen käytettävyys, kustannustehokkuus ja tätä kautta toivottavasti saavutettavat säästöt vakioitujen toimintamallien kautta eri tietoturvatasoilla. Päätelaitteella tapahtuva tietojenkäsittely on keskeisessä roolissa salassa pidettävän tiedon käsittelyssä ja sen turvaamisessa etenkin jos tietojärjestelmässä tai palvelussa on tietoturvapuutteita tai jos päätelaitteella tapahtuvaa käsittelyä ei pystytä niistä käsin rajaamaan. Näitä puutteita voi olla esimerkiksi päätelaitteen, päätelaitteeseen liittyvän palvelun, loppukäyttäjän tai pääkäyttäjän vahvassa tunnistamisessa. Puutteen vaikutus voi vaihtua eri tietoturvatasoilla riippuen tarvittavista käyttötapauksista sekä niissä käytetyistä tietojenkäsittely-ympäristöistä.

Tässä ohjeessa esitetään yleisimpiä uhkia liittyen nykyaikaisiin päätelaitteisiin sekä niihin liittyviin palveluihin, sovelluksiin ja käyttöympäristöihin. Lisäksi tämän ohjeen liitteessä esitetään täydentäviä ja täsmennettyjä vaatimuksia päätelaitteilla ja niihin liittyvissä palveluissa tapahtuvan tietojen käsittelyn turvaamiseksi. Ohjeessa keskitytään suojaustasojen IV ja III mukaisten tietojen päätelaitekäsittelyn suojaamiseen. Lisäksi käsitellään suojaustason II tietojen käsittelyä päätelaitteilla ja niihin liittyvien palveluiden järjestämistä erityisesti sisäverkosta ja sen palveluista sekä muista päätelaitteista irrallaan olevissa turvatyöasemissa (stand-alone -käyttö).

1.2 Yleistä päätelaitteista

Päätelaitteella tarkoitetaan laitetta, jolla loppukäyttäjät ja pääkäyttäjät käyttävät organisaation tietoja sähköisissä tietojärjestelmissä tai muissa palveluissa. Tässä ohjeessa päätelaitetta käsitellään laajasti. Perinteisten pöytätyöasemien ja kannettavien tietokoneiden lisäksi päätelaitteella käsitetään mm. puhelimet, älypuhelimet, päätteet ja taulutietokoneet (tabletit). Päätelaiteen tietojenkäsittely voi tapahtua laitteella ja siihen kiinteästi asennetulla ohjelmistolla tai ympäristö voidaan käynnistää ulkoiselta vaihdettavalta muistilta, esimerkiksi usb-muistilta. Päätelaitteen omainen tietojenkäsittely-ympäristö voidaan ajaa myös verkkoyhteyden kautta, esimerkiksi etätyöpöydältä. Tällöin tietyissä tapauksissa samalla fyysisellä laitteella voidaan ajaa eri tietoturvatasojen mukaisia käsittely-ympäristöjä ja eri käyttöjärjestelmiä.

Eri tietoturvatasojen ja haluttujen eri suojaustasojen tietojen käsittelyn mahdollistaminen yhdellä päätelaitteella on kuitenkin monimutkaista ja tietyissä tapauksissa mahdotonta. Tästä syystä tulee eri

komponenttien (tilat, päätelaitteet, palvelut, tietojärjestelmät, rekisterit sekä verkot) tietoturvatasot määritellä VAHTI-ohjeiden mukaisesti, jolloin voidaan määrittää tietojenkäsittely-ympäristöjen tietoturvataso ja siten määrittää päätelaitteilta vaadittu tietoturvataso.

2 Normit ja muu viitekehys

Tässä luvussa kuvataan lyhyesti keskeisimmät perusteet ja vaikuttimet, joille tämän ohjeen ohjaava sisältö perustuu.

2.1 Lait

Laki viranomaisten toiminnan julkisuudesta (621/1999) ja valtioneuvoston asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta (1030/1999) määrittelevät yleisellä tasolla, minkä tyyppiset tiedot ovat salassa pidettäviä.

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

2.2Tietoturvallisuusasetus

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) antaa asiakirjan käsittelylle määritelmän (3§), normittaa tietoturvallisuuden perusteita (4§) sekä asettaa vaatimuksia tietojenkäsittely- ja säilytystilojen turvallisuudelle (5§). Tietoturvallisuusasetuksen pykälät 13-21 asettavat luokitellun asiakirjan käsittelyä koskevat vaatimukset asiakirjan käsittelyn elinkaaren eri vaiheisiin:

- Käsittelyoikeudet ja niiden luettelointi
- Asiakirjojen säilyttämiseen ja käsittelyyn käytettäviä tiloja koskevat turvallisuusvaatimukset
- Asiakirjan käsittely viranomaisen toimitilojen ulkopuolella
- Sähköisen asiakirjan laatiminen, tallettaminen ja muokkaaminen
- Asiakirjan kopiointi
- Asiakirjan välittäminen
- Asiakirjan siirtäminen tietoverkossa
- Käsittelyn kirjaaminen

- Arkistointi ja hävittäminen

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.

2.3 Ohje tietoturvallisuusasetuksen täytäntöönpanosta (VAHTI 2/2010)

Tietoturvallisuusasetuksen toimeenpanoa edesauttava VAHTI-ohje 2/2010 (*Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta*) linjaa omalta osaltaan tietojenkäsittelyn ja tiedon elinkaaressa huomioitavia asioita tietoturvallisuusasetusta tarkemmin. Ohjetta on täydennetty muilla VAHTI-ohjeilla. Tämän ohjeen kannalta erityisesti sisäverkko-ohjeen (VAHTI 3/2010) sekä Teknisen ICT-ympäristön tietoturvataso-ohjeen (VAHTI 3/2012) tiettyjä vaatimuksia on tässä ohjeessa täsmennetty huomioiden päätelaitteet.

2.4 Sisäverkko-ohje (VAHTI 3/2010)

Sisäverkko-ohje kuvaa sisäverkkojen turvaamisen periaatteita eri tietoturvatasoille. Sisäverkko-ohje asetti luvussa 13 myös päätelaitteiden hallinnan yleisiä vaatimuksia. Tämän ohjeen sisältö korvaa kyseisen luvun 13 sekä korvaa sen vaatimukset 13.1-13.12 seuraavan taulukon mukaisesti. Täsmennetyt vaatimukset on kirjattu päivitettyyn VAHTI 3/2012 liitteen 3 vaatimuslistaukseen seuraavan taulukon mukaisesti:

Viite	**Aiempi VAHTI 3/2010 vaatimus**	**Täsmennetty vaatimus**	**Uusi viite 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 palveluita vain organisaation sisäverkosta tai kun päätelaite on kytketty VPN-yhteydellä organisaation sisäverkkoon.	2.5.1 (uusi tarkennus vaatimukseen)
13.2	Kullakin päätelaitteella on yksilöity tunnus. Identtiset laitekokoonpanot erotetaan em. tunnuksen perusteella.	Organisaatiossa on luettelot organisaation omistamista 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	Päätelaitteissa estetään niiden palveluiden näkyminen verkkoon, joita	2.5.1 (uusi tarkennus vaatimukseen)

Viite	Aiempi VAHTI 3/2010 vaatimus	Täsmennetty vaatimus	Uusi viite VAHTI 3/2012 liitteessä 3
	palomuuri.	ei ole erikseen hyväksytty.	
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 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 koko massamuisti on salattu	2.3.3 (uusi tarkennus vaatimukseen)
13.12	Pöytätyöasemien kiintolevyt on salattu	Päätelaitteilla olevat salassa pidettävät tiedot tai koko massamuisti 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)

Tietoteknisten ympäristöjen tietoturvataso-ohje (VAHTI 3/2012) edesauttaa tietoturvallisuusasetuksen toimeenpanoa teknisemmistä palvelu- ja tietojärjestelmä näkökulmista. Ohjeen luku 4 kuvaa vaatimuksia tekniselle tietotekniikkaympäristölle ja siten osaltaan myös päätelaitteille. Ohjeen liitettä 3 on täsmennetty päätelaitteiden osalta edellisen luvun mukaisesti.

2.6 VAHTI 2/2013 Toimitilojen tietoturvaohje

Päätelaitteiden tietoturvallisuuden kannalta tärkeää on, että niiden käyttö tapahtuu fyysisesti riittävällä tavalla suojatussa ympäristössä. VAHTI 2/2013 ohjeistaa toimitilojen turvallisuudesta eri tietoturvatasoilla. Ohjeessa on päivitetty myös laitetilojen turvallisuudessa huomioitavat asiat eri tietoturvatasoilla. Ohjetta tulee hyödyntää erityisesti toimitilojen muutostilanteissa.

2.7 Kansallinen turvallisuusauditointikriteeristö (2011)

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on laadittu ensisijaisesti tapauksiin, joissa turvallisuusauditoinnin avulla todennetaan elinkeinonharjoittajan valmius täyttää kansainvälisen turvaluokitellun aineiston käsittelykriteerit. Kriteeristön vaatimuksia voidaan käyttää myös julkishallinnon oman turvallisuustason määrittämisessä ja siihen liittyvissä tarkastuksissa. Turvallisuusauditointi voidaan antaa erillisen hyväksyntämenettelyn jälkeen kaupallisen toimijan tehtäväksi silloin, kun kyseessä ei ole kansainvälisen tietoturvallisuusvelvoitteen toteutumiseen liittyvä auditointi.

KATAKRIn I-sarjan (tietoturvallisuus) tietoliikenneturvallisuutta, tietojärjestelmäturvallisuutta ja käyttöturvallisuutta käsittelevissä osioissa on esitetty vaatimusluettelo perustasolle, korotetulle tasolle ja korkealle tasolle. Osa näistä vaatimukset koskettaa päätelaitteiden käyttöä, koventamista ja hallintaa. Vaatimukset pohjautuvat sekä suomalaisten viranomaisten sisäisiin vaatimuksiin, VAHTI-ohjeisiin, ulkomaalaisten viranomaisten ja tietoturvatoimijoiden julkaisuihin että kansainvälisiin turvallisuussäännöstöihin ja standardeihin.

2.8 Muu tausta-aineisto

Muuna tausta-aineistona on käytetty päätelaitealustojen, käyttöjärjestelmien ja palveluiden kovennusohjeita.

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 tuotteidensa turvalliseen käyttöön (esimerkiksi security guide- ja hardening-dokumentit). Lisätietoja näiden hyödyntämiseen 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 ohjelmistojen tehtävänä on muun muassa:

- Eriyttää eri ohjelmat ja niiden suorittaminen toisistaan

- Eriyttää eri ohjelmien käsittelemät tiedot toisistaan
- Salata laitteelle tallennetut tiedot ja havaita mikäli tietoja on muokattu ulkopuolisen toimesta
- Rajoittaa käyttäjien toimia järjestelmässä, kuten ohjelmien asennus
- Rajoittaa pääkäyttäjien toimia järjestelmässä
- Estää tai havaita haittaohjelmien toimintaa, esimerkiksi käyttäjältä vaadittavien vahvistuksien avulla
- Estää tai havainta väärinkäyttöä, esimerkiksi lokituksen avulla.

Päätelaitetta vastaan voidaan hyökätä esimerkiksi:

- Houkuttelemalla käyttäjä asentamaan haitallisia ohjelmistoja
- Houkuttelemalla käyttäjä kytkemään toinen laite (esimerkiksi oheislaite, vaihdettava apumuisti, älypuhelin tai muu laite) käyttäjän päätelaitteeseen ja ajamalla tätä kautta haittaohjelmia päätelaitteella tai varastamalla/muokkaamalla laitteen sisältämiä tai laitteen kautta käsiteltäviä tietoja
- Tartuttamalla haittaohjelma käyttäjän vieraillessa sivustolla, jossa on haittaohjelma (drive-by-download)
- Kuuntelemalla päätelaitteen tietoliikennettä tai esiintyen yhdyskäytävänä tai muuna päätelaitteen tarvitsemana palveluna
- Lähettämällä käyttäjälle haittaohjelman sisältävä tiedosto esimerkiksi sähköpostin tai pikaviestiohjelman kautta. Kun käyttäjä avaa tiedoston, asentuu haittaohjelma päätelaitteeseen.
- Tietojen kalastelulla (phishing) esimerkiksi sähköpostin tai pikaviestiohjelman kautta. Hyökkääjä voi pyrkiä esim. saamaan käsiinsä uhrin salasanan tai muuta salassa pidettävää tietoa.
- Ottamalla laitteeseen etäyhteys esimerkiksi varastettujen ylläpitotunnusten avulla
- Kohdistetulla hyökkäyksellä, jossa hyökkääjällä on tietoa organisaation IT-ympäristöstä ja henkilöistä. Tällöin voidaan käyttää esimerkiksi haavoittuvuuksia, joihin ei ole julkaistu päivityksiä eikä haittaohjelmien torjuntaohjelmat vielä tunnista hyökkäystä. Tällaista hyökkäystä vastaan on erittäin vaikea puolustautua vain päätelaitteella, vaan se vaatii hyökkäyksen tunnistamiskykyä koko tietojenkäsittely-ympäristössä.

Eri päätelaitealustat eroavat merkittävästi niihin kohdistuvien uhkien ja hyökkäysten torjumiskyvyn osalta. Organisaation tuleekin mahdollistaa tietojen käsittely kunkin tyyppisellä päätelaitteella ja niihin liittyvissä palveluissa vasta riskiarvioinnin perusteella. Tämän jälkeen voidaan määrittää tarkoituksen mukaiset turva-asetukset ja kovennukset eri käyttötapauksille, päätelaitteille ja niihin liittyviin palveluihin sekä päättää, minkä suojaustason tietoja päätelaitteella ja niihin liittyvissä palveluissa voidaan käsitellä.

Päätelaitteen tarjoamaa tietoturvaa voidaan heikentää merkittävästi käyttäjän toimesta nostamalla käyttäjän oikeuksia haavoittuvuuden avulla. Korotetuilla oikeuksilla käyttäjän on mahdollista esimerkiksi asentaa sovelluksia muistakin kuin virallisista lähteistä (esimerkiksi iOS -alustalla jailbreakin tavoite usein on

nimenomaan uusien ohjelmien asentaminen). Tietoturva saattaa tällöin lisäksi vahingossa heiketä myös muilla tavoin, esimerkiksi avaamalla uusia verkkoa kuuntelevia palveluita.

Päätelaitteissa saattaa olla myös valmistajasta, operaattorista tai muusta kolmannesta osapuolesta johtuvia tietoturvaa heikentäviä ominaisuuksia tai avoimia palveluita. Nämä on hyvä kartoittaa auditoinneilla.

Päätelaitteen turvallisuutta arvioitaessa on hyvä ottaa huomioon kaikki tietoturvan osa-alueet, eli tiedon eheys, luottamuksellisuus ja saatavuus.

3.2 Päätelaitteelle tallentuvat tiedot

Palveluita suunniteltaessa paikallisesti tallennettavat tiedot usein nopeuttavat eri palveluiden käyttöä, mutta lisäävät hyökkäyspinta-alaa ja siten tietoturvariskejä. Perustason palveluissa voikin käyttömukavuuden takia säilyttää rajatusti tietoja käyttömukavuuden parantamiseksi. Korotetun ja varsinkin korkean tason palveluissa tulee päätelaitteelle tallennettavia tietoja, niiden käsittelyä ja niiden suojaamista arvioida tarkemmin.

Päätelaitteelle tallennettavia tietoja tulee pohtia laajasti ja ainakin seuraavat muodot on hyvä ottaa huomioon:

- Käyttäjien itse tallentamat ja siirtämät tiedostot
- Väliaikaistiedostot
- Varmuuskopiotiedostot
- Eri sovelluksissa ja itse järjestelmässä tallennettavat kirjautumisen mahdollistavat tiedot (kuten pitkäaikaiset evästeet).

Edellisessä luvussa lueteltujen uhkien lisäksi tyypillinen uhka on kadotettu tai varastettu päätelaite. Usein tällöin ei ole tiedossa, ovatko päätelaitteessa olleet tiedot joutuneet ulkopuolisten käsiin. Mikäli henkilö, jolle päätelaite on päätynyt, pyrkii hankkimaan tietoja saattaa hän pystyä saamaan kaikki päätelaitteella olevat tiedot haltuunsa ja mahdollisesti päästä käsittelemään myös verkkopalveluiden sisältämiä tietoja, mikäli päätelaitteelle on tallennettu eri palveluiden kirjautumisen mahdollistavia tietoja. Päätelaitetta on myös saatettu ulkopuolisen toimesta muokata, jolloin se tekee organisaatiolle haitallisia toimia, kuten lähettää tietoja ulkopuoliselle tai murtautuu muihin laitteisiin ja palveluihin.

3.3 Päätelaitteen tietoliikenne

Päätelaitteet mahdollistavat monella eri tavalla tietoliikenneyhteyden muodostamisen. Erilaisia tapoja ovat muun muassa GSM (2G), WCDMA (3G), LTE (4G), Ethernet, WLAN, bluetooth, NFC ja RFID. Osa tavoista, kuten NFC, on lähtökohtaisesti turvaton ja osa tavoista on oikein asennettuna (kuten WLAN) perustasolle soveltuvia menetelmiä. Langattomien verkkojen osalta VAHTI 3/2010 sisältää listan vaatimuksista, joita voidaan soveltaa myös muiden langattomien yhteyksien osalta. Otettaessa käyttöön erilaisia yhteystapoja on hyvä ensin tutkia, onko niissä mahdollisesti olevissa kryptografisissa ratkaisuissa tunnistettuja heikkouksia. Lähtökohta onkin, että kaikki tietoliikennetavat suljetaan pois ja avataan vain ne, joille on työtehtävissä tarvetta ja jotka voidaan asianmukaisesti turvata.

Jotkin päätelaitteet voidaan asentaa siten, että ne tunnistavat kun ne ovat yhteydessä organisaation sisäverkkoon. Tällöin päätelaite voidaan asentaa siten, että se sallii liikenteen vapaammin kuin se sallisi muissa verkoissa. Päätelaitteelle voidaan tehdä myös terveystarkastus ennen kuin sen sallitaan liikennöidä sisäverkkoon. Terveystarkastuksessa voidaan varmistaa esimerkiksi laitekohtaisen palomuurin ja haittaohjelmien torjuntaohjelmiston olemassaolo, päivitysten ajantasaisuus ja muita tietoturvallisuuteen vaikuttavia asioita.

Edellisissä luvuissa mainittujen uhkien lisäksi tietoliikenteeseen erityisesti 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.
- Silloin tällöin eri valmistajien tietoliikennetoteutuksista löytyy haavoittuvuuksia, joita käyttäen hyökkääjä voi pystyä murtautumaan päätelaitteelle.

Sisäverkko-ohje VAHTI 3/2010 sisältää laajemmin tietoa tietoliikenteeseen vaikuttavista uhista ja niiden hallitsemisesta.

3.4 Etätyön ja liikkuvan työn uhkat

Etätyön ja liikkuvan työn merkittävimmät uhat johtuvat siitä, että päätelaite ei ole enää fyysisesti välttämättä tunnetussa eikä suojatussa tilassa ja palveluihin pitää liittyä tyypillisesti Internetin tai muun luottamattoman verkon ylitse. Tiedon luottamuksellisuuden suojaamisen lisäksi on tärkeää palveluiden ja tietojen saatavuus, eli päätelaitteilla pitää monissa käyttötapauksissa päästä käsiksi samoihin palveluihin ja tietoihin kuin päätelaitteen ollessa organisaation sisäverkossa. VAHTI 3/2012 ja varsinkin sen liite 7 sisältävät etäkäytön tekniset vaatimukset.

Salassa pidettävien tietojen käsittely on sallittua ainoastaan käyttäen ratkaisuja, joissa voidaan tehokkaasti salata päätelaitteelta tietoliikenne organisaation sisäverkkoon asti.

Kevyiden päätelaitteiden, kuten tablettien ja puhelinten osalta tilanne saattaa olla sellainen, että ne eivät milloinkaan ota yhteyttä organisaation sisäverkkoon. Tällöin niiden toiminta vastaa verkkoteknisesti aina etäkäyttöä. Tällöin on hyvä miettiä tarkasti, miten turvallisuuteen vaikuttavat toimenpiteet, kuten päivitykset, turva-asetukset ja ohjelmistoasennukset, vaikuttavat niiden ja niiltä käsiteltävien tietojen turvallisuuteen.

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 tietoon. Organisaation onkin syytä ohjeistaa päätelaitteiden käyttöä ulkomailla. Tämä on tarpeen myös mahdollisista tietoliikenneyhteyksistä syntyvien kustannusten hallitsemiseksi.

3.5 USB-muistille asennettava käyttöympäristö

Päätelaitteelle saattaa olla tarpeen asentaa erilaisia käyttöjärjestelmiä eri tilanteisiin. Esimerkiksi tietyissä tapauksissa voidaan sallia laitteen 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 siihen päästä käsiksi. Tällöin käyttäjälle pitää antaa mahdollisuus valita käynnistettävä käyttöjärjestelmä päätelaitteen käynnistymisen yhteydessä. Tätä ei kuitenkaan tule tehdä poistamalla BIOS -salasanaa käytöstä vaan esimerkiksi mahdollistamalla käynnistettävän järjestelmän valinta ilman BIOS –salasanaa tai kertomalla käyttäjälle BIOS -salasana.

Tällaisessa toteutuksessa tuleekin huomioida mm. seuraavia asioita:

- USB-muistilta ajettavat käyttöympäristöt on monesti tehty joustavaksi esimerkiksi sillä tavalla, että ne hyväksyvät monia erilaisia laitteita. Osa ympäristön hyväksymistä laitteista voi olla tietoturvan kannalta kuitenkin haitallisia.
- Käytetäänkö käyttöympäristössä vain paikallisesti tallennettuja tietoja vai käytetäänkö käyttöympäristöä ajavan laitteen tarjoamia verkkoratkaisuja. Tällöin tuleekin ratkaista se, miten erilaisia verkkoja ja niiden palveluita voidaan käyttää turvallisesti.
- Käyttöympäristössä on monesti kaksi eri ympäristöä: laitteelle asennettu käyttöympäristö ja esim. USB –muistilta ajettava käyttöympäristö. Tällöin tulee erityisesti huomioida se, onko tarvetta suojata näitä kahta käyttöympäristöä toisiltaan esim. siten, että ne eivät pääse toistensa tietoihin käsiksi eivätkä ne pysty tuhoamaan niissä olevia tietoja. Tuhoamisen estäminen voi olla helpointa toteuttaa hyvillä varmistuskäytännöillä.

3.6 Muita huomioitavia asioita

Päätelaitekanta on viime vuosina monipuolistunut ja yhdellä käyttäjällä saattaa olla useampia eri päätelaitteita käytössä, joiden tietoturva saattaa olla hyvinkin eri tietoturvatasolla. Tällöin käyttäjäohjeistuksiin ja koulutuksiin on hyvä panostaa entistä enemmän, jotta käyttäjät ymmärtäisivät miten ja mihin eri päätelaitteita saa käyttää, mitä palveluita ja tietojärjestelmiä on tietyille päätelaitteille, mahdollisesti rajatusti, mahdollistettu käyttöön.

Organisaatioissa käytetään monesti palveluja, joita oma organisaatio ei tuota. Palveluja saatetaan hankkia valtionhallinnon sisältä tai valtionhallinnon ulkopuolisilta tahoilta. Valtionhallinnon organisaatioiden tulee toteuttaa tietoturvatasojen perustaso, jolloin kaikkien organisaatioiden palvelujen ja niitä käyttävien päätelaitteiden tulee olla ainakin perustasolla. Tämä helpottaa palveluiden käyttöä valtionhallinnon eri organisaatioiden kesken. Lisäksi valtionhallinnon sisäverkot mahdollistavat päätelaitteiden käytön eri organisaatioiden tiloissa joustavammin.

4 Tietoturvatasojen soveltaminen erilaisiin päätelaitteisiin

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

4.1 Eri tietoaineistot ja suojaustasot

Salassa pidettävää tietoa säilytetään ja käsitellään organisaatiossa tyypillisesti hyvin erilaisissa paikoissa sekä monilla eri laitteilla. Tietoa on mm. sähköisesti päätelaitteilla ja sen lisälaitteilla, palvelimilla, palveluissa, tietojärjestelmissä, rekistereissä, varmistusnauhoilla sekä mm. fyysisesti kuvina ja tekstinä. Sovellettaessa tietoturvatasoja päätelaitteisiin tulee itse päätelaitteen lisäksi kuitenkin huomioida tiedon käsittely ja siirto eri järjestelmissä ja verkoissa. Jotkin järjestelmät, kuten sähköposti, sisältävät hyvin monenlaisia ja useampia eri palveluita ja järjestelmiä, joiden avulla voidaan esimerkiksi välittää usean eri tiedon omistajan tietoja. Tällaisia järjestelmiä eri päätelaitteilla käytettäessä tulee varmistua siitä, että eri päätelaitteella tai niihin liittyvissä palveluissa ei käsitellä korkeamman suojaustason tietoja kuin vastaavasti mille tietoturvatasolle päätelaite ja siihen liittyvät palvelut on organisaatiossa hyväksytty.

Tietojenkäsittely-ympäristöä tulee käsitellä kokonaisuutena. Kokonaisuutta on kuitenkin pystyttävä rajaamaan ja suojaamaan eri tavoin eri tietoturvatasoilla. Tällöin voidaan tapauskohtaisesti hyväksyä alla kuvattuja korvaavia menettelyjä, mikäli tietojenkäsittely-ympäristö tai sen osa suojaa salassa pidettäviä tietoja jollakin muulla menettelyllä kuin mikä on varsinainen vaatimuksen kontrolli. Esimerkiksi korvaava menettely korotetun ja korkean tason vaatimukseen vahvan tunnistautumisen käytöstä ulkopuolisista tietoliikenneverkoista voidaan tapauskohtaisesti riskiarvioinnin jälkeen hyväksyä, mikäli esimerkiksi päätelaite sijaitsee aina luotetussa tilassa ja teknisillä menetelmillä pystytään rajoittamaan pääsyä tilaan, palveluun, korkeamman suojaustason tietoon tai näiden kattaviin lokitietoihin riittävällä tavalla.

4.2 Päätelaitteiden käyttö eri tietoturvatasoilla

Valtionhallinnon organisaatioiden tulee toteuttaa vähintään tietoturvallisuuden perustaso. Lisäksi, mikäli organisaation toiminnassa edellytetään suojaustasoa IV ja tietoturvallisuuden perustasoa korkeamman suojaustason tietojen käsittelyä ja korkeamman tietoturvatason toimintaympäristöjä sekä viranomainen on luokitellut asiakirjat, tulee sen toteuttaa riskienarvioinnin kautta korkeampien tietoturvatasojen vaatimukset mahdollisesti rajattuihin toimintaympäristöihin viiden vuoden kuluessa siitä, kun asiakirjojen luokittelupäätös on tehty.

Organisaation tulee siis selvittää ja tarvittaessa rajata, mitkä ovat sen eri tietojenkäsittely-ympäristöt ja niiden tietoturvatasot[1] ja ainakin toteuttaa tietoturvallisuuden perustaso. Päätöksen tulee perustua riskiarviointiin, kyseisessä ympäristössä käsiteltävään salassa pidettävään tietoon ja sen saatavuusvaatimuksiin. Päätös eri tietoturvatason ympäristöistä vaikuttaa merkittävästi siihen, mitä tietoa ja järjestelmiä päätelaitteilla voidaan käsitellä (esimerkiksi sähköposti), miten päätelaitteita tulee hallita ja missä kohdin tarvitaan salausta tai muita suojauksia.

Kun organisaatio on hyväksynyt päätelaitteen ja niihin liittyvät palvelut jollekin tietoturvatasolle, voidaan sillä käsitellä kyseisen tietoturvatason mukaisen suojaustason tietoa selväkielisenä. Tietoa ei kuitenkaan

[1] Kts. VAHTI 3/2012

tule tallentaa selväkielisenä. Myös matalampien suojaustasojen tietoja voidaan käsitellä korkeamman tietoturvatason laitteella. Esimerkiksi, mikäli päätelaite hyväksytään korotetulle tietoturvatasolle, voidaan sillä käsitellä suojaustason III tietojen lisäksi suojaustason IV ja julkisia tietoja. Mikäli korkeamman tietoturvatason laitteella halutaan käyttää matalamman tason järjestelmiä, tulee käytön riskejä arvioida, ja käyttö tapahtua yhdyskäytäväratkaisun kautta (vertaa KATAKRI, ks. erityisesti I 401.0).

Päätelaitteen hyväksyntä tietylle tietoturvatasolle voidaan tehdä esimerkiksi auditoinnin kautta, jossa päätelaitteiden ja niihin liittyvien palveluiden ominaisuuksia verrataan halutun tietoturvatason vaatimuksiin. Kun soveltuvuus, asetukset ja kovennukset halutulle tietoturvatasolle on varmistettu, voidaan laite hyväksyä käyttöön. Jokaisen valtionhallinnon organisaation ei kannata erikseen auditoida eri päätelaitteita vaan on hyvä selvittää, onko jokin muu organisaatio jo selvittänyt halutun päätelaitteen soveltuvuuden halutulle tietoturvatasolle. Tässä on kuitenkin huomioitava kyseisen käyttötapauksen ja rajoitetun tietojenkäsittely-ympäristön vaikutukset.

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

Organisaatiossa voi olla useamman eri tason päätelaitteita, esimerkiksi organisaatio voi hyväksyä työasemat tietoturvallisuuden korotetulle ja älypuhelimet tietoturvallisuuden perustasolle. Tässä esimerkissä eri päätelaitteilta voi käyttää eri palveluita tai toisessa niitä voi käyttää rajoitetusti: molemmilta voidaan käyttää tietoturvallisuuden perustason järjestelmiä mutta vain työasemilta korotetun tietoturvatason järjestelmiä. Tässä esimerkissä joitakin korotetun tietoturvatason järjestelmiä ja niissä käsiteltäviä salassa pidettäviä tietoja voidaan kuitenkin rajata ja siten mahdollistaa älypuhelimilla rajattuun käyttöön.

Käytetyt järjestelmät ja niiden sisältämät salassa pidettävät tiedot ovat pohjana päätöksenteolle, mutta päätökseen voi vaikuttaa vahvasti myös se, mitä työvälineitä, palveluita, sovelluksia, tietojärjestelmiä ja rekistereitä eri päätelaitteella halutaan käyttää. Esimerkiksi mikäli organisaatio on aiemmin käyttänyt sähköpostia suojaustason III tietojen välittämiseen ja haluaa käyttää sähköpostia myös älypuhelimilla, mutta organisaation käyttämät älypuhelimet saadaan teknisesti kovennettua vain tietoturvallisuuden perustasolle, voi organisaatio päättää rajoittaa sähköpostilla välitettävän vain suojaustason IV tietoja. Tällöin uusi menettely tulee ohjeistaa sähköpostin käyttäjille ja yhteistyökumppaneille sekä ohjeistaa tarkasti, miten suojaustason III tietoja voidaan jatkossa välittää ja miten huomioida tai käsitellä aiempia viestejä ja niiden sisältämiä tietoja. Välittäminen voidaan tehdä esimerkiksi salatulla sähköpostilla tai liitetiedostolla, joita perustason laitteessa ei voida avata tai pääsy liitteisiin voidaan teknisesti estää perustason laitteilta.

Tiedon käyttöä eritasoisissa päätelaiteympäristöissä voidaan rajoittaa myös siten, että tietoaineisto merkitään DRM-leimalla (Digital Rights Management), joka kertoo tietoaineiston suojaustason. Tämän jälkeen järjestelmät voidaan konfiguroida siten, että järjestelmä tai välittävä järjestelmä ei salli pääsyä sellaisilta päätelaitteilta tai välitystä sellaisiin päätelaitteisiin tai palveluihin, jotka eivät vastaa kyseisen suojaustason mukaista tietoturvatasoa. Järjestelmässä tulee huomioida myös mahdolliset vahingossa tapahtuvat väärälle suojaustasolle luokittelut, esimerkiksi mikäli korotetun tietoturvatason päätelaitteella luokitellaan tieto suojaustasolle II, ei kyseisellä päätelaitteella enää pystytä käsittelemään materiaalia.

Lähtökohtana päätelaitteiden käytössä on, että salassa pidettäviä tietoja käsitellään vain päätelaitteilla, jotka ovat sitä vastaavan tietoturvatason mukaisia ja organisaation hyväksymiä kyseisiin käyttötapauksiin. Käytännön syistä on kuitenkin joihinkin käyttötapauksiin tarvetta käyttää päätelaitteita, joiden saattaminen kaikilta osin halutulle tietoturvatasolle on teknisesti hankalaa tai mahdotonta. Tällöin tulee tehdä tapauskohtainen riskiarvio ja päättää voidaanko korvaavan menettelyn avulla kyseessä olevia päätelaitteita käyttää, vaikka ne eivät kaikilta osin vaatimuksia täyttäisikään. Tietyissä tapauksissa tietojärjestelmän tai palvelun teknisillä ratkaisuilla voidaan osaltaan kompensoida tiettyjen päätelaitteiden tietojen käsittelyn suojauksen puutteita kyseiselle tietoturvatasolle tai rajata salassa pidettävien tietojen käsittelyä. Näin pienentyneiden riskien kautta voidaan tarvittaessa arvioida tiettyjen käyttötapausten mahdollistamista tietyille päätelaitteille. Tämä tehdään riskiarvioinnin kautta, joka voidaan tehdä mm. Valtion IT-palvelukeskuksen tietoturvallisuuden työkalupakin riskiarviointivälineellä tai VAHTI 7/2003 ”Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa” -ohjeen mukaisesti. Riskiarvioinnissa on huomioitava kuitenkin käyttötapauksessa tarvittava ja rajoitettu tietojenkäsittely-ympäristö eikä vain päätelaitetta.

Tietojen omistaja määrittelee tiedon suojaustason ja vastaavan tietoturvatason tietojen sähköiseen käsittelyyn. Tietojen omistajan on oltava myös hyväksymässä poikkeuksia turvatoimenpiteisiin. Hyväksyessään poikkeamia, voi tietojen omistaja määritellä myös reunaehtoja käytölle ja käsittelylle, kuten

- Rajallinen aika – päätelaitetta, joka ei täytä kaikilta osin vaatimuksia voidaan käyttää esim. vain kuuden kuukauden ajan, jonka jälkeen tulee siirtyä käyttämään päätelaitteita ja menettelyitä, jotka täyttävät vaatimukset

- Rajallinen käyttäjäjoukko – salassa pidettävään tietoon pääsyä ei anneta yhtä suurelle joukolle kuin annettaisiin, jos päätelaitteet olisivat kaikilta osin vaatimusten mukaisia

- Poikkeava ja rajattu käyttötapa – toteutetaan jokin menetelmä, jossa 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.

Käytännössä tietoja käsitellään useimmiten erilaisten palveluiden, sovellusten, tietojärjestelmien sekä rekisterien kautta. Samaa tietoa voidaan käsitellä useissa eri palveluissa ja tietojärjestelmissä eri käyttötapauksin, jolloin tiedon omistajan on syytä huolehtia siitä, että eri palveluiden, sovelluksien, tietojärjestelmien sekä rekisterien kautta tietoja käsiteltäessä ei kokonaisuutena aiheudu liian suuria riskejä.

Poikkeuksia arvioitaessa on hyvä kiinnittää huomiota mm. seuraaviin asioihin:

- Kuka hallinnoi ja hallitsee laitteita – voidaanko omilla hallintamenettelyillä esim. (1) tyhjentää päätelaitteen sisältö, jos huomataan, että päätelaite on kadonnut tai joutuneet vääriin käsiin, (2) muokata helposti tietoturvallisuuteen vaikuttavia asetuksia, (3) pakottaa halutut asetukset käyttöön tai (4) valvoa päätelaitteiden käyttöä

- Kuinka paljon hyötyä poikkeuksen hyväksymisestä on

- Onko rajatussa tietojenkäsittely-ympäristössä käytössä muita korvaavia menettelyjä ja aiheutuuko niistä lisäriskejä.

5 Palveluiden ja sovellusten käyttäminen päätelaitteella

Tässä luvussa kuvataan päätelaitteilla käytettävien palveluiden ja sovelluksien käyttämiseksi tehtäviä organisaation päätöksiä ja tietojen sekä palveluiden käytössä näiden huomioimista.

5.1 Tehtävät päätökset

Tärkeimmät valtionhallinnon toimijan päätökset ovat edellisessä luvussa kuvatut (1) luokittelupäätös, (2) päätökset eri päätelaitteiden sijoittumisesta eri tietoturvatasoille sekä (3) päätökset eri palveluiden, tietojärjestelmien ja rekistereiden sijoittumisesta eri tietoturvatasoille.[2] Näitä päätöksiä ohjaavat osaltaan järjestelmien tärkeys- ja kriittisyysluokitus, erilaiset rajatut tekniset tietojenkäsittely-ympäristöt, järjestelmien elinkaari, järjestelmien suojausmahdollisuudet sekä toiminnan tavoitteet ja uhat. Valtionhallinnon toimijan tuleekin tehdä riskianalyysi ennen merkittäviä päätelaitteisiin liittyviä toimenpiteitä ja kehityssuunnitelmia. Riskianalyysiin voidaan hyödyntää luvussa 4.2 mainittuja tapoja.

Organisaation päätelaitteilla käsitellään tyypillisesti suojaustasojen III ja IV tietoja. Tällöin tuleekin kartoittaa se, onko joillain päätelaitteilla tarvetta käsitellä suojaustasojen II- tai I -tietoja, jolloin niitä varten voidaan tehdä erillisratkaisuja tai kehittää olemassa olevia päätelaitteita vaatimusten mukaiselle tasolle. Lisäksi tulee kartoittaa se missä määrin on tarvetta suojaustason III tietojen käsittelyyn ja voidaanko sitä järkevästi rajata tiettyihin käyttötapauksiin, palveluihin ja järjestelmiin.

Organisaation tulee päättää, rajoitetaanko käyttäjän mahdollisuutta asentaa ohjelmia päätelaitteille. Riippuen päätelaitteesta, voidaan käyttää ainakin seuraavia malleja (turvallisimmasta turvattomimpaan):

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

Mikäli teknisesti ei estetä ohjelmien asentamista, voidaan riskiarvioinnin jälkeen päätelaitetta käyttää korkeintaan suojaustason IV tietojen käsittelyyn rajoitetusti. Tällöin on erityinen syy ohjeistaa käyttäjille, miten he voivat itse havaita haitallisia ohjelmia. Käytännössä organisaation tulee tällöinkin harkita ainakin

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

käyttäjien asentamien ohjelmien seurantaa ja rajoituksien toimivuutta eri päätelaitteilla (ja niiden alustaversioilla). Lisäksi tulee muistaa, että päätelaiteille on saatavilla paljon myös ohjelmia, jotka eivät vaadi varsinaista asentamista pääkäyttäjäoikeuksin, vaan ne voidaan ajaa vain lataamalla ohjelmatiedosto internetistä tai siirrettäviltä apumuistilta (esim. usb-muisti) ja suorittamalla sen.

Organisaation ei-julkisia palveluita voi olla tarpeen käyttää myös muilla laitteilla kuin organisaation omistuksessa ja hallinnassa olevilla laitteilla. Tällaisia laitteita ovat esimerkiksi

- Käyttäjien omat päätelaitteet:
    - Mobiililaitteet (ns. BYOD)
    - Kotikoneet
- Yhteistyökumppanien päätelaitteet
    - Toiset valtionhallinnon toimijat
    - Palvelutoimittajat
- Ei-hallittavissa olevat päätelaitteet, esim. Internet-kahvilat.

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

- Jokaiselle yllämainitun kaltaiselle päätelaitteelle julkaistavalle palvelulle tulee tehdä riskiarvio ja päättää palvelukohtaisesti, mitkä palvelut ja millä tavoin voidaan julkaista kyseisille päätelaitteille
- Käyttäjien omilla päätelaiteilla ei saa käsitellä suojaustasojen I, II tai III –tietoja.

Pääsy organisaation palveluihin voidaan mahdollistaa esimerkiksi alla kuvatulla eriyttämisellä muusta ympäristöstä, virtualisoimalla tai pääteistunnoilla. Mikäli näiden päätelaitteiden käyttöä ei riittävällä tavalla kontrolloida, on riskeinä ainakin:

- salassa pidettävää tietoa päätyy organisaation ulkopuolisille laitteille, jotka eivät välttämättä vastaa tietojen käsittelyssä vaadittavaa tietoturvatasoa
- salassa pidettävää tietoa päätyy käyttäjän omien laitteiden kautta myös kaupallisten yritysten palveluihin ja tietojärjestelmiin, jotka eivät välttämättä vastaa tietojen käsittelyssä vaadittavaa tietoturvatasoa. Palveluita, joihin tietoa voi päätyä ovat esimerkiksi eri pilvitallennuspalvelut.
- käyttäjien henkilötietoja päätyy EU-alueen ulkopuolelle, jossa lait saattavat mahdollistaa henkilötietojen laajemman hyväksikäytön
- laitteiden kautta saattaa organisaation sisäverkossa oleviin laitteisiin tarttua erilaisia haittaohjelmia
- tietoa vuotaa ulkopuolisille
- tietojen käsittelystä ei jää lokia tai muuta jälkeä, jolloin esimerkiksi rikollisen tai muutoin haitallisen toiminnan jälkiselvittely voi hankaloitua merkittävästi tai olla mahdotonta.

Monissa päätelaitteissa voidaan eristää yksittäisiä tai muutamia sovelluksia muusta ympäristöstä esimerkiksi erilaisilla virtualisointiratkaisuilla. Valtionhallinnon toimijan tuleekin päättää, mitkä ovat sellaisia olennaisia palveluja (jos sellaisia on), jotka päätelaitteessa tulee eriyttää muusta käsittely-ympäristöstä. Näillä ratkaisuilla voidaan esimerkiksi toteuttaa sellainen käsittely-ympäristö, jossa vain yksittäisen palvelun tiedot on salattu ja siinä tapauksessa, että päätelaite katoaa, voidaan poistaa vain

tämän yksittäisen palvelun tiedot. Haittapuolena tällaisten ratkaisujen käytöstä on se, että ne yleensä jonkin verran hankaloittavat päätelaitteen käyttöä.

Sovellusten eriyttämisen lisäksi voidaan eri palveluita tarjota pääteistuntojen kautta, jolloin päätelaitteille ei tallennu mitään tietoja eikä haittaohjelmilla ole niin helppoa murtautua käytettävään sovellukseen. Tällaisia ratkaisuja voidaan käyttää esimerkiksi silloin, kun itse päätelaitetta ei saada kovennettua halutulle tietoturvatasolle. Tällöin tulee kuitenkin arvioida se, täyttyykö haluttu tietoturvataso pääteistunnon tarjoaman tietoturvallisuuden kautta. Uhkana pääteistunnoissakin on mm.

- näppäinpainallusten tallentaminen (ns. keyloggerit)
- järjestelmään mahdollisesti tallentuvat pääteistunnon mahdollistavat tunnukset ja salasanat
- mikrofonin ja kameran kaappaus, jolloin murtautuja voi saada tietoonsa käyttäjän fyysisessä ympäristössä tapahtuvia asioita, kuten keskusteluista salassa pidettäviä tietoja
- kuvankaappauksia näytöstä, jolloin murtautuja voi saada tietoonsa järjestelmässä olevia salassa pidettäviä tietoja.

Monia päätelaitteita voidaan käyttää tunnistautumiseen ja maksamiseen erilaisissa verkko- tai muissa palveluissa. Loppukäyttäjien toimia ne saattavat helpottaa merkittävästi, mutta ne saattavat tuottaa vastuukysymyksiä esimerkiksi mikäli päätelaitteita vaihdetaan henkilöltä toiselle tai ulkopuolinen (tai haittaohjelma) pääsee käsiksi maksamisessa käytettäviin tietoihin. Nämä asiat tulee huomioida organisaation toiminnassa, päätelaitepolitiikassa ja käyttöohjeistuksissa.

Monia päätelaitteella käytettäviä palveluita voidaan hankkia myös pilvipalveluna tai loppukäyttäjät saattavat omatoimisesti haluta käyttää erilaisia pilvipalveluita. Organisaation tuleekin päättää, mitä palveluita käytetään pilvestä ja miten niiden palveluiden tietoturvallisuudesta huolehditaan. Lisäksi tulee ohjeistaa loppukäyttäjiä siitä, mitä pilvipalveluita saa käyttää ja mihin tarkoitukseen. Hyväksyttäessä päätelaitteita käyttöön, tulee huomioida, että monessa laitteessa on jo valmiiksi asennettuna erilaisia pilvipalveluja ja saatetaan tarvita päätelaitteen valmistajan palveluun tunnukset sekä maksuvalmius (esim. luottokorttimaksamisen tiedot). Nämä valmiiksi asennetut pilvipalvelut ovat monesti kiinteä osa päätelaitteen käyttökokemusta ja tuleekin päättää, sallitaanko niiden käyttö ja jos sallitaan, niin miten käyttöä eri käyttötapauksissa tai palveluissa tulisi sitten muutoin rajoittaa tai suojata salassa pidettäviä tietoja, turvata sisäverkon palveluita, tietojärjestelmiä ja rekistereitä. Mikäli riskiarviointia pilvipalvelujen käytöstä ei voida tehdä, on pilvipalvelujen käyttö lähtökohtaisesti kielletty.

5.2 Tietojen ja sovellusten käyttö

Pääperiaatteena erilaisten tietojen ja sovellusten käytölle on edellä kuvattu malli siitä, että päätelaitteella käsitellään vain tietoturvatason mahdollistamaa saman suojaustason tietoa (ja yhdyskäytäväratkaisujen kautta matalamman suojaustason tietoa) kuin mille tasolle päätelaite ja siihen liittyvät palvelut on hyväksytty ja kovennettu. Monia päätelaitteita, erityisesti tablettilaitteita ja älypuhelimia, ei kuitenkaan saada kovennettua kustannustehokkaasti halutulle tasolle tai se vaatisi useita eri tukipalveluita niiden riittävän turvallisesti toteuttamiseksi. Tällöin voidaan tehdä korvaavia menettelyjä yksittäisten tai korkeintaan muutaman tietoturvatasojen vaatimuksen osalta. Korvaava menettely tarkoittaa, että varsinaisen vaatimuksen kontrollin tilalle rakennetaan jokin toinen kontrolli, joka riittävällä tavalla toteuttaa alkuperäisen kontrollin tarkoituksen. Esimerkiksi mikäli päätelaitteelle ei pystytä asettamaan VAHTI 3/2010:n mukaisia salasanavaatimuksia, voidaan hyväksyä heikommat salasanavaatimukset ja

toteuttaa laitteen tyhjentäminen, mikäli salasana syötetään väärin 10 kertaa. Tarkempi ohjeistus korvaavien menettelyjen käytölle löytyy VAHTI 2/2010:n liitteestä 6.

Riskiarviointia tehtäessä tulee huomioida edellisessä luvussa 5.1 kuvatun mukaiset päätökset. Mitä paremmin näissä päätöksissä on huomioitu tietoturvallisuus, sitä paremmin voidaan hyväksyä poikkeavia menettelyitä. Esimerkiksi mikäli organisaatio rajoittaa tehokkaasti ohjelmien asentamista päätelaitteelle tai rajoittaa ohjelmien suorittamista päätelaitteella, sitä pienemmät riskit ovat erilaisista haittaohjelmista niiden hyökkäyspinnan kaventuessa.

Mikäli organisaatio päätyy päätelaitteiden käytössä yllä kuvattuihin poikkeaviin menettelyihin ja alkaa käyttää jonkin toisen valtionhallinnon toimijan tarjoamia palveluita omilla päätelaitteillaan, tulee varmistua siitä, että poikkeava menettely ei vaaranna muiden toimijoiden tietoja ja järjestelmiä. Poikkeavista menettelyistä tulee siis kertoa palvelua tarjoavalle organisaatiolle silloin, kun suunnitellaan tällaisten palveluiden käyttöönottoa.

Päätelaitteen turva-asetuksissa ja kovennuksessa sekä erilaisten palveluiden ja sovellusten käytössä voidaan myös erottaa keskenään sen käyttö organisaation sisäverkossa (organisaation sisäverkko tai valtionhallinnon sisäverkot) ja muut ei-luotetut verkot (sisältäen Internet). Mikäli päätelaitteiden suojaamisessa turvaudutaan poikkeaviin menettelyihin tulee käyttötapauksen käsittely-ympäristö huomioida riskiarvioinnissa.

Mikäli päätelaitteella käytetään organisaation ulkopuolella olevia palveluita, tulee niiden käyttöehdot lukea tarkasti. Niissä saatetaan rajoittaa palvelun tarjoajan vastuuta tietoturvallisuudesta esimerkiksi tiedon varmistuksien osalta tai sitä kautta saatavien haittaohjelmien osalta. Käyttöehdoissa voidaan myös vaatia käyttäjiltä joitakin toimia liittyen tietoturvallisuuteen.

Suojaustason IV osalta etätyössä ja liikkuvassa työssä voidaan käyttää samoja tietoja ja sovelluksia kuin organisaation sisäverkossa ja tiloissa työskenneltäessä. Tällöin tulee kuitenkin erityisesti huomioida seuraavat seikat:

- Päätelaitteen säilytys: kun päätelaitetta ei valvota sitä käyttävän tai muun henkilön toimesta, sen tulee olla lukittu (esim. suojakoodi), ja sitä tulee säilyttää fyysisesti suojatussa tilassa, esimerkiksi lukitussa kaapissa, ja sille tallennetut salassa pidettävät tiedot tai koko massamuisti on salattu.
- Yhteydet käytettäviin palveluihin: tietoliikenneyhteys voidaan salata kokonaan erilaisilla VPN-ratkaisuilla tai salaus voidaan hoitaa 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 tärkeää on, että organisaatiolla on tiedossa, millä kaikilla päätelaitteilla sen palveluita ja tietoja käytetään ja että organisaatio on määritellyt, miten erilaiset päätelaitteet tulee koventaa ja miten niitä hallitaan ennen kuin niillä voidaan päästä käsiksi salassa pidettäviin tietoihin. Kovennusten lisäksi olennaista on seurata valmistajien julkaisemia tietoturvapäivityksiä ja asentaa ne hallitusti mahdollisimman nopeasti päätelaitteille sekä seurata julkaistuja haavoittuvuuksia ja tarvittaessa rajoittaa päätelaitteiden tai sovellusten käyttöä.

Teknisten turvatoimenpiteiden lisäksi on tärkeää ohjeistaa loppukäyttäjiä ja pääkäyttäjiä heillä olevien päätelaitteiden käytöstä ja käytön turvallisuudesta. Luvussa 8 on suositukset päätelaitepolitiikan ja käyttöohjeistuksen sisällöistä.

Pääkäyttäjän ohjeistuksessa on hyvä käsitellä ainakin seuraavat asiat ja tarvittaessa laajemmin jos kyseessä on esimerkiksi ulkoisen palvelutoimittajan pääkäyttäjä:

- Pääkäyttäjän vastuut, oikeudet ja mahdolliset seuraamukset
- Mitä palveluita ja tietoa päätelaitteella saa käsitellä
    - pääkäyttäjäoikeuksin
    - loppukäyttäjäoikeuksin
- Ylätason kuvaus, miten päätelaitteen turvallisuudesta on huolehdittu ja että käyttöä valvotaan
- Käyttö oman organisaation tai muun valtionhallinnon toimijan tilojen ja sisäverkon ulkopuolella
    - pääkäyttäjäoikeuksin
    - loppukäyttäjäoikeuksin
- Päätelaitteiden siirtäminen ja säilytys
- Kenelle 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 kyseiselle tietoturvatasolle asetetut vaatimukset. Tämä voidaan tehdä esimerkiksi seuraavasti:

- Asettamalla päätelaitteen turva-asetukset paikallisesti halutuiksi
- Ottamalla päätelaite keskitettyyn hallintaan, jonka kautta laitteet voidaan koventaa sekä käyttöä valvoa.

Olennaista on varmistaa, että loppukäyttäjät tai haittaohjelmat eivät pääse itse muuttamaan päätelaitteen turva-asetuksia.

Mikäli päätelaitteita hallitaan keskitetysti, tulee varmistua, että myös käytetyt hallintapalvelimet ja hallintaan käyttävät päätelaitteet on toteutettu halutun tietoturvatason mukaisesti riippumatta siitä, ovatko ne oman organisaation tai esimerkiksi palvelutoimittajan hallinnassa.

Tietoturva-ominaisuuksia voidaan toteuttaa päätelaitteiden omilla tai päätelaitevalmistajan muilla ohjelmistoilla sekä niiden ominaisuuksilla tai erillisillä turva-ohjelmistoilla.

Perustietoturvatason kovennuksessa päätelaitteelle tulee toteuttaa ainakin:

- Estää niiden palveluiden näkyminen verkkoon, jotka eivät ole erikseen hyväksytty
- Salassa pidettävien tietojen tai koko massamuistin salaus
- Haittaohjelmien torjunta
- Tehdä päätelaitteen yksilöivät tunnisteet.

Korotetun tietoturvatason päätelaitteessa pitää lisäksi toteuttaa ainakin:

- Mahdollistaa Internetin käyttö sisäverkosta vain yhdyskäytävän (esim. välityspalvelin) kautta
- Rajata Internetin käyttö organisaation verkon ulkopuolella tapahtuvaksi vain VPN-yhteyden kautta
- Estää muiden kuin hyväksyttyjen ohjelmien suorittaminen (whitelist).

Korkean tietoturvatason verkotetulla päätelaitteella pitää lisäksi toteuttaa ainakin:

- Toteuttaa etäyhteyksien automaattinen aikakatkaisu
- Huomioida erityiset tila-vaatimukset mukaan lukien Tempest-suojaus tilalle tai laitteille
- Huomioida korkean tietoturvatason verkon, tietojärjestelmien ja palveluiden vaatimukset päätelaitteelle.

Korkean tietoturvatason verkottomalla päätelaitteella pitää lisäksi toteuttaa ainakin:

- Estää verkkoyhteyksien käyttö
- Huomioida erityiset tila-vaatimukset mukaan lukien Tempest-suojaus tilalle tai laitteille
- Huomioida ja hallita paikallisesti dokumentoidut käyttöoikeudet ja –valtuudet
- Huomioida suojaustason II tietojen käsittelyn lokitusvaatimukset
- Testata säännöllisesti ja suunnitellusti tarvittavat päivitykset
- Asentaa paikallisesti säännöllisesti ja suunnitellusti tarvittavat päivitykset
- Hallita paikallisesti suojaustason II tietojen säännöllinen varmuuskopiointi, suojakopiointi ja palauttaminen sekä näiden testaus suunnitelmien mukaisesti.

Päätelaitteilla voidaan toteuttaa myös:

- Virtualisointi tai hiekkalaatikko-ympäristö, jossa salassa pidettävä tieto rajoitetaan virtuaalisen ’kuplan’ sisään
- Paikallisen päätelaitteen tietojen varmuuskopiointi, mikäli käyttäjien sallitaan tallentaa tietoja paikallisesti
- Päätelaitteen tyhjennys etänä katoamis- ja varkaustapauksissa
- Päätelaitteen tarkastus ennen verkkoon pääsyä. Tarkastuksessa voidaan varmistaa esimerkiksi, että laitteelle on asennettuna ajanmukainen haittaohjelmien torjuntaohjelma ja että laitteelle on asennettuna viimeisimmät päivitykset. Mikäli nämä edellytykset eivät täyty, voidaan laite päästää verkkosegmenttiin, josta ei ole pääsyä organisaation tietoihin.

Yllä listattujen kovennustoimien lisäksi on suositeltavaa, että organisaatio määrittelee tarkemmalla tasolla ne kovennustoimenpiteet, joita eri tasoilla 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). Lisäksi kovennuksessa tulee erityisesti huomioida VAHTI 3/2012 mukaiset vaatimukset. Etäyhteyksien osalta organisaation tulee varmistaa myös,

että VAHTI 3/2012 etäkäytön (liite 7) vaatimukset täytetään. Lisätietoja näiden hyödyntämiseen voi tiedustella Valtion IT-palvelukeskukselta ja Viestintävirastolta.

Monia päätelaitteita, erityisesti kuluttajakäyttöön suunniteltuja älypuhelimia ja tabletteja sekä niiden tarvitsemia palveluita ei ole teknisesti helppoa saattaa tietoturvallisuuden perustason vaatimalle tasolle. Tällöin organisaation tulee riskiarvioinnin keinoin päättää, voidaanko salassa pidettävää suojaustason IV tietoa rajatusti käsitellä niillä tai tallentaa niille. Poikkeukset tulee dokumentoida ja säännöllisin väliajoin selvittää, mahdollistaako päätelaitteiden nopea kehittyminen kontrollien tai muiden suojaavien menetelmien käyttöönoton, vaikka se jossakin vanhemmassa tuotteessa tai tuotteen versiossa ei olisi ollutkaan mahdollista.

Esimerkkinä hallitusta tavasta ottaa käyttöön sähköposti ja kalenteri päätelaitteella, jossa ei pystytä kaikkia tietoturvallisuuden perustason vaatimuksia noudattamaan on seuraava:

- Selvitetään, miten tieto päätyy päätelaitteelle, jolloin havaitaan seuraavat asiat:
    - sähköpostit ja kalenterimerkinnät sisältävät vain poikkeustapauksissa salassa pidettävää suojaustason IV tietoa
    - salassa pidettävä suojaustason IV tiedot on yleensä liitteessä eikä itse sähköpostin tekstissä tai kalenterimerkinnässä
- Selvitetään, miten päätelaitetta tai niissä tarvittuja palvelua voidaan koventaa, jolloin havaitaan seuraavat asiat:
    - päätelaitteessa voidaan määritellä, että sähköposteja säilytetään siinä vain lyhyen aikaa (esim. 7 päivää) ja kalenterimerkintöjenkin näkymiseen on tehokkaat ajalliset rajoitteet
    - päätelaitteessa voidaan määritellä liitteiden noudon tapahtuvan vain erikseen pyydettäessä ohjelmalta ja tämä tulee tehdä sähköposti- ja kalenterimerkintäkohtaisesti tai tämä voidaan palvelussa tai palvelimelta estää
- Otetaan yllä mainitut asetukset käyttöön
- Lisätään päätelaitteen käyttäjäohjeistukseen tietoturvalliset käyttötapaukset ja muut huomioitavat asiat sekä erityisesti maininta siitä, että mikäli käyttäjä epäilee liitteen sisältävän salassa pidettävää tietoa, tulee se avata vasta tietoturvatasojen vaatimusten mukaisella päätelaitteella
- Dokumentoidaan riski ja tehdyt toimenpiteet riskin pienentämiseksi hyväksyttävälle tasolle ja seurataan säännöllisesti onko mahdollista koventaa laite tai palvelu paremmin, jolloin poikkeavaa menettelyä ei enää tarvita.

6.2 Päätelaitteiden omistajuus ja yhteiskäyttö

Tyypillisessä tapauksessa organisaatio hankkii päätelaitteet käyttäjien käyttöön siten, että kullakin käyttäjällä on oma päätelaite. Tämän lisäksi on nykyään jonkin verran yleistynyt malli, jossa käyttäjä käyttää organisaation palveluita itse hankkimallaan ja omistamallaan päätelaitteella (BYOD). 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, olennaista on, että organisaatio sallii salassa pidettävien tietojen käsittelyn vain niillä päätelaitteilla, jotka organisaatio on todennut ja dokumentoinut riittävän turvalliseksi

kyseisessä käyttötapauksessa tietylle tietoturvatasolle käytettäväksi. Myös käyttäjän omien laitteiden tulee olla organisaation hyväksymiä ja tietoturvallisuuden perustasolle kovennettuja, jos rajattua suojaustason IV tietojen käsittelyä halutaan niillä sallittavan.

Käyttäjien omien laitteiden käytön hyväksymisessä tulee riskiarvioinnissa käsitellä ainakin seuraavia asioita:

- Mitä päätelaitteita käyttäjillä on ja 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 ottaa haltuun heidän omat laitteet tarvittaessa väärinkäytöstilanteiden tutkimiseksi tai etätyhjentää ne
- Miten paljon organisaation toimintaa helpottaa käyttäjien omien päätelaitteiden hyväksyminen
- 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, saatetaan palveluita käyttää päätelaitteelta, jonka kaikki käyttäjät eivät ole organisaation sisäisiä. Esimerkiksi organisaatio saattaa hyväksyä tiettyjen rajattujen palveluiden käyttöä kotikoneilta, joita käyttävät myös muut perheenjäsenet. Tällöin riskejä tulee pohtia samantyyppisistä näkökulmista kuin käyttäjän omien päätelaitteiden tapauksessa.

Erityishuomiona jaetuissa laitteissa on käyttäjien tietojen erottaminen toisistaan – voidaanko päätelaitteessa esim. toteuttaa useita käyttäjätilejä tai istuntoja, jotka eivät mitenkään pääse käsiksi toistensa tietoihin. Tämä voidaan toteuttaa esim.

- Salaamalla kiintolevy ja siirrettävät apumuistit tai käyttäjähakemistot ja vaatimalla, että organisaation tietoja käsitellään vain yhdellä käyttäjätunnuksella, jota käyttää vain nimetty henkilö
- Käyttämällä pääteistuntoa.

6.3 Laitteen ja käyttäjän tunnistaminen

Päätelaitteella tulee erottaa keskenään käyttäjän tunnistaminen laitteelle sekä käyttäjän tai laitteen tunnistaminen käytettävälle palvelulle. Jo laitteelle tunnistaminen voi antaa pääsyn organisaation tietoihin niiden tietojen osalta, jotka on tallennettu päätelaitteelle tai kertakirjautumisen muodossa organisaation palveluihin.

Tietoturvallisuuden perustason järjestelmissä käyttäjä voidaan tunnistaa käyttämällä salasanaa tai vastaavaa menetelmää. Päätelaitteita ei ole täysin välttämätöntä tunnistaa tietoturvallisuuden perustason rajatuissa järjestelmissä ja palveluissa. Päätelaitteissa voidaan käyttää myös erilaisia kuvioihin perustuvia käyttäjäntunnistamisen menetelmiä salasanan sijaan, mikäli organisaatio on ensin varmistanut, että kuvion käyttö on yhtä turvallista kuin salasanan käyttö.

Korotetun ja korkean tietoturvatason järjestelmissä etäyhteyksiä otettaessa, tulee käyttää vahvaa tunnistamista. Lisäksi päätelaite tulee tunnistaa käyttämällä organisaation hyväksymää varmennetta tai vastaavaa menettelyä käyttäen. Lisäksi tulee huomioida muut ko. tietoturvatason vaatimukset.

7 Päätelaitteiden elinkaari

Tyypillisesti organisaatiossa on käytössä eri useita erilaisia ja eri aikoina valittuja ja hankittuja päätelaitteita. Hyväksyttäessä eri päätelaitteita käyttöön tulee kunkin kohdalla huomioida koko elinkaaren aikana tehtävät tietoturvatehtävät. Elinkaaren voi jakaa seuraaviin päävaiheisiin:

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

7.1 Esikartoitus

Esikartoituksen tietoturvallisuuden kannalta tärkeimmät tehtävät ovat päätös tarvittavasta tietoturvatasosta (päätelaitteilla käsiteltävien tietojen suojaustaso, millaiseen ympäristöön ja palveluihin tarve kytkeytyä ja millaisilla käyttötapauksilla) sekä päätelaitekartoitus. Tarkoituksena esikartoituksessa on varmistaa, että markkinoilla on saatavilla tuotteita, jotka täyttävät halutut käyttötarpeet ja vaatimukset.

7.2 Hankinta

Hankintavaiheessa kilpailutuksen yhteydessä tulee listata ne tietoturvavaatimukset, jotka hankittavan päätelaitteen ja niihin liittyvien palveluiden (esim. hallinta-, valvonta- ja tukipalvelut) tulee toteuttaa, jotta halutun suojaustasoista tietoa voidaan päätelaitteilla käsitellä. Tietoturvavaatimuksissa tulee ottaa huomioon kyseisen tietoturvatason vaatimusten ja tämän ohjeen läpikäynnin lisäksi lainsäädäntö ja muu regulaatio sekä organisaation toiminnan ja tarvittavien palveluiden kautta tulevat muut vaatimukset hankittaville 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 päätelaitteissa ei pystytä noudattamaan kaikkia asetettuja vaatimuksia, tulee riskienarvioinnissa huomioida, että hallintavälineet ovat erityisen tärkeitä ja varmistua, että niiden osalta ei tehdä tietoturvallisuuden heikennystä. Erityisen tärkeässä asemassa ovat niin sanotut hyppykoneet ja järjestelmät, joiden kautta voidaan päästä hallinnoimaan organisaation päätelaitteita.

Mikäli jokin osa päätelaitteiden hallinnasta on hankittu ulkoiselta palveluntuottajalta, tulee hankinnassa varmistua, että päätelaitteisiin ja niiden hallintaan liittyvät tiedot säilyvät oman organisaation omistuksessa.

7.3 Käyttöönotto

Käyttöönottovaiheessa tulee tehdä itse käyttöönottoon liittyvät tehtävät sekä suunnitella käyttöönottoa seuraavien vaiheiden tietoturvatehtävien toteuttaminen. Käyttöönottovaiheessa päätelaitteet ja niiden ohjelmistot lisätään rekisteriin.

Käyttöönottovaiheessa tyypillisesti tehdään levykuva (image) tai jokin muu järjestely, jolla kaikki tarvittavat asennukset ja asetukset tehdään. Tässä vaiheessa on tärkeää varmistua järjestelyn eheydestä, jotta siihen ei hallitsemattomasti tule muutoksia esimerkiksi haittaohjelmien toimesta. Levykuvalle tai sen mukaiselle päätelaitteelle on hyvä tehdä myös tietoturvatestaus.

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

Mikäli ohjelmistojen asennus tapahtuu käyttäen ohjelmistojen paketointia, tulee viimeistään käyttöönottovaiheessa käydä paketointiin liittyvä prosessi läpi ja varmistua, että siinä käytettävät järjestelmät ja menetelmät täyttävät halutun tietoturvatason.

7.4 Käyttö ja ylläpito

Käytön yhteydessä laitteisiin tulee usein tarvetta tehdä erilaisia ylläpitotoimenpiteitä. Mikäli huolto tai ylläpito hoidetaan palvelutoimittajan tai muun tahon toimesta, tulee huolehtia, että päätelaitteella ei ole salassa pidettävää tietoa salaamattomana. Vaihtoehtoisesti voidaan hoitaa asia esimerkiksi turvallisuussopimuksilla ja taustatarkastuksilla.

Päätelaitteiden muutoshallintaprosessissa tulee muistaa ohjelmistoasennuksien ja asennuksien poistojen päivittäminen rekisteriin. Lisäksi tulee huomioida testaus päätelaitteisiin tai niiden hallintaan käytettävien järjestelmien merkittävien muutosten yhteydessä.

Käytön aikana tulee päivityksiä ainakin päätelaitteen käyttöjärjestelmään ja sovelluksiin sekä näiden turva-asetuksiin. Mahdollisesti myös muihin osa-alueisiin, kuten firmwareen ja ajureihin. Organisaation tulee varmistaa, että kaikki tietoturvan kannalta olennaiset päivitykset (käyttöjärjestelmä, sovellukset, firmware ja ajurit) asennetaan. Asennus voidaan tehdä käyttäjien tai ylläpidon toimesta. Organisaation tulee ainakin seurata, että olennaiset päivitykset on tehty riittävän nopeasti päivityksen julkaisun jälkeen. Mikäli päivityksiä ei pystytä asentamaan, tulee riskiarvion kautta toteuttaa kompensoivia kontrolleja, jotka voidaan toteuttaa esimerkiksi verkkoteknisin keinoin tai turva-asetuksin.

Mikäli käytön aikana päätelaite katoaa ja se saadaan takaisin, tulee sen käytöstä tehdä riskiarvio. Riskinä on, että päätelaitteelle on asennettu haitta- tai vakoiluohjelma, jonka kautta hyökkääjä pääsee käsiksi päätelaitteeseen ja sitä kautta eri järjestelmiin, kun se kytketään takaisin verkkoon. Vaihtoehtoina katoamistapauksessa on pääasiassa päätelaitteen käytön jatkaminen, päätelaitteen uudelleenkäyttöönotto tai päätelaitteen tuhoaminen.

7.5 Uudelleenkäyttöönotto

Päätelaitteen elinkaaren aikana voi tulla eteen tilanteita, joissa laitteelle on tarpeen tehdä käyttöönotto uudelleen. Näitä tilanteita ovat esimerkiksi päätelaitteen siirtäminen toisen käyttäjän käyttöön tai mikäli päätelaite on haittaohjelman saastuttama. Mikäli päätelaitteen massamuisti ei ole ollut salattu, tulee se tyhjentää samoin kuin käytöstä poiston yhteydessä. Mikäli massamuisti on ollut salattu, ei toimenpide ole kaikissa tapauksissa välttämätön. Tämän jälkeen päätelaitteelle tehdään samat toimenpiteet kuin käyttöönoton yhteydessä. Mikäli päätelaitteelle on sallittu tietojen tallennus, tulee muistaa tietojen varmuuskopiointi ennen tyhjennystä.

Mikäli päätelaite otetaan uudelleen käyttöön haittaohjelmatapauksen vuoksi, on syytä selvittää haittaohjelman toimintatapa ja mikäli haittaohjelma on niin kehittynyt, että se saastuttaa muitakin osia päätelaitteesta kuin kiintolevyn tavallista tallennustilaa, tulee tehdä riskiarvio ja arvioida tarve poistaa päätelaite käytöstä. Haittaohjelma voi olla tarttunut esimerkiksi BIOS -järjestelmään 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 käytössä myös käytöstä poiston jälkeen.

Käytöstä poiston yhteydessä tulee myös varmistua siitä, että salassa pidettävät tiedot on poistettu päätelaitteelta ennen kuin päätelaite toimitetaan organisaation ulkopuolelle. Viestintäviraston sivuilta on saatavilla ohje kiintolevyn ylikirjoitukselle (https://www.viestintavirasto.fi/attachments/Ylikirjoitusohje.pdf). On sallittua käyttää myös muita kuin sertifioituja ohjelmia ylikirjoituksessa. Puhelinten ja tablettien osalta on saatavilla myös ohjelmistoja, joilla ne voidaan tyhjentää. Mikäli ylikirjoittamista ei jostain syystä voida tehdä, tulee korotetulla tietoturvatasolla massamuistit murskata. Huomioitavaa on, että tehdasasetusten palauttaminen ei ole sama asia kuin tietojen tyhjennys. Ylikirjoitus- tai tyhjentämisprosessin toimivuus tulee myös testata huolellisesti.

8 Toimeenpano ja tarkempi ohjeistaminen

8.1 Tietoturvatasojen toteutus päätelaitteiden osalta

Mikäli päätelaitteella käsitellään salassa pidettäviä tietoja, tulee päätelaitteita hallita ja niillä salassa pidettäviä tietoja käsitellä tarvittavan tietoturvatason mukaisesti. Tämän ohjeen liitteessä 1 on listattu vaatimukset tietojärjestelmien hallinnalle mukaan lukien täsmennetyillä vaatimuksilla huomioiden päätelaitteet.

Vaatimusten toteuttamiseksi on monesti helpointa hallita päätelaitteita keskitetysti, jolloin on helpompi toteuttaa ja varmistaa vaatimustenmukaisuus. Monilla kevyillä päätelaitteilla ja varsinkin BYOD-laitteilla keskitetyn hallinnan toteuttaminen saattaa olla haastavampaa ja ylläpidollisia tehtäviä (kuten päivitysten asentaminen) voidaan jättää loppukäyttäjille aiemmin kuvatuin tietyin edellytyksin ja vain rajoitetusti sallia suojaustason IV tietojen käsittely. Tällöin on kuitenkin syytä rajoittaa näillä laitteilla käsiteltävien tietojen määrää ja palvelua, valvoa toimintaa tarkemmin, kouluttaa käyttäjät hyvin ja arvioida määräajoin tästä toimintamallista syntyvät riskit. Organisaation ulkopuolisia päätelaitteita (esim. BYOD -laitteet, yhteistyökumppanien päätelaitteet ja käyttäjien kotikoneet) ei saa kytkeä organisaation sisäverkkoon, mikäli niitä ei hallita organisaation (tai sen päätelaiteympäristön palvelutoimittajan) toimesta halutun tietoturvatason mukaisesti. Käytännössä organisaation palveluiden käyttö näiden päätelaitteiden kautta on useissa tapauksissa helpoin toteuttaa erilaisilla terminaaliratkaisuilla.

8.2 Päätelaitepolitiikka, päätelaitekäytön ohjeistus ja vaatimukset

Päätelaitteisiin liittyvä tietoturva-ohjeistus voidaan toteuttaa erillisenä ohjeistuksena, mutta suositeltavaa on, että se sisällytetään yleiseen loppukäyttäjien ja pääkäyttäjien päätelaitteiden käyttöohjeistukseen. Organisaatio voi laatia päätelaitepolitiikan niin halutessaan ohjeistuksen lisäksi ja tueksi. Päätelaitepolitiikan ja käyttöohjeistuksen pääasiallinen ero on siinä, että politiikka asettaa vaatimuksia päätelaitteiden käytölle ja käyttäjille kun ohjeistus puolestaan ohjaa ja auttaa käyttäjiä tekemään asioita oikealla ja tarkoituksen mukaisella tavalla. Päätelaitepolitiikassa asioita on hyvä käsitellä ytimekkäästi kuvaten asetetut vaatimukset ja yleiset linjaukset päätelaitteissa ja niiden käytössä. Päätelaitteiden käyttöohjeistuksessa on hyvä käsitellä päätelaitepolitiikasta (tai tietoturvapolitiikasta) johdettujen vaatimuksien ja linjauksien asioita tarkemmin. Käyttöohjeistuksessa voidaan kuvata tarkemmin eri käyttötapaukset sekä niissä huomioitavat seikat sallituilla päätelaitteilla salassa pidettävien tietojen käsittelemiseksi turvallisesti. Organisaatio voi halutessaan yhdistää politiikan ja ohjeistuksen laatimalla vain kattavan ohjeistuksen. Ohjeistus voidaan myös sisällyttää tai linkittää loppukäyttäjän yleiseen ohjeistukseen.

Seuraavassa taulukossa on esitetty asiat, joita päätelaitepolitiikassa tulisi linjata ja käyttöohjeistuksessa tulisi vähintäänkin käsitellä tarkemmin. Taulukosta ilmenee myös, kummassa dokumentissa kyseisen asian esilletuominen on suositeltavaa. Yksi tapa toteuttaa päätelaitepolitiikka on käsitellä siinä vain yleiset päätelaitteisiin liittyvät asiat, vaatimukset ja linjaukset sekä vaatia turvallista käyttäytymistä ja käyttöohjeistuksen noudattamista päätelaitteilla työskentelyssä.

	Päätelaitepolitiikka	Ohjeistus
Yleiset asiat		
Dokumentin kohderyhmä (organisaation loppukäyttäjät, pääkäyttäjät, yhteistyökumppanit vai myös esim. palvelutoimittajan pääkäyttäjät)	X	X
Vaatimusympäristö, joihin organisaation päätelaitteiden tietoturvavaatimukset pohjaavat (listattu luvussa 2)	X	X
Missä ympäristössä politiikkaa / ohjetta tulee käyttää (esim. fyysiset tilat, erilaiset laitteet, organisaation/käyttäjän laitteet ja laitteiden yhteystavat)	X	X
Kohderyhmän oikeudet ja vastuut laitteiden käytössä sekä se, mitä seuraamuksia siitä on, mikäli ohjeita ei noudateta	X	X
Ylätason kuvaus siitä, miten päätelaitteen turvallisuudesta on huolehdittu	X	
Vaatimus tietoturvapoikkeamista tai niiden epäilystä ilmoittamisesta	X	
Kenelle ilmoitetaan tietoturvapoikkeamista tai niiden epäilystä	X	X
Viittaus muuhun ohjeistukseen, kuten tietoturvapolitiikkaan, päätelaitepolitiikkaan, päätelaiteen käyttöohjeistukseen, palveluiden käyttöohjeistuksiin, tietoaineistojen käsittelyohjeistukseen	X	X
Tiedon luokittelu (luvussa 4.2 käsitellään tiedon käsittelyä eri suojaustasoilla)	X	X
Päätelaitteiden käyttö		
Laitteen käsittely erilaisissa fyysisissä tiloissa Erilaisia tiloja ovat esimerkiksi • Organisaation tai muun valtionhallinnon organisaation tiloissa ja sisäverkossa (esim. eri turvallisuusvyöhykkeet) • Organisaation tai muun valtionhallinnon toimijan tilojen ja sisäverkon ulkopuolella • Etätyön sallimissa tiloissa (käyttäjän kotona tai vastaavassa tilassa) • Julkisissa tiloissa	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)

	Päätelaitepolitiikka	**Ohjeistus**
Asioita, joita tulee huomioida • Mitä salassa pidettäviä tietoja, palveluita ja tietojärjestelmiä tilassa voidaan käsitellä • Näyttösuojan käyttäminen • Salakuuntelun ja salakatselun huomiointi		
Laitteen siirtäminen • Turvattomissa tiloissa laitteen pitäminen koko ajan näkyvissä • Päätelaitteen vienti ulkomaille	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)
Omien ohjelmien asentaminen	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)
Turvallisuuteen vaikuttavien asetusten muuttaminen	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)
Kuka saa käyttää laitetta	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)
Salasanojen käsittely	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)
Tiedon tallennuspaikka ja varmuuskopiointi	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)
Laitteen lukitseminen, kun sen äärestä poistutaan tai sitä ei käytetä vähään aikaan	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)
Sähköpostin ja Internetin turvallinen käyttö	X (vaatimuksena)	X (ohjeena, miten asiat on

	Päätelaitepolitiikka	Ohjeistus
		käytännössä järjestetty)
Erilaisten verkkojen, erityisesti avoimien WLANien, käyttö	X (vaatimuksena)	X (ohjeena, miten asiat on käytännössä järjestetty)

Mikäli käytössä on BYOD-laitteita, on hyvä varmistaa, että ohjeistuksessa ja mahdollisessa päätelaitepolitiikassa asiat on kirjattu siten, että niissä on huomioitu rajattu BYOD-käyttö. Lisäksi on hyvä huomioida seuraavat asiat:

1) Käyttöjärjestelmän päivitys
2) Ohjelmistojen päivitys
3) Haittaohjelmien torjuntaohjelmiston asentaminen
4) Kiintolevyn salaus
5) Palomuurin asentaminen
6) Mitä palveluita laitteella saa käyttää (esim. sähköpostipalvelussa rajatusti salassa pidettäviä suojaustason IV tietoja).

Käyttäjille on hyvä järjestää koulutusta päätelaitteisiin ja muihin työvälineisiin liittyvistä tietoturva-asioista esimerkiksi osana yleistä tietoturvatietoisuuskoulutusta tai käyttökoulutusta. Mikäli käytössä on monimutkainen päätelaiteympäristö useine käyttötapauksineen tai käytössä on BYOD -laitteita, on suositeltavaa kiinnittää erityistä huomiota käyttäjien tietoturvakoulutukseen. Koulutuksessa voidaan käsitellä esimerkiksi ohjeistukseen kirjattuja asioita ja eri käyttötapauksissa salassa pidettävien tietojen käsittelyä. Tietoturvakoulutusmateriaalia on saatavilla esimerkiksi Valtion IT -palvelukeskuksen sivuilla[3].

BYOD-laitteiden käyttäjiltä tulee lisäksi vaatia allekirjoitettu suostumuslomake ennen kuin sillä voidaan käsitellä rajatusti salassa pidettäviä suojaustason IV tietoja. Suostumuslomakkeessa 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

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

- Päätelaitteen tietojen varmuuskopiointi
- Ohjelmistopäivitysten asentaminen
- Organisaation lisenssien mahdollinen hyödyntäminen BYOD-laitteella
- Ohjelmien asentaminen päätelaitteelle
- Ohjelmien ostaminen. Luottokorttitietojen syöttäminen päätelaitteelle ei ole suositeltavaa.
- Päätelaitteen haittaohjelmasuojaus
- Päätelaitteen käyttäjänhallinta ja tunnistaminen
- Päätelaitteen automaattilukitus
- Mahdollisen verkkoyhteyden mahdollistavan laitteen (esim. SIM-kortti) käyttäminen ulkomailla
- Pilvipalvelujen käyttö (päätelaitevalmistajien omat pilvipalvelut ja muut pilvipalvelut).

8.3 Tarkastuslista riskianalyysiin

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

1) Mitä vaikutuksia puutteilla on tiedon saatavuuteen?
2) Mitä vaikutuksia puutteilla on tiedon eheyteen?
3) Mitä vaikutuksia puutteilla on tiedon luottamuksellisuuteen?
4) Mikä tietoturvatavoite niillä vaatimuksien kontrolleilla on, joita ei noudateta? Voidaanko rakentaa muita tietoturvaratkaisuja tai käyttää muita suojaustapoja, joilla tietoturvatavoite saavutetaan?
5) Kuinka tietoturvallisia ovat palvelut, joita päätelaitteilla käytetään? Voidaanko siis tässä tapauksessa tukeutua palveluiden tietoturvaan, jolla voidaan saavuttaa haluttu tietoturvan taso?
6) Voidaanko manuaalisilla menetelmillä tai ohjeistuksella saavuttaa samoja tavoitteita kuin teknisillä ratkaisuilla?
7) Miten paljon hyötyä saadaan riskien hyväksymisestä?
8) Helpottaako poikkeama omien ohjelmien asentamista ei-luotetuista ympäristöistä päätelaitteille?
9) Helpottaako poikkeama toimintaa, jossa käyttäjä saa pääkäyttäjän oikeudet laitteeseen (niin sanottu roottaus)?
10) Mikäli poikkeaman aiheuttama riski realisoituu, vaarantuvatko tiedot vain itse päätelaitteella vai aiheutuuko siitä samalla pääsy organisaation palveluihin ja voidaanko niitä rajata?

11) Miten poikkeama vaikuttaa tilanteessa, jossa päätelaite häviää tai se varastetaan?

12) Miten poikkeama vaikuttaa tilanteessa, jossa päätelaite otetaan pois käytöstä?

13) Helpottaako poikkeama hyökkääjän mahdollisuutta houkutella käyttäjä hyökkääjän tarjoamaan langattomaan verkkoon?

Mikäli riskiarvioinnin kautta päädytään tilanteeseen, jossa kaikkia tietoturvavaatimuksia ei noudateta, on syytä samalla aikatauluttaa uudelleenarviointi, jolloin selvitetään, voidaanko vaatimuksia noudattaa tai onko riskeissä tapahtunut muutoksia.

8.4 Esimerkkejä laitteista eri turvatasoille

Alla on kuvattu esimerkkejä, miten kuvitteellisissa organisaatioissa on toteutettu eri turvatasojen käyttöönottoja. Organisaatiot voivat toteuttaa päätelaitteet myös eri tavalla. Lisäksi ratkaisuissa tulee harkita niiden sopivuutta omaan tiettyyn ympäristöön, sillä joissakin ympäristöissä saatetaan tarvita tiukempia tietoturvaratkaisuja. Nämä esimerkit eivät myöskään kuvaa kattavasti koko ympäristöä, vaan päätason ratkaisuja.

Perustason päätelaite

Organisaatiossa haluttiin ottaa käyttöön tablettilaitteita työnteon tehostamiseksi. Päätelaitteet päätettiin hankkia organisaation toimesta (vaihtoehtona BYOD-implementaatiolle) käyttöönoton tehostamiseksi ja siksi, että organisaation omistamaa laitetta voidaan perustellummin hallita ja valvoa organisaation toimesta.

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

Vaatimusten keräämisen jälkeen organisaatiossa selvitettiin, miten markkinoilla olevat laitteet vastaavat tietoturvavaatimuksia. Tässä vaiheessa selvisi, että kaikkia vaatimuksia ei pystytä toteuttamaan, joten puutteiden aiheuttamia riskejä käytiin läpi ja etsittiin keinoja pienentää riskien vaikutusta.

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

Laitteelle ei pysty helposti asettamaan vaatimusten mukaista salasanaa, joten päätelaitteelle asetettiin 5-numeroinen suojakoodi. Aiheutunutta riskiä kompensoitiin konfiguroimalla päätelaite siten, että käyttäjän syöttäessä suojakoodi väärin viisi kertaa, tyhjennetään päätelaitteesta kaikki tiedot. Suojakeino ei välttämättä olisi riittävä, mikäli päätelaitteelle tallennettaisiin paljon salassa pidettävää tietoa.

Laitteen suunnitellun käytön mukaisesti sillä voi käsitellä salassa pidettävää suojaustason IV tietoja kahdesta palvelusta, joiden teknisen arvioinnin lisäksi turvallisuus varmistettiin seuraavasti:

- Sähköposti: Varmistettiin muun muassa, että organisaation ohjeistuksen mukaan sähköpostilla voi välittää vain korkeintaan suojaustason IV tietoja, yhteys 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 tietoturvallisuuden perustason vaatimuksia. Samalla varmistettiin, että sovellus ei istunnon jälkeen jätä laitteeseen salassa pidettäviä suojaustason IV tietoja ja että sovellus vaatii perustason mukaisen tunnistautumisen.

Koska toteutettavan päätelaitteen tietoturva oli lopultakin teknisesti heikompi kuin aiemmin käytössä olleet kannettavat työasemat, päätettiin järjestää tietoturvakoulutus, jossa käyttäjille ohjeistettiin uuden päätelaitteen käyttöä ja kerrottiin pelisäännöt. Päätettiin myös, että organisaation intranetissä julkaistaan säännöllisesti jokin lyhyt neuvo tablettilaitteen turvalliseen käyttöön.

BYOD -laite

Organisaatiossa päätettiin sallia omien laitteiden käyttö rajatusti työkäytössä tableteilla ja kotikoneilla (BYOD -laitteet). Projekti aloitettiin kartoittamalla ne 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 oman keskitetyn hallinnan piiriin, joten käytännössä niille ei saada toteutettua kaikkia tietoturvallisuuden perustason vaatimuksia. Organisaatiossa ei lisäksi ollut selkeää ohjeistusta sille, mitä tietoa saadaan välittää sähköpostilla tai mitä tietoa saadaan laittaa kalenteriin. Organisaatiossa oli toteutettu dokumenttikohtainen tiedon luokittelu dokumentin metatietoihin.

Organisaatiossa tehtiin riskiarviointi ja päätelaitteen turvattomuuden vuosi päädyttiin ratkaisuun, jossa organisaation dokumentit on käytettävissä erillisen terminaaliratkaisun avulla. Ratkaisussa päätelaitteelle ei tallenneta mitään tietoa, vaan laitteelle välitetään vain kuva etätyöpöydästä ja vastaavasti laitteelta välitetään vain hiiren ja näppäimistön tiedot palvelimelle. Kyseistä terminaaliratkaisua voidaan käyttää sekä kannettavalta työasemalta että tabletilta, jolloin sama ratkaisu on käytettävissä molemmista halutuista alustoista. Tämä oli helpompi ratkaisu myös dokumenttien muokkaukseen käytettävien ohjelmistojen lisenssien kannalta. Alustan turvattomuuden vuoksi dokumenttien hallintajärjestelmä konfiguroitiin siten, että terminaaliratkaisulla voitiin käsitellä rajatusti vain suojaustason IV tietoja. Terminaaliratkaisun käyttö edellytti laitteelle asennettua ohjelmistoa sekä laitekohtaista sertifikaattia.

Sähköpostin ja kalenterin käyttö mahdollistettiin myös terminaaliratkaisun kautta. Lisäksi käyttäjien kotikoneilta mahdollistettiin sähköpostin ja kalenterin käyttö selaimen kautta sertifikaatin avulla. Tableteille tätä toiminnallisuutta ei mahdollistettu laitteen suuremman katoamisriskin vuoksi.

Organisaatio linjattiin lisäksi, että sähköpostissa ja kalenterissa saadaan käsitellä vain suojaustason IV tietoa. Lisäksi BYOD-laitteiden käyttäjiltä vaadittiin suostumuslomake allekirjoitettuna, jossa vaadittiin

luvun 8.2 mukaisia asioita. Lisäksi organisaation säännöllisessä tietoturvakoulutuksessa sekä intranetissä käsiteltiin BYOD -laitteisiin liittyviä hyviä käytäntöjä.

Korotetun tason päätelaite

Organisaatiossa päätettiin tehdä versionpäivitys päätelaiteympäristössä, jolloin päätettiin myös varmistaa sen tietoturva. Korotetun tietoturvatason päätelaiteympäristö päätettiin toteuttaa vain perinteisillä työasemilla, sillä markkinoilta ei löytynyt käytännöllistä tapaa toteuttaa tietoturvallista käyttöä puhelimilla tai tableteilla.

Projekti aloitettiin selvittämällä ympäristöön kohdistuvat tietoturvavaatimukset. Tietoturvavaatimukset saatiin arvioimalla VAHTI-ohjeiden mukaisia tietoturvatasovaatimuksia sekä organisaation toiminnan asettamia vaatimuksista. Organisaatiossa päätettiin, että ympäristöstä tullaan käyttämään mahdollisesti hyvin laajaa joukkoa eri sovelluksia, eikä ole siten mahdollista ottaa yhteyttä kaikkien käsiteltävien tietojen omistajiin, joten päätelaitteen tulee täyttää kaikki asetetut vaatimukset.

Päätelaitteet päätettiin ottaa keskitettyyn hallintaan, jolloin muun muassa päivitykset voidaan asentaa nopeasti ja luotettavasti. Myös käyttäjien hallinta päätettiin hoitaa keskitetysti ja antaa loppukäyttäjille vain käyttäjätasoisia käyttäjätunnuksia ja pitää ylläpitotunnukset vain IT-organisaation sisällä. Kaikki päätelaitteen käyttöön ja sen hallintaan liittyvät käyttäjätunnukset tehtiin henkilökohtaisiksi.

Käyttöönottoprojektin yhteydessä tehtiin dokumentti, joka kuvaa käytettävät tietoturva-asetukset ja dokumentti liitettiin muutoshallintaprosessiin siten, että muutokset tulee päivitettyä dokumenttiin.

Projektissa myös määriteltiin säännöllisten tietoturvatöiden vastuulliset. Näitä säännöllisiä töitä on muun muassa päivitysten asentaminen, palomuurisääntöjen ajantasaisuuden varmistaminen ja käyttövaltuuksien ajantasaisuuden varmistaminen.

Päätelaitteen massamuisti päätettiin salata kokonaisuudessaan, jolloin katoamistapauksessa tieto on paremmin suojattu. Päätelaitteella otettiin käyttöön myös haittaohjelman torjuntaohjelmisto ja palomuuri. Näiden ohjelmien hälytykset liitettiin organisaation poikkeamien seurantajärjestelmään.

Liiteluettelo

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