VALTIOVARAINMINISTERIÖ

Sisä-verkko-ohje

Valtionhallinnon tietoturvallisuuden johtoryhmä

3/2010 VAHTI

VALTIOVARAINMINISTERIÖ

Sisäverkko-ohje

Valtionhallinnon tietoturvallisuuden johtoryhmä 3/2010 VAHTI

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila/VM-julkaisutiimi

ISSN 1455-2566 (nid)
ISBN 978-952-251-138-6 (nid)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-139-3 (PDF)

YMPÄRISTÖMERKKI
MILJÖMÄRKT
441 002
Painotuote

Juvenes Print
Tampereen yliopistopaino Oy

VALTIOVARAINMINISTERIÖ
Hallinnon kehittämisosasto

VM/2312/00.00.00/2010
OHJE
30.11.2010

Ministeriöille, virastoille ja laitoksille

SISÄVERKKO-OHJE

Valtiovarainministeriön (VM) *Sisäverkko-ohjeen* tavoitteena on yhtenäistää ja tehostaa menettelyitä sisäverkkojen rakentamisessa sekä tukea sopivan tietoturvatason käyttöönottoa organisaatioissa. Ohje korvaa valtiovarainministeriön vuonna 2001 antaman suosituksen lähiverkkojen tietoturvallisuudesta (VAHTI 2/2001). Sisäverkko-ohjetta tulee hyödyntää yhdessä VM:n aiemmin antaman tietoturvallisuusasetuksen täytäntöönpanon yleisohjeen VAHTI 2/2010 kanssa.

Sisäverkon tietoturvaohje on soveltamisohje 1.10.2010 voimaantulleelle Valtioneuvoston asetukselle tietoturvallisuudesta valtionhallinnossa (1.7.2010/681, jäljempänä tietoturvallisuusasetus). Tietoturvallisuusasetukseen sisältyvien siirtymäaikasäännösten mukaan viranomaisen on saatettava tietojenkäsittelynsä vastamaan asetuksen 5 §:ssä säädettyjä perustason tietoturvavaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta eli 30.9.2013 mennessä.

Asiakirjojen ja tietoaineistojen luokituksen on määrä helpottaa viranomaisten välistä salassa pidettävien tietojen vaihtoa. Luokittelua vastaavat vaatimukset on toteutettava viiden vuoden kuluessa siitä, kun luokittelu otetaan käyttöön viranomaisessa.

Sisäverkon tietoturvaohje on tarkoitettu valtionhallinnon sisäverkkojen rakenteesta, rakentamisesta ja tietoturvallisuudesta vastaaville. Ohjetta käytetään sisäverkkoja rakennettaessa sekä niiden ulkoistuksissa ja tietoturva-auditoinneissa, ja siihen sisältyy sisäverkkoja koskevat perus-, korotetun ja korkean tietoturvatason linjaukset. Ohjeessa kerrotaan myös kuhunkin verkon osa-alueeseen liittyvät uhat ja taustoitetaan näitä teknisesti. Myös kansainvälisiä tietoaineistoja koskevia käsittelyvaatimuksia on otettu huomioon.

Viraston johdon tulee huolehtia ohjeen noudattamisesta ja siitä, että sisäverkkojen vastuuhenkilöt tuntevat ohjeen sisällön. Ohjeen mukaisella toiminnalla viranomainen voi saavuttaa sisäverkoissaan asetuksen mukaiset tietoturvatasot sekä tasapainottaa riskienhallinnan ja kustannustehokkuuden.

Hallinto- ja kuntaministeri — Tapani Tölli

Neuvotteleva virkamies — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: Sisäverkko-ohje (VAHTI 3/2010)

Lyhyesti VAHTIsta

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

VAHTIn 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 elintärkeiden toimintojen strategian (YETT), valtion IT-strategian, valtioneuvoston huoltovarmuuspäätöksen, kansallisen tietoturvastrategian, 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 VAHTIn asemaa ja tehtäviä hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elimenä. Peiaatepäätöksen mukaisesti hallinnonalat kohdistavat varoja ja resursseja tietoturvallisuuden kehittämiseen ja VAHTIssa koordinoitavaan yhteistyöhön.

VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta astaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTIn toiminnalla parannetaan valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on aikaansaatu yksi maailman kattavimmista yleisistä tietoturvaohjeistoista (www.vm.fi/vahti). VM:n ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita sekä laaja valtion tietoturvallisuuden kehitysohjelma.

VAHTI on saanut kolme kertaa tunnustuspalkinnon esimerkillisestä toiminnastaan Suomen tietoturvallisuuden parantamisessa.

Johdon yhteenveto

Tämä ohje on tarkoitettu valtionhallinnon sisäverkkojen rakenteesta, rakentamisesta ja tietoturvallisuudesta vastaaville. Ohjetta käytetään sisäverkkoja rakennettaessa sekä niiden ulkoistuksissa ja tietoturva-auditoinneissa. Viraston johdon tulee huolehtia ohjeen noudattamisesta ja siitä, että alueen vastuuhenkilöt tuntevat ohjeen sisällön.

Sisäverkon tietoturvaohje on soveltamisohje 1.10.2010 voimaantulleelle Valtioneuvoston asetukselle tietoturvallisuudesta valtionhallinnossa (1.7.2010/681, jäljempänä tietoturvallisuusasetus). Tietoturvallisuusasetusta sovelletaan valtion viranomaisiin, joilla tarkoitetaan valtion hallintoviranomaisia sekä muita virastoja ja laitoksia. Ohje korvaa valtiovarainministeriön vuonna 2001 antaman suosituksen lähiverkkojen tietoturvallisuudesta (VAHTI 2/2001).

Ohjeen tavoitteena on yhtenäistää menettelyitä sisäverkkojen rakentamisessa sekä tukea sopivan tietoturvatason käyttöönottoa organisaatioissa. Ohjeessa sisäverkolla tarkoitetaan viraston toimipisteiden paikallisten lähiverkkojen ja niitä yhdistävien verkkojen muodostamaa kokonaisuutta. Sisäverkon tietoturvaohjeessa kerrotaan kuhunkin verkon osa-alueeseen liittyvät uhat ja taustoitetaan näitä teknisesti. Kullekin osa-alueelle annetaan suositukset, vahvat suositukset sekä vaatimukset tietoturvallisuuteen liittyville varotoimille perus-, korotetulle ja korkealle tietoturvatasolle.

Käsiteltäviä osa-alueita ovat yhteistyökumppaniyhteydet, verkon kaapelointi, langattomat verkot, aktiivilaitteet, sisäverkon yhteydet, päätelaitteet, palvelut, tunnistautuminen, verkon hallinta ja valvonta sekä jatkuvuussuunnittelu.

Sisäverkon tietoturvaohje on tarkoitettu käytettäväksi seuraavissa asiayhteyksissä

- Tietoturvallisuusasetuksen soveltaminen: Tämä sisäverkon tietoturvaohje antaa suositukset ja vaatimukset sisäverkon tietoturvallisuuden varotoimiin.
- Sisäverkon rakentaminen: Uusi sisäverkko on rakennettava ohjeen mukaan ja sen mukaista toteutusta on vaadittava verkon rakentamiseen liittyvissä kilpailutuksissa.
- ICT-alueen ulkoistukset: Ulkoistettaessa verkkoon liittyviä toimintoja, tarjouspyynnöissä ja palveluissa on vaadittava, että tuotettava palvelu on vähintään ohjeen mukainen.

- Verkon tietoturva-auditointi: Sisäverkon tietoturvallisuutta auditoitaessa ohje antaa listan tarkastettavista asioista.

Tietoturvallisuusasetus tuli voimaan 1.10.2010. Asetukseen sisältyy siirtymäaikaa koskevat säännökset. Näiden mukaan viranomaisen on saatettava tietojenkäsittelynsä vastamaan asetuksen 5 §:ssä säädettyjä perustason tietoturvavaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta eli 30.9.2013 mennessä.

Asiakirjojen luokittelu ei asetuksen mukaan ole pakollista. Viranomaisen on syytä päättää, ottaako se luokittelun käyttöön, milloin ja missä laajuudessa. Luokittelua vastaavat käsittelyvaatimukset on toteutettava 5 vuoden kuluessa siitä, kun luokittelu otetaan käyttöön.

Luokittelun käyttöönoton suunnittelu on tärkeää. Luokituksen on määrä helpottaa viranomaisten välistä salassa pidettävien tietojen vaihtoa, minkä vuoksi luokittelu on erityisen suositeltavaa toteuttaa viranomaisissa, jotka joko saavat toisilta viranomaisilta tai luovuttavat muille viranomaisille säännönmukaisesti ja massaluonteisesti salassa pidettäviä asiakirjoja.

Yleiset ohjeet tietoturvallisuusasetuksen täytäntöönpanosta, aineistojen luokituksista, suojaustasoista ja vaatimuksista sekä tietoturvatasoista ja niiden mukaisista linjauksista annetaan ohjeessa VAHTI 2/2010.

Sisältö

Lyhyesti VAHTIsta 7

Johdon yhteenveto 9

A Esittely 15
A.1 Työryhmän kokoonpano 15
A.2 Ohjeen tarkoitus ja rajaus 15
A.3 Ohjeen rakenne 17

1 Johdanto 19

2 Mikä on sisäverkko 23

3 Tietoliikennemallit 27

4 Verkon eri tasot 29
4.1 Palvelut 30
4.2 Laitteet 30
4.2.1 Päätelaitteet (työasemat) 30
4.2.2 Aktiivilaitteet (kytkimet ja vastaavat laitteet) 30
4.3 Verkko 31
4.3.1 Arkkitehtuuri ja rakenne 31
4.3.2 Tietoliikenne 31

5 Verkon rakenne (arkkitehtuuri) 33
5.1 Tietoturvallisuustason vaikutus verkon rakenteeseen 33
5.2 Verkkojen jaottelu käyttötarkoituksen mukaan 34
5.3 Ulkoiset yhteydet 35
5.4 Dokumentaatio 35
5.5 Teknologiatausta 36
5.6 Verkon rakenteen tarkistuslista 37

6 Sisäverkkoympäristössä suojattavat kohteet 39
6.1 Suojattavien kohteiden tarkistuslista 40

7 Sisäverkkoon kohdistuvia uhkia ja vaatimuksia 41
7.1 Uhkien ja vaatimusten tarkistuslista 46

8 Yhteistyöstä muiden toimijoiden kanssa 47
8.1 Yhteistyöstä muiden toimijoiden kanssa tarkistuslista 50

9 Kaapelointi 51
9.1 Teknologiatausta 52
9.2 Kaapeloinnin tarkistuslista 53

10 Langattomat lähiverkot 55
10.1 Teknologiatausta 56
10.2 Langattomien lähiverkkojen tarkistuslista 57

11 Verkon aktiivilaitteet 59
11.1 Teknologiatausta 59
11.2 Verkon aktiivilaitteiden tarkistuslista 61

12 Sisäverkkojen väliset yhteydet 63
12.1 Teknologiatausta 63
12.2 Verkon aktiivilaitteiden tarkistuslista 64

13 Sisäverkon päätelaitteet 65
13.1 Teknologiatausta 66
13.1.1 Työasemat 66
13.1.2 Mobiilit päätelaitteet (mobiililaitteet) 67
13.2 Päätelaitteiden tarkistuslista 68

14 Sisäverkon palvelut 69
14.1 Verkon toiminnan varmistavat palvelut 69
14.1.1 Teknologiatausta: Osoitepalvelu 69
14.1.2 Teknologiatausta: Reitityspalvelu 70
14.1.3 Teknologiatausta: Nimipalvelu 71
14.2 Verkon päälle rakennettavat palvelut 71
14.2.1 Teknologiatausta: Tukipalvelut – aikapalvelu 72
14.2.2 Teknologiatausta: Kommunikaatiopalvelut – sähköposti 72

14.2.3 Teknologiatausta: Resurssien jako 72
14.3 Palveluiden tarkistuslista 73

15 Tunnistautuminen 75
15.1 Teknologiaratkaisuja tunnistautumiseen 77
15.2 Tunnistautumisen tarkistuslista 79

16 Verkon hallinta/valvonta 81
16.1 Teknologiaratkaisuja verkon hallintaan/valvontaan 82
16.2 Hallinnan/valvonnan tarkistuslista 84

17 Jatkuvuussuunnittelu 87
17.1 Häiriötilanteet 87
17.2 Poikkeusolosuhteet 89
17.3 Jatkuvuussuunnittelun tarkistuslista 90

18 Lähde- ja viiteaineistoja 93

19 Valtiovarainministeriön antamia tietoturvaohjeita 95

A Esittely

A.1 Työryhmän kokoonpano

Tämä ohje on laadittu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn alaisena ja ohjaamana . Ohjeen laatineen Lähiverkkojen tietoturvaohjeen uusimisryhmän jäseninä olivat:

- Kimmo Janhunen, Valtiokonttori, ryhmän puheenjohtaja 1.1.2010 alkaen
- Kari Keskitalo, Valtiokonttori, ryhmän puheenjohtaja 31.12.2009 saakka
- Max Hamberg, Valtionvarainministeriö
- Urpo Kaila, CSC
- Kari Keskiväli, Puolustusvoimat
- Mats Kommonen, Turun yliopisto
- Kimmo Rousku, Valtiokonttori, 1.10.2009 alkaen
- Tapio Salonsalmi, Suomen Kuntaliitto

Ohjeen laadintaan konsultteina osallistuivat KPMG:n asiantuntijat: Matti Järvinen, Kari Saarelainen ja Samuel Korpi.

Ohjeen luonnos oli avoimella ja laajalla lausuntokierroksella 12.3.2010 – 7.4.2010. Saadut lausunnot käsiteltiin työryhmän kokouksissa 3.5.2010 – 4.5.2010 ja huomioitiin ohjeen lopulliseen versioon.

VAHTI päätti ohjeen julkistamisesta syyskuussa 2010 pidetyssä kokouksessa.

A.2 Ohjeen tarkoitus ja rajaus

Valtio kehittää omaa tietoturvallisuuttaan jatkuvasti. Yhtenä osoituksena tästä ovat valtionhallinnon organisaatioille asetetut tarkentuvat vaatimukset. Esimerkkeinä tästä ovat Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä (VAHTI 7/2009) julkaistu (26.11.2009), tietoturvallisuusasetus sekä siihen liittyvä Ohje tietoturvallisuusasetuksen täytäntöönpanosta (**VAHTI 2/2010**) sekä Kansallisen turvallisuusauditointikriteeristön (KATAKRI) ja ICT-varautumisen vaatimusten valmistelu

Tämä ohje on päivitetty ja korvaava versio Valtionhallinnon lähiverkkojen tietoturvallisuus –suosituksesta (VAHTI 2/2001). Työryhmän tavoitteena oli valmistella soveltamisohje tietoturvallisuusasetuksen ja tietoturvatasojen määrityksille. Ohjeen velvoittavuus tulee tietoturvallisuusasetuksen kautta.

Ohjeen avulla on mahdollista

- Parantaa tietoturvallisuuden tasoa yhtenäistämällä tietoturvavaatimuksia valtionhallinnon sisäverkoissa
- Tukea organisaatioita sisäverkkojen tietoturvallisuuden varmistamisessa ja kehittämisessä
- Levittää jo olemassa olevia hyviä käytäntöjä organisaatioihin.

Suomi on valtiona sitoutunut lukuisissa sopimuksissa ja oman lainsäädäntönsä kautta suojaamaan sitä sopijakumppanin luokittelemaa tietoa, jonka suomalainen viranomainen tai yksittäinen henkilö saa haltuunsa. Tässä ohjeessa kansainvälisellä tietoaineistolla ymmärretään Suomen sopijakumppaneiden – olivatpa kyseessä yksittäiset maat tai kansainväliset organisaatiot – tuottamaa tietoa, joihin kyseisillä sopijakumppaneilla on tuottajanäkökantaan perustuen tiedon omistusoikeus. Laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) säädetään yksiselitteisesti kansainväliselle luokitellulle tietoaineistolle sen mukainen suoja, kuin mitä Suomen ja kansainvälisen sopijakumppanin välisessä sopimuksessa on sovittu.

Esimerkiksi EU:n turvallisuusluokiteltua[1] tietoa käsitellään useissa valtionhallinnon virastoissa ja laitoksissa ja tältä käsittelyltä edellytetään tiedon omistajan (toimivaltaisen viranomaisen) vaatimusten täyttämistä. Koska kansalliset ja kansainväliset suojausvaatimukset eroavat tietyin osin, on tässä ohjeessa pyritty tuomaan esille joitakin keskeisiä lisäsuojausvaatimuksia, joita kansainvälisen aineiston käsittely edellyttää. Eroavaisuudet tullaan kuvaamaan valmisteilla olevassa NSAn ”Kansainvälisen tietoaineiston käsittelyohjeessa”. Kaikkia vaatimuksia ei välttämättä voida toteuttaa sellaisenaan kaikissa sisäverkkokokoonpanoissa.

Tässä ohjeessa on pyritty esittämään tuote- ja toimittajariippumattomasti sisäverkkojen tietoturvallisuutta edistävät toimenpiteet. Tekniset ratkaisut kehittyvät jatkuvasti. Ohje on pyritty rakentamaan siten, että siitä on hyötyä myös uusien sisäverkkoteknologioiden käyttöönotossa.

Organisaation johto voi käyttää ohjetta hallinnollisten ja organisatoristen velvollisuuksiensa selvittämiseen sekä vastuualueiden ja tehtävien jakamiseen. Sisäverkon vastuuhenkilöt voivat käyttää ohjetta verkkojensa tietoturvallisuuden arviointiin, tietoturvallisuutta parantavan toimenpideohjelman laatimiseen ja tarvittavien muutosten tekemiseen.

---

[1] turvallisuusluokitellulla tiedolla tarkoitetaan viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2 ja 7—10 kohdissa tarkoitettuja tietoja

Organisaatiokohtaisen arvioinnin perusteella tulee harkita tarvittavat toimenpiteet. Toimenpiteissä on otettava huomioon verkossa käsiteltävien tietoaineistojen luokitus sekä yhteen sovitettava tarkoituksenmukaisuus-, taloudellisuus- ja tehokkuusvaatimukset.

Ohje pyrkii vaikuttamaan siihen, että tietojärjestelmien tietoturvallisuudesta huolehtiminen kokonaisuutena olisi vakioitujen ja hyväksyttävien menettelytapojen mukaista. Tällöin tietoturvallisuuden taso ei riipu yksittäisestä kulloinkin vastuussa olevasta henkilöstä, mikä kokonaisuutena parantaa myös järjestelmien tietoturvallisuutta. Ohjetta käytettäessä on syytä muistaa, että tietojärjestelmiin liittyvät tietoturvatarpeet ovat erilaisia. Siten mm. tarkoituksenmukaisuus-, taloudellisuus- ja tehokkuussyistä kaikkien järjestelmien osalta ei ole välttämättä tarvetta edes pyrkiä vaativimmalle tasolle. Suojattavien kohteiden rajaamisella saavutetaan näin kustannustehokkuutta.

Ohjeessa ei käsitellä sisäverkon sovelluksia, palvelimia tai päätelaitteita lukuun ottamatta näiden verkkoliitäntöjä. Poikkeuksena ovat verkon toiminnan kannalta olennaiset esimerkiksi ns. infrastruktuurisovellukset. Niiltä osin kuin ohjeen aihepiiriin liittyvistä osa-alueista on jo annettu erilliset suositukset tai ohjeet (esim. ulkoistus, etätyö, tietoaineistojen käsittely, virustorjunta, tietojärjestelmäkehitys), viitataan tekstissä kyseisiin dokumentteihin. VAHTI-ohjeet on listattu kappaleessa 19. Ohjeen lukemista helpottaa erityisesti Valtionhallinnon tietoturvasanasto (VAHTI 8/2008).

A.3 Ohjeen rakenne

Johdanto ohjaa lukijan aihepiiriin ja valottaa hieman hankkeen taustaa. Tämän jälkeen määritellään tarkemmin kohde eli sisäverkko, joka nykyisellään ei ole yhtä yksiselitteinen kuin aikanaan – tai ainakin sitä käytetään laajemmissa yhteyksissä.

Seuraavaksi, kappaleessa 3, esitellään lyhyesti yleisimmät tietoliikennemallit ja protokollat. Tämä luo teoreettisen pohjan kappaleen 4 palvelulähtöiselle näkökulmalle verkon eri tasoihin.

Kappaleessa 5 käydään läpi sisäverkon rakenne. Tämän jälkeen tuodaan esiin sisäverkkojen tietoturvallisuuden kannalta keskeiset suojattavat kohteet ja niitä uhkaavat tekijät. Omana kappaleenaan on käsitelty nykymaailmassa yhä tärkeämmäksi muodostunutta yhteistyökumppanien ja toimittajaverkoston kanssa toimimista.

Kappaleesta 9 lähtien käydään läpi sisäverkon eri osa-alueita, kaapeloinnista verkon laitteiden kautta verkon palveluihin. Langattomat lähiverkot käsitellään omana kappaleenaan.

Kappaleiden perusrakenne on samanlainen. Kappaleen alussa on johdanto aihe-alueeseen. Teknologiatausta-osio on informatiivinen ja siinä on pyritty esittelemään sellaiset asiat, jotka ovat alttiimpia teknologian vanhentumiselle.

Tarkistuslista sisältää alueeseen liittyvät vaatimukset. Kaikki vaatimukset kattava eri alueiden tarkastuslistojen yhteenvetotaulukko on ladattavissa sähköisesti Valtion IT-palvelukeskuksen (VIP) sivuilta tämän ohjeen kanssa.

Suosituksen jälkimmäinen puolisko käsittelee tietoturvallisuuden kannalta tärkeitä tunnistautumista, verkon hallintaa ja valvontaa sekä jatkuvuussuunnittelua.

Lopuksi esitetään kootusti virastoilta edellytettävät toimenpiteet ja niihin liittyvät valvontamenettelyt.

Ohjeessa käytetään seuraavia tietoturvallisuusasetuksen ja sen täytäntöönpanon ohjeen VAHTI 2/2010 mukaisia tietoturvatasoja:

- **Perustaso**
- **Korotettu taso**
- **Korkea taso**

Eri tietoturvatasoilla käytetään seuraavia termejä kuvaamaan kontrollien tärkeyttä ja toteuttamisvelvollisuutta:

- **Pakollinen vaatimus:** Organisaation täytyy ottaa tämän ohjeen mukainen toiminto käyttöön. Poikkeuksen voi tehdä vain siinä tapauksessa, että kirjallisen riskianalyysin mukaan siitä seuraa vain pieni riski ja toiminnon toteuttaminen vaatii runsaasti resursseja sekä verkon omistaja hyväksyy etukäteen toteutettavan ratkaisun. Kansainvälisen turvallisuusluokitellun aineiston osalta Viestintäviraston NCSA-FI-yksikön on hyväksyttävä etukäteen toteutettava ratkaisu kirjallisesti. Riskianalyysiin on saatavilla VIP:in Tietoturvapalveluista prosessiohje ja työväline.
- **Vahva suositus:** Organisaatio voi tehdyn kirjallisen riskianalyysin perusteella olla ottamatta suosituksen mukaista toimintoa käyttöön. Riskianalyysiin on saatavilla VIP:n Tietoturvapalveluista prosessiohje ja työväline.
- **Suositus:** Hyvä käytäntö, jonka organisaatio voi halutessaan ottaa käyttöön.

Tässä ohjeessa kontrollin velvoittavuus tulee kunkin osa-alueen yhteydessä olevista, kontrollit sisältävistä tarkastuslistoista, ei tekstisisällöstä.

1 Johdanto

Lähiverkkojen perustavoitteita olivat ja ovat edelleen datan ja resurssien jakamisen sekä käyttäjien välisen viestinnän mahdollistaminen. Lähiverkon rajaus maantieteellisesti pienelle alueelle (esim. yksittäiseen rakennukseen tai rakennusryhmään) ei kuitenkaan nykyisellään ole mielekästä. Lähiverkon palveluita käytetään yhä enemmän etäyhteyksien kautta maantieteellisesti pitkien yhteyksien yli. Yksittäisellä organisaatiolla on myös useampia toimipisteitä, jotka verkkoarkkitehtonisesti ovat yhtä ja samaa verkkoa. Lähiverkko-termin sijasta tässä ohjeessa tullaankin puhumaan organisaation sisäisestä tietoverkosta, lyhyemmin sisäverkosta.

Riippuvuus verkon toiminnasta näyttää kasvavan jatkuvasti: käyttäjien väliset yhteydet, tulostus, levyjaot, asiakas/palvelin -sovellukset, p2p-sovellukset (peer-to-peer), intranet-palvelut, ulkoiset yhteydet jne. Organisaation toiminnan riippuvuus tietojärjestelmistä ja palveluista korostaa sisäverkon toiminnan tärkeyttä. Riippuvuuden kasvaessa myös tiedon eheys-, käytettävyys- ja luottamuksellisuusvaatimukset ovat kasvaneet ja toisaalta organisaatioiden haavoittuvuus on lisääntynyt. Aikaisemmasta virka-ajan palvelutasoluokka-ajattelusta (SLA) on siirrytty vahvemmin 24/7*365-tyyppiseen malliin, jossa lyhytkin verkkokatko virka-ajan ulkopuolella voi aiheuttaa merkittäviä kustannuksia ja ongelmia.

Sisäverkkoa voidaan katsoa eri näkökulmista. Tässä ohjeessa on valittu palvelulähtöinen ajattelumalli, jossa kaikki verkon resurssit näkyvät käyttäjälle palveluina. Tulostus, levyjaot ja intranet ovat kaikki palveluita, jotka voidaan toteuttaa joko perinteisellä asiakas/palvelin -mallilla tai p2p-ratkaisuna – käyttäjän kannalta oleellista on tietää miten palveluun pääsee käsiksi ja mikä on palvelun sisältö ja tarkoitus. Toisena ääripäänä ovat fyysiset laitteet, joiden avulla palveluita käytetään. Väliin asettuu verkon arkkitehtuuri ja rakenne sekä tietoliikenne, jotka mahdollistavat laitteiden välisen viestinnän.

Sisäverkko voidaan rakentaa useilla tavoilla. Verkon rakenteella voidaan viitata joko verkon fyysiseen tai loogiseen rakenteeseen. Verkon looginen rakenne voi pitää sisällään useamman fyysisen verkon (esim. lankaverkko + langaton verkko), toisaalta yksi fyysinen verkko voidaan jakaa useampaan loogisesti erilliseen kokonaisuuteen (VLAN, virtual local area network, virtuaaliverkkoihin). Vastuu verkon rakenteen suunnittelusta, ylläpidosta ja dokumentoinnista tulee olla selkeästi määritelty ja dokumentoitu. Ilman huolellista suunnittelua

sisäverkko jää alttiiksi verkkoon kohdistuville hyökkäyksille ja muille vahingollisille tapahtumille.

Sisäverkkoon liitettäviä ja verkon muodostavia tuotteita ja niiden valmistajia on runsaasti. Erilaisten päätelaitteiden (mm. työasemat), palvelinlaitteiden, kaapelointiratkaisujen, käyttöjärjestelmien ja niiden versioiden, verkkokorttien ja muiden verkon komponenttien erilaisia yhdistelmiä on muodostettavissa markkinoilla yleisesti tunnetuillakin tuotteilla tuhansittain. Teknologia kehittyy jatkuvasti, joten sopivaa teknologista ratkaisua ja tuotetta valittaessa tulee olla huolellinen ja mielellään pitäytyä jo tunnetussa, käytössä hyviksi havaituissa ratkaisuissa.

Verkolla on oltava nimetty omistaja, joka pystyy tekemään päätöksiä verkon suhteen. Tavallisesti verkon ylläpito on delegoitu vastuuhenkilöille (pääkäyttäjät, ”administraattorit”) tai ulkopuolisille organisaatioille. Verkon omistaja on organisaation sisältä, mutta ylläpitäjä voi olla ulkoistettu. Etenkin pienimpien organisaatioiden sisäverkkojen vastuuhenkilöt on nimetty tähän vastuulliseen tehtävään usein oman päätoimensa ohella. Tällä on vaikutuksensa syvällisen osaamisen kehittämisessä, mikä korostuu verkon suunnittelussa, muutostilanteissa, tietoturvavaatimusten toimeenpanossa sekä toimintavalmiudessa poikkeuksellisissa tilanteissa.

Valtionhallinnon organisaatioilla on lisääntynyt tarve suojattujen palvelujen järjestämiseen sisäverkkorakenteita hyödyntäen. Toisaalta eri viranomaiset ovat järjestäneet kansalaisille yhteisiä palvelupisteitä, jolloin palvelupisteen työasemilta saattaa olla tarvetta päästä useamman viranomaisen sisäverkkoresursseihin.

Tekniset mahdollisuudet liittää kiinteistövalvonta ja puhelinjärjestelmän komponentit muiden tietojärjestelmien kanssa samaan sisäverkkoon sekä langattomien ja virtuaalisten sisäverkkoratkaisujen markkinoille tulo nostavat esille ajankohtaisia tietoturvallisuuteen liittyviä kysymyksiä.

Sisäverkkojen rakentamista ei ole normitettu samoin kuin televerkkoja. Kansallinen turvallisuusauditointikriteeristö (KATAKRI) asettaa turvallisuusvaatimuksia verkoille, joissa käsitellään kansainvälisiä turvallisuusluokiteltuja tietoaineistoja. Kansainvälisiä aineistoja käsitteleville verkoille on lisäksi tiedon omistajan erikseen määrittämiä normeja. Sähköisen viestinnän ohjeistus koskee sisäverkkoja silloin kun niistä on suora yhteys internet-verkkoon.

Sisäverkon suojaamisen tulee perustua riskianalyysiin, jonka osana kartoitetaan organisaation tietoon liittyvät uhat ja vaatimukset sekä turvallisuustarpeet. Riskianalyysissä tulee miettiä, miten arvokas tieto on, mitä uhkia siihen kohdistuu, miten todennäköistä uhkien realisoituminen on ja mitä eri suojausmenetelmät maksavat. Näiden perusteella voidaan päättää, miten sisäverkon tulee suojata näitä tietoja.

Valtionhallinnon organisaatioiden tietojen luokittelu perustuu lakiin viranomaisten toiminnan julkisuudesta (621/1999), siihen liittyvään asetukseen viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta

(1030/1999), asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010) sekä lakiin kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Luokiteltava tietoaineisto voidaan luokitella neljään luokkaan. Tietoturvallisuusasetuksen täytäntöönpanoon liittyviä toimenpiteitä ohjaamaan on laadittu yleisohje; Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010). Ko. ohjeessa on määritelty myös tietoturvatasoluokittelu sekä linjaukset perus, korotetulle ja korkealle tietoturvatasolle.

Nykyaikainen toimintaympäristö vaatii useiden yhteistyökumppanien kanssa toimimista ja heidän päästämistä toimimaan organisaation omassa sisäverkossa. Yhteystyökumppani voi toimia sisäverkossa käyttäjän, kehittäjän, ylläpitäjän, palvelutuottajan tai palveluntarjoajan roolissa. Samassa roolissa ja sisäverkossa voi olla myös useita toimijoita, jolloin on tärkeää määritellä, kulkevatko kaikki tieto ja viestit organisaation kautta vai voivatko eri toimijat viestiä suoraan keskenään.

Sisäverkoissa kulkee tietoaineistojen luottamuksellisuuden ohella myös käyttäjien yksityisyyden suojan kannalta tärkeää tietoa. Lähiverkon vastuuhenkilöiden tulee tuntea voimassa oleva lainsäädäntö (kuten laki yksityisyyden suojasta työelämässä, sähköisen viestinnän tietosuojalaki, henkilötietolaki, tietoturvallisuusasetus) sekä noudattaa laeissa sekä näistä johdetuissa organisaation toimintaohjeissa ja määräyksissä esitettyjä käytäntöjä.

Tässä ohjeessa esitettyjen suositusten toimeenpanosta ja valvonnasta vastaa organisaation johto. Johdon tulee valtuuttaa sisäverkosta ja tietoturvallisuudesta vastaavat henkilöt toteuttamaan suositukset sekä järjestämäämään yksityiskohtaisen seurannan toimenpiteiden toteutumisesta. Mikäli organisaatio ei pysty tai halua perustellusta ja kirjatusta syystä toteuttaa suositusten mukaista sisäverkkoa, tulee tämä hyväksyttää etukäteen tiedon omistavalla taholla (toimivaltaisella viranomaisella). Syy poikkeamaan tulee myös dokumentoida selvästi. Johdolla tulee olla käsitys siitä, vastaako verkon tietoturvallisuus tässä ohjeessa esitettyjä vaatimuksia.

2 Mikä on sisäverkko

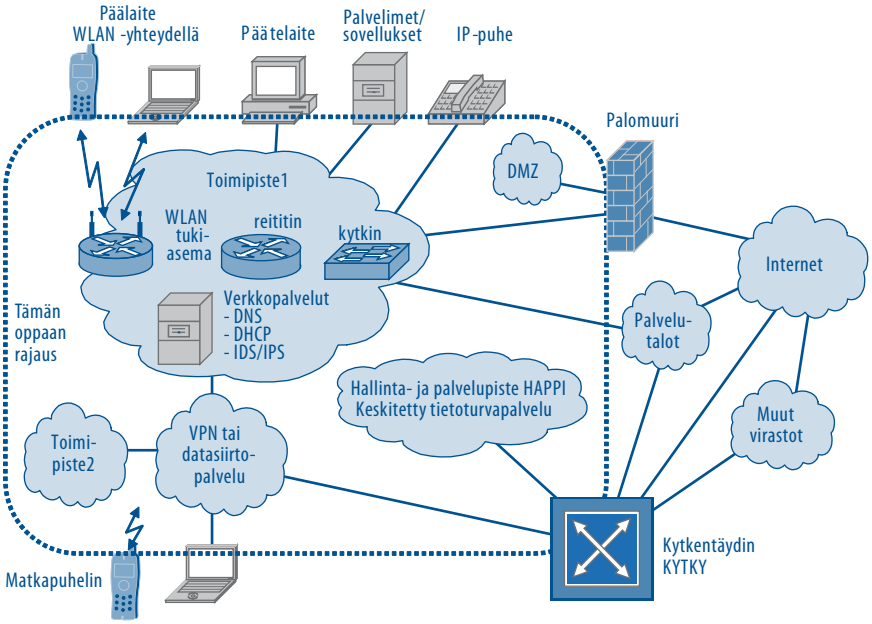
Lähiverkko (LAN, Local Area Network) on rajatun alueen nopea tietoliikenneverkko. Lähiverkko on tämän ohjeen tarkoitusta varten laajennettu käsittämään organisaation sisäisen loogisen tietoverkon sisältäen muiden toimipisteiden verkot, näiden väliset loogiset yhteydet sekä yksittäiset etäkäyttäjät. Tästä syystä on päädytty käyttämään lähiverkon sijasta termiä sisäinen tietoverkko, lyhyemmin sisäverkko. Verkkojen rakentamiseen liittyvät komponentit – toistimet, kytkimet, reitittimet sekä langattomien verkkojen tukiasemat – sekä verkon toimintaan kiinteästi liittyvät palvelut ja palvelimet, kuten DNS-nimipalvelut (Domain Name System) ja DHCP-osoitepalvelu (Dynamic Host Configuration Protocol) kuuluvat ohjeen piiriin. Protokollana verkoissa on IP-protokollaperhe. Tämä ohje soveltuu sekä IPv4- että IPv6-protokollia käyttäviin verkkoihin.

Valtion yhteinen turvallinen tietoliikenneratkaisu (VY-verkko) tarjoaa kaikille valtion virastoille nopean, luotettavan ja turvallisen tavan kytkeytyä valtion yhteisiin palveluihin, toisiinsa sekä ulkoisiin palveluihin kuten Internetiin. VY-verkko muodostaa siihen liittyneiden virastojen välisen valtion sisäisen lähiverkon.

VY-verkko sisältää mm. seuraavat komponentit:

- Tietoliikenteen solmupiste eli kytkentäydin (KYTKY), joka koostuu maantieteellisesti hajautetuista kytkentäpisteistä. Verkko on suunniteltu niin, että paikalliset häiriöt, kuten onnettomuudet tai katastrofit eivät vaikuta palvelun toimintakykyyn.
- Hallinta- ja palvelupiste (HAPPI), joka huolehtii kytkentäytimestä ja sen kautta virastoille järjestettävistä palveluista. Se valvoo kytkentäytimen toimintaa ympärivuorokautisesti, korjaa häiriötilanteita sekä tiedottaa niistä.
- Keskitetty tietoturvapalvelu, joka sisältää virastokohtaiset palomuurit, tunkeilijan tunnistuksen (IDS, Intrusion Detection System) ja eston (IPS, Intrusion Prevention System) sekä suodatukset ja haittaohjelmien torjunnan sähköposti- ja www-liikenteessä. Palvelunestohyökkäysten torjunta tehdään VY-verkon internet-operaattoreiden verkoissa.

Kuva 1 Sisäverkon tietoturvallisuuden osa-alueet ja tämän ohjeen rajaus.



Sisäverkossa voi olla tietoturvatasoltaan erilaisia rooleja tai alueita. Tavallisesti nämä toteutetaan muodostamalla samaan fyysiseen verkkoon erillisiä palomuurilla tai pääsylistoilla suojattuja fyysisiä tai loogisia virtuaalisia verkkoja (VPN, Virtual Private Network). Esimerkkejä näistä virtuaaliverkoista ovat virtuaaliset lähiverkot (VLAN, Virtual LAN), operaattoreiden käyttämän MPLS-tekniikan (Multiprotocol Label Switching) VRF:t (VPN Routing and Forwarding) sekä salauksen avulla muodostetut IPSec- ja SSL-VPN:t (IP Security Architecture VPN, Secure Sockets Layer VPN). Sisäverkon laite voi olla yhdessä tai useammassa virtuaaliverkossa samanaikaisesti. Esimerkkejä erityyppisistä virtuaaliverkoista:

- Tuotantoverkko tai toimistoverkko on verkko, johon käyttäjät työasemineen tyypillisesti liittyvät.
- Ylläpitoverkon kautta hallitaan verkon aktiivilaitteita. Tämän tyyppisessä verkossa käyttäjä on tunnistettava vahvasti. Ylläpitoverkko voi olla tuotantoverkosta kokonaan erotettu, jolloin tuotantoverkon vikatilanteet eivät estä laitteiden hallintaa. Ylläpitoverkkoon kuuluu lisäksi päätepalvelin, ts. laite, jonka kautta saadaan muodostettua konsoliyhteyksiä hallittaviin aktiivilaitteisiin (verkon kytkimet, reitittimet ja vastaavat laitteet).
- Resurssiverkko tai palvelinsisäverkko sisältää palvelinlaitteita.

- Testiverkossa testataan laitteita, ohjelmia ja kokoonpanoja, jotka mahdollisesti aiheuttavat vaaraa tai haittaa tuotantoverkon käyttäjille.
- DMZ (demilitarized zone) on verkon alue, joka sisältää internetistä tai muusta verkon turvattomammasta alueesta käsin käytettäviä laitteita. DMZ-verkkoon sijoitetaan tavallisesti internet-käyttöön tarkoitetut palvelimet (www, ulkoinen DNS) ja yhdyskäytävät esimerkiksi sisäverkkoon.
- Vierailijaverkon suojaustaso on alhaisin, pääpaino on satunnaisten käyttäjien helpolla ja nopealla liittymisellä.

Tässä ohjeessa sisäverkko tarkoittaa tuotantosisäverkkoa ja sen tietoturvavaatimuksia ellei erikseen muuta mainita.

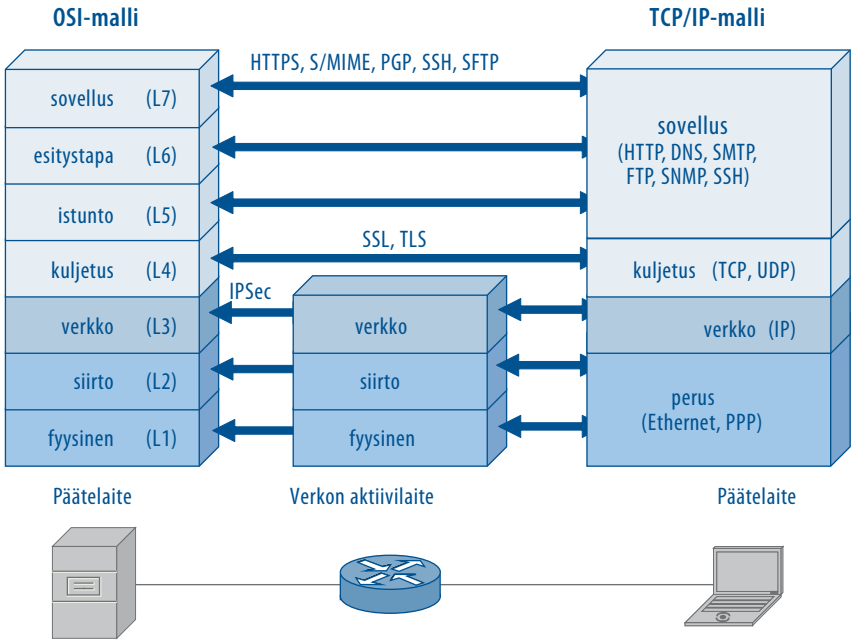
3 Tietoliikennemallit

Verkon perustehtävä on mahdollistaa verkkoon kytkettyjen laitteiden välinen vuorovaikutus. Onnistunut vuorovaikutus edellyttää yhtenäistä kieltä, jossa määritellään käytettävä sanasto, kielioppi ja säännöstö. Verkossa vuorovaikutusta kutsutaan tietoliikenteeksi ja kieltä yhteyskäytännöksi (protokolla, protocol).

Kahden sovelluksen välinen vuorovaikutus tapahtuu useassa kerroksessa, useaa yhteyskäytäntöä hyödyntäen. Tätä kuvaamaan on kehitetty ns. OSI-malli, jossa kerroksia on seitsemän.

Internetissä tiedonsiirto perustuu TCP/IP-protokollaperheen protokolliin. Tässä ympäristössä OSI-mallista on kehitetty yksinkertaistettu TCP/IP-verkkomalli, jossa kerroksia on neljä. Kuva 2 havainnollistaa OSI- ja TCP/IP-mallien suhdetta toisiinsa. Käytännössä vastaavuus ei ole aivan yhtä suoraviivainen kuin kuvassa 2.

Kuva 2 Verkkomalleja. L-kirjain (L=Layer) viittaa mallin kerrokseen. Suluissa olevat kirjainlyhenteet ovat esimerkkejä protokollista kyseisellä kerroksella. Nuolien päällä on esitetty eräitä salausta käyttäviä turvaprotokollia.



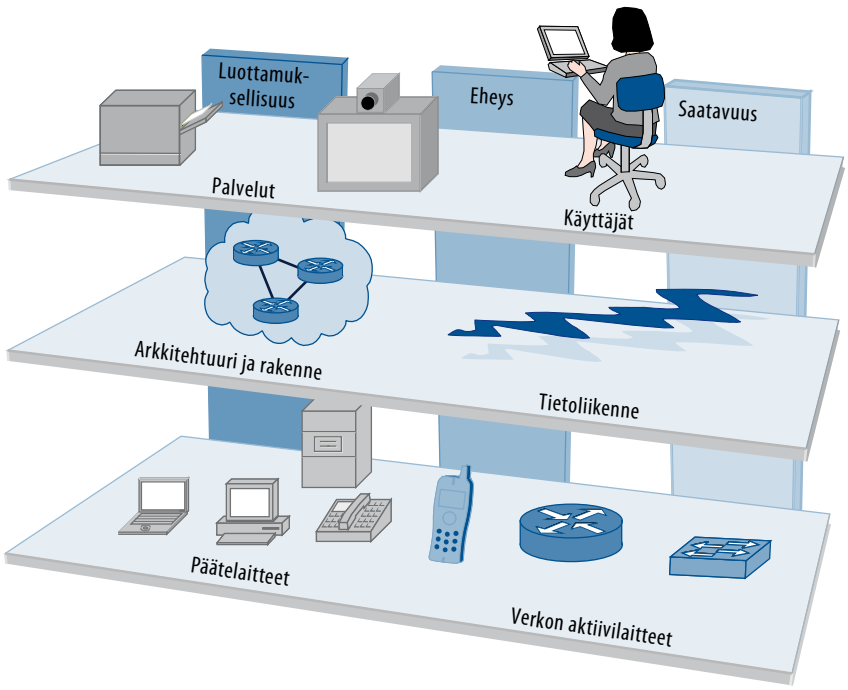
4 Verkon eri tasot

Tässä kappaleessa kuvataan verkkoa palvelulähtöisesti, ks. kuva 3.

Tietoturvanäkökulmasta verkon tulee täyttää vähintään alla listatut vaatimukset. Nämä on esitetty kuvassa pystypalkkeina, kuvastaen sitä että kaikki verkon tasot osallistuvat kyseisten vaatimusten toteuttamiseen.

a) Luottamuksellisuus, Confidentiality (tieto on vain valtuutettujen käyttäjien ulottuvilla)
b) Eheys, Integrity (tieto on vain valtuutettujen käyttäjien muokattavissa, eikä tieto muutu hallitsemattomasti esim. häiriötilanteissa)
c) Saatavuus, Availability (tieto on valtuutettujen käyttäjien saatavilla, kun he sitä tarvitsevat)

Kuva 3 Verkon tasot – palvelukeskeinen ajattelumalli



4.1 Palvelut

Palvelulähtöisessä ajattelumallissa kaikki verkon resurssit näkyvät käyttäjälle palveluina. Levyjako, verkkotulostaminen, sähköposti ja intranet ovat kaikki palveluita. Käyttäjän kannalta oleellista on tietää miten palveluun pääsee käsiksi ja mikä on palvelun sisältö ja tarkoitus.

Palvelulähtöinen ajattelumalli ei ole rajoitettu perinteiseen asiakas-/palvelin-arkkitehtuuriin vaan palvelun toteuttamiseen voi osallistua useampi palvelin tai vaikka asiakaskin. Perinteiset verkkolaitteiden roolijaot siis hämärtyvät.

Palveluiden saatavuus voidaan turvata erilaisilla kahdennusratkaisuilla.

Luottamuksellisuutta ja eheyttä pyritään varmistamaan palvelukohtaisella käyttäjänhallinnalla sekä mahdollisella salauksella ja lokituksella.

Sisäverkon palveluita käsitellään tarkemmin kappaleessa 14.

4.2 Laitteet

4.2.1 Päätelaitteet (työasemat)

Päätelaitteiden päätarkoituksena on tarjota käyttäjälle rajapinta (verkon) palveluihin. Päätelaite voi myös osallistua palvelun tuottamiseen, mutta käyttäjälle se on läpinäkyvää.

Tyypillinen päätelaite on työasema, joko pöytäkone tai kannettava. Käyttöjärjestelmä on oleellinen osa päätelaitetta.

Saatavuus ei päätelaitteiden osalta yleisesti ottaen ole kriittinen vaatimus, mikäli palvelu toimii kokonaisuudessaan verkossa. Tällöin riittää yksinkertaisesti päätelaitteen vaihtaminen. Erilaisilla varalaitejärjestelyillä minimoidaan käyttäjän havaitsema katkoaika. Mikäli palvelu edellyttää erityistä logiikkaa päätelaitteelta tai säilyttää jotain tietoja päätelaitteella, saatavuusongelmien vaikutukset minimoidaan toimivilla varmistusratkaisuilla. Suositus on käyttää kokonaisuudessaan verkossa toimivia palveluita.

Luottamuksellisuus ja eheys varmistetaan päätelaitteen käyttäjänhallinnalla ja tarvittaessa päätelaitteen salauksella ja lokituksella.

Sisäverkon päätelaitteita käsitellään tarkemmin kappaleessa 13.

4.2.2 Aktiivilaitteet (kytkimet ja vastaavat laitteet)

Aktiivilaitteiden tehtävänä on tiedonsiirto eli tietoliikenteen mahdollistaminen fyysisellä tasolla.

Saatavuus varmistetaan kahdennuksilla, hot-swap komponenteilla ja varmennetulla virransyötöllä.

Luottamuksellisuus ja eheys varmistetaan käyttäjänhallinnan keinoin ja fyysisillä suojauksilla (laitetilojen lukitus).

Verkon aktiivilaitteita käsitellään tarkemmin kappaleessa 11.

4.3 Verkko

4.3.1 Arkkitehtuuri ja rakenne

Verkon arkkitehtuuri kuvaa verkon kokonaisuutena, joka käsittää sekä verkon fyysisen että loogisen rakenteen. Verkon looginen rakenne voi pitää sisällään useamman fyysisen verkon (esim. lankaverkko + langaton verkko) ja toisaalta yksi fyysinen verkko voidaan jakaa useampaan loogisesti erilliseen kokonaisuuteen (virtuaaliverkkoihin).

Saatavuus varmistetaan kriittisten reittien kahdentamisella sekä vikasietoisilla teknologiavalinnoilla.

Luottamuksellisuus ja eheys varmistetaan fyysisin keinoin (kaapelien suojaukset jne.).

Verkon rakennetta käsitellään tarkemmin kappaleessa 5. Fyysinen toteutus voidaan tehdä joko kaapeloinnilla (ks. kappale 9) tai langattomilla ratkaisuilla (ks. kappale 10).

4.3.2 Tietoliikenne

Tietoliikenteen eli verkkoon kytkettyjen laitteiden välisen vuorovaikutuksen mahdollistaminen on verkon perustehtävä. Tietoliikennemalleja käsiteltiin kappaleessa 3.

Tietoliikenneprotokollat huolehtivat tiedonsiirrosta käyttäjän rajapinnan (käyttöliittymä) ja palvelun tarjoajan (yksittäinen tai hajautettu sovellus) välillä.

Saatavuus varmistetaan oikeilla protokollavalinnoilla. IP-protokolla perustuu pakettikohtaiseen reititykseen, jolloin ongelmatilanteessa oikein toimiva reititysprotokolla ohjaa liikenteen toimivaa reittiä pitkin (edellyttäen että vaihtoehtoinen reitti on olemassa).

TCP/IP-perusprotokollat eivät pääsääntöisesti takaa tiedon luottamuksellisuutta ja eheyttä. *Luottamuksellisuus* voidaan taata erilaisilla salausratkaisuilla. *Eheyden* varmistaminen edellyttää osapuolten tunnistamista ennen kommunikoinnin aloittamista. Tiedon hallitsematon muuttuminen esim. häiriötilanteessa voidaan estää tarkistesummilla ja uudelleenlähetyksillä – TCP-protokolla turvaa eheyttä tällä tasolla, UDP-protokollassa vastaavaa ominaisuutta ei ole.

5 Verkon rakenne (arkkitehtuuri)

Verkon rakenteella voidaan viitata joko verkon fyysiseen tai loogiseen rakenteeseen. Verkon looginen rakenne voi pitää sisällään useamman fyysisen verkon (esim. lankaverkko ja langaton verkko) ja toisaalta yksi fyysinen verkko voidaan jakaa useampaan loogisesti erilliseen kokonaisuuteen, joita kutsutaan myös virtuaaliverkoiksi.

Tästä luvusta alkavat sisäverkoille asetetut vaatimukset.

Verkolle on määritelty omistaja [Vaatimus 5.1]. Verkon rakenne ja vastuu verkon suunnittelusta ja ylläpidosta on selkeästi määritelty ja dokumentoitu [Vaatimus 5.2].

Verkkoinfrastruktuurin hankintaan ja kehittämiseen on olemassa määrämuotoinen prosessi [Vaatimus 5.3]. Muutokset verkkoon testataan, katselmoidaan ja toteutetaan muutoshallintaprosessin mukaisesti [Vaatimus 5.10]. Verkon rakenne on suunniteltu kestämään nykyinen ja arvioitu tuleva liikennemäärä [Vaatimus 5.19].

Päätelaitteiden yhdistäminen verkkoon on tehty tähtimäisillä rakenteilla (ns. tähtitopologia) hallinnan ja ylläpitämisen helpottamiseksi. ”Tähden” keskipiste (esim. kytkin), luetaan kriittiseksi verkon komponentiksi, koska sen vikaantuminen vaikuttaa esimerkiksi kaikkiin siihen liitettyjen työasemien verkkoyhteyksiin. Työryhmäkytkimiä ei yleensä tulkita kriittisiksi komponenteiksi. Kriittiset verkon komponentit on kahdennettu [Vaatimus 5.15].

Verkkoliitännät aula-/kokous-/koulutustiloissa on suojattu siten, että organisaation sisäverkkoon on pääsy ainoastaan sallituilla osapuolilla [Vaatimus 5.9].

Verkon ylläpitäjille järjestetään säännöllistä tietoturvakoulutusta [Vaatimus 5.18]. Säännöllisyys tarkoittaa tässä ohjeessa sitä, että asia on viraston omassa harkinnassa. Toistaminen ja ajoittaminen on kuitenkin kirjattava, esim. organisaation vuosikellon mukaisesti kerran vuodessa.

Vaihtoehtoiset tiedonsiirtoreitit ja -resurssit on toteutettu, dokumentoitu ja hyväksytetty asianmukaisilla tahoilla [Vaatimus 5.14].

5.1 Tietoturvallisuustason vaikutus verkon rakenteeseen

Verkkojen rakenteeseen vaikuttaa merkittävästi se, minkä tietoturvallisuustason verkko on kyseessä. Verkot jaetaan perus-, korotetun ja korkean tason

verkkoihin ja tietoverkoissa käsiteltävät tiedot suojaustasoihin (ST I – ST IV). Lähtökohtaisesti suojaustason IV tietoa voidaan kuljettaa perustason verkoissa ja suojaustason III tietoa korotetun tason verkoissa salaamattomana (tämä edellyttää että kaikki kyseisen tason vaatimukset täyttyvät).

Perustason verkkoja on mahdollista kytkeä internetiin ja muihin ei-luotettuihin verkkoihin, kunhan perustason muut vaatimukset täyttyvät. Valtionhallinnon toimistoverkot ovat tyypillisesti perustason verkkoja.

Korotetun tason verkkoja on mahdollista kytkeä internetiin ja muihin ei-luotettuihin verkkoihin, kunhan korotetun tason vaatimukset täyttyvät. Lähtökohtaisesti VY-verkko on korotetun tason verkko. Valtion kytkentäydintä ja Hansel-puitejärjestelyin hankittuja tietoliikenneliittymiä hyödyntävät virastoverkot voidaan auditoida korotetulle tasolle, mikäli virastoverkon tietoturva muutoin täyttää korotetun tason vaatimukset. Jos sisäverkossa halutaan käsitellä myös kansainvälistä turvallisuusluokiteltua tietoa, tulee sisäverkon täyttää kansainväliset lisävaatimukset. Lisätietoja kansainvälisistä turvallisuusvaatimuksista saa Viestintäviraston NCSA-FI-yksiköstä. Ennen kuin verkkoa ja/tai järjestelmää voidaan käyttää kansainvälisen turvallisuusluokitellun tiedon käsittelyyn, toimivaltaisen turvallisuusviranomaisen tulee tarkastaa ja hyväksyä se (akkreditointi).

Korkean tason verkot ovat fyysisesti ei-luotetuista verkoista eristettyjä kokonaisuuksia. Korkean tason verkkoihin ei pääsääntöisesti kytketä mitään muita verkkoja. Toimivaltainen viranomainen voi tapauskohtaisesti hyväksyä korkean tason verkon kytkemisen erikseen tarkastettuun ja hyväksyttyyn verkkoon. Korkean tason verkot ovat tyypillisesti pieniä, fyysisesti vahvasti suojattuja ja ne eivät sisällä muihin järjestelmiin kytkettyjä infrastruktuuripalveluita. Korkean tason verkoissa on mahdollista käsitellä suojaustason II tietoja salaamattomana.

5.2 Verkkojen jaottelu käyttötarkoituksen mukaan

Verkot jaetaan käyttötarkoituksensa mukaan loogisesti erillisiin aliverkkoihin, esim. sisäiseksi, ylläpito- (hallinta-/valvonta-), resurssi-, testi- tai asiakasverkoksi [Vaatimus 5.20]. Palomuurin yhteydessä tavallisesti sijaitseva DMZ on myös oma verkkoalueensa. Verkon käyttötarkoitus määrittää myös sen käyttäjäkunnan ja antaa tietyt pohjavaatimukset verkon suojaukselle ja eriyttämiselle. Eri verkot tai niiden osat on eristetty toisistaan loogisesti tai fyysisesti [Vaatimus 5.5].

Hallinta-/valvontatoiminta on erotettu muusta verkon liikenteestä esim. loogisesti erilliseen verkkoon [Vaatimus 5.11].

Kaikkien toimintojen keskittäminen samaan verkkoon lisää entisestään haavoittuvuusriskiä ja kaikkien järjestelmien riippuvuutta yhteisen resurssin toimivuudesta. Mikäli yhdistämistä kuitenkin harkitaan esim. taloudellisista syistä, käsitellään asia huolellisesti muun muassa riskien arvioinnin yhteydessä.

Verkkojen väliset yhteydet on kartoitettu ja hyväksytetty asianmukaisilla tahoilla [Vaatimus 5.12].

Fyysinen verkko on jaettu vyöhykkeisiin eri käyttötarkoituksien mukaan. [Vaatimus 5.23].

5.3 Ulkoiset yhteydet

Ulkoiset yhteydet on rakennettu keskitettyjen pisteiden kautta [Vaatimus 5.13]. Liikennettä sisä- ja ulkoverkon välillä rajoitetaan siten, että vain tarpeellinen liikenne päästetään läpi [Vaatimus 5.6]. Rajoitus suoritetaan teknisesti esim. palomuurin avulla.

Etäkäyttöyhteyksiä voidaan avata sisäverkkoon kontrolloidusti, tiettyihin rajoitettuihin palveluihin. Etäkäyttöyhteydet salataan. Ylläpitoon tarkoitetut etähallintayhteydet on sallittu ainoastaan ylläpitohenkilöstölle [Vaatimus 5.7]. Lisätietoa löytyy dokumenteista Valtion etätyön tietoturvallisuussuositus (VAHTI 3/2002), Turvallinen etäkäyttö turvattomista verkoista (VAHTI 2/2003) sekä Kansallinen turvallisuusauditointikriteeristö (KATAKRI).

Suorat, ulkoverkosta sisäverkkoon otetut yhteydet on estetty [Vaatimus 5.16]. Ulkoverkkoon tarjottavat palvelut sijaitsevat sisäverkosta erotetulla DMZ-alueella [Vaatimus 5.17].

Suorat, sisäverkosta ulkoverkkoon otetut yhteydet on oletuksena estetty [Vaatimus 5.21]. Lisäksi suositellaan, että vierailijoita varten on määritelty erillinen domain-nimi, esim. vierailija.valtionorganisaatio.fi. Ulkoverkkoon otetaan yhteyttä erityisten välityspalvelinten (proxy) kautta [Vaatimus 5.22].

Verkkoa rakennettaessa on tehty riskianalyysi ulkoisten yhteyksien käyttöön liittyen. Tässä yhteydessä on kartoitettu ulkoisten langattomien verkkojen kuuluvuus toimipisteessä ja päätelaitteiden tuki langattomille verkoille. Riskianalyysin pohjalta on määritelty jatkotoimenpiteet, joilla kahden verkkoyhteyden yhtäaikainen käyttö estetään tarvittaessa.

Sallitut yhteydet ulkoverkosta on dokumentoitu ja hyväksytetty asianmukaisella taholla [Vaatimus 5.8].

5.4 Dokumentaatio

Sisäverkon vastuuhenkilöillä on ajantasainen kuvaus sisäverkon fyysisestä ja loogisesta rakenteesta sekä verkkoon kytketyistä laitteista ja komponenteista. [Vaatimus 5.3]. Dokumentaation on mahdollistettava vioista, toimintahäiriöistä, hyökkäyksistä ja vastaavista toipumisen toimintavaatimusten mukaisesti (vrt. KATAKRI I 702).

Soveltuvilta osin voidaan käyttää verkon hallintaan tarkoitettuja ohjelmistoja, jotka pitävät yllä listaa verkon laitteista ja muodostavat ajantasaisen verk-

kokuvan automaattisesti. Tällöin huolehditaan hallintaohjelmistojen tuottaman tiedon säännöllisestä arkistoinnista ja muutosten syiden yms. kirjaamisesta ohjelmistoon.

Dokumentaatio kattaa vähintään seuraavat osa-alueet

- **Fyysinen arkkitehtuurikuva**, joka kuvaa verkon fyysisen rakenteen eli kaapeloinnit ja verkon aktiivilaitteet. Erityisesti liitäntäpisteet ulkoisiin verkkoihin tulee olla selkeästi merkitty. Fyysisestä arkkitehtuurikuvasta on selvittävä myös vastaavuus fyysisiin liitäntäpisteisiin ja näiden merkintöihin.
- **Looginen arkkitehtuurikuva**, joka kuvaa verkon loogisen rakenteen eli eri verkkoalueet ja mahdolliset virtuaaliverkot (VLAN).
- **Verkon laitelista**, jossa on määritelty vähintään kunkin laitteen osoitetiedot (MAC, IP), omistaja, fyysinen sijainti sekä käyttötarkoitus.
- **Verkon suojaukset**, joissa esitetään verkkoon suunnitellut ja toteutetut rakenteelliset suojaukset.

Laajemmissa verkkokokonaisuuksissa on suositeltavaa varata hallinnolliseen työhön ja dokumentaation sekä verkon ylläpitoon yksi työntekijä täysipäiväisesti. Pienessä organisaatiossa tähän harvoin on mahdollisuus. Tällöin kullekin dokumentaation osalle määritellään erikseen vastuullinen henkilö. Myös dokumentaation versionhallintaan kiinnitetään tällöin erityistä huomiota.

5.5 Teknologiatausta

Nykyisin rakennettavat lankaverkot ovat pääosin Ethernet-verkkoja (IEEE 802.3) ja langattomat verkot (WLAN-verkot) pääosin IEEE 802.11-verkkoja. Langattomia verkkoja käsitellään syvällisemmin kappaleessa 10.

Fyysisen verkon jakaminen useampaan loogisesti erilliseen virtuaaliverkkoon toteutetaan ns. VLAN-tekniikalla. Kyseinen tekniikka, joka on määritelty standardissa IEEE 802.1Q, lisää paketteihin ylimääräisen otsakkeen, jossa kerrotaan mihin virtuaaliverkkoon paketti kuuluu. VLAN-tuen sisältävät kytkimet osaavat lukea tämän ylimääräisen informaation ja ohjata paketit eteenpäin oikein.

5.6 Verkon rakenteen tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
5.1	Verkolle on määritelty omistaja.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.2	Verkon rakenne ja vastuu suunnittelusta ja ylläpidosta on selkeästi määritelty ja dokumentoitu.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.3	Verkkorakenne on dokumentoitu ja dokumentaatiota ylläpidetään.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.4	Verkkoinfrastruktuurin hankintaan ja kehittämiseen on olemassa määrämuotoinen prosessi.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.5	Eri verkot tai niiden osat on eristetty toisistaan loogisesti tai fyysisesti.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.6	Liikennettä sisä- ja ulkoverkon välillä rajoitetaan teknisesti siten, että vain tarpeellinen liikenne päästetään läpi.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.7	Ylläpitoon tarkoitetut etähallintayhteydet työasemiin on sallittu ainoastaan ylläpitohenkilöstölle.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.8	Sallitut yhteydet ulkoverkosta on dokumentoitu ja hyväksytetty organisaation tietoturvallisuudesta vastaavalla henkilöllä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.9	Verkkoliitännät yleisölle avoimissa tiloissa on suojattu siten, että organisaation sisäverkkoon on pääsy ainoastaan sallituilla osapuolilla.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.10	Muutokset verkkoon testataan, katselmoidaan ja toteutetaan muutoshallintaprosessin mukaisesti.	vahva suositus	vahva suositus	pakollinen vaatimus
5.11	Hallinta-/valvontatoiminta on erotettu muusta verkon liikenteestä esim. loogisesti erilliseen verkkoon.	suositus	vahva suositus	pakollinen vaatimus
5.12	Verkkojen väliset yhteydet on kartoitettu ja hyväksytty riskianalyysin kautta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.13	Ulkoiset yhteydet on rakennettu keskitettyjen pisteiden kautta.	suositus	vahva suositus	pakollinen vaatimus
5.14	Vaihtoehtoiset tiedonsiirtoreitit ja -resurssit on toteutettu, dokumentoitu ja hyväksytetty asianmukaisilla tahoilla.	suositus	vahva suositus	pakollinen vaatimus
5.15	Kriittiset verkon komponentit on kahdennettu.	suositus	vahva suositus	pakollinen vaatimus
5.16	Suorat, ulkoverkosta sisäverkkoon otetut yhteydet on estetty.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.17	Ulkoverkkoon tarjottavat palvelut sijaitsevat sisäverkosta erotetussa DMZ-alueessa.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
5.18	Verkon ylläpitäjille järjestetään säännöllistä tietoturvakoulutusta.	suositus	vahva suositus	pakollinen vaatimus

5.19	Verkon rakenne on suunniteltu kestämään nykyinen ja arvioitu tuleva liikennemäärä.	suositus	vahva suositus	vahva suositus
5.20	Verkko on jaettu loogisesti erillisiin aliverkkoihin, joihin palvelut jaetaan käyttötarkoituksensa mukaan.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.21	Suorat, sisäverkosta ulkoverkkoon otetut yhteydet on oletuksena estetty.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.22	Ulkoverkkoon otetaan yhteyttä erityisten välityspalvelinten (proxy) kautta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
5.23	Fyysinen verkko on jaettu vyöhykkeisiin eri käyttötarkoituksien mukaan.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

6 Sisäverkkoympäristössä suojattavat kohteet

Sisäverkossa tärkein suojattava kohde on tieto ja sen luottamuksellisuus, eheys ja saatavuus. Järjestelmät, joihin tieto tallennetaan, ja palvelut, joissa tietoa käsitellään, on suojattu. Myös järjestelmien ja palveluiden resurssit suojataan väärinkäytöksiltä (esim. bottiverkkojen osana toimimiselta). Verkko ja sen osat ovat olemassa nykyistä tai tulevaa tiedonsiirtoa varten. Uutta verkkoa, verkkoaluetta tai segmenttiä pystytettäessä se suojataan tietoturvallisuus huomioiden, riippumatta siitä onko se heti käytössä vai ei. Näin toimitaan, jotta mahdolliset tietoturvaongelmat käytön aikana voidaan minimoida. [Vaatimus 6.1]. Verkossa talletettava tai kulkeva tieto on luokiteltu sen luottamuksellisuuden mukaan käyttäen olemassa olevaa ja hyväksyttyä tiedon luokittelun menetelmää [Vaatimus 6.5].

Verkon suunnittelun, kehittämisen ja ylläpidon tulee tähdätä tiedon riittävän turvalliseen käsittelyyn. Tieto voi verkossa olla seuraavissa tiloissa:

- Tallennettuna palvelimella
- Käsittelyssä palvelimella
- Käsittelyssä päätelaitteella
- Tallennettuna päätelaitteella
- Liikkeessä verkon komponenttien välillä
- Liikkeessä verkosta ulos tai sisään.

Verkon ratkaisut tarjoavat riittävän tietoturvallisuuden tason tiedolle sen ollessa kaikissa näissä tiloissa.

Verkko on suunniteltu ja rakennettu siten, että se tukee tiedon suojaamista tiedon luokittelun mukaisesti siten, että kriittisemmät tiedot on suojattu paremmin [Vaatimus 6.3]. Tällöin verkon suunnittelu ja sen ratkaisut aloitetaan analyysillä siitä, mitä tietoa verkossa tallennetaan. Tiedon analysointi jatkuu verkon olemassaolon ajan säännöllisesti ja suurien muutosten yhteydessä, sillä verkossa olevat palvelut ja niiden käyttötavat muuttuvat yleensä ajan kuluessa. [Vaatimus 6.2]. Eri suojaustasoja on käsitelty luvussa 5.1.

Verkossa olevan tiedon analyysiä käytetään verkon suunnittelun pohjana esimerkiksi seuraaville asioille

- Verkon segmenttijaottelu
- Liikenteen rajoittaminen eri segmenttien välillä
- Tunnistautuminen verkon eri segmentteihin
- Pääsyrajoitukset sisäverkon ja ulkoverkon (internet) välillä: sisäverkkoon ja sisäverkosta sallitaan vain toiminnan kannalta välttämättömät yhteydet.

Kaikille tiedoille, järjestelmille ja palveluille on määritelty omistaja [Vaatimus 6.4]. Omistaja on henkilö tai taho, joka on hallinnollisesti vastuussa kyseisestä kohteesta ja näin ollen myös tietoaineiston luottamuksellisuuden tasosta.

6.1 Suojattavien kohteiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
6.1	Uutta verkkoa, verkkoaluetta tai segmenttiä pystytettäessä se suojataan tietoturvallisuus huomioiden, riippumatta siitä onko se heti käytössä vai ei.	vahva suositus	vahva suositus	pakollinen vaatimus
6.2	Verkon koko olemassaolon ajan analysoidaan säännöllisesti tietoturvaratkaisujen riittävyyttä suhteessa verkossa kulkevaan tietoon.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
6.3	Verkko on suunniteltu ja rakennettu siten, että se tukee tiedon suojaamista tiedon luokittelun mukaisesti siten, että kriittisemmät tiedot on suojattu paremmin.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
6.4	Kaikille tiedoille, järjestelmille ja palveluille on määritelty omistaja. Omistaja on henkilö tai taho, joka on hallinnollisesti vastuussa ao. kohteen määritelmistä, kuten tietoaineiston luottamuksellisuuden tasosta.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
6.5	Verkossa talletettava tai kulkeva tieto on luokiteltu sen luottamuksellisuuden mukaan käyttäen olemassa olevaa ja hyväksyttyä tiedon luokittelun menetelmää.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
6.6	Verkon suunnittelu ja sen ratkaisut aloitetaan analyysillä siitä, mitä tietoa verkossa tallennetaan	vahva suositus	pakollinen vaatimus	pakollinen vaatimus

7 Sisäverkkoon kohdistuvia uhkia ja vaatimuksia

Sisäverkon suojaaminen perustuu riskianalyysiin [Vaatimus 7.1], jonka osana kartoitetaan organisaation tietoon liittyvät uhat ja vaatimukset sekä turvallisuustarpeet. Turvallisuustarpeiden pohjalta päätetään tarvittavat tekniset ja hallinnolliset menetelmät, jotka toteutetaan suojaamaan organisaation sisäverkon tietoa ja palveluita. Suojausmenetelmät pohjautuvat kustannushyötyanalyysiin, jossa tiedon tai palvelun arvoa verrataan suojausmenetelmän kustannukseen ja siihen, miten todennäköistä uhkien realisoituminen on. Turvallisuustarpeet ja suojausmenetelmien kyvykkyys suojata tietoa muuttuvat ajan myötä, joten uhkia, vaatimuksia ja menetelmiä niiden ratkaisemiseksi käydään läpi säännöllisesti. Riskianalyysissä huomioidaan kaikki tietoturvallisuuden osa-alueet: saatavuus, luottamuksellisuus ja eheys. Erityisen tärkeää on suunnitella verkko toimimaan saatavuusvaatimuksien mukaisesti. Riskianalyysissä voi käyttää apuna myös yhteiskunnan elintärkeiden toimintojen turvaamisen (YETT) -verkkojulkaisua tai Kansallista turvallisuusauditointikriteeristöä (KATAKRI).

Sisäverkon uhkia arvioidaan luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta. Esimerkkejä yleisistä uhista ovat seuraavat

- **Haittaohjelmat:** Verkossa leviää erilaisia haittaohjelmia, jotka käyttävät hyväkseen ohjelmistoissa olevia haavoittuvuuksia tai käyttäjän hyväuskoisuutta. Nämä ohjelmat saattavat tulla sisäverkkoon esim. jonkin sisäverkossa olevan, ulkoverkkoon tarjottavan palvelun (sähköpostin ja verkkoselailun) välityksellä tai erilaisten ulkoisten medioiden kautta. Tavallisesti ne pyrkivät ottamaan työaseman tai verkon hyökkääjän hallintaan. Haittaohjelmia vastaan on mahdollista suojautua pitämällä huolta tietoturvapäivityksistä, koventamalla järjestelmät, rajaamalla käyttöoikeuksia, kouluttamalla henkilöstöä ja toteuttamalla kattava haittaohjelmien torjuntajärjestelmä.
- **Ulkopuolinen murtautuja:** Useimmat organisaatiot havaitsevat jatkuvasti eriasteisia murtautumisyrityksiä. Tärkeätä on analysoida, kuinka arvokasta tieto on ulkopuoliselle, sillä suojautuminen on erilaista riippuen murtautujan osaamistasosta ja motivaatiosta. Murtautujat voidaan jakaa seuraaviin luokkiin

- Automaattimurtautuja, joka pyrkii automaattisin, olemassa olevin, menetelmin murtautumaan jonnekin palveluun välittämättä palvelun tarjoajasta tai palvelutyypistä.
- Yksityinen osaava murtautuja, jolla on osaamista käyttää erilaisia valmiita työkaluja ja muokata niitä omiin tarpeisiin sopiviksi. Hyökkäyksen tarkoituksena ei ole hakea taloudellista hyötyä, vaan esimerkiksi saada kunnioitusta muilta henkilöiltä.
- Taloudellista etua hakeva yksityinen murtautuja.
- Teollisuusvakoilua harjoittavan organisaation hankkima murtautuja.
- Teknistä osaamista omaavat ja yleensä taloudellista hyötyä tavoittelevat rikollisjärjestöt.
- Tiedustelupalvelu.

Ulkopuolisen murtautujan tekemät hyökkäykset voidaan jakaa myös kohdistettuihin ja kohdistamattomiin. Kohdistamattomassa hyökkäyksessä hyökkääjällä ei ole valittua kohdetta, vaan murtautuja pyrkii murtautumaan mahdollisimman moneen järjestelmään. Tällaisen hyökkäyksen torjuntaan usein riittää perustason suojaus. Kohdistetut hyökkäykset, joissa hyökkääjä ottaa kohteekseen yhden organisaation, ovat suojausnäkökulmasta paljon haastavampia. Tällöin hyökkääjä saattaa käydä läpi kaikki organisaation palvelut ja etsiä niistä haavoittuvuuksia. Myös käytetystä tietojenkäsittely-ympäristöstä lähtevä hajasäteily voi paljastaa murtautujalle salassa pidettävää tietoa. Murtautujia vastaan voidaan suojautua huolehtimalla tietoturvapäivityksistä, minimoimalla tarjottavia verkon palveluita, ottamalla käyttöön IDS- tai IPS-järjestelmä sekä huolehtimalla hajasäteilysuojausten vaatimustenmukaisuudesta.

- **Oma työntekijä:** Eniten taloudellista haittaa aiheuttava uhka on omien työntekijöiden tahaton tai tahallinen toiminta. Tässä yhteydessä tulee kuitenkin pitää mielessä, että pääsyä julkisiin dokumentteihin ei pidä tarpeettomasti hankaloittaa. Omat työntekijät voidaan jakaa kahteen eri ryhmään
  - **Tavalliset käyttäjät:** käyttäjillä ei ole järjestelmien ylläpitoon liittyviä oikeuksia. Nämä käyttäjät vaarantavat tietoturvallisuuden esim. selaimen tai sähköpostin kautta tulevien haittaohjelmien kautta. Tavallisiin käyttäjiin voi liittyä myös niin sanotun vaarallisen työyhdistelmän riski, jossa yksittäisellä käyttäjällä on liikaa oikeuksia ja toiminnot pitäisi jakaa kahdelle tai useammalle henkilölle.
  - **Ylläpitokäyttäjät:** käyttäjillä on oikeus ylläpitää jotakin järjestelmää. Näillä käyttäjillä on usein laajat oikeudet muokata asetuksia ja tarkkailla järjestelmissä olevia tietoja, sekä muokata lokeja.

Omien työntekijöiden aiheuttamilta uhilta voidaan suojautua, kun järjestetään käyttöoikeudet tehtävien mukaisesti ja tarvittaessa esim.irtisanomistilanteessa poistetaan kaikki käyttöoikeudet välittömästi. Vaarallisten työyhdistelmien muodostuminen tulee estää. Vaarallisessa työyhdistelmässä henkilö itse sekä suorittaa että hyväksyy tekemänsä suoritteen.

- **Yhteistyökumppanit:** Nykyinen toimintaympäristö vaatii erilaisten yhteistyökumppanien päästämisen verkkoon joko internetin välityksellä tai suoraan sisäverkkoon kytkien. Usein pääsy sisäverkkoon muodostuu tarpeettoman laajaksi, eikä yhteistyökumppanille edes järjestetä koulutusta yhteisistä pelisäännöistä. Yhteiskäyttöiset käyttäjätunnukset ovat pääsääntöisesti kiellettyjä myös yhteistyökumppaneille. Jos niitä on pakko käyttää tarkoin harkituissa tilanteista, tulee käyttäjätunnusten jäljityksestä (audit trail) huolehtia muulla tavoin. Yhteistyökumppanien pääsy verkkoon on rajattu erityisen tarkasti silloin kun kyseessä on ylläpitotasoinen pääsy [Vaatimus 7.3].
- **Erilaiset luonnonmullistukset ja muut fyysiset tapahtumat:** Nämä tapahtumat rajoittavat verkon saatavuutta, esim. kaivinkone voi katkaista kaapelin tai tulipalo ja vesivahinko voivat aiheuttaa verkon toimimattomuuden. Näitä riskejä vastaan pystytään parhaiten suojautumaan jatkuvuussuunnittelun avulla.
- **Laiterikot, ohjelmistovirheet ja konfiguraatioviat:** Yleensä nämä ongelmat aiheuttavat ongelmia saatavuudelle, mutta myös eheys ja luottamuksellisuus ovat vaarassa, jos esim. palomuuri vaurioituu siten, että se sallii kaiken liikenteen. Näitä riskejä vastaan pystytään parhaiten suojautumaan jatkuvuussuunnittelun avulla.

Organisaation riskianalyysi pohjautuu todellisten uhkien kartoitukseen ja se kattaa kaikki yleisimmät uhat, joista yllä on esimerkkejä. [Vaatimus 7.6].

Päätelaitteiden ja palvelinten tietoturvallisuus on hoidettu riittävällä tasolla ja verkon ja sen tietoturvallisuuden vastuuhenkilö on nimetty [Vaatimus 7.4]. Verkosta vastuussa oleva henkilö pitää huolta siitä, että päätelaitteiden ja palvelinten tietoturvatehtävät ovat vastuutettu ja hoidettu [Vaatimus 7.5].

Päätelaitteiden tietoturvallisuudessa tulee päivitysten lisäksi kiinnittää erityisesti huomiota päätelaitteiden koventamiseen. Päätelaitteet on kovennettava suojaustason edellyttämän tason mukaisesti [Vaatimus 7.9]. Perustasolla edellytetään erityisesti järjestelmien ohjelmistokannan vakiointia. Vakioinnin osana edellytetään ohjelmistokannan minimointia. Korotetulla tasolla edellytetään kovennuksissa FDCC[2] :tä, tai vastaavaa tasoa. Lisätietoa päätelaitteiden kovennuksesta löytyy Kansallisesta turvallisuusauditointikriteeristöstä (KATAKRI, I 502).

[2] FDCC (Federal Desktop Core Configuration), yhdysvaltalaisen standardointiorganisaation kovennusmääritykset ja ne löytyvät osoitteesta: http://nvd.nist.gov/fdcc/

Hajasäteilysuojausten on vastattava niille asetettuja vaatimuksia [Vaatimus 7.10]. Hajasäteilyltä suojautuminen on hoidettava toimitilan fyysisellä valinnalla, vuorauksella tai käyttämällä suojattuja laitteistoja ja kaapelointeja. Useat kansainväliset organisaatiot edellyttävät, että käsiteltäessä heidän omistamaansa tietoa, hajasäteilyltä on suojauduttava suojaustasosta III lähtien. Verkoissa, joissa käsitellään vain kansallista tietoa, hajasäteilysuojauksia edellytetään tyypillisesti vasta suojaustasolla II. Lisätietoa hajasäteilysuojausten vaatimuksista voi kohteiden suunnittelua aloitettaessa kysyä Viestintäviraston NCSA-FI-yksiköstä.

Yllä listattujen uhkien torjuminen on organisaation oman harkinnan mukaista ja osin hyvinkin vapaasti tehtävissä. Organisaation toimintaan kohdistuu verkon tietoturvanäkökulmasta ulkoisia vaatimuksia, joiden noudattaminen on yleensä pakollista tai ainakin suositeltavaa. Vaatimuksia tulee seuraavista lähteistä

- Säädökset: laeista ja asetuksista tulevat vaatimukset ovat pakollisia ja yleensä ainakin seuraavat koskevat organisaatiota
  - Sähköisen viestinnän tietosuojalaki (516/2004)
  - EU - kriittisen tietoinfrastruktuurin turvaaminen (EU CIIP)
  - Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä 26.11.2009 (VAHTI 7/2009)
  - Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (Tietoturvallisuusasetus) 1.7.2010/681.
- Tiedon omistajan erityisvaatimukset: Tiedon omistaja (toimivaltainen viranomainen, yritys, kansainvälinen organisaatio, tai vastaava) saattaa asettaa organisaation käsittelemälle tiedolle omia erityissuojausvaatimuksiaan.
- VAHTI-ohjeet: Monessa VAHTI-ohjeessa on joitakin sisäverkon toimintaan liittyviä suosituksia, joista olennaisimmat ovat seuraavat
  - Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje (4/2001)
  - Valtionhallinnon etätyön tietoturvallisuusohje (3/2002)
  - Valtion tietohallinnon Internet-tietoturvallisuusohje (1/2003)
  - Tietoturvapoikkeamatilanteiden hallinta (3/2005)
  - Ohje tietoturvallisuusasetuksen toimeenpanosta valtionhallinnossa (**2/2010**)
- Kansallinen turvallisuusauditointikriteeristö (KATAKRI): Usean viranomaisen tekemät tietoturva-auditoinnit perustuvat KATAKRI:in ja sen asettamaan vaatimustasoon. Kriteeristössä asetettua suojausten tasoa edellytetään tietyiltä valtionhallinnon ja yritysmaailman toimijoilta.

- Organisaation omat, ylätason tietoturvaohjeet: Tietoverkko toteuttaa niitä periaatteita, joita ylempi johto on tietoturvallisuudelle asettanut [Vaatimus 7.8]. Tulee kuitenkin huomioida, että esimerkiksi kansainvälisten ja viranomaisvaatimusten toteuttamatta jättäminen edellyttää aina toimivaltaisen viranomaisen etukäteishyväksyntää.
- Järjestelmien tuomat rakenteelliset vaatimukset: Järjestelmät vaativat usein tietynlaista rakennetta verkon ratkaisuilta.
- Muiden organisaatioiden vaatimukset: Toimittaja tai asiakasorganisaatio voi sopimusteknisesti asettaa vaatimuksia organisaation tietoturvallisuuden tasolle, esim. luottokortteja käsittelevän organisaation tulee noudattaa PCI-DSS -standardia riippumatta käsiteltävien tapahtumien määrästä.

Jotta voitaisiin varmistua riittävällä tasolla verkon tietoturvatasosta, sisäverkon tietoturvallisuus auditoidaan säännöllisesti ulkopuolisen tahon toimesta [Vaatimus 7.2].

7.1 Uhkien ja vaatimusten tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
7.1	Sisäverkon suojaaminen perustuu riskianalyysiin	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
7.2	Sisäverkon tietoturvallisuus auditoidaan säännöllisesti ulkopuolisen tahon toimesta	suositus	vahva suositus	pakollinen vaatimus
7.3	Yhteistyökumppanien pääsy verkkoon on rajattu tehokkaasti, erityisesti ylläpitoyhteyksien osalta.	vahva suositus	vahva suositus	pakollinen vaatimus
7.4	Päätelaitteiden ja palvelinten tietoturvallisuus on hoidettu riittävällä tasolla ja verkon ja sen tietoturvallisuuden vastuuhenkilö on nimetty	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
7.5	Verkosta vastuussa oleva henkilö pitää huolta siitä, että päätelaitteiden ja palvelinten tietoturvallisuus on vastuutettu ja hoidettu.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
7.6	Organisaation riskianalyysi kattaa yleisimmät uhat, joista kappaleen 7 alussa on esimerkkejä.	suositus	vahva suositus	pakollinen vaatimus
7.7	Verkosta vastuussa oleva henkilö on nimetty	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
7.8	Tietoverkko toteuttaa niitä periaatteita, joita ylempi johto on tietoturvallisuudelle asettanut.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
7.9	Päätelaitteet on kovennettu suojaustason edellyttämän tason mukaisesti.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
7.10	Hajasäteilysuojausten on vastattava niille asetettuja vaatimuksia. *	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

* Lisätietoa hajasäteilysuojausten vaatimuksista voi kysyä Viestintäviraston NCSA-FI-yksiköstä.

8 Yhteistyöstä muiden toimijoiden kanssa

Nykyaikainen toimintaympäristö vaatii useiden yhteistyökumppanien kanssa toimimista. Yhteistyökumppani voi olla sisäverkossa käyttäjän, kehittäjän, ylläpitäjän, palvelutuottajan tai palveluntarjoajan roolissa. Yhdessä sisäverkossa voi samassa roolissa olla myös useita toimijoita, jolloin on tärkeää määritellä, kulkevatko kaikki tieto ja viestit organisaation kautta vai voivatko eri toimijat viestiä suoraan keskenään.

Ennen kilpailutusta on tehty riskianalyysi, jossa arvioidaan potentiaalisten yhteistyökumppanien aiheuttamat tietoturvariskit ja mahdolliset parannukset tietoturvallisuuden kannalta [Vaatimus 8.6]. Ennen kilpailutusta on selvitetty, missä maassa potentiaaliset yhteistyökumppanit käsittelevät salassa pidettäviä tietoja nyt ja tulevaisuudessa sekä selvitetään, vaikuttaako tietojen säilytyspaikka kilpailutuksen ehtoihin [Vaatimus 8.7]. Riskianalyysin tulokset tulee huomioida tarjouspyynnön vaatimuksissa.

Yhteistyökumppanin kanssa toiminta perustuu sopimukseen, jossa on määritelty selkeästi ainakin seuraavat asiat [Vaatimus 8.1]. Sopimukseen tulevat seikat on kerrottava soveltuvin osin jo tarjouspyynnössä.

- **SLA (palvelutasosopimus, Service Level Agreement):** Mitä palvelutasoa yhteistyökumppanilta halutaan tai mitä palvelutasoa asiakkaalle tuotetaan. SLA-tasoihin on sisällytetty myös tietoturvavaatimuksia laajemminkin kuin vain käytettävyyden näkökulmasta. SLA-tasojen määrittelyssä käytetään usein apuna ja viitteenä ITIL (IT Infrastructure Library) -kirjastoa.
- **Sanktiot:** Mitä seuraa, mikäli SLA:n mukaisia tavoitteita ei saavuteta. Yleensä nämä on sidottu palvelusta maksettavaan korvaukseen, eikä organisaatiolle aiheutuvaan haittaan, joka saattaa olla paljonkin suurempi. Tällöin kannattaa pohtia, miten tästä aiheutuvaa riskiä hallitaan.
- **Seuranta:** Miten SLA-tasojen toteutumista seurataan ja kenen vastuulla seuraaminen on.
- **Auditointi:** Sopimuksessa on määritelty, että yhteistyökumppanin toimintaa saa auditoida. Mikäli auditointiin halutaan käyttää ulkopuolis-

ta toimijaa, sopimuksessa määritellään, kuka vastaa kustannuksista. Maininta auditointioikeudesta on oltava tarjouspyynnön sopimusliitteissä.

- **Taustaselvitykset:** Mikäli yhteistyökumppanilla on pääsy salassa pidettävään tietoon (Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu, Juhta JHS 147) määritellään sopimukseen henkilöstöstä tehtävät turvallisuusselvitykset [Vaatimus 8.9]. Muun tiedon osalta turvallisuusselvitys on organisaation omassa harkintavallassa. Kansainvälisiä, vähintään suojaustason III aineistoja käsitteleviltä edellytetään lisäksi taustaselvitysten säännöllistä uusimista.
- **Turvallisuussopimus:** Salassapitovelvollisuuksista organisaatioiden kesken on sovittu ja varmistettu, että organisaatioiden henkilöt tietävät velvollisuutensa sen suhteen.
- **Sisäverkon tietoturvallisuus:** Palvelun tarjoajan tulee noudattaa tässä esitettyjä ohjeita. Voimassaolevia sopimuksia ei tarvitse muuttaa, vaan tietoturvallisuusasetukseen kuuluvan siirtymäajan tehtävänä on mm. antaa näiden sopimuskausien umpeutua, jolloin uusissa sopimuksissa nämä ohjeet voidaan ottaa huomioon.
- **Selkeät vastuualueet:** Sopimukseen ei ole merkitty pelkästään yleisluontoisia lausahduksia, kuten 'toimittaja sitoutuu toimimaan tietoturvallisesti', vaan tietoturvallisuuteen vaikuttavat asiat kirjataan yksityiskohtaisemmin, kuten seuraavien vastuualueiden määrittelyllä
    - Käyttäjähallinta: kuka vastaa käyttäjähallinnasta, käytetäänkö yhteistunnuksia, käytetäänkö keskitettyä käyttäjähallintaa ja millainen on salasanapolitiikka, miten vahva tunnistautuminen toteutetaan
    - Valvonta: mitä asioita valvotaan, kuka valvoo, kuka pääsee katsomaan valvontaa ja mitä valvontadatalle tehdään
    - Tietoturvapäivitykset: kuka on vastuussa kunkin komponentin tietoturvapäivityksistä, milloin päivitykset tulee viimeistään tehdä, miten niitä testaan ennen päivitystä ja miten valvotaan, että päivitykset tulee tehtyä kaikille komponenteille
    - Hallintamekanismit: mitä protokollia ja työkaluja käytetään, käytetäänkö erillistä hallintaverkkoa ja ketkä saavat hallita laitteita.

Yhteistyökumppanin kanssa pyritään mahdollisimman avoimeen viestintään ja järjestetään säännöllisiä palavereja, jossa käydään läpi esimerkiksi toteutuneet SLA-tasot, havaitut tietoturvaongelmat ja muut tietoturvallisuuteen vaikuttavat asiat. [Vaatimus 8.4].

Ulkoistuskumppanin sisäiset tietoturvaohjeet ja menetelmät saattavat poiketa ja olla joiltain osa-alueilta heikommat kuin ulkoistavan organisaation menetelmät ja vaatimukset. Ulkoistuskumppani on velvoitettu sitoutumaan

vastaaviin tai tiukempiin tietoturvamenettelyihin sisäverkkoon liittyvissä asioissa kuin organisaatio itse sitoutuu. [Vaatimus 8.5].

Palveluntarjoajat pyrkivät tehostamaan työtä siten, että työntekijöitä ei kiinnitetä jonkin tietyn asiakkaan palvelemiseen, vaan työtä kierrätetään. Tällöin on riskinä, että ongelmatilanteissa ei ole saatavissa osaavaa henkilöstöä riittävän nopeasti käyttöön. Palveluntarjoajan kanssa on sovittu henkilöt, jotka on kiinnitetty organisaation käyttöön ainakin normaaliolojen häiriötilanteiden aikana [Vaatimus 8.3]. Poikkeusoloihin varautumista VAP-varauksin kannattaa harkita ja korkeammilla tasoilla sopia näistä.

Näiden asioiden ja yleisen tietoturvallisuuden varmistamiseksi palveluntarjoajalle suositellaan tehtäväksi tietoturva-auditointi riippumattoman kolmannen osapuolen toimesta. Organisaation on varattava auditointioikeus verkkojen palveluntarjoajien toimintaan [Vaatimus 8.10].

Ulkoistuskumppania vaihdettaessa joudutaan usein tekemään monimutkaisia siirtotoimenpiteitä, joiden kesto saattaa olla ajallisesti pitkäkin. Tällöin varmistetaan, että siirtovaiheessa tietoturvallisuuden taso ei laske. [Vaatimus 8.8].

Tietoturvapoikkeamien hallinta on suunniteltu, ohjeistettu, koulutettu, dokumentoitu ja erityisesti viestintäkäytännöt ja –vastuut on sovittu [Vaatimus 8.11]. Verkkojen tietoturvapoikkeamista on lisäksi ilmoitettava välittömästi turvallisuusviranomaiselle (esim. CERT-FI) tai tiedon omistajan (toimivaltaisen viranomaisen) hyväksymälle taholle. [Vaatimus 8.12].

8.1 Yhteistyöstä muiden toimijoiden kanssa tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
8.1	Yhteistyökumppanin kanssa tehdyssä sopimuksessa on selkeästi määritelty ainakin seuraavat asiat: SLA, sanktiot, seuranta, auditointi, taustaselvitykset, turvallisuussopimus ja vastuualueet	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
8.2	Keskeisille verkon laitteille, liitännöille ja palveluille on palvelusopimuksin (SLA) tai muuten ylläpitojärjestelyin taattava kohteen kriittisyyttä vastaava ylläpitotaso.	suositus	pakollinen vaatimus	pakollinen vaatimus
8.3	Palveluntarjoajan kanssa on sovittu henkilöt, jotka on kiinnitetty organisaation käyttöön ainakin normaaliolojen häiriötilanteiden aikana	suositus	vahva suositus	pakollinen vaatimus
8.4	Yhteistyökumppanin kanssa järjestetään säännöllisiä seurantapalavereja	suositus	vahva suositus	pakollinen vaatimus
8.5	Ulkoistuskumppanit on velvoitettu sitoutumaan vastaaviin tai tiukempiin tietoturvamenettelyihin lähiverkkoon liittyvissä asioissa kuin organisaatio itse sitoutuu	Vahva suositus	pakollinen vaatimus	pakollinen vaatimus
8.6	Ennen kilpailutusta on tehty riskianalyysi, jossa arvioidaan potentiaalisten yhteistyökumppanien aiheuttamat tietoturvariskit ja mahdolliset parannukset tietoturvallisuuden kannalta	suositus	vahva suositus	pakollinen vaatimus
8.7	Ennen kilpailutusta on selvitetty, missä maassa potentiaaliset yhteistyökumppanit käsittelevät salassa pidettäviä tietoja nyt ja tulevaisuudessa sekä selvitetään, vaikuttaako tietojen säilytyspaikka kilpailutuksen ehtoihin	suositus	pakollinen vaatimus	pakollinen vaatimus
8.8	Ulkoistuskumppania vaihdettaessa on varmistuttu siitä, että siirtovaiheessa tietoturvallisuuden taso ei laske.	suositus	pakollinen vaatimus	pakollinen vaatimus
8.9	Mikäli yhteistyökumppanilla on pääsy salassa pidettävään tietoon, määritellään sopimukseen henkilöstön tarvittavat turvallisuusselvitykset.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
8.10	Organisaation on varattava auditointioikeus verkkojen palveluntarjoajien toimintaan	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
8.11	Tietoturvapoikkeamien hallinta on suunniteltu, ohjeistettu, koulutettu, dokumentoitu ja erityisesti viestintäkäytännöt ja –vastuut on sovittu.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
8.12	Verkkojen tietoturvapoikkeamista on lisäksi ilmoitettava välittömästi turvallisuusviranomaiselle (esim. CERT-FI) tai tiedon omistajan (toimivaltaisen viranomaisen) hyväksymälle taholle.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus

9 Kaapelointi

Päätelaitekaapeloinnit ovat lähes poikkeuksetta kierretystä parista tehtyjä yleiskaapelointeja. Kerroksissa kaapelointi päättyy tavallisesti kerrosjakamoon tai ristikytkentätelineeseen. Verkon aktiivilaitteet voivat sijaita tässä tilassa tai erillisessä laitehuoneessa.

Aktiivilaitteiden väliset runkoyhteydet ovat tavallisesti valokuitua, joskin suojaamatonta parikaapelia voidaan myös käyttää. Kiinteistöstä lähtevät kaapelit ovat joko parikaapelia (xDLS-yhteydet) tai valokuitua (nopeammat yhteydet).

Kaapeloinnissa tapahtuvat virheet voivat aiheuttaa ongelmia verkon saatavuudessa. Siksi kaapeloinnin asentamisessa on käytetty ammattitaitoista asennusyritystä. Kaapelointia ei hyväksytä ennen mittausta, joka on tehty ao. kaapeliluokalle määritellyn virallisen tyyppitestausmenettelyn mukaan [Vaatimus 9.1].

Vaikka kaapelit olisikin vedetty asianmukaisesti, voivat ne tai verkon muut laitteet rikkoutua. Kriittisten yhteyksien turvaamiseksi on rakennettu varayhteyksiä. Varayhteyksiä suunniteltaessa on varmistauduttava, että kaapeloinnit kulkevat fyysisesti eri reittejä. Varayhteydet rakennetaan usein verkon keskeisten laitteiden kahdennuksen yhteydessä.

Mikäli kaapelointi on tehty liian näkyvästi ja kaapeleihin pääsee liian helposti käsiksi, on riskinä, että murtautuja pääsee kytkemään oman laitteensa verkkoon. Siksi kaapelit on sijoitettu muoviputkiin, kaapelikouruihin, -hyllyihin, välikattoihin, yms. suojaaviin rakenteisiin siten, ettei asiatonta kytkeytymistä kaapeleihin voi tehdä huomiota herättämättä, eivätkä kaapelit ole alttiina fyysiselle vaurioitumiselle [Vaatimus 9.2]. Kaapelit on lisäksi vedetty sellaisten alueiden läpi, joihin yleisöllä ei ole pääsyä. Jakamot ja ristikytkentäpaikat ovat lukittuja tai sijaitsevat lukituissa tiloissa, joihin on pääsy vain valtuutetuilla henkilöillä [Vaatimus 9.3]. Kaapelointikanavat on rakennettu siten, että ne ovat äänieristettyjä ja suojattuja, erityisesti jos ne kulkevat toisen organisaation hallinnassa olevien tilojen läpi. Huoneiden välinen puutteellinen äänieristys kaapelikanavassa saattaa vaarantaa tiedon luottamuksellisuuden lisäksi myös työrauhan. Korkeammilla suojaustasoilla edellytetään usein lisäksi kaapeloinnin sinetöintiä, tai vastaavaa tunkeutumisen havaitsemisen mahdollistavaa menetelmää. Korkeammilla suojaustasoilla edellytetään usein joko erillisiä kaapelointeja tai kaiken liikenteen salaamista organisaation hallinnassa olevan alueen sisälläkin, mikäli korkeamman suojaustason tieto kulkee matalamman suojaus-

tason kanssa samassa fyysisessä kaapeloinnissa. Hyvänä käytäntönä pidetään värikoodattujen kaapelien käyttöä ristikytkennöissä.

Kaapeleita vedetään yleensä paljon ja kohtuullisen pitkiä matkoja, jolloin riskinä on kaapeleiden sekoittaminen keskenään. Kaapelin seinärasiassa ja ristikytkentäpaneelissa olevat päät on merkitty toisiaan vastaavasti, jotta tältä ongelmalta vältyttäisiin [Vaatimus 9.4].

Kaapelia ja liitäntäpisteitä tehtäessä on usein käytännöllistä tehdä useampia liitäntäpisteitä kuin sen hetkinen tarve on. Käyttämättömät liitäntäpisteet muodostavat kuitenkin tietoturvariskin, jos niistä on pääsy verkon sisälle. Käyttämättömät liitäntäpisteet on irrotettu aktiivilaitteesta tai ko. laitteen portit estävät oletuksena uusien asemien vapaa liittäminen sisäverkkoon [Vaatimus 9.5].

Salamaniskusta aiheutuvien ongelmien varalle on käytetty valokaapeleita runkoyhteyksillä ja varavoimalaitteita (UPS) ja ylijännitesuojia kriittisissä laitteissa.

9.1 Teknologiatausta

Parikaapeli voi olla suojaamatonta (U-UTP tai UTP, Unshielded Twisted Pair) tai foliosuojattua (F-UTP tai FTP, Foiled Twisted Pair). F-UTP-kaapelin katsotaan olevan vähemmän herkkää ulkoisille häiriöille, vastapainona ovat toisaalta maadoituksen vaativuus ja tästä mahdollisesti aiheutuvat vikatilanteet. Toimistoympäristössä kaapeloinnin tyypillä ei ole väliä. U-UTP on edullisempana ja huolettomampana vaihtoehtona yleisempi.

Kaapeloinnin suorituskyvyn määrittää komponenttien laatuluokitus, esim. tällä hetkellä kategoria 6 tai 6A. Asennetut kaapeloinnit jaetaan laatuluokkiin. Kategoria 6 tai 6A -komponenteista oikein asennettuna saadaan luokka E tai luokka EA -kaapelointi. Asennettu kaapelointi on testattu ennen käyttöönottoa luokkaansa vastaavalla menettelyllä.

Viestintäviraston yleiskaapeloinnille asettavat vaatimukset täyttyvät, kun sisäverkko rakennetaan ja mitataan yleiskaapelointeja koskevan standardisarjan EN 50173 mukaisesti.

9.2 Kaapeloinnin tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
9.1	Kaapelointi on hyväksytty ao. kaapeliluokalle määritellyn virallisen tyyppitestausmenettelyn mukaan.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.2	Kaapelit kulkevat kytkeytymistä ja fyysisiä vaurioita ehkäisevissä rakenteissa.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.3	Jakamot, ristikytkentäpaikat ja verkon aktiivilaitteet sisältävät telineet sijaitsevat lukituissa tiloissa, joihin on pääsy vain valtuutetuilla henkilöillä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.4	Kaapelointi on dokumentoitu ja näkösuojaan jäävät kaapelit on nimiöity dokumentteja vastaavasti molemmista päistään.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
9.5	Käyttämättömät liitäntäpisteet on irrotettu aktiivilaitteesta tai ao. laitteen portit estävät oletuksena uusien asemien vapaan liittämisen sisäverkkoon.	suositus	vahva suositus	pakollinen vaatimus

10 Langattomat lähiverkot

Langattomalla lähiverkolla (WLAN, Wireless LAN) tarkoitetaan IEEE 802.11-standardeihin perustuvia verkkoja, joita yleisesti kutsutaan myös Wi-Fi-verkoiksi (Wireless Fidelity). WLANien erityishaasteina on niiden kuuluvuus rakennuksen ulkopuolelle, kuulumattomuus rakennuksen sisällä, käyttäjien asentamat mahdolliset luvattomat tukiasemat, tunkeutujien asentamat tukiasemat (rogue access point) sekä tunnetut ongelmat liikenteen salauksessa. Radioliikennettä häiritsevät muut samalla taajuusalueella toimivat radiolähteet, kuten esim. mikroaaltouunit, Bluetooth-laitteet sekä toiset WLANit.

Langaton lähiverkko voidaan saada toimintakyvyttömäksi samoilla kanavilla toimivilla tehokkailla lähettimillä ja/tai suunta-antenneilla. WLANien nykyinen salaus salaa vain datan, mutta ei esim. hallintaliikennettä tai WLAN-osoitteita (laitteiden fyysiset MAC-osoitteet). Hallintaviestejä väärentämällä voidaan yksittäinen laite pakottaa pois verkosta. Liikennettä tarkkailemalla havaitaan liikennöivien laitteiden MAC-osoitteet ja sen myötä mahdollisesti henkilön paikallaolo ja sijainti. WLANien tietoturvahaasteista johtuen on sen käyttöönottoa harkittaessa tehtävä aina riskianalyysi huomioiden em. seikat erityisesti korkeilla tietoturvatasoilla [Vaatimus 10.1].

Organisaatioiden käytössä olevat WLANit rakennetaan yleensä käyttäen keskitettyä hallintaa, jonka avulla verkkoa voidaan konfiguroida ja valvoa. [Vaatimus 10.3]. Organisaatioille tarkoitetuissa WLAN-tuotteissa ja ratkaisuissa verkkojen liikenne erotetaan tavallisesti omaksi virtuaaliverkoksi (VLANiksi) langallisen verkon puolella. Näin WLAN-liikenne ei häiriydy muusta verkon liikenteestä ja WLAN-laite voi liikkua vapaasti ilman tarvetta vaihtaa IP-osoitetta. Samaan langattomaan tukiasemaan voidaan määritellä tietoturvallisuudeltaan erilaisia loogisia WLANeja, joilla on oma verkkotunniste (SSID, service set identifier) ja muut ominaisuudet ml. tietoturvaominaisuudet. Näitä loogisesti erillisiä WLANeja voivat olla esim. tuotantokäyttöön tarkoitettu WLAN ja tietoturvallisuudeltaan heikompi, vierailijoille tarkoitettu WLAN. Tietoturvatasoltaan erilaiset VLANit ja WLANit on eristettävä toisistaan turvallisesti. Langaton vierailijaverkko on toteutettava siten, että se on fyysisesti tai loogisesti eriytetty sisäverkosta ja siitä on yhteys vain Internetiin [Vaatimus 10.4]. Langattoman vierailijaverkon Internet-yhteys on kytketty erillisen Internet-liittymän kautta tai muuten hallitusti rajoitetaan ja estetään sen mahdollisuus häiritä

tai tutkia sisäverkon Internet-liikennettä [Vaatimus 10.5]. Erillinen Internet-liittymä voidaan toteuttaa käyttäen virtuaalilähiverkkotekniikkaa (VLAN).

Etäkäyttöratkaisuissa voidaan mahdollistaa langattomien verkkojen käyttö siten, että etäkäyttöyhteydet muodostetaan salattuna ja vahvasti tunnistettuna VPN-yhteytenä käyttäen langatonta verkkoa. Tällä tavalla voidaan hyödyntää ilmaisia tai edullisia, esimerkiksi hotellien tai kokous- ja koulutustilojen tarjoamia WLAN-yhteyksiä mahdollisesti muiden kalliimpien (2G/EDGE, 3G/4G) maksullisten langattomien yhteyksien sijaan. Lisäksi, jos organisaation omissa kokous- tai koulutustiloissa on jo oma erillinen WLAN-vierailijaverkko rakennettu, voidaan em. mukaisen etäkäyttöyhteyden avulla käyttää sisäverkon palveluita sen yli. Tällöin organisaatiolla ei ole välttämättä tarvetta rakentaa erillistä, suoraan organisaation sisäverkon yhteydessä toimivaa langatonta lähiverkkoa.

Jos käyttäjille tarjotaan joko vierailijaverkkoa tai organisaation sisäverkossa toimivaa WLAN-verkkoa, se muodostaa väärin toteutettuna erään keskeisimmistä tietoturvauhista, joka voi vaarantaa organisaation tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden. Tämän johdosta jokainen WLAN-verkko tulee rakentaa riskiarvioinnin jälkeen käyttäen ammattitaitoista tietoliikennetoimittajaa. Sekä vierailijaverkolle että sisäverkkoon liitetylle WLAN-verkolle vaaditaan ulkopuolisen suorittama kattava auditointi. Erityisesti sisäverkkoon liitetyn WLAN-verkon osalta tulee varata resursseja sen jatkuvan toiminnan seuraamiseen ja säännöllisiin auditointeihin, joissa varmistetaan WLAN-radioverkon (tukiasemien) konfiguraation oikeellisuus, käytettyjen tunnistus- ja salausmenetelmien riittävyys sekä havaitaan mahdolliset vieraat tukiasemat. [Vaatimus 10.2].

10.1 Teknologiatausta

WLANin tietoturvallisuudessa keskeisiä ratkottavia haasteita ovat verkkoon liittyjän tunnistaminen ja luottamuksellisuus.

WLAN-liikenteen tulee olla vahvasti salattu, mikä takaa liikenteen luottamuksellisuuden [Vaatimukset 10.6, 10.9]. WLANiin on määriteltävissä useita eri salausmenetelmiä. Esimerkkejä suositeltavista salausmenetelmistä ovat WLANin sisäinen WPA2 AES-salaus sekä VPN-yhteyksien käyttämät IPSec, SSH ja TLS, joiden osalta on syytä käyttää tarkoituksen mukaisia asetuksia. VPN-yhteyksien asetuksista kryptoasetukset määrittelevät käytetyn salausalgoritmi-salausavain-yhdistelmän. Valmistajien tuotteiden oletusasetuksissa saattaa olla hyväksyttynä myös heikompia salaustapoja, jotka on syytä poistaa käytöstä. Vanhentunutta ja helposti murrettavissa olevaa WEP-salausta ei pidä käyttää. Sisäverkkoon liitetyn WLAN-verkon osalta sen käyttäminen on kiellettyä. Korotetulla tasolla langattomat verkot ovat lähtökohtaisesti kiellettyjä. Viranomainen voi tapauskohtaisesti kuitenkin hyväksyä ratkaisun, jos liikenne on suojaustasolle hyväksytyllä menetelmällä salattu päästä-päähän (ei vain radio-

tie), ts. langatonta verkkoyhteyttä käytettäessä tieto tulee suojata, kuten siirrettäessä tietoa yli julkisen internet verkon.

Sekä verkkoon liittyvä käyttäjä että laite on tunnistettava luotettavasti [Vaatimukset 10.7, 10.8, 10.10, 10.11]. Tunnistaminen voi olla avoin, jaettuun salasanaan perustuva tai keskitetty, yksilöivästi tunnistava. Keskitetty tunnistusjärjestelmä voi käyttää IEEE 802.1X EAP-TLS-protokollaa tunnistustietojen vaihtoon WLANiin liittyvän laitteen kanssa, RADIUS-palvelinta ja keskitettyä käyttäjätietokantaa (esim. Microsoftin Active Directory) tunnistamiseen ja tunnistustietojen todentamiseen. Samaa teknologiaratkaisua ja järjestelmää voidaan käyttää myös kiinteään lähiverkkoon liittyjien tunnistamiseen.

10.2 Langattomien lähiverkkojen tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
10.1	WLANia ei oteta käyttöön ilman riskianalyysiä	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.2	WLAN auditoidaan ulkopuolisen auditoijan toimesta	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.3	WLANin tietoturvallisuutta ja suorituskykyä valvotaan ja hallitaan keskitetysti tai muulla tavoin.	suositus	pakollinen vaatimus	Pakollinen vaatimus
10.4	Vierailijaverkko: Langaton vierailijaverkko on toteutettava siten, että se on fyysisesti tai loogisesti eriytetty sisäverkosta ja siitä on vain yhteys Internetiin.	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.5	Vierailijaverkko: Langattoman vierailijaverkon Internet-yhteys on kytketty erillisen Internet-liittymän kautta tai muuten hallitusti rajoitetaan ja estetään sen mahdollisuus häiritä tai tutkia sisäverkon Internet-liikennettä	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.6	Vierailijaverkko: WLANin liikenne tulee olla vahvasti salattu.	vahva suositus	pakollinen vaatimus	Pakollinen vaatimus
10.7	Vierailijaverkko: WLANissa on käyttäjille vahva tunnistusmenettely.	vahva suositus	vahva suositus	Pakollinen vaatimus
10.8	Vierailijaverkko: WLANiin liittyvä laite ja WLAN tunnistavat toisensa luotettavasti.	vahva suositus	vahva suositus	Pakollinen vaatimus
10.9	Sisäverkkoon liitetty WLAN-verkko: WLANin liikenne tulee olla vahvasti salattu.	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.10	Sisäverkkoon liitetty WLAN-verkko: WLANissa on käyttäjille vahva tunnistusmenettely.	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus
10.11	Sisäverkkoon liitetty WLAN-verkko: WLANiin liittyvä laite ja WLAN tunnistavat toisensa luotettavasti.	pakollinen vaatimus	pakollinen vaatimus	Pakollinen vaatimus

11 Verkon aktiivilaitteet

Ethernet on yleisin ja lähes ainoa organisaatiokäytössä oleva langallinen lähiverkkotyyppi. Se koostuu kierretyillä parikaapeleilla tai valokuiduilla yhteen liitetyistä kytkimistä, joihin päätelaitteet ja palvelimet liittyvät. Verkko voidaan jakaa loogisiin osaverkkoihin, virtuaaliverkkoihin (VLAN, Virtual LAN). Lähiverkot liitetään toisiinsa reitittimillä. Tietoturvallisuudeltaan erilaiset vyöhykkeet sijoitetaan eri VLANeihin, jotka liitetään palomuurilla tai pääsylistoilla toisiinsa.

11.1 Teknologiatausta

Verkon toiminnalle on aina syytä tehdä riskianalyysi: mitä seuraa, jos verkko ei ole käytettävissä, ja kuinka paljon kannattaa tältä pohjalta panostaa lisäkäytettävyyteen. Kriittisissä verkoissa on kahdennettu keskeiset laitteet, kuten keskuskytkimet, internet-reitittimet, hakemistopalvelut, DNS-nimipalvelimet ja DHCP-osoitepalvelimet, ja/tai niiden komponentit (esim. virtalähde). Tehdyn riskianalyysin perusteella keskeisten verkkolaitteiden välille on järjestetty varayhteydet esimerkiksi Rapid Spanning Tree -protokollaa (standardi IEEE 802.1w) käyttäen. Samoin keskeiset verkkokomponentit on kahdennettu. [Vaatimus 11.1]

Keskeytymätön virransyöttö (UPS) on järjestetty keskeisille laitteille ja kaikki verkon laitteet palautuvat virtakatkon jälkeen normaalitoimintaan [Vaatimus 11.2].

Sisäverkko voidaan jakaa tietoturvallisuudeltaan erilaisiin vyöhykkeisiin. Sisäverkoissa tämä tehdään usein loogisesti käyttämällä VLAN (Virtual LAN) -tekniikkaa. VLANit ja muut erilaisen tietoturvatason omaavat vyöhykkeet tulee eristää toisistaan palomuurilla tai reitittimen pääsylistoilla. Erityisesti Internetin ja sisäverkon, sekä DMZ-alueen ja sisäverkon välillä eristys on toteutettu palomuurilla. [Vaatimus 11.3].

Liityttäessä kytkimiin ja VLANeihin laitteet tunnistetaan esim. MAC-osoitelistojen tai WLANeista tutun 802.1X:n avulla. Jälkimmäinen on näistä selvästi vahvempi tapa tunnistautua. Tuntemattomien asemien liittymistä verkkoon pyritään ehkäisemään myös poistamalla käyttämättömät kytkinportit käytöstä

joko ohjelmallisesti tai irrottamalla kaapeli. [Vaatimus 11.4]. Ulkopuolisten käytössä olevista tiloista ei ole pääsyä sisäverkkoon ilman tunnistusta (katso luku 5).

Laitteiden hallintayhteydellä käytetään riittävän vahvaa salausta ja käyttäjän tunnistusta, kuten SSL/TLS, SSH tai SNMPv3. Verkkolaitteiden hallintaliitäntään pääsevät kytkeytymään vain hallinnasta vastaavat ennalta määritellyt henkilöt ja laitteet. Laitteiden hallintayhteydellä käytetään vahvaa salausta ja käyttäjän tunnistusta. [Vaatimus 11.5]. Erityisesti toimittajan tunnistukseen liittyvät oletusparametrit, kuten salasanat ja SNMP community stringit on vaihdettu oletusarvoistaan [Vaatimus 11.6]. Hallintayhteydet (esim. SNMP) on eriytetty omaan verkkosegmenttiinsä [Vaatimus 11.7]. SNMP-protokollasta on käytössä vähintään versio 3, jos laitteisiin tehdään muutoksia. Jos laitteista vain luetaan tietoja, SNMP:n on oltava vähintään versiota 2c. [Vaatimus 11.8]. SNMP-protokollaa käytettäessä laitteissa käytetään pienempiä mahdollisia oikeuksia. Jos SNMP:n avulla ei aseteta parametreja, käytetään READ ONLY -oikeuksia. Jos SNMP-protokollaa ei käytetä laitteen hallintaan, on se poistettu käytöstä. [Vaatimus 11.9].

Verkon aktiivilaitteisiin ei ole asennettu eikä otettu käyttöön sellaisia palveluita, ohjelmia tai protokollia, joille ei ole suunniteltua ja hyväksyttyä käyttötarvetta. Tarpeettomat palvelut, ohjelmat ja protokollat on poistettu käytöstä [Vaatimus 11.10]. Verkon aktiivilaitteiden konfiguroinnissa on huomioitava, että niiden oletusasetuksissa saattaa olla myös tietoturvallisuutta heikentäviä asetuksia sekä automaattitoimintoja, jotka on poistettava käytöstä. Verkkolaitteiden asetukset on tallennettu ja varmuuskopioitu mahdollista laitteen vaihtoa ja asetusten palauttamista varten [Vaatimus 11.11].

Kytkinlaitteet periaatteessa välittävät kehykset laitteelta toiselle siten, että muista liitännöistä ei voi seurata tätä liikennettä. On kuitenkin olemassa erilaisia keinoja seurata muiden laitteiden liikennöintiä, varastaa niiden identiteetti tai kaapata meneillään oleva istunto. Kytkinverkon kuuntelu edellyttää tyypillisesti välistävetohyökkäystä (man-in-the-middle attack), jonka toteuttamiseksi on vapaasti saatavilla hakkerointityökaluja internetistä. Tällaisen hyökkäyksen suurin kynnys on ylläpitäjän oikeuksien saaminen olemassa olevaan työasemaan - tai vaihtoehtoisesti uuden (oman) työaseman liittäminen sisäverkkoon. Tätä voidaan ehkäistä työasemaporteista estämällä kytkimen työasemaliitäntöjen välinen liikenne. Verkkokytkimiä ei tulisi asettaa verkkoliikennettä kaiuttavaan toimintatilaan (HUB-toiminnallisuus). Menettelyä kutsutaan toimittajasta riippuen mm. nimillä private VLAN tai protected port. [Vaatimus 11.12]. IDS on laite tai ohjelmisto, joka valvoo verkossa epäilyttävää, tunkeutumiseen viittaavaa liikennettä. IPS pyrkii taas estämään tällaisen toiminnan. IDS- tai IPS-toiminto voi olla joko erillisenä laitteena, palvelinohjelmistona tai osana aktiivista verkkokomponenttia. On huomattava, että IDS ja IPS eivät ole ensisijaisia ratkaisuja sisäverkon tietoturvahaasteisiin, vaan puolustuslinja muiden ratkaisujen pettäessä. Ne vaativat huolellista suunnittelua ja käyttöönottoa. [Vaatimus 11.13].

Verkon aktiivilaitteiden lokitiedot kerätään erilliselle keskitetylle palvelimelle ja niitä seurataan säännöllisesti. Laitteiden kellot on synkronoitu lokitietojen yhdenmukaisuuden varmistamiseksi. Tarkempia ohjeita lokeihin liittyen löytyy Lokiohjeesta, VAHTI 3/2009. [Vaatimus 11.14].

11.2 Verkon aktiivilaitteiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
11.1	Verkolle on tehty riskianalyysi ja tämän tuloksena keskeiset verkkolaitteet, niiden komponentit (esim. virtalähde) ja yhteydet on tarvittaessa kahdennettu.	vahva suositus	vahva suositus	pakollinen vaatimus
11.2	Keskeisillä laitteilla on UPS ja kaikki verkon laitteet palautuvat virtakatkon jälkeen normaalitoimintaan.	suositus	vahva suositus	vahva suositus
11.3	Sisäverkon tietoturvallisuudeltaan erilaiset vyöhykkeet on eristetty toisistaan palomuurilla tai reitittimen pääsylistoilla. DMZ on eristetty sisäverkosta palomuurilla.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.4	Sisäverkkoon liitetyt aktiivilaitteet tunnistetaan vahvasti esim. 802.1X-menettelyllä, jolla estetään tuntemattomien laitteiden liittäminen.	suositus	vahva suositus	pakollinen vaatimus
11.5	Verkkolaitteiden hallintaliitäntään pääsevät kytkeytymään vain hallinnasta vastaavat ennalta määritellyt henkilöt ja laitteet. Laitteiden hallintayhteydellä käytetään vahvaa salausta ja käyttäjän tunnistusta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
11.6	Verkkolaitteissa on vaihdettu tunnistukseen liittyvät toimittajien oletusparametrit.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.7	Hallintayhteydet (esim. SNMP) on eriytetty omaan verkkosegmenttiinsä.	suositus	vahva suositus	pakollinen vaatimus
11.8	SNMP-protokollasta on käytössä vähintään versio 3, jos laitteisiin tehdään muutoksia. Jos laitteista vain luetaan tietoa, SNMP-protokollan on oltava vähäntään versio 2c.	vahva suositus	vahva suositus	pakollinen vaatimus
11.9	SNMP-protokollalla on pienimmät mahdolliset oikeudet tai se on poistettu käytöstä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.10	Tarpeettomat palvelut, ohjelmat ja protokollat on poistettu verkon aktiivilaitteista käytöstä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
11.11	Verkkolaitteiden asetukset on tallennettu ja varmuuskopioitu mahdollista laitteen vaihtoa ja asetusten palauttamista varten.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

11.12	Kytkimen työasemaportit on erotettu toisistaan s.e. työasemat eivät voi nähdä toistensa liikennettä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
11.13	Käytössä on verkkotason tunkeilijan tunnistus- (IDS) ja estojärjestelmä (IPS)	suositus	vahva suositus	pakollinen vaatimus
11.14	Laiteiden lokitiedot kerätään keskitetysti ja niitä seurataan säännöllisesti.	suositus	vahva suositus	pakollinen vaatimus

12 Sisäverkkojen väliset yhteydet

Sisäverkot liitetään toisiinsa saman operaattorin alueella IP-pohjaisilla MPLS- (Multiprotocol Label Switching) -palveluilla, Ethernet-pohjaisella kytkentäisellä verkolla tai Internetin yli muodostettavilla salatuilla tunneleilla. Erityisesti kansainvälisen turvallisuusluokitellun tiedon siirrossa käytetään salausta aina, kun verkko menee organisaation hallitseman fyysisen tilan ulkopuolelle. Salaukseen tulee käyttää vähintään siirrettävän aineiston suojaustasolle hyväksyttyjä salausratkaisuja.

12.1 Teknologiatausta

MPLS-tekniikan avulla operaattorit muodostavat toisistaan riippumattomia loogisia verkkoja yhteiseen fyysiseen verkkoon. Perus-MPLS ei salaa yhteyksiä, vaan siinä luotetaan operaattoriin ja kaapelireittien fyysiseen suojaukseen. Internet-yhteyden läpi voi muodostaa salatut tunnelit käyttäen esim. IPSec- tai SSL-protokollia.

Organisaation liiketoiminnan vaatimusten pohjalta arvioidaan tarvittavien yhteyksien kriittisyys. Tämän perusteella laaditaan palveluntarjoajan kanssa palvelutasosopimus (SLA), jossa määritellään parametreja liittymän suorituskyvylle ja ylläpidolle. Määriteltäviä asioita voivat olla mm. liittymän käytettävyys, valvonta-aika, tavoitteet viankorjauksen aloittamiselle sekä vian poistamiselle, datan läpäisy ja liittymän virhemäärät. Tiukemmat vaatimukset palvelutasosopimuksessa maksavat yleensä enemmän. SLA on riskianalyysin jälkeen sopeutettu vastaamaan yhteyksien kriittisyyttä ja käytettävyysvaatimuksia. SLA:n vastaavuutta toteutuneeseen seurataan joko omilla tai operaattorin tarjoamilla työkaluilla. [Vaatimus 12.1].

Samaan tapaan kuin lähiverkon komponentit ja yhteydet voidaan kahdentaa, myös toimipisteiden väliset yhteydet ovat kahdennettavissa. Reitittimet ja kytkimet voidaan kahdentaa ja yhteydet on mahdollista ohjata eri kaapelireittejä pitkin siten, että ne päätyvät operaattoreilla eri laitteisiin. Internet-yhteys on myös mahdollista kahdentaa, jopa niin, että yhteydet ovat eri operaattoreilta. Tämä kuitenkin tuo yhteydelle lisähintaa ja tehdään vasta riskianalyysin jälkeen. [Vaatimus 12.2].

Toimipisteiden välinen liikenne voidaan luokitella (QoS, Quality of Service), jolloin ennalta määritelty liikennetyyppi saa etusijan muuhun liikenteeseen verrattuna. Reaaliaikasovelluksille (esim. IP-puhe) ja liiketoiminnan kannalta kriittisille sovelluksille annetaan muita korkeampi luokitus. [Vaatimus 12.3].

Kansallisen salassa pidettävän tiedon siirrossa käytetään salausta, kun verkko menee viran-omaisen valvoman tilan ulkopuolelle [Vaatimus 12.4]. Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon siirrossa käytetään salausta aina, kun verkko menee viranomaisen valvoman tilan ulkopuolelle [Vaatimus 12.5]. Tällaisia tiloja ovat Internetin lisäksi muun muassa operaattoriverkot sekä maan alla kulkevat kaapeloinnit, joihin pääsyä ei voida itse luotettavasti valvoa. Salaus voi olla toteutettu verkon palveluna, verkon reunalaitteiden välillä tai sovellustason salauksena. Salaukseen tulee käyttää vähintään siirrettävän aineiston suojaustasolle hyväksyttyjä salausratkaisuja [Vaatimus 12.6]. Erityisesti kansainvälisen turvallisuusluokitellun tiedon salaamiseksi edellytetään käytettävän vain tiedon omistajan (esimerkiksi EU) tai salaustuotteiden hyväksyntäviranomaisen[3] hyväksymiä salausratkaisuja.

12.2 Verkon aktiivilaitteiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
12.1	Organisaation liiketoiminnan vaatimusten pohjalta on arvioitu yhteyksien kriittisyys ja sovittu palvelutasoista (SLA) palveluntarjoajan kanssa.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
12.2	Kriittiset toimipisteiden väliset tai internet-yhteydet on kahdennettu.	suositus	suositus	pakollinen vaatimus
12.3	Kriittiset sovellukset ja protokollat luokitellaan palvelulaatumäärittelyssä (QoS) muita sovelluksia korkeammalle tasolle.	suositus	vahva suositus	pakollinen vaatimus
12.4	Kansallisen salassa pidettävän tiedon siirrossa käytetään salausta, kun verkko menee viranomaisen valvoman tilan ulkopuolelle.	suositus	suositus	pakollinen vaatimus
12.5	Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon siirrossa käytetään salausta aina, kun verkko menee viranomaisen valvoman tilan ulkopuolelle.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
12.6	Salaukseen tulee käyttää vähintään siirrettävän aineiston suojaustasolle hyväksyttyjä salausratkaisuja	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

[3] CAA, Crypto Approval Authority, Suomessa Viestintäviraston NCSA-FI-yksikkö.

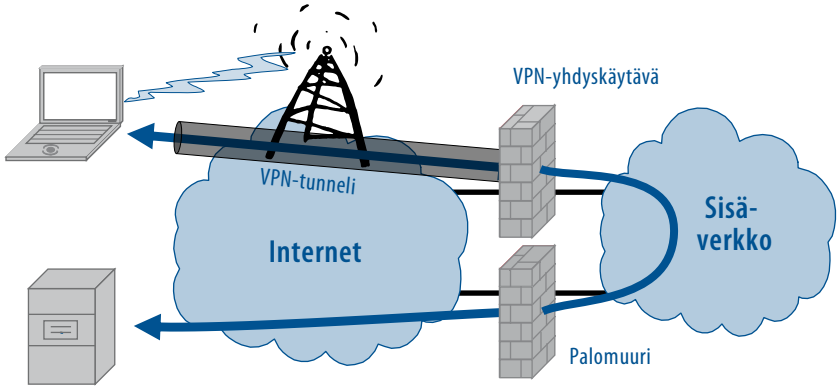
13 Sisäverkon päätelaitteet

Päätelaitteet tarjoavat käyttäjälle rajapinnan (verkon) palveluihin. Työasemien, palvelinten ja älypuhelimien lisäksi päätelaitteita ovat mm. IP-puhelimet, tulostimet, kameravalvonta, kulunvalvonta ja taloautomaation protokollasovittimet. Näiden suojaamisesta lisätietoja on saatavilla muista tietoturvallisuusohjeista (esim. KATAKRI:n I 502 ja I 604).

Päätelaitteeseen (esim. työasema) voidaan kytkeä ylimääräinen yhteyslaite (esim. ”nettitikku”) vain erityisestä syystä ja silloinkin vain tietohallintohenkilöstön toimesta. Tällöin työasemaa ei kytketä suoraan sisäverkkoon, vaan mahdollinen sisäverkkoliikenne hoidetaan vahvasti suojatun VPN-yhteyden yli erillisyhteyttä käyttäen. Tämä vaatii huolellisuutta verkkoyhteyksien konfiguroinnissa.

Internet-palveluiden käyttö on sallittu ainoastaan organisaation sisäverkosta tai etäyhteyden (VPN) kautta [Vaatimus 13.1]. Kuvassa 4 on esitetty millä tavalla liikenne kulkee käyttäjän ja Internet-palvelun välillä VPN-yhteyttä käyttäen. Teknisesti suora yhteydenmuodostus Internet-palveluihin on estetty työaseman palomuurisäännöillä ja rajoittamalla käyttäjän oikeuksia työasemaan. Poikkeustapauksia ovat esim. web-selainlaajennuksilla toteutetut SSL-VPN- / virtuaalityöpöytäratkaisut.

Kuva 4 Esimerkki Internet-palveluiden käytöstä VPN-yhteyden yli.



Päätelaitteet ovat yksilöityjä ja verkon tunnistettavissa siten, että yksittäinen laite voidaan määrittää sisäverkkoon kuuluvaksi tai siihen kuulumattomaksi [Vaatimus 13.2]. Tuntemattomien päätelaitteiden kiinnittäminen verkkoon on estetty kytkinporttien asetuksilla [Vaatimus 13.4]. Tunnistautumista käsitellään tarkemmin kappaleessa 15.

Päätelaitteissa on soveltuvilta osin käytössä laitekohtainen palomuuri [Vaatimus 13.6].

Päätelaitteille suoritetaan automaattinen tarkastus ennen niiden liittämistä sisäverkkoon. Tarkastuksen avulla varmistetaan laitekohtaisen palomuurin ja virustorjunnan olemassaolo, päivitysten ajantasaisuus, jne. Organisaatio on laatinut tarkat määritykset terveystarkastuksen sisällölle. [Vaatimus 13.7].

13.1 Teknologiatausta

Yksinkertaisimmillaan päätelaitteet voidaan tunnistaa Ethernet-verkossa laiteosoitteensa (MAC-osoite) perusteella. Laiteosoitteet ovat laitevalmistajan asettamia, mutta useimmissa tapauksissa helposti vaihdettavissa. Tästä syystä MAC-tunnistuksen tarjoama suoja on varsin rajattua. Useat verkkolaitevalmistajat tarjoavat MAC-tunnistusmahdollisuuden sisäänrakennettuna laitteissaan (esim. Cisco:n port security -ominaisuus).

13.1.1 Työasemat

Edelleen yleisin verkon päätelaite on käyttäjän työasema – joko pöytäkone tai kannettava. Käyttöjärjestelmänä on useimmiten Microsoft Windows, mutta muitakin esim. Linux- ja Mac OS -pohjaisia työasemia käytetään.

Työasemia- ja niiden oheislaitteita valittaessa on otettu huomioon ylläpidettävyys sekä osien riittävä keskinäinen yhteensopivuus ja vaihdettavuus. Etähallittavat komponentit mahdollistavat keskitetyn ylläpidon. Mitä yhtenäisempi työasemakanta organisaatiolla on, sitä helpompi on kehittää laitteistoon ja varusohjelmistoon liittyvää syvällisempää osaamista, huolehtia varajärjestelyistä sekä tehdä tarvittavia muutoksia. [Vaatimus 13.8]. Yhtenäisyys on otettu huomioon tarkoituksenmukaisella tavalla muun muassa laitteiden kokoonpanossa, asetuksissa ja työasemien hakemistorakenteessa.

Työasemilta avatut etäyhteydet eivät saa jäädä valvomatta. Istunnon aikakatkaisu tai vähintään automaattinen lukitus on otettu käyttöön. [Vaatimus 13.5]. Työasemissa on käytössä työasemakohtainen palomuuri [Vaatimus 13.10]. Kannettavien työasemien kiintolevyt on salattu [Vaatimus 13.11]. Pöytätyöasemien osalta kiintolevyjen salausta vaaditaan vasta korkealla tasolla. [Vaatimus 13.12].

Käyttäjiä on koulutettu työasemiin liittyvistä riskeistä. Päätelaitteiden turvallisesta verkkokäytöstä on laadittu lyhyet ja selkeät ohjeet – kullekin päätelaitetyypille omansa [Vaatimus 13.3].

13.1.2 Mobiilit päätelaitteet (mobiililaitteet)

Mobiileiksi päätelaitteiksi (mobiililaitteiksi) luetaan mm. älypuhelimet ja PDA-laitteet – yleisemmin taskukokoiset laitteet, joilla on mahdollista muodostaa yhteys organisaation verkkoon. Useimmiten tällä viitataan WLAN-tuen sisältäviin laitteisiin.

Mobiililaitteet, älypuhelin yleisimpänä esimerkkinä, ovat laitteita, jotka seuraavat käyttäjäänsä käytännössä kaikkialle useiden eri verkkojen alueella. Lisäksi mobiililaitteissa on usein tuki useammalle eri langattomalle yhteydelle (kuten 2G/EDGE, 3G/4G, WLAN ja Bluetooth). Tämä altistaa laitteet jatkuvasti potentiaalisille hyökkäyksille. Laitteiden tietoliikenneyhteydet ovat konfiguroitu oletusarvoisesti pois päältä ja vähintään niin, että yhteydet sallitaan ainoastaan tiettyihin verkkoihin.

Mobiililaitteet myös hukkuvat pienen kokonsa vuoksi helposti. Laitteissa on otettu mahdollisuuksien mukaan käyttöön suojausominaisuuksia, joita ovat esim. laitteen ja muistikortin salaus, suojakoodi ja etätyhjennys. Lisäksi laitteissa säilytettävän arkaluontoisentiedon määrä on minimoitu.

Mobiililaitteiden suojauksessa tulee huomioida Älypuhelimien tietoturvallisuus – hyvät käytännöt (VAHTI 2/2007) ohjeessa ja sen liitteissä annettuja suosituksia. Mobiililaiteiden loppukäyttäjiä on ohjeistettu niiden turvalliseen käyttöön, esimerkiksi käyttäen pohjana ja muokaten Älypuhelinten turvallinen käyttö –ohjetta (VAHTI 2/2007, muokattava liite) [Vaatimus 13.9].

13.2 Päätelaitteiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
13.1	Internet-palveluiden käyttö on sallittu ainoastaan organisaation sisäverkosta tai etäyhteyden (VPN) kautta.	suositus	pakollinen vaatimus	pakollinen vaatimus
13.2	Kullakin päätelaitteella on yksilöity tunnus. Identtiset laitekokoonpanot erotetaan em. tunnuksen perusteella.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
13.3	Käyttäjille on laadittu lyhyet, selkeät ohjeet päätelaitteiden turvallisesta verkkokäytöstä - kullekin päätelaite-tyypille omansa.	suositus	pakollinen vaatimus	pakollinen vaatimus
13.4	Tuntemattomien päätelaitteiden kiinnittäminen verkkoon on estetty kytkinporttien asetuksilla.	suositus	vahva suositus	pakollinen vaatimus
13.5	Työasemilta avatuissa etäyhteyksissä on automaattinen aikakatkaisu.	suositus	vahva suositus	pakollinen vaatimus
13.6	Päätelaitteissa on soveltuvilta osin käytössä laitekohtainen palomuuri.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
13.7	Päätelaitteille suoritetaan automaattinen terveystarkastus ennen niiden liittämistä sisäverkkoon.	suositus	suositus	suositus
13.8	Työasema- ja muu päätelaitekanta on yhtenäistetty.	suositus	suositus	vahva suositus
13.9	Mobiililaiteiden loppukäyttäjiä on ohjeistettu niiden turvalliseen käyttöön, esimerkiksi käyttäen pohjana ja muokaten Älypuhelinten turvallinen käyttö –ohjetta (VAHTI 2/2007, muokattava liite)	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
13.10	Työasemissa on käytössä työasema-kohtainen palomuuri.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
13.11	Kannettavien työasemien kiintolevyt on salattu	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
13.12	Pöytätyöasemien kiintolevyt on salattu	suositus	vahva suositus	pakollinen vaatimus

14 Sisäverkon palvelut

Tässä kappaleessa käsitellään sellaisia verkon palveluita, joiden avulla on mahdollista pystyttää itsenäisesti toimiva verkko.

Valtaosa sisäverkon palveluista noudattaa tätä arkkitehtuuria, vaikka P2P-arkkitehtuurin suosio onkin viime vuosina kasvanut. Ero eri arkkitehtuureissa on lähinnä se, että P2P-arkkitehtuurissa asiakas-/palvelin-roolijako on hämärtynyt (P2P-sovellus voi toimia sekä asiakas- että palvelinroolissa, aina tarpeen mukaan roolia vaihtaen). Palvelin-/asiakassovelluksien tietoturvapäivitykset pidetään ajan tasalla [Vaatimus 14.2].

Palveluiden määrä palvelimilla on minimoitu. Yksi palvelin (fyysinen tai virtuaalinen) hoitaa pääasiassa yhtä tehtävää (esim. WWW-palvelin, DNS-palvelin, tiedostopalvelin). [Vaatimus 14.8].

14.1 Verkon toiminnan varmistavat palvelut

Tässä esitellyt palvelut ovat perusedellytys toimivalle verkkoympäristölle ja mahdollistavat kommunikaation laitteiden välillä.

Kriittisten infrapalveluiden, eli osoite-, reititys- ja nimipalvelun toimivuus on varmistettu tarkoituksen mukaisella palvelutasolla ja varautumisen tasolla [Vaatimus 14.3]. Tällöin huomioidaan käytössä olevan ympäristön tietoturva- ja ICT-varautumisen tasojen edellyttämät vaatimukset. Ylimääräisten infrapalveluiden asentaminen sisäverkkoon on kielletty [Vaatimus 14.4].

Verkoissa käytetään osoite-, reititys- ja nimipalvelun lisäksi ARP-protokollaa (Address Resolution Protocol). Näihin kaikkiin liittyy yhteisenä tietoturvariskinä välistävetohyökkäys (man-in-the-middle attack). Jos verkossa on IDS/IPS-järjestelmä, on sen syytä pyrkiä tunnistamaan tämän tapaiset hyökkäykset (esim. MAC-IP-osoiteparien eroavuudet).

14.1.1 Teknologiatausta: Osoitepalvelu

Verkon toiminnallisuuden kannalta on ensiarvoisen tärkeätä yksilöidä kaikki verkon laitteet. Tämä tapahtuu verkko-osoitteella. Aikanaan, verkkojen ollessa verrattain pieniä, osoitteet asetettiin verkon laitteille käsin. Nykyisissä

verkoissa tämä ei enää ole käytännöllistä. Avuksi ovat tulleet erilaiset osoitepalvelut, mm. DHCP, jolta laite voi pyytää itselleen osoitteen.

Osoitepalvelut mahdollistavat myös osoitteiden kiinnittämisen siten, että tietty laite saa aina saman osoitteen. Tämä saattaa olla joissakin tilanteissa käytännöllistä.

Osoitteen lisäksi osoitepalvelut tarjoavat laitteille yleensä ainakin reititys- ja nimipalvelintiedot.

Osoitepalveluun liittyy seuraavia tietoturvariskejä

- Avoimeksi määritelty osoitepalvelu tarjoaa osoitetiedot kaikille verkkoon liittyville laitteille tunnistamatta niitä millään tavoin.
- Päätelaite ei tunnista osoitepalvelua, eli laitteelle voi antaa väärää tietoa, mikäli hyökkääjä saa tuotua oman osoitepalvelunsa verkkoon.
- Hallitsemattomasti käynnistetty DHCP-osoitepalvelu, esim. kotoa tuotu WLAN-tukiasema, voi sekoittaa vakavasti verkon toimintaa.
- Osoitepalvelun toimimattomuus haittaa uusien laitteiden liittämistä verkkoon. DHCP-osoitepalvelu on siis verkon kannalta kriittinen komponentti, jonka toiminta on syytä varmistaa.

14.1.2 Teknologiatausta: Reitityspalvelu

IP-osoiteavaruus on jaettu verkkoalueiksi, joiden välillä kommunikointi edellyttää reitityspalvelua. Käytännössä reitityspalvelu hoitaa tiedonsiirron sisäverkosta ulospäin (fyysisesti erilliseen verkkoon, toiseen VLANiin tai Internetiin).

Päätelaitteen kannalta on oleellista tietää oletusreitti (default gateway), jonne liikenne ohjataan, mikäli kohde ei löydy samasta verkkoalueesta. Oletusreitittimen tiedot laite saa useimmiten osoitepalvelulta.

Reitittimet hoitavat varsinaisen reitityksen. Käytännössä tämä perustuu reititystauluihin, joita reitittimet vaihtavat keskenään. Sisäverkon reititysprotokollaksi on valittu suojattua tunnistautumista tukeva protokolla [Vaatimus 14.1].

DMZ-alueella käytetään pelkästään staattista reititystä [Vaatimus 14.10].

Reitityspalveluun liittyy seuraavia tietoturvariskejä

- Mikäli hyökkääjä pääsee kiinni reititystauluihin, pystyy hän käytännössä ohjaamaan verkon liikennettä haluamallaan tavalla, esim. oman koneensa kautta.

14.1.3 Teknologiatausta: Nimipalvelu

Verkko-osoitteet ovat monimutkaisia ja vaikeasti muistettavia, minkä takia niiden päälle on rakennettu erilaisia nimipalveluita. Nimipalvelun ideana on pitää kirjaa laitteille annetuista nimistä ja löytää vastaava osoite, jolla itse kommunikointi tapahtuu.

Nimipalveluista yleisin on internetissä käytetty DNS. Lisäksi esimerkiksi Microsoft Windows-ympäristöstä löytyy ns. Netbios-nimijärjestelmä. Kummassakin menetelmässä nimipalvelua pyörittää keskitetty nimipalvelin, tai vaihtoehtoisesti nimet voi määritellä paikallisesti laitteessa itsessään (ei kuitenkaan toimi kovin laajoissa verkoissa).

DNS-nimipalvelu on hierarkinen: mikäli paikallinen nimipalvelin ei vastausta tiedä, kysyy se ylempää hierarkiasta.

DNS-nimipalvelussa ulospäin Internet-verkkoon näkyvä julkinen DNS-palvelin on erotettu sisäisestä DNS-palvelimesta. Ulospäin näkyvä palvelin palvelee ulkoverkosta tulevia kyselyitä, ja sisäinen DNS-palvelin taas organisaation sisältä tulevia kyselyitä.

Perus-DNS:n tarjoama tietoturvallisuus on rajallista, kuten vuonna 2008 julkistettu laaja DNS-haavoittuvuus (ks. esim. CERT-FI Tietoturvakatsaus 2b/2008) todisti. Riskin minimoimiseksi on otettu käyttöön DNS:n tietoturvalaajennukset eli DNSSEC (Domain Name System Security Extensions) [Vaatimus 14.5].

Nimipalveluun liittyy seuraavia tietoturvariskejä

- Mikäli hyökkääjä pääsee muokkaamaan nimipalvelun tietoja, saattaa hän pystyä huijaamaan käyttäjän omalle palvelimelleen tai muuten väärään palveluun.
- Nimipalvelu on verkon kannalta erittäin kriittinen palvelu. Jos se ei ole käytettävissä, verkossa ei käytännössä voi liikennöidä. Tästä syystä DNS-nimipalvelu onkin aina vähintään kahdennettu.
- Jos palvelin-/asiakasohjelmistot jätetään päivittämättä, niin todennäköisyys tietoturva-aukon löytymiseen ja sen hyödyntämiseen kasvaa.

14.2 Verkon päälle rakennettavat palvelut

Tässä esitellyt palvelut ovat tyypillisiä arvoa tuottavia lisäpalveluita, jotka rakennetaan edellä mainittujen verkon toiminnan varmistavien palveluiden päälle.

14.2.1 Teknologiatausta: Tukipalvelut – aikapalvelu

Sisäverkossa on oma NTP-palvelin verkon laitteiden ajan synkronoimiseen. NTP-palvelin synk-ronoidaan joko ulkoisen NTP-palvelun tai palvelimeen liitetyn radiokellon kanssa. [Vaatimus 14.9]. Esimerkiksi VY-verkko tarjoaa varmennetun, yhteisen aikalähteen.

14.2.2 Teknologiatausta: Kommunikaatiopalvelut – sähköposti

Sähköposti on yksi käytetyimmistä verkon palveluista. Tietoturvallisuuden kannalta se on ongelmallinen, sillä sähköpostin perustoiminta nojaa vahvasti keskinäiseen luottamukseen. Sähköpostin lähettäjän tiedot on helppo väärentää, eikä sähköposti edellytä salausta tai muuta tietoturvallisuutta.

Sähköpostin etä- tai mobiilikäyttö edellyttää yleensä DMZ-vyöhykkeelle sijoitettavia edusta-palvelimia (frontend servers). DMZ-alueille sijoitettavien palvelimien tietoturvallisuus on erittäin tärkeää, koska niiltä on yleensä sallittu pääsy sisäverkkoon palomuurin läpi yhden tai useamman protokollan ja tietoliikenneportin kautta. Mikäli tietomurtautuja pääsee tällaiseen DMZ-alueen palvelimeen kiinni, pystyy hän mahdollisesti sitä kautta murtautumaan organisaation sisäverkkoon.

Sähköpostin sisällön voi suojata esimerkiksi salaamalla yhteyksiä sähköpostipalvelinten välillä tai salaamalla itse sähköpostiviestit. Viestikohtainen salaus tehdään usein julkisen avaimen salausmenetelmällä, jota voi käyttää myös sähköisen allekirjoituksen toteuttamiseen. Näin voidaan varmistua myös viestin lähettäjän identiteetistä. Ilman viestikohtaista salausta sähköpostit ovat sähköpostipalvelimella salaamattomina. Myöskään Internetin yli siirrettäessä sähköposteja ei oletusarvoisesti salata, jolloin viestikohtainen salaus voi olla tarpeen. Tarkemmin erilaisia salauskäytäntöjä on käsitelty Valtion salauskäytäntöjen tietoturvaohjeessa (VAHTI 3/2008). Useat sähköpostipalvelimet tukevat TLS-salausta, jolla voidaan kustannustehokkaasti toteuttaa kahden organisaatioiden välinen sähköpostiliikenteen salaus. Esimerkiksi VY-verkko tarjoaa SMTP-välityspalvelun, jonka kautta on mahdollista luoda suojattuja yhteyksiä muihin sähköpostinvälityspisteisiin että lähettää ad hoc –salattuja viestejä.

Vastaanotetut ja lähetettävät sähköpostit skannataan virusten, haittaohjelmien ja roskapostien varalta [Vaatimus 14.6]. Esimerkiksi VY-verkko tarjoaa SMTP-välityspalvelun, jonka kautta kulkevat sähköpostit skannataan edellä mainittujen varalta.

14.2.3 Teknologiatausta: Resurssien jako

Resurssien, kuten levyjakojen ja tulostimien, jakaminen on hyvin tyypillinen verkon päälle rakennettava palvelu. Useimmat käyttöjärjestelmät mahdollistavat resurssien jaon sellaisenaan ja työasemaresursseja voi jakaa yhtä lailla kuin

palvelinresurssejakin. Tietoturvasyistä jaetut resurssit on rajattu palvelinlaitteille. Työasemien resurssien jako on estetty. [Vaatimus 14.7].

Käyttäjät eivät saa jakaa työasemiensa resursseja ja oheislaitteita (esim. levyjako, tulostus ja modeemiyhteys) muille käyttäjille. Suositeltavaa on käyttää sellaisia työasemakäyttöjärjestelmiä ja -asetuksia, ettei käyttäjillä ole edes mahdollisuutta jakaa resursseja.

14.3 Palveluiden tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
14.1	Sisäverkon reititysprotokollaksi on valittu suojattua tunnistautumista tukeva protokolla.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
14.2	Sovellusten tietoturvapäivitykset pidetään ajan tasalla.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
14.3	Kriittisten infrapalveluiden, eli osoite-, reititys- ja nimipalvelun toimivuus on varmistettu tarkoituksen mukaisella palvelutasolla ja varautumisen tasolla	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
14.4	Ylimääräisten infrapalveluiden asentaminen sisäverkkoon on kielletty.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
14.5	DNSSEC on otettu käyttöön.	vahva suositus	vahva suositus	pakollinen vaatimus
14.6	Vastaanotetut ja lähetettävät sähköpostit skannataan virusten, haittaohjelmien ja roskapostien varalta.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
14.7	Resurssien jako (esim. kiintolevy, tulostin) on rajattu palvelinlaitteille. Työasemien resurssien jako on estetty.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
14.8	Palveluiden määrä palvelimilla on minimoitu. Yksi palvelin (fyysinen tai virtuaalinen) hoitaa pääasiassa yhtä tehtävää (esim. WWW-palvelin, DNS-palvelin, tiedostopalvelin).	vahva suositus	vahva suositus	pakollinen vaatimus
14.9	Sisäverkossa on oma NTP-palvelin verkon laitteiden ajan synkronoimiseen. NTP-palvelin synkronoidaan joko ulkoisen NTP-palvelun tai palvelimeen liitetyn radiokellon kanssa.	suositus	vahva suositus	pakollinen vaatimus
14.10	DMZ-alueella käytetään pelkästään staattista reititystä.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

15 Tunnistautuminen

Sisäverkossa on tarvetta niin laitteiden kuin käyttäjien tunnistautumiselle sisäverkon eri tasoilla. Tunnistautumisessa tärkeää on, että käyttäjältä vaaditaan mahdollisimman vähän toimia pitäen silti yllä korkea tunnistautumisen taso.

Sisäverkon näkökulmasta tunnistautumiseen ovat käytössä seuraavat mahdollisuudet

- **Päätelaitteen tunnistautuminen verkkoon:** Verkko tunnistaa päätelaitteet, jotka kytketään verkkoon. Pelkän päätelaitetunnistautumisen perusteella annetaan verkkoon vain hyvin rajattu pääsy [Vaatimus 15.16], esimerkiksi vain käyttäjäntunnistautumispalvelimelle. Tämä voidaan toteuttaa esimerkiksi tekemällä verkkosegmentti, johon kaikki tunnistautuneet laitteet sijoitetaan kunnes laitteen käyttäjä on tunnistautunut.
- **Palvelimen tunnistautuminen verkkoon:** Verkko tunnistaa palvelimet, jotka kytketään verkkoon. Palvelinten käyttäjät voivat tällöin olla varmempia siitä, että he ottavat yhteyttä laitteisiin, joita kuvittelevat käyttävänsä. Lisäksi tätä tunnistautumista käyttämällä voidaan hankaloittaa välistävetohyökkäyksen (man-in-the-middle attack) suorittamista.
- **Käyttäjän tunnistautuminen verkkoon:** Verkko tunnistaa käyttäjät riittävän luotettavalla menetelmällä. Minimitaso on käyttäjätunnus ja riittävän laadukas salasana. Suositeltavaa on käyttää muita menetelmiä, kuten toimikorttia. Joissakin teknologioissa ei ole lainkaan käytössä käyttäjän tunnistautumista verkkoon.
- **Käyttäjän tunnistautuminen verkon peruspalveluihin:** Palveluun tunnistautuminen voidaan toteuttaa verkkoon tunnistautumisen avulla tai erillisellä tunnistautumisratkaisulla.
- **Ylläpitäjän tunnistautuminen:** Ylläpitäjät omaavat laajat valtuudet, joten avoimien verkkojen kautta toimittaessa heidän tunnistautumiseensa käytetään vahvaa tunnistautumista [Vaatimus 15.20].

Organisaatiossa tehtävä tunnistautuminen perustuu kirjalliseen pääsynvalvontapolitiikkaan, jossa kuvataan tunnistautumisen tavoitteet ja menetelmät

[Vaatimus 15.9]. Tunnistautumisratkaisuja tehtäessä yllä olevasta listasta valitaan sopivat menetelmät, joilla saavutetaan riittävä varmuus eri toimijoiden identiteetistä. Valinta perustuu analyysiin tunnistautumistarpeista suhteessa tunnistautumisella saatavalla pääsyllä tietoon tai palveluun. [Vaatimus 15.1]. Kaikki käyttäjät ovat hallittujen tunnistautumisratkaisujen piirissä. Mikäli tapahtumassa ei voida tunnistaa käyttäjää, on tunnistettava laite käytössä olevien tunnistautumisratkaisujen piirissä. [Vaatimus 15.4].

Käyttäjän tunnistautuminen on osa laajempaa käyttäjähallintaprosessia, jossa määritellään käyttäjien elinkaari, tunnistautumis- ja käyttöoikeustietojen välittäminen eri komponenteille sekä ylläpitoprosessit. Näillä varmistutaan siitä, että käyttöoikeudet vastaavat kulloistakin tehtävää. [Vaatimus 15.15].

Tunnistautumisessa käytetään menetelmiä, joissa tunnistautumiseen käytettävät tiedot, kuten käyttäjätunnukset ja salasanat eivät kulje verkon yli salaamattomana [Vaatimus 15.17].

Valtionhallinnon yhteisiä tietojärjestelmiä käytettäessä suositellaan käytettäväksi virkamiehen tunnistautumista (Virtu) niissä palveluissa, joissa se on tuettuna. VIP:in Virtu-palvelu perustuu virastojen ja palveluntarjoajien muodostamaan luottamusverkostoon ja mahdollistaa kertakirjautumisen (Single Sign On, SSO) valtionhallinnon yhteisiin palveluihin. Viraston Virtu IdP-palvelinta voi lisäksi käyttää kertakirjautumisessa viraston omiin palveluihin. Virtu vähentää erillisten käyttäjätunnusten tarvetta sekä säästää aikaa, vaivaa ja rahaa. Virtu-palveluun ei sen alkuvaiheessa sisälly yhteistä Virtu IdP- palvelua (=virkamiehen tunnistuspalvelu), vaan se on viraston oma tehtävä. IdP-palvelun perustaminen Virtun yhteyteen tullee kuitenkin ajankohtaiseksi vuoden 2010 loppupuolella. Käyttövaltuuksien hallinta on joko viraston tai palveluntuottajan tehtävä.

Ennen liittymistä Virtuun kotiorganisaatiot auditoidaan valtionhallinnon tietoturvatasojen korotetun tason vaatimuksien mukaisesti. Organisaation hallinnollisen tietoturvallisuuden auditoinnin osalta organisaatio rajataan Virtun kannalta tarkoituksen mukaisesti. Mikäli auditointitulosten arvioinnissa ei löydy vakavia poikkeamia perustason vaatimuksista, virasto hyväksytään Virtu-luottamusverkoston jäseneksi. Mikäli näitä poikkeamia löytyy, VIP:in Tietoturvapalvelut voivat auttaa virastoa tekemään suunnitelman niiden korjaamiseksi, ja korjausten todentamisen jälkeen virasto hyväksytään Virtu-luottamusverkoston jäseneksi. Organisaation tulee saavuttaa korotettu taso tietoturvallisuusasetuksessa edellytetyn siirtymäajan puitteissa.

Käyttäjän tunnistautumisessa käytetään henkilökohtaisia tunnuksia, yhteiskäyttöiset tunnukset ovat kiellettyjä [Vaatimus 15.2]. Ylläpitoyhteyksissä (verkon peruspalvelut ja verkkolaitteet) käytetään henkilökohtaisia tunnuksia. Ylläpitotunnukset poistetaan käytöstä, mikäli niiden käyttäjä on pitkään poissa, esim. vuorotteluvapaalla. Verkon ylläpitämiseen käytettävät tunnukset sidotaan ylläpitovarmenteisiin tai ne kirjoitetaan ylös ja talletetaan turvalliseen paikkaan, kuten kassakaappiin. Yksittäinen henkilö ei saa ottaa tunnuksia kassakaapista. [Vaatimus 15.19].

Tunkeutuja saattaa yrittää murtautua järjestelmään yrittämällä kirjautua sisään kokeillen eri tunnuksia useita kertoja peräkkäin. Tämän vuoksi tunnus lukitaan, mikäli järjestelmään yritetään kirjautua monta kertaa peräkkäin siten, että tunnistautuminen epäonnistuu [Vaatimus 15.7]. Suositeltavaa on, että tunnus lukitaan esim. viiden epäonnistuneen yrityksen jälkeen. Tietoturvallisuuden näkökulmasta vähemmän kriittiset palvelut voidaan asettaa siten, että lukkiutunut tunnus avataan automaattisesti esimerkiksi tunnin kuluttua.

Pääsynvalvontalokeja voidaan käyttää mm. väärinkäyttöepäilyjen selvittämiseen, jonka takia epäonnistuneet kirjautumisyritykset sekä muut valtuuksien puutteeseen kariutuvat toimenpideyritykset kirjataan lokiin [Vaatimus 15.12]. Pääsynvalvontalokeja säilytetään siten, että niitä ei päästä jälkikäteen muuttamaan [Vaatimus 15.8]. Tämä voidaan toteuttaa mm. keskitetyllä lokienhallintaratkaisulla.

15.1 Teknologiaratkaisuja tunnistautumiseen

Tunnistautumiseen liittyvissä tekniikoissa, kuten useassa muussa teknisen tietoturvallisuuden osa-alueessa on havaittavissa ilmiö, jossa jonkin tietyn teknologian tietoturvallisuus heikkenee koko ajan, kun tiedeyhteisö sekä sen ulkopuoliset toimijat keksivät keinoja tunnistautumismenetelmien murtamiseksi sekä tietokoneiden laskentateho kasvaa. Siksi tunnistautumista parannetaan koko ajan teknologiamielessä, jotta taso pysyisi edes samana. Tämä saavutetaan säännöllisellä arvioinnilla tunnistautumismenetelmien riittävyydestä [Vaatimus 15.18]. Alla esitetään tällä hetkellä hyviä tunnistautumiseen liittyviä tekniikoita, mutta teknologiaratkaisujen yhteydessä tulee aina selvittää, miten hyviä teknologioita on sillä hetkellä tarjolla:

- **Käyttäjätunnus/salasana:** Yksinkertaisin tapa tunnistautumiseen, joka sopii käytettäväksi silloin, kun ollaan organisaation omassa tilassa tai kun tunnistautumisen jälkeen ei ole vielä pääsyä arkaluontoiseen tietoon. Pelkkää käyttäjätunnus-/salasanaparia ei käytetä etäyhteyksien muodostamiseen [Vaatimus 15.3]. Tunnistautumiseen ei yleisesti käytetä pelkkää käyttäjätunnus/salasanaparia. Vain erityisen hyvin fyysisesti suojatussa ympäristössä voidaan kirjautua käyttäen käyttäjätunnus/salasanaparia. [Vaatimus 15.13]. Kaikkien verkkotuotteiden ja varusohjelmistojen oletustunnusten salasanat on vaihdettu oletusarvoistaan [Vaatimus 15.15]. Salasanaa ei saa säilyttää salaamattomana tai huonosti salattuna. Käytettäessä käyttäjätunnus-/salasanaparia, luodaan riittävän hyvä salasanapolitiikka, joka koskee kaikkia palveluita ja käyttäjiä [Vaatimus 15.6]. Hyvä salasanapolitiikka on vähintään seuraavanlainen

  - Salasanan pituus on vähintään 10 merkkiä
  - Salasanassa pitää olla merkkejä vähintään kolmesta luokasta (pienet kirjaimet, isot kirjaimet, numerot, erikoismerkit)
  - Salasanan enimmäisikä on 90 päivää
  - Salasanan vähimmäisikä on 1 päivä
  - Salasana ei saa olla sama kuin 5 edellistä salasanaa
  - Salasana lukitaan esim. viiden virheellisen yrityksen jälkeen ja korkean turvallisuuden järjestelmissä vapautetaan vasta ylläpidon toimesta
  - Huomattava kuitenkin on, että kaikissa järjestelmissä teknisistä syistä ei ole mahdollista noudattaa kaikkia hyvän salasanapolitiikan vaatimuksia.
- **Toimikortti:** Vahva tunnistautumismenetelmä, jossa erillisellä kortilla on tallennettuna käyttäjän tunnistetiedot. Toimikorttia käytetään silloin, kun on tarve tehdä vahva tunnistautuminen. Toimikortilla tapahtuvaa tunnistautumista voi käyttää myös tavallisessa toimistoympäristössä. Mikäli toimikorttia ei voida ottaa käyttöön, tehdään vahva tunnistaminen käyttämällä muuta vahvaa tunnistamista, kuten vaihtuvaa salasanaa, joka voidaan toteuttaa esim. alla kuvatulla tunnistelaitteella. [Vaatimus 15.5].
- **Tunnistelaite (Security token):** Laite, jota käytetään käyttäjätunnuksen ja salasanan lisäksi tuomaan lisäturvaa tunnistautumiselle. Laitteita on erilaisia ja tyypillisin käytettävä laitetyyppi on sellainen, jossa näytetään ajan mukaan vaihtuva salasanaa. Käyttämällä vaihtuvaa salasanaa voidaan tehdä vahva tunnistautuminen. Esimerkiksi matkapuhelimen välityksellä tesktiviestinä toimitettava lisätunniste on eräs keino toteuttaa vahvassa tunnistautumisessa tarvittava tunnistuslaite ja ratkaisu.
- **Biotunniste:** Tunnistautuminen, joka perustuu johonkin ihmisen piirteeseen, joka on lähes jokaisella ihmisellä erilainen, kuten sormenjäljet, ääninäyte tai kasvokuva. Biotunnisteisiin liittyy tietoturvallisuuden ja tietosuojan kannalta ratkaisemattomia ongelmia, kuten biotunnisteen vaihtaminen, biotunnisteen väärentäminen ja ihmisten liikkeiden valvominen. Tästä syystä niitä käytetään vain erittäin korkeaa tietoturvallisuutta vaativissa järjestelmissä ja tällöinkin lisänä jollekin muulle hyvälle tunnistautumiselle.
- **802.1x:** Menetelmä, jolla verkkoon liittyvä laite voidaan tunnistaa ja sille voidaan sitä kautta antaa pääsy verkkoon. Teknologiaa voidaan käyttää langallisten ja langattomien verkkojen yhteydessä. Varsinainen autentikointi tapahtuu EAP-viesteillä, joten tunnistautumiseen voi käyttää lähes mitä tahansa menetelmää, esim. salasanaa, biotunnistetta tai toimikorttia. Menetelmä mahdollistaa myös laitteen sijoittamisen

haluttuun virtuaaliverkkoon autentikointitapahtuman perusteella. Dynaamista sijoittamista tulee harkita ainakin sellaisissa paikoissa, joissa organisaation ulkopuoliset toimijat saattavat käyttää verkkoa. Tällöin laitteet on mahdollista sijoittaa automaattisesti vierailijaverkkoon, josta on esim. vain www-yhteys ulkoverkkoon, eikä mitään pääsyä sisäverkkoon.

Varmenteet ovat erittäin luotettavia tunnistautumisratkaisuja, joten niiden myöntämisessä on syytä noudattaa erityistä tarkkuutta. Varmenteiden myöntämiseen, käyttöön ja uusimiseen on tehty kirjallinen yksityiskohtainen ohjeistus [Vaatimus 15.10]. Käytössä olevista varmenteista pidetään ajantasaista listaa [Vaatimus 15.11].

15.2 Tunnistautumisen tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
15.1	Tunnistautumisten lajeista on valittu sopivat menetelmät ja valinta perustuu analyysiin tunnistautumistarpeesta.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.2	Käyttäjän tunnistamisessa käytetään henkilökohtaisia tunnuksia. Tämä koskee myös ylläpitotunnuksia.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.3	Etäyhteyksien muodostamiseen ei käytetä pelkkää käyttäjätunnus-/salasanaparia.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.4	Kaikki käyttäjät ja päätelaitteet ovat hallittujen tunnistautumisratkaisujen piirissä.	vahva suositus	vahva suositus	pakollinen vaatimus
15.5	Toimikorttia käytetään silloin, kun on tarve tehdä vahva tunnistaminen. Mikäli toimikortti ei ole käytössä, tehdään vahva tunnistaminen käyttämällä vaihtuvaa salasanaa.	vahva suositus	vahva suositus	pakollinen vaatimus
15.6	Käytettäessä käyttäjätunnus-/salasanaparia, luodaan salasanapolitiikka, joka koskee kaikkia palveluita ja käyttäjiä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.7	Tunnus lukkiutuu, mikäli järjestelmään yritetään epäonnistuneesti liian monta kertaa peräkkäin.	suositus	pakollinen vaatimus	pakollinen vaatimus
15.8	Pääsynvalvontalokeja säilytetään siten, että niitä ei päästä jälkikäteen muuttamaan.	suositus	vahva suositus	pakollinen vaatimus
15.9	Organisaatiolla on kirjallinen pääsynvalvontapolitiikka	suositus	pakollinen vaatimus	pakollinen vaatimus
15.10	Varmenteiden myöntämiseen, käyttöön ja uusimiseen on olemassa yksityiskohtainen kirjallinen ohjeistus.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus

15.11	Käytössä olevista varmenteista on ajantasainen lista.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
15.12	Epäonnistuneet kirjautumisyritykset sekä muut valtuuksien puutteeseen kariutuvat toimenpideyritykset kirjataan.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.13	Tunnistautumiseen ei yleisesti käytetä pelkkää käyttäjätunnus-/salasanaparia. Vain erityisen hyvin fyysisesti suojatussa ympäristössä voidaan kirjautua käyttäen käyttäjätunnus/salasanaparia.	suositus	vahva suositus	pakollinen vaatimus
15.14	Kaikkien verkkotuotteiden ja muiden valmisohjelmistojen oletustunnusten salasanat on vaihdettu oletusarvosta tai oletustunnus on poistettu.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.15	Organisaatio on määritellyt käyttäjänhallintaprosessin, jotta voidaan varmistua, että käyttöoikeudet vastaavat kulloistakin tehtävää.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.16	Pelkän päätelaitetunnistautumisen perusteella annetaan verkkoon vain hyvin rajattu pääsy.	suositus	vahva suositus	pakollinen vaatimus
15.17	Tunnistautumisessa käytetään menetelmiä, joissa tunnistautumiseen käytettävät tiedot, kuten käyttäjätunnukset ja salasanat eivät kulje verkon yli salaamattomana.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
15.18	Tunnistautumismenetelmien riittävyys arvioidaan säännöllisesti	suositus	vahva suositus	pakollinen vaatimus
15.19	Verkon ylläpitämiseen käytettävät tunnukset sidotaan ylläpitovarmenteisiin tai ne kirjoitetaan ylös ja talletetaan turvalliseen paikkaan, kuten kassakaappiin. Yksittäinen henkilö ei saa ottaa tunnuksia kassakaapista.	suositus	vahva suositus	pakollinen vaatimus
15.20	Ylläpitäjät omaavat laajat valtuudet, joten avoimien verkkojen kautta toimittaessa heidän tunnistautumiseensa käytetään vahvaa tunnistautumista	suositus	pakollinen vaatimus	pakollinen vaatimus

16 Verkon hallinta/valvonta

Sisäverkko ei pysy kauaa täysin samanlaisena, vaan siihen täytyy tehdä muutoksia uusien palveluiden tai päätelaitteiden lisäämiseksi tai vanhojen poistamiseksi. Nämä muutokset tehdään verkon suunnitteluvaiheen periaatteiden mukaisesti, jotta tietoturvallisuus pysyy suunnitellun mukaisena [Vaatimus 16.3]. Lisäksi verkon toimintaa valvotaan, jotta voidaan varmistaa sen toiminta tietoturvanäkökulmasta. Verkon hallintaan ja valvontaan määritellään selkeä vastuullinen henkilö tai organisaatio [Vaatimus 16.11].

Verkon hallinnassa huomioidaan seuraavat asiat

- Hallinta-/valvontatoiminta on erotettu muusta verkon liikenteestä esim. loogisesti erilliseen segmenttiin. [Vaatimus 5.11].
- Hallintaliikenne salataan riittävällä tasolla, jotta ulkopuolinen henkilö ei pysty seuraamaan tehtäviä muutoksia eikä tunnistautumaan hallintakäyttäjänä [Vaatimus 16.4].
- Verkon hallinnan yhteydessä jokaisesta muutoksesta otetaan varmuuskopio, jotta ongelmatilanteessa vikaantunut verkon laite saadaan korvattua nopeasti uudella laitteella samaan konfiguraatioon kuin vikaantunut laite oli [Vaatimus 16.5].

Verkon valvonnassa huomioidaan seuraavat asiat

- Etukäteen määritellään, mitä asioita valvotaan, mitkä ovat sellaisia asioita, että niistä tulee hälytys ja kuka on vastuussa valvomisesta [Vaatimus 16.6].
- Verkon laitteet konfiguroidaan siten, että ne tekevät riittävästi lokikirjauksia, lokit suojataan muutoksilta ja ne kerätään talteen [Vaatimukset 16.2,16.8]. Lisäksi varmistetaan, että lokeista saa tarkasti tietoa siitä, mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta (audit trail) [Vaatimus 16.15]. Verkon lokeja ja erityisesti etäylläpidon lokeja käydään läpi säännöllisesti [Vaatimus 16.18].
- Valvontaan liittyvillä tunnuksilla on vain lukuoikeus verkon lokitietoihin [Vaatimus 16.25].
- Verkon ja verkkolaitteiden kuormitustilannetta seurataan, jotta mahdolliset ongelmat havaittaisiin ja korjattaisiin ennen kuin ne ehtivät haittaamaan merkittävästi organisaation toimintaa [Vaatimus 16.14].

Verkon valvonta ja hallinta voidaan tehdä itse tai se voidaan ulkoistaa kumppanin tehtäväksi. Mikäli valitaan ulkoistus, määritellään hyvin tarkasti se, miten ja mitä toimenpiteitä ulkoistuskumppani tekee, miten ja millä toimenpiteillä valvontaa ja hallintaa tehdään. Muuten riskinä on, että varsinkin verkon valvontaa ei tehdä riittävän hyvällä tasolla. Ulkoistettaessa organisaatio säilyttää kuitenkin itsellään riittävän perusosaamisen verkoista, jotta voi ostaa siihen liittyviä palveluita. [Vaatimus 16.9].

Verkkolaitteiden ohjelmistoista löydetään säännöllisesti tietoturvaongelmia samalla tavalla kuin muistakin tietoteknisistä järjestelmistä. Verkkolaitteiden ohjelmistot päivitetään valmistajan suositusten mukaisesti [Vaatimus 16.10].

Verkon hallinnan ja valvonnan määrämuotoistamiseksi, kattavuuden varmistamiseksi ja jatkuvuuden parantamiseksi käytetyt hallinta- ja valvontaprosessit on dokumentoitu asianmukaisesti [Vaatimukset 16.12, 16.13].

Verkon hallintaan ja ylläpitoon on käyttöoikeus vain niillä käyttäjillä, jotka tarvitsevat niitä työtehtävissään. [Vaatimus 16.16]. Verkon hallinta ja valvonta tehdään laitteilla, jotka on fyysisesti erotettu muista työasemista [Vaatimus 16.20]. Ylläpitopääsy verkon laitteille on rajoitettu verkon valvonta- ja hallintatyöasemille. Rajaus on toteutettu verkon sisällä sekä verkon ulkopuolella etäylläpidossa. [Vaatimus 16.24].

Verkon fyysiset komponentit käydään säännöllisesti läpi tarkastaen, että niiden rakenne vastaa dokumentaatiota. Tarkoituksena on löytää mahdolliset merkit murtautumisyrityksistä, kuten lukkojen väkivaltaisista rikkomisyrityksistä tai ylimääräisiä verkkolaitteita ja kaapeleita. [Vaatimus 16.19].

Verkon ylläpitäjä tarkistaa säännöllisesti verkon tietoturvallisuuden tason. Tarkistuksessa käydään läpi esim. laiteasetukset, verkon palvelut ja sellaiset käyttäjät, joilla on laajat oikeudet. [Vaatimus 16.22].

Tietoturvaongelmat ja -poikkeamat saattavat olla sellaisia, että käyttäjät havaitsevat ne nopeimmin. Tästä syystä käyttäjiä koulutetaan ilmoittamaan havaituista puutteista, ongelmista ja niiden epäilyistä esimiehelle, tietoturvavastaavalle tai verkon vastuuhenkilölle. [Vaatimus 16.23].

16.1 Teknologiaratkaisuja verkon hallintaan/valvontaan

Verkon hallinnassa ja tietoturvallisuuden seurannassa voidaan käyttää useita välineitä ja monesti käytetäänkin, sillä teknologiat eivät kata kaikkia tietoturvallisuuden osa-alueita. Valvontaa ja hallintaa voidaan teknologiamielessä tehdä usealla eri tavalla, mutta etukäteen on määrämuotoisesti valittu käytettävät teknologiaratkaisut ja luotu toimivat valvonta ja hallintamenetelmät, joita käytetään ohjeistuksen mukaisesti. Näin valvonta ja hallintakäyttöön ei oteta uusia sovelluksia hallitsemattomasti. [Vaatimus 16.21]. Verkon etäylläpitoon käytetään vain turvallisinta osajoukkoa niistä välineistä, joita käytetään

tavalliseen verkon ylläpitoon [Vaatimus 16.17]. Tällä hetkellä suositeltavat hallinta- ja valvontateknologiat ovat seuraavat

- **SSH/HTTPS:** Hallinta- ja valvontayhteyksissä käytetään salattuja protokollia, joissa käyttäjätunnistuksen lisäksi koko liikenne salataan, jolloin ulkopuoliset eivät pääse tarkkailemaan tai muuttamaan liikennettä [Vaatimus 16.4]. Mikäli käytetään salaamattomia protokollia, kuten Telnet, HTTP tai FTP, huolehditaan salauksesta muilla menetelmillä, kuten tunneloimalla yhteys salaavilla VPN-yhteyksillä.
- **SNMPv3:** Hallintaan ja valvontaan voidaan käyttää SNMP-protokollaa. Sen yhteydessä varmistetaan, että se on varmasti konfiguroitu oikein, jotta kaikki liikenne salataan ja käyttäjä tunnistetaan riittävän vahvalla menetelmällä, huomioi vaatimukset 11.6 – 11.9.
- **Lokit:** Valvonnassa voidaan käyttää laitteiden tekemiä lokeja, joita kannattaa keskitetysti seurata. Laitteiden lokiasetukset on määritetty sellaisiksi, että lokeista saadaan riittävästi tietoa verkon toiminnasta [Vaatimus 16.2]. Lokit kerätään erilliselle keskitetylle lokipalvelimelle, jossa niiden säilyttäminen ja analysointi on turvallisinta. [Vaatimus 16.1].
- **IDS/IPS:** Hyökkäyksien havaitsemiseen (IDS) ja hyökkäyksien torjumiseen (IDP) käytetään niihin tarkoitettuja laitteita ja ohjelmistoja, jotka tarkkailevat verkon liikennettä ja havaitsevat verkossa mahdollisesti käynnissä olevan hyökkäyksen. [Vaatimus 16.7]. IPS-järjestelmät lisäksi estävät havaitsemansa verkossa olevan hyökkäyksen. Suositus näiden menetelmien käyttöönottoon on aloittaa IDS-järjestelmästä ja vasta siitä saatujen kokemuksien jälkeen kannattaa siirtyä käyttämään IPS-järjestelmiä. Muuten riskinä on itseaiheutettu palvelun esto, jos IPS-järjestelmä estää liikenteen, joka haluttaisiin päästää läpi.
- **Valmistajakohtaiset ratkaisut:** Monesti verkkolaitteiden hallintaan ja valvontaan ei voida tehokkaasti käyttää muuta kuin valmistajakohtaisia ratkaisuja. Tällöin varmistetaan, että yhteys on riittävällä tasolla salattu ja käyttäjäntunnistus tehdään luotettavasti. [Vaatimus 16.4].

16.2 Hallinnan/valvonnan tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
16.1	Lokit tallennetaan keskitetylle lokipalvelimelle.	suositus	vahva suositus	pakollinen vaatimus
16.2	Laitteiden lokiasetukset on määritetty sellaisiksi, että lokeista saadaan riittävästi tietoa verkon toiminnasta	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
16.3	Muutokset verkkoon tehdään suunnitteluvaiheiden periaatteiden mukaisesti.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
16.4	Hallintaliikenne salataan riittävällä tasolla, jotta ulkopuolinen henkilö ei pysty seuraamaan tehtäviä muutoksia eikä tunnistautumaan hallintakäyttäjänä	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
16.5	Verkon hallinnan yhteydessä jokaisesta muutoksesta otetaan varmuuskopio	vahva suositus	vahva suositus	pakollinen vaatimus
16.6	Etukäteen on määritelty, mitä asioita verkossa valvotaan.	vahva suositus	vahva suositus	pakollinen vaatimus
16.7	Hyökkäyksien havaitsemiseen ja hyökkäyksien torjumiseen käytetään niihin tarkoitettuja IDS/IPS laitteita ja ohjelmistoja	suositus	vahva suositus	vahva suositus
16.8	Lokit suojataan muutoksilta.	vahva suositus	vahva suositus	pakollinen vaatimus
16.9	Ulkoistettaessa verkon hallinta, • Määritellään hyvin tarkasti se, miten ja mitä toimenpiteitä ulkoistuskumppani tekee, miten ja millä toimenpiteillä valvontaa ja hallintaa tehdään • Säilytetään itsellä riittävä perusosaaminen verkoista, jotta voidaan ostaa siihen liityviä palveluita	vahva suositus	vahva suositus	pakollinen vaatimus
16.10	Verkkolaitteiden ohjelmistot päivitetään valmistajan suositusten mukaisesti.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
16.11	Verkon hallintaan ja valvontaan on määritelty selkeät vastuuhenkilöt	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
16.12	Käytetyt hallintaprosessit on dokumentoitu.	suositus	vahva suositus	pakollinen vaatimus
16.13	Käytetyt valvontaprosessit on dokumentoitu.	suositus	vahva suositus	pakollinen vaatimus
16.14	Verkkolaitteiden kuormitustilannetta valvotaan.	suositus	vahva suositus	pakollinen vaatimus
16.15	Lokeista pystytään jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta (audit trail).	suositus	vahva suositus	pakollinen vaatimus
16.16	Verkon ylläpitoon ja tietoturvallisuuden määritysten muuttamiseen on käyttöoikeus vain niillä käyttäjillä, jotka tarvitsevat niitä työtehtävissään.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

16.17	Verkon etäylläpitoon käytetään vain turvallisinta osajoukkoa niistä välineistä, joita käytetään tavalliseen verkon ylläpitoon	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
16.18	Verkon lokeja ja erityisesti etäylläpidon lokeja käydään läpi säännöllisesti	suositus	pakollinen vaatimus	pakollinen vaatimus
16.19	Verkon fyysiset komponentit käydään säännöllisesti läpi tarkastaen, että niiden rakenne vastaa dokumentaatiota. Tarkoituksena on löytää mahdolliset merkit murtautumisyrityksistä. [merkkejä lukkojen väkivaltaisesta rikkomisesta tai ylimääräisiä verkkolaitteita ja kaapeleita]	suositus	vahva suositus	pakollinen vaatimus
16.20	Verkon hallinta ja valvonta tehdään laitteilla, jotka on fyysisesti erotettu muista työasemista.	suositus	vahva suositus	pakollinen vaatimus
16.21	Valvontaan ja hallintaan käytettävät sovellukset on määritelty	suositus	vahva suositus	pakollinen vaatimus
16.22	Verkon ylläpitäjä tarkistaa säännöllisesti verkon tietoturvallisuuden tason	suositus	vahva suositus	pakollinen vaatimus
16.23	Käyttäjät koulutetaan ilmoittamaan havaituista puutteista, ongelmista ja niiden epäilyistä esimiehelle, tietoturvavastaavalle tai verkon vastuuhenkilölle	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
16.24	Ylläpitopääsy verkon laitteille on rajoitettu verkon valvonta- ja hallintatyöasemille. Rajaus on toteutettu verkon sisällä sekä verkon ulkopuolella etäylläpidossa.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
16.25	Valvontaan käytetyillä tunnuksilla on vain lukuoikeus verkon lokitietoihin	suositus	vahva suositus	pakollinen vaatimus

17 Jatkuvuussuunnittelu

Jatkuvuussuunnittelu tarkoittaa niitä toimia, joiden avulla pyritään pienentämään ja lyhentämään toimintaa haittaavien tapahtumien vaikutusta ja aikaa. Se sisältää mm. järjestelmien rakenteeseen liittyviä toimenpiteitä, jotka parantavat niiden toimintaa häiriötilanteissa; toimenpiteitä, jotka parantavat toipumista ongelmien jälkeen sekä varalaitejärjestelyitä. Jatkuvuussuunnittelu kokonaisuutena sisältää myös ne suunnitelmat ja toimenpiteet, joilla toimintoja voidaan siirtää pois tietojärjestelmiltä tehtäväksi ihmisvoimin, mikäli tietojärjestelmät eivät toimi. Tässä ohjeessa käsitellään jatkuvuussuunnittelua vain teknisestä näkökulmasta.

17.1 Häiriötilanteet

Organisaatiossa on toteutettu ja vastuutettu järjestelmien häiriöiden selvitys ja niistä toipuminen. Organisaation kaikki järjestelmät ja toiminnot on luokiteltu niiden kriittisyyden mukaan. Perustuen kriittisyysluokitteluun ja analyysiin eri järjestelmien ja toimintojen kokonaistarpeesta, on muodostettu jatkuvuussuunnitelma ja toipumissuunnitelma, joka on johdon hyväksymä. [Vaatimus 17.1]. Organisaatio on ottanut jatkuvuussuunnitelmissaan huomioon sisäverkon erityispiirteet [Vaatimus 17.2]. Suunnitelmat sisältävät mm. häiriöitä ja keskeytyksiä ennaltaehkäisevät menetelmät ja ratkaisut, häiriöiden ja keskeytysten havaitsemiseen liittyvät menetelmät ja ratkaisut sekä vikatilanteen tilapäiseen korjaamiseen ja varsinaiseen normalisointiin tähtäävät korjaavat menetelmät ja ratkaisut [Vaatimus 17.3]. Jatkuvuussuunnitelma sisältää sekä teknisen että hallinnollisen puolen [Vaatimus 17.16]. Suunnitelman mukaiset menetelmät ja ratkaisut toteutetaan niin, että tavoiteltu valmiustaso todellisuudessa saavutetaan [Vaatimus 17.4]. Jatkuvuussuunnitelman mukainen toiminta testataan ja koulutetaan organisaatiolle sekä sitä harjoitellaan säännöllisesti [Vaatimukset 17.5 ja 17.18]. Jatkuvuussuunnitelma pidetään ajan tasalla ja päivitetään vähintään vuosittain [Vaatimus 17.6].

Organisaatio pitää hallussaan tarkoituksenmukaista määrää varalaitteita ja -osia kriittisimpien järjestelmien osalta tai huolehtii niiden sisältymisestä esimerkiksi huolto-/ylläpitosopimuksiin [Vaatimus 17.13]. Varalaitteita ja -osia voidaan järjestää ilman merkittäviä ylimääräisiä kustannuksia esim. käytöstä poistettavista

laitteista. Joissain tapauksissa tulevia hankintoja voidaan ennakoida ja mitoittaa siten, että hankitaan vastaava uusi laite, joka konfiguroidaan valmiiksi odottamaan tulevaa tarvetta. Varalaitteita voidaan säilyttää myös Suomen Huoltovarmuusdata Oy:ssä, josta saa lisätietoja Huoltovarmuuskeskuksesta.

Varayhteydet ja -kapasiteetti pidetään jatkuvasti aktiivisena kuormituksen tasaamiseksi ja varajärjestelyjen toimintakuntoisuuden varmistamiseksi [Vaatimus 17.19].

Toiminnan kannalta kriittiset palvelut on kahdennettu tai monistettu muutoin niin, että kriittiset palvelut ovat saatavissa useamman kuin yhden palvelimen kautta, huolehtien kuitenkin eheysvaatimuksista. [Vaatimus 17.20].

Käyttäjiä ohjeistetaan säilyttämään työtiedostonsa palvelimilla, jotta työaseman vikaantuessa tai kadotessa tiedostoja ei menetettäisi ja tarvittaessa tiedostoja voidaan käyttää toisen työaseman kautta. [Vaatimus 17.21].

Organisaatiolla on kirjallinen varmuuskopiointipolitiikka ja -prosessi [Vaatimus 17.14]. Palvelinten tiedostojen varmuuskopiointi on automatisoitu tapahtumaan riittävän usein (tavallisesti joka yö). Varmuuskopioinnin onnistumista valvotaan systemaattisesti. Palvelinten ja muiden verkkokomponenttien varusohjelmistoympäristöstä asetuksineen otetaan varmuuskopiot ennen olennaisia muutoksia, asennuksia tai vastaavia toimenpiteitä sekä edellä mainittujen toimenpiteiden jälkeen. [Vaatimukset 17.25 ja 17.26].

Varmuuskopiotallenteita säilytetään riittävän monta varmuuskopiosukupolvea palo- ja murtoturvallisessa paikassa [Vaatimus 17.8]. Tärkeimmistä järjestelmistä otetaan suojakopioita katastrofi- ja kriisitilanteiden varalta ja niitä säilytetään palvelimista niin etäällä, etteivät sekä palvelimet että suojakopiot voi tuhoutua samassa onnettomuudessa. [Vaatimus 17.15].

Varmuuskopioilta palauttamista testataan säännöllisesti. [Vaatimus 17.7].

Verkon hallinta on organisaatioissa monesti ulkoistuskumppanin vastuulla. Tällöin on mietitty tarkkaan, mitä osaamista halutaan pitää organisaation sisällä. Mikäli sisäverkon toiminta on organisaation toiminnalle kriittistä, säilytetään riittävä osaaminen organisaation sisällä tai sopimuksin varmistettava, että riittävä osaaminen ulkoistuskumppanilta on aina saatavissa. [Vaatimus 17.22].

Verkon vastuuhenkilöstöllä on edellytykset saattaa verkko toimintakykyiseksi. Tähän tarvitaan mm. riittävä osaaminen ja soveltamisen taito, varus- ja sovellusohjelmistot, konfiguraatiotietous, asetukset, käyttäjämäärittelyt ja tiedostoista otetut varmuuskopiot. Organisaatio pystyy itse toimimaan jatkuvuussuunnitelman mukaan ilman ulkopuolisten tahojen aktiivista toimintaa. Jatkuvuussuunnitelman tekninen toteuttaminen voi olla ulkoistuskumppanin vastuulla, mutta organisaation omalla vastuulla on se, että vakavan häiriön sattuessa pystytään organisaation kriittiset toiminnot hoitamaan kunnes sisäverkko saadaan jälleen normaalikuntoon. [Vaatimus 17.9].

Verkon häiriö- ja keskeytystilanteisiin sekä verkkohyökkäyksiin on varauduttu, järjestelyt on dokumentoitu, testattu ja ylläpidetty. Järjestelyillä varmis-

tetaan, että tilanteen korjaamisesta vastaava henkilöstö voi keskittyä ko. työhön. [Vaatimus 17.10]. Järjestelmien häiriöistä pidetään kirjaa ja käytetään tietoa hyväksi riskianalyyseissä ja palvelutasosopimusten teossa [Vaatimus 17.17].

Organisaation järjestelmät ovat tärkeydeltään hyvinkin erilaisia. Järjestelmät on luokiteltu tärkeysjärjestyksittäin perustuen ICT-varautumis- ja tietoturvatasoihin. Luokittelussa otetaan huomioon se, että monet järjestelmät vaativat muiden järjestelmien yhtäaikaista toimivuutta. [Vaatimus 17.12].

17.2 Poikkeusolosuhteet

Poikkeusoloihin varautumisen lähtökohtana on, että kriittiset toiminnot turvataan. Organisaation toiminnot ja tehtävät saattavat osittain muuttua tai painopiste vaihtua normaalioloihin verrattuna. Muuttuvat toiminnot ja tehtävät voivat joissain tapauksissa olla myös sellaisia, joihin ICT-pohjaisia sovelluksia ei tällä hetkellä edes ole.

Suunniteltaessa tietojenkäsittelyyn liittyvää varautumista poikkeusoloihin, on otettu huomioon sisäverkkojen erityinen rooli ja haavoittuvuus tiedonsiirtoväylänä [Vaatimus 17.11]. Suunnittelussa ja sitä edeltävässä analysoinnissa on otettu huomioon mm. [Vaatimus 17.23]:

- Organisaation toiminnan jatkuvuuden turvaaminen ja tehtävien suorittaminen poikkeusolojen vaikutuksista huolimatta
- Valtiovallan asettamien kriisiajan valmiusvaatimusten täyttäminen
- Välttämättömän tietojenkäsittelytoiminnan ylläpitäminen
- Tietojenkäsittelytoiminnan siirtojärjestelyihin varautuminen
- Tietojenkäsittelytoiminnan supistamis- ja korvaamisjärjestelyihin varautuminen
- Edellytysten luominen normaaliolojen tilanteeseen palaamiselle.

Normaaliolojen käytettävyyttä turvaavat varajärjestelyt on rakennettu niin, että ne tukevat myös poikkeusolojen vaatimuksia ja ratkaisuja [Vaatimus 17.24]. Esimerkiksi sopivia varalaitteita, -kaapeleita ja suojakopioita hyödyntämällä voidaan tilapäisjärjestelyin rakentaa hyvinkin nopeasti pienimuotoisia sisäverkkoja, jos fyysisiin turvajärjestelyihin voidaan luottaa. Poikkeusoloissa voidaan harkita suojaustason nostoa sekä verkkojen ja liikenteen jakamista normaalioloja pienempiin kokonaisuuksiin.

Tarkempia ohjeita tietoliikennettä ja tietojärjestelmiä koskevasta poikkeusoloihin varautumisesta antavat mm. valtiovarainministeriö, Huoltovarmuuskeskus sekä eri ministeriöt omilla hallinnonaloillaan (esim. kunkin ministeriön valmiuspäällikkö). Lisätietoa saa myös yhteiskunnan elintärkeiden toimintojen turvaamisen (YETT) -verkkojulkaisusta.

17.3 Jatkuvuussuunnittelun tarkistuslista

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
17.1	Organisaatiossa on toteutettu ja vastuutettu järjestelmien häiriöiden selvitys ja niistä toipuminen. Organisaation kaikki järjestelmät ja toiminnot on luokiteltu niiden kriittisyyden mukaan. Perustuen kriittisyysluokitteluun ja analyysiin eri järjestelmien ja toimintojen kokonaistarpeesta, on muodostettu jatkuvuussuunnitelma ja toipumissuunnitelma, joka on johdon hyväksymä.	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
17.2	Jatkuvuussuunnitelmissa on otettu huomioon sisäverkon erityispiirteet.	suositus	vahva suositus	pakollinen vaatimus
17.3	Jatkuvuussuunnitelma sisältää ennaltaehkäisevät ja havaitsevat menetelmät ja ratkaisut sekä tilapäiseen korjaamiseen ja varsinaiseen normalisointiin liittyvät menetelmät ja ratkaisut.	suositus	vahva suositus	pakollinen vaatimus
17.4	Menetelmät ja ratkaisut on toteutettu niin, että tavoiteltu valmiustaso todellisuudessa saavutetaan.	vahva suositus	vahva suositus	pakollinen vaatimus
17.5	Jatkuvuussuunnitelman mukainen toiminta testataan ja koulutetaan.	vahva suositus	vahva suositus	pakollinen vaatimus
17.6	Jatkuvuussuunnitelma pidetään ajan tasalla ja päivitetään vähintään vuosittain	suositus	vahva suositus	pakollinen vaatimus
17.7	Varmuuskopioilta palauttamista testataan säännöllisesti.	suositus	vahva suositus	pakollinen vaatimus
17.8	Varmuuskopiotallenteista säilytetään riittävän monta varmuuskopiosukupolvea palo- ja murtoturvallisessa paikassa.	suositus	vahva suositus	pakollinen vaatimus
17.9	Verkon vastuuhenkilöstöllä on edellytykset saattaa verkko toimintakykyiseksi. Organisaatio pystyy itse toimimaan jatkuvuussuunnitelman mukaan ilman ulkopuolisten tahojen aktiivista toimintaa.	suositus	vahva suositus	pakollinen vaatimus
17.10	Verkon häiriö- ja keskeytystilanteisiin sekä verkkohyökkäyksiin on varauduttu, järjestelyt on dokumentoitu, testattu ja ylläpidetty. Järjestelyillä varmistetaan, että tilanteen korjaamisesta vastaava henkilöstö voi keskittyä ko. työhön.	vahva suositus	vahva suositus	pakollinen vaatimus
17.11	Poikkeusoloihin varautumisessa on otettu huomioon sisäverkkojen erityinen rooli ja haavoittuvuus tiedonsiirtoväylänä.	suositus	vahva suositus	pakollinen vaatimus
17.12	Järjestelmät luokitellaan tärkeysjärjestyksittäin perustuen ICT-varautumis- ja tietoturvatasoihin	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
17.13	Organisaatio pitää hallussaan tai varaa laitetoimittajilta varalaitteet kriittisimpien järjestelmien rikkoutumisen varalle.	vahva suositus	vahva suositus	pakollinen vaatimus

17.14	Organisaatiolla on kirjallinen varmuuskopiointipolitiikka ja -prosessi.	suositus	vahva suositus	pakollinen vaatimus
17.15	Tärkeimmistä järjestelmistä on otettu suojakopioita, jotka säilytetään eri palotilassa kuin varsinaiset varmuuskopiot.	suositus	vahva suositus	pakollinen vaatimus
17.16	Jatkuvuussuunnitelma sisältää sekä teknisen että hallinnollisen puolen.	suositus	vahva suositus	pakollinen vaatimus
17.17	Järjestelmien häiriöistä pidetään kirjaa ja käytetään tietoa hyväksi riskianalyyseissä ja palvelutasosopimusten teossa.	suositus	pakollinen vaatimus	pakollinen vaatimus
17.18	Jatkuvuussuunnitelman mukaisia toimia harjoitellaan säännöllisesti.	suositus	vahva suositus	pakollinen vaatimus
17.19	Varayhteydet ja -kapasiteetti pidetään jatkuvasti aktiivisena	suositus	suositus	vahva suositus
17.20	Toiminnan kannalta kriittiset palvelut on kahdennettu tai monistettu niin, että kriittiset palvelut saadaan useamman kuin yhden palvelimen kautta	suositus	vahva suositus	pakollinen vaatimus
17.21	Käyttäjiä ohjeistetaan säilyttämään työtiedostonsa palvelimilla	suositus	vahva suositus	pakollinen vaatimus
17.22	Mikäli sisäverkon toiminta on organisaation toiminnalle kriittistä, säilytetään riittävä osaaminen organisaation sisällä tai sopimuksin varmistettava, että riittävä osaaminen ulkoistuskumppanilta on aina saatavissa	vahva suositus	pakollinen vaatimus	pakollinen vaatimus
17.23	Suunnittelussa ja sitä edeltävässä analysoinnissa on otettu huomioon muun muassa: • Organisaation toiminnan jatkuvuuden turvaaminen ja tehtävien suorittaminen • Välttämättömän tietojenkäsittelytoiminnan ylläpitäminenpoikkeusolojen vaikutuksista huolimatta • Valtiovallan asettamien kriisiajan valmiusvaatimusten täyttäminen • Tietojenkäsittelytoiminnan siirtojärjestelyihin varautuminen • Tietojenkäsittelytoiminnan supistamis- ja korvaamisjärjestelyihin varautuminen • Edellytysten luominen normaaliolojen tilanteeseen palaamiselle	vahva suositus	vahva suositus	pakollinen vaatimus
17.24	Normaaliolojen käytettävyyttä turvaavat varajärjestelyt on rakennettu niin, että ne tukevat myös poikkeusolojen vaatimuksia ja ratkaisuja	suositus	vahva suositus	pakollinen vaatimus
17.25	Varmuuskopioinnin onnistumista valvotaan systemaattisesti.	vahva suositus	vahva suositus	pakollinen vaatimus
17.26	Varmuuskopiot otetaan myös ennen olennaisia muutoksia ja niiden jälkeen.	vahva suositus	vahva suositus	pakollinen vaatimus

18 Lähde- ja viiteaineistoja

Alla on lueteltu lähde- ja viiteaineistoja, joita on käytetty tämän ohjeen työstämiseen ja joista voi hakea lisätietoa.

- Vanha lähiverkko-ohje: Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- ISO/IEC 27001
- ISF - The Standard of Good Practice for Information Security
- BSI IT-Grundschutz Manual 2005 (English)
- BSI IT-Grunschutz-Kataloge 2008 (Deutsch)
- COBIT 4.1
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681
- Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia (YETTS)
- Sähköisen viestinnän tietosuojalaki 16.6.2004/516
- Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030
- Kansallinen turvallisuusauditointikriteeristö (KATAKRI)

19 Valtiovarainministeriön antamia tietoturvaohjeita

Alla on lueteltu voimassaolevat VAHTI-ohjeet. Tummennetut dokumentit ovat erityisen oleellisia sisäverkkojen kannalta, ja niihin on tässä ohjeessa viitattu useaan otteeseen.

- **Sisäverkko-ohje, VAHTI 3/2010**
- **Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010**
- Lokiohje, VAHTI 3/2009
- **ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin, VAHTI 2/2009**
- Hankkeen tietoturvaohje, VAHTI 9/2008
- Valtionhallinnon tietoturvasanasto, VAHTI 8/2008
- Informationssäkerhetsanvisning för personalen, VAHTI 7/2008
- **Valtionhallinnon salauskäytäntöjen tietoturvaohje VAHTI 3/2008**
- Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008
- Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007
- **Älypuhelimien tietoturvallisuus - hyvät käytännöt, VAHTI 2/2007**
- Osallistumisesta vaikuttamiseen - valtionhallinnon haasteet kansainvälisessä tietoturvatyössä, VAHTI 1/2007
- Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006
- Tietoturvakouluttajan opas, VAHTI 11/2006
- Henkilöstön tietoturvaohje, VAHTI 10/2006
- **Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006**
- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
- Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006

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

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin 09 160 01
Telefaksi 09 160 33123
www.vm.fi

3/2010
VAHTI
Joulukuu 2010

ISSN 1455-2566 (nid.)
ISBN 978-952-251-138-6 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-139-3 (pdf)